Establishment of Biometric Verification System Based on Design Science Research Methodology and Sensing System for Smart Border Control

I-Chen Lin[*] and Wei-Hsi Hung

Department of Management Information Systems, National Chengchi University,
No. 64, ZhiNan Road, Section 2, Wenshan District, Taipei City 11605, Taiwan

Rapidly increasing traveler traffic has burdened the border security and clearance service. Therefore, assisting border guards and travelers to carry out sustainable border strategies is becoming more crucial. The key of such strategies centers on the interaction between sensing systems and user characteristics, and sensing technology is of great help for an efficient clearance service and smart border control. However, a practical problem is that deciding whether to allow or prevent entry at the border is ambiguous because checking identities with only a visual inspection is cumbersome. Hence, a biometric verification system (BVS) that compares a live biometric sample of a traveler against images of them obtained from the database is needed. In this study, we model and develop a fingerprint sensing system using design science research methodology (DSRM). An integrated framework, components, workflows, and schema are proposed. The novelty of this system is that the artifact retains the flexibility of the acquisition and match processes. After presenting a case study with fingerprint modal biometrics, we evaluate the usage of such a sensing application and the results to generate a sustainable strategy for managing security issues in the border-checking environment. This study offers a solution to balance the convenience of travelers and the role of inspectors.

1. Introduction

Biometric recognition has been widely applied to commercial, government, and forensic fields, and biometric technology is playing a crucial role around the world.[1,2] It can effectively prevent unauthorized access, obtain criminal evidence, and maintain public safety. Government applications, such as national ID cards, correctional facilities, driver's licenses, social security, welfare disbursement, border control, and passport control, are related to identity verification in the public arena.[1,3,4] Furthermore, many countries use automated border control (ABC) systems with the e-passport as the required token to consolidate security at borders in the face of threats of terrorism and immigration pressures.[5–8] A fingerprint sensing application is used to manage border control in the border-checking environment.

Border guard agencies are accountable for border security, foreign population management, and immigration policy promotion, and they enhance national safety and prosperity through border checking.[9,10] According to the world's largest annual airline traveler satisfaction survey, travelers consider airport ground handling, such as wait times and staff efficiency, to be the most important factors in their travel.[11–14] In general, a traveler crosses a border in less than 45 s. Passports are judged to be genuine or fraudulent in an average time of 15 s per document, and border officers have on average only 12 s to decide whether a traveler is legitimate or not.[15–17] When examining travel documents during rush hour, officers may miss crucial information in the authentication of certain travelers. Therefore, criminals and terrorists counterfeit their identity documents to deceive inspectors.

According to statistics from the Ministry of the Interior (Republic of China, Taiwan), the total number of entry and exit travelers increased rapidly between 1998 and 2019, reaching 57 million travelers in 2019, nearly 40% of which were foreigners.[18] The cumulative number of travelers during the period is shown in Fig. 1. It appears that the increasing trend of high-pressure situations at border crossings has resulted from a large flow of people. A biometric system can facilitate the clearance procedures for travelers while maintaining high security. The cooperation between existing inspection systems and biometric systems is thus an important issue.

When manpower and facilities are limited during peak hours, agencies should implement measures to shorten the wait time for visitors by using a sensing system. Specifically, a border inspection system (BIS) is used for border management. Biometric techniques enhance border inspection procedures of verification and identification.[1,19] Thus, dealing with a huge amount of inspection procedures is time-consuming and labor-intensive. It is necessary to figure out an interaction model of the sensing system and users' characteristics.[20,21] To this end, we propose in this paper a sensing application for a biometric verification system (BVS) to create a collaborative platform and to define the data flow diagrams between the BIS and BVS. The objectives are as follows: (1) to use design science research methodology (DSRM) with problem-centered initiation as an entry point for implementing a BVS; (2) to propose a sensing system that matches the workflows of the existing BIS; (3) to construct the overall system schema,
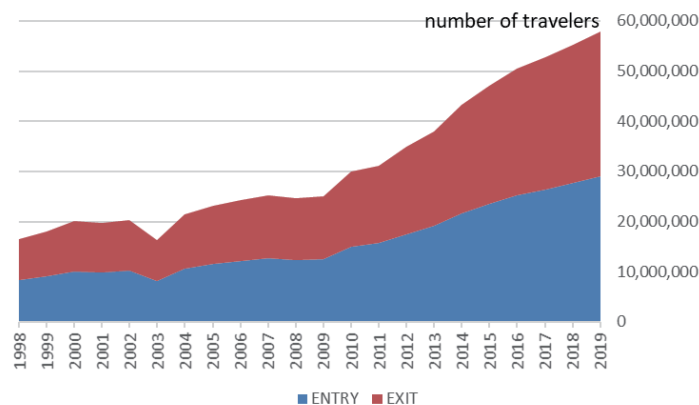

Fig. 1.   (Color online) Entry and exit travelers by year.

framework, and human–machine interface; and (4) to establish an integration system to understand sustainable border strategies. This study offers a solution to balance the convenience of travelers and the role of inspectors. It relies upon sustainable sensing systems that can be deployed at border-crossing points (BCPs).

2. Literature Review

2.1 Design science research methodology

DSRM is a design process that corresponds to business needs and related knowledge. It is used to improve the performance of system design, and its output is an IT artifact. Moreover, it refers to a tangible instantiation generated during the software development life cycle and addresses problems related to system design.[22,23] According to Peffers *et al.*, a design science process model consists of six activities: (1) problem identification and motivation, (2) definition of the objectives for a solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication.[24] It is the basis of the nominal sequence and process iteration to develop technology-based solutions to important and relevant business problems.

DSRM is fundamentally a problem-solving paradigm that is applied to the development, design, and creation of an application system. There are four possible research entry points: problem-centered initiation, object-centered solution, design/development-centered initiation, and client/context initiation.[24,25] The applicable entry point depends on the intended purpose. The outputs of DSRM, such as algorithms, human–machine interfaces, design methods, and process models, are often used in the fields of computer science and engineering, and many other disciplines.[22,23,25] In this study, problem-centered initiation is used as an entry point to establish a BVS for border control. With the six steps of DSRM, the needs of real system development can be described from the use requirements. The DSRM process model is used to implement the BVS and is shown in Fig. 2.

