Defining a Pilot Experiment to Enhance Exam Registration with Fingerprint Biometrics

Rupa Patel[a], Li Meng[a], Moises Diaz[b,c]
[a]University of Hertfordshire, Hatfield AL10 9AB, UK
[b]Universidad de Las Palmas de Gran Canaria, Spain
[c]Mid-Atlantic University, Spain

ABSTRACT

Remembering passwords, queuing to get identified by a human and carrying tokens such as ID cards are conventional approaches to authentication. With advances in biometric technologies and increased acceptance of such technologies, the conventional approaches are being gradually replaced by biometric technologies such as face, fingerprint and/or voice recognition. This paper defines an experiment to investigate how fingerprint technology can be used to enhance the exam registration and attendance monitoring processes in an educational setting, where efficiency and accuracy are crucial, but the conventional approach fails to deliver either. The findings and results of our pilot study are challenging and they are derived from a novel research project led by the authors in a University environment.

Keywords: Fingerprint Recognition, Biometrics, Exam Registration, Attendance Monitoring.

1. INTRODUCTION

Fingerprint recognition is the first biometric system, which was established in the 1800s and initially utilized in crime investigation. In recent years, fingerprint technology has undergone an extensive research and development effort. Its applications have extended beyond crime investigation to the areas such as banking[1], location tracking[2] and flight check-in[3], just to name a few. Fingerprint sensors have been embedded in mobile phones[4], portable devices[5] and ATM machines[6] to re-place passwords and PINs.

This paper presents an innovative application of fingerprint technology in an educational setting with the aim of revolutionizing its exams and attendance monitoring processes.

Fingerprint presents a good balance of the desirable properties of a good biometric modality: Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability and Circumvention[7] [8]. Fingerprint has a low introduction and implementation cost compared to the other highly accurate biometric techniques such as iris, retina or DNA.

It has been widely recognized that fingerprint has high performance, permanence and distinctiveness. The medium acceptability of fingerprint is due to the fact that it was initially used mainly in crime investigation. As the size and cost of fingerprint scanners drops, fingerprint techniques have been adopted in various applications and its acceptability has increased noticeably especially with young people. In this paper, we discuss a preliminary work about the potential use of fingerprint technique in enhancing the exam registration and attendance processes within a university environment where the target users are typically within the age range of 21 to 35. As con-firmed in our pilot survey results, the acceptance of fingerprint is high with this user group. The universality and collectability of fingerprints tend to experience issues with children, elderly population and those who use or wash their hands a lot (e.g. builders or surgeons). However, these presents no challenges with the vast majority of university students. Considering the above, we have chosen fingerprint technology as the biometric replacement of current ID cards for the exams and attendance monitoring processes.

The structure of the rest of this paper is as follows: In Section 2, the authors dis-cuss issues faced by the current ID card processes, Section 3 provides a technical overview of the proposed system, Section 4 outlines the results from a survey issued, Section 5 presents proposed solutions to issues faced by fingerprint technique and Section 6 concludes this paper followed by acknowledgements and references.

ISBN: 978-84-697-7101-3

2. THE CURRENT PROCESSES AND THEIR ISSUES

Using tokens, passwords or PINs does not only cause an inconvenience to the user when damaged, forgotten, lost or stolen but also raises data security issues if it is duplicated or gets in the hands of an unauthorized user.

Currently, the exam registration process involves manual checks of the IDs where the invigilator has to check the photograph on an ID card to see if it matches the face of the cardholder presenting the ID card. The ID check results are firstly recorded on paper by the invigilator. When additional candidates are verified, their details have to be recorded on a paper form as well. This paper-based process is time consuming and not always reliable. Training of invigilators and exam office staff as well as post-exam processing of forms all add to the costs. In addition, human error can cost not only time and money, it can also have a huge impact on the individual being affected.

When a student forgets to bring his/her ID to the exam, they are required to visit an administration office to get a temporary ID slip. Replacing lost ID cards or getting a temporary one can also be time consuming especially when the exams are due to start within minutes. In a crucial process such as exams, the absence of an ID card can have a huge impact on students leading to unnecessary stress for both students and staff as well as invigilators.

The current attendance monitoring system relies on students swiping their ID card as required by the University's attendance policy. However, ID cards can be shared and hence there is no guarantee that the swipe logged on the system confirms registration of the student whose ID card was presented to the attendance reader.

3. THE PROPOSED FINGERPRINT SYSTEM

Like all biometrics systems, the use of the proposed fingerprint system involves two phases: enrollment and authentication. Figure 1. shows an overview of our proposed system for the purpose of exam registration.

