

System Design for Food Forgery Prevention and Traceability Using RFID Technology

Tian Tian^{1,a}, Peng XiangJun^{1,b} and Nie YanFeng^{1,c}

¹Automation Department Beijing Oil Research Institute, Beijing 102300, P.R. of China

^aemail: oraclepla@126.com, ^bemail: dmpxj@163.com, ^cemail: nicenyf@163.com

Keywords: RFID; Food Forgery Prevention; Traceability; Identification

Abstract. Nowadays, food safety has drawn increasing attention because of its importance, yet the cost spent on food forgery prevention is expensive and the system is hard to maintain, therefore a low cost system is worth developing. Based on the above fact, this paper proposes a system design for food forgery prevention and traceability using RFID technology. The system's hardware section consists of RFID reader, antenna and tag, to reach the design goal and save the total cost, the following measures are taken: 1, to build a forgery prevention and traceability system; 2, to compare different communication protocols and select a system based on ISO/IEC 15693 standard; 3, to develop key hardware section, such as, setting the EAS function, designing a 16-slot anticollision flow, tuning the value of antenna's Q factor and resonant frequency. Such system has a variety of applications such as wine and cigarette.

Introduction

Food safety is becoming more and more important because of the uncontrollable sessions during the manufacturing, processing, transporting and marketing. Counterfeiting goods can be great benefit, so there are many people and organizations doing related forgery jobs. Once serious problems are exposed, it is hard to trace the source of the food and few people are punished. Take expensive wine or cigarette for example, there exist thousands of fake products yet lack of valid detection method, most of the anti-counterfeiting way are laser or security code technique, such methods can be broken easily and less expensive.

Food problems can be settled by building food forgery prevention system and traceability system, all of the useful information during the flow of production are save in the system, once there exists a problem in anywhere, we can still trace the source and find its reason. Two techniques can be adopted, barcode and RFID technique.

The former has been used widely in food traceability and the cost is even low than most of the existed RFID tag in the past few years, however, with the rapid development of VLSI technology and the progress of semiconductor, the manufacturing cost of single chip is shrinking every year, some RFID tag are cheap enough to replace barcode in many particular applications. If the application does not cost sensitive, then RFID would be the best choice.

Compare to barcode, RFID has the following advantages: 1, reading more tags at the same time; 2, has a strong power of anti pollution capacity; 3, having penetrating and reading without barrier; 4, can be reused and rewritten for over 100000 times or more; 5, more secure for the anti-counterfeiting. Based on the above advantages, and if the cost can be cut down, RFID system is the best choice.

With RFID, goods can be recognized automatically and quickly compare to slowly manual operation, with its help people will pay no worry about forgery of goods. RFID system consists of reader, middleware, antenna and tag and is based on the operating principle of electromagnetic induction, its passive advantage make it suitable for severe environment such as snowing, mining, radiation monitoring and so on. There exist several frequency ranges, the most important frequency ranges for RFID system are illustrated below: low frequency RFID ranging from 125KHZ to 135KHZ, 13.56MHZ HF RFID, UHF RFID ranging from 860MHZ to 960MHZ and 2.4GHZ microwave RFID [1].

There are some relative designs using RFID technology. For example, Ref. [2, 3] implement a RFID medical information system and entrance access control system based on ISO/IEC 15693, Ref. [4-6] implement RFID-based traceability system, yet there are nothing discussion about cost spent on the system and lack of key design such as antenna and Q factor. If the system is applied widely and needs tens of millions of tags, cost must be considered.

What kind of RFID system should we select and how can we avoid forgery draw designer's attention.

In this paper, we first design a system that can provide anti-forgery and traceability functions; second, discuss low cost RFID systems and select a kind of suitable tag which is based on selected communication standard; third, hardware design methods are expressed including anti- forgery function using EAS which is integrated inside the tag chip, anticollision function and a tuning method of Q value and resonant frequency.

