10th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2022
Belgrade, Serbia, 13 – 14 October 2022

DESIGNING THE PORTABLE BIOMETRIC STATION FOR MILITARY APPLICATION

DEJAN ĆIPROVSKI
Metropolitan University, Vlatacom Institute, Belgrade, dejan.ciprovski@vlatacom.com

BOŠKO BOŽILOVIĆ
Vlatacom Institute, Belgrade, bosko@vlatacom.com

SAŠA BOŽINOVIĆ
Vlatacom Institute, Belgrade, sasa.bozinovic@vlatacom.com

DRAGAN DOMAZET
Metropolitan University, Belgrade, dragan.domazet@metropolitan.ac.rs

Abstract: *Identification and verification of authorised users in a military context can sometimes be a matter of life or death and it is therefore essential for systems to be accurate, reliable and robust. In order to fulfill requirements for secure collecetion of military personnel biometric data for an African country, Vlatacom Institute has developed the Portable Biometric Station (PBS). Portable Biometric Station consists of rugged case with integrated devices for acquiring biometric data and a laptop which runs the Enrolment Station software application. The military application of PBS stress its hardware ruggedisation and software reliability. This paper describes in details implemented software application that collects data such as facial image, digital signature as well as fingerprints. The PBS is easy to handle, and portable which means it can be moved easly to the different remote locations. PBS can operate in both online and offline modes. The data collected during the enrolment process are, uploaded to the server application in order, their validity to be approved/rejected. The acquired data, later, can be used for military base access control, soldier identity verification, and/or in producation of the officer electronic identification (eID) cards.*

Keywords: *military, portable biometric station, vlatacom, enrolment, software.*

1. INTRODUCTION

Typically utilized in security protocols, biometric techniques can ascertain the identity of individuals via the examination of specific physiological and behavioral identifiers. The six most commonly used forensic biometric identifiers are finger, face, voice, hand geometry, iris, and signature. These biometrics are measurable, unique characteristics that are used to identify both living and/or deceased individuals [1].

Many organizations, ranging from small companies to governmental and international institutions, may run some kind of electronic personal identification system, based on human biometric data. Usually, the organisation issues a document containing biometric data to the person and keeps track of that document in its biometric information system.

A biometric system can be used for verification or identification. Verification refers to validating a person's identity by comparing the captured biometric data with their own biometric template(s) stored in the system data-base [2]. This is a one-to-one process that answers the question of whether the person concerned is who they claim to be. Identification refers to recognizing an individual by searching the templates of all the users in the database for a match. Identification is a one-to-many comparison to establish an individual's identity without the person concerned having to claim an identity.

2. RELEATED STUDIES

The term biometrics strictly relates to the statistical analysis of biological phenomena and measurements, but has become widely accepted within the security profession to describe technologies used for personal identity verification [3].

The conflicts in Iraq and Afghanistan have prompted the widespread use of biometrics in the field. In many circumstances, accurate identification becomes a matter of life or death [4]. The first large-scale use in these theatres was in 2004, at Falluja, Anbar Province. A major stronghold for insurgents and the scene of some the fiercest fighting in the whole campaign, Falluja was surrounded and contained by the US Marine Corps. No-one was allowed in or out without having their biometric details captured.

The use of biometrics was given even greater impetus later that year when an Iraqi suicide bomber gained access to a US base in Mosul and killed 22 personnel. This spurred greater efforts at positively proving the identities of anyone gaining access to US facilities, which resulted in the Biometric Identification Systems for Access

(BISA). This provided every foreign national who needed to enter a US military facility with a biometric ID card. The data was checked against two databases, Automated Biometric Identification System (ABIS) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

The value of biometrics became most readily apparent in April 2011 when 475 prisoners tunneled their way out of the Saraposa prison in Kandahar, Afghanistan. Around 35 escapees were back in jail within a few days by being identified at checkpoints, routine traffic stops and borders. Less dramatically, but perhaps more significantly, some 20-25 suspects are apprehended each week as a result of routine biometric checks.

While much biometric research involves authenticating the identity of living individuals by comparing them with who they claim to be, postmortem applications of biometrics often involve the identification of an unknown individual [5]. Therefore, postmortem biometrics such as fingerprints, irises, and facial recognition may be a useful approach toward establishing a positive identification of unknown human remains in forensic settings. With improved digital imaging capabilities that have led to more efficient capturing of biometric data, along with the increased use of biometrics as part of identity profiles, it is becoming more practical to consider these data as part of the biological profile of human remains.