2.2 Biometric recognition

The field of biometrics involves automatically identifying individuals based on their modalities, and recognition is expressed as the meaning of verification and identification. Biometric recognition refers to distinctive physiological and behavioral characteristics or identifiers (e.g., ear, face, facial thermogram, hand thermogram, hand vein, hand geometry, fingerprint, iris, retina, signature, and voice) for proving a person's identity.[19,26] Therefore, biometric identifiers can focus on the factors of universality, distinctiveness, collectability, performance, acceptability, and circumvention.[19] It is widely acknowledged that biometric identifiers should only authenticate people, rather than their possessions or exclusive knowledge. Authentication refers to enabling the system to recognize the identity of the user. Unlike possession-based (e.g., passports) and knowledge-based (e.g., passwords) schemes, identity authentication schemes (biometric identifiers) cannot be misplaced, forgotten, guessed, or easily forged.[1,19,27]
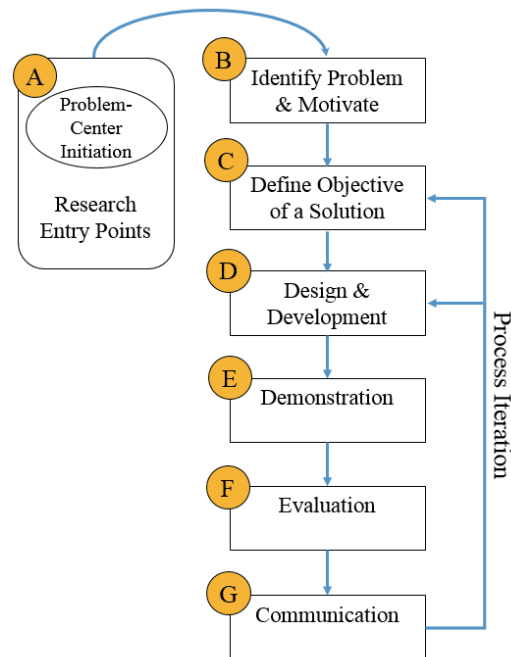
Fig. 2.　　(Color online) DSRM process model.

This study focuses on the use of sensing technologies and human–machine interaction to design an artifact. The design consideration relates to recognition accuracy, speed, resource requirements, and robustness to operational and environmental factors. Several biometric modalities lend themselves to use at the border. Owing to the requirement of the International Civil Aviation Organization (ICAO), the modalities are mostly used for identifying faces.[28,29] Furthermore, for the purposes of monitoring watch lists, which is done by police forces worldwide, fingerprint identification is also applied,[16] and faces are frequently used as the main modalities due to the above factors. When designing biometric systems, reasonable resource requirements, harmlessness to the users, acceptability by the users, and avoiding the risk of violating personal rights are all important.[30,31]

2.3　Border inspection system

The BIS is a computer system that provides law enforcement agencies with necessary information. It supports border guards in recognizing people who deserve additional scrutiny. The BIS usually combines sensor and surveillance systems to classify travelers and their cargo.[32] It also provides interfaces with the back-office administration system and information on the status of the crossing or events. The system includes a database server, application server, client terminal, and virtual private network (VPN).[33] The BIS is often located at BCPs, including border checkpoints, airports, and seaports, to track information on suspect individuals, aircraft, and cruise ships. It is also used to access records on wanted persons, identity information, criminal histories, and previous federal inspections.[16,34] It allows border guards to focus their limited resources on suspicious travelers.

The case study examined here is of the Taiwanese government, which established an interagency BIS that provides entry and exit records of the public, such as the National Police Agency (NPA), the Criminal Investigation Bureau (CIB), the National Health Insurance Administration (NHIA), and the Ministry of Foreign Affairs.[9] The BIS allows border guards to refer to all watch lists via intelligence teamwork. The BIS physically resides on distributed systems at a data center in the National Immigration Agency (NIA) and uses the mechanism of information transmission to promote public affairs, for example, epidemic prevention and social security, through cooperation between agencies.

2.4 Biometric system based on border control

A pattern verification system essentially runs by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.[1] Depending on the application scenario, a biometric system may be automatically operated either in verification mode or in identification mode. The border-crossing checks include three procedures: (1) authentication of the travel document, (2) verification of the traveler's identity, and (3) determination of whether or not the traveler is allowed to cross the border.[6,35] The BIS first checks whether the traveler is carrying valid travel documents. Then, it captures a biometric sample of the holder (typically, a face image, fingerprint, or other modality) and checks it against the image obtained from the biometric features database in verification mode. Finally, it assesses whether or not the traveler is authorized to cross the border. The ABC process steps are shown in Fig. 3.[6]

A biometric system based on border control should be combined with automated identity verification and inspection procedures. First, a traveler presents their passport, and the document
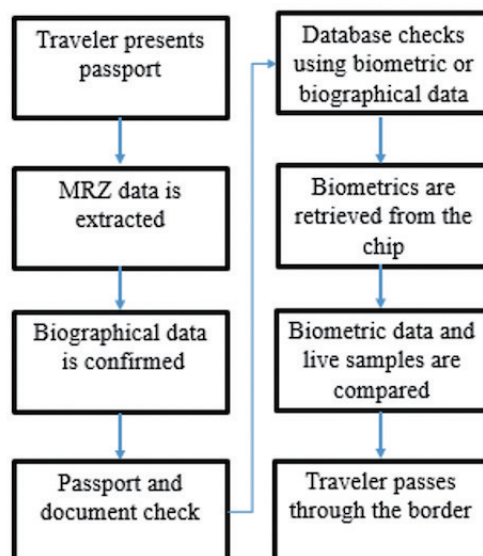

Fig. 3.   (Color online) ABC process steps.

is inspected at the entrance to security. The passport machine-readable zone (MRZ) includes two or three lines (OCR-B font text) in accordance with ICAO Document 9303.[28] The BIS extracts the passport while the BVS captures the biometrics, instructs the traveler, and compares the traveler's biometric features in real time. The artifact is useful for accurate inspection and accelerating traveler perception. As discussed in Maltoni *et al.*[19] and Labati *et al.*,[6] a biometric system has five modules: (1) a capture module, (2) a feature extraction module, (3) a template creation module, (4) a pre-selection and matching module, and (5) a data storage module. An ABC, such as an e-Gate, essentially contains components including (1) acquisition sensors, (2) an illumination system, (3) a biometric quality assessment module, and (4) a biometric verification module. As mentioned above, fingerprints captured by the acquisition sensor are highly distinctive for each individual. In addition, the illumination system complements an insufficient light source when capturing an image of a face. In this study, fingerprint modalities are adopted for a recognition mechanism in border control. A comparison with similar studies is shown in Table 1.

3. Research Design

3.1 Biometric verification system using DSRM

A. Problem-centered initiation

Travelers expect the wait time for inspection to be as short as possible, but it is difficult for border officers to quickly decide whether or not a traveler is allowed to cross the border with only a visual inspection. The lack of biometric acquisition and match workflows makes identity recognition confusing, which causes inspection procedures to become an uncertain task. The need for a more efficient solution enacted through a regular workflow triggered the design and development of the BVS in border control.

