Real Time Watermarking and Encryption Method for DMB Contents Protection

Won-Hee Kim and Jong-Nam Kim

Div. of Electronic Computer and Telecommunication Engineering, Pukyong University
{whkim07,jongnam}@pknu.ac.kr

Abstract. Watermarking and Encryption are commonly technique for data protection. DMB contents are utilized widely without protection procedure. To solve the problems, we propose real-time watermarking and encryption method for DMB contents protection in this paper. To implement watermarking, we hide key information on a redundant space of program association table (PAT) and program mapped table (PMT) of T-DMB stream and hidden parts is encrypted by a stream encryption cipher. We implements encryption method without additional information in digital multimedia broadcasting (DMB) contents using AES (advanced encryption standard) encryption algorithm. In experimental result, when we implemented a play control on PMP which have built-in DSP device to get 100Mhz processing speed, almost had not a time delay and the hiding information in T-DMB stream was possible to do a play control. Additionally, we confirmed that the saved contents in a PMP were not played in other devices without decryption key. The proposed methods can be useful in real-time applications requiring contents protection service such as video on demand, IPTV and digital TV.

Keywords: Watermakring, Encryption, DMB, Contents Protection, Real Time.

1 Introduction

Most of all, portable DMB devices are possible to storing DMB contents, because of it has an internal hard-disk drive or flash memory. There devices, which is able to storing multimedia contents, are possible to an illegal distribution without agreement of the contents producers. The illegal distribution of multimedia contents must be forbid for the growth of multimedia contents distribution. The research and implementation of the contents protection technique for illegal multimedia distribution protection is progressing but, some works for protection of an illegal distribution in portable DMB devices like PMP are little. A contents protection technique for an illegal distribution protection of multimedia contents is the watermarking and the encryption. A watermarking is not pre-blocking but post-blocking about access of users and an encryption is a pre-blocking technique, which can access just authorized users, against an illegal distribution of multimedia contents.

The encryption methods for the digital video contents protection encrypt whole bit-stream domain of a digital video and a part of bit-stream or encryption progress [1-2].

T.-h. Kim et al. (Eds.): FGIT 2010, LNCS 6485, pp. 493–501, 2010.

The farmer is possible to a strong encryption, but has high calculation complexity. The letter isn't possible to a strong encryption than the first, but has lower complexity.

In watermarking, when we classify it according to a location of hiding information, it is divided into three parts which are a spatial domain, a transform domain and bit-stream domain [3-4]. A watermark hiding of spatial domain has a lower complexity and a lower robustness, a transform domain is possible to a strong hiding of information but has higher computational complexity and a bit-stream domain has a lower complexity and a higher robustness.

In this paper, we propose a real time bit-stream watermarking method for an illegal distribution blocking of DMB contents during store contents in the internal hard-disk drive and implement on PMP. Proposed method hides encrypted play control information on redundancy parts of DMB bit-stream.

2 Related Works

There are lots of kinds of video copyright protection system. They include watermarking system, digital right management (DRM) and image encryption. Watermarking system is hiding copyright information in digital contents without decreasing image quality [3]. It is the surest way for the copyright protection, but inappropriate for blocking unauthorized users because it is not difficult for unauthorized users to access videos and then use digital contents illegally. DRM system is more effective than watermarking system in terms of conditional access. It is effectively blocking unauthorized users. DRM system prevents illegal distribution and duplication from unauthorized users.

Also, these systems permit users which use digital contents in legitimate, but protects illegal users [4]. DRM system needs network infra to share the certification key. That is difficult to use some DMB devices not having networking function. In addition, it is very expensive for implementation because DRM systems need the expensive computer systems and networking elements.

Image encryption is to distribute the partially or fully encrypted images [1]. There are many kinds of encrypt algorithms - DES, AES, SEED, and so on. DES algorithm was invented in 1977. However, this encryption algorithm is broken in 1997, so it is sure that it is not robust. To replace DES, AES algorithm was developed [2].

AES algorithm is symmetric key block algorithm and block size is 128bit key size is variable from 128bit to 250bit. Encryption and decryption speed in digital signal processor is a positive point faster than SEED and RC6 [5].

Encrypted images cannot be replayed without certification key. It is an efficient way to block unauthorized users. Image encryption technique has a weak point. That is, there is no way to block the distribution of decrypted images from legitimate users. The way we suggest is to operate encryption and decryption on a PMP and impossible to distribute the decrypted contents. Existing method of encryption technique encrypts the I-frame or P-frame in video data. However, it was not yet implemented in embedded devices (PMP or another DMB device) [6-8].