In December 2001, U.S. military forces detained Mohamed Al Kahtani as an enemy combatant on the field of battle in Southwest Asia. During repeated interrogations Kahtani denied being a combatant and offered an innocent explanation for his presence in the region. While Kahtani was in military custody, the FBI team fingerprinted him in much the same way law-enforcement officials routinely fingerprint criminal suspects in the United States. They took Kahtani's 10 "rolled" fingerprints. This collection of biometric data eventually led U.S. investigators to believe Kahtani was the missing 20th hijacker in the terrorist attacks of 11 September 2001 [6].

3. PORTABLE BIOMETRIC STATION

The Vlatacom product, Portable Biometric Station (PBS) enables government agencies to implement large-scale identity management, including biometric data, to enhance process security and protect the identity of each registered individual.

The authority performs biometric data acquisition on easily accessible sites, where the applicants apply for a personal identity documents. The collected data should finally end up at the central site, where the main databases and servers reside.

Enrolment Station is designed to collect the data, create the electronic application record and send it to a central location (online mode), or store them on the local storage device (offline mode). Upon successful submission of the application record, processing of the applicant is finished and the new enrolment process can proceed. Enrolment Station supports submission of application records to several kinds of storages, but in most cases, this storage is local enrolment server, residing on the same site as the Enrolment Station, often in the same local area network. Application records can be stored locally so that it can be transferred to the central location when it is convenient.

3.1. Components of the Portable Biometric Station

The PBS integrates all devices needed for the enrolment process into the rugged case. It includes fingerprint scanner, camera for capturing facial images, signature pad, laptop which runs the Enrolment Station application software, battery for independent power supply, cables and charges for battery and laptop.

Ruggedized case provides durable protection from impacts and environmental factors for the internal devices.

3.2. Components of the Enrolment Station

The Enrolment Station is a client-server application, where the server part runs all necessary hardware devices for capturing biometric data and the client part controls the workflow of the enrolment process, prepares the application records and submits it to the enrolment server or stores them locally.

The Enrolment Station consists of two applications. The first application is the Biometric Service Station (BSS) which initializes and runs all hardware components needed for acquiring applicant's data.

The other one is Enrolment Control Station (ECS) that is front-end application which controls the enrolment process.

3.3. Preparing Portable Biometric Station for Use

Rugged case and interior design provide protection and shock absorption to keep internal components safe from impacts and environmental factors. Portable Biometric Station is equipped with laptop, signature pad, fingerprint scanner and camera. Battery provides up to 8 hours autonomy for Portable Biometric station. It is equipped with power bar with built-in surge protection for battery and laptop charger.

Closed case ready for transport is shown in the Figure 1.

Figure 1. Closed PBS

Figure 2. PBS ready for Use

Devices integrated into the Portable Biometric Station are shown in the Figure 3:

1. Upper additional lighting for taking facial images
2. Camera for taking facial images
3. Lower additional lighting for taking facial images
4. Fingerprint scanner
5. Passive pen for signature pad
6. Signature pad

Figure 3. PBS components

4. ENROLMENT STATION APPLICATION

The Enrolment Station is an application software capable of acquiring biometric, and demographic data, for each person that is going to be introduced in the system. In the context of biometric system and Enrolment Station, the person whose biometric and other data are captured is an applicant, and in the forthcoming text, this person shall be referred as such.

Basically, there are two kinds of enrolment processes, attended and unattended. Attended process requires a trained officer who is going to guide the applicant through the process and who will guarantee that the process is performed correctly. Unattended process is self service process, where the applicant follows the instructions presented on the visual interface and all the actions are performed in an automated manner. The Enrolment Station operates in attended way. In this paper, the person who is leading attended enrolment process will be referred as the enrolment officer.

4.1. Starting the application

For the operation of the Enrolment Station, few preconditions must be met. After the Portable Biometric Station is prepared for use as described in the previous chapter, the laptop battery has to be charged and the Windows operating system on the laptop should be ready for use. Next step is starting the Biometric Service Station application. Biometric Service Station is application which configures and initialize all devices for acquiring biometric data from applicant. Biometric Service Station is running in the Console mode.

After the Biometric Service Station is successfully started, it is ready to receive requests from the Enrolment Control Station. Next step is to start the Enrolment Control Station.

When the connection between Enrolment Control Station and Biometric Service station is established, the Enrolment Control Station is started and application is ready for use.

