RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection

MING-SHEN JIAN[+], TA-YUAN CHOU[#], SHU HUI HSU[!]
[+] Department of Computer Science and Engineeing, National Formosa University, Yunlin, Taiwan
[#] Department of Computer Science and Engineeing, National Sun Yat-sen University, Kaohsiung, Taiwan
[!] International Megatrend Smart Technology Ltd., BVI.

jianms@gmail.com[+], tayuan@gmail.com[#], suhue28@yahoo.com.tw[!]

Abstract: - In this paper, a *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection* is proposed. The encryption code for each multimedia or data is embedded in the existing encryption algorithm. Furthermore, the unique ID of RFID tag can guarantee the legality of each RFID tag. Two types of RFID tag is implemented for multimedia/digital content and normal user. The encryption code is recorded and locked in the data slot of RFID tag which embedded in the digital content storage hardware. Only normal user provides the corect RFID tag with legal key for unlocking thedata slot, he encryption code can be gained. The verification shows the proposed technology 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 [2-4,18]. Patients should always wear the RFID tag is designed for 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. Furthermore, the RFID system including RFID induction antenna, RFID parser and reader, RFID tag, etc., today is cheap. Some RFID tag such as ticket or card cost only about $. In addition, the RFID hardware including antenna and reader is not only cheap but also can be a PnP device []. It means that the RFID hardware can be used as a normal user device such as the card-reader.

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, *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection* (*E/DonRFID*), is proposed. By using the *E/DonRFID*,

1) each digital content such as a multimedia 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 code/decode and hardware key induction which can be embedded in the existed systems or devices. Considering the implementation, three possible procedures are proposed in this paper.
3) only the legal user can gain/decrypt and execute/play the digital content. The digtal content is protected by two stages: 1. encryption code, and 2. The key serial number for unlocking the data slot which records the encryption code.
4) different types of RFID such as size, frequency, even appearance can be selected and designed.

The concept of *E/DonRFID* including multimedia player, RFID, and user can be shown as the Fig. 1.

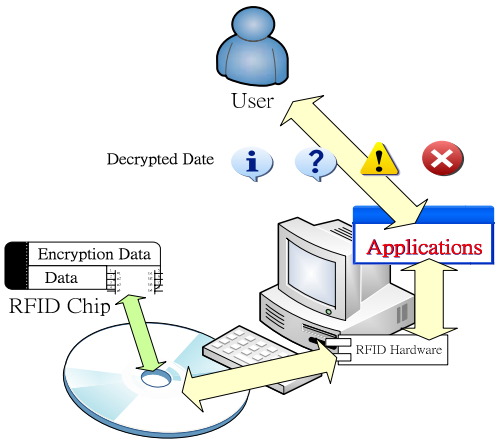


Figure 1. The concept of *E/DonRFID* multimedia player

The remainder of this paper is organized as follows. In Section 2, the proposed *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection* system and the procedure of *Encryption/Decryption* are presented. The real states and implementations of using *E/DonRFID* are shown in Section 3. At last, the conclusion is given in Section 4.

2 RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection

Due to the demand of existed system integration, the proposed *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection* includes: *PnP Middleware*, *RFID Hardware*, *End User RFID Device* and *End User RFID Tag*, and Encryption/Decryption Procedure. The system framework is shown as Figure 2. The

PnP Middleware is the main application to manage the connections and requirements from *End User RFID Device* and *End User RFID Tag*. The *PnP Middleware* also provides the RFID API and parser to communicate with the third party RFID Hardware. Furthermore, after gaining the encryption code, the *PnP Middleware* also provides the code for user's application such as multimedia player via software API.

For a normal user, there are two types of RFID devices for the *E/DonRFID* system: *End User RFID Device* for digital content or multimedia information gaining, and *End User RFID Tag* for indentifying the legal user.

