Broadcasting System Compliant with MPEG-2/4 IPMPX

Yongju Cho, Jongwon Seok, Jinwoo Hong, and Chieteuk Ahn

In this paper, we present an intellectual property management and protection (IPMP) system in a broadcasting environment to provide mechanisms for copyright and contents protection that are compliant with the MPEG-2 and MPEG-4 IPMP Extension (IPMPX) specifications. The technology for processing IPMP related information was exploited, and a terminal model has been successfully designed and implemented. In addition, interoperability, which is the main objective of MPEG-2/4 IPMPX, has been addressed in detail. The experimental results show that the implemented system performs the IPMP process well, meeting the requirements of a broadcasting environment.

Keywords: MPEG-2, MPEG-4, IPMPX, CAS.

I. Introduction

Recently, the introduction of digital media has had a tremendous impact on the development of the Internet, telecommunications, and broadcasting systems. It has enabled a dramatic reduction in the expense and time of content production. In addition, the rapid popularization of the Internet, wireless communication systems, and digital broadcasting networks have lead us to an epochal framework for content distribution and consumption. Widespread use of multimedia PCs and digital TVs have accelerated the purchasing and consumption of a vast number of media content types. These developments, however, have forced us to consider the production, transmission, distribution, consumption, and copyright protection and management of media content in a new light. A mutual linkage between networks, compatibility, and intellectual property and management (IPMP) have come to the foreground as very important fields of research.

The need for IPMP is a very serious issue to consider in a broadcasting environment. As digital technology continues to play an important role in broadcasting and communications, future broadcasting may lead us to a new paradigm of services and content that we have never before experienced. For advanced services, the development of high-quality content is important, as is the development of efficient technologies. However, if there are no proper methods for protecting and managing media content, we can hardly expect the creation of high-quality media production to flourish since so much money, time and endeavor must first be invested.

Nowadays, research and development in IPMP have received an increased interest from several international standardization groups, such as the Moving Picture Expert Group (MPEG), Open Platform Initiative for Multimedia

Manuscript received Apr. 8, 2003; revised Jan. 27, 2004.

Yongju Cho (phone: +82 42 860 6138, email: yongjucho@etri.re.kr), Jinwoo Hong (email: jwhong@etri.re.kr), and Chieteuk Ahn (email: ahnc@etri.re.kr) are with Digital Broadcasting Research Division, ETRI, Daejeon, Korea.

Jongwon Seok (email:jwseok@changwon.ac.kr) is with Changwon National University, Changwon, Korea.

