Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

Survey: Video Authentication and Tampring Attacks

Ankit N. Patel[1], Prof. Swati D. Bendale[2]

Department of Information Technology (System and Network Security),
Sardar Vallabhbhai Institute of Technology, Vasad, Gujarat, India-388306

Abstract- *In recent years, development in sophisticated video editing technology and wide use of video in our society, it is becoming important to assure the trustworthiness of video. Therefore in court of law, surveillance and other fields video content must be secured against tampering or alteration so video authentication is required. Video authentication means to check the trustworthiness of the video by verifying the integrity and source of video data. There are three main techniques of video authentication: Digital signature, Watermarking and Intelligent technique. In this paper we present a brief detail of these video authentication techniques, why video authentication is required and video forgery. We also give the advantages and disadvantages of these techniques.*

Keywords**:** *Video Authentication, Watermarking, Digital Signature, Intelligent Techniques, Forgery Attacks.*

I. INTRODUCTION

Authentication means to verify the truth of entity. In today's digital world video data is useful in many applications such as video surveillance, video broadcasting, DVDs, video conferencing, and video on demand applications where the authenticity and integrity of video data is required[4]. Alteration of digital media is very easy through the video editing software. In several applications the reliability and integrity of video data is most important such as forensic investigation, law enforcement or court of law to prove the crime activity of criminal and get punished[5]. So video authentication is the process which ascertain that the content of given video data is authentic and exactly same as when captured[4].

Why Video Authentication is Required?

Video data can be altered using sophisticated video editing software without leaving any hint of alteration or tampering. So we cannot assure that video is original or not[5]. To detect the tampering or alteration and prevent the different types of forgeries performed on video, video authentication techniques are required. In the case, when video is used as evidence in court of law, reliability and integrity of video must be verified. If video is tampered then criminals get free from being punished[4]. The aim of this paper is to examine issues of different video authentication techniques and shows their advantages and disadvantages. In section I present introduction of video authentication and discuss why video authentication is required. Section II defines the different video forgery. Section III describes the different video authentication techniques with their advantages and disadvantages.

II. VIDEO FORGERY

Video forgery is nothing but tampering or alteration the video by modifying the content of the video or changing the content of the video. The aim of the forger is to create fake video from original video. This forger video is presented in court of law to mislead to court's process or giving the wrong decision[3]. There are several methods of for video forgery, which are presented below.

A. Forgery Attacks

Video Forgery or tampering can be classified into three attacks[14].

1. Spatial Tampering Attack
2. Temporal Tampering Attack
3. Spatio-Tamporal Tampering Attack

i. Spatial Tampering Attack:

A forger can attack on video by manipulating pixel bits of the video frame. These attacks can be performed using video editing software. There are three types of spatial tampering attack.

Object Addition:

In this attack, object is inserted into a frame or set of frames. For example, if any video which is used as evidence in

court, an additional object can be inserted into frames using editing software. Because of these tamper video crime cannot proved and criminal get free from being punished.

Object Removal:

In this attack, object of the frame of video are removed or deleted. This attack is done if someone try to hide his/her presence in the video for a specific time. This attack performed on both foreground and background objects.

Object Modification:

In this attack, an existing object of the frame can be modified so that original object is changed. For modification of object, the size and shape of the object may be changed; the color of the object may be changed. This type of attack is very difficult to detect.