At present the main means is low click type and the lever type, low click type is on the bottom of the ball through attack the ball flew over obstacles, this method is able to pick the ball's advantages and makes the energy loss in institutions least, the shortcoming is the ball high requirement of the shape of the electromagnetic valve [11]. Therefore, the development of a high-performance control system of soccer robot has become an urgent desire for soccer robot fans.

In this paper, we first design a system that can provide anti-forgery and traceability functions; second, discuss low cost RFID systems and select a kind of suitable tag which is based on selected communication standard; third, hardware design methods are expressed including anti- forgery function using EAS which is integrated inside the tag chip, anticollision function and a tuning method of Q value and resonant frequency.

System Design

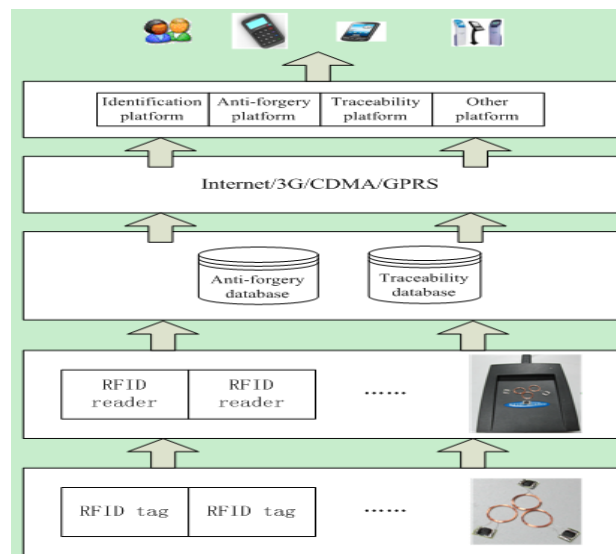


Fig.1. Food forgery prevention and traceability system

Fig. 1 shows the designed system and is composed of five levels. The bottom level includes RFID tags, with them food's basic information can be written inside the tags, such as food name, production day, out of day, enterprise ID, tag's unique ID and so on. Take wine anti-forgery and traceability for example, the tag must be packaged into fragile tag, once the tag is illegally torn out of the bottle, the tag will damage and cannot be used any more. The second level is RFID reader, it is used for the tag's read and write operation, one box of wine should configure with one RFID reader. The third level is the database which provides static product related data, there are mainly two kinds of database: anti-forgery database and traceability database, basic information is stored according to tag's unique ID. And the fourth level is the communication layer, it supports internet, 3G, CDMA or GPRS and so on. Finally, we can form a series of platform such as identification platform, anti-forgery platform, traceability platform and other platform, besides, mini POS or self service inquiry terminal can be used for any people who want to check the product's information.

To build the system, the first thing we should do is to develop a RFID system using reader and tag, yet there are several kinds of RFID, how to decide which system is the best choice is still a problem, once the first and second level are constructed, the other parts are easy to design.

Cost Analysis

Food safety is becoming more and more important because of the uncontrollable sessions during the manufacturing, processing, transporting and marketing. Counterfeiting goods can be great benefit, so there are many people and organizations doing related forgery jobs. Once serious problems are exposed, it is hard to trace the source of the food and few people are punished. Take expensive wine or cigarette for example, there exist thousands of fake products yet lack of valid detection method, most of the anti-counterfeiting way are laser or security code technique, such methods can be broken easily and less expensive.

$$C_{total} = N_{reader} C_{reader} + N_{tag} C_{tag} = N_{tag} (C_{reader} \cdot 0.01\% + C_{tag}) \tag{1}$$

Here, N means the number of reader or tag, and C is the cost of reader or tag, the tag’s cost is composed of chip and package cost and the former’s cost is the biggest one which can be expressed as formula 2 and 3:

$$\text{cost of chip} = \frac{\text{cost of wafer}}{\text{chips per wafer} \times \text{die yield}} \tag{2}$$

$$\text{chips per wafer} = \frac{\pi \times (\text{wafer diameter} / 2)^2}{\text{chip area}} - \frac{\pi \times \text{wafer diameter}}{\sqrt{2 \times \text{chip area}}} \tag{3}$$

From the above formula, it can be seen that the total cost is a strong function of the chip area, so more chips in one wafer means low cost, thus RFID chip with MCU or little Mifare crypto algorithm will be more expensive than RFID chip which is according to ISO/IEC 15693 protocol. When the number of the tag is over 10000000, the tag’s cost becomes giant, how to select possible reader and tag becomes a challenge.

