

# COMPARATIVE STUDIES BETWEEN A FACIAL RECOGNITION SYSTEM AND A FINGERPRINT RECOGNITION SYSTEM FOR ACCESS CONTROL

**Bopatriciat Boluma Mangata<sup>1</sup>, Dominique Ilunga N'kashama<sup>2</sup>, Parfum Bukanga Christian<sup>3</sup>, Donatien Kadima Muamba<sup>4</sup>**

<sup>1,3</sup>Department of Mathematics, Statistics and computer Science, University of Kinshasa, Kinshasa, D.R Congo

<sup>2</sup> Higher Institute of Arts and Crafts, Mbuji-Mayi, Mbuji-Mayi, D.R Congo

<sup>4</sup>Faculty of computer Science, University of Reverend Kim, Kinshasa, D.R Congo

\*Corresponding author  
bopatriciat.boluma@unikin.ac.cd

## Article history:

Received July 15, 2022

Revised August 14, 2022

Accepted August 26, 2022

## Keywords:

Automation; Biometric Recognition; Biometrics, Embedded System; Pattern Recognition; Single Modal.

## Abstract

This paper investigates the decisions made on two singles modal biometric systems based on facial recognition and fingerprints for access control. In order to carry out this study on the access control system based on fingerprint and facial recognition, we made biometric recognition systems based on fingerprints and facial recognition that interacts with an embedded system under Arduino to give us the possibility to assemble the performances of programming and electronics, more precisely, we programmed electronic systems for the automatic opening of doors without the action of a human being. In a sample of one hundred individuals composed of 40 females and 60 males, 75 of whom were enrolled and 25 of whom were not, our two singles modal access control systems each obtained the following results: 70 true positives, 5 false negatives, 8 false positives and 17 true negatives for the facial recognition system, compared to 73 true positives, 2 false negatives, 4 false positives and 21 true negatives for the fingerprint recognition system, which constitute our confusion matrix. From all the tests carried out, we can say that the decisions made by the fingerprint recognition system are better than the decisions made by the facial recognition system.

## 1.0. INTRODUCTION

Single-mode biometric systems suffer from several problems that make them unsuitable for current biometric applications that require high levels of reliability and security [11]. These problems include the use of a single biometric trait that is prone to noise, poor capture, lack of biometric points, and deterioration in the quality of biometric input [12].

### 1.1. Problematics

In a practical biometric system that uses biometrics for personal recognition, a number of other issues need to be considered:

- Performance: the accuracy and speed of recognition achievable in terms of the resources required, as well as the operational and environmental factors that affect accuracy and speed [9];
- Acceptability: the degree to which people are willing to accept the use of a particular form of biometric identification in everyday life;
- Bypass: the ease with which the system can be fooled using fraudulent methods.

Each of these attributes has its own characteristics compatible with the requirements of different security systems. A single modal biometric system uses a type of component based on a solitary methodology, such as fingerprints, iris, face, etc. [10].

A practical biometric system should have specified levels of accuracy, speed and recognition resources: be safe for all users, be accepted by the target population and be robust enough to withstand various fraudulent methods and system attacks [1]. The success of a biometric system depends on how the relevant information is captured, the learning strategy used and the extent to which it is resistant to variation in the data captured [8].

## 1.2. Hypothesis

The introduction of multimodal biometrics proves to be a solution to these problems as multimodal systems allow for improved recognition performance by combining several sources of information [8]. However, in this work, we will study the decisions made on two single modal biometric systems based on facial recognition and fingerprints for access control.

With this in mind, we will carry out this study on two access control systems based on decisions obtained from facial recognition and decisions obtained from fingerprints, while using an embedded system under Arduino that will give us the possibility to assemble the performance of programming and electronics, more precisely, we will program electronic systems for the automatic opening of doors without the action of a human being [4].

## 1.3. Purpose and motivation of the work

Our work consists of studying the decisions made in automatic access control systems based on single-mode biometric recognition, which exploit fingerprints and facial recognition. Our approach will achieve the following objectives:

- Design an embedded system using Arduino for automatic door opening;
- Designing biometric systems based on fingerprints and facial recognition for access control.
- Evaluate the performance of these systems using confusion matrices.

