Chapter 4.17

Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy

Ming Yang
Jacksonville State University, USA

Monica Trifas
Jacksonville State University, USA

Guillermo Francia III
Jacksonville State University, USA

Lei Chen
Sam Houston State University, USA

ABSTRACT

Information security and privacy have traditionally been ensured with data encryption techniques. Generic data encryption standards, such as DES, RSA, AES, are not very efficient in the encryption of multimedia contents due to the large volume. 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. Different categories of information hiding methodologies, as well as data embedding and watermarking strategies for digital video contents, will be reviewed. A joint cryptograph-steganography methodology, which combines both encryption and information hiding techniques to ensure patient information security and privacy in medical images, is also presented.

DOI: 10.4018/978-1-61350-323-2.ch4.17

INTRODUCTION

Information security and privacy have traditionally been ensured with data encryption techniques. Different generic data encryption standards, such as DES, RSA, AES, are not very efficient in the encryption of multimedia contents due to the large volume of digital image, video, etc. In order to address this issue, different specialized image/video encryption methodologies have been developed. They 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 systems. 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. Information hiding techniques have been utilized in many application scenarios, such as secure communication, ownership verification, distribution tracking, etc. Information hiding techniques can be combined with encryption to enhance the level of security in multimedia communication systems. In this paper, we will first present some representative image/video encryption algorithms. After that, we will move to image/video information hiding techniques and watermarking strategies. At the end, we will present a joint cryptograph-steganographic approach, which combines encryption and information hiding techniques to ensure patient information security and privacy in medical images. This paper is organized as following: in Section-2, we give a brief introduction to image encryption algorithms; Section-3 presents a review of representative joint compression-encryption algorithms; Section-4 presents different video encryption methodologies; Section-5 gives a brief introduction to information hiding techniques; Section-6 reviews different low bitrate information hiding algorithms; Section-7 addresses a special application of low bitrate information hiding – digital watermarking; Section-8 moves to high bitrate information hiding algorithms; Section-9 discusses the embedding strategies within digital video contents; Section-10 presents a joint cryptography-steganography methodology to ensure patient information security and privacy in medical images; this paper is summarized in Section-11.

IMAGE ENCRYPTION

Why Not Naïve Algorithms?

As an important multimedia data type, the digital image and its encryption have attracted a lot of research interests. There are two levels of security for digital image encryption: low-level security encryption and high-level security encryption (Figure 1). In low-level security encryption, the encrypted image has degraded visual quality, but the content of the image is still visible and understandable to the viewers. In high-level security case, the content is completely scrambled and the image just looks like random noise.

If the image data is just encrypted as a data bitstream, there is no difference between image encryption and other types of data encryption. This type of still image encryption is called a naïve algorithm. However, considering the properties of digital image/video data contents, more elaborate image/video encryption algorithms are desired for the following reasons:

- Due to the volume of digital image/video data, the naïve algorithm usually cannot meet the requirements of real-time applications. Thus, we need to avoid encrypting the image bit by bit and yet ensure a secure encryption system;