B. Problem identification and motivation

Automated biometric acquisition and match mechanisms in BIS are crucial. Thus, it is necessary to assist border guards in developing comprehensive inspection strategies. The formulation of such strategies must be based on biometric and sensing techniques. The privacy and quality of biometric data are important bases for decision-making on border-crossing policies. Inexperienced travelers who are not familiar with the BVS can have trouble performing biometric acquisitions.

Table 1
Design elements of biometric systems.

	Maltoni *et al.*[19]	Labati *et al.*[6]	This study
Component	Five modules	Four modules	Four modules
Workflow	Match-on-card, System-on-a-chip	ABC process steps	Acquisition/match workflows
Framework	N/A	Logical architecture	Logical architecture
Schema	N/A	N/A	Hardware/software
Instantiation	N/A	e-Gate	BVS

C. Objective

The objective is to develop a solution involving a sensing system embedded in border inspection procedures. The main challenge is to adapt the biometric data standards to routine operations. The BVS provides a systematic operational workflow that improves national security—the long-term goal.

D. Design and development

An artifact is an interactive BVS that automatically supports inspection procedures and has a user-friendly interface. The collection of a fingerprint sample is arranged in a biometric database system. This study illustrates the schema of the BIS and BVS systems. The redesigned artifact includes four components: (1) acquisition sensors, (2) a biometric quality assessment module, (3) a biometric verification module, and (4) a biometric matching module.

E. Demonstration

After developing proof-of-concept prototypes, which were tested in 2013 at Kaohsiung International Airport in Taiwan, the artifact was used widely by border officers. In the case study, the BVS was fully deployed at all airports and seaports in 2015. It was also demonstrated in a related report that the BVS can help prevent fraudulent and falsified passports from being used to cross the border. Demonstrations of the BVS are discussed in Sect. 4.3.

F. Evaluation

As many factors affect the accuracy and performance of a system, the BVS helps to improve entry and exit inspection procedures. Confirming the accuracy of a traveler's identity through a manual check can only identify minor problems. However, the BVS was found to be effective in border control field applications, and its usage can be evaluated by measuring the proportion of acquisitions and matches.

G. Communication

Papers relating to the BVS have been published in academic conference proceedings and professional outlets. The development of the biometric system was presented in the National Development Council government service report. Moreover, the adoption of the BVS has received widespread media attention in Taiwan.

3.2 Biometric acquisition workflow

Regulatory compliance is the basis for the adoption of biometric policies (i.e., Who should acquire the biometric sample?). A traveler arrives at the inspection counter and presents their passport to the inspection officers. First, the MRZ data are extracted, and the passport and biographical data are used to check whether or not the traveler is a multiple-passport holder. Next, the traveler places both index fingers on the acquisition sensors. Almost simultaneously, the BVS captures an image of the traveler's face using a camera. The following acquisition workflow (A to I) was used for the system design (see Fig. 4 for the biometric acquisition workflow):
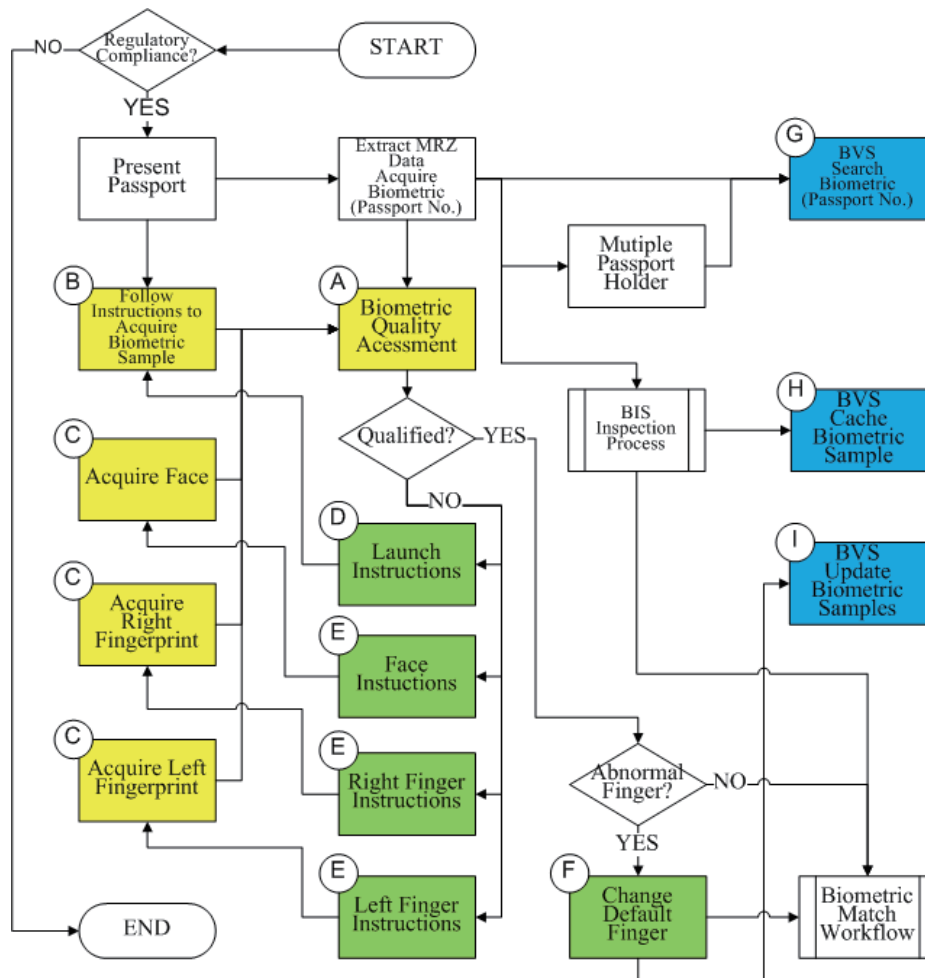
Fig. 4. (Color online) Biometric acquisition workflow diagram.

A. The BVS automatically evaluates the quality of the biometric data (i.e., the face and the fingerprint). A quality score is displayed as a color, such as red (bad), yellow (medium), or green (good), which is shown on the quality monitor.

B. The navigator monitor provides animated instructions to help the traveler understand how to place their index fingers on the scanner and where to look at the camera.

C. According to the biometric assessment on the quality monitor, inspectors can trigger the appropriate biometric acquisition process (face, right finger, or left finger) and ask the traveler to follow the instructions on the navigator monitor again.

