Indonesian Journal of Electrical Engineering and Computer Science
Vol. 20, No. 1, October 2020, pp. 405~413
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v20.i1.pp 405-413

Multimodal access control system combining RFID, fingerprint and facial recognition

Mohamed El Beqqal[1], Mostafa Azizi[2], Jean Louis Lanet[3]
[1,2]Department of Computer Science, University Mohamed First, ESTO, Morocco
[3]Department of Security, Institute Inria, France

Article Info

Article history:

Received Jan 11, 2020
Revised Mar 13, 2020
Accepted Mar 27, 2020

Keywords:

Access control
Fingerprint
Identification
Multimodal biometric
RFID

ABSTRACT

Monomodal biometry does not constitute an effective measure to meet the desired performance requirements for large-scale applications, due to limitations such as noisy data, restricted degree of freedom and unacceptable error rates. Some of these problems can be solved through multimodal biometric systems that involve using a combination of two or more biometric modalities in a single identification system. Identification based on multiple biometrics represents an emerging trend. The reason for combining different modalities is to improve the recognition rate. In practice, multi-biometric aims to reduce the False Acceptance Ratio (FAR) and False Rejection Ratio (FRR) which are two standard metrics widely used in the accuracy of biometric systems. In this paper, we will examine the different possible scenario in multimodal biometric systems using RFID, fingerprint and facial recognition, that can be adopted to merge information and improve the overall accuracy of the system.

Corresponding Author:

Mohamed El Beqqal,
Department of Computer science,
University Mohamed First Oujda,
BP 473 Al Qods University Complex, Oujda 60000, Morocco.
Email: elbeqqal.mohamed@gamil.com

1. INTRODUCTION

By definition, biometric is a biological measure of any human physiological or behavior characteristics that can be used to verify the identity of an individual [1]. An identification system based on biometrics operates in two modes, namely enrollment and authentication [2]. In enrollment mode, the biometric data of a user is acquired using a biometric reader and stored in a database, while in authentication mode, the biometric data of a user is acquired again, and the system uses this to verify the user's declared identity or identify his identity [3]. Indeed, the verification represents the comparison of the acquired biometric information with only the models corresponding to the claimed identity, whereas the identification involves the comparison of the acquired biometric information with models cor-responding to all the users of the database.

Biometric identification systems, which include physical features such as fin-gerprints, face, ear, iris, and voice, provide much greater security than password and number systems [4-6]. Obviously, every biometric technology has its strengths and limitations, and no biometric should effectively meet the requirements of all verification or identification applications.

Sometimes, a single biometric lacks precision to allow the identification of a large number of users. The physical characteristics of a person for the selected biometric may not be always available or readable. On the other hand, biometric systems based on multimodal biometrics involve using a combination of two or more biometric modalities in a single identification system to improve the overall accuracy of the recognition [7-9]. In a biometric system, the main challenge is to minimize error rates, to make it work successfully for

the entire population for a given application and to ensure that it is not compromised [10]. The FAR is the percentage of imposters that are incorrectly granted access. The FRR is the percent-age of valid users who are incorrectly denied the access [11, 12].

The paper is organized as follows: in Section 2, we present the fundamental concepts of access control. In Section 3, we indicate some developed works for the multimodal system. In Section 4, we study the proposed system and we eval-uate the effectiveness of our system by some experimental results. Finally, in Section 5, we give a conclusion.

2. BASICS AND ACCESS CONTROL

Access control to an information system consists of associating access rights and / or resources to an entity (person, computer, etc.), thus enabling the entity to access the desired resource, if she has the correct rights. The access control can be logical and / or physical (password, card, key, biometrics, etc.) and offers the possibility to access to physical resources (building, room, etc.) or logical resources (computer system, smartphone) [10].

The RFID technology is widely used in several access control systems due the ease of deployment and the fast processing aspect [13], whereas the technology does not allow to prove the real identity of the person carrying the tag [14]. Thus, the security aspect of RFID needs to be strengthen using a biometric technique.

Many biometric techniques are available in the authentication process such as finger print recognition, eye pattern recognition, face recognition, voice pattern recognition, vein recognition and others. However, the fingerprint pattern recognition remains the most used technique for its simplicity of use of and cost effective [15-17]. The facial recognition is also considered as a good alternative to fingerprint since no physical interaction with the user is required and the results of matching are accurate if the image is well captured [18].