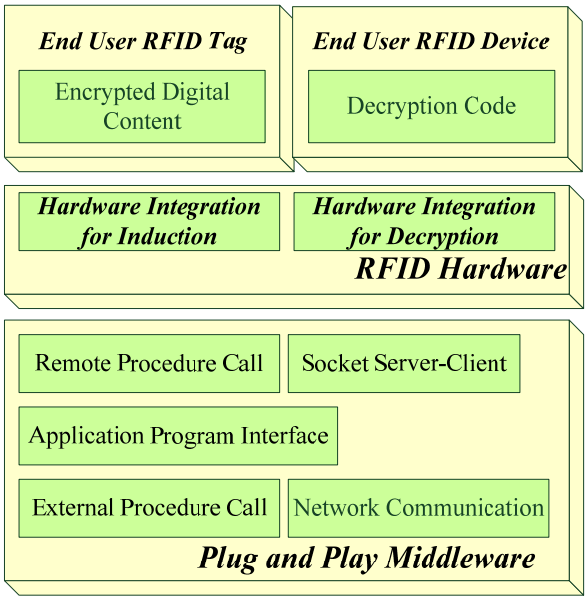


Figure 2. The framework of *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection*

In this paper, *E/DonRFID* not only provides the RFID based protection procedure but also includes the *Encryption/Decryption* method based on RFID character. The encryption and decryption can be implemented by hardware or software solution. The original digital data is encrypted by 1) hardware, 2) software, or 3) combination of hardware and software. Corresponding to the encryption method, suitable RFID tag of user for decrypting is needed.

2.1 End User RFID Facilities

For the end users, two possible facilities: *End User RFID Tag* and *End User RFID Device* are proposed in the paper.

For example, the encrypted digital content is recorded in the storage hardware such as CD-ROM disk or Flash Memory Disk. The storage hardware may equip the RFID tag. The unique ID (UID) of the storage is used to provide the information for identifying that this storage hardware is valid or not. Since the RFID tag embedded in the hardware is not re-writable, the UID for each RFID tag can be on demand assigned individually. In other words, each storage hardware can be equipped a different and unique ID for legitimate rights proof of user. In addition, the secured field of RFID tag can also provide the information such as decryption key. In other words, to decode or decrypt the digital content,

In this paper, the hardware which stores the encrypted digital content, or equips the RFID tag, or further equips both, is called *End User RFID Device*.

In opposition to *End User RFID Device*, according to possible states of encryption method, the end user must have the decryption key for executing and obtaining the encrypted digital content. In this paper, the hardware (RFID tag) which records the decryption key is called *End User RFID Tag*.

Figure 3. The sample of *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 Figure 4.

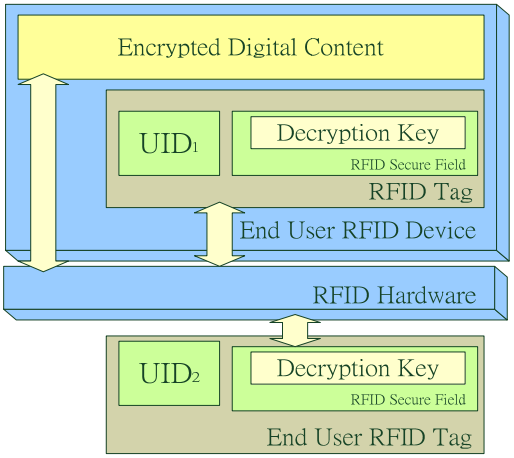
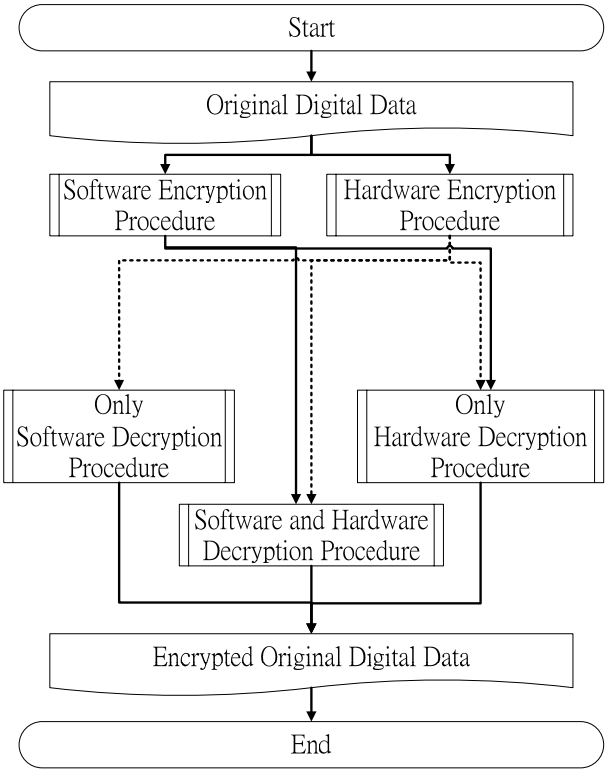


