# Improve the Performance of Traceability System by Using a Digital Certificate Enabled Anti-counterfeit QR-Code Mechanism

Yu-Tso Chen and Ching-Chung Chen

***Abstract*—The issues of solving food safety problems have attached great importance for years. The application of traceability system especially those invites ICT technologies plays a critical role of providing considerable solutions. However, the ICT-supported traceability system may still have problems for example the recorded data is incomplete, the traceability information is tampered, so that affects the practical performance of product traceability. This paper proposes a novel Anti-counterfeit QR-Code (AQRC) mechanism capable of delivering the functionality of integrity and non-repudiation for traceability system through adopting information security schemes including digital certificate and digital signature. The contribution of the proposed AQRC mechanism is to improve the performance of product traceability operations; meanwhile, it also indicates a valuable research direction of inviting information security concepts to solving product traceability problems.**

***Index Terms*—Anti-counterfeit, information security, QR-code, traceability system.**

## I. Introduction

Food safety is a critical social and economic issue that emphasizes global attention for years. Food safety problems are frequently happened in a variety of types, such as original products were mixed with inferior ingredient, products were substituted with low-priced fake products, and so on. The roles involved in the whole production and marketing process including producer, jobber, salesperson, and consumer are all worried about whether they have fallen into the food safety related troubles. Therefore, in recent years, a large number of researchers have interested in studies aiming at the solutions potential to the improvement of traceability for food production and marketing. Through using the appropriate approach, it is expected to enables the quality evaluation, control, and guarantee for produced food as well as the semi-finished product and raw materials.

The behavior of counterfeiting the food (including the semi-finished product and raw materials) seriously threatens the economic development and the health of people. The counterfeited food mostly causes the contamination of the food, foodborne diseases, food mixed with inferior materials and food fraud. In fact, such problems are reported daily on the world, like the fake bottled water and artificial plastic rice in China, counterfeit Smirnoff vodka in Europe, mislabeled seafood in the U.S., and so on [1]. Via analyzing the reports, it shows that the problem of food-counterfeiting is not in connection with high-priced food products, but also the cheaper ones. In order to comprehensively prevent the human health against the threats of counterfeit food, how to realize the product traceability in an easy-access fashion for general public is a challenge.

To realize the operation of product traceability, not only for food traceability, in a systematic manner has attached great importance by academic and industrial circles. In theory, with the support of information and communications technology (ICT), the information related to product ingredients, the process of production and marketing can be efficiently converged for people to identify the status, check the validation and verify the performance of the product they concerned. Meanwhile, a systematic traceability approach can easily record all the necessary data that will be useful for figuring out the responsibility if any kind of argues is arisen.

However in practice, there are some sort of technical problems to be solved. Especially, the functionality of information security is lack considered in most of existed traceability systems so that the reliability of the traceability system is a predicament that will directly affect its applications. Two associated problems are as follows.

### A. The Traceability Record of the Product is Tampered without the protection of information security technology

No matter the traditional paper-based labels or the ICT-based electronic ones like RFID (Radio Frequency Identification) tags, the production and marketing information of the product can be modified and hardly exposed.

### B. The poor Efficiency and Effectiveness in Accessing Traceability Information

Although consumers and manufacturers can readily access product traceability information through reading QR-codes or surfing websites providing product traceability services, these approaches are limited for the users to verify the integrity of the received information. In case of the traceability information is tampered or lost, the process of product tracing and tracking is therefore invalid. Since the traceability is invalid, the conscienceless merchandise will easily shirk their responsibility.

Based on the above, this paper proposes a novel product

Manuscript received January 31, 2017; revised May 1, 2017. This work was supported in part by Lien-Ho Foundation, Taiwan R.O.C., under the grants 106-NUU-TC-01.

The authors are with the Department of Information Management, National United University, Miaoli, 36003 Taiwan (e-mail: yutso.chen@nuu.edu.tw, swtyuo56322p@gmail.com).

doi: 10.18178/ijssh.2017.7.8.885

traceability mechanism on the strength of QR-Code and information security functionality including digital certificate, digital signature, and etc. The proposed digital certificate supported QR-Code, called Anti-counterfeit QR-Code, is able to solve the mentioned problems and thus improve the performance of product traceability operations.

