A Novel Approach for an Interoperable Biometric Verification

https://doi.org/10.3991/ijim.v12i6.9528

Mohamed El Beqqal(✉), Mostafa Azizi, Jean Louis Lanet
University Mohamed First Oujda, Oujda, Morocco
elbeqqal.mohamed@gmail.com

Abstract—Increasingly, safety is present in everyday life, at work, at home, in recreational environments, and in all places where there is a flow of people who share a common space. Using biometric fingerprint technique for identity verification has become a primordial due to the Reduced costs of implementation, maturity of this technology in the market and the ease of use. Many implementations exist using this technique , however, these systems are hard coupled with the environment in which they were developed and the hardware used to capture biometric data. Consequently, the interoperability issue is hard present in case of changing the environment or using new fingerprint reader. In this paper, we propose a new architecture to solve this problem by dividing the main biometric application to layers based on a flexible communication between components and supporting heterogeneous platforms and biometric readers.

Keywords—Fingerprint, Authentication, SDK, Interoperability, Biometrics.

1 Introduction

The fingerprint solutions represent the large part of the market for biometric processes. It is clearly the preferred solution for companies working in this field. The strength of this process is that the use of the fingerprint is generally easier to accept by the community and is one of the most effective and least expensive [1].

In spite of the large advantages offered by this biometric technique, many challenges remain an object of interest and field of study for researchers and companies such as the privacy aspect, the optimization of image enhancement algorithms and matching techniques. The technical solutions proposed by the companies including hardware and software allowing biometric recognition are largely diversified which result the existing of several biometric implementations that are strongly coupled to the architecture proposed by the supplier. Hence our proposal solves this interoperability problem.

The paper is structured as follows: Section 2, we present the basic information concerning the biometric fingerprint from classification to most used characteristic points. After this, we give an overview of the prominent issues in this field and we present the state of art of some academic biometric fingerprint implementations in which we discuss the issues existing in these systems. In section 5, we present the proposed architecture of our implementation. More precisely, we explain the role and communication

between each component's layer. In section 6, we discuss the obtained results. Finally, we conclude the paper with a conclusion and future works.

2 Basics on biometric fingerprint

A fingerprint is a drawing formed by the lines of the skin. It is found in different parts of the body. When we talk about fingerprints, we are referring to the lines of the skin of the fingers. This last are analyzed by a fingerprint reader to establish a numeric template.

Several classifications of fingerprint exist in the research field. As mentioned in [2], among the most used ones, we found the three main categories (Arch, loop and whorl) as shown in figure 1. Other sub-categories was listed by author in [3] deriving from the Henry classification which provides five classes of fingerprints .

Fig. 1. Fingerprint main categories

In addition to the singular points (core and delta points) which allow the determination of type of fingerprint, the characteristic points better known under the name of minutiae constitute the base of the process of matching between two fingerprints. Both of this technical information are extracted based on image processing algorithms.

A minutia is a point that is located on the change of continuity of the ridges lines. Among the most used characteristic points in the matching algorithms, we have the bifurcation ridges and ending ridges as indicated in [4]. Figure 2 shows the schema of these two minutiae.

About fifteen of these minutiae are enough to identify someone, but the level of precision can go up to 100 points according to the security context.

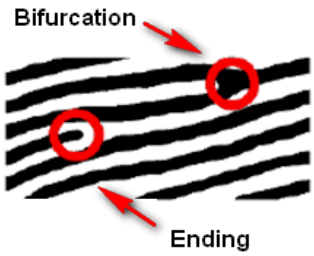

Fig. 2. Bifurcation ridge and ending ridge in fingerprint

3 Issues

The authentication using fingerprint technique has widely being used in various areas and domains including access control, attendance control and criminal investigation. However, despite of its large benefits, many concerns and challenges still being attracting more and more researchers aiming to implement a polyvalent identity verification system especially the interoperability, performance and security issues.

