A Novel Secure Fingerprint-based Authentication System for Student's Examination System

Abdullah Alshbtat[1], Mohammad Alfraheed[3]
Department of Computer Science and Information
Technology, Faculty of Science
Tafila Technical University, Tafila, Jordan

Nabeel Zanoon[2]
Department of Applied Science
Al-Balqa Applied University
Aqaba, Jordan

***Abstract*—In the fingerprint image processing, various methods have been suggested as using band pass filter, Fouries transform filter and Fuzzy systems. In this paper, we present a useful and an applicable fingerprint security system for student's examination using image processing on such away and a well-organized algorithm is applied. As a university team work, we have recently tested this security procedure for different samples of students in our institution. The experimental results show a high level of accuracy is obtained. Due to the need to connect and manage the connection, we use the Ethernet card and the Arduino Uno card which they are combined together in such a way to do so. Moreover, the administrator runs a special website in the PC to assign ID to the scanned fingerprint. The calculation of the proposed system is carried out by uploading a suitable Adafruit fingerprint library to the used Audruino Uno card. Finally, the most important security point is that the PC has been used not only to send the developing software into the Uno card but also to disconnect the process electronically while the code is running.**

Keywords—Finger-print; examination system; image processing; bio informatics

I. Introduction

The authentication plays an important role in examination systems. The most authentication approach applied in those systems is identity- based authentication. However, the reality in a lot of developed examination system is that the identity-based authentication is not enough to verify the student identification.

One of authentication solutions is the biometric processing based on iris or fingerprint data. Because of cost related issues, fingerprint has been adopted as an automatic data analysis for identification. The main difference between the password-based authentication and fingerprint based authentication is that the first one cannot sometimes protect from unauthorized accessing to users data especially in examination based website applications. Using the fingerprint data does not mean that the examination system avoids using the password-based authentication. In addition to the password-based authentication, the examination system has to be boosted therefore by biometric process such fingerprint data.

Several advantages were found by using fingerprint. The simplicity of using fingerprint as a method to verify and prove the student identities helps allowing in entering the exam. In other hand, the high level of accuracy offered by each single unique human fingerprint helps to prevent any method for identity theft. The unlimited capacity of fingerprint sensors as advantage related to conversion each fingerprint to an image, where latterly it processed in the database. The portability of the fingerprint sensors considered as advantage because of the small device with the tiny components.

The fingerprint-based system offers usually a reliability of such systems with different challenges. Using an external database, however, affects the efficiency of fingerprint-based system. Furthermore, the commercial devices developed by the fingerprint have been constructed to store the fingerprint features for limited users. Those devices have been developed also as an individual unit with their own interface and database, once the user places the fingerprint confirmation message arisen on the output screen without other details (text or password). Another challenge related installation process where the commercial device has to be fixed in a place and connected to the facility networks, where the data transfer to and from the database server. This process increases the cost and chance of hacking. The security web services developed for the examination system represents another challenge. These services could be a promise way to improve the security of examination system once it addressed with biometric processing such as fingerprint.

In this work, a novel secure fingerprint-based authentication system has been developed to discuss these challenges in context of web services. The developed system has been developed to further ensuring for usability, confidentiality and portability of such fingerprint based system.

II. Related Works

Identity authentication considered a topic of interest in the recent years, while increasing the need for more reliable and useful identity authentication systems for security [1]. The old traditional authentication systems depend on using passwords or ID cards found to be less reliable [2]. Indeed, the traditional authentication systems are not able to recognize the original person from the cheater using the password [1].

The case of how to improve the security in conjunction with increase usability and decrease interventions still under work [3], so in order to reduce such negativity related traditional authentication systems biometrics was used.

Biometrics is the physiological and behavioural characteristics that can be measured in the human body and used to confirm the identity and differentiate it from others [4] such as fingerprint. The strength of such biometric methods come from the inability to be stolen or lost as well as difficult to be faked [3].

