Computers in Industry 62 (2011) 32–41

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Physimetric identification (Physi-ID)—Applying biometric concept in physical object identification

S.K. Kwok *, Ocean P.H. Ng, Albert H.C. Tsang, H.M. Liem

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

ARTICLE INFO

Article history:
Received 17 April 2009
Received in revised form 14 April 2010
Accepted 31 May 2010
Available online 3 July 2010

Keywords:
Physimetric identification
Biometrics
Automatic identification
Physical object authentication
Physical asset management
Anti-counterfeit

ABSTRACT

By relying on business intelligence technologies, services can be delivered to customers automatically by computer systems. To provide the right services to the right person, a methodology that precisely identifies a personal's identity must be in place. Biometrics offers a secure and reliable method for computerized personal identification and authentication. It accurately recognizes and determines the unique identity of a person based on her physiological and/or behavioral characteristics. In the case of physical objects, they may also be required to be identified automatically in order to provide additional services, such as at checkout counters of supermarkets or customs clearance checkpoints. Numerous crimes and business losses (e.g. counterfeit products) are related to mis-identification of physical objects. This paper introduces physimetric identification, an approach that applies the concept of biometrics for physical object identification. It addresses the problem through authenticating physical objects based on their unique physical and/or chemical characteristics. Apart from introducing the concept of physimetric identification, issues such as real applications, deployment considerations and limitations of the proposed technology will also be discussed.

1. Introduction

Identifying physical objects is an essential aspect of industrial applications. Physical objects must be identified through the use of different technologies ranging from pen and paper, barcode, 2D barcode, to Radio Frequency Identification (RFID), so that they can be managed and operated. In the current IT era, through the use of suitable identification technologies, computer systems can recognize physical objects automatically by reading the barcodes or RFID tags attached to these objects. By combining artificial intelligent and decision support technologies, such systems can automatically identify physical objects and take appropriate actions accordingly. There are, however, drawbacks associated with existing technologies. One of the major limitations is that computer systems recognize physical objects by verifying the identification technology used on the object instead of by verifying the physical object itself. Mis-identification problems will exist in industrial applications if mistakes or errors are made by the automatic identification technologies used.

It is realized that identification technology applied to human beings is well developed and mature. Biometrics is widely adopted in different areas to provide effective and accurate identification. It follows that we can improve physical object identification by exploiting the lessons learnt from the success of human identification technology. Every person has distinctive physiological and behavioral characteristics (e.g. face, voice). Our brains are able to verify these characteristics and match them with patterns in our memories. This way, humans can recognize each other accordingly. The use of biometrics enables computers to accurately identify a person by verifying the person's physiological and/or behavioral characteristics since the mid 19th century. It is noted that physical objects also contain some specific physical or chemical characteristics which can be used for unique identification. If those characteristics such as texture pattern and spectra can be captured, measured and verified by the computer system, and integrated with existing identification technologies, the accuracy of physical object identification can be improved significantly.

This paper introduces the concept and mechanism of Physimetric identification (Physi-ID) which will improve the accuracy in identification of physical objects by verifying their unique physical and chemical properties. In the following sections, the features and limitations of current identification technologies will be discussed. Biometrics as a mature human identification technology will then be reviewed. The workflow and advantages of the proposed Physi-ID will then be explained in detail. At the end of this paper, application examples of Physi-ID will be presented, along with

* Corresponding author. Tel.: +852 2766 6578; fax: +852 2362 9308.
E-mail address: mfskkwok@inet.polyu.edu.hk (S.K. Kwok).

0166-3615/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.compind.2010.05.014

discussion on the deployment considerations and limitations of the technology.

2. Review on identification and authentication technologies

2.1. Current automatic identification technologies

Automatic identification (Auto-ID) is developed to deliver object information to computer systems that support business operations [1]. It acts as an ID container that stores the digital identity of an object. Tagged objects are identified by the process of automated extraction of digital identity stored in the ID container. The extracted information is processed by a computer system for further manipulation. Nowadays, nearly all products are packaged with a barcode for its identification. In recent years, RFID becomes another hot Auto-ID technology for physical object identification in various industries. The value and benefits of using Auto-ID technology to facilitate automatic physical asset management have been reported in operations such as retail management [2], manufacturing management [3] and supply chain management [4]. Auto-ID typically involves the use of a serial number, i.e., an ID, which is related to the physical object. Details of an object can be retrieved from the database by using the object's serial number (ID) as the key. Therefore if an RFID tag on a bottle of water is read by an RFID reader, the system captures the information stored in the tag, and then uses the information to retrieve data from the database to identify the physical object as a bottle of water. This approach changes the traditional way of physical object identification, and can be performed without human involvement. It dramatically speeds up item management operations and significantly reduces human effort and error in data entry. The captured data can be automatically fed into enterprise applications for further processing.

