Chapter 3
Multimedia Content Encryption for Secure Multimedia Communication

Shiguo Lian
France Telecom (Orange Labs) Beijing, China

ABSTRACT

The principal concern of this chapter is to provide those in the secure multimedia communication or content protection community with an overview of multimedia content encryption technology. Multimedia (image, audio or video) content encryption technologies are reviewed, from the background, brief history, and performance requirement, to research progress. Additionally, the general encryption algorithms are classified, and their performances are analyzed and compared. Furthermore, some special encryption algorithms are introduced. Finally, some open issues and potential research topics are presented, followed by some conclusions. The author hopes that the chapter will not only inform researchers of the progress of multimedia content encryption but also guide the design of practical applications in industry field.

INTRODUCTION

With the development of computer technology and Internet technology, multimedia data (images, videos, audios, etc.) are used more and more widely, such as video-on-demand, video conferencing, broadcasting, and so on. Now, multimedia communication is in close relation with daily life, such as education, commerce,

DOI: 10.4018/978-1-61350-135-1.ch003

politics, military, etc. In order to keep privacy or security, some sensitive data need to be protected before transmission or distribution. Originally, access right control method is used, which controls media data's access by authenticating the users. For example, in video-on-demand, the pair of user name and password is used to control the browsing or downloading operations. However, in this method, multimedia data themselves are not protected, and may be stolen in transmission process. Thus, to realize secure multimedia communication, multimedia data should be encrypted before transmission or distribution.

Till now, various encryption algorithms have been proposed and widely used, such as DES, RSA or IDEA (Mollin, 2006), most of which are used in text or binary data. It is difficult to use them directly in multimedia data, for multimedia data (Furht, 1999) are often of high redundancy, of large-volumes and require real-time operations, such as displaying, cutting, copying, bit-rate conversion, etc. For example, the image Figure 1(a) is encrypted into Figure 1(b) by DES algorithm directly. As can be seen, Figure 1(b) is still intelligible in some extent. This is because the adjacent pixels in an image are of close relation which cannot be removed by DES algorithm. Besides security issue, encrypting images or videos with these ciphers directly is time cost and not suitable for real time applications. Therefore, for multimedia data, some new encryption algorithms need to be studied.

During the past decades, various multimedia encryption algorithms have been studied. In the following content, the basic knowledge, brief history and Intellectual Property investigation are introduced. Additionally, the general requirement, general encryption schemes and special encryption schemes are analyzed and compared in detail. Finally, some open issues are presented, and conclusions are drawn.

THE BASIC OF MULTIMEDIA CONTENT ENCRYPTION

Multimedia content encryption refers to adopt cryptographic techniques to protect multimedia content. Thus, the basic includes both cryptographic techniques and multimedia techniques.

Cryptography

In cryptography, cryptosystem design and cryptanalysis are two close-related topics. Cryptosystem includes traditional ciphers and some new ciphers. Traditional ciphers are often based on the computing difficulty of attack operations. For example, RSA is based on the difficulty to factor a large prime number, Ellipse Curve Cipher is based on the difficulty to solve a discrete logarithm, and such block ciphers as DES and AES are based on the computing complexity caused by iterated confusion and