Figure 4. The framework of *End User RFID Device* and *End User RFID Tag*

2.2 Possible Encryption Method

Since three possible ways to protect the digital content are proposed above, for the end users, there will be at least five possible states and method of *E/DonRFID*, to gain the protected digital data, shown as follows:

1. Encryption and Decryption by Hardware and Software combination,
2. Encryption only by Hardware with Hardware and Software combination Decryption
3. Encryption only by Software with Hardware and Software combination Decryption
4. Encryption only by Hardware with Hardware Decryption
5. Encryption only by Software with Hardware Decryption



Corresponding to the encryption methods, normal users have to provide the correct security key information for data decryption. Due to the possible encryption / decryption method, the digital data may need the hardware, software, or both for decryption. In other words, a user has to provide the corresponding RFID tag or adopt the corresponding RFID application which matches the requirements for gaining the data recorded in the *End User RFID Device*.

Encryption Method 1: via using hardware. Depending on the *End User RFID Device* such as CD-ROM disk or Flash Memory 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. In other words, the owner of the digital content can input the monopoly security identification mark such as security code, password, etc. into the RFID tag. These RFID tag embedded in the storage hardware is not rewritable. Therefore, different digital content can be assigned different encryption code, RFID unique ID. Furthermore, the information of the digital content or authentication serial number can be also recorded in the RFID tag. Hence, different disks equip the different IDs, information, and data of RFID tag. In other words, the digital content that recorded in the storage device (such as CD-ROM disk) can be secured.

In addition to UID of RFID tag, each RFID tag provides the secured field via limited memory. Only when the user has the correct password the information secured in the RFID memory can be gained. Therefore, some information for encryption and decryption, such as decryption key or coding, can be also secured in the RFID tag.

Encryption Method 2: since the content or data are digital, these software, content or data, can be encrypted as the secret codes or cipher. The digital content such as multimedia is transferred to coded digital data, or locked/secured by the on demand password or coding method. Without the specific key or password, these secret codes or ciphers cannot be recovered as the original data.

2.3 Corresponding Decryption Method

When the storage hardware with RFID tag is inserted into the reader, the embedded RFID reader will induct the RFID tag of the storage hardware. The information about this storage can be scanned and read.

No matter the digital data is encoded or encrypted via using hardware or software, the corresponding key or password is needed. The decryption key can be recorded in the RFID tag embedded in the storage or a palm RFID tag (such as a RFID toy). To gain the digital content, according to the possible encryption method, end users have to provide or use the corresponding encryption hardware or software.

Decryption Method 1- Encryption by Hardware with only Hardware Decryption: the *End User RFID Device* equips the RFID tag. In addition, only the hardware for decryption is needed. The end user should own a corresponding *End User RFID Tag*. When the end user wants to read or obtain the digital content, the hardware, corresponding/valid *End User*

RFID Tag, should be inducted. Then, the digital content can be obtained and decrypted.

If the decryption code is protected and recorded in the *End User RFID Device*, the password to unlock the memory of RFID tag in *End User RFID Device* is needed. The end user has to provide the *End User RFID Tag* which records the password. Then, the decryption key/code can be used to decrypt the digital content or data.