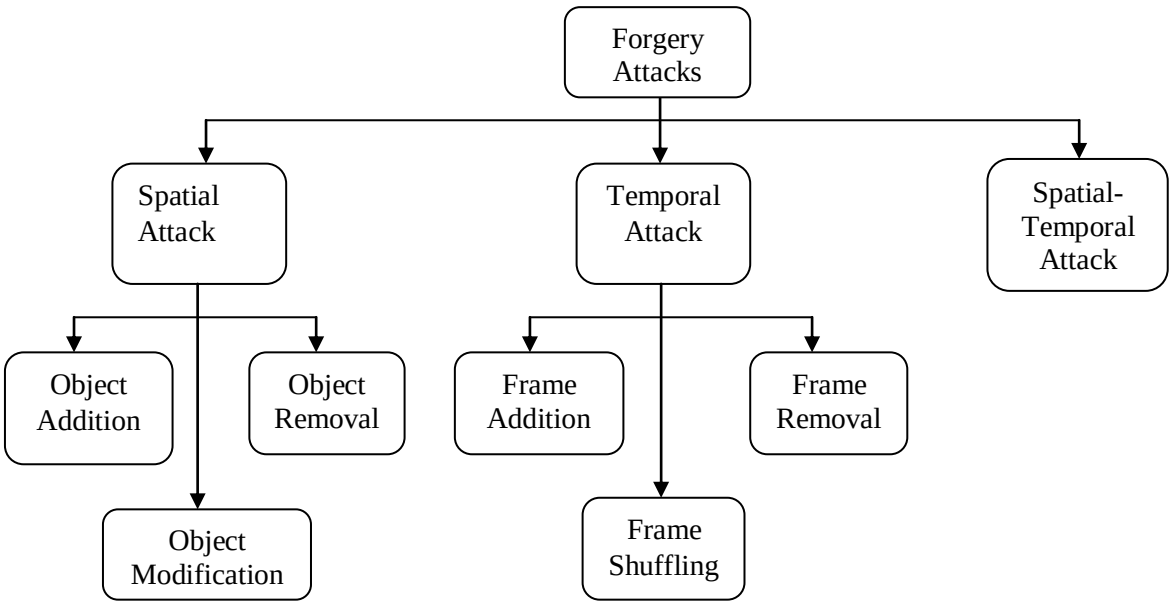

Fig. Video Forgery Attacks.

ii. Temporal Tampering Attack:

This type of attack is done on the frame and sequence of frame. There are three types of attack.

Frame Addition:

In this attack, add the frame from another video which has same properties into original video at some random location.

Frame Removal:

In this attack, frames of video are removed from a specific location or can be removed from different locations.

Frame Shuffling:

In this attack, frames of video are shuffled or reordered. When this attack is performed fake video is produced.

iii. Spatio-Temporal Tampering Attack:

It is a combination of spatial and temporal tampering attack. The sequence of frames is changed and graphics of the frame are changed.

III. VIDEO AUTHENTICATION TECHNIQUES

There are three main techniques of video authentication[5].

I. Digital Signature

II. Watermarking

III. Intelligent Technique

Out of these three techniques, digital signature and watermarking are widely used for video authentication.

3.1 Digital Signature:

Digital signature method introduced by Diffie and Hellman in 1976. Integrity of video can be verified using the digital signature method. Sender firstly encrypted the data using it's private key and at the receiver side, receiver decrypt these data using sender's public key. The advantage of this technique is that it is a very simple and easy technique and main disadvantage of this technique is that it might detect the modifications file but it cannot find the regions where the image has actually been modified[14].

3.1.1. Structural Digital Signature:

For incidental manipulations structural digital signature can be used for image authentication. This approach makes use of an image's content to construct a structural digital signature (SDS) for image authentication. In this approach many incidental manipulations which can be detected as malicious modifications in other digital signature verifications, can be ignored[14].

3.1.2. Content Base Digital Signature:

Content based digital signature approach for image/video authentication using edge characteristics. In this scheme to generate a digital signature by encrypting the feature points positions in an image. In this approach authentication is accomplished by comparing the positions of the feature point extracted from the targeted image with those decrypted from the previously encrypted digital signature[14].

In [1] S. Bhattacharjee and Martin Kutter proposed a digital signature technique for compression tolerant image authentication. These image authentication technique consist of two processes: (i) Digital signature generation process (ii) Verification of digital signature. There are two steps for generating the digital signature of image. Firstly extract the coordinates of the image which gives the feature of image. There are many techniques available for feature extraction process. In second step these extracted feature is encrypted with a public key encryption technique such as RSA. Result we get digital signature for image, it can then stored in database for verification process. Now in verification process we can test the authenticity of image A, which is unmodified version of other image A'. To verify the integrity of image A, firstly we extract the key features of image A. Now digital signature of image A' is decrypted to obtain the features of image A'. If features are match then image A' is considered as authentic. If features do not match then image is consider as modified and not authentic.

Author in [2] proposed a scheme for video authentication in which two processes is done: digital signature generation and authentication process. In first process, video is divided into different shots. For each video shots find the key frame (Ki). After that quantize the luminance values for all the frames(key frames and non key frames). Now compute the signature at three level: key frame level, shot level and video level. Key frame level signature called key-secret (Sk) which is computed using non key frames. We have now key secret so we can generate signature at shot level using key frame (Ki) and key secret (Sk) for all shots. Finally compute signature at video level which is called master secret from all shot secret. And master secret is encrypted using a private key to form the signature for video. Second process is authentication process, it also done at three level at key frame level, shot level and video level.