The enrollment process in our proposed system would require a user to present their finger to a fingerprint sensor. The relevant features would be extracted and converted to an encrypted template. This would then be stored, with the provided university ID number and name, into a database on a secure server. This enrollment process is independent of any other systems.

Unlike the enrollment process, the fingerprint authentication process of our system always relies on the information provided by other systems. As shown in Figure 1, in the case of exam registration, our system relies on the information from both the ID card system and the exams system of our university. During the authentication stage, the user will be required to present their finger to a fingerprint scanner to be identified before they take their exam. The relevant features will be extracted and checked using feature matching process to generate matching scores against the templates enrolled in the fingerprint database, with the highest matching score being returned.

If the highest score is greater than the open-set identification threshold, then the ID number from fingerprint database will be returned and the user will be registered for the exam as an expected candidate. Otherwise, another process (for example the current ID card check process or a fingerprint matching between the test template against all the templates enrolled in the fingerprint database) will take place to obtain the ID number of the user and the user will be registered for the exam as an unexpected additional candidate. As the IDs in the fingerprint database, the ID card data-base and the exams database are identical of the same user, the ID number returned by the fingerprint matching process (either via the 'yes' or the 'no' branch) will be used to retrieve the full personal details of the identified user from the ID card sys-tem. These user details will then be combined with the exam information of the location, processed by the exam registration unit and finally stored either locally or into the database of the exams office.

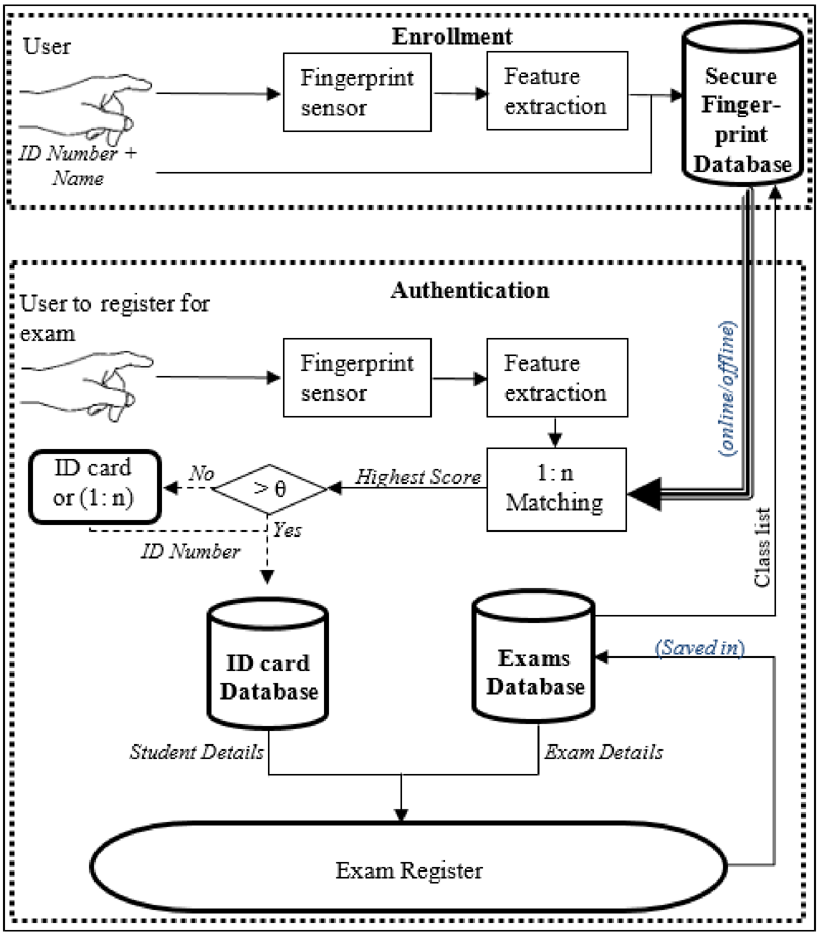

Figure 1 Proposed fingerprint system

The registration process before an exam must be as efficient as possible and is expected to last less than 10 minutes. The entire student population size of our university is more than 23,000. This means that the fingerprint matching for each exam candidate would require a 1-to-23000 matching and there are often more than 100 candidates in an exam room. To make the fingerprint-based exam registration more efficient and practical, our system retrieves an exam class list from the exams database. This exam class list shows which users are expected in the particular room of examination. This list is then used to retrieve the fingerprint templates of the expected exam candidates. These fingerprint templates can be retrieved from the exams database online in real time or it can be downloaded offline and stored on the local fingerprint terminal beforehand. This additional operation can reduce the number of fingerprint matching for each candidate from 23,000 (size of the student population at the university) down to less than 30 (number of candidates in an exam room).

