Advances in Engineering Research, volume 166
3rd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2018)

Research on Recognition and Carving Techniques of Monitoring Video Fragments based on Structural Features

Xu Chang[a], Jian Wu[b], Shanshan Pei[c]
Shandong University of Political Science and Law, Jinan, Shandong Province, China
[a]changxumail@163.com, [b]jinanwujian@163.com, [c]peishan616@163.com

Keywords: Fragments Recognition; Video Carving; AVI

Abstract. The purpose of this paper is to research how to identify and restructure the binary data fragments which were stored on device efficiently and accurately. Take widely used AVI video file format for example, we proposed a method to identify fragments and carve them into files based on structural features, after the studying of carving technical principle of video and AVI file structure. At last, make a simulation to test the method. The results show that it can recover AVI video files from storage devices without Meta system information and achieved very high percentage of accuracy.

Introduction

With the development of information technology, equipment for road monitoring or vehicle video forensics is widely used. As an important source of evidence, monitor video plays an important role in order management and traffic accident handling. Usually, the data of monitor video is huge, and it is often stored in sequential or non-sequential form in storage devices. Because of limited storage space, repeated erasures are needed during use, which will make the data severely fragmented and caused a great obstacle to forensic.

The traditional recovery method relies on system meta-information. It is difficult to recover when the meta-information is incomplete, even if the data is not covered. Data carving technology overcomes the shortcomings of traditional data recovery techniques. It attempts to recover and reconstruct files from an unstructured raw disk image binary data stream, without relying on the file system of the source disk image, carving the "shape" of certain documents from a digital "plane" under the conditions of automatic or minimal manual intervention [1]. This article focuses on AVI format video files that are widely used in surveillance video and driving recorders. It focuses on how to efficiently and accurately identify and extract target fragments in seemingly indistinguishable binary fragmented data, and reorder and reconstruct the fragment files.

As an important part of computer forensic analysis, its tools or methods has continuously improved, and theoretical research is constantly deepening and improving[2]. Video files are complex and have a large amount of data. In the early days, There is less research on video files, Most of the research focus on case analysis which taken by specific video tools. The data carving methods are not universal, such as WS. Van Dongen [3] recovers the video which recorded by Samsung Video Recorder; Huang Bugen [4] recovers the MP4 video in the SANYO camera.

In recent years, in order to cope with the various types of document processing and complex fragments carving requirements, many researchers have introduced related field theories from different perspectives. For example, foreign researchers have introduced graph theory and greedy algorithms into document carving, which brought many new carving theory and methods, enriched carving theory. Andrew B. Lewis [5] researched the compressed data and proposed a method of carving MPEG video. In 2013, Huang Wei [1] used a combination of keyword and binary gap carving to complete the carving; in 2014, Gi-Hyun Na [6] proposed a frame-based MPEG video carving method, carving MPEG video successfully. In 2015, Liu Liying [7] proposed an AVI data extraction method based on the internal features of AVI files and an AVI fragment reorganization method based on the frame length information in each frame and file index. Li Zichuan [8] proposed a debris-level search technique for video file data by recording time in WFS non-universal file system. Xia Rong et

al. [9] proposed a method for efficient video recovery forensics using WinHex scripting tool. In general, the current research on the theory and tools has made great progress. However, there are still many problems that need to be resolved in the face of a wide range of equipment and document types and different levels of damage.

Analysis of AVI Format

AVI is a digital video and audio file format that conforms to the RIFF file specification. It is the most complex RIFF file currently in use, and can simultaneously store audio and video data. RIFF files use four-character code (FOURCC) to characterize data types. The structure of the entire AVI file is: a RIFF header, a list for describing media stream formats, a list for storing media stream data, and an optional index block. The expanded structure of the AVI file is roughly as shown in Fig.1:

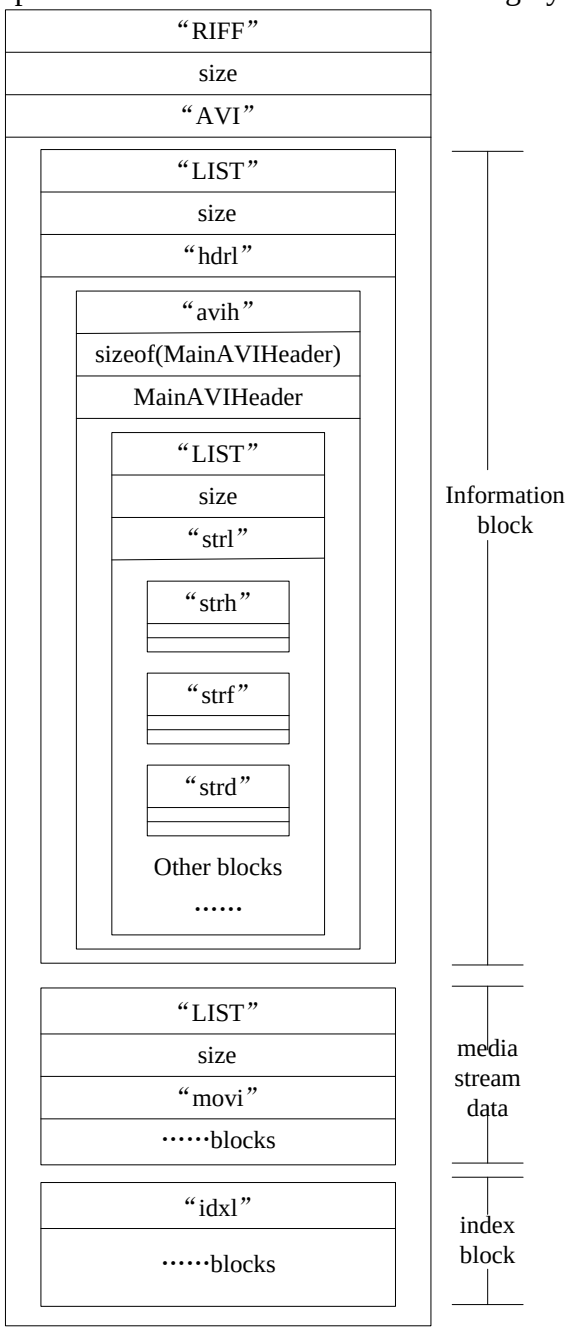
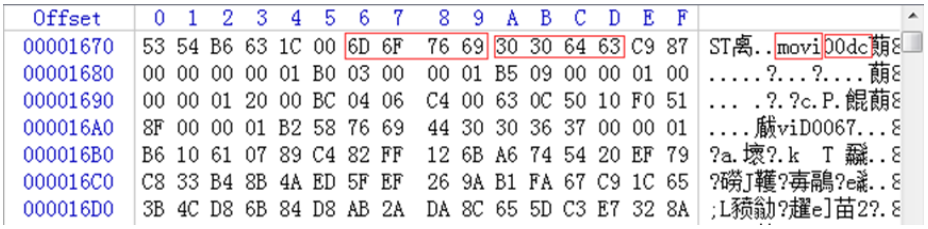


Fig.1 Expanded structure of AVI

The List block with ID “hdrl” is used to describe the format information of each stream in the AVI file (each media data in the AVI file is called a stream). The list nests a series of blocks and sub-lists, including an "avih" block and one or more "strl" sub-lists for recording global information about AVI files (eg, number of streams, width and height of video images). Each "strl" sublist contains at least

one "strh" block containing the header information of the stream and a "strf" block that specifies the specific format of the stream, "strd" block (requires configuration information for the codec to be saved) and "strn" block (The name of the save stream) is optional.

