Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 3; January-March, 2015 pp. 233-236
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Review of Techniques of Digital Video Forgery Detection

Mrs. J.D. Gavade[1] and Mrs. S.R. Chougule[2]

[1]Dept. of Electronics, TEI, Ichalkaranji
[2]Dept. of Electronics, BVCOE, Kolhapur
E-mail: [1]jayashree2k2@gmail.com

Abstract—*Now days, digital technology has become predominant technology for creating, processing, transmitting and storing information in various forms such as audio, video, text and image all together we can call it as multimedia data. With the innovations and development in sophisticated video editing technology and a wide spread use of video information and services in our society, it is becoming increasingly significant to assure the trustworthiness of video information. Therefore in surveillance, medical and various other fields, video contents must be protected against attempt to manipulate them. Such malicious alterations could affect the decisions based on these videos.*

As video editing techniques are getting very complicated, modified videos are hard to detect. However, when a video is modified, some of its basic properties get changed. Then to detect those changes which is also called as forgery detection, it is needed to use complex video processing techniques and algorithm. This paper presents review of the various existing methods in literature, that are used to find whether the video is real one or not.

Keywords: -*Multimedia data, Forgery detection, Video forensic, Video processing techniques etc.*

1. INTRODUCTION

The widespread availability of the Internet, coupled with the easily available video and image capturing devices, such as low-price cameras, digital camcorders and CCTVs have become integral part of the society. Developments in visual (video) technologies such as compression, transmission, storage, retrieval, and video-conferencing have helped in many ways to the society. In the socio-economic knowledge and scientific development, the images and videos available at various video sharing and social networking websites (like YouTube, Face Book, etc.) are playing a significant role. Besides this, other applications like entertainment industry, video surveillance, legal evidence, political videos, video tutorials, advertisements, etc. signify their unprecedented role in today's context [1]. Apart from many good things, there are some darker sides of visual (video) information such as misuse or the wrong projection of information through videos. One of them is video tampering, where a forger can intentionally manipulate real (actual or original) videos to create tampered or doctored or fake videos for malpractice [1-3]. This in turn means that the images and videos that are seen in mass media such as television, popular Internet websites such as YouTube, may have been tampered and the adage "a picture speaks a thousand words" while still holding true – may now have a hidden and subverted meaning, i.e., their authenticity can no longer always be taken for granted. [04]

Hence, though the images and videos from cameras, digital camcorders and CCTVs can serve as very powerful "evidences" in both legal courts and public opinion, it is important to ask whether the images and videos produced by these devices are truly authentic and has not been tampered with. Easy availability of many sophisticated video editing tools provides a platform for forger to manipulate real videos and create perceptually indistinguishable fake videos. Therefore, in many serious scenarios like court trials, law enforcement, defamation, politics, and defense planning, etc. authenticity of presented video needs to be examined.

Forensic tools and experts play a key role to examine the authenticity of videos by detecting traces of tampering. Here, success or failure of tools and experts depends on how intelligently tampering has been carried out by the forger. It is difficult for forensic experts to detect tampering with videos if there are no (or little) traces left by forger while tampering.

Unfortunately, due to lack of established methodologies to examine the authenticity of videos, detection of tampering with videos have posed challenges before the scientific community, and its seriousness in many scenarios (e.g. videos as evidence during court trials) seeks immediate attention. This paper takes the review of various methods that have been suggested in literature to detect the forgery or tampering in video.

The remaining part of the paper is organized as follows. In Section II the notion of video authentication and framework are briefly introduced. Section III explains types of tempering

in video. Section IV provides a concise review of existing techniques for video authentication. Some of the new challenging scenarios are briefly introduced in section V. Finally the summary and future research directions are discussed in sec.

2. TAMPERING OF VIDEO

Video signals are spatial-temporal signals or simply stated a sequence of time varying images. The information they convey is "visual". A monochromatic still image can be mathematically represented by **x (h, v)**, where **x** is the intensity value at the horizontal location **h** and vertical location **v**. The monochromatic video signal can be represented by **x (h, v, t)**, where x is the intensity value at the **h** horizontal, **v** vertical and **t** temporal locations respectively. Video tampering is relatively new area as compared to image doctoring as it is as old as the art of photography itself where we have numerous incidences of serious cases of fake photographs **[04].**

Tampering the digital video is nothing but modifying or changing the contents of videos. This can be done by various methods which are presented in following subsections. While tampering a video, objective of a forger is to create a tampered or doctored or fake video from real or actual or original video. These real videos are the source for creating tampered videos. The seriousness of video tampering depends on how and where these tampered videos have to be used. Court trials are one of the most widely used application areas where these tampered videos are presented as evidence to mislead the court proceedings. Thus, whenever videos are presented as evidence during court trials, their authenticity are to be examined before considering them as evidence **[04].**