Each record in the ID card database consists of ID number, first name, last name, card serial number and a link to the student photograph. Each record in the exams database consists of data relating to an exam, including module number, room number, exam date, start time, exam duration, a class list (in terms of ID number and candidate names), invigilator name, and module information, etc. Each record in the fingerprint database will consist of an encrypted fingerprint template, name of the enrolled user and his/her university ID number. As mentioned, the link among these databases is the identical university ID number of a student.

The attendance monitoring process would work in the same way but instead of in-formation about an exam location, it would log their attendance based on information about a classroom at the time of attempted attendance registration

4. SURVEY RESULTS: A PILOT STUDY

An initial survey was issued to students of the University of Hertfordshire to gather their views on the use of fingerprint technology. The survey consists of 7 questions and was open for 4 weeks. The results were collected through an online portal and face-to-face communication.

Out of 817 respondents and 754 completed responses, overall the survey was well-received with nearly 73% of the respondents supporting the use of fingerprint recognition technology to verify their identity during exams and 64% for attendance. Table 2 shows our survey questions and results in detail.

As per responses for Q1 and Q2, almost 80% of respondents have used fingerprint technology within the last 5 years and 77% feel comfortable using the technology. Responses to Q3 demonstrate a higher acceptance for controlled access as well. This is due to the fact that the students recognize the automatic nature of the fingerprint technology. As it requires no involvement of manual operation, it is always available 24/7. This is also confirmed by results of Q4 where 76% of respondents prefer using fingerprint technology.

Table 1. Survey Results

Questions	Response
Q1: Have you used fingerprint technology within the last 5 years?	• Yes: 79.93% (653) • No: 20.07% (164)
Q2: Do you/would you feel comfortable using fingerprint technology?	• Yes: 77.27% (622) • No: 22.73% (183)
Q3: Would you be willing to give fingerprint data for any of the following processes instead of using an ID Card?	• To verify your identity during exams: Yes: 72.97% (575), No: 27.03% (213) • To register your attendance: Yes: 64.34% (507), No: 35.66% (281) • To gain access into controlled areas: Yes: 75.38% (594), No: 24.62% (194)
Q4: Considering that the cost of replacing an ID card is £10 (for lost ID card), would you prefer using fingerprint recognition system instead of paying for a replacement one in urgent cases i.e. during exams, checking in for attendance, gaining access into library or borrowing books?	• Yes: 76.09% (595) • No: 23.91% (187)
Q5: Do you think that using a fingerprint recognition system would make University processes quicker?	• Yes: 68.04% (530) • No: 31.96% (249)
Q6: Would you have any concerns with the University of Hertfordshire storing your encrypted fingerprint data for the duration of your course at UH?	• Yes: 31.87% (247) • No: 68.13% (528)
Q7: When do you think it is appropriate for the University to delete your encrypted fingerprint data?	• Every year (capture it at the beginning of each year of study): 40.66% (307) • Within a month of leaving University: 47.95% (362) • Other (please specify): 11.39% (86)

In the latter part of survey results, respondents believe that the fingerprint technology would make processes quicker compared to traditional methods as per responses received for Q5. Results of the last two questions, Q6 and Q7, confirm privacy concerns from the students, which will be discussed in the next section.

5. POTENTIAL ISSUES WITH FINGERPRINT TECHNIQUE AND OUR PROPOSED SOLUTION

Most technologies come with problems of its own and fingerprint technology is no exception. Hygiene is the most talked about issue when the application of fingerprint technology involves a group of people rather than a single individual.

To tackle the hygiene issue, a touchless fingerprint system could be implemented to alleviate this concern from the end users. The touchless fingerprint technology does not require any contact between the skin of the finger and the surface of the scanner. It uses a digital camera to acquire the fingerprint image. However, the cost of a touch-less fingerprint scanner is often more expensive. For instance, a touchless fingerprint scanner from a supplier would cost around £10000, which is around £9000 more expensive than the standard scanner from the same manufacturer. In addition, anti-spoofing features are usually not available with touchless fingerprint scanners. For monitored processes such as exam registration, this would not raise any issue. But for processes such as attendance registration or access control which are often not monitored, this may allow misuses of the system. A way to reduce this risk is to enroll multiple fingers of each individual but request a randomly selected finger during authentication. On one hand, this would increase the difficulty for an attacker to fake an identity as multiple fake fingerprints are required for each identity. On the other hand, this will no increase the processing time or the inconvenience to a user during authentication as it still requires only one fingerprint.