## II. Literature Review

### A. Traceability System

In recent years, many investigations aiming at product traceability particularly for the issues of food safety were announced. The traceability defined as a functional activity to trace, track and retrieve information is often implemented as a record-keeping system. In addition, a traceability system can also achieve the need of object identification.

The purpose of traceability applications is not only for the government and companies to win the trust of customers, but also beneficial to realize the complete food safety. In general, the use of RFID is a considerable means of designing a traceability system. Aung and Chang [2] proposed a RFID based traceability system enabling to systematically recording the information of production and distribution. The users can access their proposed traceability system through RFID devices or bar codes to obtain the detailed information of products and make the purchase assured.

### B. Traceability for Food Production and Marketing

The general definition of food traceability is to record the necessary information about food from production, processing, transportation, warehousing to retailing. How to make the customers accessing the information conveniently and efficiently like QR-Code is a practical issue worthy of studying. A QR-Code is a two-dimensional barcode containing the information about the attached object. It efficiently saves the data by following four standardized encoding modes including numeric, alphanumeric, byte/binary and kanji. As a machine-readable optical label, a QR-Code can let the user easily access the data through using an intelligent device like tablet, smartphone, and etc. Tarjan et al. [3] presented a concept of applying QR-Code into a traceability system. With embedding a QR-Code on the product, consumers could rapidly and easily get the relevant information of the product instead of remotely accessing data from the database on Internet. In addition, Qian et al. [4] suggested that, a QR-Code featured in its high capacity and low cost provides a better means of identifying the different packages of food. Besides, a QR-Code could be scanned and used within a short time; i.e., high-speed access, it could be applied not only in getting information on site but also in accessing the remote database to get more detailed data by surfing QR-Code coded URL.

### C. The Anti-counterfeit Approach

In general, the purpose of labeling or embedding the associated information with the distributing products is to avoid or reduce the threat of buying the compromised or fake products; however, it will fail if the information is tampered. In order to overcome such problem, an anti-counterfeit mechanism would be a good alternative.

A variety of studies aiming at the design and performance evaluation in terms of anti-counterfeit techniques have been presented. Xu and Zhao [5] designed a two-factor product anti-counterfeiting management system for secure tracking. The concern they stated is that it is too hard to guarantee the products which have ever been replaced only relying on the support of RFID. Their proposed system enables a two-factor anti-counterfeiting authentication mechanism by combining RFID and two-dimensional bar code technology to strengthen the performance of anti-counterfeiting.

Furthermore, Narimanova [6] introduced an anti-counterfeit consumer product authentication system in conjunction with a QR-Code checking method enabling integrity and authenticity by Narimanova [7]. With using the QR-Code for product, it makes the authentication operation of the system becomes quite simple, low-cost and convenient for consumer use. Such authentication technique could be applied for protecting the private data of the products against the risks of counterfeiting and fake products.

### D. Summary

The reviewed literatures address the following ideas related to designing a better traceability system.

1) A labeling system like RFID, QR-Code is a good way for the users to easily access the required data.
2) The ICT technology can provide a complete process covering all the functions for all the stakeholders in operating product traceability related works online or offline.
3) The counterfeit is a key feature to enhance the usability and reliability of a traceability system. The realization of counterfeit can be implemented by information security approaches like digital certificate, digital signature, and the like.

## III. Design of the AQRC Approach

In this section, a novel Anti-counterfeit QR-Code (AQRC) approach is presented. The AQRC is designed on the basis of the QR-Code generation algorithm in conjunction with digital signature operation with accessing the keys encapsulated in the digital certificate. In considering the size of the generated codes for different applications, the AQRC approach could be performed in two operation types, as depicted in Figure 1. The main difference between these two types is whether the generated AQRC code contains digital certificate or not; i.e., Type-1 contains the necessary digital certificate, but Type-2 not. Instead of attaching the necessary digital certificate, Type-2 assumes that the digital certificate is accessible by a Certificate Management Center on Internet. The symbol definition and the details of the Type-1 and Type-2 operation are introduced respectively as the follows.