A. Tempering Attacks in Video

When a malicious alteration is performed on a video sequence, it either attacks on the contents of the video (i.e. visual information presented by the frames of the video), or attacks on the temporal dependency between the frames. Therefore based on the regional property of the video sequences, we can broadly classify the video tampering attacks into three categories: spatial tampering attacks, temporal tampering attacks and the combination of these two, Spatio-temporal tampering attacks [04] **[05].**

a) Spatial Tempering

A forger can tamper source videos spatially by manipulating pixel bits within a video frame or in adjacent video frames. The operations that can be done as tampering attack in spatial tampering are cropping and replacement, morphing, content (object) adding and removing etc**.** These attacks can be efficiently performed with the help of video editing software such as Photoshop.

b) Temporal Tempering

This type of manipulation is done on the sequence of frames. Temporal tampering attacks are mainly affecting the time sequence of visual information, captured by video recording devices. The common attacks in temporal tampering are frame addition, frame removal and frame reordering or shuffling**.**

c) Spatio-Temporal Tempering

Spatio-temporal tampering attacks are the combination of the both kinds of tampering attacks. Frame sequences are altered as well as visual contents of the frames are modified in the same video**. [04][05]**

B. Levels of Tempering Attacks

In addition of these types of tampering attacks, tampering can be done at different levels in video sequences.

a) Shot Level Tampering

At the scene level, an entire scene of a video is manipulated like deletion of a video scene (i.e. scene or shot cut), copying of a video scene to another place, etc. It can be done using either spatial or temporal tempering.

b) Frame Level Tampering

In this attack, the manipulation is done on frames of the video. The forger may remove the frames, add the frames, reshuffle the sequence of frames, and duplicate the frames from a given video to alter the contents of video. This can be done using temporal tempering.

c) Block Level Tempering

In this type of attack, the content of the video frames are treated as blocks on which the tampering attacks are applied. Blocks (a specified area on the frame of the video) can be cropped and replaced, morphed or modified in any way in block level tampering. Spatial tampering attacks are commonly performed at block level.

d) Pixel Level Tempering

In pixel level tampering, contents of the video frames are modified at pixel level. The video authentication system should be robust enough to differentiate the normal video processing operation and pixel level tampering, since many normal video processing operations are performed at pixel level. Spatial tampering attacks are commonly performed at pixel level. [04][05]

3. FORENSIC TOOLS FOR VIDEO FORGER DEDTECTION

In the following subsections we survey existing techniques for video doctoring detection. We group them according to the type of analysis they rely on.Section3.1 covers camera-based techniques. Section3.2 covers coding-based techniques. In

Section3.2, we analyze the problem of identifying frames, or portion of frames, i.e. copy-move forgeries.

A. Camera Based Coding Detection

Already it is proved that, camcorders usually leave a characteristic fingerprint in recorded videos. Although these kinds of artifacts are usually exploited just for device identification, some works leverage on them also for tampering detection.

Mondaini *et al.* **[07]** proposed a direct application of the PRNU fingerprinting technique to video sequences: the characteristic pattern of the camcorder is estimated on the first frames of the video, and is used to detect several kinds of attacks. Specifically, authors evaluate three correlations coefficient: a. the one between each frame noise and the reference noise b. the one between the noise of two consecutive frames, and c. the one between frames (without noise extraction).Each of these correlation coefficients is threshold to obtain a binary event, and different combinations of events allow detecting different kind of tampering. Experiments are carried on both uncompressed and MPEG compressed videos: results show that the method is reliable on uncompressed videos, not on MPEG-videos.

Hsu *et al.* **[08]** adopt a technique based on temporal correlation of noise residues, where the "noise residue" of a frame is defined as what remains after subtracting from the frame its denoised .Each frame is divided into blocks, and the correlation between the noise residues of temporally neighboring blocks evaluated. When a region is forged, the correlation value between temporal noise residues will be radically changed: it will be decreased if pixels of the blocks are pasted from another frame/region, while it will be raised to 1 if a frame replication occurs. But the success of this algorithm is only 55% only.

Hence from above discussion, it can be stated that camera based methods are effective on uncompressed videos. However, videos are typically stored in compressed format in most practical applications. This motivates the investigation of camera footprints that are more robust to aggressive coding.