## 1.4. Interest of the subject

The interest of such an approach is to provide a valuable help to the scientific community by providing a reliable analysis for automatic access control and biometric pattern recognition [13].

## 2.0. METHOD AND DISCUSSION

### 2.1. Implementation of A Biometric Access Control System Based on Fingerprints

In this section, we will realize an access control system based on fingerprints, we will use an embedded system under Arduino which will give us the possibility to assemble the performances of programming and electronics, more precisely, we will program electronic systems for the automatic opening of doors without the action of a human being [1-2].

#### A. Hardware architecture of fingerprints recognition system

The hardware architecture of the project is as follows:

- Personal Digital, a fingerprint reader, communicating via the USB port;
- A computer, containing a biometric application in C# that allows instructions to be given to the Arduino board via the serial port and a database replicated in three different instances that represent our three sites.
- The Arduino board, which is programmed to analyze and produce electrical signals, in order to perform automatic door opening and closing tasks (access control).
- TOWER PROTM Micro Servo 9g SG90, a stepper motor that will allow us to make the opening and closing movements of the doors.

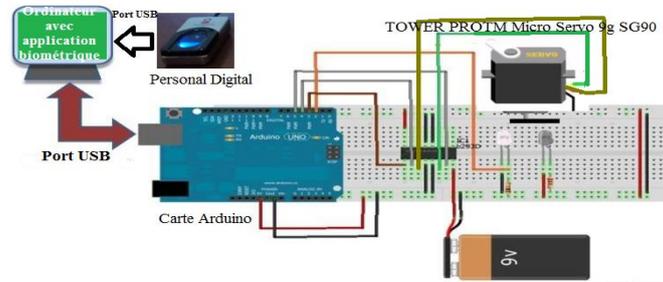


Figure 1. The project's hardware architecture

**B. Result of fingerprints recognition**

Here is the representation of some graphical interfaces of our application:

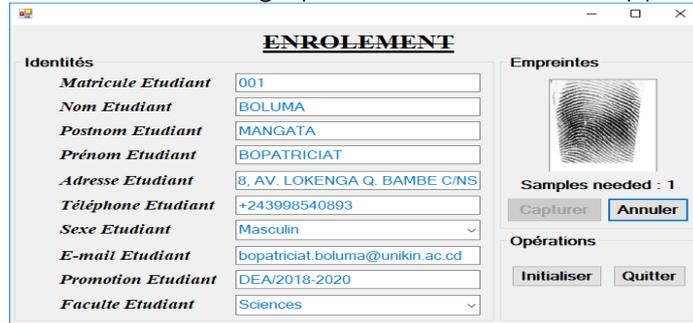


Figure 2. The enrolment windows



Figure 3. The verification window with a valid fingerprint

**C. System performance of fingerprints recognition**

This work item evaluates the performance of our fingerprint-based recognition system for automatic access control. On a sample of 100 individuals composed of 40 women and 60 men, of which 75 were registered and 25 non-registered, our access control system obtained the following results: 73 true positives, 2 false negatives, 4 false positives and 21 true negatives, which constitute our confusion matrix.

Table 1 Confusion matrix of fingerprints recognition system

	True Positive	False Negative	True Negative	False Positive	Sum
Women	29	1	9	1	40
Men	44	1	12	3	60
Sum	73	2	21	4	100

Based on this result, which allowed us to evaluate the performance of our system, we can graphically represent it with the help of a bar chart as follows:

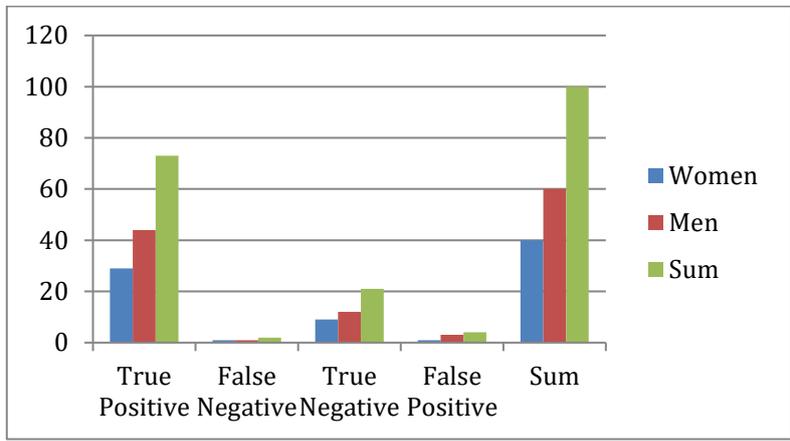


Figure 4. Verification performance with fingerprints

**2.2. Implementation Of A Biometric Access Control System Using Facial Recognition**

In this part of our work, we will realize an access control system based on the facial recognition system, we will use an embedded system under Arduino which will give us the possibility to assemble the performances of programming and electronics, more precisely, we will program electronic systems for the automatic opening of doors without the action of a human being [14].

**A. Hardware architecture of facial recognition system**

The hardware architecture of the project is as follows [3-6]:

- A camera/webcam, communicating with a computer;
- A computer, containing a biometric application in #C that allows instructions to be given to the Arduino board via the serial port.
- The Arduino board, which is programmed to analyze and produce electrical signals, in order to perform automatic door opening and closing tasks (access control).
- TOWER PROTM Micro Servo 9g SG90, a stepper motor that will allow us to make the opening and closing movements of the doors.

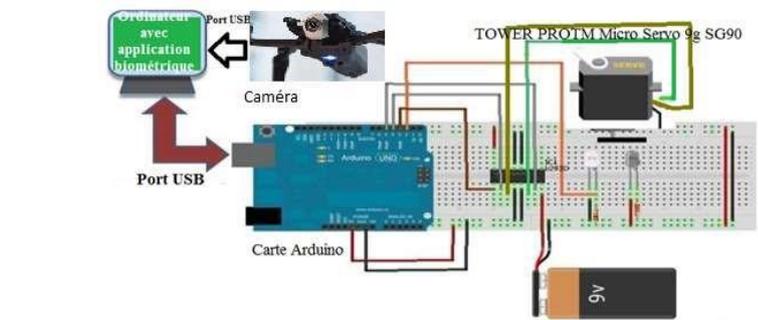


Figure 5. The project's hardware architecture

**B. Result of facial recognition**

Here is the representation of some graphical interfaces of our application:

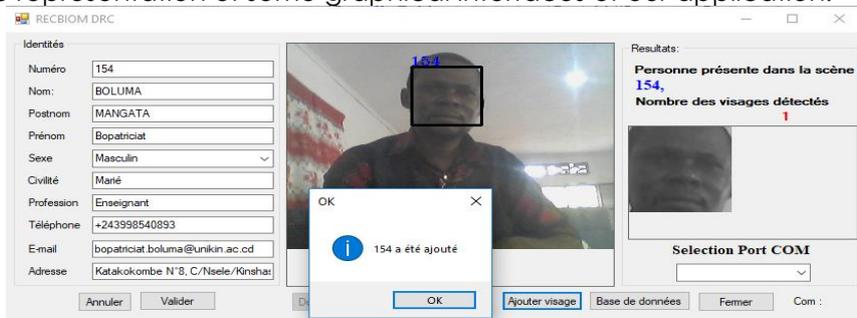


Figure 6. The enrollment windows

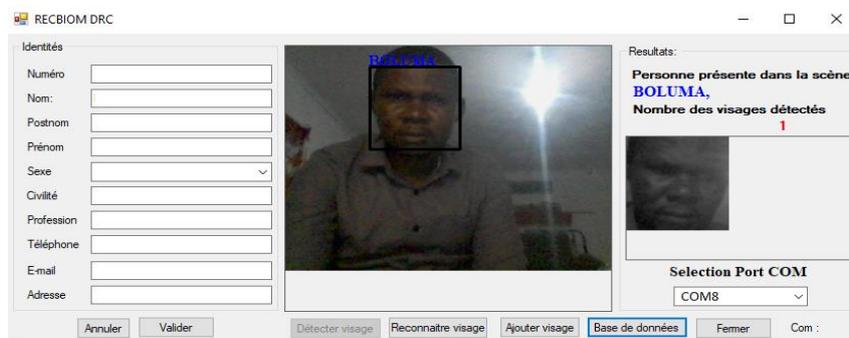


Figure 7. The verification window with a valid face

### C. System performance of facial recognition

This work item evaluates the performance of our facial recognition-based access control system for securing premises. On a sample of 100 individuals composed of 40 women and 60 men, of which 75 were registered and 25 non-registered, our access control system obtained the following results: 70 true positives, 5 false negatives, 8 false positives and 17 true negatives, which constitute our confusion matrix [5].

