A Two-factor Authentication System using Radio Frequency Identification and Watermarking Technology

S.L. Ting*, Albert H.C. Tsang

Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong

*Corresponding author. Tel.: +852-2766-6613; fax: +852-2774-9308.

Email address: jacky.ting@polyu.edu.hk

Address: Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hum, Hong Kong, China

Keywords: Anti-counterfeiting, Counterfeit, Product Authentication, Radio Frequency Identification (RFID), Watermarking

Abstract
Counterfeiting has been growing at an alarming rate worldwide. The increasing number of counterfeit products has penetrated into various industries, especially the luxury goods industry. Numerous anti-counterfeit and product authentication technologies are available to combat this problem. At present, the verification principle in product authentication mainly relies on optical detection and security feature identification which require human experts or machines to determine the product's genuineness. As a result, the current approach to product authentication presents formidable challenges to customers in determining the product's authenticity. Attempted to address the challenges, this paper proposes a Watermark-RFID based Self-validation System (WARDS) that provides a self-validation and two-factor authentication approach through integration of Radio Frequency Identification (RFID) and watermark technology by means of a mobile platform. The system architecture and a framework for development of WARDS are presented. Critical issues at different stages of constructing WARDS in organizations are identified. Furthermore, the capability, benefits and advantages of using the proposed system in combating counterfeiting problems are illustrated in the findings of a trial implementation presented in this paper.

Keywords: Anti-counterfeiting, Counterfeit, Product Authentication, Radio Frequency Identification (RFID), Watermarking

1. Introduction

Counterfeiting has grown at an alarming rate in recent years, making it a serious threat to economies around the world [1-3]. It was estimated that counterfeit goods accounted for 5-7% of the world trade in 2006, totaling US$600 billion annually. Annual revenues of such goods have increased by more than 100 folds in the past two decades [4]. The counterfeiting problem has significant negative economic and social impact on governments, consumers and businesses [5]. Moreover, it threatens the economies of developed and developing countries alike, undermines trading relations, scares off vital new investment, and increasingly endangers public health and safety [6].

The increasing number of counterfeit product is penetrating into various industries, such as electrical equipment, pharmaceuticals, wallets, handbags, etc. The high price of luxury goods offers illicit actors opportunities to reap high profits; counterfeits make up about 10 per cent of the luxury goods trade [7]. The counterfeiting problem in luxury goods industry is getting more serious, especially commodities of handbags and wallets which experienced about 100% increase in counterfeit activity in 2007-08 [8]. The consumption of counterfeit luxury goods is a worldwide phenomenon and it does not seem to slow down in the foreseeable future.

In order to combat the counterfeit problems, numerous anti-counterfeit and product authentication technologies are currently available in the market, such as direct authentication, security labeling and security printing [9-10]. However, the verification principles of these product authentication technologies mainly rely on optical detection and security feature identification which require human experts or machines to determine the product's genuineness, creating formidable challenges to customers in determining the product's authenticity themselves. There is a lack of product authentication approaches that provide customers with responsive and cost-efficient practical applications for self-authentication [11-12].

Radio Frequency Identification (RFID) technology is recently recognized as a promising vehicle to combat counterfeiting by its advanced automatic technology, ability of cryptographic resistance against cloning and its strong security features [13]. In the current RFID-based product authentication approaches, RFID tag is generally attached to a product's package or stuck onto the product. However, there is a problem that the authentication system can be tricked if the tag of a genuine product is stolen and attached to a counterfeit product, it will then be recognized as genuine product, but not counterfeit any more [14]. Also, if tag is applied to the package, but not directly attached to the product, it only ensures that the tag and the packaging are staying together, but it cannot ensure the product inside has not been changed.

With a view to addressing the deficiency of current RFID-based product authentication approaches, this paper introduces a two-factor product authentication system that allows customers to validate a product's authenticity under the ubiquitous communication environment by using their mobile devices. A case study will be presented to illustrate the feasibility and procedures of implementing the proposed system. In the following sections, the features and limitations of current product authentication technologies will be discussed. The workflow and system architecture of the proposed approach will then be explained in detail. At the end of this paper, performance evaluation of the proposed approach will be presented.

2. Literature Review

2.1 Current State of the Global Counterfeiting Problem

Product counterfeiting refers to unauthorized production of articles which copy certain characteristics of genuine goods, and claiming that these articles are the registered products. It has developed into a severe threat to consumers and brand owners alike [6]. The problem of counterfeiting is getting more and more serious worldwide, it becomes one of the world's fastest growing crimes. It has a negative impact on the economic growth of countries, trading relations, investment intentions in new projects, as well as public health and safety [4]. Also, counterfeiting has destroyed 120,000 jobs each year in the United States, and 100,000 jobs in Europe over the past ten years [15]. As stated in a study [16], companies may suffer from counterfeits in: (a) loss of revenue directly; (b) damage to the company's reputation; (c) reduced effort and investment on marketing, research and development; (d) increased liability claims relating to defective counterfeit products; and (e) more competitors in future as illicit actors will acquire the skills and knowledge of producing the product in the process of counterfeiting, and develop into enterprises that produce products of their own design and brands eventually.

2.2 Current Status of Counterfeiting Problem in Luxury Goods Industry

In recent years, counterfeiting has grown at an alarming rate in various industries, such as electrical and electronic goods, pharmaceuticals, headwear, sunglasses, cigarettes, and handbags [9]. It is found that the top three commodities in counterfeiting seizures are footwear, handbags/wallets and pharmaceuticals; counterfeit products in these categories mainly imitate the brand in luxury goods industry [17]. Counterfeited luxury goods consumption is a worldwide phenomenon and it does not seem to slow down in the foreseeable future. The counterfeiting problem has a negative impact on the protection of intellectual property rights; it also causes large number of job losses in countries like Italy, France and Switzerland [18]. While both low- and high-quality counterfeits can be found in today's counterfeit market, high quality fakes are perceived to be a more serious long term problem because customers are more easily displeased when tricked into thinking that they are buying a genuine product, and the brand owner's revenues are more directly affected.

2.3 Anti-counterfeiting Approaches used in Luxury Goods Industry

With the aim of accurately identifying counterfeit products, product authentication systems are developed. Since different authentication methods have different characteristics, an overview of their principles, benefits and limitations are discussed below.

2.3.1 Direct Authentication

Direct authentication is based on a product's innate feature. The exploitation of a natural product property distinguishes direct authentication from all other authentication approaches, as the latter are based on an artificial feature that is added to a product with the purpose of enabling authentication [19]. The product properties that can be used for authentication purposes are very diverse, and according to a study [20], they include:

- Physical properties (e.g. density, weight)
- Chemical properties (e.g. chemical properties, ingredients, composition)
- Visual properties, either on characteristics measured on a microscopic level or the general appearance of a product (e.g. the surface structure of a product)

In luxury goods industry, the direct authentication is widely used in product validation. It is because most of the goods in this industry have high quality, detailed specifications, and bear with an artificial security features. The goods with certain characteristics are suitable for direct authentication, such as diamonds, gems, jewellery and leather goods. However, it is challenging for customers to acquire the professional knowledge for product authentication. Even if the customers are willing to learn, manufacturers and brand owners might be reluctant to release detail information on how to identify genuine products to the public. It is because such information is highly confidential which may also be used by counterfeiters to improve the quality of fakes. Most importantly, it is time-consuming and costly to send the suspicious product to an expert and wait for a conclusive answer [19].