B. Detection Based on Coding Artifacts

Digital videos are usually compressed with MPEG-x or H-26x coding standard. The tampering has to be accomplished in uncompressed domain in order to perform the operations such as frame deletion, frame insertion and many more. Considering facts that include size and format, tempered video has to be encoded. Thus, the occurrence of double compression may expose digital forgery.

In [09], the I-frames of the video are considered and the histogram of two quantized DCT coefficients is studied in order to search a convex pattern that characterizes double-encoded videos. By adopting a simple yet effective approach, the method is extended also to the challenging CBR case: macro blocks are separated in different sets, according to their quantization parameter, and the analysis is carried separately for each set.

An approach based on Benford's law is presented in [10], where the first digit distribution of DCT coefficients of I-frames is considered and a 12-dimensional feature is extracted to be classified using Support Vector Machines. Besides detecting double encoding, the method also classifies the second encoding as being at a higher or lower bitrate with respect to the first one. On the other hand, this method may not work when the two encodings are performed using different implementation of the MPEG-2standard.

Generalizing also to other video coding standards, a very recent work has been published about double encoding detection for MPEG-4 videos [11], based on Markov statistics extracted from DCT coefficients.

All the above mentioned works target the detection of double compression but does not contribute to forgery localization. Switching to tampering detection, an effective method for detecting removal of frames was proposed in [12], where the de-synchronization (induced by the tampering) between the GOP used for the first and for the second encoding is detected, by searching for a periodic behavior in the magnitude of motion vectors

Another work from the same authors **[13]** provides a more accurate description of double compression in MPEG videos, which allows them to detect doubly compressed macro-blocks (16 × 16 pixels) instead of frames. Consequently, this approach allows to detect if only *part* of the frame has been compressed twice, which usually happen when the common digital effect of green screening is applied (that is, a subject is recorded over a uniform background then it is cut and pasted into the target video).Performances of this technique depend on the ratio between the two compression quality factors: for ratios over 1.7 the method is almost ideal (99.4 detection rate) while for ratios less than 1.3 detection drops to 2.5%.

C. Copy Move Detection in Videos

Copy-move attacks are defined for video both as intra- and inter- frame techniques. An intra-frame copy-move attack is conceptually identical to the one for still images, and consists in replicating a portion of the frame in the frame itself (the goal is usually to hide or replicate some object). An inter-frame copy-move, instead, consists in replacing some frames with a copy of previous ones, usually to hide something that entered the scene in the original video.

Several forgery detection techniques related to image have been proposed till date; however there are only few video copy move forgery detection techniques.

The video copy paste forgery is addressed in **[14] [15].** In **[14],** the authors use temporal and spatial correlation in order to detect duplication. A temporal correlation matrix is computed between all frames in a given sub-sequence of frames and spatial correlation matrix is computed for each frame in a given subsequence. The temporal and spatial correlation matrix is then used to detect duplication. Although the detection performance is good for detecting frame duplication, the region duplication detection efficiency is very low for small forged regions such as 64 × 64. In addition this technique assumes that the forged region belongs to the same video.

In **[15]**, the authors the detection of forged region based on the inconsistencies of noise characteristics, which occurs due to the forged patches from different videos. However the noise properties depend on the intrinsic properties of camera, the noise characteristics are not useful when the forged patch comes from the same video. In addition, the noise characteristics may not be estimated correctly under the low compression rates.

In [16], the authors have detected the spatial and temporal copy paste tempering base on HOG (Histogram of Oriented Gradients) features matching and video compression properties. Here the authors have tested their algorithm on various modification performed on forged area. The algorithm shows the good results for detection. But as the block size goes on decreasing, the accuracy of algorithm also goes on decreasing.Also the authors have not made any comment on the computational efficiency of the algorithm.

Hence from the above discussion we can say that this type of forgery detection area is still under research and open problem to the researchers.

4. CONCLUSION

Throughout this literature survey, a number of video forgery detection mechanisms and techniques have been discussed with different perspectives. Video tampering is done using different methods. So it is obvious that there should be different methods to detect these different types of video forgery.

No single detection method works best for every situation. So what video forgery detection method is appropriate for a given situation depends on a number of reasons such as:

- Techniques used for video forgery
- Available technology
- Computational restrictions
- Video quality
- Video formats

So it is essential to understand the requirement and the environmental parameters as described above in video forgery detection.

As it has been shown in the previous sections, video forensics is nowadays a hot research issue in the signal processing world opening new problems and investigation threads. Also, video signals pose new challenges in the forensic application world because of the amount and the complexity of data to be processed

REFERACES

[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.