Managing authentication is a very important activity by fingerprints in order to ensure the integrity, accelerate the process, decrease error rate and fasting verification process, where in a study reviled that time needs for students attendance verification using manual process 23.66 second per student, more than 6.65 second using fingerprint [5].

The most common mechanism for biometrics authentication systems consist of two phases [6]. The enrolment phase used in collecting data and mathematically analyzed it using specific algorithms to perform a data base. The releases phase that interest in comparing and verifying the identity. The general scenario for scanning the figure by using sensor based on capturing two main fingerprint characteristics; the valleys and ridges [7].

Several reasons were considered as advantages for using fingerprint for authentication. The easy to apply is the most important one; the low cost of the uses device as well as don't need much power [6]. Although of the different advantages for fingerprint some disadvantages presented with the complexity in obtaining high quality images of finer patterns related to present of tear, dirty and cuts of finger which will affect the accuracy, time of response and reliability [6].

In order to enhance fingerprint authentication system, different approaches have been deployed in authentication system, where they in other hand have been fused in fingerprint systems for indoor localization [8] by analyzing each indoor algorithms to use the strengths and step down the weakness points to build the best systems.

In other hand, effective identity authentication should be available for wireless networking. So a new robust authentication algorithm based on the phase noise fingerprint of the physical-layer was built [9]. As well as a security authentication scheme of combined physical-layers fingerprints to ensure the survivability of the network from attacks [9].

The security associated with fingerprint-based system is an important issue to be taken inconsideration.

Fingerprint-based system has been addressed in different applications. It was designed for ATM accesses, computer network accesses, class room entering and building door looks [10]. Fingerprint authentication system presented also in mobiles and smart devices where some security insights on touch dynamic provided [3]. New technique by using 3 dimensions magnetic finger motion pattern based implicit authentication to provide highly accuracy was used in smart phones [11], [12].

For attendance checking, the used system built based on fingerprint technology bonded with GPS presented in smart phones to check user availability at anywhere [12]. In very large countries like India, fingerprint-based system was used as a voting system for all population by removing the geographical constrains [13].

Using fingerprint as an access control in information systems depends usually on user awareness and acceptance. User could choose one of two categories of fingerprint-based system on the measurements. Unimodal systems uses only one finger mostly the index (14), which proposed for low/medium security places. Multi modal systems uses two or more fingers for authentication, mostly using the index and middle one, where it consider preferable for medium/high security items [14]. These systems found to be best related to low error rates and high efficiency.

A multi-intance fingerprint based authentication system has been developed which consider more invincible to different problems encountered in previous systems using the crossing number technique [15]. The developed system considered highly efficient in verification the user with highly accuracy and low run time. Also, the system provides the flexibility to switch from multi-intance to unimodal in case of fault tolerance in order to preserve their independency [15].

Indeed, the fingerprint based authentication system developed to possesses the features of highly reliable and easy for secondary development, as well as having several advantages such highly secure, highly accurate, easy in use and being standardized make it applicable in different areas needs authentication such as educational institutions, factories, offices, security and access control systems [16].

III. Design of Proposed System

The fingerprint-based system has been developed in the context of examination system. Two phases have to be carried out; registration and verification.

A. Registration Phase

In this phase, the user (i.e. the student) is requested to add the fingerprint in the database. The fingerprint is previously processed to extract its features in which the fingerprints are uniquely distinguished from each other. A website interface is firstly assigning the user's Identifier UI (i.e. the university student number) to the scanned fingerprint. Once the administrator send on order to scan the fingerprint, a secure connection is established between the front interface and the proposed device of the fingerprint-based system. In addition, a random password-based text is generated and assigned to the user identifier. The proposed system is then activated to start the scanning process.

