Digital Content and Data Intellectual Property Protection based on Specific RFID Hard/Soft-Encryption/Decryption Technology

MING-SHEN JIAN[+], KUEN SHIUH YANG[*], TA YUAN CHOU[#], SHU HUI HSU[!]
[+]Department of Computer and Communication, Shu-Te University
[*]International Semiconductor Technology Ltd.
[#] Department of Computer Science and Engineeing, National Sun Yat-sen University
[!] International Megatrend Smart Technology Ltd.
Kaohsiung, TAIWAN
jianms@gmail.com[+], ksyang@ist.com.tw[*], tayuan@gmail.com[#], suhue@imst.htmlplanet.com[!]

Abstract: - In this paper, a *Digital Content and Data Intellectual Property Protection based on Specific RFID Hard/Soft-Encryption/Decryption Technology* that integrates the existed multimedia/digital-content systems and RFID system is proposed. The proposed technology provides the API module and related parser that can easily embed other systems in. The digital content and data intellectual property protection can be achieved by the RFID encryption/decryption technology. The verification shows that the *sRFID-EDT* is realistic and only users who have the legal RFID tag can gain the digital multimedia content.

Key-Words: - RFID, Multimedia, Intellectual Property, Digital Label, System Integration.

1 Introduction

RFID today is the popular wireless induction system [5-7, 11-13]. Each RFID tag in RFID system is given a unique ID (UID) which records the on demand information. When an independent RFID tag approaches the RFID antenna, the induction between RFID tag and antenna happens. The information and content recorded in the tag is transmitted to the RFID antenna and translated into the computational data. Following up the data translation, the tag recognition can be completed and related applications are provided.

Due to the popularity of RFID, many local or small area wireless applications were proposed. The RFID tags were proposed to be used in hospital or health care [2-4]. Patients should always wear the designed RFID tag for himself identification. The patient's current location and condition is monitored every time and everywhere within the hospital. It means that patients are under cared even an emergency state happens. Some entrance guard systems are also based on RFID system. The RFID ticket or RFID card [5-7, 12] is used to identify that a user is legal or not. According to the short-distance wireless signal, the RFID tag users can be monitored within the specific area. In other words, the RFID systems are generally used to be the hardware identification in many applications.

In opposition to using the RFID system as the hardware identification, many software applications adopt software encryption as the identifications to protect the intellectual property of the applications or files. Considering the serious situations of pirate, intellectual property protection is important and becomes a famous issue.

Password protection is the popular encryption method to protect the applications. Each application or file of software is assigned an on demand given serial numbers or calculation function. People who use this application have to input the correct serial number then enable the application.

Considering today's applications, personal multimedia services or software applications are popular. Customers use the personal multimedia devices such as MP3, PDA, iPod, Laptop, etc., to download the multimedia or application files from the server or website via Internet. In other words, many files or data are disseminated and exchanged via Internet. In addition, many hackers can crash the software encryption with fewer costs (Only program tools or applications needed). It makes that the piratical files are transmitted widely and the protection of intellectual property exists in name only.

For the purpose that the right of intellectual property and the right of the valid users are further protected and maintained, integration of the software and hardware encryption is needed. Since each RFID tag with a unique ID (UID) which records the on demand information can be used as the individual identification, the small and cheap RFID tag can be considered as the hardware/software encryption/decryption key corresponding to the files or applications.

Some researches presented that the embedding RFID can be plugged into a small device such as handheld host [1]. The handheld device users can plug in the SD or CF interface of reader card. Hence, the users can scan and induct the RFID tag everywhere. In other words, to integrate the RFID system hardware into the mobile devices is practicable.

Since the RFID systems are popular and ripe for distinguishing treatment of individual target [8,9], the unique characteristic or identification of RFID can be the solution of intellectual property protection. Many researches proposed the possible way to protect the intellectual property, products, or applications. In some applications [10], the RFID chips are embedded in the cap of bottle. The medicine can be differentiated between fake and true. In addition, the RFID chip can be placed in the CD or DVD disk. The CD-ROM can accesses and reads the information of the RFID for valid identification check. Only the CD or DVD with the authorized RFID can be played. Although the content is protected, the self-made content that burned in the CD-R/RW or DVD-R/RW may not provide the authorized RFID information. In other words, the private, non-business, or free digital content made by the individual may be limited and cannot be transmitted free. In addition, even the CD or DVD disks are protected, the digital content such as files or data still can be copied from the disk to other devices such as hard disc or MP3 player. Therefore, how to separate the right of the digital content for each user and how to protect the digital content from illegal use become the important issues.

