ENABLING SECURED TRACEABILITY OF FISHERY PRODUCTS USING 2D CODE AND DIGITAL ENCRYPTION

Sadayoshi Mikami, Future University - Hakodate, s_mikami@fun.ac.jp
Yuta Takahashi, Mayumi Yoshikawa, Akira Nagano (Future University – Hakodate), Shinji Kuwabara (NJPC Co.), Hideto Narumi (NDC Co.), and Takashi Wakabayashi (AHC Co.)

ABSTRACT

Technologies that enable traceability for fishery products are increasing their demands. Recently proposed technologies are mainly based on disposal RF(IC) tags which are able to record information directly onto them. However, the current systems based on RF tags have problems of expensive price of tags, and weakness of reading information if applied onto surface of products containing much water, which prevents to construct practically feasible systems using the RF tags. To provide a traceability system that uses much inexpensive media and that assures as high security as the RF tags, we propose a system based on a combination of printed 2D codes and internet connection, with security control similar to on-line electronic transactions. The proposed system identifies a fishery product by giving it a unique serial ID, which is issued by a database server, and printed in 2D code onto a paper or a plastic plate, which is directly put on the product. All the trace information sent from client (producer, transporters, and retailer) via internet is associated to the ID and stored to the server. Since 2D code is able to be read by such as mobile phones with built-in camera, a consumer is able to get history of the product with a single scanning operation. For the weakness of printed codes against duplication by copying, we propose a method to identify its validity by digital encryption, along with identification by weight information. The system is assured its usability by a series of experiments conducted for the distribution of cultured flounder in Hakodate, Japan.

Keywords: Traceability; Brand Fish; 2D Code; Mobile Phone; Falsification

INTRODUCTION

The demand for the safety of foods is world-widely increasing in recent years [TRACEFISH 2004]. However, in Japan, the situation around the issue is a bit complicated. The problem is not only of the safety of foods itself, such as illegal uses of chemicals or concealing of diseases, but also of the forgery of foods and its production areas. In 2002, BSE infected cows were found in Japan and the government had taken immediate action of buying all the domestic beefs to burn away. But some food traders abuse the measure, and forged cheap imported beefs as a domestic ones, to get much higher payments. In fishery industry in Japan, the problem of such a kind of forgery seems to be much common. In retailers, there seem some cases where use-by dates are illegally rewritten for expired fish. In brokers, cheap imported shellfish or fish are sometimes forged as domestic brand shellfish or fish. To protect fishery producers and consumers from forgery, it is an urgent request to establish a fishery traceability system, that not only stores products information but also protects against illegal copies and falsification, while providing these information directly to consumers.

To this end, we propose an internet-based secured traceability system which uses a printed 2 dimensional code (extended barcode) as a tag [Takahashi 2004]. One of our aims is constructing cheap and open source based system. The cost of realising IT based system is sometimes extremely high if the system uses technology that is not in common yet today. The cost issue is essential for the system to be wide spread as one of infrastructures. Technologically, a secured traceability system can be easily made by using RF tags (radio-frequency IC tags). Since an RF tag has its own serial ID number in production phase, it is therefore strong enough against duplication. But there are some problems of using RF tags on fishery products:

1. It is very costly technology. A cheapest RF tag still costs more than half a dollar. Also RF readers are not so common. There seems three or more years that the tag's price drops down to 1 cent and the readers will wide spread.
2. Safeness of the tag as to be applied onto food (fish) itself is a bit concerned. In cases of live fish distribution, the tag might be applied onto the surface of the fish. Since the tag contains silicone and metal, its concern is that the part of the tag might be mixed into fish meat.
3. Some radio frequencies used in the tag is absorbed by water. Therefore, a fishery product which contains much water may sometimes cause inability to readout.

For the alternative method, we decide to use paper-printed code technology, such as barcodes [ISO 2000]. The printed codes are easily duplicated by photocopy. But, if there is a description (phrase) in a code which exactly corresponds to one product such as a weight of that, the label containing the code is exactly for the product itself. In this case, it is impossible to be used for another product (fish). But it the description is easily writable by others, there will be duplication for the tag by changing only the descriptions corresponding to each forged product. To this end, we encrypt the product-identification (such as fish weight) information by using public-key encryption method. In this case, since the others do not know the secret key for encryption, any unauthorised person can not rewrite the tag [Burnett 2001].

Standard barcodes does not have enough capacity for this method. Recent years, extensions of barcodes, known as 2-dimensional codes, are proposed [Denso-wave 2004]. One good point for these codes is that some kinds of mobile phones with built-in cameras have a function to read the codes. The read information is directly shown to users or used internally in a Java application embedded onto the mobile phone. By using the latter function, we are able to provide a software for consumer to directly read the tag, send the information to the traceability server, validate, and receive information of authorised traceability data.

