Chapter XXII
Copyright Protection of
A/V Codec for
Mobile Multimedia Devices

Goo-Rak Kwon
Chosun University, Korea

Sung-Jea Ko
Korea University, Korea

ABSTRACT

The objective of this chapter introduces an advanced encryption of MP3 and MPEG-4 coder with a quality degradation-based security model. For the MP3 audio, the magnitude, and phase information of modified discrete cosine transform (MDCT) coefficients is encrypted. DCT coefficients and motion vectors (MVs) are used for the scrambling of the MPEG-4 video. This encryption scheme has a level of security, secures in perception, keeps format compliance, and obtains high time efficiency though reducing the encrypted the volumes of multimedia contents. These properties make it practical to incorporate encryption and decryption process into compression and decompression process, and thus suitable for secure A/V transmission or sharing.

INTRODUCTION

With the advance of multimedia technology, multimedia sharing among multiple devices has become the main issue. This allows users to expect the peer-to-peer distribution of unprotected and protected contents over public network. Many audio and video (A/V) processing software including DVD players, CD rippers, MP3 encoders, and A/V players have been posted for free on the Web allowing users to build their own A/V record collections from their own CD and DVD. Inevitably, this situation has caused an incredible piracy activity and some Web sites have begun to provide copyrighted A/V data for free. In order to protect the contents from illegal attacks, digital rights management ( DRM) is required as shown in Fig. 1.
The DRM system generally provides two essential functions: management of digital rights by identifying, describing, and setting the rules of the content usage, and digital management of right by securing the contents and enforcing usage rules. The basic principle of the DRM model (Schneier, 1996; Piva, 2002; Petitcloas, 1999) is to separate and identify three core entities: Users, Content, and Rights. Users can be any type of users from a rights holder to an end-consumer. Content is any type of contents at any level of aggregation. A right is an expression of permissions, constraints, and obligations between Users and Content. This model provides the greatest flexibility when assigning rights to any combination or layering of Users and Content. Fig. 2 shows the example of contents distribution service using DRM. In Fig. 2, a user A requests image, audio, or video in the network and goes through payment. Billing system informs payment approval, and then CP delivers encrypted contents to only an authorized user through the network.

Various encryption techniques for DRM have been researched. These techniques are classified into two approaches: scrambling and watermarking. Scrambling that is generally based on old and proven cryptographic tools, efficiently ensures confidentiality, authenticity, and integrity of messages. However, it does not protect against unauthorized copying after the message has been successfully transmitted and descrambled (Matsunaga, et al., 1989; Schneier, 1996; Spanos, et al., 1995). This kind of protection can be handled by watermarking (Piva, 2002; Aeng, 2003), which is a more recent topic that has attracted a large amount of research and is perceived as a complementary aid in encryption. A digital watermark is a piece of information inserted and hidden in the media content (Bassia, 2001; Borujeni, 2000; Cox, 2000; Li, et al., 2004; Neubauer, et al., 1998; Yeh & Kuo, 1999). This information is imperceptible to a human observer but can be easily detected by a computer. Moreover, the main advantage of this technique is to provide the nonseparability of the hidden information and the content.

A watermarking system consists of an embedding algorithm and a detecting function. The embedding algorithm inserts a message into a media and the detecting function is then used to verify the authenticity of the media by detecting the message. The most important properties of a watermarking scheme include robustness, fidelity,
Related Content

Understanding User-Curated Playlists on Spotify: A Machine Learning Approach
[www.igi-global.com/article/understanding-user-curated-playlists-on-spotify/187139?camid=4v1a](www.igi-global.com/article/understanding-user-curated-playlists-on-spotify/187139?camid=4v1a)

Predicting Key Recognition Difficulty in Music Using Statistical Learning Techniques
Ching-Hua Chuan and Aleksey Charapko (2014). *International Journal of Multimedia Data Engineering and Management* (pp. 54-69).
[www.igi-global.com/article/predicting-key-recognition-difficulty-in-music-using-statistical-learning-techniques/113307?camid=4v1a](www.igi-global.com/article/predicting-key-recognition-difficulty-in-music-using-statistical-learning-techniques/113307?camid=4v1a)

Communication and Relation Building in Social Systems
[www.igi-global.com/chapter/communication-relation-building-social-systems/19854?camid=4v1a](www.igi-global.com/chapter/communication-relation-building-social-systems/19854?camid=4v1a)

Student Performance and Perceptions of Business Courses Delivered Using Lecture Capture
[www.igi-global.com/chapter/student-performance-perceptions-business-courses/75414?camid=4v1a](www.igi-global.com/chapter/student-performance-perceptions-business-courses/75414?camid=4v1a)