An efficient implementation of a low-complexity MP3 algorithm with a stream cipher

Chih-Hsu Yen · Yu-Shiang Lin · Bing-Fei Wu

Abstract For portable devices with MP3 codec, the demands of digital right management arise recently. To provide a secure scheme to the most portable devices with MP3 codec, this work efficiently implements a secure MP3 algorithm on a dual-core system with one DSP and one RISC. The secure MP3 algorithm is a combination of a proposed low-complexity MP3 algorithm and a stream cipher. The low-complexity MP3 algorithm is executed on DSP and the stream cipher is on RISC. This separated design can dynamically update the type of stream ciphers in various applications. However, some of the main data, rather than an entire MP3 file, is encrypted in the MP3 frame. The partially encrypted data have variable size, determined by the specified security level. The security scheme offers two advantages. The first is that the encrypting and decrypting structures are identical. The second is that the scheme easily determines the quality of the encrypted MP3. For saving the computational power to obtain long playing time for a portable device, a low-complexity MP3 encoder and decoder are implemented using ADSP-2181 with 16-bit fixed-point data precision. MP3 encoding requires only 27.2 KB/16.8 KB (data RAM/program RAM), and decoding requires 23.6 KB/20.7 KB for decoder. The peak MIPS of the encoder and decoder are 21.05 and 17.67, respectively. This work can be applied to a Digital Rights Management (DRM) system for limiting the access of the music.

Keywords MP3 · Multimedia security · DRM · DSP · Low complexity
1 Introduction

The digitization of media has profoundly affected copyright and intellectual property. Online MPEG Layer III (MP3) sharing seems to threaten the music industry. Accordingly, topics in the area of protecting content have become increasingly important over recent years. The access to content could be restricted in several ways, including encryption, watermarking, finger-printing, mechanism of access control and others. However, the encryption is a method to limit the access of the protected music. This work proposed an encryption scheme by embedding a stream cipher into MP3 algorithm to protect MP3 files.

Some studies of the encryption of MP3 have been published. Torrubia et al. [21] presented the perceptual cryptography of MP3 streams. They employed two primitives—scalefactor encryption and Huffman-codeword substitution. Thorwirth et al. [20] presented a selective encryption algorithm, that encrypts the main data of MP3 granules. The encrypted part is determined by mapping the byte index of Huffman codeword onto the exact frequency boundaries. Both schemes can be used to encrypt the already encoded MP3 files. However, both schemes involve extra computations to determine accurately the quality of the encrypted MP3 files. This work presents a simple method for adaptively encrypting the main data in MP3 frame, and yields similar results to those of Torrubia et al. [21] and Thorwirth et al. [20]. The security level can be varied from 0% (lowest security) to 100% (highest security). In this proposed scheme, any stream cipher can be employed to generate the random bitstreams. The advantage of the partial encryption/decryption is that it accelerates processing overall. Additionally, the encryption scheme and decryption scheme are identical, so only one security scheme is required to perform both encryption and decryption. Following encryption, the format of MP3 frame remains valid. Therefore, the MP3 algorithm could directly decompress the encrypted MP3 without decryption, but the consumers receive only the low-quality music. Content providers can use this feature to provide free music to consumers.

Most playback devices are dual-core systems, DSP and RISC, so the proposed approach are implemented and accelerated on such a system. The security phase is on RISC, and the MP3 phase is on DSP. The security phase executes parsing and encryption/decryption of the XOR operation. The MP3 phase performs as does the MP3 algorithm. The low-complexity MP3 algorithm in [23] is implemented on ADSP-2181, and accelerated for ADSP-2181. The optimization for ADSP-2181 is completed by simplifying the nonuniform quantization and dequantization, and introducing a data format of dynamic fixed-point to improve the quality for a 16-bit fixed-point DSP. Hybrid schemes that involve the lookup-table (LUT) method and linear approximation are employed to simplifying the quantization and dequantization. The approximation of quantization is a piecewise linear interpolation. The approximation for dequantization includes two steps—piecewise linear interpolation and fine approximation. The implementation of the low-complexity MP3 encoder requires a data memory of 27.2 KB, program memory of 16.8 KB and computation power of 21.05 MIPS. The decoder needs data memory of 23.6 KB, program memory of 20.7 KB, and computation power of 17.67 MIPS.

Section 2 briefly describes the proposed secure MP3 scheme, describes the scheme and analyzes the security thereof. This section also presents the low-complexity MP3 algorithm proposed in [23]. Section 3 presents the realization of the