In this paper, a realistic application, *Specific RFID Hard/Soft - Encryption/Decryption Technology* (*sRFID-EDT*), is proposed. By using the *sRFID-EDT*,

1) each digital content such as a file or an application, or a set of files or applications, can be protected by specific and different RFID tag,
2) the *Encryption/Decryption* procedure consists of software and hardware which can be embedded in the existed systems or devices.
3) only the legal user can execute or play the digital content. Even a true digital file without RFID assisting cannot provide the services.
4) different types of RFID such as size, frequency, even appearance can be selected and designed.

the concept of *sRFID-EDT* multimedia player can be shown as the Fig. 1.

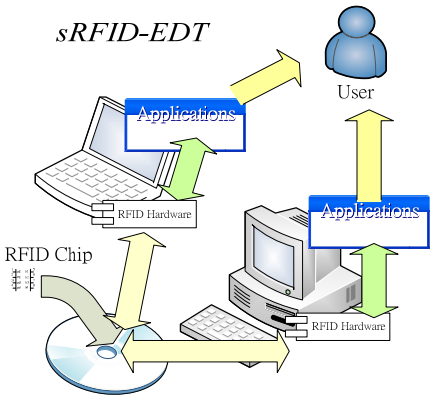


Fig. 1. The concept of *sRFID-EDT* multimedia player

The remainder of this paper is organized as follows. In Section 2, the proposed *sRFID-EDT* system and the procedure of *Encryption/Decryption* are presented. The real states and implementations of using *sRFID-EDT* are shown in Section 3. At last, the conclusion is given in Section 4.

2 *Specific RFID Hard/Soft - Encryption/Decryption Technology*

Due to the demand of existed system integration, the proposed Specific RFID Hard/Soft - Encryption/Decryption Technology includes: Embedded Service Middleware Application, End User RFID Device/Tag, and RFID Hardware. The system framework is shown as Fig. 2. The Embedded Service Middleware Application is the main system to manage the internal and external system connections. The Embedded Service Middleware Application provides the optional RFID API and parser to communicate with the third party RFID Hardware.

For the end users, *End User RFID Device/Tag* which colored pink consists of two appliances: *end user RFID tag* and *end user RFID device*. A user can only use a given RFID tag or a device such as PDA or CD player which equipped a *RFID Hardware*, or use both appliances.

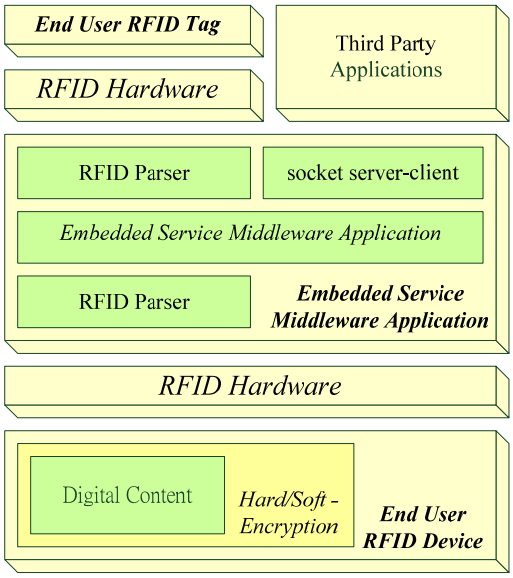


Fig. 2. The framework of *Specific RFID Hard/Soft - Encryption/Decryption Technology*