2.3.2 Authentication by Means of Security Feature

There are two kinds of security feature, including overt and covert technologies in security feature authentication. In luxury goods industry, overt technologies are quite commonly added to the packing, labels, or product. The common technologies are micro engravings, holograms, printing with infrared ink, and so on [11]. Since overt features are visible to naked eyes, they can be duplicated by counterfeiters easily. In contrast, covert features are invisible to naked eyes. Thus, they are not made public that can prevent counterfeiters from duplicating. However, it requires special devices to read these features.

2.3.3 Verification of Unique Identifiers

There are three main types of unique identifiers, including serial number, random number and codes. They are guaranteed to be unique, and given to set of objects with unique identification feature for specific purpose [21]. The unique identifiers can help to detect counterfeit products and grey market activities by verifying the identifiers and supply chain analysis. It is a cost-effective way to combat counterfeit trade [22]. Luxury goods, like handbags and watches, commonly use serial numbers for product authentication purposes. By checking the validity and consistency of the unique identifier with the numbering scheme, counterfeit products can be detected by brand owners.

All these existing product authentication approaches have common characteristics which are difficult to replicate and provide effective product identification. Table 1 summarizes the characteristics of these three main product authentication approaches. In order to provide an even higher level of product authentication measures, Tuyls and Batina [13] claimed that RFID technology is a promising tool to combat counterfeiting due to its advanced automatic technology, ability of cryptographic resistance against cloning and its strong security feature.

2.4 Radio Frequency Identification (RFID) and Its Applications in Anti-Counterfeiting

In today's market, most anti-counterfeiting technologies require some form of physical examination, such as examining hologram or applying a solution to a chemically coded product. These methods are time consuming when buyers, manufacturers or law enforcement authorities have to check all products rather than a representative sample. Also if a third party mixes counterfeit goods with genuine ones, it may be difficult to undertake a representative sample check to ascertain the authenticity of the goods. In order to perform effective examination on item level, RFID technology has the potential to automate the product authentication process [23-24]. RFID is an advanced automatic identification technology that can acquire data from tags

within certain read range by using radio frequency signals [25]. This technology is a promising vehicle to combat counterfeiting because it performs better than other approaches in various types of product. The following introduces several RFID-based anti-counterfeiting solutions.

2.4.1. Plausibility Checks based on Unique Serial Numbers

Individual items are marked with RFID tag which provides unique serial numbers for them. Marking objects with unique identifiers helps to monitor the flow of goods, and thus to detect illicit trade activities. In the system, the manufacturer generates a random number (ID), writes it to the data carrier (RFID tag) and stores it in a database. When the product is checked, a reader retrieves the ID from the tag and sends it to an application offered by the manufacturer, which looks up the number in the database. If the number is found to be valid, it can be interpreted as evidence that the product is authenticated.

2.4.2 Plausibility Checks based on Track and Trace

In a track-and-trace system, each product is embedded with an RFID tag. When the product moves through the supply chain, each node in the supply chain updates the product pedigree information to a central repository [38]. Thus, the central database contains real time information on the trail of exchange of a product, which includes the origin, destination, timestamp, and company names of each transaction. This way, a product can be tracked and traced with a complete product pedigree when it moves from the manufacturer to retailers. By reviewing the recorded information, the product's authenticity can be determined. Track and Trace is an important and promising technology to avert counterfeiting [13].

2.4.3 Benefits and Limitations of Using RFID in Anti-counterfeiting

In general, RFID brings the following benefits in the process of combating counterfeits:

- Provides accurate and detailed information that enhances item level traceability throughout supply chains and store networks
- Improves stock accuracy to avoid costly discrepancies
- Improves product restocking efficiencies and visibility
- Provides instant notification about incidents
- Strengthens brand protection
- Provides real time information of product movement

However, in the above mentioned RFID-based product authentication approaches [12, 24, 26-28], RFID tag is generally attached to the product packages or stuck onto the product itself to serve as a security measure for product genuineness determination. In these approaches, the authentication measure is moved from the product itself to the information carried and stored in the RFID tag. However, such authentication system can be tricked if a tag from a genuine product is planted to a counterfeit one, the product will then be recognized as genuine, but not a counterfeit one any more [14].

Although RFID is a promising technology in combating counterfeiting, it still has weaknesses as a security measure. Therefore, other technologies are considered to integrate with RFID technology to form a more powerful product authentication solution. One such solution incorporates a watermarked image in the product label [29]. This is particularly useful for luxury goods each item of which is typically attached with a brand label. It is believed that digital

watermark technology can protect the tag from being cloned by malicious parties, thereby enhancing the authentication measure. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove [30]. This technology makes imperceptible changes in the luminance of a selected area of an image which is undetectable by humans, but can be read by a machine. This design approach is a "two-factor authentication" mechanism as it requires users to match the information stored in the RFID tag with that retrieved from the watermark on the product label.

A Watermark-RFID based Self-Validation System (WARDS) is designed to implement the above mentioned "two-factor authentication" mechanism as a solution to address the challenges encountered in the current product authentication measures. So far, WARDS is the first attempt to incorporate features in the product label (in form of hidden watermarked images) in a self-served product authentication solution. The design theory [39] is followed in the development of this solution:

1. Purpose and scope

The purpose is to develop a solution that will address the challenges of combating counterfeiting of luxury goods, that is more cost effective than the currently available solutions from the perspectives of consumers and retailers. It will cover the processes of product authentication and product registration.

2. Constructs

Examples of constructs in WARDS include product items, information on the relationship of a product's unique label number and its extractable product feature, encoding and decoding schema.

3. Principles of form and function

A self-validation and two-factor authentication system architecture (with an encryption and decryption mechanism) is adopted to verify a product's genuineness. The product's identification number and the information embedded in the watermark obtained from a scan of the product label are matched with the corresponding information retrieved from a central database for unique identification of individual units of products (See Section 3).

4. Artifact mutability

The scheme for embedding information in the watermark may need to be refined after learning from results of trial runs with a prototype of WARDS, to make it more robust in real-use environments.

5. Testable propositions

The security level achieved and workflow of WARDS are determined from results of a case study for comparison with performance of the traditional approach (See Section 5).

6. Justificatory knowledge (kernel theories)

The approach proposed is synthesized from a number of security feature authentication approaches and technologies.

7. Principles of implementation

A prototype has been developed for conducting proof-of-concept trials of the proposed methodology for product authenticate and registration.

8. Expository instantiation

An example of employing WARDS in action is provided through a case study.

3. System Architecture of Watermark-RFID based Self-Validation System (WARDS)

The architecture of the Watermark-RFID based Self-Validation System (WARDS) is illustrated in Figure 1. It consists of four tiers, namely Presentation Tier, Communication Tier, Application Tier, and Information Supporting Tier. The philosophy behind this breakdown is to separate the major activities of system applications into logical sections of display, processing logic and data services. Translation of tasks and results is managed by the Presentation Tier and Communication Tier, evaluation of real-time product authentication handled by the Application Tier, and storage and retrieval of information are performed by the Information Supporting Tier.

3.1 Presentation Tier

The Presentation Tier represents the devices or media for user to access the system. It converts and displays application data into a human-legible form. The main users of this system are customers who can employ mobile devices with the RFID reader and camera function, like mobile phones or Personal Digital Assistant (PDA), to verify a product by retrieving information stored in its RFID tag and its digital watermarked label. If the customers do not have such mobile devices, they can also employ a Kiosk in the shop to perform the same validation. Through a secure connection with the Communication Tier, clients can enquire the system and obtain information such as authentication results, product information, registration record, etc. Once an enquiry is conducted, the authentication logic and algorithm will be processed in the Application Tier, so that the captured data can be sent to and displayed on the mobile device or Kiosk through the Internet.