4.2. Enrolment Process Workflow

Acquiring biometric and other data necessary for introducing the applicant to the biometric information system runs in a pre-determined workflow. The enrolment process workflow consists of several steps performed in a single pass. The enrolment officer can go back and forth among steps in order to create enrolment record. What must be fulfilled in order to create enrolment record is that each step is completed correctly and without errors. The workflow can be cancelled at any time, but with the loss of previously collected data. The workflow steps are:

– General data step

– Facial image data step

– Signature data step

– Fingerprint data step

Passing from one step to another will not lead to the loss of the previously captured data. After successful submission of the record, all captured data are cleared and the first step is displayed again, ready for the next applicant's enrolment process.

4.2.1. General data step

General data step provides form for the enrolment officer to enter demographic and additional data. Step with demographic data is shown in the Figure 4.

Every piece of demographic data has its graphical field on the screen for entering the actual data. The type of the field depends on the type of the data.

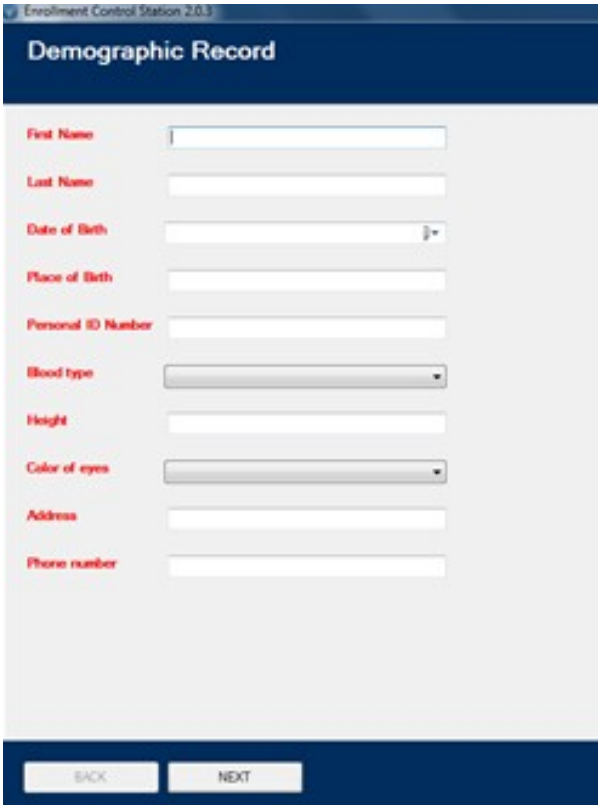

Figure 4. General data step window

Simple textual fields, where the officer can type in arbitrary text are aimed for entering following data:

– First Name
– Last Name
– Date of Birth
– Place of Birth
– Personal ID Number
– Blood type
– Height
– Color of eyes
– Address
– Phone number

Fields containing lists with predefined values of the data that can be selected are aimed for entering following data:

– Blood type
– Color of eyes

There is also field for entering only date:

– Date of Birth

All of the fields are marked as mandatory and they are in red color. That means that filed must be filled before submitting enrolment record. When the enrolment officer enters correct value in the field which is marked as red, the field will change its color to black.

4.2.2. Facial image step

Facial image step screen is shown in the Figure 5. This screen presents live preview from the camera on the left side of screen. The enrolment officer is able to see the position and expression of applicant placed in front of the camera and guide him/her to the correct position. Live preview is started and enrolment officer captures the facial image of the applicant. Live preview is stopped and captured image of applicant is displayed on the right side of the screen.

The software then tries to automatically crop the facial image according to the standards and if succeeds the cropped photo is displayed on the screen and the corresponding value is shown below the picture representing the quality of the image. If the automatically crop fails then the enrolment officer can do it manually using the green rectangle shown on the screen and adjusting the appropriate size.

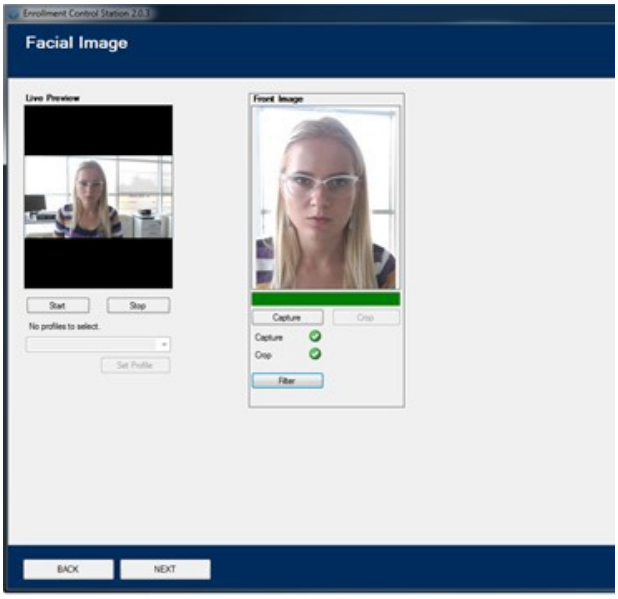

Figure 5. Facial image step window

After cropping the facial image, the enrolment officer optionally can select 1 out of 10 available filters. Each filter contains different values of brightness and contrast (Figure 6).