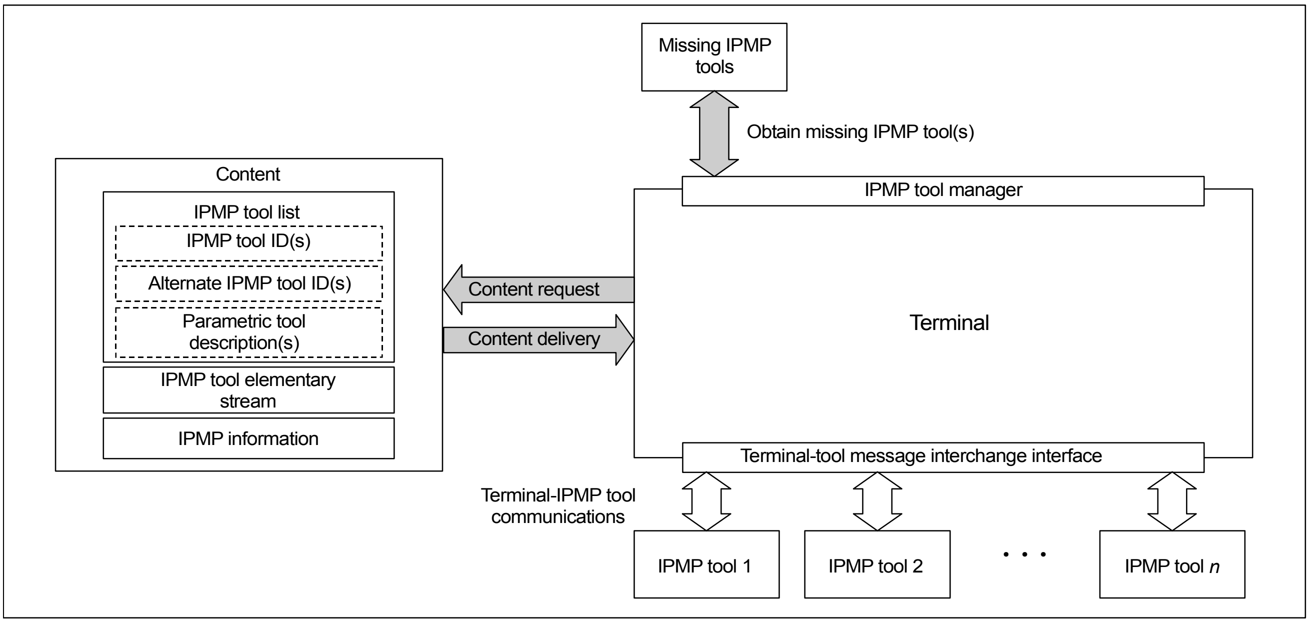

Fig. 1. A basic structure of MPEG IPMP.

Access (OPIMA) and Secure Digital Music Initiative (SDMI). In particular, MPEG has actively been working on establishing a standard for MPEG-2 and MPEG-4 IPMP Extension (IPMPX) to efficiently and systematically secure digital content and copyrights [1], [2].

Not only do MPEG-2 and MPEG-4 IPMPX provide functionalities for content identification and protection, but they also provide for the interface between a terminal and the various IPMP tools used to safely protect and efficiently manage content within a terminal. In addition, one important goal, the interoperability between a terminal and IPMP tools, can be accomplished by the creation of an MPEG-2 and MPEG-4 IPMPX-compliant interface [3].

This paper describes copyright and content protection and a management broadcasting system that are compliant with MPEG-2 and MPEG-4 IPMPX. The system is designed and implemented to parse and process both MPEG-2 and MPEG-4 IPMPX data used to apply the proper IPMP tools at a defined control point[1)] in a terminal and to process protected MPEG-2 and MPEG-4 media data and copyright information along with the needed IPMP tools.

The proposed hybrid system-compliant MPEG-2 and MPEG-4 IPMPX affords secure protection and management of MPEG-2 and MPEG-4 media content and copyright information in a digital broadcasting environment. It may also be used in the near future as a reference model for security systems and applied in many different fields.

1) A point on a given elementary stream or given object in a terminal where IPMP processing for media data shall be carried out.

This paper consists of the following. Section II gives an explanation of the general MPEG IPMPX, including the procedure for IPMPX in a terminal. Section III introduces the structure of the proposed broadcasting system, and a procedure for content consumption is described in detail. Section IV discusses our simulation results including an MPEG-2/4 IPMP procedure and security tools. Finally, on the basis of the simulation results, the strength of the proposed system is indicated in section V.

II. MPEG IPMPX

IPMP, an MPEG term of Digital Rights Management, is a technology used to provide efficient and systematic copyright protection and management of multimedia content [4], [5]. IPMP embraces such technologies as encryption for content protection, watermarking for copyright protection, and management of content and copyrights. In addition, it provides interoperability by defining the interface between a terminal and IPMP tools. Figure 1 shows a basic structure of an MPEG IPMPX system. As shown in the figure, the IPMPX system consists of a terminal (system decoder), IPMP tools, and an interoperable interface. A terminal is a platform used to consume media content with respect to MPEG IPMPX specifications. An IPMP tool is an entity used to provide content encryption, decryption and watermarking. The interface is a standard for supporting exchanges of IPMPX related data between a terminal and IPMP tools.

IPMP system procedures are as follows:

Step 1. Content Request by a User

IPMPX data is conveyed to a terminal at the same time as, or prior to, media content. The information concerning the access or restriction of the content shall be transported before the transmitting of the media stream.

Step 2. Parsing of IPMP Tool Information

A terminal receives the IPMP tool list information and determines which tools to be used for media content consumption.

Step 3. IPMP Tool Set-up

When the required tools are not available in a terminal, they are downloaded to the terminal. If the tools are located in the terminal, this procedure is not necessary.

Step 4. Instantiation of an IPMP Tool

A terminal instantiates the required IPMP tools.

Step 5. Initialization of IPMP Tools and Media Contents Consumption

With the initial information about the IPMP tools, a terminal initializes the tools. Secured (encrypted or watermarked) media content are then conveyed to the determined IPMP tools to make them accessible in a terminal.