3.2 Communication Tiers

The Communication Tier acts as a bridge between the Presentation Tier and the Application Tier. With the use of wired connection such as Local Area Network (LAN), or wireless connection like Wi-Fi, 3G and General Packet Radio Service (GPRS), a secure connection will be established. They facilitate communications between clients' requests in the Presentation Tier and data transmission in the Information Supporting Tier. When a user queries the product information, the related data will be communicated through wireless network with mobile devices or wired connection with Kiosks.

3.3 Application Tier

Two systems, namely Product Authentication System and Product Registration System, are designed in this tier.

3.3.1 Product Authentication System

There are two layers in this system: one for Product Encoding and the other for Genuineness Authentication. This system performs the product authenticity checking function. To perform product authentication, the system needs to obtain the unique identification code, Electronic

Product Code (EPC), stored in the RFID tag and the embedded data from watermarked image for data matching. After getting both data, the system will start to query a related database in the Information Supporting Tier to check the extracted data. The EPC acquired from the tag will be compared with the data extracted from the watermarked image, and then further information such as registration record will also be checked. If data extracted from the watermarked image matches that embedded in the RFID tag, and the product has not been registered, it will then be determined as genuine. This process enables customers to perform self validation of a product that is attached with an RFID tag and a watermarked label. The following sections will discuss the process of product encoding and data processing in more detail.

3.3.1.1 Product Encoding

This process is designed to provide a numbering system and extractable product feature for unique identification of individual units of products. In other words, it enables a product to be encoded with RFID tag and a digital watermarked label.

In WARDS, each product is attached with an RFID that contains an encrypted unique identification number (i.e. EPC). In order to enhance the authentication mechanism between tag and product, a watermarked label will also be attached to the product. The idea of watermarking is to embed information in the host data by applying minor changes in such a manner that human eyes cannot read the embedded data. The original pattern on the label constitutes the host image, and a product code in the form of a secure message will be embedded on the host image. In order to enhance accuracy and reduce time for detection of the watermark, a fast and robust digital watermarking approach is used to embed and extract the secure message which serves to link the product to its tag with the unique identification number.

Encryption in RFID

It is proposed that the RFID tag will adopt EPCglobal Class-1 Generation-2 standard in order to be compatible across companies and geographical regions [31]. By using 96-bit EPC Tag that consists of four basic data elements: a header, an EPC manager, an object class, and a serial number. Each product unit can have its own unique identification number after registering information into these elements. More details of the unique EPC are provided in Section 3.3.2.

Digital Watermark Embedding and Detection

The proposed watermarking system is a fast and robust digital watermark detection approach for mobile devices with camera function. It has three parts: watermark embedding, attaching and detection functions.

In the beginning, there are input parameters which are k-bit watermark information for the embedding process. The watermark information is then be converted into an n-bit codeword which will enhance its robustness against the server attacks in attacking function, such as perspective transformation caused by the shooting angle, phase distortion due to lens aberration and a slight curvature of the printed material [32]. After generating the codeword, a block pattern in 2D sin curve is formed based on the value of the codeword. Finally, the image with the embedded codeword can be obtained by superimposing the 2D pattern of the watermark on the host image [33].

In order to facilitate the correction of the geometric distortion that may exist in the photograph, a frame is placed around the watermarked image as shown in Figure 2. Using the method proposed by Katayama et al. [33], the corner points of the frame are utilized to determine the transformation caused by rotation, scaling and translation in the image processing operation. This method is highly robust for detection of quadrangles even when the contrast is insufficient, as in the case of a bright image on white paper. The corner points approach makes it possible to detect quadrangles by referring to only a few pixels (typically less than one tenth of the entire captured image), which contributes to faster processing in mobile application [32].

In the authentication process, the embedded image will be captured, and these operations are known as attacking function for the watermarked image. In the watermark detecting process, the watermark information will be extracted from the image. With the help of the frame, the watermarked area can be identified after geometric distortion correction. Then the 2D pattern of the watermark will be detected and then converted into its codeword. As a result, the watermark information can be recognized from the codeword [34].

3.3.1.2 Data Processing from Encoded Product

With the purpose of functioning among different vendor environments, middleware software is designed to translate various reader data formats into a single, normalized format for easier integration. In the proposed system, data is normalized and transformed in eXtensible Markup Language (XML) with the use of middleware. Normalization is the process of turning the data in scanned RFID tags into the same format. And XML is a common information format which can be used on the Internet, Intranets and elsewhere. It is simple and extremely legible. Apart from providing machine readable context information, it can produce meaningful message to human readers.

3.3.2 Product Registration System

In order to prevent unauthenticated products hat may get through illicit channels, all products are to be registered at the company's database after being purchased. In the proposed system, the cashier will register the mobile phone number of the customer after the product is purchased. Customer will then receive a Short Message Service (SMS) that includes a product reference code. With that reference code, the customer can check product information and register the product via a company portal at her convenience.

The product reference code of each product is unique and the pattern of code is standardized. With reference to the EPC schema [36], the product reference code is separated as: header, manager, object class, and serial number. The header identifies the band or manufacturer of the product. The second part is the manager of the code which refers to the shop of selling such product. The third is the object class which represents the type of product. The fourth is the serial number which is unique to the item. Therefore, the product reference code can provide a unique code for every item with a standardized pattern for the identification.

3.4 Information Supporting Tier

The Information Supporting Tier contains the system databases that maintain all the information of the WARDS. All the registered products with unique product reference code and product details such as product brand name, product description, country of origin, etc are recorded in the

database. Also the RFID tag records the transactions of products within the supply chain into the database, all the track and trace information including location and time of product move from one supply chain participant to another. A 96-bit EPC is generated and assigned to a genuine product once the product is produced, the database will store all such information and the related transactions will continue to be updated until the product is purchased by a customer. When the user enquires product information, the product authentication tier will be able to get the related information from the database. This Information Supporting Tier acts as an information repository of the system.

4. Implementation of WARDS

In order to verify the performance of the proposed system, a trial implementation of WARDS is conducted. An eight-phase development framework for implementation of the WARDS is adopted. The significance and issues to be addressed in each phase are explained in the following parts.

4.1 Business Process Analysis

This phase is a preparation stage of the whole development. In order to facilitate the implementation process of the new system, it is better to review and analyze the current processes used by the organization [35]. The analysis mainly focuses on the existing anti-counterfeit approach and the workflow across different departments. It helps one to understand the existing business process, and such information is useful for identifying existing weaknesses that need improvement. Since the overall system design is established before development, the business process analysis helps the designer to customize WARDS to different companies, so that it will match the needs and situation. Then, a scope is identified to serve as a boundary of the project, and a goal is determined for target setting. It aims to control the project to proceed in the right direction and produce the desired deliverables.

4.2 System Accessories Selection

After getting a general picture of a company, it is critical to choose the most appropriate technology, experts and vendors to perform the development. By selecting the right facilities and technologies, work can be done effectively and efficiently. It not only lessens the interruption and disturbance that the implementation may cause to the daily operations, but also enhances the satisfaction of the user organization. In this study, the technology and tools used in various components is shown in Table 2.