Fingerprint data is sensitive personal data. Therefore, storage and use of such data often raise concerns. To collect views on this topic, questions 6 and 7 in our survey were around the storage of the fingerprint image and template and the acceptable duration of the storage. Although the overall response was positive with over 68% stating they wouldn’t have any concerns, nearly 32% of the 817 respondents shared their concerns with this question receiving 183 comments, the highest number of comments recorded for a single question in our survey. These were mainly around hacking/theft and sharing of this information with third parties.

The General Data Protection Regulation (GDPR)[9] due to be implemented in May 2018 has recognized biometric information as sensitive information which is currently excluded in the Data Protection Act[9]. Hence, the way in which this in-formation is stored should be given prime importance when considering fingerprint technology system. Different encryption methods, including Fourier processing[10], fuzzy vault[10] and symmetric encryption[11] may be explored to secure data and protect privacy.

In a University environment where there could potentially be more than twenty-three thousand fingerprint records stored in the system at a time, system performance could be affected when using fingerprint technology to identify a candidate from the entire university population. To speed up the authentication process and enhance system accuracy, a class list of who are expected in a specific room, for example from the exams office or the room booking system, can be used to reduce the population size from the entire university student community (23,000+) to a small group of students (10 to 200).

Another concern raised via the survey was around the network stability and temporary loss of network connection. Where network is unstable, a proposed solution is to download and temporarily store the enrolled fingerprint templates of the expected individuals as well as the authentication results on a local fingerprint device.

6. CONCLUSION

In this paper, we have demonstrated a novel approach to using a fingerprint recogni-tion system to enhance exams and attendance processes within an educational set-ting. A pilot survey has been conducted with the target users and the results indicate a high acceptance rate of fingerprint technology to be implemented in a University environment. Solutions to key issues with the fingerprint technology have also been discussed.

Once this application has been delivered successfully, the fingerprint recognition system can potentially be used for various other processes within the University. Some of these include: student attendance monitoring system, access control and monitoring, security checks, coursework submission and the library loan system. In our future research, we plan to carry out further experimentation so as to reinforce the hypothesis evaluated in this article.

ACKNOWLEDGEMENTS

This work has been supported by the University of Hertfordshire Proof of Concept award and the Diamond Fund within the project, "A Biometric Approach to Prevent False Use of IDs"

REFERENCES

[1] B. Frank. (2016), Five Examples of Biometrics in Banking Available: http://www.alacriti.com/biometrics-in-banking Accessed on 11/04/2017

[2] D. A. Tran and T. Zhang, "An Online Algorithm for Fingerprint-based Location Tracking," *IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, 2014.

[3] B. Pemberton, "Era of fumbling for your boarding pass could be over: Alaska Airlines trials fingerprint identification for passengers to shorten airport queues (but experts warn the system can be tricked)," in *MailOnline*, ed: www.dailymail.co.uk, 2015.

[4] M. Liu, "A Study of Mobile Sensing Using Smartphones," *International Journal of Distributed Sensor Networks*, 2013.

[5] R. Shilkrot, J. Huber, C. K. Liu, P. Maes, and S. C. Nanayakkara, "FingerReader: A Wearable Device to Support Text Reading on the Go," 2014.

[6] D. Sunehra, "Fingerprint Based Biometric ATM Authentication System," *International Journal of Engineering Inventions*, vol. 3, pp. 22-28, 2014.

[7] A. K. Jain, D. Maio, D. Maltoni, and S. Prabhakar, "Handbook of Fingerprint Recognition," 2003.

[8] A. Khairwa, K. Abhishek, S. Prakash, and T. Pratap, "A comprehensive study of various biometric identification techniques," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*, 2012, pp. 1-6.

[9] Sensitive data and lawful processing. Available: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/25--guide-to-the-gdpr--sensitive-data-and-lawful-processing.pdf?la=en

[10] A. Cavoukian and A. Stoianov. (2007, Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. Available: https://pdfs.semanticscholar.org/9744/21ad38c326a48ee26a3a5937ad59a0a2df28.pdf

[11] P. Prabhusundhar, V. K. N. Kumar, D. B. Srinivasan, and P. Narendran, "Fingerprint Biometrics Identification Scheme Using Secret Key Cryptographic Security," IJAIR, 2013.