Journal of Computing Research and Innovation (JCRINN) Vol. 7 No. 2 (2022) (pp43-53)
https://jcrinn.com : eISSN: 2600-8793 doi: 10.24191/jcrinn.v7i2.289
https://doi.org/10.24191/jcrinn.v7i2.289

Implementation of an Access Control System based on Bimodal Biometrics with Fusion of Global Characteristics: Application to Facial Recognition and Fingerprints

Bopatriciat Boluma Mangata[1]*, Ilunga N'kashama Dominique [2], Tebua Tene Patience Ryan[3], Bukanga Christian Parfum[4]
[1,4]Faculty of Science and Technology, University of Kinshasa, Kinshasa, D.R.Congo
[2] Faculty of Computer Science, Institut Supérieur des Arts et Métiers, Mbuji-Mayi, D.R.Congo
[3] Faculty of Computer Science, Catholic University of Congo, Kinshasa, D.R.Congo

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

Received Date: 14 July 2022
Accepted Date: 12 August 2022
Revised Date: 20 August 2022
Published Date: 1 September 2022

HIGHLIGHTS

- Implementation of the facial recognition system: Enrolment and identification.
- Implementation of the fingerprints recognition system: Enrolment and identification.
- Implementation of the embedded system under Arduino for access control to secure premises by facial recognition and fingerprints recognition system.
- Evaluation of the performance of the access control system by the confusion matrix.

ABSTRACT

Single-mode biometric systems suffer from several problems that make them unsuitable for current biometric applications that require high levels of reliability and security. These problems include the use of a single biometric trait that is prone to noise, poor capture, lack of biometric points, and deterioration of biometric input quality. In this paper, we are interested in decision fusion access control on a biometric bimodal pattern recognition system based on fingerprints and facial recognition. To realize this access control system based on facial recognition and fingerprints, we used an embedded system under Arduino, we programmed electronic systems for the automatic opening of doors without human action being. The performance evaluation of decision fusion access control on a biometric bimodal pattern recognition system is realized by means of the confusion matrix, the calculations of the evaluation parameters (Sensitivity, Specificity, Positive Predictive Value, Negative Predictive Value and False Negative). From a sample of 500 individuals, 250 of whom were registered and 250 non-registered, our access control system obtained the results of 248 true positives, 2 false negative, 1 false positive and 249 true negatives which constitute our confusion matrix. However, from the set of tests performed we can conclude that by taking advantage of the fusion of these two modalities, we increase the verification performance of system as the verification performance of bimodal system (fingerprint decision fusion and facial recognition) is applied to give even better results compared to single mode systems.

Keywords: Embedded system, biometrics, access control, automation, facial recognition, fingerprints pattern recognition

GENERAL 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 (Benaliouche & Touahria, 2014). These problems include the use of a single biometric trait that is prone to noise, poor capture, lack of biometric points, and deterioration of biometric input quality (Bopatriciat Boluma Mangata et al., 2022).

Problematics

In a practical biometric system that uses biometrics for personal recognition, a number of other issues need to be considered (Mathivet, 2017):

- ✓ Performance: the accuracy and speed of recognition achievable in terms of the resources required, and the operational and environmental factors that affect accuracy and speed;
- ✓ 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 (Norman, 2011). A single-modal biometric system uses one type of component based on a solitary methodology, such as fingerprints, iris, face and others (Raji & Fried, 2021).

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 (Wirotius, 2005). 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 (Kaur, Krishan, Sharma & Kanchan, 2020).

Hypothesis

The introduction of multimodal biometrics is a solution to these problems because multimodal systems can improve recognition performance by combining several sources of information (Bowers, D. M. (2013).).

To realize this access control system from the fusion of decisions on facial recognition and fingerprint systems, 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 (Bopatriciat Boluma Mangata et al., 2021).

Purpose and motivation of the work

Our work consists in studying, designing and implementing biometric bimodal individual recognition systems based on global decision fusion for automatic access control, while exploiting fingerprints and facial recognition.

Multimodal systems allow for improved recognition performance by combining several sources of information. They also address the problem of non-universality of some biometrics and offer a high degree of flexibility, since biometric traits that are unusable or not preferred in some individuals can be compensated for by other biometric modalities. They limit the possibility of fraud as they provide additional protection, as it is more difficult to obtain and reproduce several features at once (Cao & Jain, 2018).