4.3 Content Selection

Since a structured and unique identification code is generated for each product in WARDS, product information can be recorded in the attached RFID tag. The system database stores the basic product information such as the product name, product code, country of origin, etc, and it also records the product movements in the supply chain of the logistics network. In order to present the useful product information to customers effectively, it is better to have good content management. In WARDS, only the related information will be displayed in the user interface. For example, basic product information, validation result and registration record are shown rather than the product movement records along the supply chain which may be difficult to understand by customers. Moreover, providing clear user guidelines, consistent outlook and good classification in the display pages which let the system becomes more user-friendly.

4.4 System Design

Nowadays, the verification principle in product authentication mainly relies on optical detection and security feature identification which require human experts or machines to determine the product's genuineness. However, both methods in product authentication present formidable challenges to customers in determining the product's authenticity themselves. Therefore, this system is designed for self-validation, based on the two-factor authentication with RFID and watermark technology that enables customers to verify the products through a mobile device or Kiosk. By using WARDS, customers can perform a self-validation in product authentication instead of relying on retailers.

This system consists of 2 functions, namely, Product Authentication Function and Product Registration Function, to provide customers with a reliable product authentication solution and higher product information transparency.

4.4.1 Product Authentication Function

This product authentication function provides customers with a convenient and reliable way to distinguish counterfeits from genuine products. Every product is attached with an RFID tag and a watermark embedded label, the RFID tag is embedded with an EPC number which is unique to each individual product item. Customers can verify a product's authenticity by scanning the tag and uploading an image of the label with an RFID embedded mobile device or a Kiosk. Results will then be displayed to customer instantly to show if the product is a genuine, counterfeit or registered product (Figure 3). If the result is shown as "Unauthenticated" or "Already Registered", it represents the product may be counterfeit or come from an unofficial channel. Customers need to contact their seller or brand owner immediately. If result is shown as "Authenticated", it means that the product is genuine.

4.4.2 Product Registration Function

In order to prevent unauthenticated product from illegal channel, all products are highly recommended to be registered after being purchased. In WARDS, the cashier will record down the mobile phone number of customer after the product is purchased. The customer will then receive an SMS included with a product reference code. With that reference code, customers can check product information and register the product conveniently via a company portal. If it is the first time registration, the customer will be asked to enter some basic personal information and purchase record to finish the registration process. Only the product information will be shown after the product registration (Figure 4).

4.5 System Integration

After the development of the system components, system integration is the essential to be undertaken. It designs to connect the individual or existing systems together, and ensure system can be operation before the actual deployment

Before having the system integration, it is better to indicate the existing data and system, such as the product information database, product encoding system, product registration system, etc. And company can overview the connection between system components generally, and consider an appropriate data flow will be generated after the integration.

Moreover, it is recommended to take the pilot approach in system integration, and combine every two parts together each time and test their performance. If the system can demonstrate the desired functions and acceptable results, it will then be integrated with other parts. It is aimed at averting generating a sudden flood of bugs which are hard to define their source of errors.

4.6 Pilot Test

In order to build a cost-effective and practical anti-counterfeiting solution in a realistic environment, a pilot test is important to evaluate the performance of the proposed system. It helps to identify bottlenecks in a system, estimate the performance tuning effort and collect data to help stakeholders make informed decisions related to the overall quality of the proposed system.

In the pilot test, there is a scenario designed for WARDS to evaluate its performance in product authentication and registration. In the scenario, the total time spent on the entire process of WARDS and that of the current product authentication and registration will be measured. By comparing the total process time and steps on two approaches, the improvement in verifying product authenticity and registration process after adoption of WARDS can be measured.

So far, there are three fundamental approaches to product authentication, namely direct authentication, incorporating security features into product, and plausibility checks of track and trace data. The technologies applied in WARDS belong to the approach of incorporating security features, it is better to compare with the product authentication approach in the same category.

In this pilot test, barcode labeling is chosen as the current product authentication approach. It is because barcode labeling is a commonly used as a security feature in product authentication. By scanning the bar code attached to the product, a corresponding unique number will be returned. The unique number can be mapped to database, thus providing product information and tracking records.

4.7 System Establishment

After the pilot test, all the errors and bugs were fixed, the system is ready to be released as an application program. In order to implement the system successfully, user training is recommended to be provided. During the training session, the company can realize the concerns and difficulties of staff and try to modify that. Also, training allows the staff to be more familiar with the operation of the new system which helps to implement the system effectively.

4.8 Maintenance and Performance Review

With the purpose of ensuring the system performs well, a regular maintenance and performance review is required. By conducting visual check on the equipment of the system as well as sample testing of the system‘s functions, it can help to understand and evaluate the system‘s performance. If unusual phenomenon is detected in the system, the technician can carry out a detail check so as to avert sudden break down of the system.

5. Performance Evaluation and Discussion

5.1 Comparative Analysis

Table 3 compares the direct authentication and printed labeling which are the current product authentication approaches in luxury goods industry with WARDS. It shows that WARDS has superior performance in security and applicability aspects.

5.1.1 A More Efficient Product Authentication and Registration Process

Tests had been conducted to compare WARDS with the current product authentication approach in terms of performance in the product authentication and registration process [12]. The trial results are shown in Tables 4 and 5. It is found that WARDSS can significantly simplify the seven-step product authentication process to one with four steps. Most of the manual tasks in barcode labeling (Steps 1 to 4 in Company Side) are eliminated by the automated product authentication function featured in WARDS. The new system takes an average of 112 minutes to complete the product authentication process, which is a mere 17.5% of the average time (642 minutes) needed for the existing approach (642 minutes on average). According to the trial results, WARDS is able to reduce the process time for product registration almost by half (49.2%) when compared to the current approach (see Table 5).

In summary, the total process time for the entire product authentication and registration process can be drastically reduced by 72.8% through implementation of WARDS. Thus, it can be claimed that WARDS is more efficient than the current approach.

5.1.2 A More Effective Approach to Anti-counterfeiting

Security is important in anti-counterfeiting. It aims to protect genuine products from cloning and to keep authorized distribution channels free from counterfeit products. There are two main steps in the process of security, namely, prevention and detection [37]. Prevention can be accomplished by making it difficult to clone products or their means of identification; detection refers to the ability of detecting cloned products. The ways in which WARDS enhances anti-counterfeiting security are summarized below:

- Prevention: (i) Two-factor authentication, and (ii) database makes the connection between the product and its tag
- Detection: (i) Track-and-trace based authenticity check, and (ii) presentation of the registration record on demand by authorized parties via the Internet

5.1.2.1 Higher Level of Security with Two-factor Authentication

Since the authentication system can be tricked if a tag from genuine product is stolen and attached to a counterfeit product, it will then be recognized as genuine product, but not counterfeit any more. Also, if tag is only applied to package but not directly to the product, this binding mechanism only ensure that the tag and the packaging are staying together, but not further ensure the product inside is not changed.

In WARDS, it applies two-factor authentication in the product authentication. This authentication associated with a strong authentication. It is a system with two different factors (i.e. RFID information and watermarked image) in authentication. By using two factors rather than one factor in authentication, it generally gives a higher level of assurance.

In WARDS, RFID technology is integrated with digital watermarking technology, RFID tag and a watermarked label are the two factors in authentication. If one of the technologies is failed in authentication or broken, the other one becomes invalid. The interaction and linking between tag and product increase the security level of product authentication and raise the threshold in terms of costs and expertise for counterfeiters. Moreover, the data between tag and digitally watermarked label are connected together, it increase the blinding between tag and product, and ensures the product cannot be changed even the tag is just attached to the package.