There are two kinds of DMB, in which one is Terrestrial DMB (T-DMB) and the other is Satellite DMB (S-DMB). These two DMB systems use the same video compression algorithm. For the compression, H.264/MPEG-4 Part 10 AVC technology is used. Our implemented system is based on T-DMB.

3 The Proposed Methods

In the section, we introduce proposed watermarking method and explain implantation on PMP. An implementation of a real time bit-stream watermarking on a portable DMB device is difficult to an implementation using a conventional method. In case of DMB, it is consisted of a packet unit of TS and is possible to a real time watermarking when we do watermarking in especially small part of TS packets [9]. Proposed method encrypts hiding watermark information for a play control using by Dragon stream cipher and then hides play control information in redundancy data which isn't a active video data in TS packets. Fig. 1 show a structure of DMB transport stream (TS). TS have a length of 188 bytes and are consisted of header and payload. Headers of TS packet have various information which is sync information, transport error information, PID information, transport priority information, adaptation field control information and so on. We use PID information to find program allocation table (PAT), program mapped table (PMT) and packetized elementary stream (PES) in header information of TS packets.

Fig. 1. To a watermarking DMB bit-stream, we have to find PAT or PMT packet in TS packets. If PID value of TS packet is '0', it indicates PAT. Fig. 2 shows PAT structure. PMT is presented one program map PID in PAT.

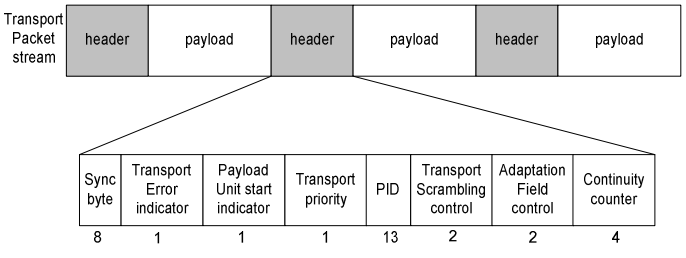


Fig. 1. A structure of DMB transport stream

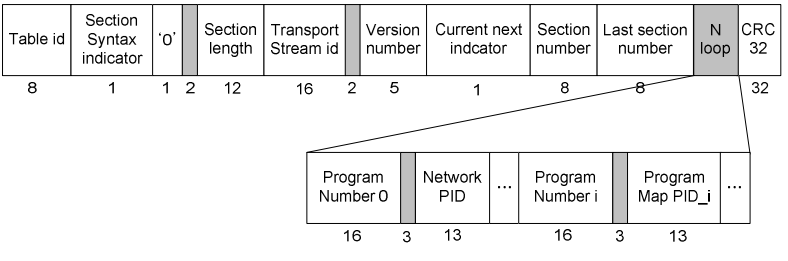


Fig. 2. PAT structure

Program map PID is included information to know where program map table (PMT) in TS. PMT is payload of TS such as PAT and include PID for elementary stream location in TS, the structure of PMT show to Fig. 3. IOD_descriptor and elementary stream ID is included in PMT, so we can find PID which includes packetized elementary stream (PES) location in TS without additional descriptors. PES is compressed video data of DMB contents.

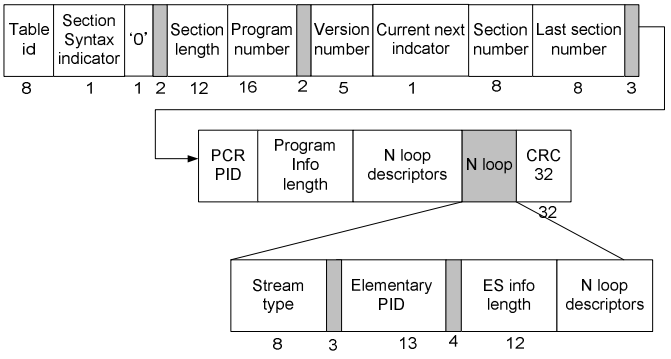


Fig. 3. PMT structure

In our implementation method, we must find padding data space in PAT and PMT. For finding padding data, we find PID '0' with TS parsing in receiving DMB stream and then find PAT on next TS packet and find PMT part in TS with 'Program map ID' in PAT. And we find value of 'Section length' in PAT and PMT.

We used TVUS 900 PMP from Homecast, Fig. 4 shows DMB processing procedure in PMP. Our implemented system embeds a watermark for play control on video stream data which is a result of TS parsing module of DMB and extracts a hidden watermark on video stream data.