### A. The Definition of the Symbols

| *Symbol* | *Definition* |
|---|---|
| $Cert_a$ | The digital certificate owned by participate A. An A is a commercialized company or an individual. The certificate is issued by the government. |
| $T_a$ | The information composed by A to be transmitted |

| | |
|---|---|
| | and used for product traceability. |
| $DS_a$ | The digital signature generated by $T_a$. The $DS_a$ is made by using standard digital signature algorithm. |
| $T_a$’ | The data corresponding to $T_a$. It should be checked and verified according to the digital signature approach. |
| $DS_a$’ | The data corresponding to $DS_a$. It should be used in verifying the $T_a$’ in the digital signature operation. |
| $K_{Ra}$ | The private key of A |
| $K_{Ua}$ | The public key of A. |

### B. *The Operation of Type-1*

*Sender side:*

Step 1. To calculate the hash value of $T_a$, Hash($T_a$).

Step 2. To compose the $DS_a$ from Hash($T_a$) through using $K_{Ra}$ and digital signature approach.

Step 3. To cascade the $Cert_a$, $DS_a$, and $T_a$ into a package to be transmitted out.

*Receiver side:*

Step 4. To decompose the received transmission package into $DS_a$’, $T_a$’ and $Cert_a$’.

Step 5. To get the $K_{ua}$ from the $Cetr_a$’.

Step 6. To calculate the hash value of $T_a$’, H’=Hash($T_a$’).

Step 7. To compute the H from the $DS_a$’ from using $K_{Ua}$ and digital signature approach.

Step 8. To verify the integrity of the content $T_a$’ by comparing H’ and H. Only when H’ equals to H, the $T_a$’ is equal to $T_a$; means the information for traceability check, the $T_a$’, isn’t been tampered.

### C. *The Operation of Type-2*

*Sender side:*

Step 1. To calculate the hash value of $T_a$, Hash($T_a$).

Step 2. To compose the $DS_a$ from Hash($T_a$) through using $K_{Ra}$ and digital signature approach.

Step 3. To cascade the $DS_a$, and $T_a$ into a package to be transmitted out.

*Receiver side:*

Step 4. To decompose the received transmission package into $DS_a$’, $T_a$’.

Step 5. To get the $K_{ua}$ from the $Cetr_a$’ stored on the Certificate Management Center.

Step 6. To calculate the hash value of $T_a$’, H’=Hash($T_a$’).

Step 7. To compute the H from the $DS_a$’ from using $K_{Ua}$ and digital signature approach.

Step 8. To verify the integrity of the content $T_a$’ by comparing H’ and H. Only when H’ equals to H, the $T_a$’ is equal to $T_a$; means the information for traceability check, the $T_a$’, isn’t been tampered.

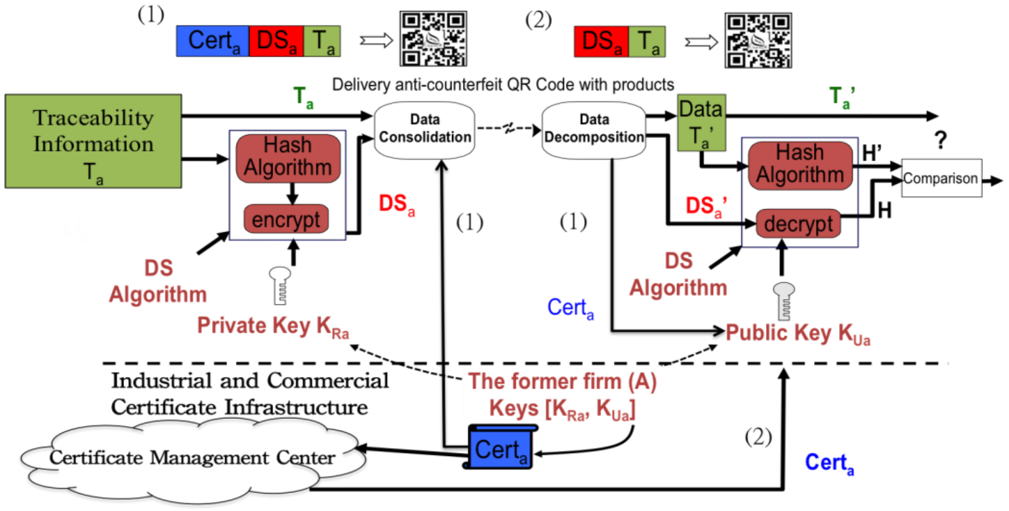

Fig. 1. The AQRC operation with using digital certificate and digital signature functions.