Table 2 Confusion matrix of facial recognition system

	True Positive	False Negative	True Negative	False Positive	Sum
Women	28	2	7	3	40
Men	42	3	10	5	60
Sum	70	5	17	8	100

Based on this result, which allowed us to evaluate the performance of our system, we can graphically represent it with the help of a bar chart as follows:

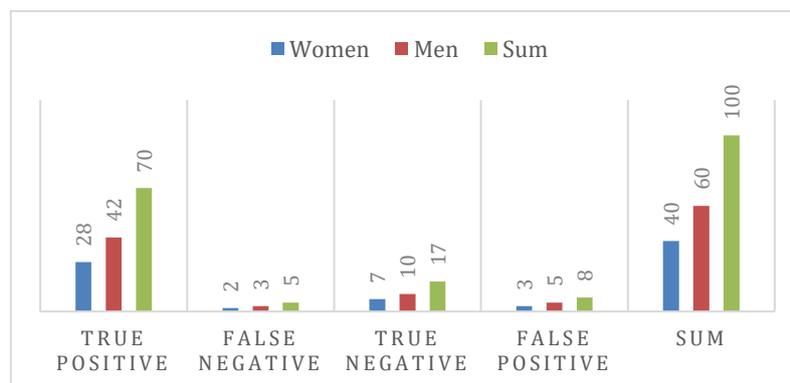


Figure 8. Verification performance with face recognition

### 2.3. Discussion on Fingerprint-Based Access Control Systems and Facial Recognition

In this section, we will perform analyses on two access control systems based on facial recognition and fingerprints.

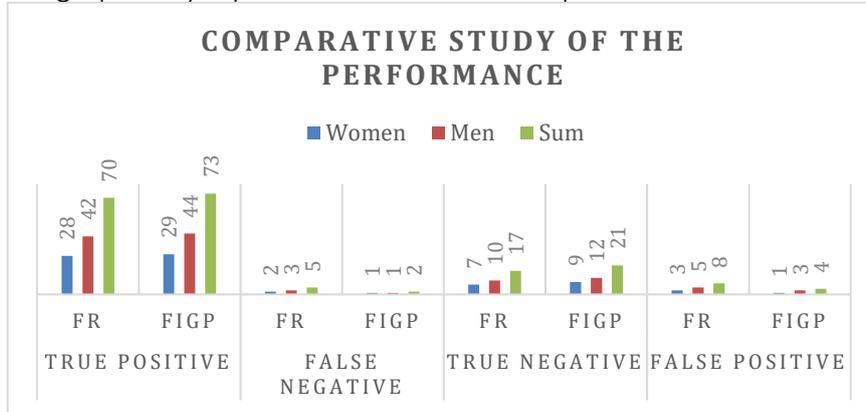
- **System performance of fingerprints and facial recognition**

In this section, we investigate the decisions made by our two access control systems based on facial recognition and fingerprints and evaluate the performance of our two access control systems. In a sample of one hundred individuals composed of 40 women and 60 men, 75 of whom were enrolled and 25 of whom were not, our two single modal access control systems each obtained the results of 70 true positives, 5 false negatives, 8 false positives and 17 true negatives for the facial recognition system, compared to 73 true positives, 2 false negatives, 4 false positives and 21 true negatives for the fingerprint recognition system, which constitute our confusion matrix hereafter [7]:

Table 3 **Confusion matrix of facial recognition and fingerprint recognition**  
(FR: facial recognition and FigP: Fingerprint)

	True Positive		False Negative		True Negative		False Positive	
	FR	FigP	FR	FigP	FR	FigP	FR	FigP
Women	28	29	2	1	7	9	3	1
Men	42	44	3	1	10	12	5	3
Sum	70	73	5	2	17	21	8	4

Based on these results, which allowed us to evaluate the performance of our two systems, we can graphically represent them with the help of a bar chart as follows:



**Figure 9.** Comparative study of the performance of our two systems

From all the tests carried out, we can say that the decisions made by the fingerprint recognition system are better than the decisions made by the facial recognition system.