Using the defined procedure above, a terminal exchanges data, at which point content protection and management can then be achieved by connecting the IPMP tools with the predetermined control points such as the ones just prior to or after decoding.

A content generator, on the other hand, shall define and include IPMP data within the media content so a terminal can recognize how to access the content.

III. Broadcasting System Compliant with MPEG-2/4 IPMPX

The structure of the proposed security system and a procedure for content consumption are described in detail in this section.

1. Structure of the Broadcasting System

Basically the terminal resembles a set-top box except for the front-end, which receives the broadcasting waves. Broadcasting contents are encrypted and watermarked MPEG-2 and MPEG-4 for protection and management.

The broadcasting terminal consists of several entities and modules used for copyright and content protection as well as management of broadcasting contents: MPEG-2 modules to process MPEG-2-related content, MPEG-4 modules to process MPEG-4-related content, and IPMPX modules to process

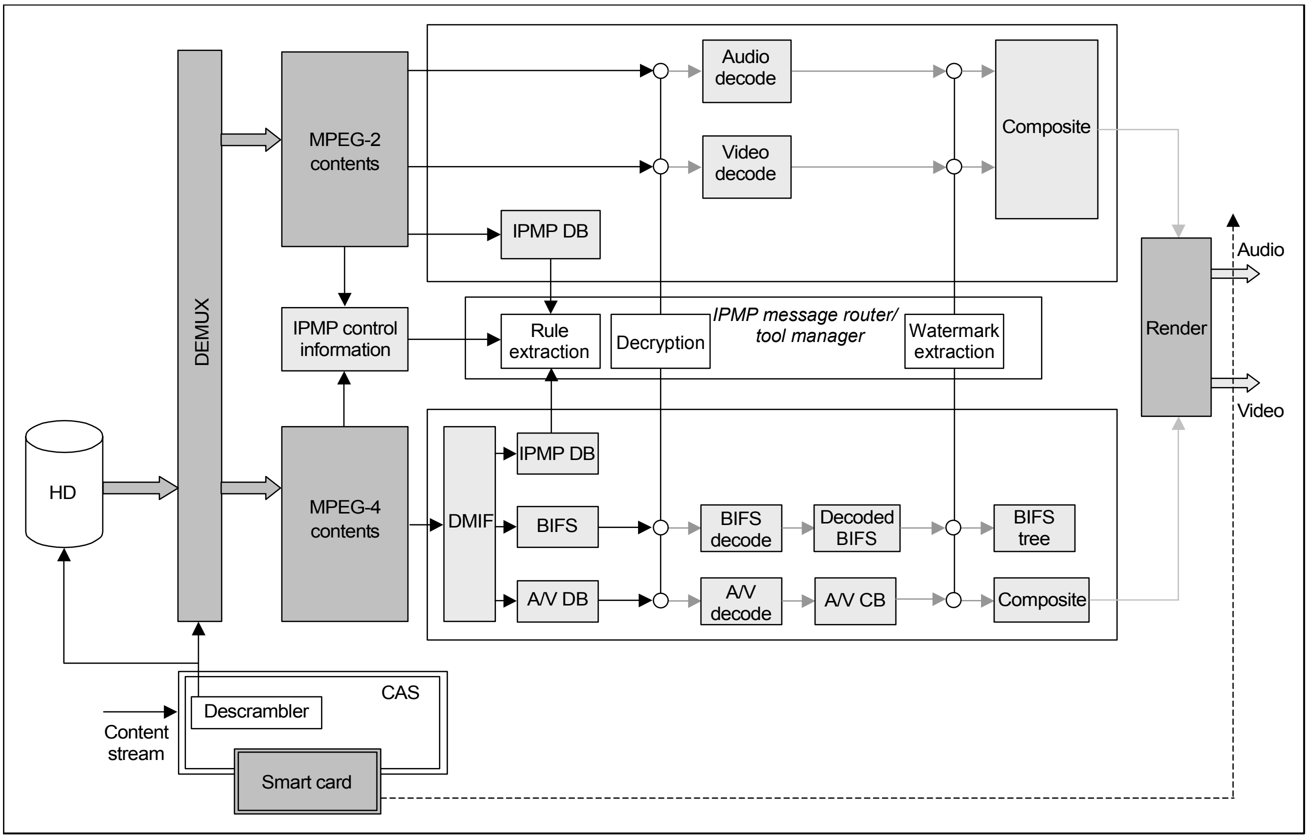

Fig. 2. The structure of proposed system.