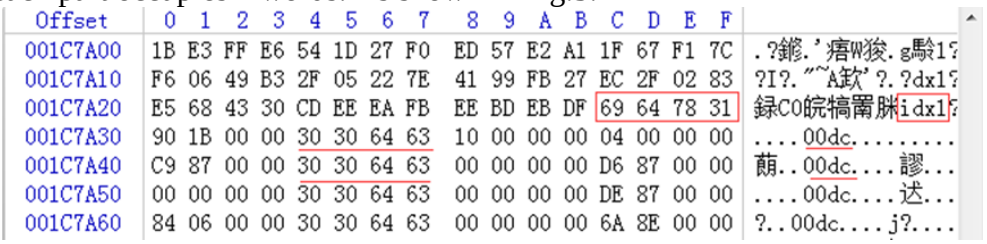
The list with ID "movi" is used to save the real media stream data. When the AVI file contains multiple streams, the data block uses FOURCC codes to represent the types of data blocks of different streams. The four-character code consists of a 2-byte type code and a 2-byte stream number. The standard type codes are defined as follows: "db" (uncompressed video frame), "dc" (compressed video frame), "pc" palette change, "wb" (audio data), as shown in Fig.2 "00dc" Compress video frames.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00001670	53	54	B6	63	1C	00	6D	6F	76	69	30	30	64	63	C9	87
00001680	00	00	00	00	01	B0	03	00	00	01	B5	09	00	00	01	00
00001690	00	00	01	20	00	BC	04	06	C4	00	63	0C	50	10	F0	51
000016A0	8F	00	00	01	B2	58	76	69	44	30	30	36	37	00	00	01
000016B0	B6	10	61	07	89	C4	82	FF	12	6B	A6	74	54	20	EF	79
000016C0	C8	33	B4	8B	4A	ED	5F	EF	26	9A	B1	FA	67	C9	1C	65
000016D0	3B	4C	D8	6B	84	D8	AB	2A	DA	8C	65	5D	C3	E7	32	8A

Fig.2 Data of media stream

The index block is followed by media stream data, which represented by the AVI file “idx1”. The index block uses consecutive 16 bytes to index each media data block in the AVI file to record the label, attribute, location of the sub-block relative to the "movi" list and sub-block length in the data block, and each part occupies 4 words. As shown in Fig.3.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
001C7A00	1B	E3	FF	E6	54	1D	27	F0	ED	57	E2	A1	1F	67	F1	7C
001C7A10	F6	06	49	B3	2F	05	22	7E	41	99	FB	27	EC	2F	02	83
001C7A20	E5	68	43	30	CD	EE	EA	FB	EE	BD	EB	DF	69	64	78	31
001C7A30	90	1B	00	00	30	30	64	63	10	00	00	00	04	00	00	00
001C7A40	C9	87	00	00	30	30	64	63	00	00	00	00	D6	87	00	00
001C7A50	00	00	00	00	30	30	64	63	00	00	00	00	DE	87	00	00
001C7A60	84	06	00	00	30	30	64	63	00	00	00	00	6A	8E	00	00

Fig. 3 Index block

The List block with the ID "JUNK" is used to represent special data. It is used to fill internal data. The application program generally ignores the actual meaning of these data blocks.

Fragments Recognition and Carving based on Structural Features

The carving process for video files is divided into two stages: data extraction stage and data fragment reconstruction.

Identification and Extraction of Fragments. Scan the original image in terms of bytes, and extract header information, media stream data information, and index information of the suspected AVI file according to the characteristics of the data structure. During the search, the data is located by flag bits, and each frame data is combined with the data length according to the searched flag bit and data length to determine the integrity of the data. Save the fragmented data if the data is complete.

Identification and Extraction of Header Information. AVI video files are complex in structure and can be extracted from data blocks in the data area or extracted from header information. The break zone of the file also appears mainly in the data area "movi" list. The list of file headers is usually considered as complete and generally does not appear fragmented. Therefore, extracting the header information can get the size and attribute information of the file, which helps to carry out the work of carving.

After the “RIFF” flag is located, scanning continues. If the subsequent data can satisfy the AVI file header structure feature, the data is considered to be a complete AVI header. Search for "52 49 46 46" in the image to search for file header information. If it exists, skipping 12 bytes can find the next flag bit "LIST", and turn it to "INFOISFT" and other flags until the "movi" flag. Starting from the "RIFF" flag and before the "movi" flag is a typical AVI file header. After the header information is extracted, analyze and save the detailed structure.

