A Study on DRM System for On/Off Line Key Authentication

Kun-Won Jang†, Chan-Kil Park ††, Jung-Jae Kim ††† and Moon-Seog Jun††††

Dept of computer Science, Soongsil University, Postal Code 156-743, Seoul, Korea

Summary
This paper proposes hash chain algorithm that generates more secure key than conventional method and secure encryption method that each key generated by hash chain algorithm is respectively applied to block. Also, we encrypt separate key using key separate method after authenticating user by user authentication method via on/off line, and attacker cannot get complete key although the key is disclosed by sending the key to client one by one. After we design and implement proposed system, we take experiment for a performance analysis using various size of digital content files. As a result, proposed system can securely transmit a key, and the key is encrypted not to decrypt whole data against key disclosure. Finally, the time for an encryption and decryption is analogous to conventional method when client system replays video file.

Key words:
DRM, Symmetric key, Agent, PKI.

1. Introduction

The generalization of Internet incurs the modification of digital information through cyber space. As the distribution context of digital information resource changes quickly, the demand of digital contents such as sound, picture, image, and publication increases rapidly. However, the popularity of digital content brings inevitably the need of digital right management against illegal reproduction because digital writings may be copied without deterioration

For protecting digital writings, we need information security technology for stability and security and DRM (Digital Right Management) technology for the watch of digital right and whole distribution process [2].

Many researchers proposed various DRM technologies that protect digital right against the violation of intellectual property rights and provide trusted environment for production, distribution and usage of digital writings [4].

Conventional DRM solutions take many times because system encrypts data with a secret key and user must decrypt it when downloading a file

Also, when decrypting data, a large sale of digital writings must be replayed only after decrypting whole file, so user cannot replay it in real time. Addition to this, because a secret key for encryption and decryption is transmitted via wired network, attacker may get the key and the security of digital writings become vulnerable [1].

Manuscript received August 2005.

Accordingly, this paper proposes DRM system using on/off line key transmission method for solving DRM system problems, provides services such as user authentication and decryption key distribution of encrypted data for digital writings, and proposes unified DRM system for preventing illegal replay.

2 Conventional DRM system

2.1 InterTrust's DRM system

The feature of InterTrust's DRM solution is to use encryption technology and watermarking for work protection, and achieves the collection of particulars, record, and payment treatment according to the rule. This system uses the agent to achieve payment treatment, license, and the execution of work. Because the encrypted work may be distributed in advance, license agent confirms the license, transmits the information of payment, and contracts a business when user uses the work on computer. Accordingly, user can use the payment method as credit card or e-money [6, 7, 8]. Also, because the writings may be protected by encryption, users can exchange the writings each other as redistribution (Super Distribution) [2].

However, InterTrust's DRM system can replay the data after decrypting it. Because the data is encrypted by only one key, this data is not secure if the key is exposed. Also, because the entire file is encrypted, the time to encrypt and decrypt the file is longer than other system, and the file can be replay only after decrypting an entire file at the replay

2.2 Microsoft's DRM system

Microsoft's DRM system is end to end DRM system that distributes securely digital media file to a work provider and consumer [9]. Core control unit is WMRM (Windows Media Rights Manager) and Rights Manager in WMRM delivers a media such as secure music and video into encrypted file on the Internet. Each server or client instances receive a pair of key through the process of individualization, and the instances, which may be cracked

or not secure, may be revoked using CRL. CRL is distributed through the web site of Microsoft. The key is included in a license, and license and writings are distributed separately.

However, the time to encrypt after encoding the entire file is very long at the encryption because Microsoft's DRM system can only support its WMV and WMA file format.

2.3 I-Frame DRM system

Figure 1 show I-Frame DRM system that keeps content ID (CID) and symmetric key value in a server database after selecting AES or SEED algorithm and encrypting I-Frame of movie GOP (Group Of Picture) by a symmetric key [1].

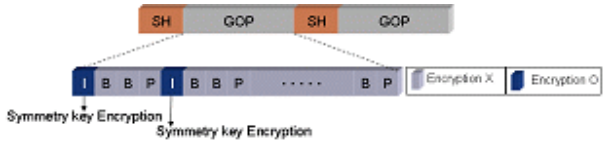

Figure 1. I-Frame DRM system encryption method

When user plays an encrypted movie, sever encrypts the key used in encryption by user public key after achieving user authentication using user certificate. User can get the symmetric key value used in encryption using his private key, decrypt only movie I-Frame, and play the movie after keeping in a buffer with B, P frame.

