

A Study on Frame Encryption for Protecting IPTV Contents

Boseung Kim*, Jongseok Choi, Jeongjai Kim, Yongtae Shin

Department of Computer, Soongsil University, Sangdo5-dong Dongjak-gu, South Korea

{bskim, jschoi}@cherry.ssu.ac.kr, {argniss, shin}@ssu.ac.kr

Abstract— IPTV provides information services, video contents and broadcast services using high-speed network. It is in the limelight after its commercialization and vitalizations. For protecting and authenticating the transmitted contents, IPTV system is equipped with a combination of CAS and DRM system for VOD contents but the system is too complicated and the construction is too costly. To address this problem, multicast DRM system was on the rise but it also has a problem that unauthorized users can illegally watch broadcasting if the key is leaked out to malicious users. This study proposes a scrambling encryption method which involves rearranging images by changing the values for each pixel using hash function instead of complicated encryption process in multicast DRM system. After designing and implementing the proposed system, performance and validity have been examined through testing its safety and computing speed.

Keywords— Scrambling, Encryption, Multicast DRM, CAS, IPTV

I. INTRODUCTION

IPTV (Internet Protocol Television) is a service that combines communication and broadcasting, and it provides digital information, video contents and various customized services via TV using high-speed internet network. All the contents provided by IPTV must be digitalized before transmission, and anyone using their computer can easily copy the digitalized contents which can be spread rapidly in the same quality as the original. Therefore, security and copyright protection for digital contents are becoming an important issue. Many studies are being conducted on the technologies for preventing illegal duplication and distribution of contents. The two representative security technologies are CAS allows the contents to be transmitted only to the authenticated users but once the contents are distributed, there is no continuous protection which enables illegal copy and distribution. So, IPTV system is currently using CAS in combination with DRM technology for VOD contents. However, such system is costly, complicated and it requires hardware.

This study proposes a system for protecting the contents from malicious users by applying scrambling encryption method to into multicast DRM system without of using CAS. The study consists of the following; the technologies used in IPTV environment such as CAS and DRM will be discussed in Chapter 2, and the composition and features of the proposed system will be described in Chapter 3. In Chapter 4, the implementation of the proposed system, and comparison with

existing encryption methods will be discussed. Also, the safety of the proposed algorithm, will be verified through encryption and decryption tests using scrambling method. Chapter 5 will be the conclusion.

II. RELEVANT STUDIES

A. Digital Protection Technology

The advantage of digital data is that it allows flexible operation and various functionalities between media. However, it is easy to copy and manipulate, and it's difficult to distinguish between the copied data and the original. Such weakness can cause damage to the copyright holder's intellectual property, and technologies for protecting digital data are absolutely needed. To name a few, steganography, watermarking and scrambling are the technologies for protecting digital data. Table 1 shows the comparison between these technologies[6].

TABLE 1. COMPARISON BETWEEN DIGITAL PROTECTION TECHNOLOGIES

	Watermarking	Scrambling
Image Recognition	Possible	Impossible
Image Contents	Real information	Real information
Hidden Information	Ownership and license	None

1) Watermarking

Watermarking refers to a technology that changes the work into a form unperceivable to the human eye in order to keep the message of the work[7]. In other words, it attaches information such as ownership or license to the original contents to protect intellectual property and to prevent illegal distribution and manipulation.

Generally, a watermarking system is composed of an embedding device and detecting device. The embedding device has the message to be input as a watermark and the target image to which the mark is to be input as the input values. The value calculated from the embedding device is given as the input value for the watermark detecting device. Most of the detecting devices determine if any watermark exists and if there is a calculated value with the input message.

2) Scrambling

Scrambling refers to a technology that changes or encrypts and transmits the original image data with a certain key in order to allow only the receiver with the key to be able to restore the image [4, 5]. Therefore, only the authorized users with the restoring key can restore the distorted image from scrambling to the original image. On the other hand, unauthorized receiver can only see the distorted image even if they manage to decrypt the image. This can protect the legal receivers' rights. Figure 1 shows a typical scrambling system.