IPMPX data from MPEG-2 and MPEG-4 data. MPEG-2 modules contain audio and video decoders, a demultiplexer, and a conditional access system (CAS), whereas MPEG-4 modules consist of an Initial Object Descriptor/Object Descriptor (IOD/OD) decoder, a BIFS decoder, and an audio and video decoder. IPMPX modules include a Tool Manager (TM) and Message Router (MR) in the system decoder, IPMP tools to decrypt/de-watermark secured contents, and a message interface between a broadcasting terminal and the IPMP tools [4]. Figure 2 shows the structure of the system, and a functional description for an individual module is as follows.

A. MPEG-2 Modules

▫ MPEG-2 Demultiplexer

A demultiplexer receives and demultiplexes an MPEG-2 transport stream (TS) consisting of the required packets. Each packet is 188 bytes in size and has its own packet ID. A TS contains packets for the Program Specific Information (PSI) and Program Elementary Streams. The PSI is classified into five tables, a Program Association Table, Program Map Table, Conditional Access Table, Network Information Table and a TS Description Table.

The Program Association Table provides the correspondence between a program number and the packet ID value of the TS packets. The Program Map Table provides the mappings between the program numbers and the program elements that comprise them. The Conditional Access Table is required in order to include needed information about scrambled programs, while the Network Information Table is used to contain the information about the physical network.

▫ Conditional Access System

The CAS extracts the conditional access information from the Entitlement Management Message (EMM), the Entitlement Control Message (ECM) and the Conditional Access Table in the scrambled broadcasting content. Using the extracted control word and access information, it decodes the scrambled content and determines the access level and usage. The CAS relies upon two independent mechanisms: the scrambling of the AV stream and the management of commercial entitlements, which have to be transmitted as secured messages to the descrambler box (control access). Scrambling can easily be applied to a media stream. In this case, all of the bits are encrypted using an encryption algorithm such as Data Encryption Standard (DES). The data is scrambled using a control word. The control word or key will change after a short period. To send the new keys to the descrambler, ECM and EMM are used [6], [7].

An ECM is transmitted together with the scrambled signal. An EMM is generally not transmitted in a synchronous way with the program to which it applies. It must be transmitted in advance in order to give access to the authorized consumer. Any network can be used to transmit the EMM to the receiver: via modem, mail, or broadcast stream.

B. MPEG-4 Modules

This subsection shortly describes the basic MPEG-4 modules [8]-[11].

▫ OD/IOD Decoder

An Initial Object Descriptor (IOD) decoder is assigned to parse the IODs that contain initial access information such as the profile and level of MPEG-4 content, including a Tool list descriptor to indicate the IPMP tools required to access the media content.

An OD contains elementary stream descriptors used to express the logical dependencies of the elementary streams and Tool descriptors used to describe the IPMP tools required to access the media content. The OD decoder parses the information conveyed in the OD stream.

▫ MPEG-4 Audio/Video Decoder

An MPEG-4 Audio and Video decoder decodes different types of audio and video media content, such as H.263, MPEG-4 video, G.723.1, MPEG-2 AAC, JPEG, BMP and GIF that are broadcasted as additional data for a main program.

▫ BIFS Decoder

A BIFS decoder parses the scene description information, i.e., the temporal and spatial placement of AV objects. It also organizes the AV objects conveyed in the OD using this information.

C. IPMP Modules

▫ Tool Manager

A TM parses the IPMP tool list in the IOD to determine the tools to be used for the protection of secured (watermarked/encrypted) contents or copyright information and loads the tools into the terminal. In addition, it is assigned to download any missing tools by means of an IPMP tool stream and to connect the terminal and tools at defined control points using the IPMP information parsed and sent out by the MR.

▫ Message Router

The MR is allotted the important role of communicating with the tools by using defined messages. It first parses the Tool Descriptors conveyed in the OD stream, and then it sends the parsed data to the TM for further control in the terminal and to the tools for data consumption. After the initial process, it exchanges messages with the tools according to the MPEG-4 IPMPX interface.

