Integrity Verification of Video Files in a Video Event Data Recorder

Choongin Lee, Jehyun Lee, Sangwook Lee and Heejo Lee*
Department of Computer Science and Engineering, Korea University
Seoul 136-713, Republic of Korea
[e-mail: {choonginlee, arondit, ook7777, heejo}@korea.ac.kr]

Abstract

Most surveillance camera systems are not equipped with proper built-in integrity protection functions. Consequently, manually determining whether digital contents have been falsified is becoming extremely difficult for investigators. Hence, systematic approaches to forensic integrity verification are essential for ascertaining truth or falsehood. To this end, we propose an integrity verification method that utilizes the structure of video files in a Video Event Data Recorder (VEDR). The proposed method finds the difference in frame index fields between a forged file and an original file. Experiments conducted using commercial VEDRs and video files forged by a video editing tool demonstrate that the proposed integrity verification method is able to detect the broken integrity of video files.

Keywords: Integrity verification, Video forgery, Digital forensics, File system forensics

1. Introduction

The increased utility of surveillance cameras in the past few years has resulted in them being rapidly deployed worldwide [1]. Even considering that surveillance devices might infringe on privacy, this distribution trend is unavoidable because recorded videos can play a key role as evidence in disputatious situations [2]. Further, surveillance devices also help criminal investigators by providing significant amounts of evidence.

Nevertheless, video files are increasingly at risk of being forged with the advent of easy-to-use video editing tools [3]. Frames in a video file can be deleted or replaced by the use of video editing tools. Consequently, it is entirely possible that the forged video might be submitted to a court as evidence. In such a scenario, because there is no guarantee that the video is genuine, the evidence can be used for influencing an incorrect verdict in a criminal matter. Thus, it is essential that the integrity of video data be verified.

In this paper, we propose an integrity verification method for a VEDR video that uses the frame index data in video files. By checking for anomalies in the index artifact of the video files stored in the File Allocation Table 32 (FAT32) file system, the proposed method verifies the integrity of various types of video files. We primarily considered Audio Video Interleave (AVI) file since AVI is one of the most popular video file formats used in VEDR.

Pre-employed integrity check codes or watermarks of video frames reserved at the recording time have been proposed for video integrity verification in previous studies [4] [5]. However, these pre-employment approaches have deployment problems because those schemes need to be embedded in the target VEDR devices by the manufacturers. In addition, Post-processing approaches involving image analysis have also been proposed to detect image manipulation [6] [7]. However, they do not cover frame editing cases, in which no changes occur in the remaining images, such as frame deletion

*Corresponding author
☆This research was supported by the Public Welfare & Safety Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2012M3A2A1051118)

without re-encoding. In this study, we achieved video file integrity verification without using any pre-employment schemes and overcame the limitations identified in previous proposals.

We evaluated the proposed method using video files recorded by VEDR devices and modified using a video editing tool. The evaluation results show that the proposed scheme is able to identify compromised integrity. Of the eight forged samples, all eight were identified as being tampered when various amounts of frames are deleted from the original video file.

2. Integrity Verification Scheme for Disk Storage in VEDR

Fig. 1 shows the overall flow of the proposed VEDR video file integrity verification scheme. The scheme extracts the frame indices from the logical disk storage of a VEDR device using residual space (slack space and unallocated space) and allocated space parsers. Then, forged video files are detected by comparing the frame indices extracted from each space.

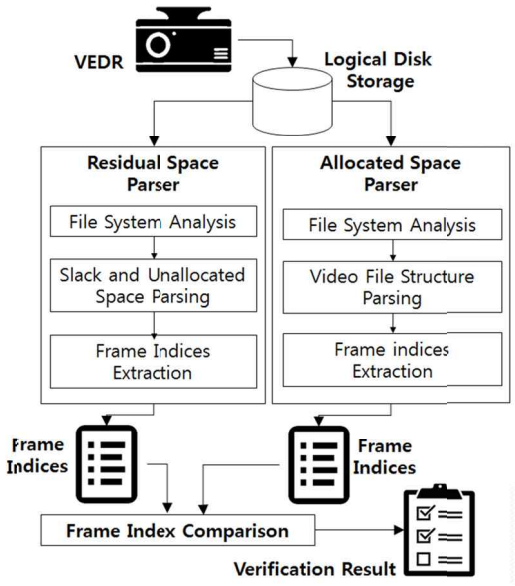

Fig. 1. Process flow of proposed VEDR video file integrity verification scheme

In the case of AVI video files, it is possible to use the index information to verify integrity. According to Microsoft [8], the AVI format comprises `LIST hdrl`, `LIST movi`, and `idx1`. Byte string `idx1` indicates a starting point to a field listing AVI frame indices. Because `idx1` follows LIST `movi`, it is located at the tail part of the AVI video file.

Fig. 2 graphically illustrates the concept of index-based verification. If a suspect overwrites a forged video file with an original video file, two `idx1` fields should remain in a file allocation area. Because the forged video usually has fewer frame indices than the original video [9], another `idx1` field remains in the residual space. We call the idx1 field stored in the residual space `idx1'`.

To verify the integrity of an AVI file, we refer to the size data of every frame index retrieved from `idx1` and `idx1'`. Let us suppose that the suspect deletes part of the frames. Frame size data in all the frame indices from `idx1'` are partially identical to that of those from `idx1`. In the situation, any mismatching frame in between `idx1` and `idx1'` means the existence of frame manipulation in the video file. From this principle, we are able to ascertain the integrity of the AVI file is broken.