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 (Hamann & Smith, 2019).
- ✓ Evaluate the performance of these systems using confusion matrices (Zeng, 2020).

Interest of the subject

The interest of such an approach is to bring a valuable help to the scientific community, by providing them with a reliable tool for automatic access control and biometric bimodal pattern recognition.

Research methodology

Critical analysis and analytical and experimental methods articulate our work. Such work is punctuated by theoretical activities (documentary research), and above all practical activities (participation in workshops, seminars and colloquia, as well as the convening of exchange/discussion sessions relating to specific aspects of the project with the other residents in their disciplinary diversities and specificities).

Implementation of a biometric bimodal access control system based on fingerprints and facial recognition

In this point of our work, we will realize an access control system from the fusion of decisions on facial recognition and fingerprint systems, 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 (Conger, Fausset & Kovaleski, 2019; Benaliouche & Touahria, 2014).

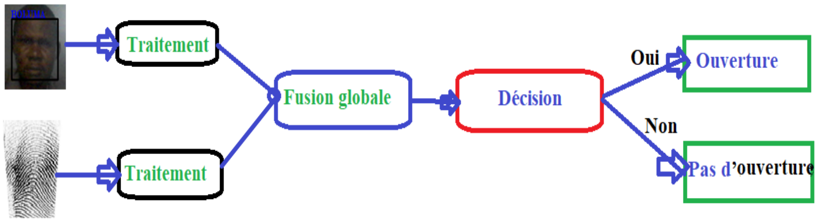


Figure 1: The global decision fusion

Hardware architecture of the system

The hardware architecture of the project is as follows (Douaa, & Radhwane, 2019):

- ✓ A camera/webcam, communicating with a computer;
- ✓ 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.

The Arduino board**,** which is programmed to analyse 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.

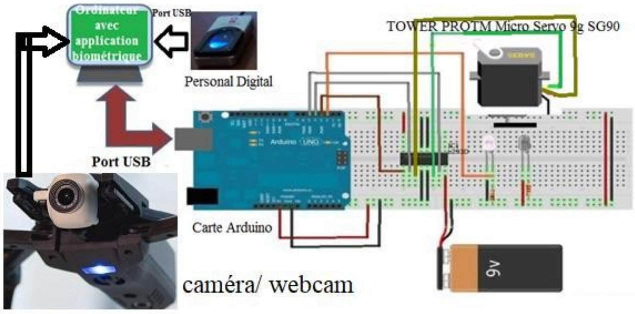
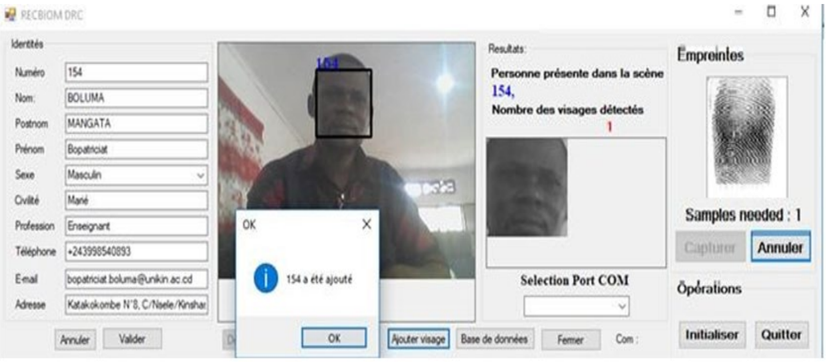

Ordinateur avec application biométrique
Port USB
Personal Digital
TOWER PROTM Micro Servo 9g SG90
Port USB
Carte Arduino
caméra/ webcam
9v

Figure 2: The project's hardware architecture

RESULTS

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



RECBIOM DRC

Identités

Numéro: 154
Nom: BOLUMA
Postnom: MANGATA
Prénom: Bopatriciat
Sexe: Masculin
Civilité: Marié
Profession: Enseignant
Téléphone: +243998540893
E-mail: bopatriciat.boluma@unikin.ac.cd
Adresse: Katakokombe N°8, C/Nsele/Kinshas

OK

154 a été ajouté

Resultats:

Personne présente dans la scène
154,
Nombre des visages détectés
1

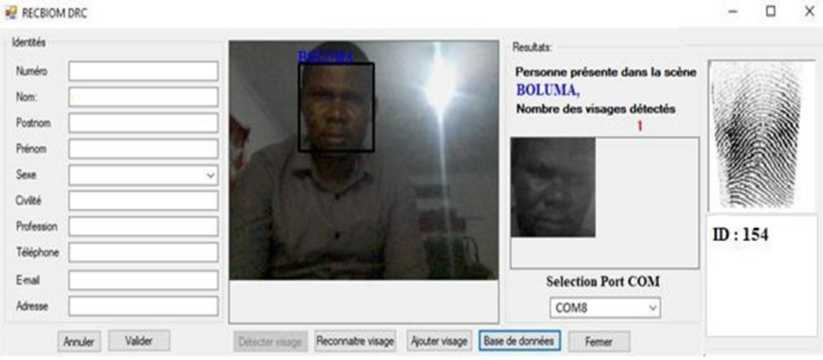
Empreintes

Samples needed : 1

Selection Port COM

Opérations

Figure 3: The enrolment window with two modalities



RECBIOM DRC

Identités

Numéro
Nom:
Postnom
Prénom
Sexe
Civilité
Profession
Téléphone
E-mail
Adresse

Resultats:

Personne présente dans la scène
BOLUMA,
Nombre des visages détectés
1

ID : 154

Selection Port COM: COM8

Figure 4: The verification window with two modes

SYSTEM PERFORMANCE

This paper item evaluates the performance of our fingerprints recognition and facial recognition-based access control system for securing premises (Conger, Fausset & Kovaleski, 2019).

On a sample of five hundred individuals, of which 250 were registered and 250 non-registered, our bimodal access control system obtained the following results: 248 true positives, 2 false negative, 1 false positive and 249 true negatives.

Estimation of evaluation parameters

When we have a representative sample of a population, we can summarize the data of the experiment by a 2x2 confusion matrix, on which the numbers are indicated (Guizani, Zavala & Funamizu, 2016).

Given two fundamental subspaces of the space E, the random events are B_1: "being enrolled" and B_2: "not being enrolled" (Caelen, 2017).

Let VP, FP, FN and VN be the events from the fundamental set E.

The elements of E, possible results of the tests are as follows (Bopatriciat Boluma Mangata et al., 2022):

- ✓ VP (True Positives), represents the individuals enrolled (E+) and accepted by the system {S} ;
- ✓ FP (False Positives), represents the individuals not enrolled (E-) and in whom the system has accepted them {S} ;
- ✓ FN (False Negatives), represents the individuals enrolled (E+) and in whom the system has rejected them {S-} ;
- ✓ VN (True Negatives), represents individuals who were not enrolled (E-) and where the system rejected them {S-};

Confusion matrix

In supervised machine learning, the confusion matrix is a matrix that measures the quality of a classification system. Each row corresponds to a real class, each column corresponds to an estimated class. The cell row L, column C contains the number of elements of the real class L that have been estimated as belonging to the class C (Heydarian, Doyle & Samavi, 2022).

One of the interests of the confusion matrix is that it quickly shows whether a classification system manages to classify correctly.

Table 1: Confusion Matrix

	E+	E-
S+	VP	FP
S-	FN	VN

Estimation of sensitivity and specificity

The sensitivity of a sign for a disease is the probability that the sign will be present if the subject has the disease in question. It is therefore the conditional probability that can be noted (Markoulidakis, Rallis, Georgoulas, Kopsiaftis, Doulamis & Doulamis, 2021):

By definition, the $Sensitivity = \mathrm{Se} = \mathrm{IP}(S/E)$ (1)

This conditional probability is estimated by the ratio of the corresponding numbers to the observed confusion matrix:

$$Se \approx \frac{VP}{VP+FN} \tag{2}$$

Note: True parameters, which are conditional probabilities, and their estimates, which are ratios of observed numbers, are noted identically, following established usage (Xu, Zhang & Miao, 2020).

The specificity of an access control test is the probability that the individual will not be enrolled and the system will deny access.

$$Specificity = \mathrm{Sp} = \mathrm{IP}(\bar{S}/\bar{E}) \approx \frac{VN}{VN+FP} \tag{3}$$

A diagnostic test is therefore all the more specific as subjects free of the disease present the S sign less often.