The following sections describe the detail of the method we constructed.

FISH TRACEABILITY SYSTEM VIA INTERNET

Internet based traceability system

The architecture of the proposed system is shown in **Figure 1**. It is designed to store all information concerning a fish into a remotely situated database server. Each time a new fish is registered, the server generates a unique ID number for the fish, and all the information about the fish will be subsequently associated to the number. The first registration is actually done by a client software for fishery produces written in Java, which runs on a PC connected to internet. The data flow is as follows:

1. After a fish being caught by a fisherman, the information of the fish, including its production area and the weight, is input into a client PC that runs the Java codes. Through internet connection, it requests to register the fish in the database server. The server then generates the unique ID, which have enough digits to cover the expected amount of the target fish in market.
2. The client Java software receives the ID number and the encrypted weight digits, which was generated by the server using a secret key stored there.
3. The software generates an image of the 2D code (QR-code) for the ID and the encrypted digits.
4. A paper or a plastic label printer connected on the client PC prints out the 2D code onto a paper/plastic tag.

5. It is put on a fish or a container of the fish. In live fish case, the plastic tag may be directly put on the body of the fish by a plastic string injected by needle gun.

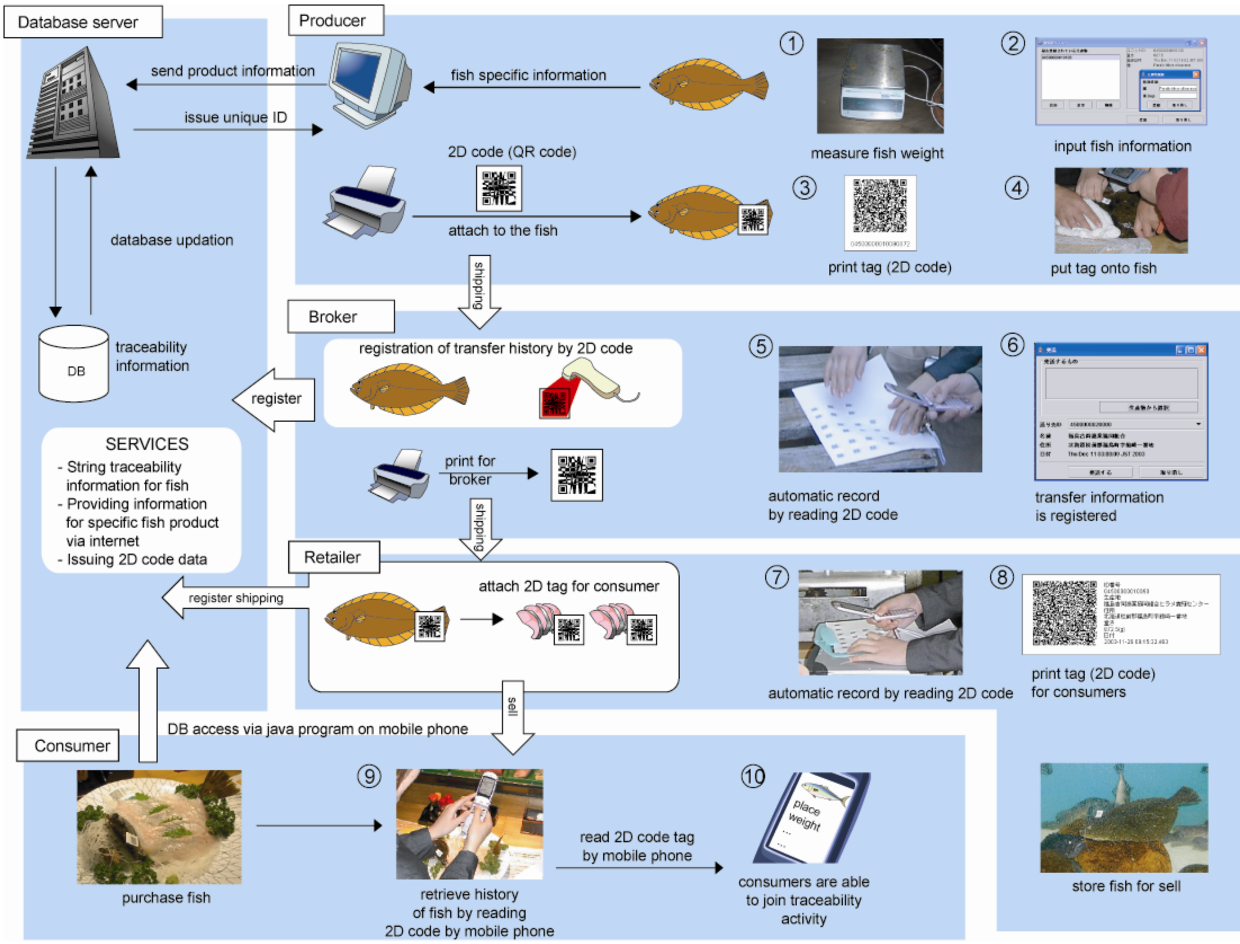

Figure 1. Proposed traceability system using 2D code.

Storing traceability information by 2D code

The history of the fish distribution will be recorded by using the 2D code onto the tag. For a broker and a retailer, a client PC with 2D code scanner is used. Alternatively it is possible to use a mobile phone that runs embedded Java and that has 2D code reading facility. In either case, the Java software for broker/retailer is used. The data flow is as follows:

1. A broker receiving the fish will read the 2D code tag by using 2D scanner connected to the PC.
2. The PC sends the code to the database server. The server checks validity of the code, and records transit information such as date, time, and the name of the broker.
3. Similarly, a retailer receiving the fish reads the codes on the fish by using the scanner on a PC.
4. The PC also sends the code to the database server, and the server registers transit information while validating the code.

After traceability information is stored, a consumer who buys the fish may be able to read the tag and access to the database server to check the validity and the traceability information. This is done by not only a PC with scanner but also a mobile phone having the specs described above.

Consumer-readable tag

As a mobile-phone readable code, we used ‘QR-code’. QR-code is an ISO standard 2 dimensional code, which is readable from any directions. **Figure 2** shows an example of the code used in our experimental traceability system. There are some other characteristics feasible to be used as fishery traceability:

1. The code area is small enough to be used with a very long (typically more than 100 alphabetical characters) ID number and the extra digits for security information.