▫ Message Interface

The TM/MR interfaces with the IPMP tools in the form of messages defined by the MPEG-4 IPMPX. The messages have their own structure and are used between the TM/MR and IPMP tools according to the purpose of their usage. All terminals and tools supporting this message interface can communicate with each other. In other words, interoperability is achieved with use of the interface.

▫ IPMP Tool

The IPMP tool can be used as an encryption or watermarking tool to support copyright and content protection and management. It can also be used to check the integrity of the media content or to extract copyright information. Any IPMP tool can communicate with any MPEG-2 or MPEG-4 IPMPX terminal by using the defined message interface.

For audio watermarking, a new echo embedding technique is developed, which improves the robustness of signal processing attacks without deteriorating the host audio quality [12]. A watermarking system can embed a relatively large echo without compromising quality. It increases the reliability of the system, and thus its robustness. In order to make this possible, an echo kernel is designed based on psychoacoustic analysis. Watermarking is evaluated through subjective quality and robustness tests, and the results are compared with conventional echo embedding methods. Moreover, to obtain a further increase in robustness under a signal processing attack, some novel techniques are applied, such as a dual-echo kernel method, pilot kernel method, start-point synchronization method, etc. A watermark embedding and detection procedure follows the SDMI Phase 2 screen functionality. We embed a watermark and compress the corresponding audio file using an Advanced Audio Coding (AAC) or Audio Coding-3 (AC-3) encoder. The robustness of the watermarking is already checked by the SDMI robustness test procedure.

The video watermarking tool applied in the proposed system is used to embed video content ID into the host data using a spread spectrum method [13]. For video watermarking, we have to consider two points, flickering effects and compression techniques. If the watermark is embedded into the portions where there is no similarity between frames, the flickering effect may be reduced, and the watermark will be robust against MPEG compression. For these reasons, the payload of length L is divided into k round-payloads of n bits. Each round-payload is embedded into r frames to resist frame attacks. Watermarking is used to construct watermarking region R using the motion features of video frames and to add the watermark into the discrete cosine transform coefficients of region R. Region R, for watermarking, is retrieved from three continuous frames $f(t)$, $f(t+1)$ and $f(t+2)$ by computing the values between two frames. These values are used to indicate the motion feature of the video frame, that is, whether or not there is a lot of motion between frames. Extraction of the payload is based on the correlation values scheme between the watermarked region and the watermark. Watermarked video frames have about a 43dB peak signal-to-noise ratio, and a robustness against MPEG 2 as well as re-compression can be provided. Also, the proposed method is robust against frame attacks such as frame dropping, frame averaging, and frame collusion.

2. Procedure of the Proposed System

This section describes the entire IPMPX procedure in detail, as shown in Fig. 3, from reception to consumption of the media content in the proposed broadcasting system, compliant with MPEG-2 and MPEG-4 IPMPX. This section also consists of the procedural steps to initiate a terminal and the IPMP tools and to protect and manage the copyright and content.

A. Process of Terminal and Tool Initiation

A broadcasting system receives the streaming or file format of the MPEG-2 or MPEG-4 content (TS/mp4/trif) as input and decodes the IPMP control information table in the PSI or the IOD first-enclosing tool list descriptor to find the IPMP tools required to access the content and initial access information. When the required tools are ready to be used in the terminal, the TM instantiates the tools. When the required tool is absent, the TM is assigned to download the missing tool through the IPMP tool elementary stream with the alternative tool information indicated in the tool list descriptor. The MR parses the tool descriptors, including the control point information, and sends the information to the TM to connect the IPMP tool at the defined control point, as shown in step 2 in Fig. 3.

Once the required tools are connected with the terminal at the defined control point, the IPMP data containing the initial information about the tool, and conveyed by means of the IPMP stream, is sent to the tool by the MR in the form of a message. The tool initializes itself with this information. The terminal and tools instantiation process is then finished, and the terminal and tools are ready to consume the media content.

B. Process of IPMPX

After the initialization process, the terminal starts performing the IPMP process to consume the content. If the content is encrypted and watermarked, the terminal consumes the AV media content using 2 different tools at the defined control points--before and after the media decoder.

First, the encrypted media content is sent to the determined decryption tool in the form of a message and is decrypted by the tool using its own process (step 3). Communication between the MR in a terminal and the tools is based on an MPEG-2 and MPEG-4 IPMPX-compliant message interface. The decrypted content is then conveyed back to the media decoder through the MR (steps 4 and 5).

