Multimedia Content Protection Technology

Shiguo Lian
France Telecom R&D Beijing, China

INTRODUCTION

Since the beginning of 1990s, some multimedia standards (Joan, Didier, & Chad, 2003) related to image compression, video compression, or audio compression have been published and widely used. These compression methods reduce media data's volumes, and save the storage space or transmission bandwidth. After the middle of 1990s, network technology has been rapidly developed and widely spread, which increases the network bandwidth. With the development of network technology and multimedia (image, audio, video, etc.) technology, multimedia data are used more and more widely. In some applications related to politics, economics, militaries, entertainment, or education, multimedia content security becomes important and urgent. Some sensitive data need to be protected against unauthorized users. For example, only the customers paying for a TV program can watch the program online, while other customers cannot watch the content, only the administrator can update (delete, insert, copy, etc.) the TV program in the database, while others cannot modify the content, the TV program released over Internet can be traced, and so forth.

Multimedia content protection technology protects multimedia data against the threats coming from unauthorized users, especially in network environment. Generally, protected properties include the confidentiality, integrity, ownership, and so forth. The confidentiality defines that only the authorized users can access the multimedia content, while others cannot know multimedia content. The integrity tells whether media data are modified or not. The ownership shows media data's owner information that is used to authenticate or trace the distributor.

During the past decade, various technologies have been proposed to protect media data, which are introduced in this chapter. Additionally, the threats to multimedia data are presented, the existing protection methods are compared, and some future trends are proposed.

BACKGROUND

There are some threats (Furht & Kirovski, 2006) to multimedia data, especially in network environments, such as eavesdropping, malicious tampering, illegal distribution, imitating, and so forth. Among them, eavesdropping denotes the activity to steal multimedia data from the transmission channel, malicious tampering means to modify the media content intentionally, illegal distribution is the phenomenon when the authorized customer distributes his media copy to unauthorized customers, and imitating denotes the activity when unauthorized customers act as authorized customers.

To conquer some of the threats, some technologies have been reported. The well-known ones include steganography (Johnson, Duric, & Jajodia, 2001) and cryptography (Mollin, 2006). Steganography provides the means for secret communication. In steganography, the secret information is hidden in the carrier (image, video, audio, text or computer program, etc.) and transmitted to the receiver combined with the carrier. In this case, eavesdroppers do not know whether there is secret information in the transmitted carrier or not, and cannot apply attacks. Differently, in cryptography, media data are transformed from one form into another form that is unintelligible. Thus, only the authorized user can recover the intelligible media data.

Generally, using one kind of technology, such as cryptography, cannot resist so many attacks, and various threats should be considered when designing a multimedia content protection system. Digital rights management (DRM) system is a good example, which protects all the rights of content provider, service provider, and customer. For example, open mobile alliance (OMA) (OMA, 2005) provides the DRM system

for protecting mobile multimedia communication, Internet Streaming Media Alliance (ISMA) (ISMA, 2005) provides the one for protecting streaming media over network, and advanced access content system (AACS) (AACS, 2004) provides the one for protecting digital video discs. In existing DRM systems, only the framework is standardized, which defines the method to package multimedia content and access rights (read, copy, write, etc.) and the protocol to exchange access keys. But, the technologies resisting different attacks are optional. These technologies include encryption algorithm (Furht & Kirovski, 2006), hash function (Ho & Li, 2004), watermarking algorithm (Cox, Miller, & Bloom, 2002), and so forth. Encryption algorithms transform original data into the unintelligible form under the control of the key. Thus, only the user with the correct key can recover the original data. Hash function generates a data string from original data. Generally, it is easy to compute the data string from original data, while difficult to compute original data from the data string. Watermarking algorithm embeds copyright information into media data by modifying media data slightly. Generally, there are slight differences between original data and the watermarked data, which cannot be detected by human perception.

The protection technologies should be selected according to the performance requirements of practical applications. Traditionally, for text data or binary data, there are some means to protect the confidentiality or integrity, such as ciphers or hash functions (Mollin, 2006). However, these protection means are not suitable for such data as image, video, or audio due to the special properties: (1) image, video, or audio is often of large volumes; (2) image, video, or audio is often compressed before transmission or storing; (3) image, video, or audio is often processed by cutting, resizing, resampling, and so forth; and (4) real time transmission or interaction is required by the applications based on image, video, or audio.

Firstly, it is difficult to encrypt multimedia data completely with traditional ciphers. Because media data are often of large volumes, encrypting media data completely costs much time, which is difficult to support real time applications. Additionally, in multimedia communication, the format information of compressed multimedia is often used to realize synchronization that reduces the effects caused by transmission errors. Thus, partial encryption algorithm (Furht & Kirovski, 2006) is more suitable, which leaves such information as the file format unchanged.

Secondly, traditional hash functions are not suitable for multimedia data authentication. Generally, such data as image, video, or audio are often operated by compression, resizing, resampling, analog-to-digital conversion or digital-to-analog conversion, and so forth. Traditional hash functions are sensitive to data changes, that is, a slight change in media data causes great changes in the hash value. Thus, traditional hash function will detect the acceptable operations, and a new hash function (Ho & Li, 2004) that enables acceptable operations is preferred. Additionally, it is often required to detect not only the tampering, but also the tampered location (Wang, Lian, Liu, & Ren, 2006). Thus, for these applications, traditional hash functions are not suitable again, and some new functions are expected.

Thirdly, with only encryption algorithm and hash function, the super distribution problem (Moulin & Koetter, 2005) cannot be solved. That is, after decryption, multimedia content can be redistributed from one person to another freely, and the ownership cannot be authenticated. Thus, new technology is required to protect multimedia data's ownership, such as watermarking technology that embeds ownership information into media data and can survive such lossy operations as compression, resizing, resampling, and so forth.

For such data as image, video, or audio, better encryption algorithms, hash functions, or watermarking algorithms are required to protect the content. Since the past decade, some algorithms have been proposed, which are classified and analyzed in detail as follows. Because only image, video, and audio are focused, multimedia data denote only image, video, and audio in the following content.

CONFIDENTIALITY PROTECTION OF MULTIMEDIA CONTENT

To protect the confidentiality of multimedia content, multimedia data are encrypted into the unintelligible form, and only the authorized user can decrypt the multimedia data into the plain form (Furht & Kirovski, 2006). Generally, multimedia data are encrypted partially or selectively, that is, only parts of them are encrypted while other parts are left unchanged. This is based on two reasons: firstly, by reducing the encrypted