## IV. SYSTEM PRACTICE

### A. *Development Tools and Techniques*

Software:

- Microsoft Windows 7
- MySQL
- Java JDK7.0
- Android SDK(Software Development Kit)

Hardware:

- Server Host: NAS
- Label Printer: EPSON LW-600P
- Barcode Reader: QuickScan QD2430

Techniques:

- Asymmetric encryption/decryption function
- Hash function
- Digital Signature function
- Functions for accessing digital certificate

### B. *System Demonstration*

The operations of the AQRC system respectively for producer, jobber, and consumer are demonstrated in Figure 2. Also, the steps of the operations are detailed as follows.

Producer side:

Step 1. Producer uses the system to generate food traceability by entering the food information of production.

Step 2. With the AQRC approach, the system automatically generates an anti-counterfeit QR-Code.

Step 3. Producer prints QR-Code through the system.

Step 4. Producer pastes the QR-Code on the packaged food product.

Step 5. After checking the relationship between food product and QR-Code is correct, producer can ship the product out.

Jobber side:

Step 1. After getting the product, jobber uses the scanner to scan out the data of QR-Code.

Step 2. With the system, jobber uses the public key of the former manufacturer got from QR-Code or Industrial and Commercial Certificate Cloud Platform to verify the integrity of food traceability data.

Step 3. If the verification result is true, the system will show the traceability information and the jobber could increase the new data into system. If the verification result is false, system would show the warning message, then the jobber could find out the problem with system and look for the manufacturer to clarify the responsibility.

Step 4. After increasing the new data, the system would update the traceability and generate a new anti-counterfeit QR-Code.

Step 5. Jobber prints QR-Code through the system.

Step 6. Jobber pastes the QR-Code in sequence on the packaged food product.

Step 7. After checking the relationship between food product and QR-Code is correct, jobber can ship the product out.

Consumer side:

Step 1. After getting the product, Consumer uses the application to scan out the data of QR-Code.

Step 2. With the system, Consumer uses the public key of the former manufacturer got from QR-Code or Industrial and Commercial Certificate Cloud Platform to verify the integrity of food traceability data

Step 3. If the verification result is true, the system will show the traceability information so that the consumer could realize the relevant information of food product. If the verification result is false, system would show the warning message, then the consumer could decide to quit the purchase or communicate with the manufacturer.

During the transportation process, if the content of QR-Code has been modified, through using the AQRC approach, the system will alert the QR-Code receiver to the problem of product. A consumer catch the warning with App could quit the purchase or notify the manufacturer to trace the origin of problem. A manufacturer catch the warning with system could trace the authenticity of product with the last manufacturer, since the data of QR-Code has the integrity and non-repudiation.