System	Freq.	Distance	Eeprom	Tag Price	Reader Price
15693	13.56	0-70	256~1024	0.6	100
14443	13.56	0-10	1024~8192	1.0	200
UHF	860-960	0-100	256~512	0.6	1000

Tab.1. Possible systems for anti-forgery and traceability (Units: Freq. (MHZ), Distance (cm), Eeprom (bits), Price (CNY))

Table 1 shows different systems and their important characteristics, for selecting a suitable system, it is wise to compare their read and write distance, typical eeprom size, tag price and reader price. It is obvious that system base on ISO 14443 has high security, yet its valid distance is short, though the distance of UHF system is really long, its reader price is expensive. System based on ISO 15693 has a good performance of read and write distance and an acceptable price for both tag and reader. There are several manufacturers such as NXP, TI and ST, their typical products are ICODE, Tag-it and LRI2K. The latter two products are based on basic ISO/IEC 15693, yet NXP supports extra EAS commands which can be used for anti-counterfeiting. Therefore, NXP’s ISO/IEC 15693 product would be better for the system design.

Hardware Design

The key performance of the hardware includes reader, anti-forgery function, anticollision function and long read and write distance, then the following sections are further discussed.

A. Reader Design

Reader should be designed to communicate with tags, it must support all of the commands according to ISO/IEC 15693 protocol and some NXP’s proprietary command such as EAS command. Table 2 shows the supported command of the designed reader. To get the unique ID of the tag, Inventory command should be used; to get the data written in eeprom, read single block

command should be executed.

Fig. 2 shows the demo software of RFID reader, click ‘inventory’ button you can acquire tag’s UID; click ‘W’ button and fill in the corresponding data such as DSFID, AFI or block data, you can write message into eeprom; click ‘R’ button and select the block number, you can read data out of eeprom; the right side of the software includes data stored in eeprom, such as addresses, block data and lock bit.

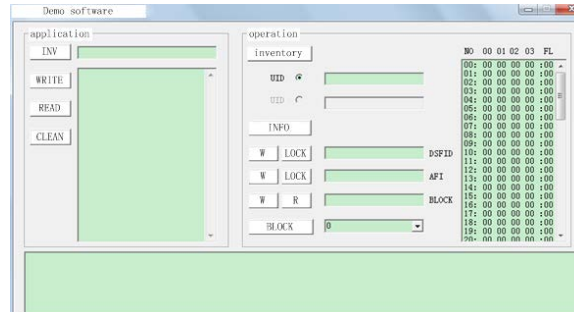


Fig.2. Demo software of RFID reader

	command	meaning
ISO15693 mandatory command		
01H	Inventory	Get UID
02H	Stay quiet	Enter into quiet state
ISO15693 optional command		
20H	Read single block	Read data from eeprom
21H	Write single block	Write data into eeprom
22H	Lock block	Lock single block
23H	Read_Multi_blocks	Read multiple blocks
25H	Select	Enter into select state
26H	Reset to ready	Enter into ready state
27H	Write AFI	Write AFI into eeprom
28H	Lock AFI	Lock AFI area
29H	Write DSFID	Write dsfid into eeprom
2AH	Lock DSFID	Lock DSFID area
2BH	Get_System_info	Get system information
2CH	Get_M_Blk_Sec_St	Get multiple block security status
NXP only		
A0H	Inventory Read	Can read data during inventory command
A1H	Fast Inventory Read	Speed is double
A2H	Set EAS	Set EAS bit
A3H	Reset EAS	Reset EAS bit
A4H	Lock EAS	Lock EAS bit
A5H	EAS Alarm	Read EAS sequence

Tab.2. Supported command of the designed reader

B. Anti-forgery

Two ways can be used to realize anti-forgery function, one is to search the anti-forgery system using the unique ID in the RFID tag, the other is to execute EAS command. There are total four EAS commands including set EAS, reset EAS, lock EAS and EAS alarm. The EAS commands are shown in Table 2.

