International Journal of Signal Processing, Image Processing and Pattern
Vol. 2, No.1, March, 2009

Real-Time DMB Video Encryption in Recording on PMP

Seong-Yeon Lee and Jong-Nam Kim
Dept. of Electronic Computer Telecommunication Engineering, PuKyong Nat'l Univ.
sylee9997@pknu.ac.kr, jongnam@pknu.ac.kr

Abstract

At July 2008, the nationwide DMB (Digital Multimedia Broadcasting) has got started. As DMB device's volume of sales has been over 12 million already, the development of rapidly changing network systems has increased the dangers of infringing the copyright of DMB contents. For solving this problem, we suggest that real-time encryption algorithm without additional expenses, and implemented that on PMP. We used the SEED algorithm for encryption. As the experimental result, we confirmed that the real-time encryption and decryption of DMB videos were working well. Also confirmed that recorded contents in PMP were not replayed in other devices, and also the contents recorded by other devices were not played in PMP. Suggested algorithms can be useful in the VOD, IPTV or cable TV.

1. Introduction

As the diffusion rate of DMB device increases, the protection technology of DMB contents copyright is needed. Some DMB devices can provide the function to record DMB contents for users' convenience; they are easily exposed to copyright infringement because the duplication and dissemination are not hard. Common copyright protection systems were implemented in various ways, the common goal is not to show the contents in not permitted systems. These systems must be robust against the attack and minimize the overhead during the cording for real time processing. Also, legitimately gaining the contents applied to the copyright protection, the data must not be damaged when replaying.

In this paper, we suggest the effective copyright protection and interception ways of not confirmed users by DMB contents encryption using SEED Algorithm. For this, we implemented the real time encryption system in the PMP programmable for DMB contents copyright protection. And confirmed this way is sure to be effective, because it makes the contents destroyed without the knowledge of the key.

This composition is written about preexistence research in section 2 and described how implement the encryption for the PMP in section 3. In section 4, we subscribe the result and analyze and finished in section 5.

2. Related Works

There are lots of kinds of video copyright protection system. They include watermarking system, DRM (Digital Right Management) and image encryption. Watermarking system is concealing copyright information without deterioration [1]. It is the surest way for the copyright claim, but inappropriate for "Blocking unauthorized users" because it is not difficult when unauthorized users get videos illegally then replay. Watermark system will be

installed in the transmission terminal and receipt terminal. It is causative of additional expenses.

DRM system is more advanced than watermarking system. It is effectively blocking unauthorized users. DRM system prevents the digital contents illegal distribution and duplication, permits only users with legitimacy to use the contents and protects the contents providers by charges for using [2]. DRM system needs network infra to share the certification key. That is difficult to use for some DMB devices not having the network function. In addition, it is very expensive for implementation, because DRM system has royalty and needs the expensive computer systems and network.

Image encryption is to distribute the part or whole encrypted images. There are many kinds of encrypt algorithms - DES, AES, SEED, RSA etc. DES, AES, SEED are block-based algorithms. They are processing the fixed sizes as separated data. The block-based algorithms' encryption key and decryption key are identified. RSA is the shared-key algorithm. On the average, the block-based algorithms are faster than the shared-key algorithm.

DES algorithm was invented in 1977. However, this encryption algorithm has broken in 1997, so it is sure that it is not robust. To replace DES, AES algorithm was developed. AES is 128-bit-sized block-based algorithm. It is not accompanied with additional expenses, but the encryption speed is not fast [3].

SEED is 128-bit block-based encryption algorithm. It has been developed in KISA (Korea Information Security Agency). This algorithm is very robust and fast. Definitely, it is free and easy to implementation [4].

Encrypted images cannot be replayed without certification key. It is the right 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 [1]. The way we suggested is to operate encryption and decryption in the PMP and impossible to distribute the decrypted contents, so encryption is the best way. Existing method of encryption technique is to encrypt video's I-frame or P-frame or both. However, it is not yet implemented in embedded device (PMP or another DMB device) [5].

There are two as the kind of DMB. One is T-DMB (Terrestrial DMB) and the other is S-DMB (Satellite DMB). Both DMBs' compression algorithms are identified. For the compression, H.264/MPEG-4 Part 10 AVC technology was used. We use T-DMB; it is free charge in Korea.

Figure 1 shows T-DMB's specification [6].