In the literature, the studies based on biometric systems have shown that the use of several biometric methods will be necessary to obtain acceptable identification accuracy for an identification application of a large population of users [19]. In any case, it is not necessary for the different measurements to be mathematically combined. For example, a system with RFID, fingerprint and facial recognition would be considered multimodal even if the OR rule was applied, allowing users to be verified using one or other of the modalities [1].

In addition, not all individuals are able to enroll in a selected biometric system due to the use of damaged or illegible biometric data [4]. A high failure rate in terms of enrollment implies that a certain number of users must be authenticated by another method. This can lead to reduced security and the need to maintain at least two authentication methods. However, all biometric data requires some kind of exception handling to treat those who cannot register.

3. RELATED WORKS

Several means exist to prove the person identity and thus obtain access authorization in a control access system or be identified in attendance check system. It can be verified by what we know (a password, a code), what we have (a badge, a phone, a license plate) or what we are with a biometric identification, or a combination of these means.

Authors in [20] developed a control access system based on RFID technology and password verification, the system is connected to a digital door which is unlocked if RFID tag is matched in database record and the correct password is entered. The advantage in this system is the use of an inexpensive technology which is more convenient implement and consumes considerably less space for installation and maintenance purposes. The system also generates reports of all check-in, check-out transactions to maintain the status of visitors. The inconvenient in this system is both password and RFID tag can be borrowed by another person and no physical criteria are used to allow access to the protected area. In the security study carried out in [21], the author mentions that the RFID tag can also be cloned.

In [22], the authors combined face recognition with RFID technology to implement an access control system for hostels in both user entrance and exit operation and RFID with password to access to mess hall. In case of no matching records with the database an emergency call is performed throughout a GSM modem device. The facial recognition step is based on the record of detected RFID TAG. This technique allows a fast verification since the system compares the captured image face with an identified record. However, if there is any problem in RFID verification or the user forgets his tag, the whole verification system will be interrupted.

The paper [23] proposed a hybrid biometric system based on facial recognition and fingerprint verification. In this system, a fusion at features extracting and, matching level and decision-making level was proposed based on merging the both features extracted on one biometric template in database which would make it difficult to localize independently the type of biometric data in database. Hence, this technique will secure the exposition of data, but it will slow the search of biometric information during the process of identification. Furthermore, no priority on biometric technique was specified or threshold management between the two techniques was exposed to take the decision of accepting or refusing the candidates.

Authors in [24] have implemented an automatic attendance system management for professors using multimodal verification. The authors used the Adafruit Fingerprint algorithm coupled with Arduino for fingerprint verification and Viola-Jones algorithm for facial detection in addition to Principal Component Analysis to the matching process. In this system, the fingerprint has been prioritized as a first verification, if the result is satisfied the system can process to a facial recognition step. In addition, the measures results show that the facial recognition method is largely related to measurement conditions while calculating the Euclidean distance between uncontrolled environment and almost non-moving subject.

4. PROPOSED SYSTEM

4.1 Goal and motivation

As discussed in the section 3, the use of biometrics in authentication process has become a necessity since RFID technology allows identification of the tag and not the real identity of the tag holder. In addition, to rely on one biometric technique could be sanctioning if the matching process does not provide the correct result within the supported threshold of acceptance. Hence, we have opt-ed for a multi-modal authentication system combining RFID and hybrid bio-metric techniques compromising fingerprint verification and facial recognition.

4.2 Data acquisition

4.2.1 RFID

Since our system is designed to be used in university context, an enrollment phase is supposed to be done to save information concerning the students. Hence each student should be equipped with an RFID tag representing his unique ID within the university campus. This information represents the primary key of the student / the user data. User class diagram as shown in Figure 1.

For RFID data acquisition as shown in Figure 2 below, we have used the module RC522 MIFARE Module responsible to receive the Tags IDs through his antenna operating at a frequency of 13.56 MHz allowing reading data over short distances (between 3cm and 5 cm) with a Transmission speed of 106KB/sec.