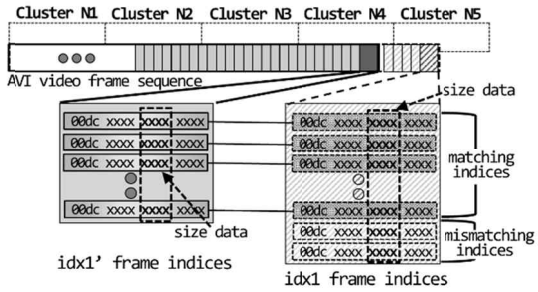

Fig. 2. Comparison of frame indices in both idx1

3. Evaluations

As proof of concept, we evaluated the proposed scheme with a self-implemented prototype and AVI video files forged using a commercial video editing tool that supports the frame editing technique. Overall, the proposed scheme successfully detected that the VEDR video files had been tampered. The proposed scheme was applied to video contents in two commercial automobile VEDRs, *iPass Black ITB-100HD* made by *iTronics Corporation* and *Provia4UFHD* made by *Provia Corporation.*

Both of the VEDRs are equipped with a FAT32 formatted 8 GB flash memory card.

The recorded video files were stored on the SD flash memory card and were in AVI format. We tested 12 video samples in total, which include 4 original videos and 8 manipulated videos with each frame editing scenario. Two of the original videos were one minute long, 1920 × 1080 resolution, 30 fps, H.264 encoded format, and consisted of approximately 1,800 video frames. The other two original videos had the same attributes with the former two original videos except that those videos were 1280 × 720 resolution.

Table 1 shows the detection result when the proposed scheme is applied to forged samples. The subscripts 10 and 50 on the forged samples ***S1-S4*** mean the percentage of deleted frames. When the verification tool found both matched frame indices and mismatched frames, it determined that the target file was a manipulated sample. On the other hand, if only matched frames were found, it determined that the sample was cloned from the original but not forged. The original video samples were found to be genuine when the detection mechanism was applied.

Table 1. Integrity verification results

Forged Sample	Original indices	Matched indices	Mismatched indices	Forgery detected
$S1_{10}$	1,809	**1,629**	**180**	**Yes**
$S1_{50}$	1,809	**909**	**900**	**Yes**
$S2_{10}$	1,810	**1,630**	**180**	**Yes**
$S2_{50}$	1,810	**910**	**900**	**Yes**
$S3_{10}$	1,800	**1,620**	**180**	**Yes**
$S3_{50}$	1,800	**900**	**900**	**Yes**
$S4_{10}$	1,800	**1,620**	**180**	**Yes**
$S4_{50}$	1,800	**900**	**900**	**Yes**

4. Conclusion

This study proposed a video file integrity verification scheme for investigating VEDR records. The proposed scheme detects image frame editing involving frame deletion by checking anomalies in the frame index fields. The proposed index-based scheme is a post-processing approach that operates without the need for any kind of pre-deployed on the VEDR devices. Further, it detects video file manipulation performed using a frame editing technique, which is difficult using conventional image based approaches. The evaluation results indicated that our proposed scheme could help in situations where maintaining reliable video records is essential for legal evidence.

References

[1] KOTRA, "Market trends of VEDR in USA," 2014. [Online]. Available: http://tradedoctor.kotra.or.kr/bp/cn/gw/BPCNGW011M.html?BBS_ID=19&ARTICLE_ID=5016869&MENU_CD=M00001&UPPER_MENU_CD=M00002&MENU_CD2=M00005.

[2] EveningStandard, "How car's black box trapped speeding Rich List heir who left baby paralysed in Range Rover crash," 3 April 2008. [Online]. Available: http://www.standard.co.uk/news/how-cars-black-box-trapped-speeding-rich-list-heir-who-left-baby-paralysed-in-range-rover-crash-6615218.html.

[3] Fox News, "Proposed new federal rule could put 'big brother' in your driver's seat," 12 August 2013. [Online]. Available: http://www.foxnews.com/politics/2013/08/12/proposed-new-federal-rule-could-put-big-brother-in-your-driver-seat/.

[4] M. Kim and K. Kim, "Data Forgery Detection for Vehicle Black Box," in *Proc. of Information and Communication Technology Convergence (ICTC), IEEE*, 2014.

[5] T. Jayamalar and V. Radha, "Survey on digital video watermarking techniques and attacks on watermarks," *International Journal of Engineering Science and Technology,* Vol. 2, No. 12, pp. 6963-6967, 2010.

[6] J. Wang, G. Liu, Z. Zhang, Z. Wang and Y. Dai, "Detection of forgery in digital video based on pattern noise," *Journal of Southeast University (Natural Science Edition),* No. S2, 2008.

[7] C. Hsu, T. Hung, C. Lin and C. Hsu, "Video Forgery Detection Using Correlation of Noise," in *Proc. of Multimedia Signal Processing, 2008 IEEE 10th Workshop, IEEE*, 2008.

[8] Microsoft, "AVI RIFF file reference," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd318189(v=vs.85).aspx.

[9] S. Lee, J. Song, W. Lee, Y. Ko and H. Lee, "Integrity Verification Scheme of Video Contents in Surveillance," *IEICE TRANSACTIONS on Information and Systems,* Vol. 98, No. 1, pp. 95-97, 2015.