Chapter III
Multimedia Encryption Technology for Content Protection

Shiguo Lian
France Telecom R&D Beijing, China

ABSTRACT

The principal concern of this chapter is to provide those in the multimedia 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, 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 the 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 data are in close relation with daily life, such as education, commerce, politics, military, and so forth. 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
Multimedia Encryption Technology for Content Protection

Multimedia content encryption refers to adopting cryptographic techniques to protect multimedia content. Thus, the basics include both cryptographic techniques and multimedia techniques.

Cryptography

In cryptography, cryptosystem design and cryptanalysis are two closely 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 diffusion operations. Besides traditional ciphers, some new ciphers have been studied in the past decade. The typical one is chaotic cipher (Dachselt & Wolfgang,
Related Content

An Exploratory Study of the Cyberbullying and Cyberstalking Experiences and Factors Related to Victimization of Students at a Public Liberal Arts College
[www.igi-global.com/article/exploratory-study-cyberbullying-cyberstalking-experiences/48525?camid=4v1a](www.igi-global.com/article/exploratory-study-cyberbullying-cyberstalking-experiences/48525?camid=4v1a)

Ethical Theories and Computer Ethics
[www.igi-global.com/chapter/ethical-theories-computer-ethics/21580?camid=4v1a](www.igi-global.com/chapter/ethical-theories-computer-ethics/21580?camid=4v1a)

A New Printing Revolution? 3D Printing as an Agent of Socio-Political Change
[www.igi-global.com/article/a-new-printing-revolution-3d-printing-as-an-agent-of-socio-political-change/152808?camid=4v1a](www.igi-global.com/article/a-new-printing-revolution-3d-printing-as-an-agent-of-socio-political-change/152808?camid=4v1a)

ICT Ethical Issues, Globalization and Knowledge Society
[www.igi-global.com/chapter/ict-ethical-issues-globalization-knowledge/60421?camid=4v1a](www.igi-global.com/chapter/ict-ethical-issues-globalization-knowledge/60421?camid=4v1a)