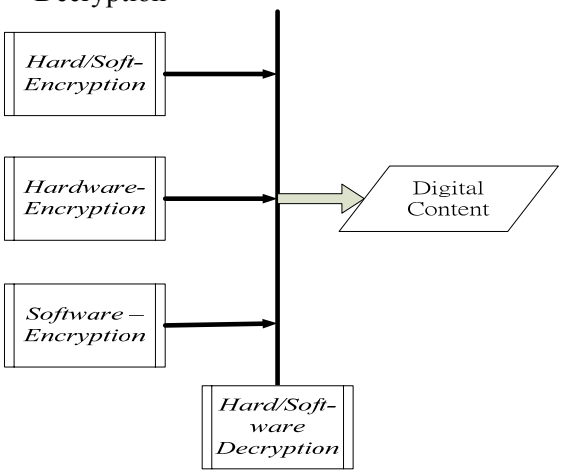
In this paper, *sRFID-EDT* provides the *Encryption/Decryption* principles. If the digital content and data is protected via a given RFID tag, the related information of the commercial data or multimedia is locked and encrypted by the *sRFID-EDT*. In other words, there are two possible ways to protect the digital content.

First, depending on the digital content storage hardware such as CD-ROM disk, the commercial RFID tag can be embedded into the disk when the disk is made. According to the characteristic of RFID tag, each RFID tag can be set with different individualities. The different encryption code, unique ID, information of the digital content, or authentication serial number can be recorded in the RFID tag. In addition, the RFID tag embedded in the disk is not rewritable. Hence, different disks equip the different IDs of RFID tag. When the RFID reader inducts the tag, the information about this storage can be scanned and presented. In other words, only the digital storage with the valid RFID tag is legal and true.

Second, since the content or data are digital, these software, content or data, can be encrypted as the secret codes or cipher. The key for encryption and decryption can be recorded in the RFID tag. Without the specific key, these secret codes or ciphers cannot be recovered as the original data. In other words, the digital content that recorded in the storage device (such as CD-ROM disk) can be secured. The decryption key can be recorded in the RFID tag embedded in the storage or a palm RFID tag (such as a RFID toy).

Since there are two possible ways to protect the digital content, for the end users, there will be at least three possible states of *sRFID-EDT Hard/Soft - Encryption/Decryption* shown as follows:

1. Combination of Hard/Soft-Encryption/Decryption
2. Only Hardware-Encryption with Hard/Soft -Decryption
3. Only Software – Encryption with Hard/Soft-Decryption



2.1 *End User RFID Device/Tag*

For the end users, *End User RFID Device/Tag* is proposed in the paper. The storage, whether hardware (CD-ROM) which includes the encrypted digital content, or software (files or ciphers), is called *End User RFID Device*. If the *End User RFID Device* is hardware, the third party *RFID Hardware* can induct the RFID tag embedded in the hardware. After identifying the *End User RFID Device*, the application or user can execute and read the digital content if only *Hardware - Encryption/Decryption* is used.

According to three possible states, the end user must have the decryption key for executing the digital content. In this paper, the hardware (RFID tag) or software for the decryption key is called *End User RFID Tag*. After identifying the *End User RFID Device*, the end user has to provide the *End User RFID Tag* for the *Embedded Service Middleware Application*. Only the information or password of *End User RFID Tag* is correct and can be used to gain the secured decryption key which recorded in the *End User RFID Device*, the digital content recorded in the *End User RFID Device* can be presented. In this paper, the *End User RFID Device/Tag* key for encryption and decryption can be presented as Fig. 3.

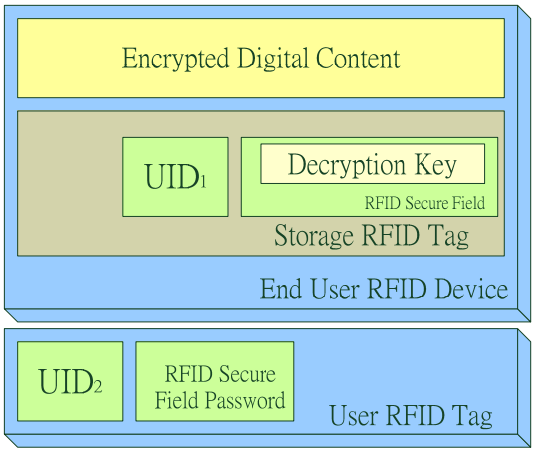


Fig. 3. The framework of *End User RFID Device/Tag*

2.2 *RFID Hardware*

Considering that the three possible states of *sRFID-EDT Hard/Soft - Encryption/Decryption* are based on the RFID induction, the *RFID Hardware* in this paper is divided into two types of equipments: for *End User RFID Device* and for *End User RFID Tag*.