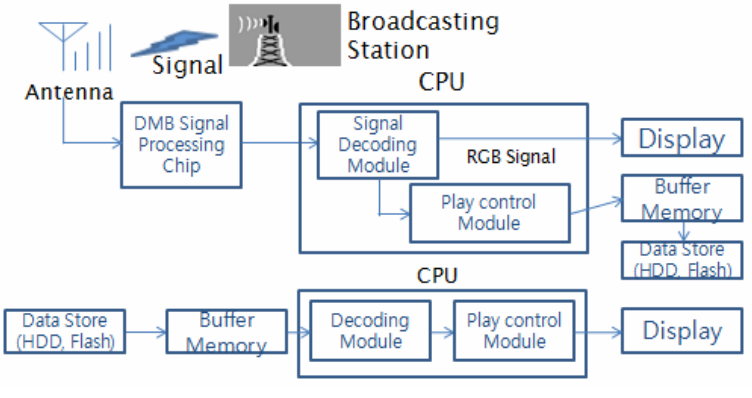


Fig. 4. Proposed PMP system structure

A TVUS of Homecast using DM320 main processor is related to internally four threads for a DMB play. Each thread is BSI, BSO, MAF and GUI. GUI handles about it in case of manipulating button on PMP and informs start of run to BSI, BSO and MAF using a start event when open the media file. BSI transfer frame information of video according to GUI event order to MAF and MAF store decoded video data using DSP in shared buffer. Saved video frame format is YCbCr(4:2:2). BSO convert YCbCr to RGB format to play stored video frame.

In DMB stream a watermarking on PMP, first of all we stored one TS packet (188 bytes size) using TSD module of BSI thread in the buffer, and then extract PAT and PMT in TS packet. PAT and PMT are indicated to 'Section Length". It indicates padding information in packet.

In this paper, we find watermarking parts for play control in DMB bit-stream, we analyzed PAT packet. PAT header has 'Selection Length' which indicates PAT data length in TS packet. If a length of PAT data sufficiently small, remaining parts except PAT data length is filled with padding data which haven't any data information. Padding data hasn't any information about a video data and header, we do hiding the play control information without any change of bit-stream format and size.

In DMB stream encryption in PMP, first of all is stored in the buffer one TS packet (188 bytes size) using TSD module of BSI thread, and then extract PAT and PMT in TS packet. PAT and PMT information is used to find PID of PES in TS packet. If payload of TS packet is PES, then we select encryption parts according to the data in the buffer. First 4 bytes of the buffer which is stored PES packet is TES header, next 18 bytes is PES header and after 22th byte in the buffer is video data parts.

In this paper, to find DMB encryption parts in PES packet check PID which know a kind of payload in PES packet. If PES payloads are video data, PID is '0x50' or '0x113'. PID indicate a video data, next step check an adaptation field value, adaptation field is payload start location in PES packet, if adaptation field value is '00b' or '10b' then do not exist payload in PES packet. Start point of payload in the buffer is IDR slice, IDR slice is included I-frame information. From data of first macro block to end data of macro block in IDR slice is encrypted by AES algorithm and then stored in PMP. If it is not IDR slice or first macro block in IDR slice then we do not encryption. Decryption procedure is loaded encryption video data in PMP hard disk using internal program of PMP, and then find encrypted payloads using the same method of encryption procedure. We decrypt encrypted macro blocks using by AES decryption algorithm.

4 Experimental Results

Used to implement the system is PMP and PC. Used PMP is TVus900 model. It made by HOMECAST Corporation, Korea. Software development tool is Microsoft's eMbedded Visual C++ 4.0 and Microsoft's Platform Builder 5.0. We ported PMP with debugging board offered from HOMECAST Corporation. Also, firmware source was offered from there.

For performance assessment, we processed the experiment as following conditions. For play encryption DMB video and decryption on PC. Specification of PC is Intel Pentium-4 2.8GHz CPU, 1GByte RAM and Microsoft Windows XP SP3. To play DMB contents in PC, we can use OnTimeTek Corporation's DMBO Filter and Gretech Corporation's GOM Player. Fig. 5 shows PMP used by this implementation.

Fig. 6 shows a play control configuration program. It is program for a play control test and this program is activated on PC. In figure, 'File' is sequence to insert the play control information and 'Remain' indicates a remaining number for DMB contents playing and 'Insert' is a number which is inserted for playing of DMB contents.

Fig. 5. Homecast™ TVUS 900 PMP

Fig. 6. A play control configuration program

Fig. 7 shows a play control program of DMB contents. This program is possible to a play control using hiding information in padding data of TS packets. DMB contents of Figure 8 is inserted play control information (in this test, we use 5).

Encryption test program is designed like PMP's encryption and decryption module using Microsoft Visual Studio 8.0's MFC code.

Fig. 8 is DMB contents encryption and decryption result using Test program. Fig. 8(a) is original content. Fig. 8(b) is encryption result of 8(a). Fig. 8(c) is decryption result of 8(b).

