© 2016 IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Digital Video Forgery Detection and Authentication Technique - A Review

Aldrina Christian[1], Ravi Sheth[2]
[1]M. Tech. Student, Department of Information Technology, Raksha Shakti University Ahmedabad, Gujarat, India
[2]Asst. Prof. Department of Information Technology, Raksha Shakti University Ahmedabad, Gujarat, India

ABSTRACT

Digital video is very important in day to day life. It is important in multimedia data for creating, processing, transmitting and storing digital information in many forms like image, audio, and video. The invention of video editing technology, video are used in a wide spread. Digital video is useful in education, medical treatment, and various another field. Unauthorized alteration or modification is done by an attacker to maliciously forge a video sequence for video forensic e.g. Frames are repeated, cropping the frame, copying the frame, deleting the frame. In this paper present review of several video forgery detection methods, those are used to find whether the video is real or fake and video authentication technique.

Keywords : Digital Video, Multimedia Data, Video Forensic, Frames, Video Forgery Detection, Video Authentication Technique

I. INTRODUCTION

The Internet is used by most of the people and they watch a movie and download that movie also. And the movie is digital video. Digital videos are easily available and easily downloaded also. And these digital videos are made up with the use of cameras, camcorders, CCTV and smartphone also. Developments of digital technologies like the transmission of video, video conferencing, compressed video have helped in many ways. Videos are shared on social networking website like YouTube, Facebook, Whatsapp, gender, IMO etc. Additional used in Bollywood, Hollywood, legal evidence, Advertisement, educational video tutorial, online education etc. indicate their extraordinary role in today's environment [1]. A coin has always two sides, so every good thing has some darker side also like misuse video like a wrong projection of data through the use of video. One is video tampering where an attacker can intentionally modify the original video to create tampered video or doctored video for misuse [1-3]. Video are seen in television, Internet website like YouTube have been tampered their authenticity can no longer always be taken for granted [4]. Video are taken from smartphone, mobile, digital camera, CCTV can serve very powerful evidence in legal court. It is asked to users that video are taken is really authentic or not. Video editing tools are available in the market. Forger can tamper the video by himself or any tech savvy person who are professionally done video editing. The authenticity of the video is needed to be examined in court means law enforcement, defense planning, defamation, politics etc. The authenticity of video is needed to be examined by an expert or any forensic tool that video tampers or not. Here how the attacker is intelligently tampered the video that forensic tool cannot be identified and detect video is genuine. Due to lack of a method for examining tampered video or authenticity of the video, videos are becoming a challenge before scientist or scientific community. This paper is a review of various methods that have been suggested to detect forgery in the video.

II. METHODS AND MATERIAL

1. Forgery in Video

Forgery in the video is nothing but tampering the video by modifying the content of the video or changing the content of the video. This can be done by various

methods which are presented below subsection. Tampering the video, the aim of the forger or attacker is to create tampered or doctored or fake video from original video. The original video is the source to create tampered video. The seriousness of the forged video is where to use tampered video. This tampered video is presented in court to mislead the court's process or giving the wrong decision. Because that tampered video is presented as evidence in a court trial. And authenticity is to be examined before allowing for the video in court as evidence [4].

A. Forgery attack on video

Video forgery or tampering can be classified in three ways: Spatial tampering attack, Temporal tampering attack and Spatio-temporal tampering attacks [4][5].

1) Spatial tampering: A forger can attack source of the videos are spatially by manipulating pixel bits within the video frame. In tampering attack the process that can be done in spatial tampering are added, delete , crop , replace the content etc. This attack can be performed by video editing software [04][05].
2) Temporal tampering: This type of attack is done in the sequence of frames. These attacks are mainly distressing the time sequence of visual data, captured by recording devices of the video. The attacks in temporal tampering are an addition, deletion and of frame reordering or shuffling [04][05].
3) Spatio-Temporal Tempering: This type of attack is the combination of the spatial and temporal kinds of tampering attacks. The sequence of frames are changed and graphic of the frames are changed in the same video [04][05].