Description		Contents
Frequency band used		VHF, L-Band, UHF*
Bandwidth		1.536MHz
Modulation method		DQPSK
Transmission method		OFDM
Channel coding		RS(204,188), Convolutional Byte Interleaver
Multiplexing		MPEG-4 SL, MPEG-2 TS
Audio		MPEG-1/2 Layer 2(MUSICAM)
A / V CODEC	Video	MPEG-4 Part 10 AVC(H.264)
	Audio	MPEG-4 Part 2 BSAC
Data service		MPEG-4 Part 1 BIFS PAD, NPAD, TDC, MOT, BWS, IP-tunneling, Slideshow, TTI, middleware, etc.

Figure 1. T-DMB's specification

For transportation's convenience, T-DMB signal is transmitted on MPEG-2 TS (Transport Stream) stream.

3. Implementation of DMB contents encryption in PMP

This paper suggests encryption and decryption systems not to permit to play the contents for specified devices in unauthorized users. Typical DMB device is PMP, Cellular phone, Navigation system, etc. These devices' performances are inferior to personal computer. Therefore, encryption algorithm must be lightweight. Suggested algorithm is designed as very light one.

Figure 2 is block diagram of SEED algorithm. This encryption algorithm is processed by 128bits, basically. The entire system consists of Feistel composition that encrypts input data dividing the half and using 128-bit sized key [4].

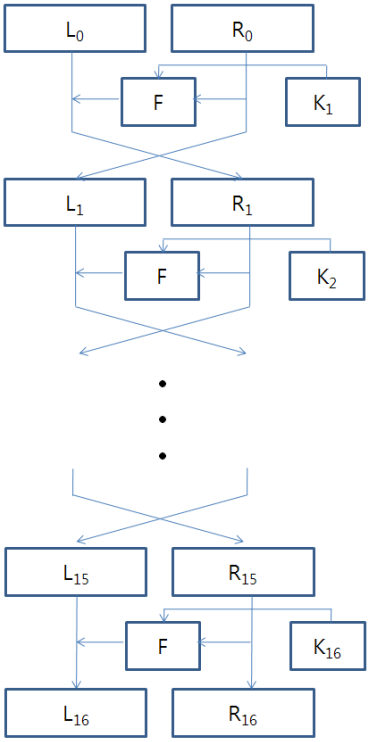


Figure 2. SEED algorithm's data flow

Suggested method is encryption. The encryption implemented in this paper encrypts the first 16 bytes (128bit) of I-frame excepting the header of recording contents, TS stream and the header of PES packet for lightweight. If the part of the header is encrypted, the whole information of the content will become encrypted so there may be a problem to the player when unauthorized contents are played. Figure 3 is MPEG4/AVC video data's frame structure.

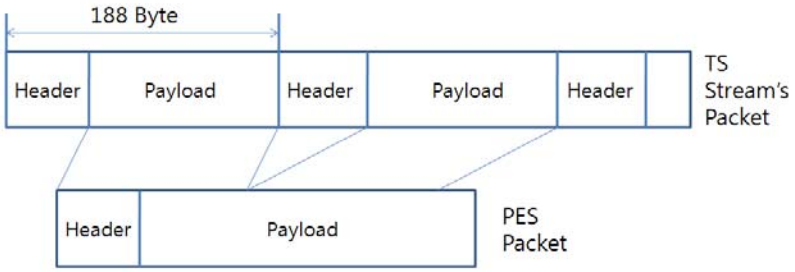


Figure 3. DMB video stream's structure

TS stream consists of 4byte size of TS header and payload. Payload is the group of PES packets. PES packet is divided to 16-byte size of PES header and variable size of payload. PES packet data includes compressed video and audio data. In this paper, the encrypted part is PES packet data's first 16 byte, not include header. When PMP plays the recorded DMB data, CPU is parsing the header data. If you encrypt the header data, CPU will not recognize the file.

The encrypted part is very small, and it is that reduces overhead of encryption. Suggest algorithm is a very small portion of an encryption. However, it is enough not to output the whole I-frame normally only with this. Small data change of first part is caused from large distortion arose from decoding process applied inversely to Huffman coding when decoding, RLE, DCT, Quantization [5]. Also next coming P-frame destroys the whole contents effectively because it decodes on a set of I-frame. Next 29 frames are P Frame. These frames are not encrypted. Also the next coming I-frame encrypts only 16 bytes in front of Payload excepting TS header and PES header. That is represented in Figure 4.