Decryption Method 2- Encryption by Software with only Hardware Decryption: as the decryption method 1, the end user should own a corresponding *End User RFID Tag*. The device which records the encrypted digital data may not equip the RFID tag. The data is encrypted with the specific key/code. Hence, when the user tries to obtain the content, the user has to provide the *End User RFID Tag*.

When the encrypted data is read, due to the *Intellectual Property Protection*, the user should provide the corresponding *End User RFID Tag*. The specific RFID tag will be inducted be the *RFID Hardware*. Then the information such as encryption code will be gained from the *End User RFID Tag* for the application (ex. Media player).

After identifying the information recorded in the RFID tag or the password, users who provide the correct RFID tag or password can gain the data. Therefore, only the digital storage or content with the valid RFID tag can be decrypted.

Since the digital content is encrypted and recorded in the hardware, to read or gain the data from the storage, the corresponding reader is needed. In the following sections, the detail procedure of decryption will be presented.

2.4 *RFID Hardware*

Considering that the five possible states of possible encryption method in the proposed *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection,* the obtainment of digital data or content are based on the RFID induction.

Therefore, the corresponding hardware to induct the RFID tag, decrypt or decode the digital data, and present the content is important. The *RFID Hardware* in this paper is divided into four types of equipments: *RFID Antenna*, *RFID Reader*, and the *Hardware Integration for Induction*.

The *RFID Antenna* is the main component for RFID tag induction. The antenna continuously spreads the electromagnetic wave. The energy is transmitted to the RFID tag. After induction, the *RFID Antenna* also receives the signal from the RFID tag.

After receiving the signal, the *RFID Reader* translates the signal into the digital data such as the UID of this RFID tag. Then, the *RFID Reader* sends the digital data to the corresponding systems or applications.

However, according to the *Possible Encryption Method* to protect the digital content, when the protection is based on *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection*, it means that there is a RFID tag as the hardware key or lock embedded in the storage of the digital content. Corresponding to the *Decryption Method* and the types of the storage, suitable decryption hardware is needed. For example, if a tag is embedded in the CD-ROM disk, the user should have a CD-ROM with the *RFID Hardware* when reading the disk. Hence, in this paper, *Hardware Integration for Induction* is used to induct the RFID tag of the storage.

Hardware Integration for Induction

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. The general used as the multimedia storage or hardware can be CD, VCD/DVD, memory disk/card, or flash memory. Most storage needs the corresponding reader such as CD-ROM or Card Reader. To enable the *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection*, these corresponding readers must equip the *RFID Antenna* and *RFID Reader*. In this paper, the reader that can induct the RFID tag of the storage is called the *Hardware Integration for Induction*.

However, not all the storage equips the RFID tag. In other word, the storage not only with but also without RFID tag is available and should be readable via a reader. To ensure the validity of the digital content recorded in the storage, different corresponding procedures are proposed:

1) *End User RFID Device* Induction: since the RFID tag is embedded in the storage hardware, the corresponding reader must equip the *RFID Antenna* and *RFID Reader*. For example, the *RFID Antenna* and *RFID Reader* can be plugged or embedded in the CD-ROM. When the *End User RFID Device* is read, the *RFID Antenna* and *RFID Reader* of CD-ROM induct the storage device.

However, not all the storage device equips the RFID tag. Therefore, the integrated hardware has to separate the device into two types: Normal/Privacy device without the RFID tag and the *End User RFID Device*.

2) If the device cannot be inducted or without the RFID tag, called Normal/Privacy device, only the digital content without the *Intellectual Property Protection* can be read. If there is content with protection, only when the user provides the decryption key the protected content can be read. In other words, the *Hardware Integration for Decryption* is needed.

Hardware Integration for Decryption

Then, when the storage is defined or separated into the *End User RFID Device*, the corresponding decryption method at the end user reader, *Hardware Integration for Decryption* is needed:

1) Encryption and Decryption by Hardware and Software combination: since the digital content is protected by the *End User RFID Device*, the *Hardware Integration for Induction* can induct the RFID tag embedded in the device. Then, the UID information and corresponding password or decryption code can be obtained.