Interoperability is considered as a crucial issue since many system implementations for biometric verification and identification exist using several software and SDK required by the specific scanners available in the market. Performance can also be a key factor while the number of available records in database is important and the processing time of identity verification should not exceed a specific lapse of time. RFID technology can be an optimal solution for fast identification since the comparison is done by the ID which ensure unique identity, whereas no security and authenticity are guaranteed since the RFID tag can be possessed by another person.

4 Related works

Joseph Kalunga and Simon Tembo [5] have proposed a biometric fingerprint system for verification and vetting management. In this project, many features were modeled and implemented such as Criminal Vetting, Fingerprint enrolment,Criminal Investigation, Identity Verification. All these functionalities are implemented using specific System Development Kit (SDK) for U 4500 fingerprint reader using visual studio 2010 for implementing the backend verification functions. If we decide to use another reader which SDK provides only java interface, we will need to design new code for this application.

In [6,7], authors present a biometric fingerprint system for access control in university context. The verification process of fingerprint is done after a successful enrollment of student in database. During the authentication step, the collected finger print is matched with all fingerprint templates stored in database which can be a time consuming operation in case of a large number university database records. Author in [6] answers this need by combining RFID technology with biometric fingerprint to quickly identify the concerned template based on the appropriate RFID tag.

In [8], the classroom attendance system designed and developed by author aims to bring the portability aspect by using Arduino as a local processing unit which interacts with a mobile fingerprint reader. The student's data is stored in a memory card as encrypted templates. Furthermore, the author used the ZFM20 fingerprint scanner for finger identification to reduce the processing load on Arduino main processor. Besides the ZFM20 scanner will be also used for storing template in ImageBuffer area available in RAM space module as explained in [9]. However, no encryption or protection of the collected fingerprint was assured, since users can read and write in the buffer dedicated for storage using instructions. The storage of fingerprint's template in ZFM20 ImageBuffer and SD card in different format can cause a serious problem of redundancy and synchronization between the two.

5 Proposed system

In this section, we present the prominent ideas behind our system implementation

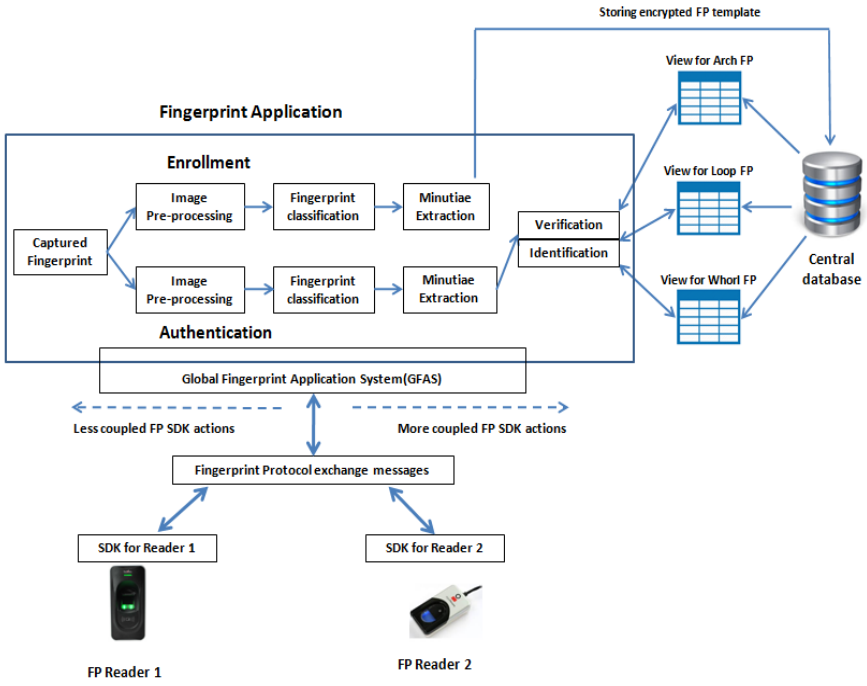

Fig. 3. Architecture of the proposed system

As shown in the figure above, the system is composed of 3 parts:

- Fingerprint Application (FA) and the global Finger Application System (GFAS)
- Database interaction
- Communication with fingerprint readers

5.1 FA and GFAS

The Fingerprint Application (FA) stands for the front-end and back-end parts developed by the user to manage a full authentication and enrollment based on biometric data collected from the readers.