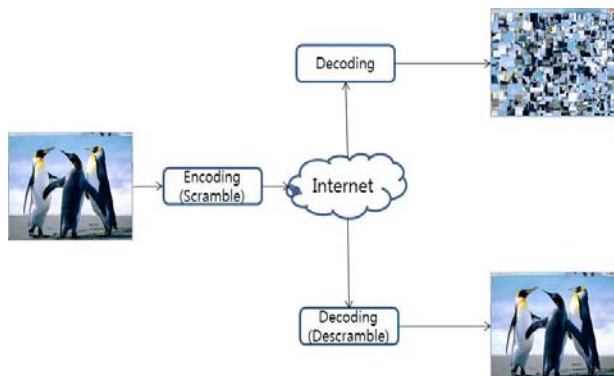


Figure 1. Scrambling System

Scrambling can be broadly divided into two: scrambling method in spatial domain and scrambling method in frequency domain. Other than those, there are methods using motion vector, encryption algorithm and etc[3].

a) Scrambling Method in Spatial Domain

This most commonly used method involves distorting images directly in the spatial domain shown on the screen. As for scrambling methods in spatial domain, there are line reversal, line inversion, line substitution and cut and rotate scrambling methods.

- **Line Reversal Scrambling:** This is the simplest scrambling method and it reverses the scan line from end to end, from right to left and from left to right. The method that reverses transmitting orders also belongs to the same category. It is easy to build but it has poor security.
- **Line Inversion Scrambling:** After the brightness value of each scan line has been obtained, black and white are changed. The entire image or a part of scan line is distorted by inverting the brightness value. It is easy to build but the quality is bad. The degree of distortion is insignificant and it has poor security.

b) Scrambling Method in Frequency Domain

Scrambling in frequency domain might be more efficient than that in spatial domain. Nowadays, studies on scrambling in frequency domain such as DCT(Discrete Cosine Transform), DFT(Discrete Fourier Transform) and

DWT(Discrete Wavelet Transform) are being conducted vigorously. As for scrambling methods in frequency domain, there are wavelet based scrambling, bit scrambling and the scrambling method using encryption algorithm.

B. Digital Protection Technology

CAS has been used as a basic system for the access control of paid broadcasting service since analog broadcasting days [1].

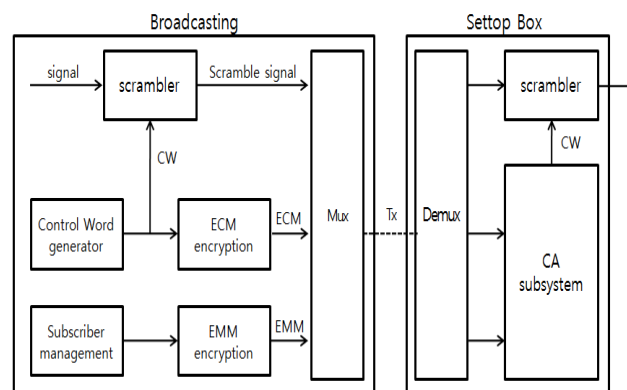


Figure 2. Diagram of CAS

CAS is for allowing only the subscribers of the broadcasting system to receive certain programs and its objective is to protect business profits of the paid broadcasting service providers. Major features of the system are scrambling & descrambling, entitlement control, entitlement management. Figure 2 shows the diagram of CAS [3].

1) Scrambling & Descrambling

Scrambling involves changes the original TV signal form to make it unintelligible to unauthorized receivers. Its methods differ depending on TV program forms (audio/video/data) and signal forms (analog/digital). Descrambling can only be performed at the receivers that can have CW (Control Word), which is the key of descrambling. In DVB projects, scrambling methods for EP-DVB applications have been designed to minimize the possibilities of long term external attacks. Therefore, the scrambling method consists of advanced encryption mechanism.

2) Entitlement Control

Before a transmission is made from the transmitter to receiver, CW is used to encode the authentication key, and CW is included in ECM(Entitlement Control Message) to be transmitted. CW is generated regularly and encrypted. There are control variables included in ECM, and every receiver compares the transmitted control variables to the authentication variables of the receiver. For a good user, CW is decoded with the secret key in the smart card and the received contents are descrambled.

3) Entitlement Management

It manages the entitlement of the receivers and encodes the authentication key. It generates and transmits EMM

IV. PERFORMANCE EVALUATION

In order to conduct a performance evaluation for the proposed system, the method using AES encryption algorithm and another method using scrambling encryption method were evaluated. Also, a safety evaluation was conducted.

A. Speed Comparison between AES Algorithm and Scrambling

The following diagram shows the speed comparison between AES encryption algorithm and the proposed scrambling method.