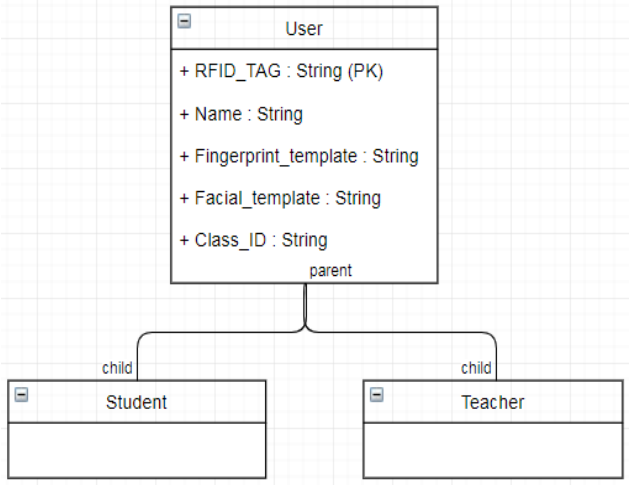

Figure 1. User class diagram

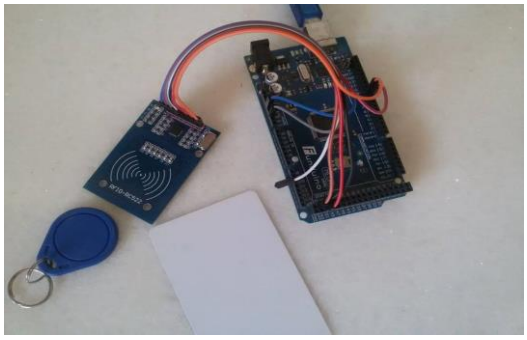

Figure 2. RFID data acquisition system

Once the RFID library is included in Adruino IDE and the program of reading RFID tags into the Arduino card is loaded, the RFID module will be ready to collect ID of Tags coming in range of the reader and send it to the microcontroller ATmega 2560 using serial connection. The Figure 3 shows an example of reading RFID tags.