2. It is strong against dirt and scratch. In fishery usage, dirt and scratch are very common. Especially, if we apply tags onto live fish, these damages are unavoidable. But, in our pre-experiment, the code, printed onto a plastic tag by thermal printer and put on a live flatfish, was still readable after two months in a fish-tank.

ID番号
04500000010090
生産地
福島吉岡漁業協同組合ヒラメ養殖センター
住所
北海道松前郡福島町字館崎一番地
重さ
872.5(g)
日付
2003-11-26 09:15:32.463

Figure 2. An example of a 2D code tag. This tag is designed so that basic information can be read directly by the code and the detail information is retrieved via internet connection by a java application on a mobile phone. Digitally encrypted weight information is included in this tag.

Many mobile phones sold in Japan have a facility to download and run a small Java application, which is called such as an embedded Java, or ‘i-appli’. The application can access to built-in hardware. In many mobile phones, including 505IS series by NTT-Docomo companies, it is possible for Java application to read QR codes. Also the application can send information via internet.

Combining these functions, we made a Java software for consumers which reads the QR code on fish, send the information to the database servers to validate and draw traceability information. The software then receives traceability information in html format, which is shown to consumer by the mobile phone’s built-in web browser.

This technology allows direct connection between consumers and traceability information. In another word, a consumer is able to ‘join’ a traceability activity by using their mobile phones. This provides quite an important effect over the reliability of fishery products; a consumer is able to get precise knowledge about the fishery product and will put a good price for the products worth buying, which fosters producers to provide more reliable and high quality fishery products.

Securely printed codes by using digital signature method

A potential problem against authorisation of a 'paper printed tag' is an easy duplication by photocopy. It is therefore necessary to maintain one-to-one correspondence between a tag and a fishery product. Our idea is to use a specific value intrinsic to a product as an identification number. At the moment, we use the weight of a fish, since it is one of the easily measured values which individually vary. Also we apply a mechanism that any unauthorised person can not generate the value. The method is called a 'digital signature,' which is originally used to protect copyright of digital pictures or validate the genuineness of a file or a software.

The idea of digital signature is based on a public-key digital encryption method. In public key method, there are two sets of 'keys' – a fixed length digits – one is called a 'secret key' and the other a 'public key'. A sequence of numbers is converted into a different sequence of numbers through an encryption equation with a key. This is called an 'encryption' process. The number sequence converted by using a 'secret key' is 'decoded' to an original sequence of numbers by using a 'public key' which corresponds to the 'secret key'. However, it is impossible to generate the 'encrypted' numbers by using the 'public key'; it is only used for the purpose of decoding. Therefore, a consumer who is given a public key is able to decode the encrypted numbers and observe the intrinsic value, which means that the value is surely converted by the person having the secret key which corresponds to the public key.