B. Level of tampering attack

1) Scene level: the Whole scene of the video sequence is manipulated in such a way that not even the scene itself is altered but the scene of the video is altered. Copying of a video scene to another place or delete a scene. In this spatial and temporal both kinds of tampering can be done at the scene level.
2) Shot Level Tampering: In shot level tampering, a particular shot of the given video is altered. In shot level tampering shot can be added or deleted from the video. It can be performed at spatial as well as temporal both kind of tampering.
3) Frame Level Tampering: In Frame level tampering, the alteration is done on video's frames. The attacker may delete the frames, add the frames, reshuffle the sequence of frames, and replicate the frames from a given video to change the contents of the video. This can be done using temporal tempering.
4) Block Level Tempering: In Block level Tempering, the content of the video frames are treated as blocks. And on which the tampering attacks are applied. Blocks mean a specific part of the video's frame can be replaced, cropped, altered or modified in block level tampering. Block level tampering attacks are commonly performed at spatial tampering.
5) Pixel Level Tempering: In pixel level tampering, the content of the video frames are altered at the pixel level. The video authentication system should be strong enough to differentiate the regular video processing operation and pixel level tampering since normal video processing operations are performed at the pixel level. Pixel level attacks are performed at spatial tampering. [04][05]

2. Video Forger Detection

A. Camera-based coding detection techniques.
B. Detection based coding artifact techniques.
C. Copy-move detection in videos.

A. Camera Based Coding Detection

Camcorders leave a fingerprint in recorded videos. Mondaini et al. [07] suggested a straight application of the PRNU fingerprinting method to video sequences: the distinctive pattern of the camcorder is projected on the video's first frame. And it is used to detect several types of attacks. Specially, authors evaluate 3 correlations coefficient:

1) The one between every single frame noise and the reference noise.
2) The one between noises of two consecutive frames.
3) The one between frames without noise extraction.

This correlation coefficient is the threshold to get a binary event and various combinations of binary events allow detecting a different kind of tampering.

Hsu et al. **[08]** accept a technique of noise residues constructed on temporal correlation, where it is defined as what remains after deducting from the frame it's without noise. Each and every frame is divided into blocks, and on temporally, neighboring blocks evaluated the correlation between the noise residues. When the attack is in a region between temporal noise residues the correlation value will be drastically changed, and pixels will be decreased of the blocks are pasted from another region or frame, while it will be raised up to 1 if a frame repetition occurs. But this algorithm is successes only 55%. Hence it can be stated that camera based methods are effective on uncompressed videos.

B. Detection Based on Coding Artifact

Digital videos are usually compressed with H-26x or MPEG-x coding standard. The tampering has to be able in the uncompressed area in order to perform the processes such as frame deletion, frame insertion etc. It includes size and format, the tempered video has to be encoded. Double compression might expose digital forgery. The I-frames of the video are considered, and the two quantized DCT coefficient's histogram is studied in order to check a convex pattern that describes double encoded video [9]. Benford's law is presented in [10], I-frames first digit distribution of DCT coefficients is considered and extracted 12-dimensional feature and classified using Support Vector Machines. Detecting double encoding method classifies the second encoding as being at a lower or higher bitrate with respect to the first one. Whereas, this method may not work when the two encoding are done using a different implementation of the MPEG-2standard. In [11], based on Markov statistics extracted from DCT coefficients. Above works are for double compression detection, and not for forgery localization. In tampering detection, an effective method for detecting deletion of frames [12], where the de-synchronization between the GOP(Group of pictures) used for the first and for the second encoding by examining for a periodic performance in the magnitude of motion vectors is detected.

C. Copy Move Detection in Videos

Copy-move attacks are defined for inter and extra frame techniques of video. An intra-frame means copy-move attack is for still images and replicating a portion of the frame in the frame itself the goal is usually to hide or replicate the object. An inter-frame consists in replacing some frame with a copy of previous ones. It is used to hide some data that are in the real video. There is few video copy-move forgery detection techniques. The video copy-move forgery is addressed in [14] [15]. The authors in [14], use both temporal and spatial correlation to detect duplication. A temporal correlation is computed between all frames in a given sequence of frames and spatial correlation is computed for each frame in a given sequence. Both spatial and temporal correlation matrix is used to detect duplication. The detection performance is good for detecting frame replication; the region replication detection efficiency is very little for small forged regions such as 64 × 64. In [15], the authors the detection of forged area created on the discrepancies of noise features, which occur due to the forged areas from different videos. Noise properties are depending on camera's properties. When the forged patch comes from the same video the noise characteristics are not useful. The noise characteristics may not be projected correctly under the low compression rates.

3. Video Authentication Techniques

A. Digital Signature

The digital signature invented by Diffie and Hellman in 1976. The digital signature shall depend on secret data which is known by signer [16]. So it cannot be forged and the judge can confirm that the content of video data matches the data contained in the digital signature. The sender first removes the key from the original video and then the data encrypted by a private key that give signature [19]. The receiver can use sender's public key to decrypt the signature to authenticate the received video. The signature is stored somewhere else than the media [19]. And it stored separately in user defined field. Because the video is stored in a specific format, and the digital signature is being embedded in the video [16]. Chih-Hsuan Tzeng and Wen-Hsiang Tsai [17], has presented a new authentication scheme which uses new type of digital signature, which works for color and geometric visual appearance, and prevents an explosion of the signature size in the meantime [17]. They proposed technique composed of two processes,

signature generation and authentication using authentication and tamper localization.