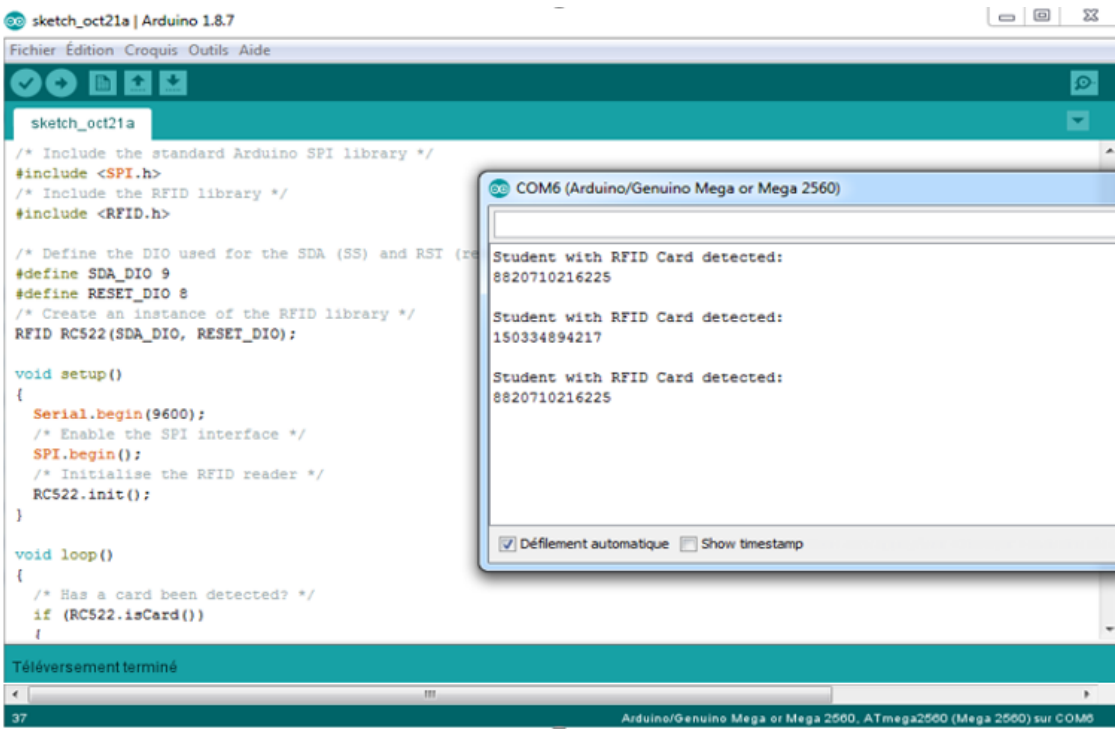

Figure 3. Reading RFID tags using Arduino AT MEGA2560

4.2.2 Fingerprint

The quality of the acquired biometric template is critical for the application's overall accuracy. While in some cases, identification or verification can take place daily, enrollment is usually done only once, and it is essential to acquire the best possible fingerprint templates. Higher is the enrollment quality, easier is the recognition. A good fingerprint quality makes efficient the task of recognition. For this reason, we have opted for the MorphoSmart 350 reader which is able to acquire very high-quality impression images, to generate biometric templates and distinguish individuals (authentication & identification). The internal database can store up to 5000 users. Besides, the reader supports multiple template formats such us ANSI/INCITS 378, ISO 19794-2 and other proprietary formats).

As shown in Figure 4, when the received image contains no fingerprint or if the fingerprint quality is under the required threshold, then the received image is ignored. Only fingerprint images with quality values greater or equal to the threshold are considered for the next step. This quality value lies between 0 and 255 (0 is the lowest quality and 255 the highest quality).

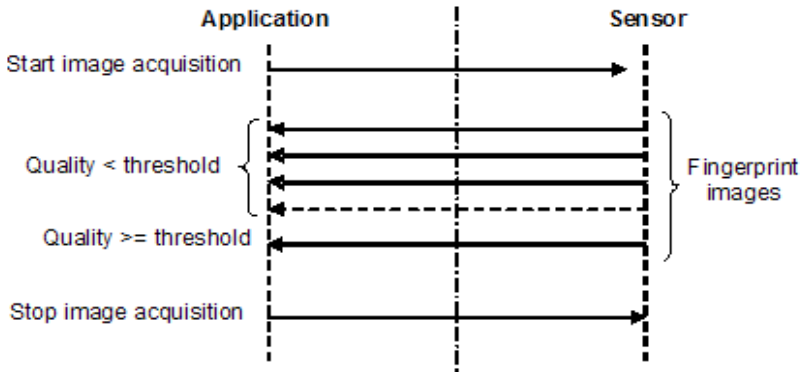

Figure 4. Fingerprint acquisition process

In addition to the quality of acquisition, the matching threshold is another important parameter to be considered during the identification and verification process. This parameter specifies the value of the FAR device. A more secure check (higher threshold value, higher FAR, lower FRR), a more comfortable check (lower threshold value, lower FAR, higher FRR), or a balance value between the FAR and the FRR.

For experimentation, we have used the SDK 6.14 of MorphoSmart reader which provides many libraries and algorithms for biometrics functions [25]. After a successful enrolling, we have fixed the matching threshold value to 2 that corresponds to a higher FAR defined in the morpho device. This threshold allowed us to recognize the real fingerprint as shown in Figure 5. Whereas, while using a secure check with a threshold of 8 that corresponds to a lower FAR, the user was not recognized, even if the same fingerprint was used as shown in Figure 6.

