International Journal of Innovative Computing, Information and Control
Volume **6**, Number **3(A)**, March **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 897–911

AN “ALL-IN-ONE” MOBILE DRM SYSTEM DESIGN

Chin-Ling Chen

Department of Computer Science and Information Engineering
Chaoyang University of Technology
Taichung 41349, Taiwan
clc@mail.cyut.edu.tw

Received September 2008; revised January 2009

Abstract. *Intellectual property violation events have caused enterprises to respect digital content protection. However, valuable digital content without effective management mechanisms will make the content vulnerable to unauthorized copying, modification and re-distribution, causing revenue losses to service providers. In this paper, we propose an efficient digital rights management protocol for mobile devices.*

We integrate the role of the Mobile Network Service Provider (MNSP) and Content Provider into our scheme to provide an “All-In-One” mobile DRM system. The proposed scheme is superior to the Microsoft and OMA DRM system in privacy protection. Our scheme extends the non-repudiation service in a OMA-based DRM version and also proposes a novel DRM content format (DCF) structure that integrates the existing applications. To overcome the computing resource weakness problem in mobile devices, we also integrate a password mechanism and a one-way hash function such that the security, individualization, flexibility, efficiency and practicability issues will be assured. In this way, the mobile user can conduct a ‘preview-before-buy’ transaction anywhere and anytime and the digital content provider will not suffer from unauthorized mobile users accessing digital content.

Keywords: M-DRM, DRM, Security, Digital content, Authentication

1. Introduction.

Digital content can be easily acquired and implemented with the progress in software and hardware technologies. The rise of the information industry has changed our ideas and lifestyles. The most important factor is the rapid expansion of network technology allowing the widespread use and transference of digital content. People can download various kinds of digital content via the network. However, without digital content rights protection and management, the ease of copying and re-distribution makes digital content vulnerable to unauthorized copying, modification and re-distribution, causing revenue losses to service providers. Thus, how to construct an effective Digital Rights Management (DRM) system has becomes an emergency issue.

Related works. Along with the rapid development of the information industry, multimedia communication service will further amalgamate of data, video and voice. Therefore, Zhang et al. [26] proposed session initiation protocol (SIP) in the security analysis for the next generation network. Recently, many researchers [1,2,7,8,12-15,19,22,25] have proposed Digital Rights Management (DRM) issues. Some literature focused on mobile DRM [1,18,20], but others [4,5] focused on enterprise DRM. Unfortunately, some works have existing flaws. For example: Onieva et al. [21] pointed out that non-repudiation service had not been included so far in DRM specifications. Therefore, they involved a trusted third party (TTP) to coordinate the transaction. However, it is difficult to find a true TTP in the real world. Moreover, Sun et al. [23] pointed out that privacy and practicability issues should be respected.