EAS is short for Electronic Article Surveillance, with its help retail industry can avoid goods from forgery. To use it, developer first must make sure that the tag itself must support EAS function; second, write EAS bit through set EAS command, lock EAS bit through lock EAS command; third, place the tag on your goods in terms of special package. If you want to check the product whether it is forgery or not, you just use reader to send EAS alarm command and check the EAS sequence, if

the sequence is OK then the product is good and vice versa. The steps are shown in Fig. 3.

EAS sequence is shown below, starting with the least significant bit which is transmitted first:

```

11110100 11001101 01000110 00001110 10101011 11100101 00001001 11111110
00010111 10001101 00000001 00011100 01001011 10000001 10010010 01101110
01000001 01011011 01011001 01100001 11110110 11110101 11010001 00001101
10001111 00111001 10001011 01001000 10100101 01001110 11101100 11110111

```

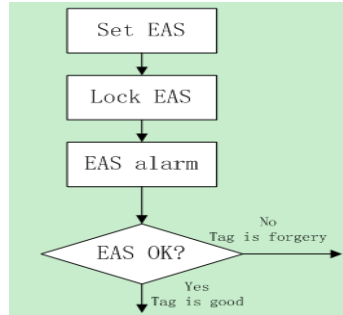


Fig.3. EAS command flow

C. Anticollision

Once the reader and tag is ready, the first thing we should do is to recognize a tag, if there exists several tags in the reader's field at the same time, the reader should find all of them, then anticollision method is introduced.

There are several collision detection methods, such as bit oriented anticollision method (ISO/IEC 14443-A), random slot number anticollision method (ISO/IEC 14443-B), 16 slots number anticollision method (ISO/IEC 15693) [7], when tags in the field increase, the latter method becomes excellent, in this paper, anticollision method based on ISO/IEC 15693 is analyzed and developed.

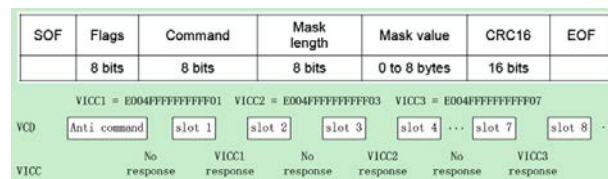


Fig.4. example anticollision flow of ISO/IEC 15693

Fig. 4 shows the example anticollision process flow. After anti command is sent, slot number (4-bit) begins to increase from 0 to 15. The mask value is padded with 4-bit slot number and compare itself with equal length of VICC's UID, if matched then the related VICC will response with its UID, if not then no response is return. In this way, tags in the field will be identified. From the example flow, we can find out that VICC1 response in slot 1, VICC2 in slot 3, and VICC3 in slot 7. The following pseudo algorithm illustrates the above flow and includes post processes such as EAS and stay quiet. If there are hundreds of tags in the field, the 16 loops can be executed more than once until all of the tags are found.

```

Initial();           //activate electromagnetic field
Send_antcollision(); // search tag in the field
for (i =0; i < 16; i++)
slot_number = slot_number + 1
if (response OK)
save_UID();         //save received UID
eas_alarm();        //send EAS command
send_stay_quiet();  //make the tag to be quiet

