Discussion on the Practice of Forensic Authenticity for Digital Video Recordings

Cheng Yan

Department of computer science and engineering, East China University of Political Science and Law, Shanghai, China

chengyan@ecupl.edu.cn

Abstract. Forensic authenticity of the digital video recordings is an important part of the forensic audio-video examination. There are a few relative practices in this field. In this paper, some practical methods of forensic authenticity for the digital video recordings were discussed and some anomaly judgment principles were given at last.

Keywords: Video recording, Forensic authenticity, Digital, tampered

Introduction

In the digital multimedia age, applications of video surveillance equipment have made the dramatic increase in the amount of video data. Since the videos can convey the real world scenes more vividly and credibly, they are the important evidences for the criminal investigation and civil cases. However, with the advent of high-resolution digital cameras and sophisticated multimedia editing software, the manipulation of videos is becoming more common. If the tampered videos are used in some important ways, it will cause many adverse effects. Therefore, the forensic authenticity of the digital video recordings is the important part of the forensic practices to use the video recordings more effectively.

The video signal can be regarded as the extension of the static image on the time-line. So an straight idea of the forensic authenticity is to separate several independent frames from the original video and detect the authenticity by using the image forensic technologies. But in fact, it is not ideal for the results. Besides the computational burden, the main disadvantage of the above idea is that it ignores many spatial and temporal information of video frames. The feature analyses in the time dimension will be missed, which will result undetected for some tampering operations, such as copy frames, cancel frames, etc. Compared to the image (single frame) forensic authenticity, video authenticity is more difficult for having much more data information, complicate format and variable compression. It has the considerable practical significance and becomes the present hot issues of the multimedia safety technology.

Forensic Methods

Basic identification method

1. Check EXIF information

The EXIF (Exchangeable Image File, EXIF) information of any recording material includes video and audio properties. We can check the general EXIF information by the Windows properties viewer directly. Usually, the general properties conclude the file size, occupied size, created time, modified time, access time. The video properties conclude length, frame size, frame rate. The audio properties conclude bit rate, channels and sample frequency and so on. Moreover, we can use some other professional software such as Exif Tool or MediaInfo Video Encoding Viewer to check the professional properties. As the Fig.1 shown, we can get more video and audio properties in detail, such as the information of coded mode, frame depth, GOP parameters and delay time, etc. Especially, we should pay more attention to the following properties as created time, modified time, coded time, coded mode and the relative parameters of video and audio. This is because there are some logical contradiction of these parameters in the modified or tampered video recordings sometimes. For

example, for some cameras, the ‘Encoded time’ shown in MediaInfo is Greenwich Mean Time (GMT) and will be set as the imaging time in default. In most cases, the time usually remain unchanged even after being tampered, which will cause a logical contradiction with the modified time, access time, or other time properties, which will give us an identification idea.