3.2 Watermarking:

Watermarking is a process of hiding a predefined logo or image into multimedia data like image/video. Watermark logo or image is embedded in multimedia data in a way that quality and imperceptibility of media is preserved. The main advantage of watermarking is that it can be embedded without degrading the quality of multimedia data too much[7].

There are many applications of digital watermarking[6].

- Content Archiving
- Copyright protection
- Broadcast monitoring
- Tamper detection
- Digital fingerprinting
- Authentication and Integrity

Digital Watermarking has two processes: Watermark embedding and Watermark extraction process. There are two types of watermarking techniques.

- Spatial Domain Technique

- Frequency Domain Technique

3.2.1. Spatial Domain Technique:

In spatial domain technique, watermark is embedded into image by changing the values of luminance and chrominance of the selected pixels. The main advantages of spatial domain technique are its low computational complexity and simplicity. These techniques consume a less time than frequency domain technique but spatial domain technique is less robust to the attacks then the frequency domain techniques. The most known method of spatial domain technique is LSB (least significant bit)[6].

Least Significant Bit (LSB):

These method embed a watermark in LSB of randomly chosen pixels of original image. Each pixel of original image is presented by 8-bit stream, watermark is embedded in LSB of selected pixels of original image. This method is easy but it is not very robust against the attacks. The advantage of this method is that it does not affect the quality of original image after embedding the watermark[6].

3.2.2. Frequency Domain Techniques:

Frequency domain techniques are more robust than the spatial domain techniques. In this technique, manipulation of watermarking is more difficult than in spatial domain technique. The known method of frequency domain is Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Singular Value Decomposition (SVD)[7].

Discrete Wavelet Transform (DWT):

Wavelets are the functions that are used for signals representation. DWT is decomposed a image in to the low frequency, high frequency and middle frequency bands. After that watermark image is embedded into these frequency bands. DWT is mostly used for watermarking because of multi-resolution analysis. The disadvantages of DWT are: it is more complex and it takes longer computation time and computation cost is also high[8].

Discrete Cosine Transform (DCT):

DCT is used for transformation signal from spatial domain to the frequency domain. DCT decompose image into different frequency band for embedding the watermark. Firstly image is segmented into 8×8 non overlapping blocks. After that DCT is applied on that block and get high and low frequency band. Now embedding the watermark into frequency bands[10]. DCT is robust against the attacks like low-pass filtering, brightness and contrast adjustment, blurring etc. It is not more robust against geometric attacks like rotation, scaling, cropping etc[11].

Discrete Fourier Transform (DFT):

DFT technique is divides into two types: first technique is to direct embedding and second technique is template based embedding. Magnitude and Phase coefficient are modified for embedding process in direct embedding technique. Where template based embedding technique propose the idea of template. The main advantage of DFT is that it can robust against the geometric distortion. And the main disadvantage of DFT is that output of DFT is always a complex value, required more frequency rate and bad computational efficiency[6].

Singular Value Decomposition (SVD):

In SVD method, image will be treated as a matrix, this image or frame is broke by SVD method directly into three matrices like U, S and V, where U and V are unitary matrix and S is diagonal matrix. After that embedding watermark into the singular values of these diagonal matrix (S) because changes in the matrix S does not affect the true quality of video frame[13]. SVD method is robust against small rotations, resizing and flipping of video frame[12].

3.3 Intelligent Technique:

Intelligent technique is not used as much as other techniques for video authentication. In[14] intelligent technique, use database of videos which consist of original videos and tampered videos. For the identification of original and tampered videos, this method uses a support vector machine (SVM). SVM is powerful methodology for solving problems in non linear classification, function estimation and density estimation. Intelligent technique has two steps: (i) SVM training and (ii) Tamper detection and classification. In first step, if video is tampered then assigned a -1 label to it and if video is original then assigned +1 label to it for training of SVM. Relative correlation data between two adjacent frames of video is computed from the training videos by using corner detection algorithm. The equation for compute relative correlation is:

$$\text{RC} : \frac{1}{m} \sum_{i=1}^{m} Li$$

Where Li is local correlation between two frames for i= 1, 2….m. Here m is number of corner points in these two frames. These RC is calculated for each video. Label information with RC for all videos are provided as a input to the SVM. Now SVM is classify the tampered video and non tampered video. The main advantage of this technique is that it

does not require the computation and storage of secret key or embedding of watermark. The main drawback of this technique is that we need database comprises of authentic video clips and tampered video clips[14].