```

Antenna Design

Since the passive characteristic of the tag, all of the energy needed for the operation is provided by the reader and is transferred through antenna, an excellent antenna generate strong power supply

and the valid work distance is long. According to ISO/IEC 15693 protocol, the basic work frequency is 13.56MHZ, and the electromagnetic coupling antenna should be used. The antenna can be wound using coil, the coil is composed of inductance L, capacitance C and resistance R. There are two main parameters which decide the performance of the antenna: Q factor and resonant frequency, both of them have close relationship with electromagnetic field. The magnetic field strength H can be expressed as formula 4:

$$H = \frac{INab}{4\pi\sqrt{(\frac{a}{2})^2+(\frac{b}{2})^2+x^2}} \left[\frac{1}{(\frac{a}{2})^2+x^2} + \frac{1}{(\frac{b}{2})^2+x^2} \right] \quad (4)$$

Suppose the antenna is Rectangular, N is the number of windings, I is generated current, a and b are the length and width of the antenna, x is the distance, thus H has strong relationship with x when N, a and b are static.

To give a better understand, experiments are done using TCL2 tool of Micropross [8]. Table 3 shows the RFID field test under the condition that the reader's emitting power is at normal level, column 1 stands for the distance x and is ranging from 0 to 10cm, column 2, 3 and 4 stand for three groups of tested field and column 4 is the average field. Fig. 5 depicts the relationship between magnetic field H and distance x. As we can seen from the results that the field strength is shrinking fast as the distance increasing, at the distance of 10cm, the field is about 0.26A/m and the tag still works since the minimum field is 0.15A/m.

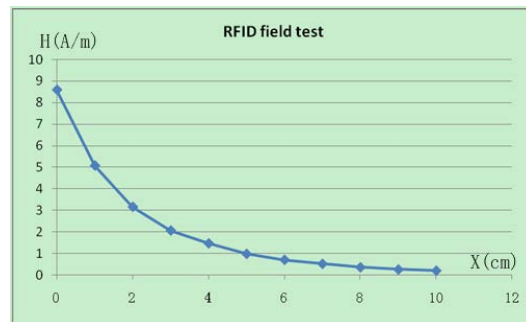


Fig.5. Relationship between RFID magnetic field H and distance x

Distance (cm)	Field 1 (A/m)	Field 2 (A/m)	Field 3 (A/m)	Average (A/m)
0	8.475	8.617	8.662	8.584667
1	4.874	5.205	5.15	5.076333
2	3.054	3.45	2.983	3.162333
3	2.018	2.104	2.076	2.066
4	1.487	1.455	1.473	1.471667
5	0.919	0.966	1.066	0.983667
6	0.686	0.719	0.72	0.708333
7	0.515	0.482	0.562	0.519667
8	0.379	0.354	0.348	0.360333
9	0.259	0.264	0.257	0.26
10	0.205	0.21	0.202	0.205667

Tab.3. RFID field test

To design a suitable antenna for 13.56MHZ RFID reader and tag, it is important to match the resonant frequency which can be calculated through the equation of formula 5:

$$1/2\pi\sqrt{LC} \quad (5)$$

Here L is the inductance of antenna, and C is the total capacitance of antenna and chip, for NXP's ICODE product [9], its chip's input capacitance is about 23.5pf, suppose L is known, then it is easy to figure out the resonant frequency. To measure the exact value of resonant frequency, TCL2 tool is also used, as shown in Fig. 6, Fig. 7, Fig. 8, the measured RFID reader's resonant frequency is about 12.94MHZ and 13.1MHZ for the tag.

The other important characteristic is Q factor which can be adjusted by changing the value of L2, R2 and C2 of the antenna, as shown in Fig. 9, here R2 is the resistance of the tag's antenna, RL is the load resistor of the tag chip, C2 is the total capacitance which is the sum of parasitic capacitance Cp and parallel capacitor C2'. The larger Q value makes the longer read and write distance, yet Q cannot be increased any more when it has reached a certain value because the valid bandwidth is decreased, that will make the tag unstable and generate blind spot. As shown in Fig. 7 and Fig. 8, the tested results show that, the Q value of RFID reader is about 71.6 and 131 for RFID tag.



