Chapter 10

Algorithms for Secure Multimedia Delivery over Mobile Devices and Mobile Agents

Amit Pande  
University of California Davis, USA

Joseph Zambreno  
Iowa State University, USA

ABSTRACT

Rapid advances in embedded systems and mobile communications have flooded the market with a large volume of multimedia data. In this chapter, the authors present a summary of multimedia compression and encryption schemes, the way they have evolved over the decades. They first discuss the traditional approach to data encryption and their extension to video encryption. Next, they present the next generation algorithms for secure multimedia delivery, namely the Joint Video Compression and Encryption (JVCE) approach and give the reader an introduction to these approaches, the underlying assumption, advantages and limitations. The authors discuss the implementation of JVCE algorithms in light of requirements of mobile devices and propose how mobile agents can facilitate such an implementation.

INTRODUCTION

Security is becoming an escalating concern in an increasingly multimedia defined world. The recent emergence of embedded multimedia applications such as mobile-TV, video messaging, and telemedicine have increased the impact of multimedia and its security in our personal lives. For example, a significant increase in the application of distributed video surveillance technology to monitor traffic and public places has raised concerns regarding the privacy and security of the targeted subjects.

Multimedia content encryption has attracted more and more researchers and engineers owing to the challenging nature of the problem and its
interdisciplinary nature in light of challenges faced with the requirements of multimedia communications, multimedia retrieval, multimedia compression and hardware resource usage.

With the continuing development of network communications (wired and wireless), ease of capturing videos and rapid advances in Internet technology and embedded computing systems multimedia data (images, videos, audios, etc.) is being used more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. Now, it is closely related to many aspects of daily life, including education, commerce, defense, entertainment and politics. In order to maintain privacy or security, sensitive data needs to be protected before transmission or distribution.

The advancements in ubiquitous network environment, and rapid developments in cloud computing has promoted the rapid delivery of digital multimedia data to the users. Users are eager to not only enjoy the convenience of real-time video streaming but also share various media information in a rather cheap way without awareness of possibly violating copyrights. In view of these, encryption and watermarking technologies have been recognized as a helpful way in dealing with the copyright protection problem in the past decade. Encryption allows secure end-end communication of data while digital watermarking allows still faces some challenging difficulties for practical uses, there are no other techniques that are ready to substitute it.

Within the signal processing and multimedia communities, many schemes have been proposed for protecting sensitive information while allowing certain legitimate operations to be performed. These schemes typically lack a rigorous model of privacy, and their protection become questionable when scaled to large datasets. The cryptography community has long developed rigorous privacy models and provably secure procedures for data manipulations. However, these procedures are primarily designed for generic data. As a result, they usually lead to a blowup in computational costs and overheads when applied to real-life multimedia applications.

MULTIMEDIA ENCRYPTION PROBLEM

Multimedia encryption involves changing the multimedia datastream itself to ensure secure transmission of video data between client and server. It can be accomplished by means of standard symmetric key cryptography where multimedia bitstream is treated as a binary sequence and the whole data can be encrypted using conventional cryptosystem such as AES or DES (Stinson, 2002). In general, when the application requirements are not dynamic (not a real-time streaming) we can treat bitstream as a regular binary data and use the conventional encryption techniques. Encrypting the entire multimedia stream using standard encryption methods is referred to as the naive algorithm (Agi and Gong, 1996). There are many practical constraints in case of mobile multimedia which make such a scheme not practical in real-life scenario. First there are issues with available computational resources in mobile devices which combined with low battery life and limited device area limit the application of AES or DES like ciphers. Unlike desktop processors, dedicated AES co-processor will cause high power and area requirements. This can be understood with the example of GSM mobile phones which use a much lighter cryptographic cipher for data encryption. A5 is the stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard and is used in various variants. A5/0 utilizes no encryption while A5/1 is the original A5 algorithm used in Europe. A deliberate weakening of the algorithm was proposed as A5/2, but it was cryptanalyzed the same month as it was published. The A5 algorithm is much simpler in implementation than AES, and is implemented using stream ciphers. A5/3, also