Identification and Extraction of Media Stream Data. The AVI file is a complex audio and video file. The main data area can be divided into video streams, audio and video alternating mixed streams and other forms. In general, it consists of a video stream and an audio stream. The two stream numbers are "00" and "01". The video data FOURCC is encoded as "db" or "dc" and the audio FOURCC is encoded as "wb". Therefore, the suspect data frame can be located by searching for the FOURCC flag. This article uses the following methods to identify and extract data fragmentation.

Step1: Search FOURCC code, record the offset O, jump to Step2;

Step2: After extracting the FOURCC code, four bytes of sub-data length Li, jump to Step3;

Step3: Jump to the (O+Li) offset position and judge the FOURCC code for the next sub data exist or not. If not exist jump to Step1. If exist, the data block before saving the initial offset O to the next FOURCC code position is a fragment Fi, which is stored in the fragment library, fragment length and the relative position of “movi” are recorded at the same time.

Extraction of Index Block. The FOURCC code of the AVI index tag is "idx1". This data has a small proportion in the AVI file and is not easily divided into fragments in general. Therefore, this article directly searches for the location "idx1" and extracts the index data based on the index length information.

Reconstruction of Fragments. Carving the video fragments needs to reconstruct three parts of the file, contains header, media stream data and index block. First, read the extracted file header information and analyze the length; second, read the index block information, and sequentially extract 16 words of tag, attribute, relative position and length information. Compare the relative positions and data lengths of the data fragments with the data from fragment library. If match, add the flag "hit". If not, generate empty data and add the flag "miss" to construct media stream data area information; third, read additional index block data again; finally reconstruct each part of data required by the video file and compare it with the data length in header. If match, means carve completely. The specific reconstruction process is shown in Fig.4.

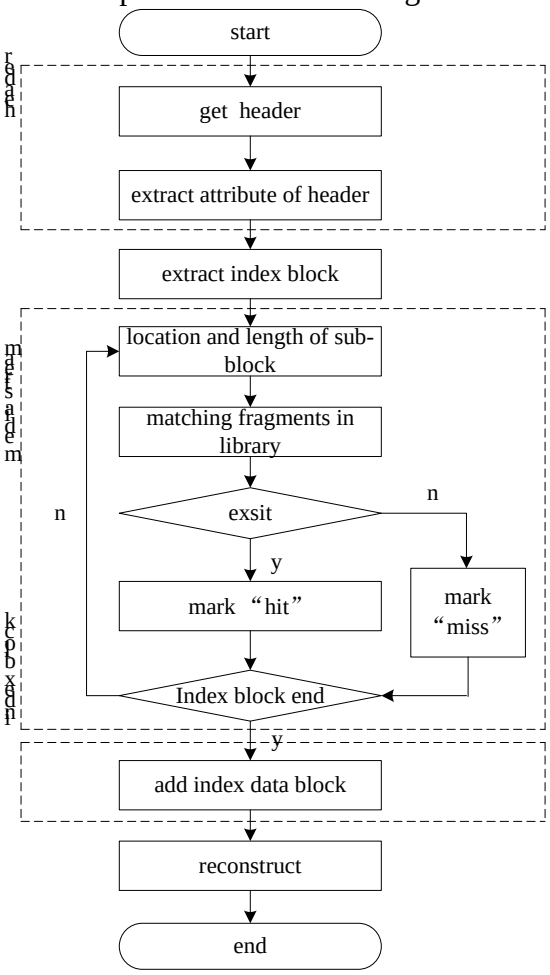


Fig.4 Flowchart of fragments reconstruction

Experiment and Result Analysis

This article uses a 4G U disk to make a test disk to simulate a real-life usage scenario. This U disk has been used for more than one year every day and has not been formatted during this period. Randomly collects 200 commonly used file types such as docx, txt, jpg, avi, etc. Including four avi files, followed by Cap1.avi, Cap2.avi, Cap3.avi, Cap4.avi. Then read, write and delete, In order to generate file fragments naturally. Ensure the fragment size and locations are random. During the experiment, the U disk file system is ignored, the target fragment is extracted from the "undifferentiated" binary fragmented data, and the video file based on structural features is reconstructed to recover the required video files. After the experiment, the four files were successfully carved and played normally, as shown in Fig.5.