In [8] proposed a Discrete Wavelet Transform (DWT) method for video watermarking. In this method DWT is applied on frames of video and find the low frequency and high frequency component for this frame. Watermark image and binarized low frequency component is used for generating the key during embedding process and these key is used for extract the watermark during extraction process. In these paper blind watermarking is used which requires only key to extract the watermark during extraction process. To check the robustness of algorithm compares the extracted watermark and original watermark using parameter. This method is not robust against frame dropping attack.

In [15] proposed a Digital Watermarking Technique using Discrete Cosine Transform (DCT). This method is based on image segmentation and DCT technique. In this technique firstly frame of video is segmented and then for each segment is subdivided into pixels blocks of 8×8 size. After that DCT is computed for each block and embed the pseudorandom sequence in DCT domain of each segment. To get the watermarked image reverse process is performed.

In [16] proposed watermarking using combination of three technique Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition. In embedding process DWT is applied on frame and get high frequency, mid frequency and low frequency component now select high and mid frequency component and applied DCT on it. SVD is performed on DCT coefficient. Same process also applied on watermark image and embeds singular values of watermark image into singular values of frame. Embedded watermarks are extracted with inverse process of embedding. This method is not robust against the frame dropping attack.

To solve this problem of frame dropping attack, use scene change detection and scrambling watermark technique with Discrete Wavelet transform (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD).

IV. CONCLUSION

Now a day's, where fast development in video editing software and easily availability this software, video authentication is very important because video have several application such as forensic investigations, court of law, video surveillance where the authenticity and integrity of video is very important. So in these paper, propose some techniques for video authentication like digital signature, watermarking and intelligent technique. Out of all this techniques, watermarking is widely used technique for video authentication purpose.

VII. ACKNOWLEDGEMENT

Second author of the paper offers the sincere gratitude to the Head of the Department and faculty members in Department of Information Technology of Sardar Vallabhbhai Patel Institute of Technology for the constant encouragement and unparalleled support provided throughout the period of this research work.

REFERENCES

[1] Sushil Bhattacharjee, Martin Kutter," Compression Tolerant Image Authentication" IEEE 1998.
[2] Chih-Hsuan Tzeng, Wen-Hsiang Tsai, "A New Technique For Authentication of image/video for Multimedia Applications", MM & Sec 2001: 23-26.
[3] Aldrina Christian, Ravi Sheth,"Digital Video Forgery Detection and Authentication Technique - A Review" IJSRST 2016.
[4] Saurabh Upadhyay, Sanjay Kumar Singh, "Video Authentication- An Overview", IJCSES 2011.
[5] Zarna Parmar, Saurabh Upadhyay," A review on video/image authentication and tamper detection techniques", IJCA 2013.
[6] Ritu Rawat, Nikita Kaushik, Soumya Tiwari," Digital Watermarking Techniques", IJARCCE 2016.
[7] Smita Pandey, Rohit Gupta,"A Comparative Analysis on Digital Watermarking with Techniques and Attacks", IJARCSSE 2016.
[8] Sneha Kadu, Ch. Naveen, V. R. Satpute, A. G. Keskar," Discrete Wavelet Transform Based Video Watermarking Technique", IEEE 2016.
[9] Shaikh Shoaib , Prof. R. C. Mahajan," Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT", IEEE 2015.
[10] Shinfeng D. Lin and Chin-Feng Chen, "A Robust DCT based watermarking for copyright protection", IEEE 2000.
[11] Bhupendra Ram," Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", IJART 2013.
[12] Tomas Kanocz, Peter Goc-Metis, Patrik Gallo, Dusan Levickey," Real-time Digital Video Watermarking Based on SVD",IEEE 2011.
[13] Lama Rajab, Tahani Al-Khatib, Ali Al-Haj." Video Watermarking Algorithms Using the SVD Transform" EJSR

2009.
[14] Saurabh Upadhyay, Sanjay Kumar Singh," Video Authentication: Issues and Challenges", IJCSI 2012.
[15] Mrs. Deepati Agrawal, Mr. Vikas Gupta, Mr. Gaurav Mehta," Digital Watermarking Technique using Discrete Cosine Transform" IJEIR 2013.
[16] C. N. Sujatha, P. Satyanarayana," High Capacity Video Watermarking based on DWT-DCT-SVD", IJSETR 2015.