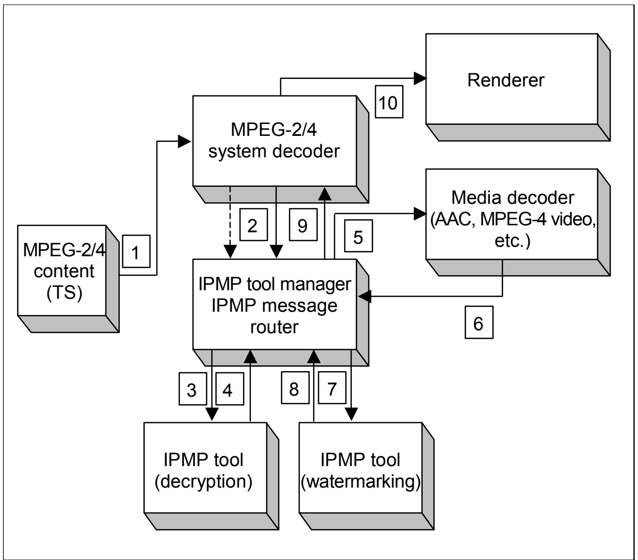

Fig. 3. System procedure.

The decoded media content is still watermarked and accordingly sent to the defined watermarking tool in the same way as the encrypted content (step 7). After extraction of the watermarked information, the media content and the watermarked information are sent back to the TM and rendered for display or further processing (steps 8 thru 10). In the proposed system the watermarked information is used for content usage or content integrity, checking the information used in the terminal for content/copyright protection and management.

It is, however, important that the terminal check the IPMP control information table in the PSI and IOD, periodically, and perform the entire process if needed, since the required tools and usage restrictions for accessing certain content varies according to the type of content or the user's rights.

IV. Experimental Results

1. Experiment

The proposed broadcasting system was successfully implemented on a regular PC using no special hardware for MPEG-2 and MPEG-4 decoding or security tools. In order to verify the proposed system with MPEG-2 content, four different TS files from such genres as sports, movies, and education were used. MPEG-2 media content, watermarked as AC3 audio and MPEG-2 video, were used for this experiment. To support conditional access in the system, we generated a Conditional Access Table, ECM and EMM packets transmitted as a TS. To support MPEG-2 IPMPX, an IPMP control information table was also generated to contain the tool lists and tool information. (IPMP tool descriptors were also contained in the Program Map Table). To consume the MPEG-2 content, an MPEG-2 system consisting of a video and AC-3 decoder was used.

MPEG-4 reference software, IM1 2D player v5.7, was used as the MPEG-4 system decoder consisting of the IOD/OD, BIFS, and AV decoders for MPEG-4 content. The MR/TM was realized and linked to the MPEG-4 system decoder to form an IPMPX compliant terminal. A trif file of MPEG-4 content was used to test and verify the proposed system. As MPEG-4 media content, the AAC audio data was encrypted with a symmetric key. It was also watermarked with ASSERT and No More Copy (NMC) information to check content integrity and usage restriction.

For IPMP tools, we implemented symmetric encryption, decryption, and AV watermarking tools, as described in section III.1, and tested them with the proposed IPMP terminal for the experiment. Since the objective of the experiment was not to test the performance of the tools but to verify the IPMP procedure in the system, a simple symmetric encryption tool and decryption tool were each implemented using an 8-bit key. The functionality of the AV watermarking tools is described in section III.1.

In addition, the interface between a terminal and IPMP tools followed the message interface, as defined in MPEG-2 and MPEG-4 IPMPX specifications.

2. Results

The proposed system successively executed content/copyright protection and management. Figures 4 and 5 show an initial screen and an example of the main display window. Also, the entire IPMP procedure is depicted in Fig. 6. The debug window shows individual object information and the IPMP process including conditional access, IPMP message exchanges, and watermarking results.

Decryption and watermarking processes for AAC and AC-3 audio data also performed successfully in the system by the exchange of IPMP related information between the terminal and the IPMP tools.

Fig. 4. Initial screen of the client for broadcasting.

Fig. 5. An example of the main display window.