The user has to follow the prompt massages shown in the LCD screen. The secure established connection which automatically disconnected when the scanning process is activated. Another connection is established between the proposed device and the target record at the database. Both the fingerprint features and the random password are integrated into the user's record. The operation of the registration phase is given as follows:

- The user (i.e. student) U_i is given his identifier. The identifier represents the university student number STD.
- A random password is computed R_i = Rand(U_i).
- U_i imprints his finger print FPion the sensor.
- Compute ID_i=h(FP_i),where h(.) denotes one way hash function which is used to convert the FP_i to identifier.

- 5. Compute $Rec_i= U_i+ID_i+R_i$
- 6. Reterive Rec_i*from the DB, $Rec_i*= (U_i, ID_i, R_i)$
- 7. Rec_i* ?= Null
- 8. Store Rec_i at the Database DB, iff $Rec_i* = Null$

B. Verification Phase

Within this phase, the main target of the proposed system is offered. Two scenarios have been introduced to double check whether the user has been authorized to access the examination system or not. First, the student has to imprint his fingerprint via the proposed system. Then the password shown on the LCD screen; if the user has the access permission, otherwise the proposed system has to display access denied. In the second scenario, the proposed system has been developed to be directly connected with login page of the examination system. Once the student is successfully given the access permission, the exam page is automatically activated for the student. His details are also shown in the exam page. In order to ensure the security issue both scenarios have been developed to open a secure connection once the proposed system is enabled to connect with the database. The database is required to disconnect the connection after the response is sent to the proposed system.

The suggested scenarios are expected to be run. Both of them are initiated by the student who imprints his fingerprint on the sensor. The following operations are therefore carried out:

- Compute $ID_i* = h (FP_i)$.
- Compute $C = h (ID_i*+ T)$ where T is the current timestamp of the login process.
- Retrieve the Rec_i from the database, where $Rec_i = (U_i, ID_i, R_i)$.
- If $(ID_i \neq ID_i*)$, the system reject the retrieved $Rec_{i.}$
- In first scenario, the system sends a prompt message $M=(R_i)$ to displayed on the LCD screen.
- In second scenario, an activated order is sent to the login page order= (U_i, R_i) for authentication process.
- Compute $C'=h(ID_i*+T')$ where T' is the current timestamp for receiving the activated order.
- If $(C'-C) \geq \Delta T$, where ΔT is the expected valid time interval for transmission delay, the login phase has to reject the activated order. This kind of timestamp is for double check and to protect the proposed system from attackers.

IV. System Description

The idea of the fingerprint-based examination system has been introduced while the computerized exam was running. Some of students were trying to do the computerized exam instead of his colleagues. Since the password was previously given to student, it is easy to exchange their passwords while the exam's advisor is distracted. Furthermore, the student could sometime impersonate his colleagues.

When it came to designing a fingerprint-based system, some non-functional requirements have been taken in our account. They are Simplicity, Probability, Security and Flexibility. The proposed system has been developed to be directly connected to the administrator's PC. An Ethernet card has been add to the system for managing the network connection. In addition to the fingerprint, LCD screen has been fixed in the proposed system, which is used as an output screen. These entire components are connected to the Arduino card which works as the system brain.

A. Hardware Implementation

As shown in Figure 1, the components of the proposed system have been installed and fixed with each other. These components have been connected into the Arduino Uno card via the appropriate Pins (i.e. Pin 1 to Pin 14). The Ethernet card has been fixed above the Uno Arduino card due to the need to control and manage the connection with the administrator's PC and the need to save more space. Making the proposed system more secure against the attackers, the PC has been used not only to send the developing software into the Uno card but also to disconnect electronically the connections (via Ethernet card) while the code of the proposed system is running. Moreover, the administrator runs special website in the PC to assign ID_i to the scanned fingerprint.

B. Software Implementation

The adafruit fingerprint sensor Library has been downloaded from the RET. The library has been uploaded to the Arduino card which, in turn, controls and manages the operation and calculation of the proposed system. The library has also developed to use the Ethernet card in the network connection. The Arduino card has been also provided by a developed code to show the user's identifier, the user's password and the prompt messages.