5.1.2.2 Higher Level of Security in Delivering Reference Code for Product Registration

In the current product registration approach, such as barcode labeling, customer needs to find the product code on the package or product, and then register the product via the Internet or telephone. Since the product code is visible on the package or body of the product, it is less secure and can be easily cloned. In WARDS, product reference code is directly given to customer's mobile phone through SMS from the company that ensures the code is only displayed to customer.

5.1.3 High Customer Involvement

The current product authentication approaches, such as the direct authentication and printed labeling, rely on optical detection and security features identification in verification. Therefore, experts and machines are required to examine the inherent features and the label, which becomes a challenge to customers in verifying the product's genuineness themselves.

By applying the RFID and watermark technologies in WARDS, both features can be extractable by machines and convert to meaningful message to human-readable. As a result, customer can highly involve in product authentication. Table 6 compares the characteristics of different product authentication approaches with WARDS in customer involvement issue.

5.1.4 Help Brand Owners Increase Consumer Trust

With the RFID and watermark, consumers can check product authenticity and status such as registration record, also obtain more product information such as product code, product description and country of origin through mobile devices with an RFID reader and camera function, kiosks, or company web portals. This information transparency is an essential prerequisite for enhancing public confidence in the authenticity of the product. Furthermore, the effective product authentication approach and traceability will help brand owners increase consumer trust.

5.2 Industrial Feedback

For the evaluation of WARDS, two anti-counterfeit experts from intellectual property protection agency were interviewed. Those experts mentioned that such automatic identification and tracking system (i.e. RFID-based authentication system) is becoming more important in industry. It is because the counterfeits are constantly increasing in quality, making it more difficult even for experts to determine the genuineness of products. Therefore, the counterfeiters have higher chances of injecting counterfeit products into the licit supply chain. Thus, it will be better to know the complete trail and visualize the product life-cycle of each product in the licit supply chain.

However, they are concerned the customer's handling ways for product during product authentication. As the value of luxury good is high, in order to avoid any damage for the product, the staff will handle it carefully. During the authentication process, the customer may handle it roughly that may harm the products and affect the value. They suggested that some staff is better to support and guide the customer in product authentication. This can ensure the products are handling in good condition.

As mentioned by the experts, almost all luxury brands provide the after-sales services for their customer, including product repair, maintenance, clean, etc. And the company will ensure the product is genuine first before any repair or maintenance. But many people utilize this after-sales service to check the genuineness of their products which are purchased from the second-hand market. This group of people heavily increases the workload of the staff, and consumes more resource in the company. But with the systematic product authentication measure, both interviewed experts think that WARDS can help the customer to verify the authenticity of product; and it may reduce the demand for checking genuineness in the after-sales services.

In summary, WARDS offers an effective solution to address the product authentication and anti-counterfeiting issues. Results of the case study validate feasibility of adopting the proposed approach. The highly effective detection of fakes will deter counterfeiting to a significant extent.

6. Conclusion

Anti-counterfeiting is an important and complicated issue, and become major challenge to luxury goods industry. The proposed system in this paper provides a self-validation and two-factor authentication approaches by integrating the RFID and watermark technology by means of mobile platform. It enables customer self validate product efficiently and effectively. And this report provides a feasible solution to the system architecture and implementation framework.

Compared with the current product authentication methods, WARDS provides a higher level of security, more effective and ease-to-use approach for customer to verify product genuineness via mobile devices. Users can validate the product authenticity or get detail product information anywhere and anytime. Also, the two-factor authentication approach provides adequate association between tag and the product itself, which give a higher level of assurance in product authentication. The finding from the pilot test indicates that the proposed system get a encouraging results in product authentication and registration.

Acknowledgement

The authors would like to express their sincere thanks to the Research Committee of The Hong Kong Polytechnic University for financial support of the research work.

References

[1] T. Staake, F. Thiesse, E. Fleisch, The emergence of counterfeit trade: a literature review, European Journal of Marketing 43 (3/4) (2009), 320-349.
[2] K. Wilcox, H.M. Kim, S. Sen, Why do consumers buy counterfeit luxury brands?, Journal of Marketing Research XLVI (2009), 247-259.
[3] C.S. Gautam, A. Utreja, G.L. Singal, Spurious and counterfeit drugs: a growing industry in the developing world, Postgraduate Medical Journal 85 (1003) (2009), 251-256.

[4] U.S. Department of Health and Human Services, Combating counterfeit drugs, 2004, available at: http://www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf
[5] S. Bastia, Next generation technologies to combat counterfeiting of electronic components, IEEE Transactions on Components and Packaging Technologies 25 (1) (2002), 175-176.
[6] T. Staake, E. Fleisch, Countering counterfeit trade, Springer-Verlag, Berlin, Germany, 2008.
[7] E. Zurich, Problem-analysis report on counterfeiting and illicit trade, SAP Research, Brisbane, 2007.
[8] K. Newmometum, Brand risk: counterfeiting, 2009, available at: http://www.newmo.com/enterprise_risk_management_challenges.html.
[9] ICC Counterfeiting Intelligence Bureau, Countering counterfeiting: A guide to protecting and enforcing intellectual property rights, ICC, United Kingdom, 2005.
[10] D. Hopkins, L.T. Kontnik, M.T. Turnage, Counterfeiting exposed: protecting your brand and customers, Hoboken, N.J., Wiley, 2003.
[11] S.H. Choi, C.H. Poon, An RFID-based anti-counterfeiting system, IAENG International Journal of Computer Science 35 (1) (2008), 1-12.
[12] S.K. Kwok, J.S.L. Ting, A.H.C. Tsang, W.B. Lee, B.C.F. Cheung, Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication, Computers in Industry 61 (7) (2010), 624-635.
[13] P. Tuyls, L. Batina, RFID-tags for anti-counterfeiting, Springer, Berlin, Germany, 2006.
[14] SToP, Description of the status quo of existing technical countermeasures, their benefits and shortcomings, SToP, HSG, New York, 2008.
[15] International Chamber of Commerce Commercial Crime Services, Counterfeiting Intelligence Bureau, 2009, available at: http://www.icc-ccs.org/home/cib.
[16] S. Thorsten, F. Elgar, Countering counterfeit trade: illicit market insights, best-practice strategies, and management toolbox, Springer, Germany, 2008.
[17] U.S.Customs and Border Protection, U.S. Immigration and Customs Enforcement, Fiscal year 2010 seizure statistics –Final report, 2011, available at: http://www.ice.gov/doclib/news/releases/2011/110316washington.pdf.
[18] M. Phan, P. Lu, Counterfeit purchase motivations: A cross-cultural exploratory study, in: Proceedings of the Global Marketing Conference in Shanghai, Yonsei University, Seoul, South Korea, 2008.
[19] M. Lehtonen, J. Al-Kassab, F. Michahelles, O. Kasten, Anti-counterfeiting business case report, BRIDGE Project, 2007.
[20] M. Rieback, B. Crispo, A. Tanenbaum, RFID Guardian: A battery-powered mobile device for RFID privacy management, in: Proceeings of the Austrlasian Conference on Information Security and Privacy (ACISP), 2005.
[21] R. Elz, R. Bush, Serial number arithmetic, Network Working Group, USA, 2006.
[22] D. Johnson, G. Roger, An anti-counterfeiting strategy using numeric tokens, International Journal of Pharmaceutical Medicine 19 (3) (2005), 163-171.
[23] P. Lei, F. Claret-Tournier, C. Chatwin, R. Young, A secure mobile track and trace system for anti-counterfeiting, in: Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, Hong Kong, March 29 – April 1, 2005, pp. 686-689.