D. If the traveler does not follow the instructions, inspectors can trigger the replay of the instructions or assist them directly.

E. After showing the acquisition instructions for the face, right fingerprint, and left fingerprint (with animations displayed separately), the instructions can be replayed to the traveler while the inspectors assess any poor-quality data.

F. If a traveler's index finger cannot be captured by the sensors (a rare occurrence), the thumb, middle finger, ring finger, and little finger can sequentially replace the index finger scan and be recorded in the BVS.

G. The BVS searches the biometric template using the passport number and the database. The search result should be no, one, or multiple biometric records.

H. The BVS temporarily caches the biometrics and images in the industry personal computer (IPC).

I. If a traveler has abnormal fingers (such as no features or a missing finger), the inspector will ask them to remove their fingers from the scanner and make a note in the record. The BVS updates the biometric samples.

3.3 Biometric match workflow

Following the workflow discussed in Sect. 3.2, the biometric acquisition process is completed. The BIS presents biographical data and sends the biometric data to the BVS for matching. The BVS caches biometric data to provide continuous comparisons. When a traveler is a high risk, the BIS will alert the inspectors. Later, senior inspectors will conduct further investigation procedures on travelers. The following match workflow (A to I) was used for system design (see Fig. 5 for the biometric match workflow).
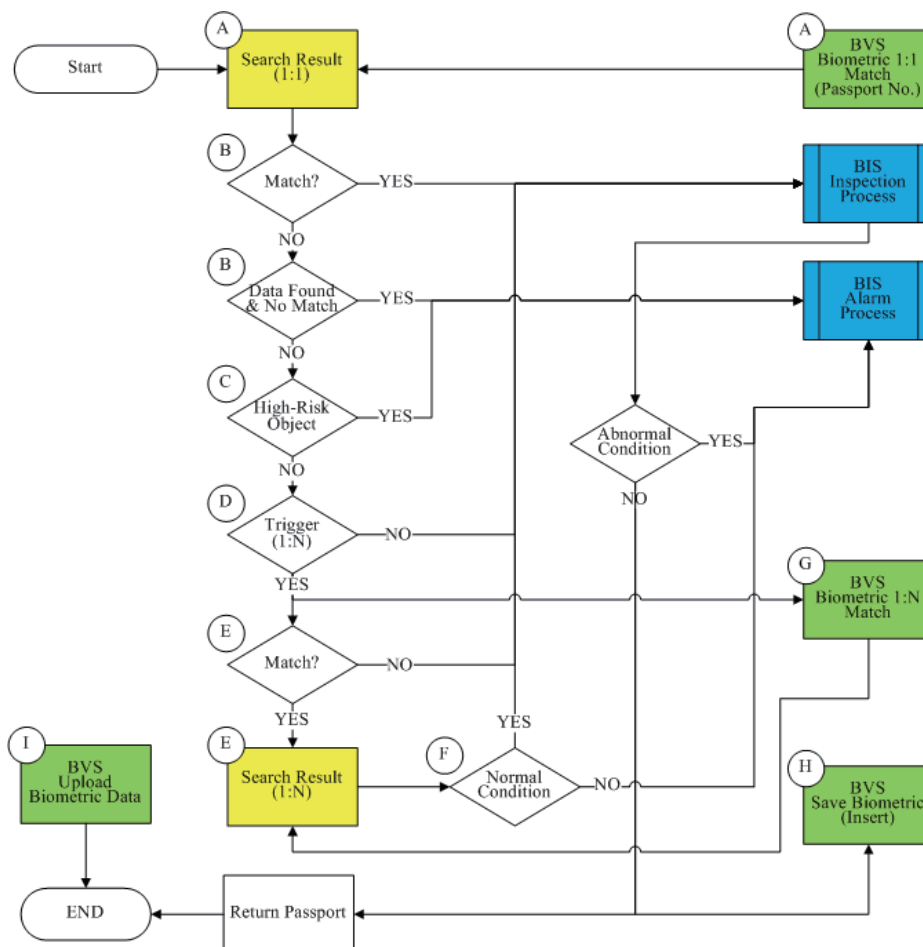
Fig. 5.   (Color online) Biometric match workflow diagram.

A. The BVS returns the search result of a biometric 1:1 match and displays the result on the IPC monitor. Inspectors can clearly see whether or not the traveler is a high risk.

B. The biometric search result (1:1) is also presented as a color, such as red (high risk), yellow (medium risk), or green (low risk), and is shown on the IPC monitor. Next, inspectors check the traveler's biographical data to decide whether or not they are an abnormal (high) risk.

C. If someone is a high-risk traveler, such as a person on a watch list, from a specific country, or the target of specific monitoring, their biographical or biometric data will have been noted before. Next, the BIS will alert the inspectors.

D. If the inspectors cannot decide whether or not a traveler is an abnormal risk, they may trigger the 1:N match in the BVS or continue the inspection process in the BIS.

E. The BVS returns the search result of the 1:N match on the IPC monitor. Again, inspectors should know whether or not the traveler is an abnormal risk.

F. The BVS provides more biometric information (e.g., the traveler is a multiple-passport holder or a document is a forgery). Next, the BIS alerts the inspectors. Senior inspectors will conduct further investigation procedures on the traveler.

G. The biometric search result (1:N) presents the decision using a color, such as red (high risk), yellow (medium risk), or green (low risk), which is shown on the IPC monitor.

H. At this point, the inspection procedure is complete. The BVS saves the latest biometric data corresponding to the traveler's passport number, nationality, the inspectors, and the inspection time.

I. The BVS updates and synchronizes the biometric data to the backup database on schedule.

3.4 System components

By using the biometric acquisition and match workflow mentioned previously, the framework is constructed as described in Sect. 4.1; likewise, the schema and interface are discussed in Sect. 4.2. Table 2 shows the BVS components, workflows, and functions. The system components are as follows:

Table 2
Component, workflows, and functions of the BVS.

Component	Workflow	Function
Acquisition sensors	Sect. 3.2.A–3.2.D	Appropriate placement Customized device Two-way interaction
Biometric quality assessment module	Sect. 3.2.E–3.2.I	Quality score Adjustable threshold Retry mechanism
Biometric verification module	Sect. 3.3.B–3.3.D Sect. 3.3.F Sect. 3.3.H–3.3.I	1:1 match Comparison mechanism System integration
Biometric matching module	Sect. 3.3.A Sect. 3.3.E Sect. 3.3.G	1:N match In-memory database Performance monitor

A. Acquisition sensors

When the biometric sample is captured, the navigator monitor will inform the traveler of how to provide the biometrics. The illustrations should indicate the correct placement of the biometric trait toward the device for a better interaction. Moreover, the capture device may be manually adjusted to the characteristics of the traveler's fingerprint. The duration of this process is less than one second.