The main purpose of the proposed system is to control and manage the attendance procedure of students in the examination class room. Therefore, two hypertext preprocessor (PHP) pages have been developed as shown in Figure 2.

The login page has been developed to provide the proposed system by User's identifier (ID_i), User's name, User's Password (R_i), once the administrator presses the scan button, the page start the scanning process as shown in Figure 3.

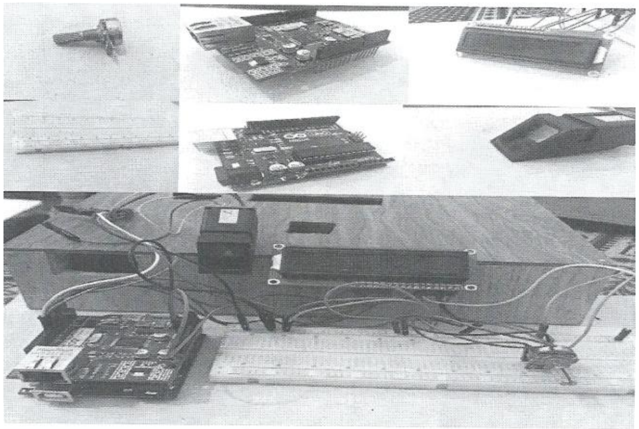

Fig. 1. Components of Fingerprint-Based System.

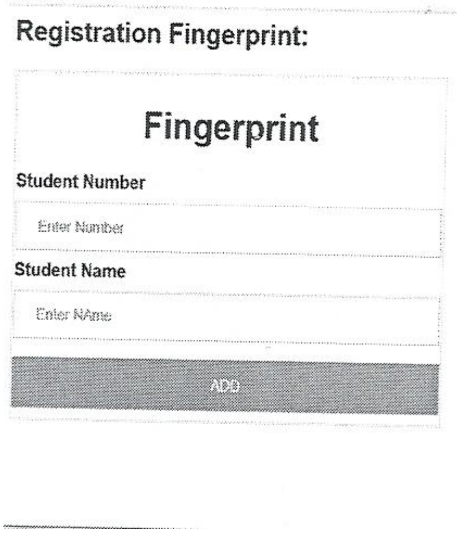

Fig. 2. Registration Page.

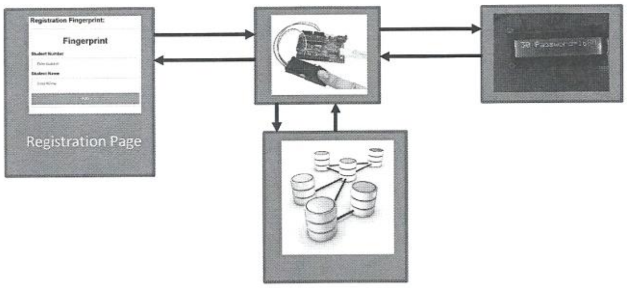

Fig. 3. Scanning Process.

The Login page as shown above has been developed to start the scan process again. However, the Login page sends an order to retrieve the user's identifier and user's password from the database via the proposed system. Therefore, other commands have been developed and uploaded into the Arduino card to communicate with other components of the developed system.

V. Network Security

To ensure a secure network connection, the Ethernet card has been used as a firewall. Moreover, the Ethernet card has been installed to be only connected with the Administrator's PC. Since the proposed system has been introduced as an authentication system for the examination system, the core of the proposed system will be an interested target for attackers. Once the PC is activated to send or receive data from the proposed system, the Ethernet card is enabling to build a secure connection between the proposed system and the PC. After deactivation is the communication is automatically and immediately dissolved. This mechanism aims to separate the proposed system from surrounding and keep it in touch only with the PC. In this way, the proposed system could ensure the network security by accepting the activation order given only by login page or registration page. In other hand, the link of the URL is stored in the SD memory where the server sends a request to retrieve it when needed.