Figure 4. The part of encryption in TS stream

PMP’s main feature is to play the videos, but some PMPs provide the feature of receiving DMB. They have a signal processing chip, main processor (CPU) and buffer memory for signal processing. Figure 5 is the PMP's organization diagram.

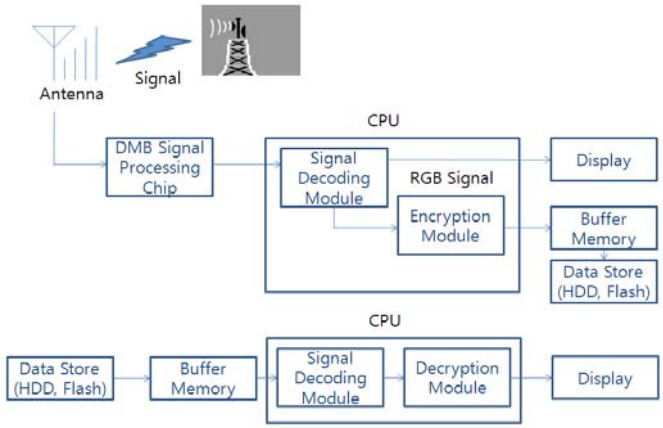


Figure 5. The Organization diagram of PMP system

Video data's encryption is processed only I-Frame. Therefore, we must know frame's class. Above all, find PID values including VIDEO stream parsing TS packet including PMT in TS packet. Next, access VIDEO stream using found PID values and exclude TS header and PES header. Then, analyze the header encoded to H.264 and we can find whether it is I-frame or not.

If it think as I-frame, we can find the encrypt part like this. First, TS packet stream's header size is fixed as 4bytes. Second, read the PES packet header's offset size. Then, jump into the video data point. That area is contains data encoded by H.264. Read it first to 16bytes, encrypt its data by encrypt module.

4. Experimental Result

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. Figure 6 is the test program for DMB contents encryption and decryption.

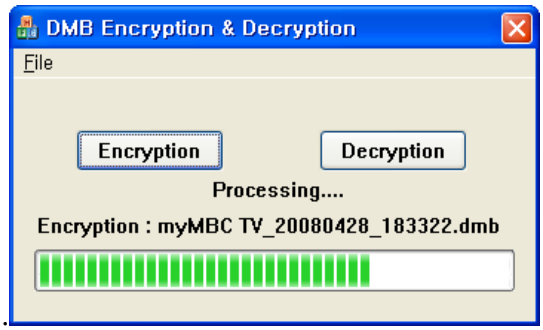
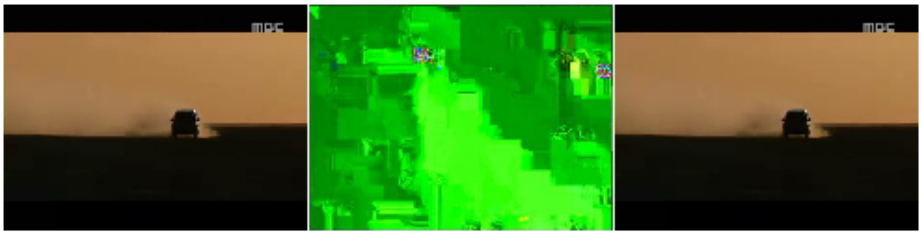


Figure 6. Test program for DMB video data's encryption and decryption

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



(a) (b) (c)

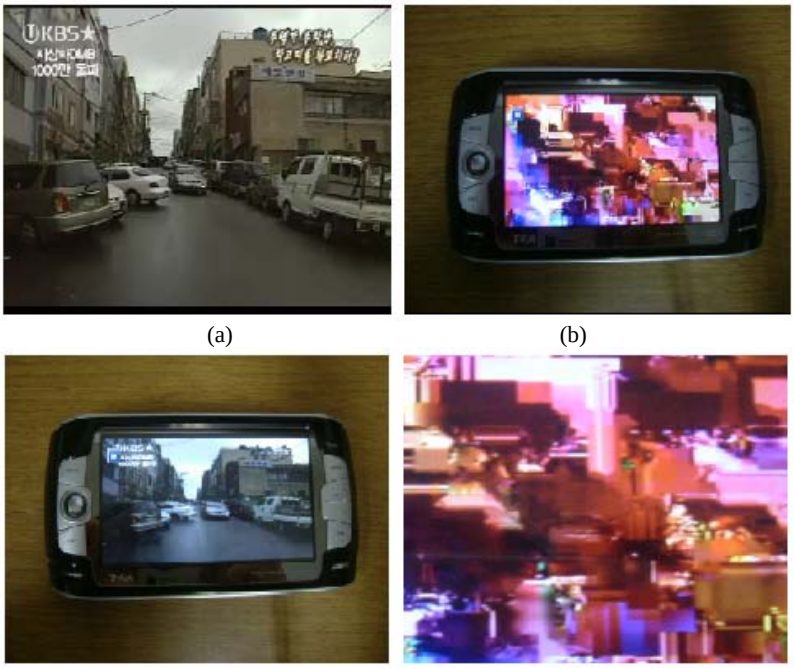
Figure 7. Result of encryption and decryption on PC