The introduction of new Auto-ID technologies, including 2D barcode and RFID, and the mature development of Internet and networking infrastructure make unique object identification become possible. Unique identification defined by Department of Defence (DoD) of the United States Government refers to a set of data representing tangible assets that are globally unique and unambiguous. Integrity and quality of the unique ID must be assured throughout the life cycle of the object being identified, so as to support multi-faceted business applications and users [5]. Unique identification aims to enhance the visibility of physical objects in the supply chain in order to improve item management and accountability, and finally to achieve product life cycle information management. To achieve unique identification, apart from embedding globally unique product identifier (e.g. RFID) in the product, there must be a linking mechanism to product information that may be stored in backend systems and a network approach to share unique product information among various parties around the world. Distributed information architectures for collaborative Logistics (DIALOG), World Wide Article Information (WWAI) and Electronic Product Code (EPC) are the currently known approaches to implement unique identification [6]. In the example of EPC and EPCglobal network infrastructure proposed by Auto-ID Center is designed to achieve seamless sharing of RFID-related data. Products with unique ID (EPC) are traced and tracked from end to end of the supply chain, and information of the products is shared among parties in this network [7,8]. In the pharmaceutical industry, unique object identification is being adopted to trace and track each item of the pharmaceutical product. With such technology and network, the product pedigree which is a certified record that contains information about each distribution of prescription drug [9] can be retrieved for the enhancement of logistics visibility, product authentication and anti-counterfeit applications [10,11].

2.2. Limitations of current automatic identification technologies

While Auto-ID technology enables total automation of unique physical asset management and availability of real-time data in enterprise applications, it is not faultless. Many research studies show the unreliability of Auto-ID applications and systems. When no corrective action is taken, even a low data error rate may create severe problems and data inaccuracy in computer system [12]. The underlying reason is that the computer system identifies physical objects by making reference to the information stored in the attached Auto-ID instead of the object itself. The major problem of this approach is that the system will deliver erroneous data when mistakes are made in the Auto-ID reading process, such as capturing incorrect or non-existent data known as reading ghost tags, and failing to capture existent data (e.g. missing tags) in RFID systems [13].

The existing applications of Auto-ID technology assume that the information stored in the Auto-ID is always precise and the data capture process is error-free. In practice, these assumptions are often invalid, and existing automatic physical object identification applications typically do not have exception handling routines to cope with those situations. Human involvement is thus required in these cases to deal with reading errors of the system, limiting the realization of the full benefits of automatic identification. At retail stores, human operators are still needed to present the goods to barcode scanners to eliminate reading errors. More serious problems will happen when a genuine Auto-ID is cloned and the cloned one is attached to a counterfeit product. This is a serious weakness of anti-counterfeit and authentication applications. Barcode scan is an example that has this limitation of Auto-ID. Visualize this: a dishonest shopper used a home-use printer to produce the UPC (Universal Product Code) barcodes for a lower priced product, and then placed them over the correct bar codes on higher priced products. Since products are identified purely on the basis of the barcode read by the Point-of-Sale system, the dishonest shopper will be able to buy higher priced products at lower prices undetected. Wal-Mart lost USD 1.5 million in 2004 because of this fraud [14].

Readability is always a challenge of automatic physical object identification. In the case of barcode, it will be unreadable when blocked from the line of sight of the barcode reader, or when the laser beam of the barcode reader does not target the barcode accurately. In the case of RFID, readability is influenced by radio wave reflection, refraction, interference, RFID tag orientation, and other environmental factors [15]. Lodewijks et al. [16] concluded that reliability of RFID systems depends on the application factors, the RF technology used and deployment environment. In addition, environmental change may distort system reliability. Thus, there is a need for the verification of the physical object itself in automatic identification of physical objects. Reliability of the current Auto-ID applications is far from the Six Sigma level. The three major types of errors made by Auto-ID systems are: (1) physical object with improper Auto-ID, (2) physical object without Auto-ID and (3) Auto-ID without physical object. All these will generate inaccurate information to the management system and thus trigger inappropriate actions.

3. Lessons learnt from human identification technology (Biometrics)

In pursuit of a better approach to physical object identification, lessons may be learnt from Biometrics – the relatively mature human identification technology. Biometrics is also one of the automatic identification technologies commonly applied to verification of living individuals by using physiological and behavioral characteristics [17,18]. A biometric system essentially includes a pattern recognition system which acquires biometric data from an individual, a feature extraction module or program