VI. Result and Discussion

Here, the proposed system has been tested and the results has been monitored and collected. First of all, the functionality of the individual components (i.e. device of the proposed system) has been successfully verified while the proposed system was running either in registration and verification phase. Then the proposed system has been tested as a whole for any error. The test has been carried out using the code of Arduino and the initial parameters have been passed via the Ardiuno's interface. Consequently, the proposed system has be successfully constructed and run.

As for fingerprint testing, the proposed system has been run in different conditions. The testing has been carried using 30 users. The proposed system has been connected to the normal (i.e. Core i3). As presented in Table I below, during the testing one user has been asked to place the fingerprint partially on the fingerprint sensor. The proposed system failed to recognize the fingerprint's features and did not successfully read the fingerprint. In addition, the captured image of the fingerprint does not include the main features so the verification failed as (case 2). A female student interested in using beauty cream, therefore, the proposed system failed when the finger was very oily to scanned and verified (case 3). Usually the male students tend to do hard life duties, so in (case 4) the fingerprint was partially disappeared as shown in Figure 4 The proposed system failed detecting the fingerprint as well as the verifying. For the remaining 27 samples which presented with normal case in printing processes, they have been successfully tested by the proposed system.

In general, the proposed System seems to get successfully threading when the Finger is less Dirty, Oily or wet. Using the tested cases (i.e.30 students), the proposed system claims to have more than 99% accuracy rate. As for the failed cases (2,3,4), it can be solved by using another fingerprint from the user's hand. In case all user's fingerprint are failed to be registered in the proposed system, the pass can be traditionally using the user's password.

TABLE I. Results of Proposed System

Number of students	Case 1	Case 2	Case 3	Case 4
30	27	1	1	1

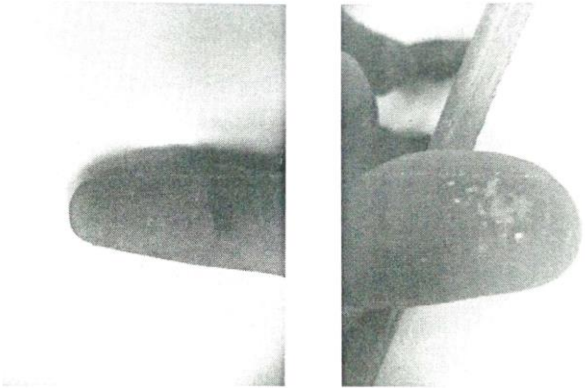

Fig. 4. Burned Finger.

In comparison with other different devices, the proposed system recognized itself from others by different characteristics. Portability which means the capability to move the device from one place to another is applicable in the proposed system so it easy to use indoor and outdoor places not like others used inside doors only [13],[17],[18].

The simplicity of the proposed device affects its ease of development by different institutions where the approximate manufacturing cost around 100 dollars. This simplicity makes it cheaper as well as it is compatible with the android system "open source", on the contrary with other different systems considered expensive and mainly used paid operating system [18], [19].

Connections with external networks done by the control PC (lap top) only which consider the first wall protection that increase the security for the proposed device. In other hand, other devices depend on connecting the fingerprint device to the external networks using network card, which could affect the security and make them high risk to breakthrough [19],[20]. Furthermore the proposed device depends on a temporary communication channels with the device to send and receive biometric data, after that the system disconnect immediately so become harder to hack.

VII. Conclusion

This research work discussed in detail fingerprint pre-processing, minutiae extraction and minutiae matching. This research work has been able to provide a physical security and authentication for students before entering the class room. The experimental result shows efficient registration and verification of subjects with accuracy over 98%.

Acknowledgment

Special thanks are given to our students Mohammad Abu Osbah and Almuthna Alsaide for their efforts in items installation. Moreover, we would thank the president of Tafila Technical University for his financial support.