Figure 2 shows that I-Frame DRM system uses double buffer algorithm to replay the file before decrypting an entire movie. Because I-Frame DRM system encrypts only I-Frame among MPEG (Moving Picture Expert Group) data, this system is a partial encryption system and the encryption and decryption speed of this method are faster than other system. Also, this system can support real-time service because this method replays a movie after decrypting one part.

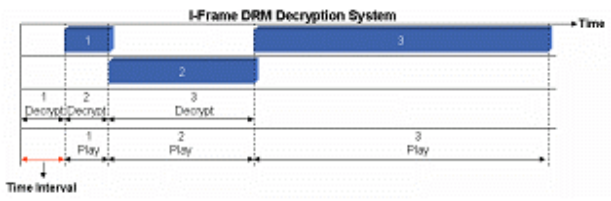

Figure 2. Decryption method of I-Frame DRM system

However, this system still spends much time to read all GOP headers because this system computes the size of I-Frame and decrypt it after reading all headers of GOP group to extract I-Frame. Also, because this system uses only one key, encrypted movie becomes insecure if the key is exposed and the delay time of replay to decrypt the first block occurs at the replay.

3 Encryption/decryption scheme

3.1 Encryption phase

Proposed system performs pre-processing works for encrypting each block after dividing raw data into blocks before encrypting digital content. When performing pre-processing work, the size of first block is assigned as the delay time (TI: Time Interval) before original data and the size of second block is assigned as 100~200 % of previous block size. This method may prevent a user from collecting data limitlessly, generate fair size of block as raw data size, and provide stable replay rate at the decryption. We form a group out of several blocks when generating group and a group is within 12 times of first block size. If a user replay a file using double buffer within 12~13 times of first block size after decrypting, there is no delay time of processing. Same method is applied from the second and last group, so we can form several groups out of blocks. This method is for providing stable encryption scheme that uses compensational double buffer at the encryption and decryption and improves the speed of encryption and decryption.

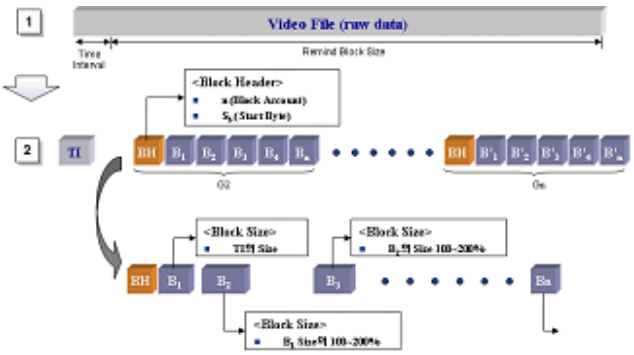

Figure 3. Separate handling of digital content block

Next, proposed system verifies the size of file after receiving digital content, initializes the array, and prepares the processing by block. After checking and saving the amount of delayed time before processing a image, the size of first block is divided and encrypted as the size of delayed time. This system verifies whether data remain or not after encrypting the first block and the phase of block

division is finished if there is no data. If there is data, the data is divided into blocks within 100~200% of previous block size by random function. Same process is repeated until there is no data. The size of a group is within 12 times of delayed time size when decrypting data using double buffers, and second group is within 12 times of last block size of previous block among the rest of the blocks. This process is repeated until there is no block so that the delay time of decryption may decrease because decrypting data using mutual double buffer by group and system can prevent broken replaying of data. Table 1 shows that double buffer can prevent broken replaying by performing both replaying and decryption at the decryption

Table 1. Comparance decryption time with playing time

Interval	Decryption time		Playing time	
	Time (second)	Size (Kbyte)	Time (second)	Image size (Kbyte)
G1	0.1	508	0.1	40
G2	1.238	6287	1.238	508
G3	15.328	77,841	15.328	6,287
G4	189.785	963,752	189.785	77,841
G5	2349.720	11,932,174	2349.720	963,752

System can check early file size as a pre-processing work and is designed to keep the size of block when handling data by block size using the array. Also, proposed system can check the delay time when replaying content and divide data into blocks after computing the rest size of digital content. Separate blocks are to be a group, and group is repeatedly generated until there is no block.