B. Biometric quality assessment module

The quality of a biometric sample represents the degree to which it fulfills the quality score in a quantitative expression. Quality evaluation and capture retry are included for quality assurance. Inspectors check the quality of the acquired image. If it is not high quality, the BVS may ask the traveler to retry the acquisition a specified number of times. To ensure an effective verification process, the captured biometric image must be compliant with international standards. In this way, it is possible to accurately perform the matching.

C. Biometric verification module

The most common biometric operation performed by the BVS is identity verification in which it performs a comparison between live-captured samples and the biometric data stored in a biometric database. In some circumstances, the BVS uses biometrics to perform a verification match, which involves a biometric search in a 1:1 match. If a traveler is rejected, it could be due to the traveler being undocumented or the system needing to check a watch list for more information.

D. Biometric matching module

The BVS compares the live-captured data with what is stored in the travel document or database to determine whether they correspond to the same person. The result of the identification ($1{:}N$) process is the acceptance or rejection of the matching. For performance issues, this is completed using the in-memory database. The result depends on a threshold defined by the border authority according to the security level, and it is displayed as the false acceptance rate (FAR) and false rejection rate (FRR). Therefore, the threshold value also has an impact on the performance of the system.

The biometric application programming interface (BioAPI) specifies a standard architecture for the communication between the software and the biometric sensors of different vendors.[36] The acquisition sensors have to guarantee high image quality. Moreover, they may automatically adjust to the characteristics of the traveler. The quality assessment module checks the quality of the image. The verification module applies feature extraction to create a biometric template and matching algorithms; this is done to check whether the live-captured image and the one present in the biometric database correspond to the same person.

4. Results

4.1 System framework

The BVS framework was adopted for the BIS to solve the problems of border officers. The system examines travelers' documents, takes photos, and captures fingerprint biometrics to assist the inspection process and check each traveler's identity. This prevents people from entering and exiting the country using forged documents. The framework of the BVS produced by DSRM can be used as a practical artifact, especially for applications in the field of border security and other related fields. In this study, we designed and developed an interactive BVS by implementing the framework.

The result of the verification process and the related details, such as the matching score or the reasons for rejection,[37] are shown to the border officers at the monitoring station. The matching module is implemented with a commercial software development kit (SDK) for fingerprint identification, which is designed for biometric systems developers and integrators. The SDK ensures system performance with fast, reliable fingerprint matching in one-to-one and one-to-many modes. The biometric matching response time should not be longer than 0.6 s,[38] even in a centralized system where the process is more complex due to the involved distributed computing nodes. Moreover, the system framework is constructed to handle privacy, inspection, and system issues. To monitor the risk of travelers, the BVS integrates the BIS, the restriction system (watch list), the document authority system (DAS), and the advance passenger information (API) system. The framework of the BVS is shown in Fig. 6.
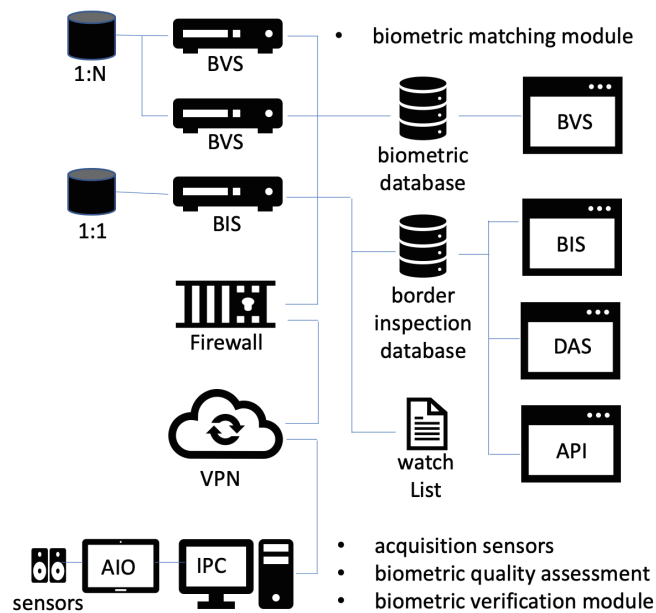

Fig. 6.   Framework of the BVS.

4.2   System schema

Figure 7 shows the schema for the BIS and BVS. The system was designed using a web service for a human–machine interface and is controlled by the program that checks the biometric data. First, All in One (AIO) captures the fingerprint of the index finger and takes a picture of the traveler's face for feature extraction. If the fingerprint quality does not meet the threshold, images of other fingerprints can be captured and recorded separately to achieve satisfactory image quality. The schema of the frontier client (the BIS and BVS) is listed as follows:

A. IPC/monitor: Industry personal computer with a monitor used for displaying the BIS and BVS information to the officer.
B. MRZ reader: ICAO-standard-compliant e-Passport or ID documents.
C. AIO: Linux OS, 32 GB SSD, 2 GB RAM. Includes the acquisition sensors and the biometric quality assessment module.
D. Quality monitor: 13.3-inch LCD with 1366 × 768 pixels used for displaying the biometric quality score and the matching result.
E. Fingerprint/picture acquisition: Dual-finger module with 500 dpi, and a dual camera with 2 M dpi.
F. Navigator monitor: 7-inch LCD used for displaying instructions to travelers.

4.3   Demonstration

In Taiwan, border control organizations, which are situated in 10 airports and 15 seaports, are responsible for maintaining border security.[9] The locations where the system is installed in Taiwan are shown in Table 3. The traveler clearance service at international BCPs has motivated
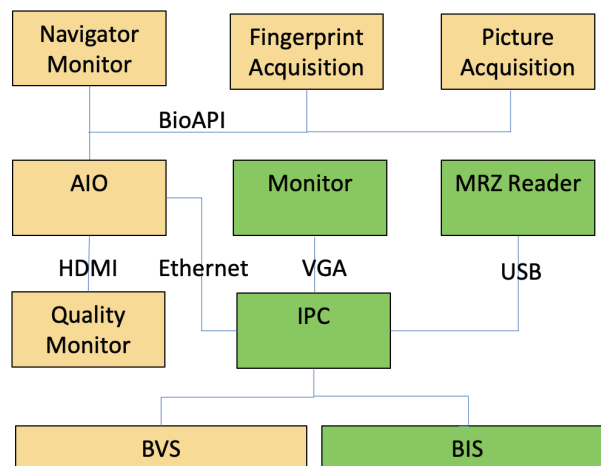
Fig. 7.   (Color online) Schema of the BIS and BVS.