References

[1] J. Zhou, G. Su, Ch. Jiang, Y. Deng, C. Li (2007). A face and fingerprint identity authentication system based on multi-rout detection. Neurocomputing, 70(1): 922-931.

[2] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Z. Fardi, S. Samad (2018). Authentication systems: A literature review and classification. Telematics and Informatics, 35(5): 1491-1511.

[3] P. Sh. Teh, N. Zhang, A. B. J. Teoh, K. Chen (2016). A survey on touch dynamics authentication in mobile devices. Computer and Security, 59(1): 210-235.

[4] M. H. Hammad, A. Mohammed, M. E. Eldow (2015). Design an electronic system use the audio fingerprint to access virtual classroom using artificial neural networks. International conference on computer, communications and control technology (14CT), Kuching,1(1): 192-195.

[5] I. A. Justina (2015). Fingerprint-based authentication system for time and attendance management. British journal of mathematics and computer science, 5(6): 735-747.

[6] I. M. Alsaadi (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: a review. International journal of scientific and technology research, 4(12): 285-289.

[7] A. Suganya, G. M. A. Sagayee (2015). A Delaunay pentangle-based fingerprint authentication system for preserving privacy using topology code. International journal of research in engineering and advanced technology, 2(6): 142-149.

[8] M. Chiputa, L. Xiangyang (2017). Real time Wi-Fi indoor positioning system based on RSSI measurements: A distributed load approach with the fusion of three positioning algorithms. Wireless personal communications: An international journal, 99(1): 67-83.

[9] C. Zhao, M. Huang, L.Huang, X. Du, M. Guizani (2017). A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. Computer networks, 128(1): 164-171.

[10] D. Sunehra (2014). Fingerprint based biometric ATM authentication system. International journal of engineering inventions, 3(11): 22-28.

[11] Y. Zhang, M. Yang, Z. Ling, Y. Liu, W. Wu (2018). Finger auth: 3D magnetic finger motion pattern based implicit authentication for mobile devices. Future generation computer system (ISSN 0167-7399).

[12] B. Soewito, F.L.Gaol, E. Simanjuntak, F. E. Gunawan (2015). Attendance system on android smart phone. International conference on control electronics, renewable energy and communications, Bandung, pp: 208-211.

[13] D. Khojare, V. Chaudhary, M. Malviya, Sh. Shukla (2018). FPKIVS-A stellar approach to voting systems in India. Advances in intelligent systems and computing, 653(1).

[14] S. Ribaric and N. Pavesic (2008). A finger based identification system. The 14th IEEE Mediterranean electrotechnical conference, Ajaccio, pp: 816-821.

[15] A. Llugbusi and A. O. Adetunmbi (2017). Development of a multi-intance fingerprint based authentication system. International conference on computing networking and informatics (ICCNI), Lagos, pp: 1-9.

[16] P. Sana, Sh. Prajakta, P. Kamini (2017). Fingerprint based exam hall authentication system using microcontroller. International journal of engineering researches and management studies, 4(2): 89-91.

[17] B. Molina, E. Olivares, C. E. Palau, M. Esteve (2018). Amultimodal fingerprint-based indoor positioning system for airports. IEEE Access, 6(1): 10092-10106.

[18] K. Chow, S. He, J. Tan, G. Chan (2019). Efficient locality classification for indoor fingerprint based systems. IEEE Transactions on mobile computing, 18(2): 290-304.

[19] J. J. Stephan, S. A. Abdullah, R. D. Resan (2017). Use fingerprint technology in developing country security. Annual conference on new trends in information and communications technology applications, Baghdad: 57-62.

[20] J. Baidya, T. Saha, R. Moyashir, R. Palit (2017). Design and implementation of a fingerprint based lock system for shared access. IEEE 7th annual computing and communication workshop and conference, Las Vegas: 1-6.