The IPMP process results, the hidden information of ASSERT and NMC, as shown in Fig. 6, proved that the system performed as expected. However, due to the limited computational power for decryption and the de-watermarking process of both audio and video, the system slowed down and could not perform seamless decoding. In the case of the Advanced Encryption Standard, applied solely to the video, though, the system supported real-time processing. Therefore, more optimized IPMP tools will be required for real-time processing when both audio and video content are used. Otherwise, only selected content will need to be IPMP-applied.

Since the audio watermarking tool extracts the hidden information every 15 seconds, the extracted information is sent to the terminal to check the integrity and usage restrictions of the media content, accordingly, and is then displayed periodically. As depicted above, the proposed system, which is compliant with MPEG-2 and MPEG-4 IPMPX, has been successfully tested and verified, although limited media resources and IPMP tools were used for the experiments. For a more accurate verification of the system, various types of content and tools such as Data Encryption Standard will be tested later. However, the current experiment clearly shows that the proposed system performs the IPMP process securely and achieves interoperability by meeting the requirements of an MPEG-2 and MPEG-4 IPMPX interface. Moreover, we believe that the constraints mentioned above will be resolved by implementing them as a hardware and in mobile environments which adopt the IPMP system.

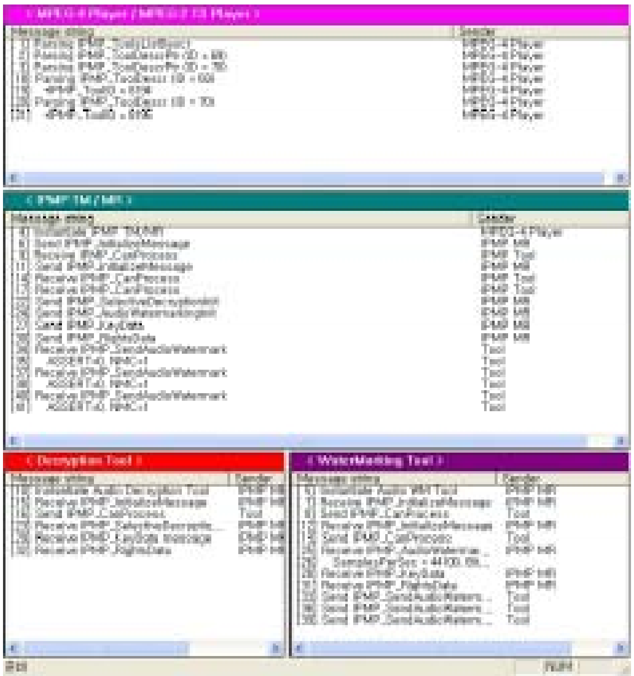

Fig. 6. Debug window showing the entire procedure.

V. Conclusion

The fast development of digital communication has brought a great deal of convenience to users and has recently resulted in the growth of digital content related industries. This growth has enabled digital content to be easily produced, copied and distributed anywhere in a short period of time. However, it has also highlighted the need to resolve copyright and content protection problems which have definitely affected technology development. The development of a security system to effectively solve these problems is seriously required.

For this reason, many standardization groups and industries have put their efforts on the R&D of content/copyright protection and management. We have proposed a security system that is compliant with MPEG-2 and MPEG-4 IPMPX as a solution for this important security problem. The proposed system performs copyright/content protection and management systematically and efficiently. In addition, it also provides an interoperability that is distinguishable from others by defining its own message interface. This interoperability enables IPMP entities and modules to be easily adapted to any terminal, and enables IPMP tools to be applied to the terminal. As an example of its potential application, the interactive broadcasting terminal providing various services to users can utilize the IPMP mechanism for secure content consumption in a broadcasting environment. The proposed system can resolve possible conflicts over copyright between content producers and consumers. It will also help industries related to production, transmission, distribution, consumption, and copyright protection and management for content to bring about a revolution of technical improvements.

In the future, further studies will be needed for more accurate verification. More detailed mechanisms, including copy control, retention control, and super distribution, will also be required.

References

[1] Craig A. Schultz, *Information Technology – Coding of Moving Pictures and Audio: Study of FPDAM ISO/IEC JTC1 SC29 WG11 N4849, FPDAM ISO/IEC 14496-1:2001/AMD3*, May 2002.

[2] Wookjoong Kim and Jinwoong Kim, "MPEG-21 Multimedia Framework Summary and its Trend," *Broadcasting and Technology*, vol. 81, 2001 (in Korean).