Table 3
Location of BVSs at border control points in Taiwan.

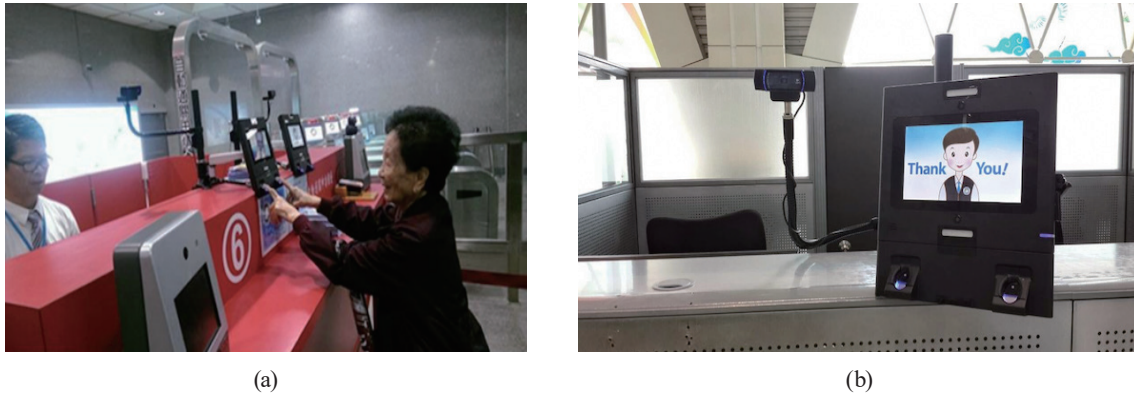| BCPs	Location	Num	Percent
Airport	Songshan, Taoyuan, Taichung, Chiayi, Tainan, Kaohsiung, Taitung, Hualien, Kinmen, and Penghu	258	71.67
Seaport	Keelung, Taipei, Taichung, Mailiao, Budai, Anping, Kaohsiung, Hualien, Heping, Suao, Magong, Shuitou, Fuao, Liaoluo, and Baisha	102	28.33

(a) (b)

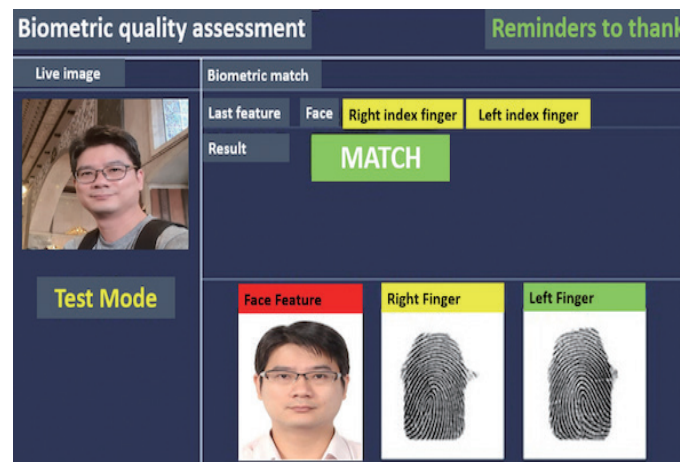Fig. 8. (Color online) BVS in use at (a) Kinmen harbor and (b) Songshan Airport.

Fig. 9. (Color online) Interface of the BVS.

research to find more efficient solutions. Border officers are in charge of inspecting and examining travelers and cargo. They strive to facilitate a balance between efficiency and integrity, providing travelers with a high-quality immigration clearance service, so as to contribute to a positive image for international exchange.

By establishing the system mentioned above, border guard agencies can upgrade their overall clearance service quality and stop illegal activities effectively. This prevents travelers carrying falsified travel documents from entering the country. We propose a BVS schema and framework using DSRM. Figures 8(a) and 8(b) show the BVS in use at Taiwanese BCPs, and Fig. 9 shows the human–machine interface.

4.4   Evaluation

The number of acquisitions indicates how many travelers were successfully saved to the biometric database. Figure 10 shows the total monthly number of biometric acquisitions of entry and exit travelers in 2018 and 2019. The monthly average is 1,415,984, with 807,062 (57%) entry travelers and 608,923 (43%) exit travelers. While there were more entry travelers than exit travelers who provided biometric data, biometrics are more likely to be captured and extracted from travelers entering Taiwan than from those who are leaving. Also, the border guards at entry points are more concerned about collecting biometrics than their counterparts at the exit points.

The 1:1 match number represents travelers for whom the one-to-one comparison procedure was performed for the biometric sample using AIO equipment. Equivalently, the 1:N match number represents travelers who performed the one-to-many comparison procedures for biometric samples using the biometric database. Figure 11 shows the total monthly number of 1:1

Fig. 10.   (Color online) Number of biometric acquisitions of travelers at entry and exit points.

Fig. 11.   (Color online) Number of travelers subjected to 1:1 and 1:N matches at entry BCPs.
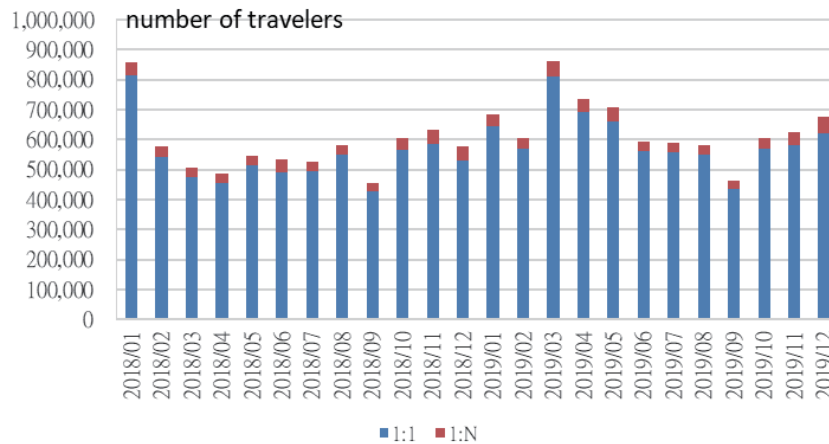
Fig. 12.   (Color online) Number of travelers subjected to 1:1 and 1:*N* matches at exit BCPs.

and 1:*N* biometric travelers in 2018 and 2019 at entry BCPs. The number of 1:1 matches was 7,787,629, whereas that of 1:*N* matches was 11,623,917. Furthermore, the monthly average number of 1:1 matches was 324,485, whereas that of 1:*N* matches was 484,330. The total monthly average was 808,815. Regarding entry BCPs, the proportion of 1:*N* matches (59.88%) was higher than that of 1:1 matches (40.12%). Clearly, the border guards are used to match biometrics with one-to-one and one-to-many comparisons in common scenarios at entry BCPs.