According to the three possible ways to protect the digital content, when the protection is based on the Combination of *Hard/Soft-Encryption/Decryption* and Only *Hardware-Encryption* with *Hard/Soft –Decryption*, the *RFID Hardware* for *End User RFID Device* is needed. Due to that the digital content is protected by the RFID tag embedded in the hardware, the information recorded in the tag has to be inducted before using. For example, if a tag is embedded in the CD-ROM disk, the user should have a CD-ROM driver with the *RFID Hardware* when reading the disk. In other words, if the protection is based on the hardware belongs to *End User RFID Device*, the corresponding reader with *RFID Hardware* is necessary. The *RFID Hardware* can be embedded in the CD-ROM driver, reader, or other multimedia devices.

In opposition to *End User RFID Device*, when the *sRFID-EDT* decryption is based on the *End User RFID Tag* key, end user has to own the valid RFID tag for decrypting the digital content. For example, the decryption code is recorded in the RFID tag of *End User RFID Device*. However, the decryption code is secured by the password which locks the data slot of RFID tag. Without the correct password, end user cannot gain the decryption code that secured in the RFID tag of *End User RFID Device*. To provide the password, the end users should have the *RFID Hardware* such as the USB-RFID reader, etc.

2.3 *Embedded Service Middleware Application*

In this paper, there are two partitions: *End User RFID Device* and *End User RFID Tag*. Therefore, the application for communicating these two parts is needed.

To manage the RFID information, *Embedded Service Middleware Application* is proposed to parse the information from the *RFID Hardware*. Due to that there are different RFID product, an RFID parser is needed for analyzing and parsing the information from *RFID Hardware*. After gaining the requirements or response, the *Embedded Service Middleware Application* searches the corresponding applications and passes the information. Figure presents the framework of *Embedded Service Middleware Application*.

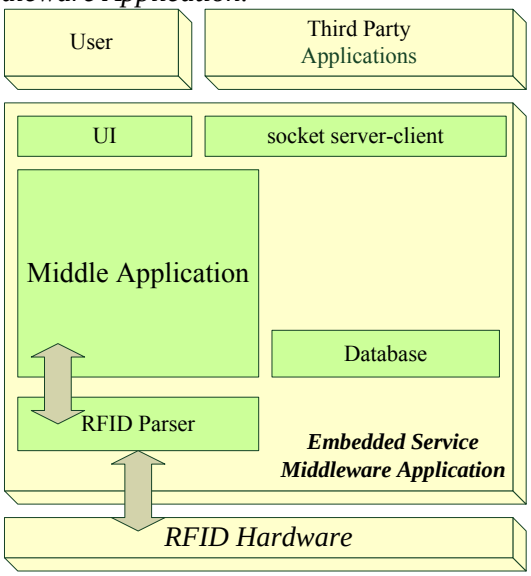


Fig. 4. The framework of *Embedded Service Middleware Application*.

In Fig. 4, for the purpose of common communication between different applications, the *Embedded Service Middleware Application* implements the socket server-client structure for communication with other existed or third party applications. The information comes from the *End User RFID Device*, such as specific password-requirement, will be recorded in the database of middleware application. The requirement will be maintained based on the on demand limitation of the period of validity or when the *End User RFID Device* is removed. In addition, when an end user tries to gain the digital data from the *End User RFID Device*, the middleware application request the end user for the password. Fig. 5 shows the flowchart of executing or gaining the digital content recorded in the *End User RFID Device*.