According to the decryption method mentioned above, the client user may need the *End User RFID Tag* to decrypt the protection. If the *End User RFID Tag* is needed, the client user should provide the corresponding *End User RFID Tag*.

To induct the *End User RFID Tag*, in this paper, the RFID inductor for *Hardware Integration for Induction* is proposed and designed as the small induction-panel which can be embedded in the MP3 player. When the user put the *End User RFID Tag* on the induction panel, the decryption information will be obtained and used to decrypt the *Intellectual Property Protection*.

For example, the decryption code is recorded in the RFID tag of *End User RFID Tag*. 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. By using the *End User RFID Tag*, the application (Media Player Application) gains the decryption code and then can play the multimedia file.

2.5 *Plug and Play Middleware*

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. When using the *End User RFID Device*, 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. Due to that there are many types of *RFID Hardware*, the application program interface (API) for the different third party *RFID Hardware* is needed. In addition, the end user applications are various. Hence, the plug and play middleware for different hardware and applications is important.

To manage the RFID information from different *RFID Hardware*, and the communication with different applications, the *Plug and Play Middleware* is proposed. To realize the concept of *Plug and Play*, the proposed middleware has to manage the information from the all possible third party *RFID Hardware*, deal with and parse the information, and then provide the required information to the corresponding applications. Therefore, the main purposes of the proposed *Plug and Play Middleware* are:

1) to parse the information from the *RFID Hardware*. Due to that there are different RFID product, the RFID parser is needed for analyzing and parsing the information from *RFID Hardware*. The information about UID, password, etc. will be parsed as the string for the further execution of applications.

In this paper, two possible parsers are established. First, the *Plug and Play Middleware* provides the remote procedure call (RPC) function for the third party *RFID Hardware*. The UID of the RFID tag inducted by the *RFID Hardware* will be formulated as the string. In addition, the password or requirements for further information such as decryption code recorded in the *End User RFID Device* can be provided by the remote procedure call function.

Second, for general communication, the *Plug and Play Middleware* also provides the sever-client socket link between the *RFID Hardware* and the middleware. In other words, even the *RFID Hardware* cannot implement the remote procedure call, depends on sever-client socket link, the information can be transmitted between *Plug and Play Middleware* and *RFID Hardware*.

2) to provide the application program interface (API). Since the *RFID Hardware* may not directly communicate with the applications, the *Plug and Play Middleware* has to implement the corresponding API for other third party applications or software.

In this paper, the *Plug and Play Middleware* also implements two possible APIs: the external procedure call and network communication. If the application is embedded in the *Plug and Play Middleware*, the external procedure call sends the required information to the specific application. In addition, some communications of the related applications such as database query are also established by the external procedure call. Then, the *Plug and Play Middleware* deals with the results

from the external procedure call. In opposition to external procedure call, for the concept of *Plug and Play*, normal network communication is implemented. The third party software or applications can communicate with the *Plug and Play Middleware* via sending the information in string format. For example, if the third party application requires the further checking, the *Plug and Play Middleware* sends the required information such as UID to the server via Internet. After obtaining the response from the server, the *Plug and Play Middleware* acknowledges the third party application and then decrypts the digital content.

After gaining the requirements or response, the *Plug and Play Middleware* searches the corresponding applications such as media player and passes the information to the specific application. Figure presents the framework of *Plug and Play Middleware*.