Figure 12 shows the total monthly number of 1:1 and 1:*N* biometric travelers in 2018 and 2019 at exit BCPs. The total number of 1:1 matches was 13,704,375, whereas that of 1:*N* matches was 909,773. The monthly average number of 1:1 matches was 571,016, whereas that of 1:*N* matches was 37,907. The total monthly average number was 608,923. At exit BCPs, the proportion of 1:*N* matches (6.23%) was less than that of 1:1 matches (93.77%). This means that the border guards are used to match biometrics with one-to-one comparisons in common scenarios at exit BCPs. Since inspectors can decide the timing of one-to-many comparisons, we infer that the policy of border inspection procedures is to control entry but not exit during a predetermined period of time.

5.   Conclusions

Using the advantages of sensing technology, different types of sensors are introduced to connect with various computers and mobile devices and to transfer the data collected by each device to the required system.[39] In this study, fingerprint sensors are applied as input devices, and the BIS and BVS are used as a communication platform to deliver the detected biometric data from the sensors to the server.

The establishment of a BVS is expensive and time-consuming. To accelerate the stage of system development, we proposed a workflow, schema, and framework for system design and development. In this study, we identified the problem of the BIS and used problem-centered initiation for an entry point. The artifact is based on the needs of identity verification and

identification for border security. We refer to the main biometric modalities for the proposal of a BVS interface to implement a practice and improve inspection procedures through biometric security solutions.

In this paper, we propose an interactive BVS based on sensing technology and design science research demonstrated in Taiwan. By utilizing biometric data, identity verification, and matching policies in the BVS, counterfeit identity cases can be solved in a short period for border control and management.[40] This study offers a solution to balance the convenience of travelers and the role of inspectors. It relies upon rigorous methods that can be deployed at BCPs and will be of great help for achieving an efficient clearance service and smart border control.

5.1   Implications

Academically, the aim of this study was to design an interactive BVS with DSRM and to verify the design elements by testing at Taiwan's border. The first BVS on Taiwan's border was also discussed to demonstrate the real-life usage. Past studies of the conceptual framework of biometric recognition systems were discussed. The preliminary work proposed by Maltoni *et al.* (2009) and Labati *et al.* (2016) explained the fundamental components, but it lacked a specific application in frontier client and systematic connections between inspection procedures and sensing technologies. In this study, we redesign the components and workflows. Its novelty is that the artifact retains the flexibility of the acquisition and match processes. It also improves the detailed operation principles of the system and transforms them into a system framework, schema, and human–machine interaction interface.

Practically, we proposed a collaborative platform for the BIS and BVS. The platform can save time and cost in system development. Furthermore, through a friendly user interface (for travelers and inspectors), the satisfaction of travelers can be maintained while inspectors acquire high-quality biometric samples. The novelty of our system is that travelers can complete the biometric capture process in a semi-self-service interaction, and the inspector retains the authority over efficient service decisions and inspection procedures. Consequently, the accuracy of the BVS is ensured and border security is achieved.

5.2   Limitations and future research

One limitation of this study is that the system design is applied to the BCPs of Taiwan, whereas the biometric workflows could be different when applied to the immigration policies of other countries. To attract foreign people into the country, Taiwan adopts a friendly and flexible policy that allows border guards to maintain autonomy in certain scenarios and decide whether or not to initiate further identification ($1{:}N$) workflows. The involvement of senior inspectors is also limited by border guard training,[12] and it is affected by the biometric and inspection procedures. According to this study, we found that Taiwan's biometric strategy is to manage entering travelers more carefully than exiting ones. Different countries may have different border policies, so the design should be adjusted according to local requirements.

In future work, we will investigate the use of enhanced technologies that employ multiple sensors and modalities, such as facial expressions and artificial intelligence techniques. It will be interesting to use a multimodal biometric framework for biometric integration in border control systems that rely on machine learning techniques to improve border control management and traffic flow. Moreover, the IaaS (infrastructure as a service) resource pool, cluster computing, and hyper-converged infrastructure may enable system managers to easily adjust the settings and improve performance. Unimodal biometric systems may be overtaken by those that use multiple biometric modalities (e.g., a person's face and fingerprints).[41] Multimodal biometrics can extract data from multiple sensors, multiple samples, and multiple algorithms. Facial recognition can also be adopted to other applications. Ultimately, the goals of the BVS are to develop efficient and perfect verification that improves both the integrity of borders and the speed of the travel flow. Future research may reveal how to effectively adopt these technologies in different contexts.

References

1 A. K. Jain, A. Ross, and S. Prabhakar: IEEE Trans. Circuits Syst. Video Technol. **14** (2004) 4. https://doi.org/10.1109/TCSVT.2003.818349

2 L. R. Carlos-Roca, I. H. Torres, and C. F. Tena: Proc. 2018 Int. Joint Conf. Neural Networks (IEEE, 2018) 1–7.

3 D. O. Gorodnichy: Proc. 2011 IEEE Workshop Computational Intelligence in Biometrics and Identity Management (IEEE, 2011) 44–53.

4 A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed: Comput. Stand. Interfaces **66** (2019) 1. https://doi.org/10.1016/j.csi.2019.04.002

5 T. Caldwell: Biom. Technol. Today **2015** (2015) 5. https://doi.org/10.1016/S0969-4765(15)30079-5

6 R. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza: ACM Comput. Surv. **49** (2016) 24. https://doi.org/10.1145/2933241

7 R. D. Labati, A. Genovese, E. M. Ballester, V. Piuri, F. Scotti, and G. Sforza: Proc. 2015 IEEE Symp. Series Computational Intelligence (IEEE, 2015) 354–361.

8 D. C. Cantarero, D. A. P. Herrero, and F. M. Méndez: Proc. 2013 European Intelligence and Security Informatics Conf. (IEEE, 2013) 277–280.

9 NIA: About the National Immigration Agency, https://www.immigration.gov.tw/5475/5478/141386/141392/ (accessed July 2020).

10 S. Trochu and O. Touret: Proc. 2013 European Intelligence and Security Informatics Conf. (IEEE, 2013) 281–284.

11 Skytrax: Awards Methodology, https://www.worldairlineawards.com/awards-methodology/ (accessed July 2020).

12 L. Salmela, S. Toivonen, M. Kulju, and M. Ylikauppila: Proc. 2018 European Intell. and Secur. Informatics Conf. (IEEE, 2018) 61–64.