We used DMB contents for encryption recording ten from PMP. Used contents for test are the size of MPEG4/AVC, 320x240 that is Korean standard, and one I-frame and 29 P-frame make up one GOP (Group of Picture).

Fig. 9 is the experimental result of DMB encryption module in PMP. Fig. 9(a) is the played content in PC, not encrypted content. It is not applied to protection (encryption), we can see clearly play. Fig. 9(b) is the played Fig. 9(a) content in PMP. However, this content is not permitted to be played in PMP. Therefore, we cannot see any image but it is distorted and destroyed. Fig. 9(c) is played in PMP which is

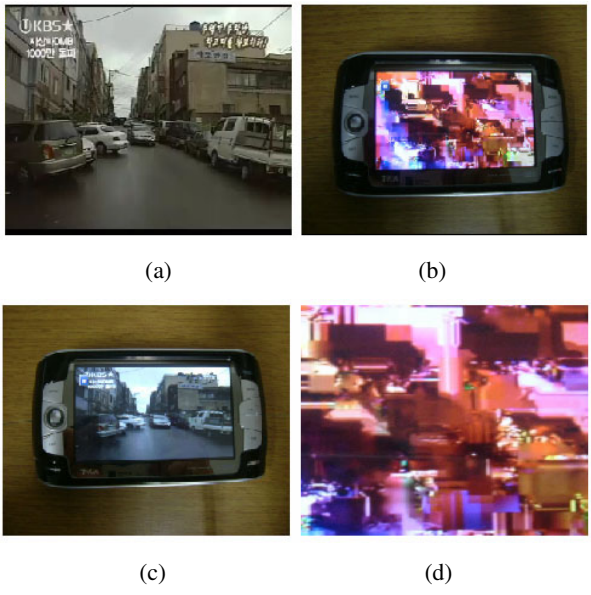
encrypted in the PMP. That content is authorized in PMP. It can be played in the PMP. Fig. 9(d) is played in PC, encrypted content. It is not played in PC that is unauthorized. Therefore, this content must not be played in PC.

Fig. 7. A play control shot of DMB contents

(a) (b) (c)

Fig. 8. Result of encryption and decryption on PC

After encrypting and recording content in test, we transfer recording files from PMP to PC and replay them in PC. In consequence, all contents did not be played normally. Also, we replay decrypted recording files in PMP applied to encryption module. Then all contents did not be played normally and output destroyed in PMP.



(a) (b)

(c) (d)

Fig. 9. Result of experiment

5 Conclusions

In this paper, we proposed real-time watermarking and encryption method for DMB contents protection. Suggested real-time watermarking hides a play control information in padding data of TS packets. . Suggested real-time encryption system encrypts only I-frame using AES algorithm. In consequence, it is not allowed to view the contents without decryption module and certification key. It is possible to use our suggested algorithm's solidity into practice. In experimental result, when we implemented a play control on PMP which have built-in DSP device to get 100Mhz processing speed, almost had not a time delay and the hiding information in T-DMB stream was possible to do a play control. Additionally, we confirmed that the saved contents in a PMP were not played in other devices without decryption key. The proposed methods can be useful in real-time applications requiring contents protection service such as video on demand, IPTV and digital TV.

Acknowledgments. This research was financially supported by MEST and KOTEF through the Human Resource Training Project for Regional Innovation, and supported by LEADER.

References

1. Wu, M., Mao, Y.: Communication-friendly encryption of multimedia. In: IEEE Workshop on Multimedia Signal Processing, pp. 292–295 (December 2002)
2. Doomun, M.R., Soyjaudah, K.S., Bundhoo, D.: Energy consumption and computational analysis of rijndael-AES. In: 3rd IEEE/IFIP International Conference in Central Asia on Internet, pp. 1–6 (September 2007)

3. Cox, I., Miller, M., Bloom, J.: Digital watermarking. Press of Morgan Kaufmann, San Francisco (2001)
4. Nishimoto, Y., Baba, A., Kurioka, T., Namba, S.: A digital rights management system for digital broadcasting based on home servers. IEEE Transaction on Broadcasting 52(2), 167–172 (2006)
5. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
6. Qiao, L., Nahrstedt, K.: A new algorithm for MPEG video encryption. In: Proceeding of International Conference on Imaging Science, Systems, and Technology, pp. 21–29 (July 1997)
7. Liu, J., Zou, L., Xie, C., Huang, H.: A two-way selective encryption algorithm for MPEG video. In: International Workshop on Networking, Architecture, and Storages, p. 5 (August 2006)
8. Zheng, L., Xue, L.: Motion vector encryption in multimedia streaming. In: Proceedings. 10th International Multimedia Modelling Conference, pp. 64–71 (January 2004)
9. T-DMB white paper Press of Electronic and Telecommunication Research Institute, Korea (December 2006)