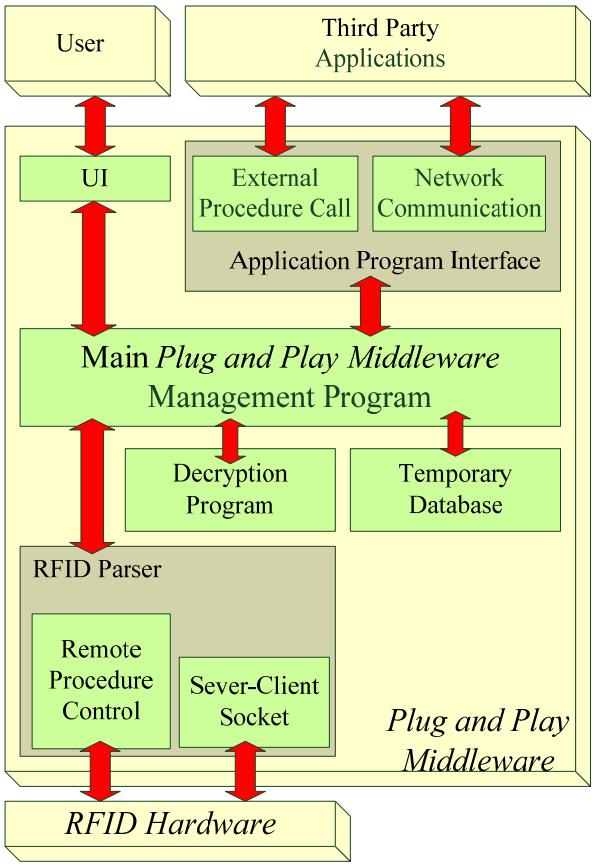


Figure 6. The framework of *Plug and Play Middleware*.

In Figure 6, for the purpose of *Plug and Play* common communication between different applications, the *Plug and Play Middleware* implements the socket server-client structure and remote procedure call 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 managed. In opposition to *End User RFID Device*, the password or decryption code from the *End User RFID Tag* will be recorded in the temporary database of *Plug and Play Middleware*. The requirement will be maintained based on the on demand limitation of the period of validity or when the *End User RFID Device* or *End User RFID Tag* is removed. In addition, when an end user tries to gain the digital data from the *End User RFID Device* via other third party application or software, the *Plug and Play Middleware* will communicates with the specific application via external procedure call or network communication. Figure 7 shows the flowchart of executing or gaining the digital content recorded in the *End User RFID Device*.

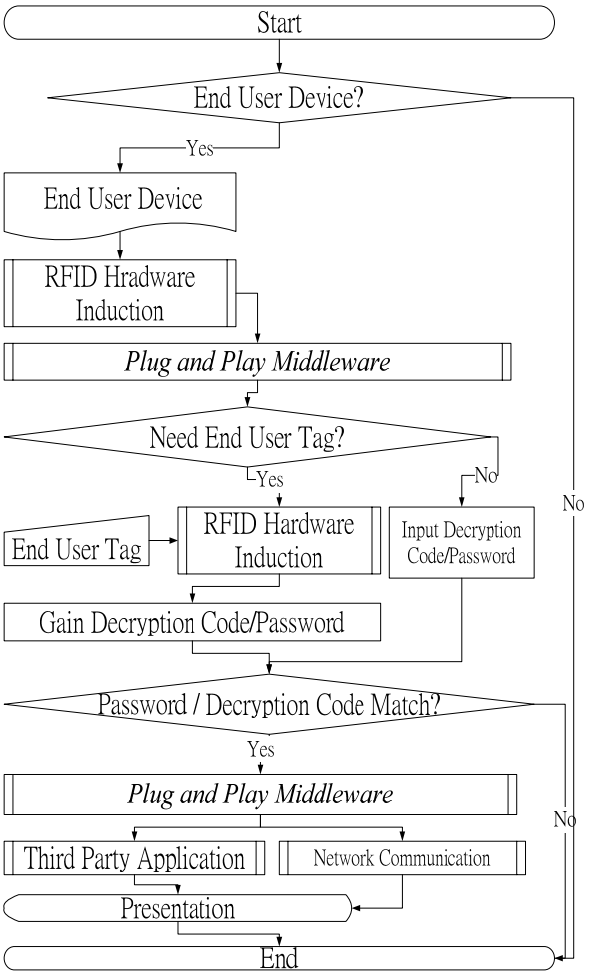


Figure 7.The flowchart of executing or gaining the digital content recorded in the *End User RFID Device*.