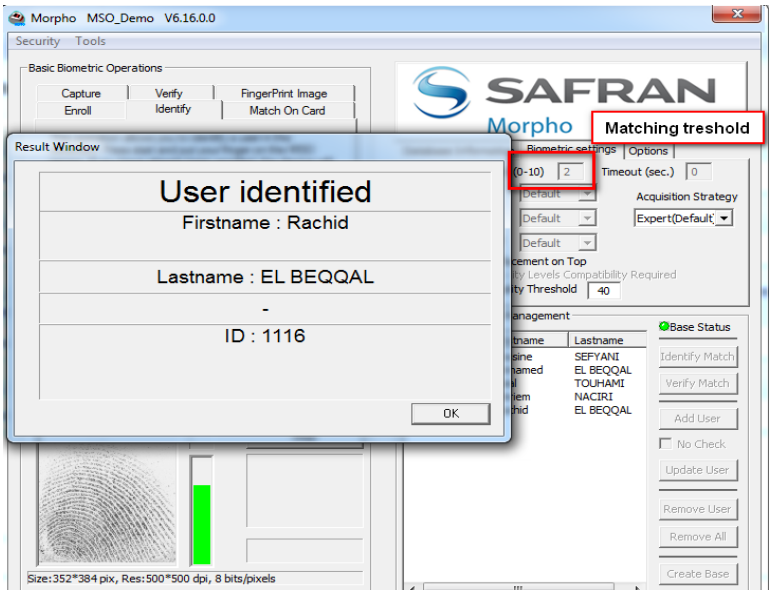

Figure 5. Identify fingerprint with low matching threshold value

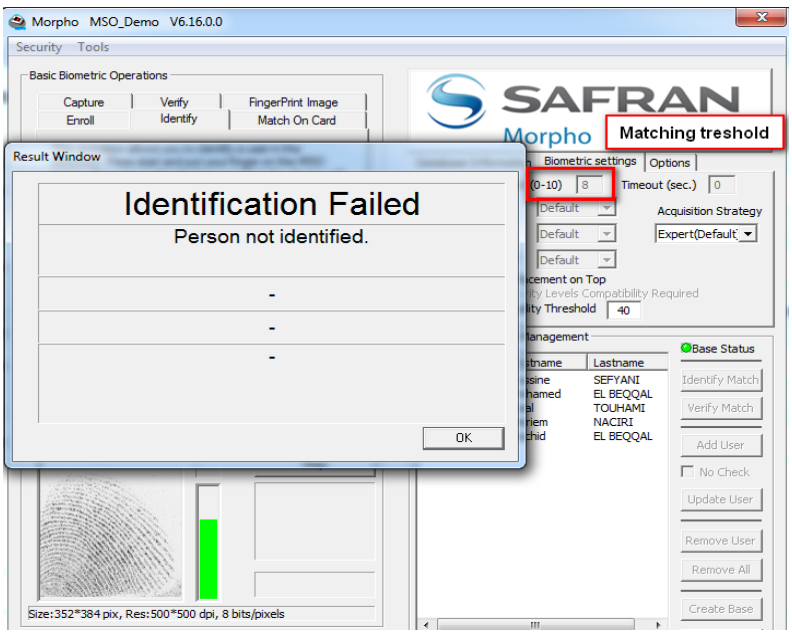

Figure 6. Identify fingerprint with high matching threshold value

4.2.3 Facial recognition

For the task of facial recognition, a preliminary step of preparing data was done by collecting pictures of several students in the university. During the enrollment process and for more reliable results, we have saved five images per each enrolled student to cover many face positions since the facial recognition is sensitive to the position of the captured image. These images are grouped in directories, each for one student. A step of transforming an image to specific pixel size with a grayscale color format was done to prepare data for the matching process.

After the dataset were prepared, we have used MATLAB version R2018b load all the prepared data and identify each selected person. The Figure 7 shows an example of identifying an image of a student, the result was found in the five already prepared data of this student.

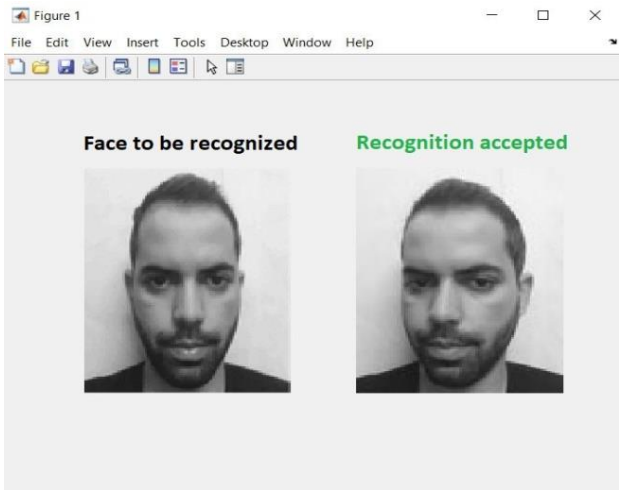

Figure 7. Facial recognition using MATLAB

4.3 Matching decision

After the step of data acquisition, we have defined a Matching Threshold (MT) based on many experimentations done on several students. For this reason, we have used the MorphoSmart SDK to calculate the matching score. For more accurate results, we have recorded 4 attempts for each student to consider the fact of bad finger positioning. Thereafter, we have calculated the average of these records matching score. The choice of this interval [2000, 3000,…, 8000] is made according to the obtained results. In the Table 1 bellow we present the several measurements for each interval:

Table 1. Matching scores of enrolled students

Students	FP Quality	MT:5000	MT:6000	MT:7000	MT:8000	MT Average:5364,43
1	86	8006	8108	8180	8300	8148.50
2	119	10307	10050	10007	10600	10241.00
3	64	7123	6478	6011	6278	6472.50
4	62	5820	5203	5349	5289	5415.25
5	112	9184	9100	9302	9580	9291.50
6	75	8215	8108	7684	7845	7963.00
7	81	9156	9311	9087	9334	9222.00
8	62	5801	6625	6768	6815	6502.25
9	88	8140	8211	8115	8805	8317.75
10	69	6487	6890	6245	7156	6694.50
11	74	7168	7100	7008	7228	7126.00
12	84	9906	9010	9120	9085	9280.25
13	61	6906	7431	7122	6802	7065.25
14	76	7208	7056	7124	7151	7134.75
15	92	10105	10031	9023	10086	9811.25
16	68	7902	7009	7105	7381	7349.25
17	87	8121	8426	7807	8187	8135.25
18	55	4565	4204	4100	4532	4350.25
19	68	7140	7623	7951	7809	7630.75
20	64	4912	5070	4300	5026	4827.00

To allow the calculation of the FRR, we have asked the students already enrolled in the database to identify themselves using the same finger used in enrollment phase. For each interval, we have calculated the number of false rejected attempts regarding the total number of attempts. At the same way, to allow the calculation of the FAR, we have asked the students not enrolled in the database to identify themselves and for each interval we have calculated the number of accepted attempts regarding the total number of attempts. Tables 2 and 3 show the obtained results.

Based on the both experimentations, we have calculated the average of 40 student attempts; it is equal to 5364.43. As shown in Table 3, for more secure check (higher threshold values), we have a higher FAR and a lower FRR. Nevertheless, for more comfortable check (lower threshold), we have a lower FAR and a higher FRR.

Table 2. Matching scores of unenrolled students

Students	FP Quality	MT:2000	MT:3000	MT:4000	MT:5000	MT Average:5364,43
21	91	3245	3706	3651	3926	3632.00
22	78	2612	2514	2348	2852	2581.50
23	67	2689	2457	2159	2647	2488.00
24	102	4567	4128	3896	4215	4201.50
25	59	2136	2598	2478	2315	2381.75
26	71	3265	3485	3128	3981	3464.75
27	66	2965	3178	3228	2846	3054.25
28	62	2147	2254	2687	2365	2363.25
29	105	4128	4684	4265	4386	4365.75
30	67	2173	2984	2485	2975	2654.25
31	85	3874	3245	3120	3725	3491.00
32	66	2374	2145	2531	2513	2390.75
33	71	2138	2483	2445	2674	2435.00
34	119	5102	4856	5007	5215	5045.00
35	77	2426	2876	2434	2921	2664.25
36	98	4021	3982	3823	4037	3965.75
37	75	2547	2365	2659	3125	2674.00
38	96	3214	3256	3481	3125	3269.00
39	81	2736	2156	2971	2765	2657.00
40	93	2647	3580	3210	2963	3100.00

Table 3. FAR and FRR results of the experimentation

Matching threshold	2000	3000	4000	5000	6000	7000	8000	AVG 5364,43
Total FRR %	0%	0%	0%	10%	15%	35%	60%	10%
Total FAR %	100%	50%	10%	5%	0%	0%	0%	0%

4.4. Combined matching

Based on the results of Table 3, we noticed that the most appropriate threshold to implement should be between [4500, 6000] since this interval stands for the balance value between the FAR and the FRR giving the priority to the FRR (supporting until 15% rate). In fact, FRR varies from one kind of population to another, and it is better with individuals who perform limited manual labors and have good quality fingerprints (which is the case of most of students) than with hard manual laborers with damaged fingerprints. In addition to that, we have chosen to deal with the false rejections and false acceptance cases within the defined matching threshold using the facial recognition as a second check (see Figure 7). The Figure 8 shows the model of combining the RFID, fingerprint and facial recognition check.