3.2 Design of encryption key using hash chain

To encrypt separate blocks, proposed system generates a key with user authentication number from the first hash function (H1) using two different hash functions and encrypts the first block using the key.

The second key (H2) is generated from the first key using hash function, and the second block is encrypted with the key. The third key is generated by sending the second key (H2) to H1 function and the third block is encrypted with the key.

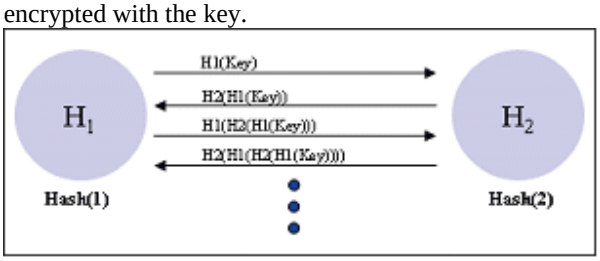

Figure 4. Hash chain method

These processes are repeated until there is no content and all blocks are encrypted, and key is generated by double hash function and encryption is performed using the key. Because digital content is encrypted with two hash functions, encryption is stable and attacker cannot decrypt other blocks because he does not know the hash algorithm although one key is disclosed.

Figure 5. Each block is encrypted with the value of hash chain

This paper uses separate algorithm as figure 5. Key is generated using hash algorithm and each block is encrypted with the key. Block Header (BH) includes the information of position and size of block in group, and the information that control whole group consist of LAU (License Acquisition URL) and Container Header (CH) that includes contents ID. Main Header (MH) includes the size of group and the value hashed DID.

BH includes the information of each encrypted block that is the number and beginning bit of block in group. Also, to manage whole data, CH includes content ID and information of beginning location of each block header so that processing speed is improved at the decryption.

Sever includes MH that saves the size of group and device ID and provides these information to authenticated user. So, although content is disclosed, content is secure because authenticated user can receive the information of main header.

3.3 Design of user authentication and key transmission method

User authentication and control system issue the value of authentication related to instruction to content user. To block information disclosure and verify the user, server provides user authentication number (1) via wireless network after verifying the user, and user inputs the authentication number as a key value (2) and asks the decryption key via wired network (3). After verifying the user authentication number, agent generates decryption key with OTP (One Time Password) and transmits the key to user using secure algorithm.

The generated key is divided into 2 keys (Keys_1, Keys_2) using key partition algorithm, Key1 is hashed by session increase and user authentication value using an agent and the key is transmitted to user (4). User system hashes user authentication number and Keys_1 with random value and transmits them to server (5). Server

recognizes the receipt of Keys_1, hashes partition key Key2 with user authentication number and random value, and transmits it to user (6).

For secure key transmission, this paper proposes key transmission protocol as figure 6. This protocol verifies a user by user authentication phase, generates a key with OTP, and transmits the key to user.

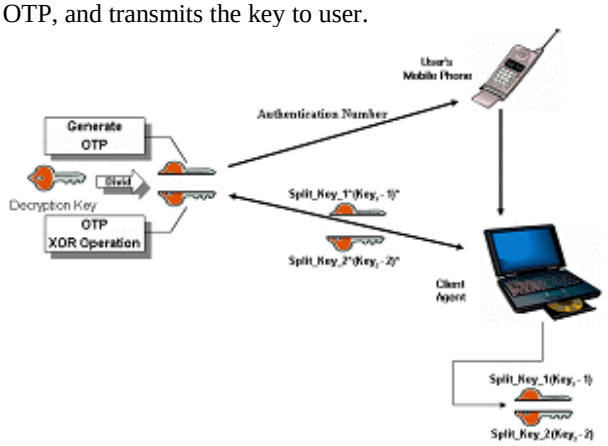

Figure 6. Key transmission method

Ka as Keys_1 and Kb as Keys_2 are respectively provided. (1) User authentication number (101023) is generated by server and transmitted securely to user via mobile service of SSL channel.

