Abstract

The digital rights management (DRM) techniques are very important in the fields of multimedia security. The major areas of multimedia data security include secrecy, ownership protection and traitor tracing. Even though, a number of encryption techniques were developed for multimedia encryption, most of them are vulnerable to several types of attacks. Hence, an encryption system having better security with minimal level of system complexity is an important requirement in multimedia security. In this paper, the cryptanalysis of two arithmetic coding based encryption techniques (randomized arithmetic coding (RAC) and chaotic binary arithmetic coding (CBAC)) were proposed and proved that these schemes are vulnerable to known-plaintext attack. Then, a modified secure arithmetic coding based encryption system by providing block-wise shuffling of DCT matrix prior to the CBAC stage (block-shuffled CBAC) is proposed to improve the overall security of the system. In order to provide content protection after decryption for the proposed scheme, the joint fingerprinting and decryption (JFD) technique is provided at the receiver stage. Finally, this idea of image encryption has been extended to video (H.264 coding standard). Here, the work is based on a correlation preserving sorting algorithm whereby a comparable compression performance is obtained in
addition to the high level of security. The proposed systems are tested against various types of attacks and it has been proved that these methods are able to withstand various types of attacks with good compression performance and minimal level of increase in system complexity.

References


Index Terms
Computer Science Image Processing

Keywords
Digital Rights Management Chaotic-based Encryption Secure Arithmetic Coding Joint Fingerprinting and Decryption