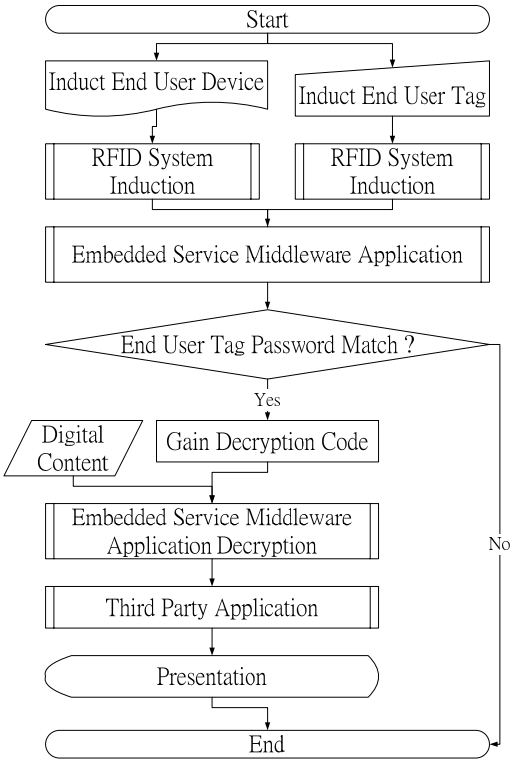


Fig. 5.The flowchart of executing or gaining the digital content recorded in the *End User RFID Device*.

After receiving the password, the middle application transmits the password and tries to gain the decryption code. If the password is correct, the decryption code will be transmitted to the user application such as multimedia player, etc. Otherwise, the digital content cannot be decrypted and used.

Therefore, only the two conditions: 1) the key information of *End User RFID Tag* matches the password requirement of *End User RFID Device*, and 2) the decryption code is correct in decrypting the digital content are satisfied, the user can gain the information from the *End User RFID Device*.

3 Implementation

To real test and verify the proposed *Specific RFID Hard/Soft - Encryption/Decryption Technology*, we develop the *Embedded Service Middleware Application* in Java language. The tag product of International Semiconductor Technology Ltd. (IST) [10] RFID reader and antenna are selected for the RIFD system real implementation. The tag product of IST is used for *End User RFID Tag* and *End User RFID Device*.

3.1 *RFID Hardware*

To enhance the convenience of RFID users, appropriate RFID systems and deployments is important. The frequency of RFID system used can be classified as LF (low frequency, 125~134KHz), HF (high frequency, 13.56 MHz), and UHF (ultra high frequency, 915MHz). The characteristics of these RFID systems are different and shown in Table 1.

Table 1. The characteristics of different RFID systems

	Low Frequency	High Frequency	Ultra High Frequency
Induction Distance	<2 Feet	<3 Feet	<10~30 Feet
Normal Application	Keyless entry	Smart Card	Electronic Toll Collection
Data Rate	Low ←----------→High		
Tag Size	Large←----------→Small		
Performance Near Metal / Liquids	Better←----------→Worse		

Furthermore, there are different antenna sizes of the RFID systems. Due to the power and size of RFID antenna, the induction distance between antenna and tag changes. To serve for normal user, embedded in normal user device, and keep the high security of RFID induction, the HF system with limited power for on demand induction distance can be a good solution.

In this paper, to implement the *RFID Hardware* that embedded in the digital content reader, only the RFID reader and antenna hardware are embedded in the reader. Fig. 7 shows the verification device. In Fig. 7 (a), the *RFID Hardware* is embedded in inside the sample mp3 player. Then, according to the application, the mp3 player with *RFID Hardware* can be re-modified as different model such as a toy platform shown in Fig. 7 (b)

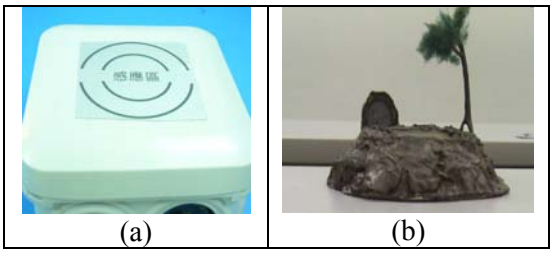


Figure. 7. The sample verification of mp3 player with *RFID Hardware*.

The *RFID Hardware* mainly consists of antennas and a reader. No matter the RFID tag is used, a individual and unique ID, and finite information are recorded in each RFID tag. The tag is triggered when it approaches the RFID antenna. The information recorded in the tag is transmitted through the antenna

to the RFID reader. To guarantee the stability and accuracy of RFID tag detection and identification within the finite time, the state of antenna and reader are always on.

3.2 *End User RFID Device/Tag*

According to the end user behavior, the *End User RFID Device/Tag* should be designed as small as possible. In this paper, the suitable size of *End User RFID Device/Tag* especially for information appliances is important. Therefore, the RFID tag with antenna in Φ8.5x0.96 (mm), ISO-14443A/15693-2-3, Operation Frequency(MHz) 13.56, with Memory Size(Bits) 256 / 1024, is selected for verification test.