The Global Finger Application System (GFAS) represents the main features used in a biometric fingerprint system. These features were collected based on many exiting implementations of fingerprint verification system. Among the most common actions we have:

FP capture: This action consists of scanning the live finger to get a digital image in a specific format depending of the scanner supported image extension. We noticed that the BMP format is widely used in several SDKs specifications.

FP pre-processing: Many image processing steps can be done to the captured finger from normalization, thinning to binarization. These three transformations are primordial for each initial finger image. However other steps could be performed to produce a best image quality.

***Minutiae extraction*:** At end of this step, a template is produced containing the information about characteristic point. Each of the representation in minutiae template is covered by various standards such as ANSI-NIST and ISO/IEC 19794-2 which ensures the interoperability of the different recognition algorithms as mentioned in [10].

***FP enrollment*:** The Fingerprint enrollment step in which the template obtained from minutiae extraction is encrypted and saved in central database. The quality of this captured fingerprint is considered as critical since all the upcoming verifications will be done based on this model. This point justifies the fact that most of the finger biometrics systems are based on three attempts capturing finger to recover the most accurate image.

***FP identification*:** TheFingerprint identification consists of comparing the captured Fingerprint template with all instances exiting database until we obtain a satisfying-matching score.

FP verification: The verification step is special case of identification when the matching is done between the live Fingerprint template and a specific template in database that have already been identified.

5.2 Database interaction

As shown in figure 3, our storage model consists on the central database which is directly called only during the enrollment process. In this step, the database is less solicited since the registration will consist on inserting a new record in the appropriate database table. However, the time dimension can be crucial during the authentication process mostly if the database contains thousands of biometric records.

For this purpose, we propose in our system to use database views which are created depending on the fingerprint classification considered. More precisely, we use materialized views to store physically the biometric records as presented in [11]. The number of views depends on the chosen classification. For example, we have created three materialized views which will reduce the matching time during the identification process.

Here, if the person has a loop fingerprint, the process of searching and matching will consider only a specific part of database. Furthermore, the database is kept hidden and not exposed during the verification of fingerprints since we customize materialized views to be accessible only for reading.

5.3 Communication with fingerprint readers

In this section, we will present the communication between the three layers:

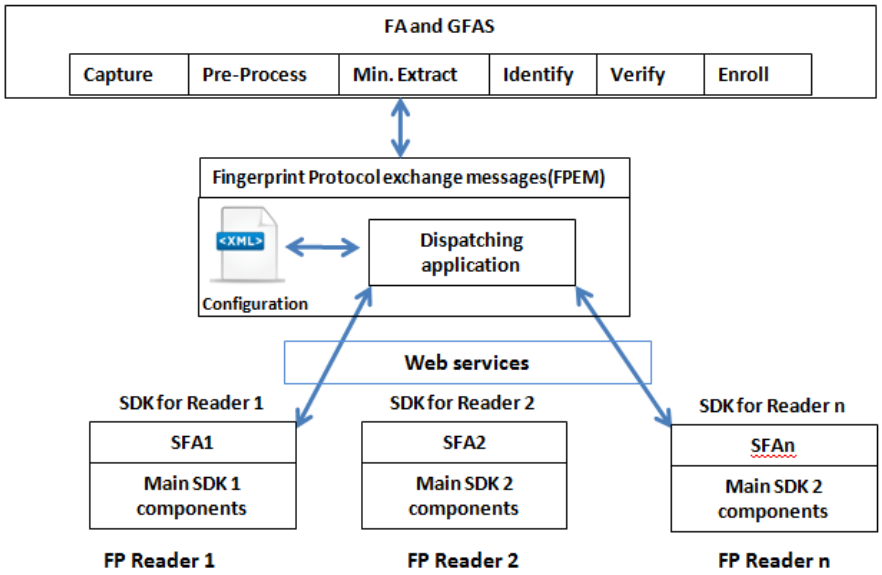

Fig. 4. Communication between BA and FP readers

As shown in figure 4, when the Fingerprint Application (FA) triggers an action which is already specified in the Global Finger Application System (GFAS), this action is expressed in form of high level message able to be treated only by the FA methods and independent of the type of the SDK used to execute this action. For this purpose the FA will call an intermediate layer FPEM using web services. This layer consists of application which take as input some parameters as action to be executed, reader to use and other optional attributes. The data concerning each reader is specified in an XML file. This last contains rooting and information to communicate with the SDK layer. For example, the configuration file will contain the port number, IP address and the web service to call depending on action coming from FA layer. Once the information is gathered, the FPEM main application will dispatch calls to SDK layer.

As indicated in figure 4, for each reader we have the main SDK components that consist of technical objects allowing the physical communication with the reader. Some companies offers DLL (Dynamic Link Library) libraries based on Windows execution, others offer JAR (Java Archive) files requiring JVM(Java Virtual Machine) environment and others systems can be supported by the SDK. To answer to this

interoperability problem, for each reader used in our system, a Specific Fingerprint Application (SFAi) will be developed. The main goal of SFAi is to capture the web service request from FPEM application and convert the incoming message to specific message supported by the SDK which will be used in its turn by the methods offered by the SDK library.

6 Results and Discussion

The system implementation presented above provides many advantages from flexibility, performance, scalability and interoperability:

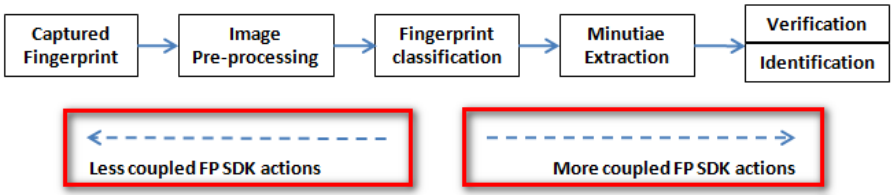

Fig. 5. Fingerprint processing steps

The flexibility aspect is shown on the possibility to use relevant actions of the reader to make profit of the optimized methods and algorithms of fingerprint processing and communication with the reader. However, the more we make use of the reader SDK features, the more we will be coupled to this last as shown in the figure 5. For example, in our implementation, we forecast the use of the reader for scanning the fingerprint and image pre-processing to get a binary image, since the classification is not supported by all fingerprint readers and the minutiae extraction provides several templates format that are not common for all readers. Besides, with this implementation, we ensure a performance coming from the reduced number of matching operations due to the use of materialized views resulting from the fingerprint classification used for storage.

The scalability aspect is ensured with the ease of adding a new fingerprint device to the system. This step consists in adding a new record in the configuration XML file in the FPEM layer. In addition, a SFAi should be developed to convert the incoming requests to a comprehensible actions for the SDK. Using this mechanism allows to make use of several readers supporting heterogeneous languages such as java, c# and others in an interoperable biometric system.

7 Conclusion

In a situation where institutions aim to use different biometric fingerprint readers for identity verification, each scanner requires its own application design and development. In order to answer this need and unify system functional authentication process, we have proposed a new architecture based on intermediate middleware layer which will abstract the main biometric authentication solution from the technical hardware

specifications. Furthermore, the proposed system is designed to be adaptable for adding biometrics readers in the system. In addition, we have optimized the database model design and interaction during the biometrics matching process. As a future work, we aim to continue on the implementation of our system architecture and validate our solution by real test cases.

8 Acknowledgement

This research is performed inside the MATSI Lab., ESTO, University Mohammed First, Oujda (Morocco).

9 References

[1] A. N. Kataria, D. M. Adhyaru, A. K. Sharma, and T. H. Zaveri, "A survey of automated biometric authentication techniques," in 2013 Nirma University International Con-ference on Engineering (NUiCONE), 2013.

