|  |  |  |
| --- | --- | --- |
| **RESEARCH** **ARTICLE** |  | **OPEN ACCESS** |

Manuscript received March 27, 2023; revised April 20, 2023; accepted April 21, 2023; date of publication April 30, 2023
Digital Object Identifier (**DOI**): <https://doi.org/10.35882/jeemi.v5i2.288>

**Copyright** © 2023 by the authors. This work is an open-access article and licensed under a Creative Commons Attribution-ShareAlike 4.0 International License ([CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)).

How to cite: Bopatriciat Boluma Mangata, Odette Sangupamba Mwilu, Tebua Tene Patience Ryan, Mate Landry Gilgen, “Evaluation of Two Biometric Access Control Systems Using the Susceptible-Infected-Recovered Model, vol. 5, no. 2, pp. 119–124, April 2023.

Evaluation of Two Biometric Access Control Systems Using the Susceptible-Infected-Recovered Model

Bopatriciat Boluma Mangata1 , Odette Sangupamba Mwilu2 , Tebua Tene Patience Ryan2 , Mate Landry Gilgen3 

1 Section d’Environnement et Développement Durable, Institut Supérieur des Etudes Agronomiques de KIYAKA-GUNGU, Gungu,

 Democratic Republic of Congo

2 Faculty of Computer Science, Université Catholique du Congo, Kinshasa, Democratic Republic of Congo

3 Centre de Recherche Interdisciplinaire de l’Université Pédagogique Nationale, Université Pédagogique Nationale, Kinshasa, Democratic

 Republic of Congo

Corresponding author: Bopatriciat Boluma Mangata (bopatriciat.boluma@unikin.ac.cd).

ABSTRACT In this work, we evaluate the efficiency of decision-making in two single-mode biometric systems using facial recognition and fingerprints for access control. To do so, we first implemented an embedded system on the Arduino that opens and closes the door, then we programmed two biometric recognition systems, namely facial recognition and fingerprint recognition, and finally, we exploited the Susceptible-Infected-Covered model without demographic data to evaluate the effectiveness of these two access control systems. The variables used in the analysis are the number of individuals enrolled in the biometric system to be subjected to access control (Susceptible), the number of individuals enrolled in the biometric system and denied access by the system, as well as the number of individuals not enrolled in the biometric system and allowed access by the system (Infected), and the number of false acceptance rates and false rejection rates at time t in the systems (Recovered). In a sample of 600 people, partitioned into two balanced classes, 300 enrolled and 300 non-enrolled individuals (who are considered as impostors to allow us to know whether the systems will accept them or not). Based on the experimental tests and using the confusion matrices, our two systems obtained the following results: The facial recognition system has 270 true positives, 30 false negatives, 48 false positives, and 252 true negatives, while the fingerprint recognition system has 288 true positives, 12 false negatives, 24 false positives, and 276 true negatives. Based on the results of these confusion matrices, we used the false rejection rate and false acceptance rate to correct for these imperfections using the SIR model, i.e., 78 infected individuals for the facial recognition system, compared to 36 infected individuals for the fingerprint recognition system which we projected over 216 days. The results show that the fingerprint recognition system is more effective than the facial recognition system, according to the SIR model without demographic formulation.

INDEX TERMS access control, biometrics, Euler method for system of tree ODEs, Euler method for SIR model, pattern recognition, SIR model.

**I. INTRODUCTION**

Epidemiology is the study of the prevalence and causes of health-related conditions or occurrences within a population. It is acknowledged as the field of science that investigates infection in the human population. Epidemiology knowledge is used to investigate, plan, and assess methods for preventing health issues. The SIR and SEIR are two of the fundamental models utilized in epidemiology in this approach. Compared to the SEIR model, the SIR model is the most straightforward [6, 8, 10, 25]. We will focus more on the SIR model rather than the SEIR model for the simple reason that the SIR model is the one chosen for this work than SEIR. The SIR model divides the population into three categories: susceptible (S), infectious (I), and recovered (R). Those who are exposed to the sickness are considered susceptible (S). Those who are infectious (I) are people who have the disease and can actively spread it.

Recovered (R) refers to a class of those who have been exposed to an infection and have developed resistance to it.

The SIR technique is used to create a model for the spread of infectious illnesses among a large population in a closed environment at a specific time. Under several presumptions, the SIR model is an effective model to apply. These presumptions include that the community is set, that there is no genetic resistance that the only ways for people to exit the susceptible group are by being contagious and by recovering from the virus [19, 23, 24].

Immunity is acquired once the person has recovered [5, 7, 9]. SIR models have been used to research the spread of infectious diseases including the flu and dengue since 1760, and severe acute respiratory syndrome.

The epidemiological explanation of the mechanisms of dissemination provided by this mathematical model demonstrates its strength. It makes it possible to monitor the pace of transmission and better understand the mechanism of disease transmission. The SIR model is also applicable in a wide range of industries, including networks, computers, economics, and finance [11, 12, 21]. Because of this, we thought it would be interesting to use it in our current research to assess how effective biometric access control systems are. This study aims to evaluate the performance of two biometric access control systems using fingerprints and facial recognition by the susceptible-infected-recovered (SIR) model, which is used in epidemiology

The contribution of this study is as follows:

1. To prove that the performance of biometric systems can be evaluated using the SIR model;
2. To determine the best access control system between fingerprints and facial recognition;
3. To apply EULER METHOD FOR SIR MODEL to evaluate the performance of biometric access control systems.