For a "perfect" test, i.e. one that makes no errors, the sensitivity and specificity values are equal to 1.

Estimation of predictive values

In practice, let’s assume, when a doctor receives the result of a complementary examination, positive or negative, he does not know whether the patient suffers from the condition he is trying to diagnose or not, and the probabilities he is interested in are expressed as follows: what is the probability of the presence of disease E in this patient, knowing that the examination has given a positive (or negative) result?. These probabilities are called predictive values (Ruuska, Hämäläinen, Kajava, Mughal, Matilainen & Mononen, 2018).

Specifically, we have:

- ✓ The positive predictive value (VPP**)** of a sign for a disease is the probability that the subject will have the disease if the sign is present;
- ✓ The negative predictive value (VPN) of a sign for a disease is the probability that the subject is free of the disease if the sign is absent (Zeng, 2020).

The estimates are obtained from the same data table:

$$VPP = \mathrm{IP(E/S)} \approx \frac{\mathrm{VP}}{VP+FP} \tag{4}$$

$$VPN = \mathrm{IP}(\bar{E}/\bar{S}) \approx \frac{VN}{VN+FN} \tag{5}$$

Calculation of the evaluation parameters

Let us compute the estimators of these parameters in the case where we want to evaluate the performance of the access control system on the fundamental set E, consisting of five hundred individuals distributed in the confusion matrix below:

Table 2: Individuals distributed in the Confusion Matrix

	E+	E-
S+	248	1
S-	2	249

Calculation of the evaluation parameters on the partitions of E

Let's consider events $A_1 \ldots A_n$ such that they form a partition of the fundamental set *E* (Bopatriciat Boluma Mangata & al. (2022).). By definition, A_i *are* mutually exclusive and their union is *E*:

$$\forall\ (i \neq j), \left(A_i \cap A_j \ = \emptyset\right); \tag{6}$$

$$\bigcup_{j=1}^{n} A_i \ = E \tag{7}$$

The following table illustrates the composition of our ten events that create the partition of the fundamental set E (Haghighi, Jasemi, Hessabi & Zolanvari, 2018):

Table 3: Ten events create the partition of the fundamental set E.

N°	VP	FN	FP	VN	Total
1	25	0	1	24	50
2	25	0	0	25	50
3	25	0	0	25	50
4	25	0	0	25	50
5	25	0	0	25	50
6	25	0	0	25	50
7	25	0	0	25	50
8	25	0	0	25	50
9	24	1	0	25	50
10	24	1	0	25	50
Total	248	2	1	249	500

Let's compute the estimators of these parameters in the case where we seek to evaluate the performance of the access control system.

For given thresholds S_1, S_2 ... S_{10}, and Average (AVG), we obtain the table below (Se=VP/(VP+FN), Sp=VN/(VN+FP), VPP=VP/(VP+FP), VPN=VN/(VN+FN), and FN = 1-Sp) :

Table 5: Calculation of estimating parameters.

Group	Se	Sp	VPP	VPN	FN
S_1	1	0.96	0.961538	1	0.04
S_2	1	1	1	1	0
S_3	1	1	1	1	0
S_4	1	1	1	1	0

S_5	1	1	1	1	0
S_6	1	1	1	1	0
S_7	1	1	1	1	0
S_8	1	1	1	1	0
S_9	0.96	1	1	0.961538	0
S_{10}	0.96	1	1	0.961538	0
AVG	0.992	0.996	0.996154	0.992308	0.004

Representation using bar graphs

Here’s our bar chart for the distribution of a quantitative statistical variable. This diagram represents the results of the 10 groups including the average of the observations:

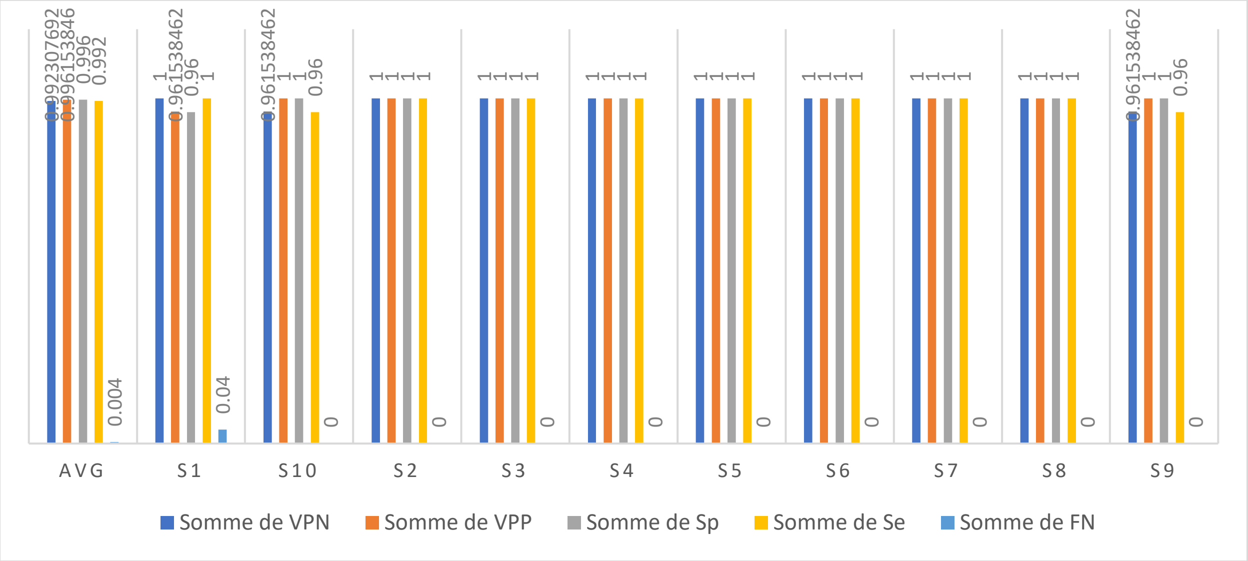


Figure 5: Bar graph

As we can notice on the figure above, the average values are represented as follows: Sensitivity is 0.992, Specificity is 0.996, Positive predictive value is 0.996154, Negative predictive value is 0.992308 and False Negative = 1-Sp is 0.004.

Graphical representation using ROC curve

A ROC curve is a plot of the sensitivity values Se versus 1-Sp.

According to the performance indicator realized through the ROC curve above, we can confirm that our model is therefore a better classifier that can diagnose whether the individual is accepted or not.

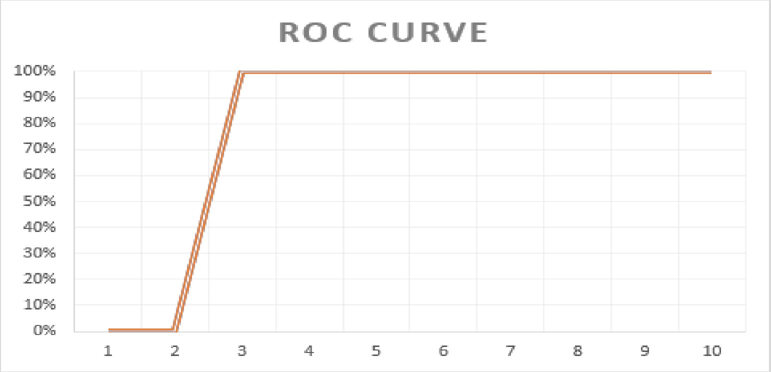


Figure 6: ROC curve

CONCLUSION

This paper consists in implementing and studying biometric bimodal individual recognition systems based on global decision fusion for automatic access control, while exploiting fingerprints and facial recognition.

Single-mode biometric systems suffer from several problems that make them unsuitable for current biometric applications that require high levels of reliability and security. These problems include the use of a single biometric trait that is prone to noise, poor capture, lack of biometric points, and deterioration of biometric input quality. That is for why in this paper, we are interested in decision fusion access control on a biometric bimodal pattern recognition system based on fingerprints and facial recognition.

To realize this access control system based on facial recognition and fingerprints, we 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 programmed electronic systems for the automatic opening of doors without human action being.

The performance evaluation of decision fusion access control on a biometric bimodal pattern recognition system is realized by means of the confusion matrix, the calculations of the evaluation parameters (Sensitivity, Specificity, Positive Predictive Value, Negative Predictive Value and False Negative).