1) Signature generation: In digital signature generation process, the algorithm of edge detection was applied to classify each non-overlapping block with same size n×n in two types, smooth block, and edge block [17].

This size is fixed as a standard unit to detect tampering.

The pixel value of the standard deviation feature was used in a smooth block. The feature was encoded with a digital signature. A precedent bit with value zero was set to specify the existence of a smooth block. Blocks of edge contain more details and have greater color variances than the smooth blocks and it is neither sufficient nor efficient to signify edge blocks using only color information [17].

2) Authentication Process: The features of the video are compared with the features recorded in the corresponding digital signature. It will display that the particular video is tampered [17]. The decryption key is used in the process decrypts the digital signature. Accept block classification is performed on the block B of a frame, and the result B' was derived. And this result might not be similar as the block type B [17]. The verification process was performed on four combinations of these two types of block.

- ✓ B and B’ are new blocks.
- ✓ B and B' are edge blocks.
- ✓ B is a smooth block and B' is an edge block
- ✓ B is an edge block and B' is a smooth block.

The SHA algorithm was applied for hashing function and digital signature.

B. Watermarking

In watermarking, the data used as authentication is embedded with multimedia data**.** Various watermarking schemes are proposed to prevent illegal copying and malicious modification. The watermarking methods work on either uncompressed or compressed information [18]. For copyright-related applications, to be protected from different types of malicious attack the embedded watermark is required. The watermarking techniques can be working in spatial or frequency domain using various transforms like Fourier, DCT, DWT etc. [18].

1). Watermarking technique for spatial domain: The watermarking technique is implemented using these steps.

- ✓ Convert Video Color Space
- ✓ Motion Estimation
- ✓ Block Selection Criteria
- ✓ Generation of watermark
- ✓ Embedding of watermark
- ✓ Extraction of watermark
- ✓ Quality Measurements

The authors in [18] have implemented the steps that are used to embed the watermark with the input video.

- ✓ Extract loaded the color video into frames.
- ✓ Block matching motion applied in estimation techniques on the succeeding frames.
- ✓ Select only those frames that have enough number of motion blocks which is well-matched with the watermark size.
- ✓ From the selected frames to select the best blocks to use threshold during the matching process use a given threshold.
- ✓ Perform the wavelet transformation on the selected finest blocks.
- ✓ Random Gaussian distribution is embedded as a proposed watermark into the selected blocks (Apply only to the LH and HL wavelet bands).
- ✓ Extract the watermark which is embedded.
- ✓ Apply some attacks on the watermarked frames into the video.
- ✓ The conducted results are evaluated using PSNR for embedding and similarity for the extracting process before and after attacks.

2) Watermarking technique for Frequency domain : In the frequency domain the video watermarking scheme follows the same steps used for the spatial domain [18], but the watermark is embedded and extracted to/from the wavelet blocks (HL and LH) bands. The HL and LH bands are embedded with watermark because of two reasons:

- ✓ LL band consists of a large amount of energy in the signal. So, if there is an abrupt motion in the video frames, the inserted at watermark cannot

be robustly extracted when it is threatened by attacks [18].

- ✓ HH band consists only of some details data and it is fragile to embed a watermark in it [18].

A recoverable image authentication algorithm based on digital watermarking is proposed in [19]. In this method, the image was first fragmented into separate, equal size and was examined to acquire two set of information**:** one for tamper detection and other for image recovery [19]. In tamper detection, between image blocks, the relations were recognized in order to depress an opponent's attempt to alter the image [19]. In addition, the designed authentication system was tactless to the regular image processing operations. Moreover, in order to attain the improved recovery result, a block of the image with more complex contents referred to as an edge block was further divided into sub-blocks [19].

III. CONCLUSION

There are many numbers of video forgery detection and authentication mechanisms and techniques have been discussed. Video tampering is done by different methods so there should be many different methods to detect video forgery. No single detection method works best for every condition. So which video forgery detection method is appropriate for a given situation depends on the following reasons such as:

Video forgery Techniques, Available technology, Computational restrictions, Video quality, Video formats.