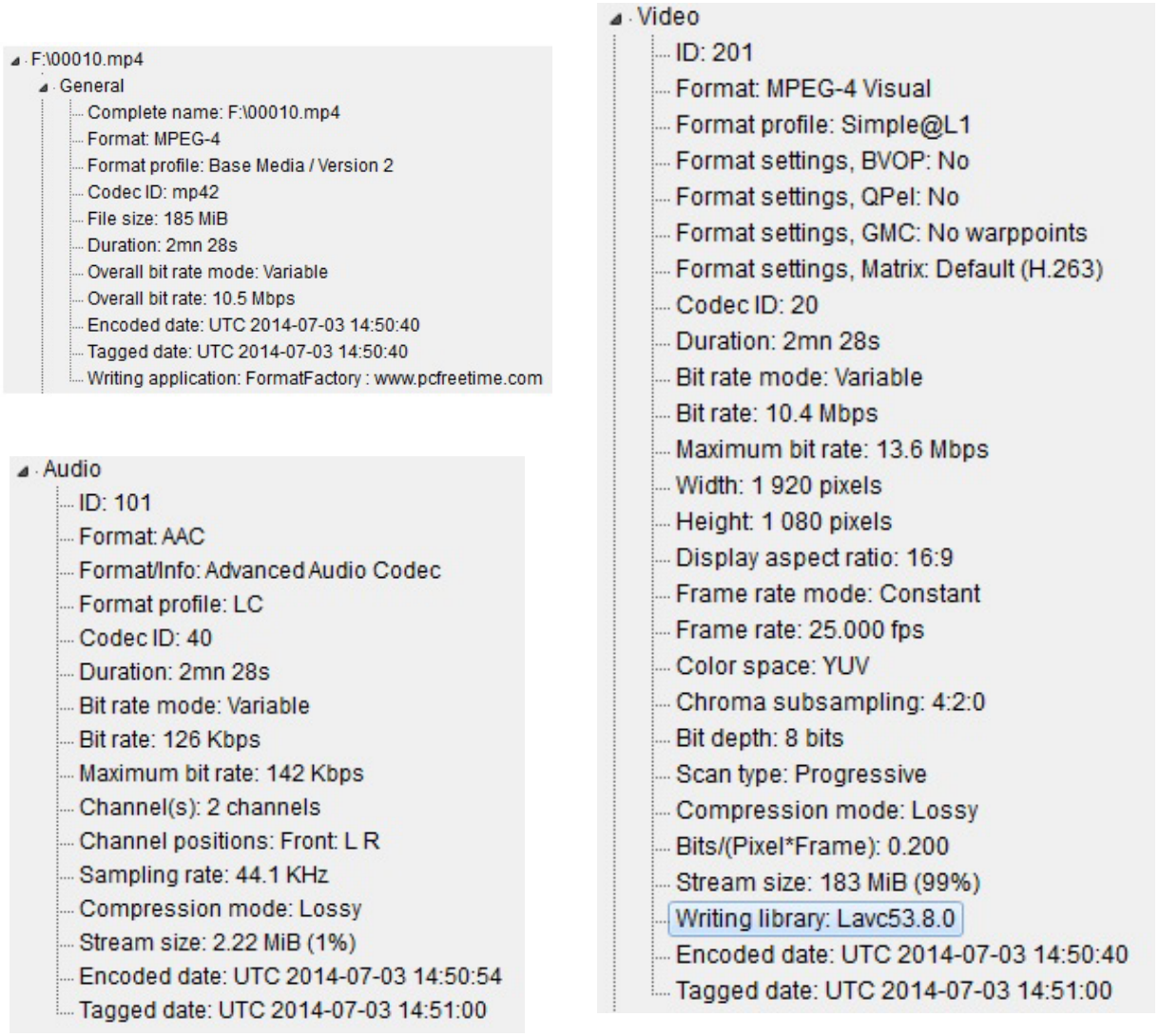

Fig. 1 MediaInfo Properties Viewer

2. Simulation test

Different types of cameras have different technical parameters, so the recordings surely have their own characteristics. In order to recognize the performance and characteristic of the recording process of the hardware equipment, we should make the recording samples for the simulation test by using the same equipment offered by the clients. The most important factors we should observed in the simulated samples are:

(1) The equipment type and the setting parameters, such as the recording time, the environment and background of the video recordings;

(2) Content of the video recordings such as the actors, scenes and their characters;

(3) The recording process and whether there is some abnormal or special operations in the recording process.

Comparing the properties between the forensic and simulated samples, we can make some pre-judgements on the authenticity of the forensic sample by the following points:

(1) Whether the content of the sample video recording is consistent with the formation process. Actually, the video surveillance system uses some fixed cameras, whose position and angle are usually fixed, as a result, the shooting of the pictures are mostly overlooking with a stable view. However, the personal recording comes from the hand-held camera or recording while walking, so

the pictures are not stable. If the lens zoom is frequent, the picture content will produce suddenly away or near effect. Therefore, we must confirm the formation process of the forensic sample first.

(2) Whether the characteristics and rules of the file formation are same to those of the test sample. When comparing, the identifiers should try to find out the most possible contradictions in the video recordings. For example, a video named "20160219_194748.mp4" is taken by SM-G7100 and restored in the path as '/storage/extSdCard/DCIM/Camera'. From the filename rule, we can know that the video is recorded on Feb.19, 2016 and the numbers after the underline shows that the recording time is 19:47:48. Through the further examination, we can know the file size is 1280*720 and the format is MP4. So, if the file size or the filename rule of the forensic recording does not meet the characteristics of the simulated sample, the forensic recording may be changed or the recording equipment is not true.

(3) The analyses of the video content, view and angle of the field is consistent with the scientific principle, the same as the imaging point of view, the perspective and depth of the relationship between scientific principle.

3. Detect the recording content

The conception of the detection of the recording content is that the experts analyze the video and audio contents by comprehensively using visual inspection, hearing test, waveform and spectrum analysis method.

(1) Video content detection

In the identification process, experts usually focus on finding out the abnormal phenomenon or contradiction of the video. The analysis aspects are as follows.

① Observe the image features, such as image sharpness, contrast, color, density, imaging spot, shadow and intensity distribution, and check whether they are consistent with the exposure and imaging rules.