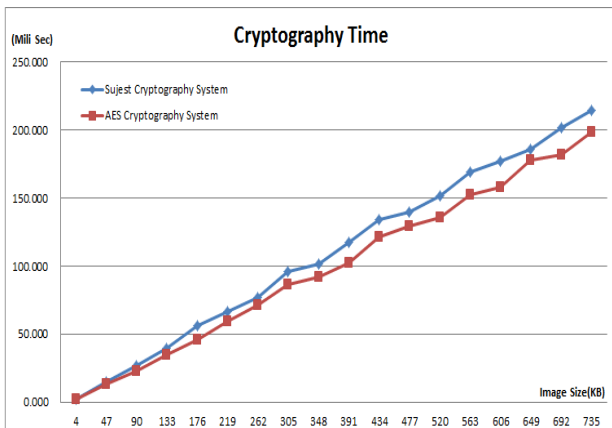


Figure 6. Cryptography Time Comparison

Images of different file size have been compared and evaluated and the testing environment was Quad 2.6GHz. As shown in Figure 6, it was found that as for the whole image, the scrambling encryption method was slower than AES encryption algorithm. AES algorithm directly encodes using the file's stream but the proposed system loads the image, puts it into the memory stream and then encodes the bit string. That is why the scrambling encryption method is slower. However, AES encryption system encodes the whole file, whereas the proposed system allows users to encode a part of the file. In case of electronic documents, instead of encoding the whole file, leaving unnecessary parts (empty space) without encoding can greatly improve the speed. Moreover, AES encryption system encodes the entire file properties, whereas the proposed system shows the encoded image as if it has a lot of noise.

B. Safety Evaluation

According to 140-2 of NIST FIPS(Federal Information Processing Standard), the data encoded by AES 128Bit encryption algorithm is still safe. However, encoding data using the encryption algorithm involves encoding the entire property values and it cannot be known which data has been encoded. In order to reproduce contents, the proposed system requires a key to represent the encoded data, and the reproduction is not possible without the key which is a weakness. However, the proposed system keeps the properties of a frame image file intact through scrambling encryption because it only requires rearranging the color values of different pixels. Also, changing the position values of pixels

instead of changing bit colors allows understanding that the image is the same as the original through histogram. Moreover, the partial encryption algorithm feature allows setting and modifying the zone for scrambling leaving unnecessary portion without encoding.

Assuming that decoding is carried out using the image without a key, an image of 100 x 75(W x H) pixels and a BMP file of 24Bit RGB color values were used in the test. The total number of pixels is 7,500 and each pixel can have 24Bit(224) color value. Therefore, the probability of finding it using the same number of pixels as the original is $7,500 \times 16,777,216 = 125,829,120,000$ (1/125,829,120,000). There is no way to know which color is arranged for the original image so the probability is almost zero. When an image is opened, as for the encryption algorithm, analysis is made to understand if it is an image file. On the other hand, the proposed system keeps the image properties intact, and it does not even allow understanding if the image represented in pixels is encoded or not. For instance, if there is an image with a black dot on a white paper, it is impossible for users to know if the one with a lot of dots like a two-dimensional bar code or the one with everything white or the one with the contents is the original.

This algorithm is impossible to backtracking because it changes the original the color values of the frame that multiple the color values are distributed, using a hash function.

In case that the range of color value is narrow like single color value, the color value changes by other hash function value, therefore it is secure.

C. Comparison for encryption and decryption in terms of saving image in video frame

The encryption and decryption of frame image files such as JPEG, BMP, PNG and etc can be broadly classified into a lossless compression image and lossless frame image. BMP and PNG fall into lossless file category. When an original image is encoded and if it is decoded back into the original image, it will be restored as shown in Figure 7.