13 E. C. S. Ku and C. D. Chen: J. Air Transp. Manage. **32** (2013) 87. https://doi.org/10.1016/j.jairtraman.2013.07.001

14 C. Morosan: J. Air Transp. Manage. **55** (2016) 120. https://doi.org/10.1016/j.jairtraman.2016.05.005

15 MOTC: Accelerate the Promotion of Smart Airports and Improve the Efficiency of Clearance Service, https://www.motc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=201812180008&aplistdn=ou=data,ou=news,ou=chinese,ou=ap_root,o=motc,c=tw&toolsflag=Y&imgfolder=img%2Fstandard (accessed May 2020) (in Chinese).

16 Publications Office of the EU: Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, https://op.europa.eu/en/publication-detail/-/publication/e81d082d-20a8-11e6-86d0-01aa75ed71a1/language-en (accessed January 2021).

17 M. Gariup and G. Soederlind: Proc. 2013 European Intelligence and Security Informatics Conf. (IEEE, 2013) 231–238.

18 MOI: Statistical Yearbook of Interior, https://www.moi.gov.tw/files/site_stuff/321/2/year/year_en.html (accessed May 2021).

19   Handbook of Fingerprint Recognition, D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Eds. (Springer, London, 2009) 2nd ed., pp. 8–29.
20   R. Blanco-Gonzalo, O. Miguel-Hurtado, C. Lunerti, R. M. Guest, B. Corsetti, E. Ellavarason, and R. Sanchez-Reillo: IEEE Trans. Hum.-Mach. Syst. **49** (2019) 397. https://doi.org/10.1109/THMS.2019.2913672
21   J. J. Robertson, R. M. Guest, S. J. Elliott, and K. O. Connor: IEEE Trans. Hum.-Mach. Syst. **47** (2017) 983. https://doi.org/10.1109/THMS.2016.2611822
22   A. R. Hevner, S. T. March, J. Park, and S. Ram: MIS Q. **28** (2004) 75.https://doi.org/10.2307/25148625
23   K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen, and J. Bragge: Proc. Int. Conf. Design Science Research in Information Systems and Technology (DESRIST, 2020) 83–106.
24   K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee: J. Manage. Inf. Syst. **24** (2007) 45. https://doi.org/10.2753/MIS0742-1222240302
25   G. L. Geerts: Int. J. Accounting Inf. Syst. **12** (2011) 142. https://doi.org/10.1016/j.accinf.2011.02.004
26   C. H. Lin, J. C. Liu, and K. Y. Lee: Sens. Mater. **30** (2018) 385. https://doi.org/10.18494/SAM.2018.1757
27   C. Vinothkumar and P. J. B. Parakkal: Res. J. Pharm. Technol. **8** (2015) 1264. https://doi.org/10.5958/0974-360X.2015.00229.2
28   ICAO: Machine Readable Travel Documents 9303, https://www.icao.int/publications/pages/publication.aspx?docnum=9303 (accessed June 2020).
29   H. M. Nguyen, A. Rattani, and R. Derakhshani: 2019 IEEE Int. Symp. Technology for Homeland Security (IEEE, 2019) 1–7.
30   M. Ylikauppila, S. Toivonen, M. Kulju, and M. Jokela: Proc. 2014 IEEE Joint Intelligence Security Informatics Conf. (IEEE, 2014) 168–175.
31   M. A. S. Abomhara, S. Yildirim Yayilgan, A. H. R. Nymoen, M. Shalaginova, Z. Székely, and O. Elezaj: Proc. e-Democracy 2019 (Springer, 2019) 94–109.
32   R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza: Proc. 2015 IEEE Int. Symp. System Engineering (IEEE, 2015) 412–419.
33   A. Kanak: IET Biom. **7** (2018) 510. https://doi.org/10.1049/iet-bmt.2018.5067
34   S. Gold: Biom. Technol. Today **2012** (2012) 9.https://doi.org/10.1016/S0969-4765(12)70149-2
35   Publications Office of the EU: Twelve Seconds to Decide: In Search of Excellence: Frontex and the Principle of Best Practice, https://op.europa.eu/en/publication-detail/-/publication/75d39cda-0447-4ba6-829e-23214486e261 (accessed January 2021).
36   X. Yuan, S. C. Hui, M. H. K. Leung, and Y. Gao: Comput. Stand. Interf. **26** (2004) 289. https://doi.org/10.1016/j.csi.2003.09.002
37   D. Gorodnichy, S. Yanushkevich, and V. Shmerko: Proc. 2014 IEEE Symp. Computational Intelligence in Biometrics and Identity Management (IEEE, 2014) 118–125.
38   Neurotechnology: VERIFINGER SDK, https://www.neurotechnology.com/verifinger.html (accessed January 2021).
39   C. Y. Cheng and J. F. Tu: Sens. Mater. **32** (2020) 1731. https://doi.org/10.18494/SAM.2020.2690
40   C. Morosan: J. Hospitality and Tourism Technol. **3** (2012) 176. https://doi.org/10.1108/17579881211264477
41   L. Hong, A. K. Jain, and S. Pankanti: Proc. AutoID (Citeseer, 1999) 59–64.

About the Authors

I-Chen Lin received his bachelor's degree and master's degree from the Department of Information Management, Central Police University, Taiwan, in 2000 and 2005, respectively. He is currently working toward his Ph.D. degree in management information systems at National Chengchi University, Taiwan, while working as a project manager within the National Immigration Agency, Taiwan. He is responsible for traveler clearance system design. His research interests are in the areas of design science, process reengineering, sensors, and biometric systems. (106356502@nccu.edu.tw)

Wei-Hsi Hung is a professor of management information systems at National Chengchi University, Taiwan. He received his Ph.D. degree and master's degree (with 1st class honours) from the Department of Management Systems, University of Waikato, New Zealand. His research interests are in the areas of e-commerce, IS alignment, knowledge management, and supply chain management. His research papers have appeared in journals such as Decision Support Systems, Communications of the Association for Information Systems, Journal of Global Information Management, Internet Research, Industrial Marketing Management, Technology Analysis & Strategic Management, Journal of Computer Information Systems, Telematics and Informatics, Computers in Human Behavior, Industrial Management & Data Systems, International Journal of Logistics Research and Applications, Asia Pacific Management Review, International Journal of Web Portals, Communications of the ICISA, Pacific Asian Journal of Association for Information Systems, and Journal of Information Management. (fhung@nccu.edu.tw)