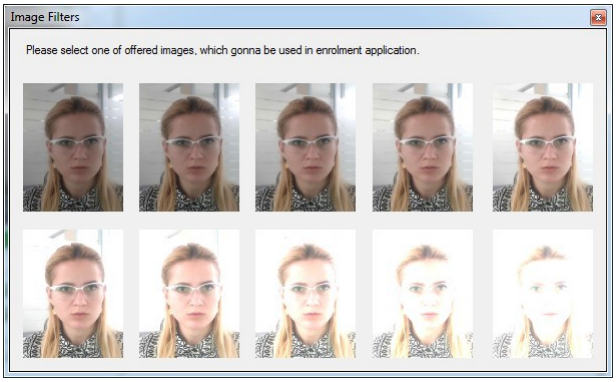

Figure 6. Available Image filters

4.2.3. Signature step

When Signature step is shown on the screen, the signature pad device is automatically set to capture applicant's signature. The enrolment officer should instruct the

applicant to sign on the pad, and when the process is done, the officer should capture the signature. The signature image is displayed on the screen (Figure 7).

Figure 7. Available step window

4.2.4. Fingerprint step

Fingerprints are captured using the fingerprint scanner. There are numerous types of scanners. The one used on the Portable Biometric Station provides capturing multiple fingerprints simultaneously. Left little finger, ring finger, middle finger and index finger are all together make the left slap and, accordingly, the same fingers of the right hand make the right slap. Both thumbs together are thumbs slap.

Figure 8. Fingerprint step window

To scan a slap, the officer should guide the applicant to put the fingers correctly on the scanner. First, the officer should perform the action for capturing the slap image. When the scanner is ready for scanning the applicant should put its fingers on the scanning area. After a few moments, slap image is displayed in the corresponding image box. The software automatically segments slap images extracting fingerprint images of each of the fingers and determines the quality of the images. This quality is important because the higher the quality is, the more accurate results of the later matching are. If the quality is above predefined threshold, the fingerprint is accepted. The slap segmentation and quality assessment are in progress after the slap image is displayed and the officer should wait for the results. Once the results are ready, each segmented fingerprint is displayed on corresponding image box below the slap image and the quality level is displayed.

If the quality of each finger is good enough the background of the quality result is green. Otherwise, the dialog with info message will be displayed and officer should repeat capturing procedure. Capturing the slap fingerprint image can be repeated as many times as needed in order to get a good quality of the fingerprints. Bellow the fingerprint image box there are additional information about the fingerprints which are requested by the enrolment process.

Applicant can have some of the fingers missing, or temporarily unavailable for scanning. In that case the exemptions have to be assigned for each unavailable fingerprint with the reason of exemption.

4.2.5. Submitting enrolment record

After all data are acquired, enrolment application record is ready to be submitted. Before the enrolment officer submits enrolment record, completeness and correctness of the data should be checked, especially the demographic data since typographic mistakes are very common in this case.

After the process is successfully submitted, officer is presented with confirmation window that contains the application number assigned to the submitted record, which can be used in searching for the application across the system (Figure 9). After the process is submitted, the enrolment data are cleared and the first step is displayed ready for the new enrolment process.

If submission fails, message is displayed informing about the failure and the reason that caused it.

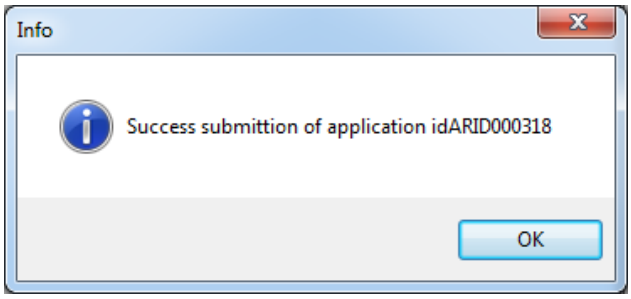

Figure 9. Submit done

4.2.6. Cancelling the enrolment process

The current enrolment process of an applicant can be cancelled at any time but any previously captured data will be lost. If the officer chooses to cancel the process, for any reason, all the data previously acquired are deleted.