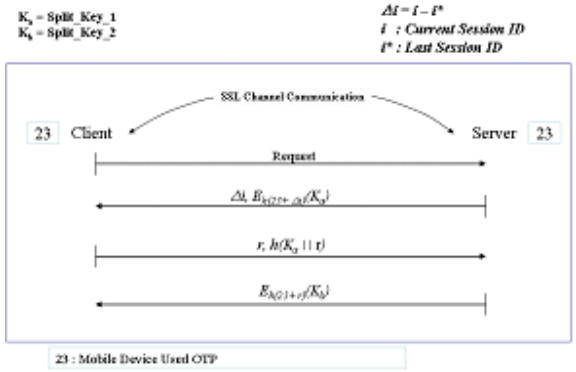

Figure 7. Key transmission protocol

User can request decryption key with an authentication number provided by server. If new user requests decryption key with an authentication number, server generates the key using key partition algorithm and securely transmits it to user using key transmission protocol.

Proposed system distinguishes the existing user from new user. The existing user needs not to request duplicate key, because server can verify the session value i that user keeps. i is session value and Δ i is the increase value of session. Also, we define previous session as i* and present session as i. Accordingly, the existing user can verify the increase value of session and use old key. However, because new user does not have the increase value of session, he must receive a key. Figure 7 shows these processes.

3.4 Decryption phase

Proposed system checks container content ID, and whether identical license is present or not. If there is not identical ID, system moves into LAU (License Acquisition URL) of container header, gets a license, and stores the hash value of user DID (Device ID : Mac Address).

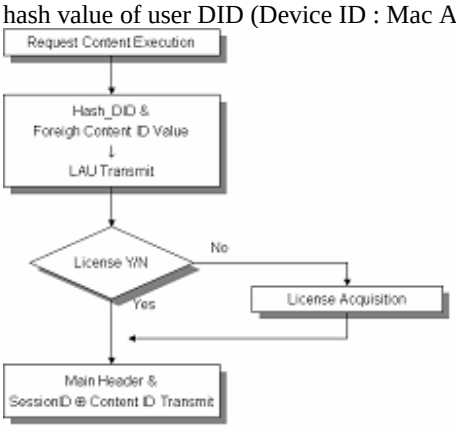

Figure 8. Preprocessing for a decryption

When user asks system to replay a movie as figure 8, new user gets a license and decrypts movie using license.

User receives a decryption key for user authentication and decryption phase when he gets a key. User requests MH (Main Header) of digital content with content ID, and transmits hashed DID value of user and main header with user public key. Next, user decrypts main header with his private key and checks whether the hash value of main header is identical to the hash value of user computer or not. If the verification phase is successful, user can replay a movie.

MH (Main Header) is encrypted (Epu(MH)) with user public key PU, and is decrypted with user private key. User acquires key using user authentication method after he gets the position information of BH, and Gk (B1~Bn) is decrypted with the key.

4 Performance Analysis

This paper compares replay time with other system by analyzing decryption time when replaying digital content. Also, we compare the delay time of proposed algorithm with the delay time of conventional decryption algorithm.

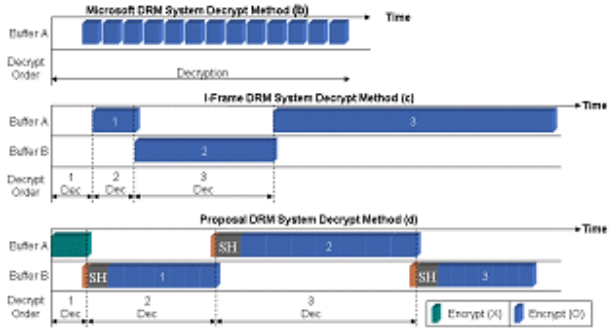

Figure 9. Comparison the delay time of our system with conventional system

Because Microsoft's DRM system replays content file after decrypting whole encryption data, user needs much time to replay a file. Because I-Frame system encrypts only I frame of I, B, P frames that construct a movie and uses double buffers after decrypting only one section, the delay time for processing is brief. Proposed algorithm replays content file by decrypting one section for the delay time before replaying and decrypts next block while replaying. Accordingly, the delay time does not exist and playback does not interrupt.

In DRM system, an encrypted file is in user computer. Because user may rewrite and disclose writings if this file is kept in unencrypted format, a file must be encrypted. Accordingly, when replaying writings, user must wait much time because user agent decrypts data and a large sale data needs much time to decrypt.

Figure 9 shows the difference between proposed DRM system and conventional DRM system.