[3] Rob Koenen, *Information Technology – Coding of Moving Pictures and Audio*: *Overview of Intellectual Property Management and Protection in MPEG Standards*, 2001.

[4] ISO/IEC JTC1 SC29 WG11 N4701, FPDAM ISO/IEC 14496-1:2001/AMD3, Mar. 2002.

[5] ISO/IEC JTC1 SC29 WG11 N4701, ISO/IEC 13818-1:2000 FPDAM2, Mar. 2002.

[6] Digital Video Broadcasting (DVB), *Support for Use of Scrambling and Conditional Access (CA) within Digital Broadcast Systems*, ETSI (Informative), ETR289 ed.1, Oct. 1996.

[7] Digital Video Broadcasting (DVB), *DVB SimulCrypt; Part1; Head-End Architecture and Synchronization*, TS101 197-1 v.1.1.1, June 1997.

[8] ISO/IEC 14496-1, *Information Technology – Coding of Audio-Visual Objects: Systems*, International Standard, 1999.

[9] ISO/IEC 14496-1, *Information Technology – Coding of Moving Pictures and Audio: Systems*, Study of Draft Technical Corrigendum 1, 2000.

[10] Ji Ming and Craig A. Schultz, ISO/IEC JTC1 SC29 WG11 N4850, *Information Technology – Coding of Moving Pictures and Audio: MPEG-2 and MPEG-4 IPMP Extension Reference Software Architecture Based on IM1*, May, 2002.

[11] ISO/IEC JTC1/SC29/WG11 m3111, *APIs for Systems Software Implementation*, Nov. 1997.

[12] Jongwon Seok, Jinwoo Hong, and Jinwoong Kim, "A Novel Audio Watermarking Algorithm for Copyright Protection of Digital Audio," *ETRI J.*, vol. 24, no. 3, June 2002, pp. 181-189.

[13] Hyejoo Lee and Jinwoo Hong, "Video Watermarking System Using Selection and Overlapping of Region by Features of Consecutive Frames," *Proc. SPIE*, vol. 5020, 2003, pp. 462-470.

Yongju Cho received the BS and MS degrees in electrical and computer engineering from Iowa State University in the U.S.A. in 1997 and 1999. He joined the Electronics and Telecommunications Research Institute (ETRI) in Korea as a member of engineering staff in 2001 while going on for a doctorate. Since then, he has been engaged in the Development of a Data Broadcasting System based upon MPEG-4 systems, IPMP and in the MPEG-21 area. His research interests include digital signal processing in the field of data broadcasting and multimedia systems.

Jongwon Seok received the BS and MS degrees in electronics from Kyungpook National University, Taegu, Korea in 1993 and 1995, and the PhD degree in electronics from the same university in 1999. He was a Senior Member of the Research Staff in the Electronics and Telecommunications Research Institute (ETRI) from July 1999 to February 2004, where he engaged in the Development of a Multichannel Audio Codec System, Digital Broadcast Content Protection and Management. Since March 2004, he has been with Changwon National University, where he is currently an Assistant Professor at the School of Computer, Information and Communications. His research interests include digital signal processing in the field of multimedia communications, multimedia systems, and digital content protection and management.

Jinwoo Hong is a Team Leader and Principal Member of the Technical Staff in the Digital Broadcasting Research Division of ETRI, Korea. He received his BS and MS from Kwangwoon University, Korea, in Feb. 1982 and 1984, and the PhD from the same university in Aug. 1993. Since he joined ETRI in 1984 he has been involved in developing digital audio systems, IPMP, and broadcasting technology. His recent work has been focused in developing a multimedia framework for convergence of broadcasting and telecommunication based on MPEG-21 technology. His main interests are in the areas of multimedia signal processing, IPMP, and digital audio broadcasting.

Chieteuk Ahn is Vice-President and a Principal Member of the Technical Staff in the Digital Broadcasting Research Division of ETRI, Korea. He received the BS and MS from Seoul National University, Korea, in Feb. 1980 and 1982, and the PhD from University of Florida, U. S. A. in Aug. 1991. Since he joined ETRI in 1982 he has been involved in developing digital switching systems, MPEG standardization and broadcasting technology. His recent work has focused on MPEG technology as well as in developing interactive multimedia technology. He has served as an HOD of MPEG-Korea and SC29-Korea since 1996. His main interests are in the areas of multimedia signal processing, broadcasting and communications.