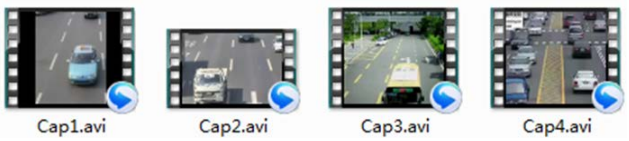


Fig.5 successfully carved AVI video files

The recovered file is not significantly different from the source file by manual observation. Using Winhex to view the data size and comparing with the source file, the file carving effect is shown in Table 1.

Table 1. Carving result statistics

File Name	**Comparison before and after recovery**			
	File size after carving (bytes)	***Original file size***	***Miss number***	***Carving rate***
Cap1.avi	3248144	3,248,562	0	99.98%
Cap2.avi	9205533	9,226,192	1	99.77%
Cap3.avi	1838587	1,873,348	1	98.14%
Cap4.avi	10187084	10,187,920	2	99.99%

In the simulated mirroring environment, the target video file is relatively small, and the degree of fragmentation is lighter, so the recovery effect is better. According to the experimental data analysis, the proposed method based on the structural characteristics of the video file carving complex data carving is feasible and effective. Especially suitable for non-file system storage devices, the data is relatively complete fragmentation data. For fragmented data resulting from incomplete coverage, only the identified fragmented files can be used to maximize the carving based on the existing structural features. Like the file index header and index block are completely covered at the same time, the extracted condition cannot be recognized.

Conclusion

AVI format is widely used in video surveillance applications. The research on carving of AVI video files is of great significance and it is helpful for the development of forensics and electronic recovery technologies. Due to the wide variety of existing file types, it is difficult to implement universal file reconstruction tools that are currently applicable to all files, and more cases are studied for specific types of data. The next step will be to further study the case where the structural features are incomplete and the fragments are out of order. Identify fragments depend on the content features and design algorithm which are used to implement the judgment and reorganization of adjacent fragment data.

Acknowledgment

This work was funded by the Science and Technology Project of Universities in Shandong Province, with the project approval number: J16LN19; the university-level project of Shandong University of Political Science and Law, and the project approval numbers are: 2016Z03B, 2016Z04B, 2015Z03B,

2016JYA001; Key Laboratory of Evidence-Identifying in Universities of Shandong (Shandong University of Political Science and Law).

References

[1] Huang Wandi, Wang Zhongxia, Wu Zhendong. carving of AVI files in electronic forensics. Chinese Journal of Forensic Sciences, 2013 (3), pp. 57-61.

[2] Nicholas Mikus. An analysis of disc carving techniques . Master thesis. Monterey: Naval Postgraduate School, 2005, pp.23–25.

[3] Van Dongen W S. Case study: Forensic analysis of a Samsung digital video recorder. Digital Investigation, 2008, 5(1): pp.19-28.

[4] Huang Bugen, Huang Zheng, Liu Jianjun. Restoration of Deleted Video in SANYO Digital Camera. Journal of Internet Information and Security, 2011, pp 143-155.

[5] Lewis A B. Reconstructing compressed photo and video data [D]. Cambridge: University of Cambridge, 2012.

[6] Na G H, Shim K S, Moon K W, et al. Frame-based recovery of corrupted video files using video codec specifications. IEEE Transactions on Image Processing, 2014, 23(2), pp. 517-526.

[7] Liu liying. A study of AVI Video Carving [D], Nanjing University of Posts and Telecommunications, 2015.

[8] Li Zichuan. Research on Data Search and Recovery Technology of WFS Video Surveillance System, Journal of China Interpol College, 2015, pp.42-45.

[9] Xia Rong, Wu Bin, Yuan Wenqin. Research on surveillance video recovery technology, industry and application security, 2017, pp. 126-129.