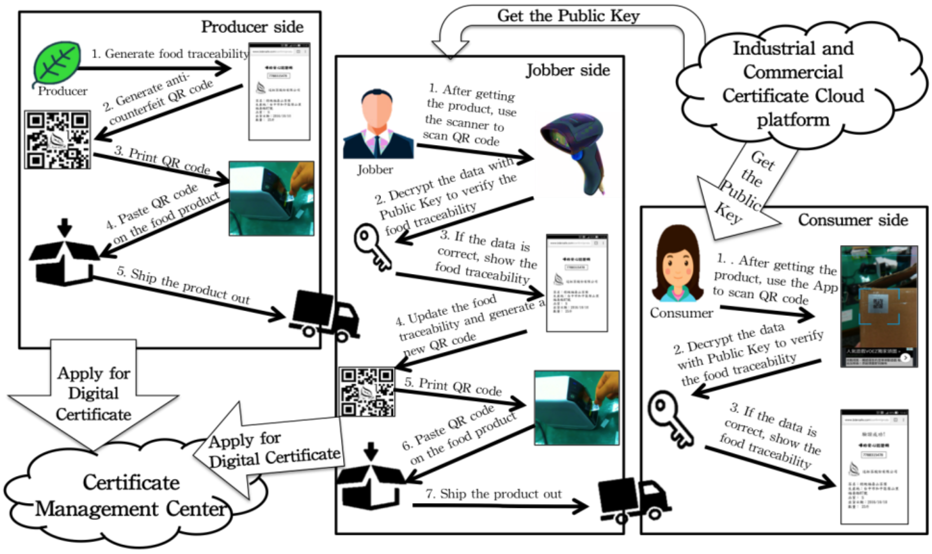
Producer side
Producer
1. Generate food traceability
2. Generate anti-counterfeit QR code
3. Print QR code
4. Paste QR code on the food product
5. Ship the product out
Apply for Digital Certificate
Certificate Management Center
Apply for Digital Certificate
Get the Public Key
Jobber side
Jobber
1. After getting the product, use the scanner to scan QR code
2. Decrypt the data with Public Key to verify the food traceability
3. If the data is correct, show the food traceability
4. Update the food traceability and generate a new QR code
5. Print QR code
6. Paste QR code on the food product
7. Ship the product out
Industrial and Commercial Certificate Cloud platform
Get the Public Key
Consumer side
Consumer
1. . After getting the product, use the App to scan QR code
2. Decrypt the data with Public Key to verify the food traceability
3. If the data is correct, show the food traceability

Fig. 2. A demonstrated AQRC system going through the operations respectively on producer, jobber, and consumer sides.

## V. Discussions

### A. The Pros and Cons of Combining Digital Certificate with the Food Traceability System

Generally, the lack of information security protection for products in transmission may cause the undetected incident of data tampering and face the difficulty in precisely accusing the responsibility on the dishonest manufacturers in the process of tracing. The proposed AQRC supported system leveraging the information security functions provides the features of integrity and non-repudiation to enhance the practical performance for product tracing.

However, there would be more procedures to be done and cause some overhead (may require additional time consuming and works). Moreover, with the government promotion, the active participation of people for tracing the fake and illegal food product, and the assistance of interrelated laws, the proposed system would be more workable.

### B. Food Traceability System Should take the Logistic Process Information into Account

The logistics is certainly a part of product transaction. Without recording the logistics associated data, it is difficult to figure out the responsibility of the participated logistics operators in case of the food safety problems are happened. Furthermore, some splenetic logistics operators may tamper the products in transmission and make invalid tracing to compromise the traceability.

Hence, the traceability system should deal with the relevant data of logistics. Based on such concern, adding the logistics works into the AQRC system would complicate the overall operation process. That is, the logistics operators have to dedicate additional time to operating the AQRC functions for accessing the logistics-associated data. Accordingly, the capacity of the QR-Code has to be raised.

### C. Comparison of Whether the Anti-counterfeit QR-Code Contains the Digital Certificate or Not

In case that the AQRC code has enough capacity to carry the digital certificate data, the user can directly obtain the data from the AQRC code and get the public key to help verifying the integrity of traceability data. In such situation, the users can directly access the digital certificate via the Internet. However in practice, carrying a full-version digital certificate in a QR-Code is a significant burden. For realistically implementing a QR-Code based traceability system, it has to carefully consider whether the storage capacity of the used QR-Code format is enough to save all the necessary data without referring to other data access means.

### D. The pros and Cons of Using QR-Code for Anti-Counterfeiting

The use of QR-Code gains several attractive peculiarities such as low-cost for code generation, simple and convenient operation and relative high capacity for data access. In order to increase the storage capacity to store more data, the size of the QR-Code image should be corresponding enlarged but may be not easily pasted on the pack of the delivering product. In other words, a designed anti-counterfeit QR-Code must contain information security supported codes like digital certificate or public key; it will be certainly to generate a larger or higher resolution QR-Code image. But even a high-resolution printer can make a high-degree QR-Code image; there are still few devices that can scan the high-resolution image correctly.