So, it is necessary to understand the requirement as described above in video forgery detection. Video forensic is hot research issue in signal processing. And this, the paper represents different authentication techniques offered by the researchers, which are mainly classified into digital signature based and watermarking based. It is essential that the information represented is safe to the different kind of manipulations to some extent. Besides, these techniques are not only limited to video but also can be applied on images.

IV. REFERENCES

[1] A. Rocha, W. Scheirer, T. Boult, S. Goldenstein, "Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics", ACM Computing Surveys (CSUR), Volume 43 Issue 4, October 2011, Article No. 26, doi: 10.1145/1978802.1978805.

[2] Redi, J. A., Taktak, W., and Dugelay, J. L., "Digital image forensics: a booklet for beginners," Multimedia Tools Appl, Vol. 51, Issue 1, Jan 2011, pp. 133–162. DOI: 10.1007/s11042-010-0620-1.

[3] Wang, W., "Digital video forensics," Ph.D. dissertation, Department of Computer Science, Dartmouth College, Hanover, New Hampshire, June 2009.

[4] Saurabh Upadhyay, Sanjay Kumar Singh, "Video Authentication: Issues and Challenges" in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012 ISSN (Online): 1694-0814.

[5] Peng Yin, Hong heather Yu, "Classification of Video Tampering Methods and Countermeasures using Digital Watermarking ,"Proc. SPIE Vol. 4518, p. 239-246, Multimedia Systems, and Applications IV.

[6] Mondaini, N.; Caldelli, R.; Piva, A.; Barni, M.; Cappellini, V.: Detection of malevolent changes in digital video for forensic applications, in Proc. of SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX, E. J. D. III and P. W.Wong, eds., vol. 6505, no. 1,SPIE, 2007, 65050T.

[7] Hsu, C.-C.; Hung, T.-Y.; Lin, C.-W.; Hsu, C.-T, "Video forgery detection using correlation of noise residue", in 2008 IEEE, 10th Workshop on Multimedia Signal Processing, October 2008, 170–174.

[8] J. Xu, Y. Su, and Q. Liu, "Detection of double MPEG-2 compression based on distributions of DCT coefficients," International Journal of Pattern Recognition and Artificial Intelligence, vol. 27, no. 01, p.1354001, 2013.

[9] T. Sun, W. Wang, and X. Jiang, "Exposing video forgeries by detecting MPEG double compression," in Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on, 2012, pp. 1389–1392.

[10] X. Jiang, W. Wang, T. Sun, Y. Shi, and S. Wang, "Detection of double compression in MPEG-4 videos based on Markov statistics," Signal Processing Letters, IEEE, vol. 20, no. 5, pp. 447–450, 2013.

[11] D. Labartino, T.Bianchi, A. De Rosa, M. Fontani, D. V´azquez-Pad, A. Piva, M. Barni, "Localization of Forgeries in MPEG-2 Video through GOP Size and DQ Analysis" MMSP'13, Sept. 30 - Oct. 2, 2013, Pula (Sardinia), Italy.

[12] Wang, W.; Farid, H, "Exposing digital forgeries in video by detecting double quantization", in Proc. 11th ACM Workshop on Multimedia and Security, MM & Sec '09, ACM, New York, NY, 2009, 39–48 online]. Available:http://doi.acm.org/10.1145/1597817.1597826

[13] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," MM&Sec'07, September 20–21, 2007,Dallas, Texas, USA.

[14] Kobayashi, M.; Okabe, T.; Sato, Y.: Detecting forgery from static scene video based on inconsistency in noise level functions. IEEE Trans. Info. Forensics Secure 5(4) (2010), 883–892.

[15] Subramanyam, A. V. and Emmanuel, S., "Video forgery detection using HOG features and compression properties," in Proc. IEEE 14th International Workshop on Multimedia Signal Processing (MMSP 2012), Sept 17-19, 2012, pp.8994.DOI:10.1109/MMSP.2012.6343421.

[16] Ching-Yung Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection," Ph.D. Thesis, Columbia University, Dec. 2000

[17] Chih-Hsuan Tzeng, Wen-Hsiang Tsai, "A new technique for authentication of image/video for multimedia applications". MM&Sec 2001: 23-26

[18] Jamal HUSSEIN1 and Aree MOHAMMED2, "Robust Video Watermarking using Multi-Band Wavelet Transform", IJCSI International Journal of Computer cience Issues, Vol. 6, No. 1, 2009.

[19] Yuan-Liang Tang and Chih-Jung Hung, "Recoverable Authentication of Wavelet-Transformed Images," ICGST International Journal on Graphics, Vision and Image Processing, Vol. SI1, pp. 61-66, 2005.