[24] T. Staake, F. Thiesse, E. Fleisch, Extending the EPC Network – The potential of RFID in Anti-counterfeiting, in: ACM Symposium on Applied Computing, Santa Fe, New Mexico, 2005.
[25] S. Lahiri, RFID Sourcebook. Upper Saddle River, N.J., Pearson plc 2006.
[26] A. Juels, RFID security and privacy: A research survey. Journal of Selected Areas in Communication (J-SAC) 24 (2) (2006) 381-395.
[27] R. Koh, E. Schuster, I. Chackrabarti, A. Bellman, Securing the pharmaceutical supply chain, in: White Paper, Auto-ID Labs, Massachusetts Institute of Technology, 2003.
[28] S.K. Kwok, S.L. Ting, A.H.C. Tsang, C.F. Cheung, A counterfeit network analyzer based on RFID and EPC, Industrial Management & Data Systems 110 (7) (2010), 1018-1037.
[29] S. Craver, N. Memon, B. Yeo, M.M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks,and implications, IEEE Journal of Selected Areas in Communications 16 (4) (1998), 573-586.
[30] T. Nakamura, A. Katayama, M. Yamamuro, N. Sonehara, Fast watermark detection scheme for camera equipped cellular phone, in: Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia, pp. 101-108.
[31] D.N. Due, J. Park, H. Lee, K. Kim, Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning, in: Proceedings of the 2006 Symposium on Cryptography and Information Security, 2006.
[32] T. Nakamura, A. Katayama, R. Kitahara, K. Nakazawa, A fast and robust digital watermark detection scheme for cellular phones, NTT Technical Review 4 (3) (2006), 57-63.
[33] A. Katayama, T. Nakamura, M. Yamamuro, N. Sonehara, New high-speed frame detection method: Side trace algorithm (STA) for i-appli on cellular phones to detect watermarks, in: Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia, College Park, MD, USA, pp. 109–116. ACM, New York, 2004.
[34] A. Pramila, Watermark synchronization in camera phones and scanning devices, Master's Thesis, Department of Electrical and Information Engineering, University of Oulu, Oulu, Finland, 2007.
[35] A. Basu, A. Kumar, Research commentary: Workflow management issues in e-business, Information System 13 (1) (2002), 1–14.
[36] EPCglobal Inc., EPCglobal Standards Overview, 2009, available at: http://www.epcglobalinc.org/standards.
[37] S.E. Schechter, Quantitatively differentiating system security, in: Proceedings of the First Workshop on Economics and Information Security, May 16-17, 2002.
[38] R.S. Chen, M.A. Tu, Development of an agent-based system for manufacturing control and coordination with ontology and RFID technology, Expert Systems with Applications 36 (4) (2009), 7581-7593.
[39] S. Gregor, D. Jones, The anatomy of a design theory, Journal of the Association for Information Systems 8 (5) (2007), 312-335.

List of Tables

Table 1 Characteristics of three common approaches to product authentication

	Direct Authentication	Security Feature Authentication		Unique Identifiers
		Overt technology	Covert technology	
Operating Principle	Based on a product's inherent feature	Artificial feature that is in or on the product, and on the authenticity of that feature		Based on the numbering scheme assigned
Weaknesses	● Time-consuming ● Costly ● Requires professional knowledge to determine genuineness	● High possibility of replication by others ● Requires professional knowledge to determine genuineness	● Costly ● Requires specialized reading devices	● High possibility of replication by others

Table 2 Technology Adopted in WARDS

Component	**Standard / Brand**	**Description**
RFID Tag	Class 1 (13.56 MHz) Gen 2 Passive Tag	➢ Smaller size, longer life and much lower cost than active tag ➢ Smaller size tag will have less influence on the package design
Air-interface Protocol	EPC Generation2	➢ Able to generate up to 68 billion unique serial numbers for each registered company [25], enabling the adoption of item-level identification ➢ Widely accepted by the world's leading corporations
Antenna	ASA Fixed Reader Antenna Panel 312002	➢ Broadcasts the RF signals generated inside the reader's transmitter into the immediate environment ➢ Supports long distance identification with a large reading volume ➢ Provides sufficient reading volume for cattle walk-through installations
RFID Label Printer	Zebra R4Mplus RFID Smart Label Printer	➢ Support EPC RFID standards ➢ Able to print label with different size and in high speed
RFID Middleware	BEA Middleware	➢ The clear market leader for middleware used in the telecommunications industry ➢ Provide a variety of solutions to

		support business deployment
Computer		➢ Function as system server ➢ Allows high speed access and provides large storage capacity
Networking	Wired and wireless networking	➢ Wireless network allows customers to access the system remotely with their mobile devices ➢ Wired network is used to gain access to the system via a Kiosk
Database Management System	Microsoft SQL Server 2005	➢ Widely used in database management
.NET framework	Microsoft Visual Studio Web Express Edition	➢ A functional development tool that is easy to use and easy to learn ➢ Provides new Web and Windows controls, automated debugging, and a new Visual Basic that simplify .NET and ASP.NET Framework development

Table 3 Comparison between Two Current Product Authentication Approaches and WARDS

	Current Product Authentication Approaches in luxury goods industry		**Proposed System**
	Direct Authentication	**Printed Labeling**	**WARDS**
Principle	Based on product's inherent features	Read the unique number on product visually or by machine	Read the RFID tag and capture the watermark on product
Verification	Customer does not have professional knowledge to determine	Difficult for customers to verify the product's authenticity	Customer can determine product's authenticity easily
Visibility to the naked eye	Yes	Yes	No
Complexity of checking	High	Low	Low
Security criteria			
Clone detection	No	No	Yes
Imitation	Depends on the feature complexity	Easy: Label can be duplicated	Difficult: Chance of successful in decryption of the EPC RFID tag is low
Privacy in product registration	Low Visible on the package or product body, which can be duplicated by counterfeiter	Low The serial number is visible on the package or product body, which can be duplicated by counterfeiter	High: Product reference code given by SMS

Applicability criteria			
Needed expertise to check a product	High	Medium	Low
Customer Involvement	No	No	Yes
Needed equipment to check a product	No	Scanner	An mobile phone with RFID reader and camera function/ kiosk
Value-added Functions	No	No	Yes: Extra product information such as registration recode help making decisions

Table 4 Trial results of WARDS and Barcode Labeling in Product Authentication

Product Authentication Process of WARDS		1st Trial (second)	2nd Trial (second)	3rd Trial (second)
Customer Side				
Step 1	Scan RFID tag by a mobile device	20	33	25
Step 2	Take a snapshot of the label on the product	18	20	21
Step 3	Upload the photo to the application	7	5	5
Company Side				
Step 1	Retrieve information from database and display authentication result on the customer's mobile device	60	60	60
Total Time		106	118	111
Notes: Data given in the above table are obtained from proof-of-concept trials of WARDS. The performance results will differ with volume of service requests.				
Product Authentication Process of current approach (i.e. Barcode labeling)		1st Trial (second)	2nd Trial (second)	3rd Trial (second)
Customer Side				
Step 1	Find the barcode label on the product	73	88	80
Step 2	Call the customer service hotline for checking	16	25	28
Step 3	Waiting for response	188	235	160
Company Side				
Step 1	Receive call from customer	50	48	10
Step 2	Listen to customer requests	183	200	221
Step 3	Check the information from database	17	16	20
Step 4	Interpret the related information and inform the customer accordingly	92	77	100
Total Time		619	689	619