After receiving the password, the *Plug and Play Middleware* differentiates that the hardware decryption is needed or not. According to the possible encryption method, the hardware, *End User RFID Tag*, may be required for the password to

obtain the secured decryption code which protected in the tag memory of *End User RFID Device*. If the *End User RFID Tag* is needed, the *Plug and Play Middleware* searches for the *End User RFID Tag* and tries to gain the information such as the UID, decryption code, or the password for the *End User RFID Device*.

After obtaining the information from the *End User RFID Tag*, the *Plug and Play Middleware* transmits the password and tries to gain the decryption code. If the decryption code is correct, the *Plug and Play Middleware* acknowledges the application and provides the decryption code for data decoding. When the *End User RFID Tag* is needed, if the password is correct, the decryption code recorded and secured in the *End User RFID Device* 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 *RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection*, we develop the *Plug and Play Middleware* in both Java and Visual Basic language.

3.1 *RFID Hardware*

To enhance the convenience of RFID users, appropriate RFID systems and deployments is important.

The tag product of International Megatrend Smart Technology Ltd. (IMST) [10] is used for *End User RFID Tag* and *End User RFID Device*. Due to the hardware control and possibility of realization, in this paper, the *End User RFID Device* is implemented as the MP3 player embedded with the RFID reader and antenna. The normal music file without any intellectual property protection can be played directly. If the music files are protected, the implemented MP3 player will try to induct the *End User RFID Tag* via modular *RFID Hardware*. Only the valid corresponding *End User RFID Tag* is inducted the application can decrypt and play the music files. Furthermore, in our implementation, the multimedia data can be on demand encrypted and saved in the mp3 player. The proposed MP3 player is designed that the application can automatically play the music file which is corresponding to the *End User RFID Tag* inducted.

Generally, 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. In addition, 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. In our implementation, considering the induction distance and the power consumption, the LF *RFID Hardware* is selected for our MP3 player.

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		

In this paper, to implement the *RFID Hardware* that embedded in the MP3 player, only the RFID reader and antenna hardware are embedded in the player. Figure 8 shows the verification device. In Figure 8 (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 Figure 8 (b)

(a)

(b)

Figure 8. The sample verification of mp3 player with *RFID Hardware*. (a) The prototype of none decoration MP3 player. (b) Decorated MP3 player (with the RFID induction panel)

The *RFID Hardware* mainly consists of antennas and a reader. No matter the various types of RFID tag surface are used, an individual ID (UID), and finite information are recorded in each RFID tag. The test tag is triggered when it approaches the MP3 RFID antenna. The information recorded in the test tag is transmitted through the antenna to the RFID reader embedded in the MP3 player. 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.

(a)

(b)

Figure 9. The *End User RFID Tag* used for the proposed MP3 player. (a) the original size of the RFID tag embedded in the 3D toy. (b) the prototype of *End User RFID Tag*.

In addition, the test *End User RFID 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. The size of the *End User RFID Tag* is small enough for the end user.

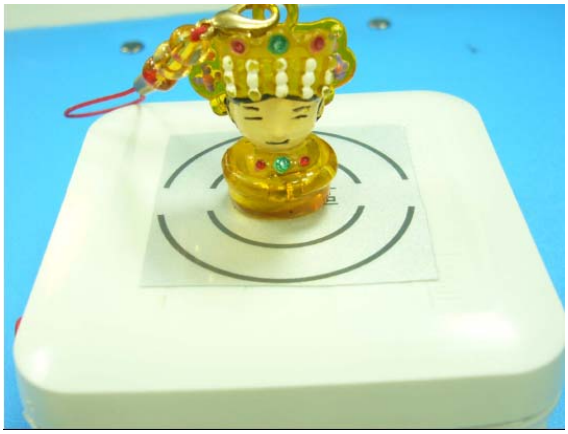


Figure 10. The sample verification of mp3 player with the *End User RFID Tag*.

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 Systems, 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 Systems, 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
[18] C.L. Lai, S.W. Chien, S.C. Chen, and K. Fang "Enhancing Medication Safety and Reduce Adverse Drug Events on Inpatient Medication Administration using RFID," WSEAS Trans. on Communications, vol. 7, pp.1045-1054, Oct. 2008.