The RFID added value consists on the performance aspect since its security cannot be trusted as the RFID tag can be borrowed by other students. However, the presence of RFID tag allows to the student to perform a verification of his biometric data for a specific record than to be identified in the back-end against the whole database. Depending on the matching score whether it belongs to threshold matching interval defined in Subsection 4.3, the facial recognition will be performed to validate the final decision. The other cases represent whether the student is hardly accepted if the matching score is greater than 6000 or refused if the matching score is under 4500. Effectively this threshold intervals could be adjusted depending on the incoming experimentations and more precisely, based on a midleware approach which will allow to have synchronized and more precise measurements as mentioned in [26].

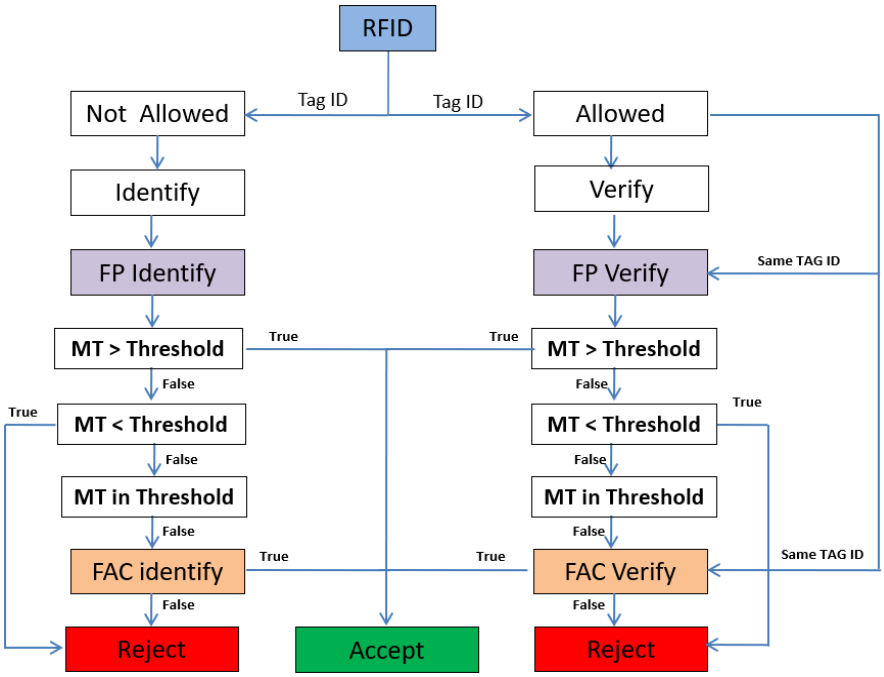

Figure 8. Combined biometric matching decision

5. CONCLUSION

Identity verification is a crucial matter in the context of access control. The use of multimodal authentication techniques became a necessity to ensure the real identity of an individual. For this reason, we have proposed a multimodal system based on RFID, fingerprint and facial recognition to ensure both perfor-mance and security aspects. The experimentations done allowed us to determine the threshold matching value to make balance between FAR and FRR. Then, the matching decision is based on the matching score of each student depending on defined threshold interval.

As a future work, we aim to continue dealing with middlewares that link the three considered technologies in order to gather more accurate results based on other criteria such as execution time or work volume.