Table 5 Trial results of WARDS and Barcode Labeling in Product Registration

Product Registration Process of WARDS		1st Trial (second)	2nd Trial (second)	3rd Trial (second)
Customer Side				
Step 1	Record the mobile phone number to cashier after purchasing	18	15	20
Step 2	Enter the Product Reference Code in SMS to company websites	4	6	5
Step 3	Fill in the personal information	88	102	92
Company Side				
Step 1	Send SMS to customer	12	15	13
Step 2	Retrieve information from database and display product information	3	3	3
Step 3	Record the information in database	2	2	2
Total Time		127	143	135
Notes: Data given in the above table are obtained from proof-of-concept trials of WARDS. The performance results will differ with volume of service requests				
Product Registration Process of current approach (Barcode labeling)		1st Trial (second)	2nd Trial (second)	3rd Trial (second)
Customer Side				
Step 1	Find the product code on package or product	93	100	88
Step 2	Search the model of product	15	22	20
Step 3	Enter product information to company website	46	40	50
Step 4	Enter personal information	88	102	92
Company Side				
Step 1	Retrieve information from database and display product information	12	12	12
Step 2	Record the information in database	2	2	2
Total Time		256	278	264

Table 6 Comparison between two Current Product Authentication Approaches and WARDS in Customer Involvement

	Direct Authentication	**Printed Labeling**	**WARDS**
Customer Involvement	X	X	✓
Require human expert to check a product	High	Medium	Low