From a sample of 500 individuals, 250 of whom were registered and 250 non-registered, our access control system obtained the results of 248 true positives, 2 false negative, 1 false positive and 249 true negatives which constitute our confusion matrix.

However, from the set of tests performed we can conclude that by taking advantage of the fusion of these two modalities, we increase the verification performance of system as the verification performance of bimodal system (fingerprint decision fusion and facial recognition) is applied to give even better results compared to single mode systems (Jacob,2019).

ACKNOWLEDGMENTS

The authors appreciate the reviewers for their contributions towards improving the quality of this research.

CONFLICT OF INTEREST DISCLOSURE

All authors declare that they have no conflicts of interest to disclose.

REFERENCES

Benaliouche, H., & Touahria, M. (2014). Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. The Scientific World Journal, 2014.

Bopatriciat Boluma Mangata & Al. (2021). 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), p2-5.

Bopatriciat Boluma Mangata & al. (2022). Performance evaluation of a single access control system. Journal of research in engeneering and applied sciences. Volume (7 Issue 01), p4-6

Bowers, D. M. (2013). Access control and personal identification systems. Butterworth-Heinemann.

Caelen, O. (2017). A Bayesian interpretation of the confusion matrix. *Annals of Mathematics and Artificial Intelligence*, *81*(3), 429-450.

Cao, K., & Jain, A. K. (2018). Automated latent fingerprint recognition. *IEEE transactions on pattern analysis and machine intelligence*, *41*(4), 788-800.

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). San Francisco bans facial recognition technology. *The New York Times*, *14*, 1.

Douaa, M. E. C. H. T. A., & Radhwane, G. H. E. R. B. I. (2019). AUTOMATISATION DES TACHES DOMOTIQUES D'UNE MAISON A L'AIDE D'UNE CARTE ARDUINO ET LABVIEW (Doctoral dissertation, UNIVERSITE MOHAMED BOUDIAF-M'SILA).

Guizani, M., Zavala, M. L., & Funamizu, N. (2016). Assessment of endotoxin removal from reclaimed wastewater using coagulation-flocculation. Journal of Water Resource and Protection, 8(9), 855-864.

Haghighi, S., Jasemi, M., Hessabi, S., & Zolanvari, A. (2018). PyCM: Multiclass confusion matrix library in Python. *Journal of Open Source Software*, *3*(25), 729.

Hamann, K., & Smith, R. (2019). Facial recognition technology. *Criminal Justice*, *34*(1), 9-13.

Heydarian, M., Doyle, T. E., & Samavi, R. (2022). MLCM: multi-label confusion matrix. *IEEE Access*, *10*, 19083-19095.

Jacob, I. J. (2019). Capsule network based biometric recognition system. *Journal of Artificial Intelligence*, *1*(02), 83-94.

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, *60*(2), 131-139.

Markoulidakis, I., Rallis, I., Georgoulas, I., Kopsiaftis, G., Doulamis, A., & Doulamis, N. (2021). Multiclass Confusion Matrix Reduction Method and Its Application on Net Promoter Score Classification Problem. Technologies, 9(4), 81.

Mathivet, V. (2017). L'intelligence artificielle pour les développeurs: concepts et implémentations en C#. Éditions ENI.

Norman, T. L. (2011). Electronic access control. Elsevier.

Raji, I. D., & Fried, G. (2021). About face: A survey of facial recognition evaluation. *arXiv preprint arXiv:2102.00813*.

Ruuska, S., Hämäläinen, W., Kajava, S., Mughal, M., Matilainen, P., & Mononen, J. (2018). Evaluation of the confusion matrix method in the validation of an automated system for measuring feeding behaviour of cattle. *Behavioural processes*, *148*, 56-62.

Wirotius, M. (2005). Authentification par signature manuscrite sur support nomade (Doctoral dissertation, Tours).

Xu, J., Zhang, Y., & Miao, D. (2020). Three-way confusion matrix for classification: A measure driven view. *Information sciences*, *507*, 772-794.

Zeng, G. (2020). On the confusion matrix in credit scoring and its analytical properties. Communications in Statistics-Theory and Methods, 49(9), 2080-2093.