Multimedia Encryption

Shujun Li
FernUniversität in Hagen, Germany

Zhong Li
FernUniversität in Hagen, Germany

Wolfgang A. Halang
FernUniversität in Hagen, Germany

INTRODUCTION

Multimedia technology becomes more and more popular in today's digitized and networked world. Many multimedia-based services, such as pay-TV, remote video conferencing, medical imaging, and archiving of government documents, require reliable storage of digital multimedia files and secure transmission of multimedia streams. In addition, in course of the recent booming of diverse multimedia functions/services provided by consumer electronic devices and digital content providers, more and more personal data are created, transmitted, and stored in multimedia formats, which also incur increasing concerns about personal privacy (i.e., multimedia data security). To fulfill such an overwhelming demand, encryption algorithms have to be employed to secure multimedia data.

Apart from concerns about data security, there also exist serious concerns about copyright protection issues, which are mainly raised by multimedia content providers as a hope to protect their multimedia products or services from pirate copies and unauthorized distributions. Digital watermarking is the main technique to realize such a function, by embedding digital patterns in multimedia products to be detected.

Multimedia encryption and digital watermarking constitute the kernel of **digital rights management** (DRM) systems. Recently, a lot of efforts have been made to define DRM systems for multimedia encoding standards. Two ISO/IEC standards have officially been released in the past three years: JPSEC (Security Part of JPEG2000) in 2004 and MPEG-4 i**ntellectual property management and protection** (IPMPX, eXtensions) in 2006. To ensure flexibility and renewability, both standards define only a framework and interfaces between different modules so that any available tool can be freely chosen by the content providers/owners in a real implementation. In this way, a malfunctioning encryption or watermarking component can be replaced by a new one without changing other parts of a system.

In recent years, some surveys have been published about multimedia encryption (Furht & Kirovski, 2004; Furht, Muharemagic, & Socek, 2005; Uhl & Pommer, 2005; Zeng, Yu, & Lin, 2006). In this article, we will also introduce some very new results that are not covered in previous surveys.

MULTIMEDIA ENCRYPTION: WHY?

Modern cryptography has been well developed since 1970s. A large number of ciphers have been proposed, among which some have been standardized and widely adopted all over the world, that is, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman public-key encryption algorithm (RSA). So, it seems natural to use any established cipher to encrypt a multimedia file/stream bit by bit. This simple and easy approach is called ***naïve encryption*** in the literature and has been used in some DRM systems. However, naïve encryption does not suit many multimedia-related applications, due to some special features required in these applications.

The first problem is that many traditional ciphers cannot run fast enough to fulfill the needs of real-time multimedia applications. For example, for video-on-demand (VoD) services, generally there are always a large number of videos stored in many servers, and a large number of video streams transmitted from these servers to end users. In this case, the encryption loads of the VoD servers may be too high to ensure smooth running of the services. Another scenario is about medical imaging systems, in which lossless

compression algorithms (instead of lossy algorithms) may have to be used due to legal considerations. This means that the compression efficiency will be limited, so the resulting multimedia data will be much more bulky and the encryption load will be much higher. In applications of this kind, ***total (full) encryption*** of multimedia data (i.e., naïve encryption in term of the amount of encrypted data) should be avoided and ***selective (partial) encryption*** is suggested.

Another important requirement in many multimedia-related applications is ***format-compliance*** (Wen, Severa, Zeng, Luttrell, & Jin, 2002). In some applications, encrypted multimedia data should still (partially) comply with the encoding standard so that some post-processing can be further performed without the secret key. In some other applications, encrypted multimedia data are even required to be fully decodable for any standard-compliant decoder. One of such applications is a trial-and-buy service, via which consumers can preview low-quality versions of multimedia products and then decide to buy high-resolution ones. To achieve format-compliance, some syntax elements must be left unencrypted as decoding markers. This means that format-compliant encryption should be realized with the idea of selective encryption, and the encryption part has to be integrated into the compression process.

Many other special features can be further derived from the feature format-compliance, some of which are listed as follows:

- ***Scalable (multiple-layer) encryption*:** Some multimedia encoding standards support scalable encoding of multimedia data. By selectively encrypting one or more layers, one can achieve multiple-layer encryption.
- ***Perceptual encryption*:** Under the control of a quality factor q, encrypted multimedia data can be decoded by any standard-compliant decoder to get a visual quality corresponding to the value of q. This feature can be considered as an enhanced version of multiple-layer encryption, but it may not depend on the embedded scalability in the encoding standard.
- ***Region-of-interest (ROI) encryption*:** For some applications, only part of the multimedia data (such as faces of some people in a documentary movie) needs encryption.
- ***Error-tolerating encryption*:** In some applications, noise over transmission channel may be a big problem. So, it will help if the encryption algorithm itself can also offer some mechanism against noise, together with the embedding mechanism in the multimedia encoding standard.

MULTIMEDIA ENCRYPTION: HOW?

For multimedia data in compressed form, encryption can be exerted before, after, or during the compression process. For encryption schemes working during the compression process, there are some different points at which encryption operations can occur. For example, for multimedia encoding standards based on discrete cosine transform (DCT) or discrete wavelet transform (DWT) and entropy encoding, encryption operations can take place between any two consecutive stages of the following ones: DCT/DWT transform, quantization, run-level encoding (RLE), entropy encoding, and packetization. In addition, one can also replace any part in the original compression process with an encryption-involved counterpart.

Although a large number of multimedia encryption schemes have been proposed in the past two decades, most of them were designed based on the following basic encryption techniques:

- ***Secret permutations*:** As basic components of designing common block ciphers, secret permutations also play an important role in multimedia encryption. There are a lot of elements that can be permuted. For digital images/videos, these permutable elements include pixels, bitplanes, color channels, transform coefficients, quantized coefficients, RLE coefficients, fixed-length codewords (FLC), variable-length codewords (VLC), blocks (group of some pixels), macroblocks (group of blocks), slices (group of macroblocks), pictures/frames, and group of pictures (GOPs). For speech and audio signals, these include samples, frames, groups of samples, transform coefficients, and so on. Generally speaking, secret permutations will not influence format-compliance, but some extra operations may have to be made on the resulting syntax streams. The secret permutations of different elements can be further combined to obtain a more desirable performance.
- ***FLC encryption*:** This technique works for most multimedia encoding standards, because of the