List of Figures

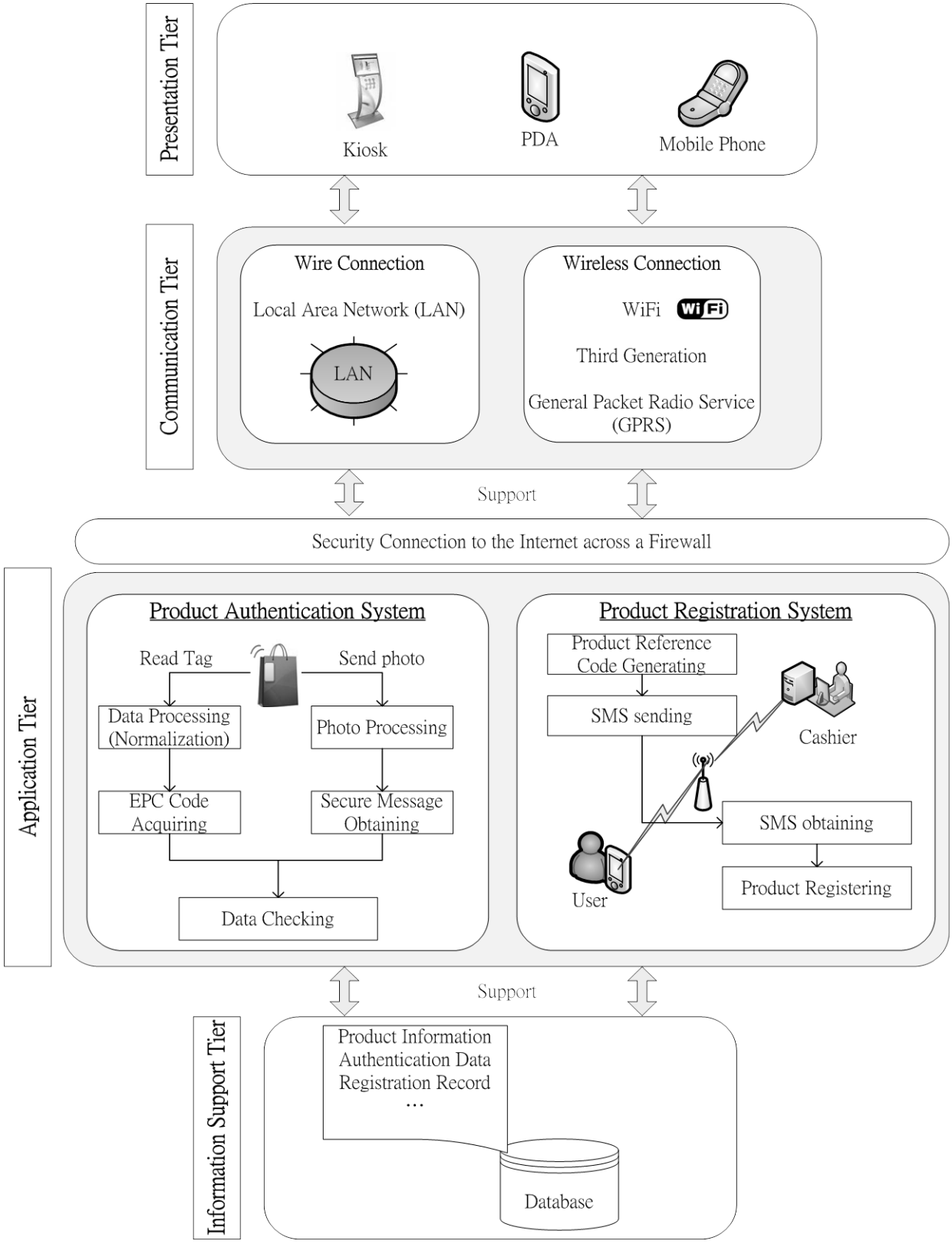

Figure 1 System Architecture of WARDS

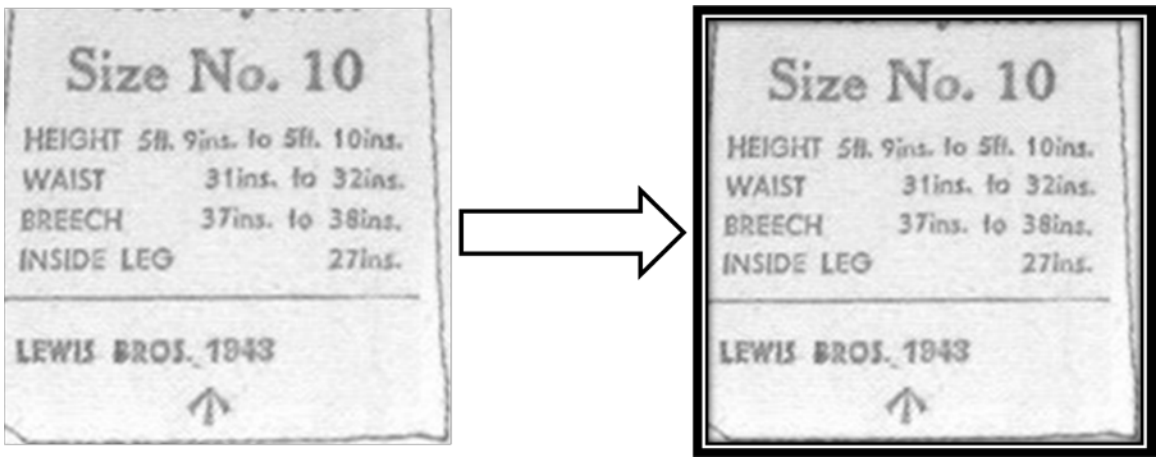

Figure 2 Host Image and Framed Image

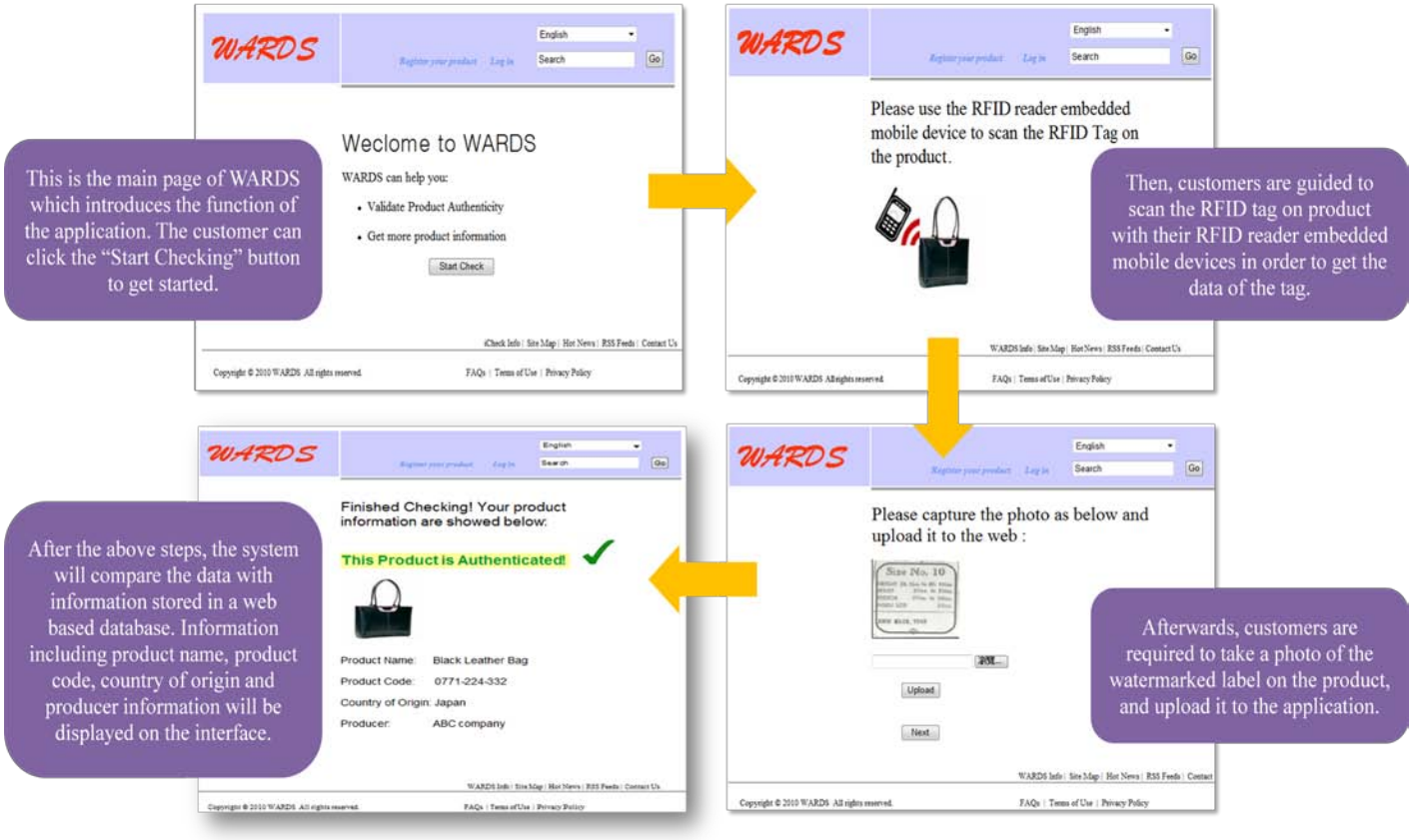

Figure 3 Mechanism of Product Authentication Function

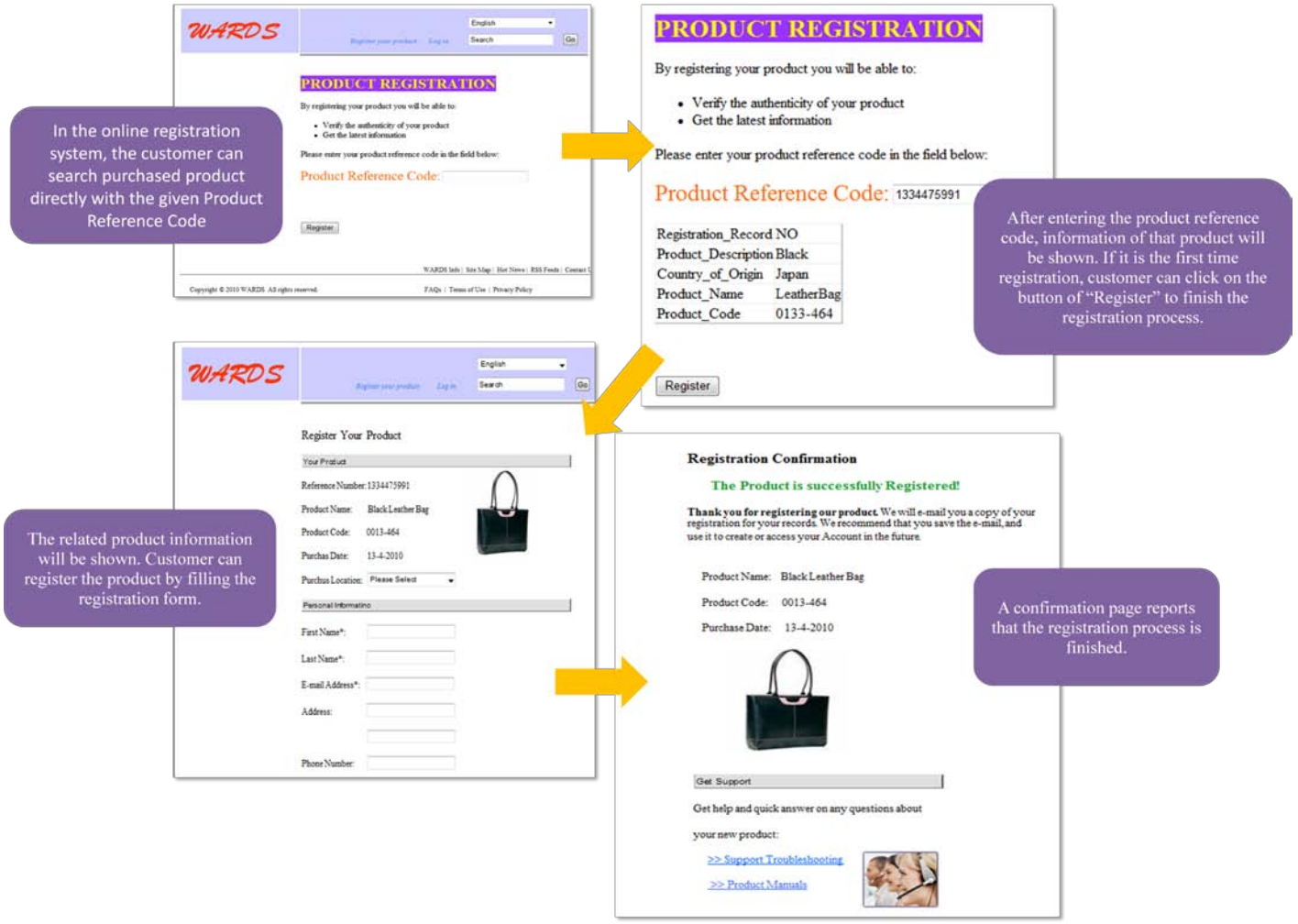

Figure 4 Mechanism of Product Registration System