In addition, this RFID inlay tag is embedded in the ID 3D toy or the metal paster. These 3D RFID toy tags are small and can be used as the *End User RFID Tag* which record the unique ID and on demand given data. Furthermore, considering the currently possible and realistic Specific RFID Hard/Soft - Encryption/Decryption Technology, the Software – Encryption with Hard/Soft- Decryption is implemented. The multimedia data that on demand encrypted is saved in the mp3 player.

4 Conclusion

In this paper, a *Digital Content and Data Intellectual Property Protection based on Specific RFID Hard/Soft-Encryption/Decryption Technology* is proposed to integrate the existed service systems, multimedia storage devices, and application. The *sRFID-EDT* provides the API module and related parser that can easily embed other systems in. The verification shows that the *sRFID-EDT* is realistic and can provide the encryption/decryption for digital content.

References:

[1] Hoboken RFID-enables Its Parking Permits, *RFID Journal*, June 2006, http://www.rfidjournal.com/article/articleview/2421/1/1/

[2] Hospital Uses RFID for Surgical Patients, *RFID Journal*, July 2005, http://www.rfidjournal.com/article/articleview/1714/1/1/

[3] RFID Hospital: Columbus Children's Hospital To Install RFID System From Mobile Aspects, *RFID Solution Online*, March 2007.

[4] RFID trial tracks hospital equipment, http://www.computing.co.uk/computing/news/2168717/rfid-trial-tracks-hospital

[5] RFID Takes a Swing at Ticket Fraud, *RFID Journal*, December 2005, http://www.rfidjournal.com/article/articleview/2060/1/1/

[6] Moscow Metro Tries RFID-Enabled Ticketing, *RFID Journal*, February 2007, http://www.rfidjournal.com/article/view/3049/

[7] Beijing Olympic Games Prompts RFID Development in China, http://www.rfidglobal.org/news/2007_9/20070931653253861.html

[8] Ming-Shen Jian and Shu-Hui Hsu, "Location Aware Public/Personal Diversity of Information Services based on embedded RFID Platform," Proc.ICACT'09, pp.1145-1150, Feb. 2009.

[9] Ming-Shen Jian, Kuen Shiuh Yang, and Chung-Lun Lee, "Modular RFID Parking Management System based on Existed Gate System Integration," WSEAS Trans. on System, vol. 7, pp.706-716, Jun. 2008.

[10] http://www.ist.com.tw/

[11]Ming-Shen Jian, Kuen Shiuh Yang, and Chung-Lun Lee, "Context and Location Aware Public/Personal Information Service based on RFID System Integration," WSEAS Trans. on System, vol. 7, pp.774-784, Jun. 2008.

[12] Z. Pala and N. Inanc, "Smart Parking Applications Using RFID Technology," *Proc. of 1st Annual RFID Eurasia*, pp. 1 – 3, September 2007.

[13] M. F. Lu, S. Y. Chang, C. M. Ni, J.-S. Deng, and C. Y. Chung, "Low Frequency Passive RFID Transponder with Non-revivable Privacy Protection Circuit," *Proc. of WSEAS Inter. Conf. on Instrumentation, Measurement, Circuits, and Sys.*, pp. 166-169, Hangzhou, China, April 2006.

[14] M.vilammi, L.vSydänheimo, P. Salonen, and M. Kivikoski, "Read Range Analysis of Passive RFID Systems for Manufacturing Control Systems," *Proc. of WSEAS Inter. Conf.*, pp. 2081-2085, May 2002.

[15] S.-C. Cha, K.-J. Huang, and H.-M. Chang, "An Efficient and Flexible Way to Protect Privacy in RFID Environment with Licenses," *Proc. of IEEE Inter. Conf. on RFID*, pp. 35-42, April 2008.

[16] S. Yoo, J. Lee, Y. Kim, and H. Kim, "An integrated mobile REID service architecture between B2B and B2C networks," *Proc. of ICACT Inter. Conf.* , pp. 90-93, February 2007.

[17] M. M. Hossain and V. R. Prybutok, "Consumer Acceptance of RFID Technology: An Exploratory Study," *IEEE Tran. on Engine. Manag.*, Vol. 55, No. 2, pp. 316-328, MAY 2008