Figure 7 is DMB contents encryption and decryption result using Test program. Figure 7.a is original content. Figure 7.b is encryption result of 7.a. Figure 7.c is decryption result of 7.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).

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.

Figure 8 is the experimental result of DMB encryption module in PMP. Figure 8.a is the played content in PC, not encrypted content. It is not applied to protection (encryption), we can see clearly play. Figure 8.b is the played 8.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. Figure 8.c is played in PMP which is encrypted in the PMP. That content is authorized in PMP; it can be played in the PMP. Figure 8.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.



(a) (b)

(c) (d)

Figure 8. Result of experiment.

5. Conclusions

In this paper, we suggested the implementation of DMB contents encryption and decryption. Used programmable PMP in this paper, is TVus 900 model, which was made by HOMECAST Company. Suggested real-time encryption system encrypts only I-frame's first 16 bytes using SEED 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. This algorithm is applicable to anything for copyright protection like not only DMB broadcasting, but also VOD, IPTV.

Acknowledgement

This work was supported from Advanced Technology Project by SMBA and RIS Project by KOTEF.

References

.

[1] I. Cox, M. Miller, and J. Bloom, “Digital Watermarking,” Press of Morgan Kaufmann, San Francisco, Oct. 2001.

[2] Y. Nishimoto, A. Baba, T. Kurioka, and S. Namba, “A digital rights management system for digital broadcasting based on home servers,” *IEEE Transaction on Broadcasting*, VOL. 52, NO.2, pp. 167-172, Jul. 2006.

[3] W. Stalling, “Cryptography and network security: principles and practice 3/E,” Press of Prentice Hall, New Jersey, 2002.

[4] “A design and analysis of SEED,” Press of Korea Information Security Agency, 2003.

[5] L. Qiao and K. Nahrstedt, "A New Algorithm for MPEG Video Encryption," *Proc of the First International Conference on Imaging Science, Systems, and Technology (CISST'97)*, pp. 21-29, Jul. 1997.
[6] "T-DMB White Paper" Press of Electronic and Telecommunication Research Institute, Korea, Dec. 2006.
[7] "Information Technology - Coding of Audio-Visual Objects - Part2: Visual, ISO/IEC 14496-1:2001", ISO/IEC/SC29/WG11, Nov.1998.
[8] Jyh-Ren Jerry Shieh, "On the security of multimedia video information," *Proc. IEEE 37th Annual 2003 International Carnahan Conference*, pp. 51 – 56, Oct. 2003.
[9] L.S. Choon, A. Samsudin, and R. Budiarto, "Lightweight and cost-effective MPEG video encryption," *Proc. IEEE Information and Communication Technologies: From Theory to Applications*, pp. 525-526, Apr. 2004.
[10] W. Zeng, "Format-Compliant Selective Scrambling for Multimedia Access Control," *Proc of IEEE ICASSP*, pp. 77-80, Apr, 2002.

Authors

Seong-Yeon Lee He received the B.S. degree in computer science from Pu-kyong National University, Korea, in 2008. He is currently working towards the M.S. degree in the Division of Electronic, Computer and Telecommunication Engineering at Pu-kyong National University, Korea. His research interests include image/video compression, image processing, image/video encryption for copyright protecting.

Jong-Nam Kim He received the M.S. and Ph.D. degree from Gwangju Institute of Science and Technology (GIST), Korea, in 1997 and 2001 respectively. He worked for the Technical Research Institute (TRI) of Korean Broadcasting System (KBS) from 2001 to 2004. From 2004, He joined Department of Computer Engineering of Pukyong University as an adjunct professor. His research interests include image/video processing, image/video compression, image/video watermarking, video communication, and VLSI design for real-time video applications.