Moreover, an anti-counterfeit QR-Code wouldn’t work well if it is used on a fake or wrong product. For solving such problem, it is suggested to use a void sticker to produce the disposable AQRC label for one-time use. In case of someone tears off the one-time label, the label's surface would be left the "void" words. Therefore, the AQRC label couldn't be used any more. Besides, during the process of operating the proposed AQRC works, it is suggested to paste all the product-related AQRC image on the correct product in sequence so that could complete the expected performance of product traceability.

## VI. Conclusion and Future Works

This paper introduces a novel digital certificate supported AQRC mechanism capable of improving the performance of traceability system. While using the proposed AQRC system, Type-1 or Type-2, the system users can easily complete the traceability operations just generate, transfer, and scan the AQRC code with using the common QR-Code printer and handheld device like smart phone or tablet computer. With inviting the features of digital signature, an AQRC code containing the information in terms of the manufacturer, the jobber, or even the logistics provider, as well as the traceable production and marketing information is powered with information integrity and non-repudiation. As the result, the product traceability is well-proved through verifying the data in AQRC code is tampered or not.

The contribution of the proposed AQRC mechanism is to demonstrate the potential improvement of product traceability operations; meanwhile, the result of this paper also indicates a valuable research direction of inviting information security concepts to solving product traceability problems. Based on the proposed concept and its system prototype, there are some considerable issues that might merit future researches.

1) To make a real trail on a selected living zone with using the Living Lab approach.
2) How to build an operation model on the basis of the proposed AQRC mechanism?
3) How to realistically evaluate the performance difference between the AQRC supported traceability operation and the traditional one?

## Acknowledgment

The authors thank Hao-Yun Chang, Hsin-Shan Lin, Hsuan-Ting Chang, Yu-Chen Chiang, and Yun-Ju Hsu, for their comments and suggestions for this work.

## References

[1] S. A. Kronenberg. Food fraud – More emerging risks. [Online]. Available: https://foodlawblog.com/tag/fake-food/

[2] M. M. Aung and Y. S. Chang, “Traceability in a food supply chain: Safety and quality perspectives,” *Food control,* vol. 39, pp. 172-184, 2014.

[3] L. Tarjan, I. Šenk, S. Tegeltija, S. Stankovski, and G. Ostojic, “A readability analysis for QR code application in a traceability system,” *Computers and Electronics in Agriculture*, vol. 109, pp. 1-11, 2014.

[4] J. P. Qian, X. T. Yang, X. M. Wu, L. Zhao, B. L. Fan, and B. Xing, “A traceability system incorporating 2D barcode and RFID technology for wheat flour mills,” *Computers and Electronics in Agriculture*, vol. 89, pp. 76-85, 2012.

[5] W. Xu and X. Zhao, “A two-factor product anti-counterfeiting and secure tracing management system based on RFID and two-dimensional bar code,” *Applied Mechanics and Materials*, vol. 469, pp. 490-493, Nov 2013.

[6] O. V. Narimanova, “Development of anti-counterfeit consumer product authentication system,” *Праці Одеського політехнічного університету, Вип*., vol. 2, no. 46, 2015.

[7] O. V. Narimanova, “Authenticity and integrity verification of QR-code,” in *Proc. X International Scientific Conference “Military Education: Present and Future*, p. 63, 2014.

**Yu-Tso Chen** received his Ph.D. degree from Institute of Information Management, National Chiao-Tung University, Taiwan, in 2004 and his M.S. degree from Department of Information Management, National Yunlin University of Science and Technology, Taiwan in 1998. He was a researcher of Industrial Technology Research Institute, Taiwan from 2004 to 2009. He is now an assistant professor with the Department of Information Management, National United University, Taiwan. His research interests include internet of things (IoT), information security, ICT-enabled service innovation, as well as industrial technology foresight and strategy management.

**Ching-Chung Chen** is an undergraduate student of the Department of Information Management, National United University, Taiwan. His research interests include information system analysis and design, object Oriented programming, internet of things (IoT), and big data.