[2] K. Sasirekha and K. Thangavel, "A novel fingerprint classification system using BPNN with local binary pattern and weighted PCA," International Journal of Biomet-rics, vol. 10, no. 1, p. 77, 2018. https://doi.org/10.1504/IJBM.2018.090133

[3] M. Galar et al., "A survey of fingerprint classification Part I: Taxonomies on feature extraction methods and learning models," Knowledge-Based Systems, vol. 81, pp. 76–97, Jun. 2015. https://doi.org/10.1016/j.knosys.2015.02.008

[4] Q. Gao and D. Pinto, "Some challenges in forensic fingerprint classification and inter-pretation," in 2016 IEEE Long Island Systems, Applications and Technology Confer-ence (LISAT). 2016.

[5] G. B. Iwasokun, O. C. Akinyokun and O. J. Dehinbo, "Minutiae Inter-Distance Meas-ure for Fingerprint Matching," International Conference on Advanced Computational Technologies and Creative Media (ICACTCM),pp. 1-7. 2014

[6] J. Kalunga and S.Tembo "Development of Fingerprint Biometrics Verification and Vetting Management System," American Journal of Bioinformatics Research, Vol. 6 No. 3, pp. 99-112. 2016

[7] M. El Beqqal, M. A. Kasmi, and M. Azizi, "Access Control System in Campus Com-bining RFID and Biometric Based Smart Card Technologies," in Advances in Intelli-gent Systems and Computing, Springer International Publishing, 2016, pp. 559–569

[8] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani, and V. K. Mittal, "Fingerprint bio-metric based Access Control and Classroom Attendance Management System," in 2015 Annual IEEE India Conference (INDICON), 2015. https://doi.org/10.1109/INDICON.2015.7443699

[9] N. I. Zainal, K. A. Sidek, T. S. Gunawan, H. Manser, and M. Kartiwi, "Design and development of portable classroom attendance system based on Arduino and fingerprint biometric," in The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), 2014.

[10] H. Zhian , Technologies Co., Ltd (2008). "ZFM-20 Series Fingerprint Identifica-tion Module User Manual, " Retrieved April 15, 2018 from http://www.adafruit.com/datasheets/ZFM%20user%20manualV15.pdf

[11] B. J. Wing, "The ANSI/NIST-ITL standard update for 2011 (data format for the inter-change of fingerprint, facial and other biometric information)," International Journal of Biometrics, vol. 5, no. 1, p. 20, 2013. https://doi.org/10.1504/IJBM.2013.050731

[12] Docs.oracle.com. (2018). "Materialized View Concepts and Architecture". Retrieved April 23, 2018 from https://docs.oracle.com/cd/B10500_01/server.920/a96567/repmview.htm.

10 Authors

Mohamed EL BEQQAL graduated from ENSAO (National Higher School for Applied Science, Oujda) with a degree of state engineer Software Quality in 2011. He is currently a Ph.D. candidate at MATSI-Laboratory/ Mohammed First University of Oujda, B.P. 524, 60000, Oujda, Morocco under the supervision of Pr. Mostafa AZIZI. His research focus on: RFID, Biometrics, Internet of things, Access control, identification, authentication. (e-mail: elbeqqal.mohamed@gmail.com)

Mostafa AZIZI Ph.D., Ing, Professor, MATSI-Laboratory, ESTO, University Med 1st, Oujda, B.P. 524, 60000, Oujda, Morocco. His researches focused on: Verification/ CoVerification, Testing, Computer Security, Software Development, Hardware/Software Systems. (e-mail: azizi.mos@ump.ma)

Jean Louis Lanet Ph.D. He is member of the Tamis research team at INRIA-Rennes where he manages the LHS. His researches focused on: Security of small systems like smart cards and software engineering. (e-mail: jean-louis.lanet@inria.fr)

Article submitted 11 September 2018. Resubmitted 20 October 2018. Final acceptance 21 October 2018. Final version published as submitted by the authors.