Chapter 11
Multimedia Information Security:
Cryptography and Steganography

Ming Yang
Jacksonville State University, USA

Monica Trifas
Jacksonville State University, USA

Nikolaos Bourbakis
Wright State University, USA

Lei Chen
Sam Houston State University, USA

ABSTRACT

Information security has traditionally been ensured with data encryption techniques. Different generic data encryption standards, such as DES, RSA, AES, have been developed. These encryption standards provide high level of security to the encrypted data. However, they are not very efficient in the encryption of multimedia contents due to the large volume of digital image/video data. In order to address this issue, different image/video encryption methodologies have been developed. These methodologies encrypt only the key parameters of image/video data instead of encrypting it as a bitstream. Joint compression-encryption is a very promising direction for image/video encryption. Nowadays, researchers start to utilize information hiding techniques to enhance the security level of data encryption methodologies. Information hiding conceals not only the content of the secret message, but also its very existence. In terms of the amount of data to be embedded, information hiding methodologies can be classified into low bitrate and high bitrate algorithms. In terms of the domain for embedding, they can be classified into spatial domain and transform domain algorithms. In this chapter, we have reviewed various data encryption standards, image/video encryption algorithms, and joint compression-encryption methodologies. Besides, we have also presented different categories of information hiding methodologies as well as data embedding strategies for digital image/video contents. This chapter is organized as following: in Section-1, we give a brief introduction to data encryption system as well as the state-of-the-art encryption standards; Section-2 presents a review of representative image encryption algorithms; Section-3

DOI: 10.4018/978-1-61520-783-1.ch011

first gives a brief introduction of lossless compression and then moves to joint compression-encryption algorithms; Section-4 presents different video encryption methodologies; Section-5 gives a brief introduction to information hiding techniques; Section-6 presents different categories of low bitrate information algorithms; Section-7 presents different categories of high bitrate information algorithms; Section-8 discusses the embedding strategies within digital video contents; this chapter is summarized in Section-9.

INTRODUCTION

In modern information and communication systems, information security is becoming an increasingly important issue due to the threats from all different types of attacks. Traditionally, information security has been ensured with data encryption. With the development of modern information hiding theory, researchers start to resort to information hiding techniques to enhance the security level of data encryption systems. In this chapter, we will first review different encryption techniques for multimedia data, including digital image and video contents. After that, we will move to the information hiding techniques for digital multimedia contents.

General Model

Encryption is a method to protect information from undesirable attacks by converting it into a form that is non-recognizable by its attackers. Data encryption mainly is the scrambling of the content of data, such as text, image, audio, video, etc. to make the data unreadable, invisible or incomprehensible during transmission. The inverse of data encryption is data *decryption*, which recovers the original data. Figure 1 is the general model of a typical encryption/decryption system. The encryption procedure could be described as $C = E(P, K)$, where P is the plaintext (original message), E is the encryption algorithm, K is the encryption key, and C is the ciphertext (scrambled message). The ciphertext is transmitted through the communication channel, which is subject to attacks. At the receiver end, the decryption procedure could be described as $P = D(C, K')$, where C is the ciphertext, D is the decryption algorithm, K' is the decryption key (not necessarily the same as the encryption key K), and P is the recovered plaintext.

Claude Shannon pointed out that the fundamental techniques to encrypt a block of symbols are confusion and diffusion. Confusion can obscure the relationship between the plaintext and the ciphertext, and diffusion can spread the change throughout the whole ciphertext. Substitution is the simplest type of confusion, and permutation is the simplest method of diffusion. Substitution replaces a symbol with another one; permutation changes the sequence of the symbols in the block

Figure 1. Data Encryption/Decryption System