5. PORTABLE BIOMETRIC STATION UPGRADES

The acquired data can be used for soldier identification system using the Automated Biometric Identification System (ABIS). The ABIS is a highly specialized system for identification which compares templates generated from probe biometric data (raw biometric data acquired from a person or another source) with templates of previously acquired biometric data stored in the database. Biometric modalities used for comparison can be physical, such as facial, iris, fingerprint, and hand geometry; or behavioral like gait, keystroke, signature, etc. Some modalities, like the voice, can be considered

both physical and behavioral.

One of the possible upgrades of the PBS could be to support iris recognition. Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person's iris. It is a form of biometric technology in the same category as face recognition and fingerprinting.

It allows law enforcement officers to compare iris images of suspects with an existing database of images in order to determine or confirm the subject's identity. Iris scans are quicker and more reliable than fingerprint scans since it is easier for an individual to obscure or alter their fingers than it is to alter their eyes. Iris scanning raises significant civil liberties and privacy concerns. It may be possible to scan irises from a distance or even on the move, which means that data could be collected surreptitiously, without individuals' knowledge, let alone consent. There are security concerns as well: if a database of biometric information is stolen or compromised, it is not possible to get a new set of eyes like one would get a reissued credit card number. And iris biometrics are often collected and stored by third-party vendors, which greatly expands this security problem.

In the future, the system can be upgraded to produce and issue electronic identification (eID) cards to the employees. The eID card holds the chip and can be used within access control system and to gain access to the military base. Only enrolled employees with issued eID card could access the military base.

Usually, the eID card contains the applicant's data. Facial image and demographic data are printed on the front side. The back page of the eID card consists of date such as the date of the card issuance, card number, issued by (authority name) and Machine Readable Zone (MRZ) [7]. MRZ consists of three lines of 30 characters and is created according to the ICAO 9303 standard [8]. The data stored within MRZ are Given name, Surname, Gender, Nationality, Issuing Country, ID number.

Figure 9. MRZ example

Among the numerous security data stored on the chip, it contains the same data stored within MRZ plus Facial Image, Fingerprints, Address, Martial Status, and Master PIN. Master PIN code is used for handling situations where the user PIN code is locked or the card is locked is locked due to the unsuccessful authentication.

This paper is written within Vlatacom Institute for the purposes of the project P105 as a part of the PhD studies.

5. CONCLUSION

Today, Biometric Identification Systems are an essential part of the modern society. Automated Fingerprint Identification System (AFIS) compares input fingerprint record (set of records) with fingerprint record (set of records) from database. Facial Image Identification System (FIIS) and it compares input facial image record with a fingerprint record or records from the database. The PBS developed and manufactured by Vlatacom Institute described in this paper, collects biometric data such as facial image, digital signature, fingerprints. The purpose of the PBS is to help authorities within military base to enroll employees and store the data in the central database.

References

[1] K.Sauerwein, T.B. Saul,D. W. Steadman, and C.B. Boehnen, "The Effect of Decomposition on the Efficacy of Biometrics for Positive Identification," J. Forensic Sci., vol. 62, no. 6, pp. 1599–1602, 2017, doi: 10.1111/1556-4029.13484.

[2] M. Zwanenburg, "Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law," Int. Law Stud., vol. 97, 2021.

[3] R. L. Sherman, "Biometrics futures," Comput. Secur., vol.11, no.2, pp.128–133, 1992, doi: 10.1016/0167-4048(92)90037-R.

[4] S. Mansfield-Devine, "Biometrics at war: The US military's need for identification and authentication," Biometric Technol. Today, vol. 2012, no.5, pp.5–8, 2012, doi: 10.1016/S0969-4765(12)70091-7.

[5] S. Chauhan, A. S. Arora, and A. Kaul, "A survey of emerging biometric modalities," Procedia Comput. Sci., vol.2, pp.213–218, 2010, doi: 10.1016/j.procs.2010.11.027.

[6] K. Phillips-Fein, The 9/11 Commission Report, vol.2007, no.97. 2007. doi: 10.1215/01636545-2006-022.

[7] Y. Kwon and J. Kim, "Recognition based Verification for the Machine Readable Travel Documents," He Статья!!, 2008, [Online]. Available http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.9373&rep=rep1&type=pdf

[8] P. Porwik, "The biometric passport. The technical requirements and possibilities of using," Proc. - 2009 Int. Conf. Biometrics Kansei Eng. ICBAKE 2009, no.2252, pp.65–69, 2009, doi:10.1109/ICBAKE.2009.14.