# Chapter XIV
# Multimedia Transcoding in Mobile and Wireless Networks:
## Secure Multimedia Transcoding for Scalable Video Streams

**Shiguo Lian**
*France Telecom R&D Beijing Center, China*

## ABSTRACT

Secure multimedia transcoding is a challenge that operates the encrypted multimedia content directly. For example, the encrypted multimedia data's bit rate is changed directly in order to adapt a narrow channel. However, since it avoids the triple operations decryption-transcoding-re-encryption, it is suitable for the application scenarios requiring low cost operations, such as wireless or mobile multimedia communication. In this chapter, the secure transcoding scheme for scalable video coding is proposed and analyzed, together with the introduction to scalable video coding and multimedia encryption, the overview of existing secure transcoding schemes, and some open issues in this field. The chapter is expected to provide researchers or engineers valuable information on secure multimedia transcoding and communication.

## INTRODUCTION

With the development of multimedia technology and network technology, multimedia data are used more and more widely in a human's daily life, such as mp3 sharing, video conference, video telephone, video broadcasting, video-on-demand, p2p streaming, and so forth. For multimedia, data may be in relation with privacy, profit, or copyright, and multimedia content protection becomes necessary and urgent. It permits that only the authorized users can access and read the multimedia data.

Additionally, with the development of wireless network, mobile multimedia communication becomes more and more popular in a human's daily life. Due to the diversity of mobile devices or wireless services, the transmission bandwidth is not certain in the mobile/wireless environment. Thus, it is necessary to transcode the multimedia content in order to adapt different transmission channels. Generally, multimedia transcoding is implemented by routers or mobile agents, not by the sender or receiver. It is a challenge to protect media content against routers or mobile agents since media content is often leaked out during transcoding.

Generally, multimedia content is encrypted (Qiao & Nahrstedt, 1998) and transmitted by the sender, then decrypted by the receiver. Intuitively, for media content is always in cipher form during transmission, routers or mobile agents should be decrypted, transcoded, and re-encrypted in order. However, this is not practice in mobile or wireless communication for two reasons: (1) After decryption, media content is known to routers or mobile agents; and (2) The decryption-transcoding-re-encryption operations increase the loading of the energy-constraint devices.

Alternatively, there are some solutions for progressive media streams. A progressive media stream is often composed of the substreams corresponding to different layers. For example, MPEG2 stream (MPEG2, 1994) is composed of base layer and enhancement layer, and JPEG2000 stream (ISO, 2000) is composed of various passes. Wee and Apostolopoulos (2001, 2003) proposed the scheme to encrypt a progressive stream segment by segment in which the stream's bit rate can be changed by cutting the segments directly from the end. Lian, Sun, Zhang, and Wang (2004d) proposed the scheme to encrypt JPEG2000 stream pass by pass in which the stream's bit rate can be changed by cutting some passes directly from the end.

MPEG4 SVC (Scalable Video Coding) (Li, 2001) is a standard published recently that provides a framework for constructing scalable streams. In a scalable video stream, the substreams are arranged according to spatial scalability, temporal scalability, and Peak Signal-to-Noise Ratio (PSNR) scalability. Each substream is composed of some Network Abstract Layer (NAL) units. The video stream's bit rate is changed by removing or cutting some NAL units directly. Scalable video coding provides more refined streams by introducing more scalable parameters. Secure transcoding for SVC streams is more challenging than for progressive streams because of the scalable parameters. For example, removing or cutting NAL units are not directly done from the end. They should be controlled by the scalable parameters so that the result stream can be decrypted successfully. Additionally, some means should be taken to assign NAL units subkeys, which make it easy to synchronize the decryption subkeys with the encryption subkeys.

In the following content, we introduce some related work in scalable video coding and multimedia encryption, review the existing secure transcoding schemes, propose a secure transcoding scheme for scalable video coding, analyze the scheme's performances, and present some open issues in this research field.

## SCALABLE VIDEO CODING

Scalable coding provides a unique bitstream whose syntax enables a flexible and low complexity extraction of the information so as to match the requirements of various devices and networks.

To date, several video coding methods supporting scalability have been proposed, which can be classified into four types: layered scalable coding, MPEG4 FGS, wavelet based codecs, and MPEG4 SVC.