Fig.6. TCL2 test tool for Q factor and resonant frequency

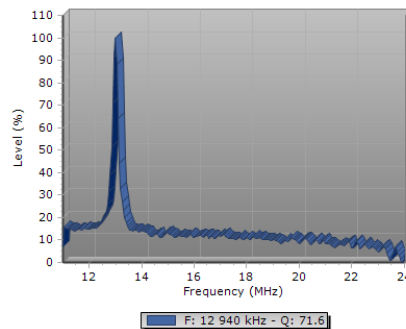


Fig.7. reader's antenna test: Q value and resonance frequency

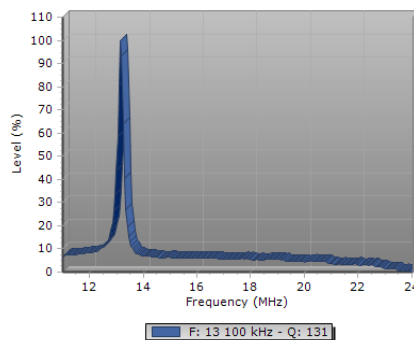


Fig.8. tag's antenna test: Q value and resonance frequency

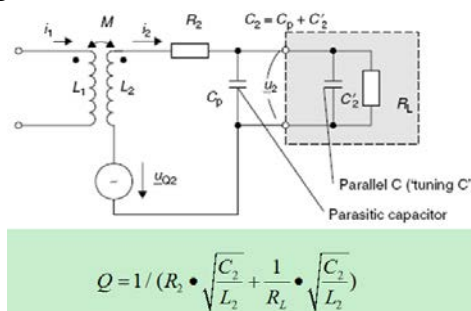


Fig.9. equivalent circuit for the interface of reader and tag, and the formula of Q factor

Conclusions

This paper introduces a system design for the applications of food forgery prevention and traceability using ISO/IEC 15693 protocol. First, a basic system is constructed which includes five levels; second, cost analysis is done and selects a suitable RFID system for the designed purpose; third, hardware design method is given at the aspect of anti-forgery function, anticollision function and antenna design. Compare to other systems like barcode or UHF, our system has a low cost characteristic while the performance and security are remain high. Such system has good performance and has a lot of successful applications in some company of China, for example, wine or cigarette forgery prevention and so on.

References

- [1] K. Finkenzeller: RFID handbook: Fundamentals and Applications in Contactless Smart Cards and Identification (Second Edition), John Wiley & Sons, pp. 162, 2003.
- [2] S. T. Hsieh: RFID medical information system: A system implementation on MSP430 platform, 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), XianNing, pp. 1 – 4, 2011.
- [3] Z. Y. Ma: An ISO15693 based Entrance Access Control System: Design, Implement and Key Issues, 2011 International Conference on Electronics, Communications and Control (ICECC), Zhejiang, pp. 153 – 157, 2011.
- [4] F. H. Huang. Design and Application of Quality Traceability System Based on RFID Technology for Red Jujubes. IFIP Advances in Information and Communication Technology, v 368 AICT, n PART 1, pp. 371-380, 2012.
- [5] W. Z. Cao. General framework for animal food safety traceability using GS1 and RFID. IFIP Advances in Information and Communication Technology, v 317, pp. 297-304, 2010.
- [6] D. Lee. RFID-based traceability in the supply chain. Industrial Management and Data Systems, 108(6), pp. 713-725, 2008.
- [7] INTERNATIONAL STANDARD: Identification cards — Contactless integrated circuit(s) cards — Vicinity cards Part 3: Anticollision and transmission protocol.
- [8] TCL2 information on <http://www.micropross.com/product-91-MP300-TCL2.html>.
- [9] Philips Semiconductors. I•CODE SLI Smart Label IC SL2 ICS20 Functional Specification, Revision 3.1, 2005.