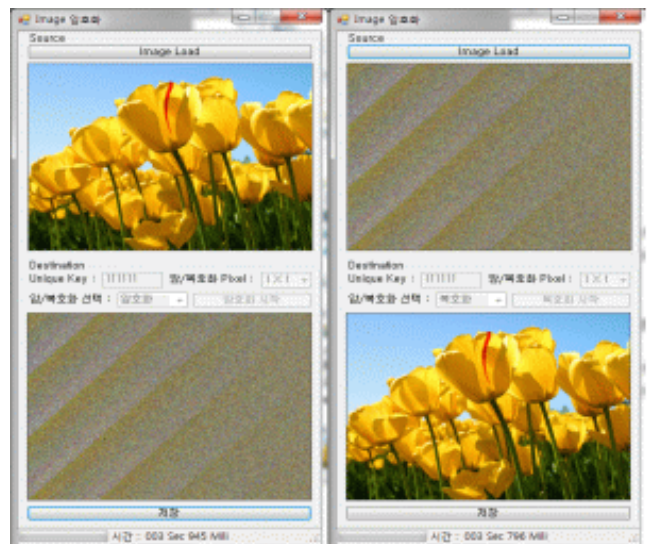


Figure 7. Encryption and Decryption of Lossless Compression Frame Image

However, for loss compression such as JPEG showed the results shown in Figure 8. During DCT conversion, the palette color has been changed, and although the image was recognizable it was distinctly different from the original.

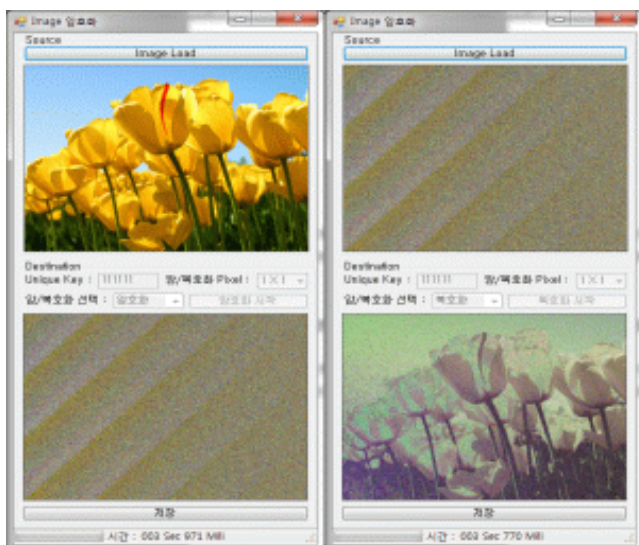


Figure 8. Encryption and Decryption of Loss Compression Frame Image

V. CONCLUSION

Nowadays, IPTV is in the limelight providing information and broadcasting through high-speed network as it is being commercialized and vitalized. However, due to the digitalization of contents, there have been many problems with the protection and authentication of contents. To address such problems, a system equipped with a combination of CAS and DRM technology for VOD has been designed but it has some weaknesses as the system is too complicated and costly. Also, although the multicast DRM system can address the problems of CAS which has the structure suitable for one-way broadcasting, it cannot prevent users from illegally watching broadcast if the key is leaked out.

This study proposed a low-cost system which allows utilizing all the features of the previous system through a method where the values of each pixel are changed using hash function in multicast DRM system. The proposed system is designed to address both the protection and authentication of contents through 2 element authentications with a status information server utilizing the strength of IPTV that is allows two-way communication.

Future research is expected to study the better performance by using the algorithm through a mobile device which is significantly less computing power.

ACKNOWLEDGMENT

This work was supported by the Seoul R&BD Program(10581).

REFERENCES

- [1] Ahmet M. Eskicioglu, "Protecting Intellectual Property in Digital Multimedia Networks", IEEE Computer, Vol.36, pp.39-45, July, 2003

- [2] B. Rosenblatt, B. Tripple, And S. Mooney, Digital Rights Management - Business and Technology, M&T Books, 2002
- [3] EBU, Functional Model of a Conditional Access system, EBU Project Group B/CA, October, 1995
- [4] B. Rosenblatt, B. Tripple, And S. Mooney, Digital Rights Management - Business and Technology, M&T Books, 2002
- [5] EBU, Functional Model of a Conditional Access system, EBU Project Group B/CA, October, 1995
- [6] W. Kanjanarin and T. Amornraksa, "Scrambling and key distribution scheme for digital television". IEEE International Conference on Networks, pp.140-145 Oct. 2001
- [7] Baofeng Liu, Wenjun Zhang, Tianpu jiang, "A scalable key distribution scheme for conditional access system in digital pay-TV system" Consumer Electronics, IEEE Transactions on, Vol.20, No.2, pp.632-637, May, 2007
- [8] Shigue Lian, "Digital Rights Managements for the Home TV Based on Scalable Vidio Coding", IEEE Trans. on Consumer Electronics, Vol.54, 2008
- [9] P. Loo, N. Kingsbury, "Watermark detection based on the properties of error control codes," Vision, Image and Signal Processing, IEEE Proceedings, Vol. 150, Issue. 2, April.2003, pp.115-121.