By this method, the product-identification information is digitally validated. It should be noted that the database server must securely keep the secret keys.

EXPERIMENTS IN LIVE FISH DISTRIBUTION

To examine the practical usability of the system, we conducted an experiment in an existing live fish distribution. The targeted live fish distribution was for farmed flat fish cultured at Fukushima town in Hokkaido Japan and send to a restaurant in Hakodate city in Japan.

The database server was settled in the computer centre at Future University Hakodate. Since the shipped flat fish is kept in a fish-tank at the restaurant, the QR code is printed out onto a thin water-proof plastic plate by using thermal transfer printer. The tag is put onto a body of flat fish using a nylon string.

Figure 3 shows a flat fish attached a tag and kept in a fish-tank. Actual usage of the system is illustrated in **Figure 1**. **Figure 4** shows a consumer reading a tag by using a mobile phone with camera. Throughout the experiment, we tested to use mobile phones for receipt registration. It was found that the mobile phone based receipt system is still insufficient for practical use. But the system was usable enough for the cases of using 2D code scanners onto a PC. Also it was found that the mobile phone based consumer software worked sufficiently for the purpose of checking traceability information in front of the fishery product.

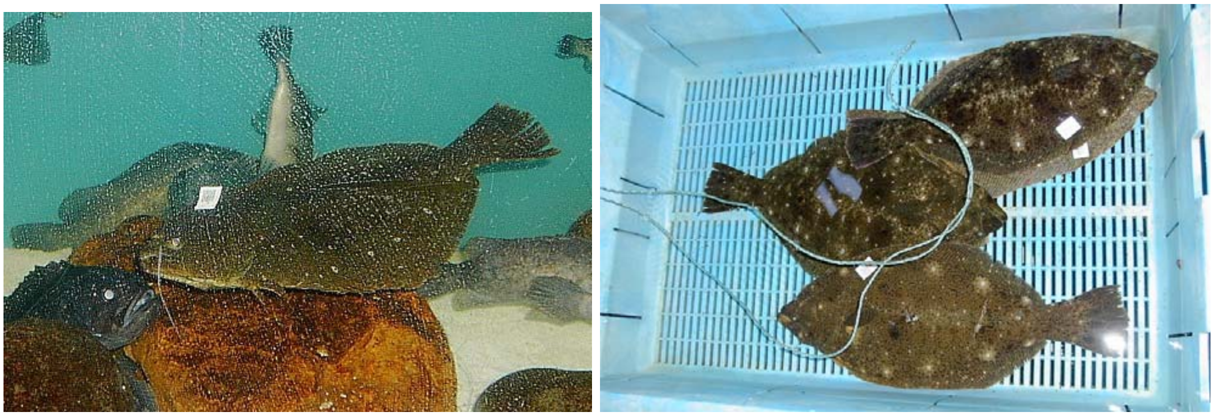

Figure 3. Tagged flatfish in a fish-tank in a retailer.

Figure 4. A consumer reading a tag on a served raw flatfish in a restaurant.

CONCLUSIONS

For secured traceability system with relatively low cost, we proposed a QR code based printed tag system for internet connected PCs and mobile phones with built-in cameras. Through an experiment of live fish, we could conclude that this design is practically usable in Japan. There are still some problems such as authorisation of the central database servers or a treatment of some fishery products that requires complicated distribution such as shellfish. However, the most important point of the system is the involvement of consumers into traceability activity. Therefore, even though there still needs some further years to camera enhanced mobile phones available in common in world-wide, we believe that this kind of system with consumer-readable interface should be important.

REFERENCES

TRACEFISH Project, 2004, *http://www.tracefish.org/*.

ISO catalogue of International Standards, 2000, *Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code*, ISO/IEC 18004:2000.

Denso-wave QR code site, 2004, *http://www.denso-wave.com/qrcode/index-e.html*.

Steve Burnett, Stephen Paine, 2001, *RSA Security's Official Guide to Cryptography*, McGraw-Hill.

Yuta Takahashi, Mayumi Yoshikawa, Sadayoshi Mikami, et al., 2004, *Reliable Fishery Traceability System Using 2D Code and Digital Signature*, Proceedings of Hokkaido Information Processing Symposium 2004, pp. 46-50 (in Japanese).

ACKNOWLEDGMENTS

The authors would like to thank The Japanese Institute of Technology of Fishing Ports, Grounds, and Communities for the financial support of this research.