1) Conventional method decrypts a file when user replays it. When user replays writings, agent verifies the validity of license via server, and agent decrypts and replays writings if user license is valid.
2) Because conventional decryption methods can replay digital content only after decrypting whole digital content, user must wait long time until decryption phase is over. Accordingly, these methods cannot provide real time service because a large scale digital content needs much time to decrypt.
3) Although proposed full decryption system also uses double buffers algorithm, user cannot immediately replay digital content because all frames of digital content are in encryption.

5 Conclusion

This paper proposes mutual authentication protocol for protecting digital content and design of encryption method on on/off line

DRM system is a management technology that protection, distribution, and using for intellectual property rights of digital writings can be achieved in trusted environment. Also, DRM system prevents unauthorized user from replaying digital content and protects continuously the rights and profits of an author.

However, because conventional DRM systems use a secret key method as a encryption algorithm, encryption cannot be achieved in advance. Accordingly, user must wait a long time to download because encryption is achieved when downloading the data file of digital content. Also, these systems have serious problems because the security of digital rights is not guaranteed if secret key is disclosed. Conventional DRM systems try to use public key algorithm or both secret key and public key for solving these problems. However, these systems are not satisfied due to the speed of encryption and decryption.

To prevent a user from disclosing a key, conventional systems use an agent for managing encryption, decryption, and rights, but these systems have many limitations in respect of function and treatment on off-line.

This paper proposes the method that encrypts whole data using several secret keys as security agent for preventing user from disclosing secret key in respect of authenticating the user of digital content. Accordingly, an attacker cannot decrypt whole writings although one secret key may be disclosed. Also, user can immediately download a file because encryption is achieved in advance.

After designing and implementing the proposed system, we perform the experiment using various sizes of video data files for performance evaluation. Proposed system can decrease the delay time including the decryption time of large scale digital content when replaying data file in client system.

References

[1] J. Kim, J. Park, and M. Jun, "DRM system based on public key pool for the security of movie data," Korea Information Processing Society paper, Vol. 12-C, NO. 02, pp 0183-0190, April, 2005.

[2] Brad Cox, Superdistribution : Objects As Property on the Electronic Frontier, Addision-Wesley, May 1996.

[3] Sung, J Park, "Copyrights Protection Techniques," Proceedings International Digital Content Conference, Seoul Korea, Nov. 28-29, 2000.

[4] V.K Gupta, "Technological Measures of Protection," Proceedings of International Conference on WIPO, Seoul Korea, October 25-27, 2000.

[5] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, Vol. IT-22, NO.6, pp.644-654, November 1976.

[6] Intertrust : http://www.intertrust.com/main/overview/drm.html
[7] Joshua Duhl and Susan Kevorkian, "Understanding DRM system: An IDC White paper," IDC, 200.
[8] Joshua Duhl, "Digital Rights Management: A Definition," IDC 2001.
[9] Microsoft: http://www.microsoft.com/windows/windowsmedia/d-rm.asp

Biography

Kun-Won Jang received the B.S. degree in English Literature and Management Information System from Korea Univ., Korea, in 1998, and the M.S. degree in Computer Engineering from Soongsil Univ., Korea, in 2002. His research interests include in the Network Security, Sensor Network, PKI, and Information Hiding.

Chan-Kil Park received the B.S. and M.S. degrees in Department of Computer Science & Engineering from Seoul National University of Technology, Korea, in 1990 and 1995, respectively, and the Ph.D. degree in Computer Engineering from Soongsil Univ., Korea, in 2006. His research interests are in the network security, ubiquitous, DRM, and sensor network.

Jung-Jae Kim received the B.S. degree in Computer engineering from Youngdong Univ., Korea, in 1999, the M.S. and the Ph.D. degrees in Computer engineering from Soongsil Univ., Korea, in 2001 and 2005, respectively. His research interests are in the network security, RFID, Multimedia agent system, and DRM System.

Moon-Seog Jun received his B.S. at Soongsil Univ, M.S. and Ph.D degrees in computer science from University of Maryland, USA, in 1985, 1988. He taught computer Network at Morgan State University and researched Physical Science Lab. New Mexico, USA. He has been taught and researched as a full professor at Soongsil University. His research interests include Network Security, Cryptography, Computer Algorithms, and Network Protocol.