### 3.0. CONCLUSION

Our work consists of studying the decisions made on two single modal access control systems based on facial recognition and fingerprints. To realize this access control system based on fingerprint and facial recognition, we have realized biometric recognition systems based on fingerprints and facial recognition that interacts with an embedded system under Arduino to give us the possibility to assemble the performances of programming and electronics, more precisely, we have programmed electronic systems for the automatic opening of doors without the action of a human being. In a sample of one hundred individuals composed of 40 females and 60 males, 75 of whom were enrolled and 25 of whom were not, our two single modal access control systems each obtained the following results: 70 true positives, 5 false negatives, 8 false positives and 17 true negatives for the facial recognition system, compared to 73 true positives, 2 false negatives, 4 false positives and 21 true negatives for the fingerprint recognition system, which constitute our confusion matrix. From all the tests carried out, we can say that the decisions made by the fingerprint recognition system are better than the decisions made by the facial recognition system.

### REFERENCES

- [1] Benaliouche, H., & Touahria, M., Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. *The Scientific World Journal*, 2014.
- [2] Bopatriat Boluma Mangata et al, Contribution of an Embedded and Biometric System in a Replicated Database for Access Control in a Multi-Entry Institution. *International Journal of Science and Research (IJSR)*, Volume 10 (Issue 3), 2021.
- [3] Bopatriat Boluma Mangata et al, Performance evaluation of a single access control system. *Journal of research in engineering and applied sciences*. Volume 7 (Issue 01), 2022.
- [4] Bowers, D. M., *Access control and personal identification systems*. Butterworth-Heinemann, 2013.
- [5] Guizani, M., Zavala, M. L., & Funamizu, N., Assessment of endotoxin removal from reclaimed wastewater using coagulation-flocculation. *Journal of Water Resource and Protection*, 8(9), 855-864, 2016.
- [6] Markoulidakis, I., Rallis, I., Georgoulas, I., Kopsiaffis, G., Doulamis, A., and Doulamis, N., Multiclass Confusion Matrix Reduction Method and Its Application on Net Promoter Score Classification Problem. *Technologies*, 9(4), 81, 2021.

- [7] Melnykov, V., Chen, W. C., & Maitra, R., MixSim: An R package for simulating data to study performance of clustering algorithms. *Journal of Statistical Software*, 51, 1-25, 2012.
- [8] Miao, Y., Tian, Y., Peng, L., Hossain, M. S., & Muhammad, G., Research and implementation of ECG-based biological recognition parallelization. *IEEE Access*, 6, 4759-4766, 2017.
- [9] Williams-Young, D. B., De Jong, W. A., Van Dam, H. J., & Yang, C., On the Efficient Evaluation of the Exchange Correlation Potential on Graphics Processing Unit Clusters. *Frontiers in chemistry*, 951, 2020.
- [10] Mathivet, V., *Artificial intelligence for developers: concepts and implementations in C#*. Éditions ENI, 2017.
- [11] Norman, T. L., *Electronic access control*. Elsevier, 2011.
- [12] Távora, S., Schliep, A., & Basu, D., Federated Learning of Oligonucleotide Drug Molecule Thermodynamics with Differentially Private ADMM-Based SVM. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (pp. 459-467). Springer, Cham, 2021, September.
- [13] Douaa, MECHTA, & Radhwane, GHERBI, AUTOMATION OF THE DOMOTIC TASKS OF A HOUSE WITH THE HELP OF AN ARDUINO AND LABVIEW MAP (Doctoral dissertation, UNIVERSITE MOHAMED BOUDIAF-M'SILA), 2019.
- [14] Wirotius, M., *Authentication by handwritten signature on mobile media* (Doctoral dissertation, Tours), 2005.