② Observe the position and state of an actor or object of the sequential frames, and check whether the movements or the trajectories are continuous without any sudden change.

③ Observe the similarity of the pattern noise, brightness and color of the sequential frames, and check whether there is a sudden flicker, jitters, pulse, or loss of the signal in the video.

④ Observe the imaging features at the start and end time of the video. Compared with the simulated sample data, and check whether both of the features shown at the two times are similar.

(2) Audio content detection

If the forensic sample contains the audio signal, we can further judge the authenticity by detecting the audio signal. First, we should extract the audio part as a separate file from the recording. Since the speaker's tone is coordinated with his action, we can detect the integrity and coordination of the semantics of speech firstly. On the other hand, human speech has the features of speech situations, that is to say, the features of speech with different emotional states of the loudness, tone, speech rate, rhythm will have obvious different effects. Sometimes, the speaker will show different features of sound effects due to the physical condition, anxiety, emotion with cough, excitement, fear,anger etc. That is also the basis of our judgement. Moreover, all kinds of noise may be introduced during imaging process, the video recording will include many noises such as environment noise, equipment noise, channel noise and so on. If the audio signal is original, the background noise and the speaker's physical condition is usually in a stable state. The clipping operation of the audio will destroy the stability of the noise and make the discontinuous state at the splice point, so we should further detect the features of the break points, discontinuity points or mutation points through observing the waveform and frequency spectrum.

Algorithm analyses

The basic identification method mainly depends on human vision, hearing, and observing of the signal spectrum or waveform analysis etc. The rate of correct detection is susceptible to human experience and subjective factors. When the human eyes are not sensitive to some changes of the tampered video recordings, digital algorithm analyses can widely be used in identifying the source of capturing device and the originality/integrity of the information, such as document, image and video.

As we all known, the video tampering operation is a signal processing process. It will certainly destroy the continuity of the digital data and leave some traces, which will provide the guarantee for the identification of the authenticity of the video and audio. The practical use of these techniques depends upon the accurate modeling of the intrinsic features of the capture devices, such sensor noise, and the feature of information, thus techniques are restrictive for specific application use.

Anomaly judgement principle

The authenticity of the video recordings focuses on the identification of abnormal points. But we can not easily draw a conclusion that the video recording is tampered if it has some abnormalities. Usually, we have the following anomaly judgement principles,

First, whether the abnormal points are relative to the hardware. For example, if the monitoring system used the infrared camera, the restored images will be shown in the true color when the daylight is sufficient. Otherwise,the images will be biased when the light at night is insufficient. So if the color of the clothes is inconsistent with the actual,we can not simply judge the forensic sample is tampered.

Second, whether the abnormal points are caused by human factors. For example, people manually press the pause button frequently when recording, it will cause the abnormal interrupt or discontinuous phenomenon in playing. That is not means that the video is tampered.

Third, whether the abnormal points are caused by external environmental factors. For example, when we recording, a sudden sharp sound will produced abrupt points in the corresponding frequency signal and the video scene changing will produce different background and environmental noise in the video. Thus, combining with the pre-checked of the video and the simulation experiment, we should make the judgement by the comprehensive analyses of the causes of abnormal video points.

References

[1] Du. Z.C. Survey of Justice Identification [M], Law Press China, 2010

[2] Yang Y.Z. Forensic Image Technology[M], People’s Public Security University of China Press, 2007

[3] Wang Y.Q. Forensic Imaging Appraisal Practice, Law Press China, 2013

[4] H.Farid, M.J.Bravo, “Image forensic analyses that elude the human visual system,” In SPIE Symposium on Electronic Imaging, San Jose, CA,2010

[5] Simson L. Garfinkel. Digital Forensics Rearch: The Next 10 Years. Digital Investigation, 2010, 7(1):64-73

[6]China Daily website: http://www.chinadaily.com.cn/hqgj/jryw/2013-09-13/content_10105397.ht

ml

[7] Luo W.Q, Qu.Z.H. Pan F. A survey of passive technology for digital image forensics [J]. Frontiers of Computer Science in China, 2007, 1(2):166-179

[8] Chen W.B, Yang G.B.,etc. Digital Video Passive Forensics for its Authenticity and Source, Journal on Communication, vol.32(6),2011:177-183

[9] Ding Q, Ping X.J. Digital Speech Tamper Detection based on Speaking Conditions, Journal of Computer Applications, 31(5), 2011:1284-1287

[10] Zhang X, Li Z.H. Wang X. A Survey of Video Forensic Technology, Forensic Science and Technology, 40(2),2015: 87-93