REFERENCES

[1] Ko, T. "Multimodal biometric identification for large user population using fingerprint, face and iris recognition". In *Applied Imagery and Pattern Recognition Workshop*, Proceedings. 34th, IEEE, p. 6, 2005.
[2] S. C. Hoo and H. Ibrahim, "Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements," *Journal of Sensors*, vol. 2019, pp. 1–25, Sep. 2019.
[3] M. E. Beqqal, M. Azizi and J. L. Lanet, "Polyvalent Fingerprint Biometric System for Authentication". In *Information Systems and Technologies to Support Learning*, pp. 361–366. Springer International Publishing, 2018.
[4] Galbally, J., Marcel, S., & Fierrez, J. "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition". *IEEE transactions on image processing*, vol. 23, no. 2, pp. 710-724, 2014.
[5] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994-6009, 2019.
[6] R. E. O. Paderes, "A Comparative Review of Biometric Security Systems," in *2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)*, 2015.
[7] A. A. Joshi, P. Deshpande, and A. S. Tavildar, "Enhancing accuracy for personal identification usinghierarchical based fusion of finger geometry and palm print modalities," in *2014 International Conference on Electronics and Communication Systems (ICECS)*, 2014.
[8] V. Conti, "Biometric Authentication Overview: a Fingerprint Recognition Sensor Description," *International Journal of Biosensors & Bioelectronics*, vol. 2, no. 1, Jan. 2017.
[9] H. Benaliouche and M. Touahria, "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint," *The Scientific World Journal*, vol. 2014, pp. 1-13, 2014.
[10] Duarte, T., Pimentão, J. P., Sousa, P., & Onofre, S. "Biometric access control systems: A review on technologies to improsve their efficiency". In *Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International, IEEE*, pp. 795-800, 2016.

[11] M. Sivaram, M. U. A. A, D. Yuvaraj, G. Megala, V. Porkodi, and M. Kandasamy, "Biometric Security and Performance Metrics: FAR, FER, CER, FRR," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 2019.
[12] A. Bansal, R. Agarwal, and R. K. Sharma, "FAR and FRR based analysis of iris recognition system," in *2012 IEEE International Conference on Signal Processing, Computing and Control*, 2012.
[13] M. E. Beqqal and M. Azizi, "Review on security issues in RFID systems," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 6, pp. 194-202, Dec. 2017.
[14] M. E. Beqqal, M. A. Kasmi, and M. Azizi, "Access Control System in Campus Combining RFID and Biometric Based Smart Card Technologies," in *Advances in Intelligent Systems and Computing, Springer International Publishing*, pp. 559-569, 2016.
[15] Rahim, M. R. "Implementation of biometric authentication methods for home based systems (Doctoral dissertation", Cardiff Metropolitan University), 2016.
[16] A. Pinto et al., "Counteracting Presentation Attacks in Face, Fingerprint, and Iris Recognition," in Deep Learning in Biometrics, CRC Press, pp. 245-293, 2018.
[17] P. S. Sanjekar and J. B. Patil, "Multimodal biometrics with serial, parallel and hierarchical mode at decision level fusion," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 3, p. 1303, Dec. 2019.
[18] Jahromi, M. N., Bonderup, M. B., Asadi-Aghbolaghi, M., et al. "Automatic Access Control Based on Face and Hand Biometrics in A Non-Cooperative Context". In *Computer Vision Workshops (WACVW), 2018 IEEE Winter Applications of, IEEE*, pp. 28-36, 2018.
[19] Z. Wu, J. Yang, J. Zhang, and H. Yue, "Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method," *Security and Communication Networks*, vol. 2018.
[20] Shafin, M. K., Kabir, K. L., Hasan, N., et al. "Development of an RFID based access control system in the context of Bangladesh. In *Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015 International Conference on, IEEE, pp. 1-5, 2015.
[21] M. E. Beqqal and M. Azizi, "Classification of major security attacks against RFID systems," in *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, 2017.
[22] Farooq, U., ulHasan, M., Amar, M., Hanif, A., & Asad, M. U. "RFID based security and access control system. *International Journal of Engineering and Technology*, vol. 6, no. 4, p. 309, 2014.
[23] Mahesh Naidu, K., & Govindarajulu, P. "Biometrics hybrid system-based verification. *(IJCSIT) Int. J. Comput. Sci. Inf. Technol*, vol. 7, no. 5, pp. 2341-2346, 2016.
[24] Cruz, J. C. D., Paglinawan, A. C., Bonifacio, M. I. R., Flores, A. J. D., & Hurna, E. V. B. "Biometrics based attendance checking using Principal Component Analysis". In *Humanitarian Technology Conference (R10-HTC)*, 2015 IEEE Region 10, IEEE, pp. 1-5, 2015.
[25] IDEMIA. (n.d.). MorphoKit. [online] Available at: https://www.morpho.com/fr/morphokit [Accessed 22 Aug. 2018].
[26] M. E. Beqqal, M. Azizi, and J. L. Lanet, "A Novel Approach for an Interoperable Biometric Verification," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 12, no. 6, pp. 124-132, 2018.