**II. METHOD**

Here is a detailed explanation of the data gathering and analysis procedures used in this study.

***A. DATA COLLECTING TECHNIQUES***

Data from two biometric recognition systems experiments the facial recognition system and the fingerprint recognition system was gathered. A recognition system that makes use of the confusion matrix findings. Also, we employed bogus acceptance and rejection rates.

***B. DATA ANALYSIS TECHNIQUE***

The analysis procedure will begin with the model formulation, followed by the computation of the fundamental reproduction number, and eventually getting the numerical solution which, we projected over 216 days, or one academic year. For this phase, we employed the Euler technique for the SIR model without demography (at the rate of six working days multiplied by 4 weeks, during 9 months). SIR model version three without demographic formulation [18, 22]. The access control system population is divided into three categories in the SIR model without demographics: susceptible, infected, and recovered, as shown in (FIGURE 1).



**FIGURE 1. Flowchart of SIR model without demographics**.

The sections' specifics are [3, 10, 15]. The people who are anticipated to be exposed to access control at a specific moment are referred to as S(t) - Susceptible. Both the number of people who are not enrolled in the biometric system but were given access at time t and the number of people who are enrolled in the system but were denied access are considered to be I(t)- Infected. The incorrect acceptance and rejection rates at time t are recovered as R(t). The parameter is the recovery rate of the number of people who were exposed to access control at a specific period, and the parameter is the transmission rate of the number of people whose access to the systems has been inappropriately granted (false rejections and fake acceptances) [2, 6, 20]. The total population, *N* at time *t* is, as formulated in equation (1).

*N(t) = S(t) + I(t) + R(t)*. (1)

***C. EULER METHOD FOR SYSTEM OF TREE ORDES***

In this section, we will present Euler's method for solving the system of three differential equations [17, 18, 19], as formulated in equations (2), (3) and (4):

$\frac{dx}{dt}= f\_{1 }(t,x,y,z),$ (2)

$\frac{dy}{dt}= f\_{2 }(t,x,y,z),$ (3)

$\frac{dz}{dt}= f\_{3 }(t,x,y,z),$ (4)

for $t\_{0 }\leq t \leq t\_{n } , $step size = h, with the initial conditions.

x($t\_{0 }) $= $x\_{0 }$ $, y(t\_{0 })= y\_{0 }$, z($t\_{0 })$= $z\_{0 }$; the numerical solutions are formulated in equations (5), (6) and (7):

$x\_{i+1 }=x\_{i }+hf\_{1 }(t\_{i },x\_{i },y\_{i },z\_{i })$, i=0,1,2,3,...,n-1 (5)

$y\_{i+1 }=y\_{i }+hf\_{2 }(t\_{i },x\_{i },y\_{i },z\_{i })$, i=0,1,2,3,...,n-1 (6)

$z\_{i+1 }=z\_{i }+hf\_{2 }(t\_{i },x\_{i },y\_{i },z\_{i })$, i=0,1,2,3,...,n-1 (7)

where : $x\_{i }=x\left(t\_{i }\right), x\_{i+1 }=x\left(t\_{i+1 }\right),$ ... and $t\_{i }=t\_{0 }+ih, t\_{i+1 }= t\_{i }+h$

***D. EULER METHOD FOR SIR MODEL***

In this section, we will present the Euler method for solving the susceptible-infected-recovered model without demographics as follows [3, 10, 16, 17], as formulated in equations (8), (9), and (10):

$S^{'}\left(t\right)= -\frac{βSI}{N} ,$ (8)

$I^{'}\left(t\right)= \frac{βSI}{N}- γI,$ (9)

$R^{'}\left(t\right)= γI,$ (10)

where S, I, and R represent, the susceptible, infected, and recovered total number of individuals representing each compartment. *N* is the total population size, as defined in equations (11) and (12):

Since,

$\frac{dS}{dt}+ \frac{dI}{dt}+ \frac{dR}{dt}=0$ (11)

Follows that,

$N=S\left(t\right)+I\left(t\right)+R\left(t\right) N=Constante$ (12)

The dynamics of the infectious class depend on the following ratio, as formulated in equation (13):

$R\_{0}= \frac{β}{γ} ,$ (13)

It's called a basic reproduction ratio. This ratio is derived as the expected number of new infections called secondary infections from a single infection in a population. If the value of the reproduction ratio is,

$$R\_{0}<1 ,$$

Each infected individual will only infect one other individual, and the disease will eventually die out. $R\_{0}=1 .$ Each infected individual will infect one more individual, and the disease will continue to spread yet remain stable. $R\_{0}>1 .$ Each infected individual will infect other individuals, and the disease will continue to spread and expand, with the potential to become a pandemic.

for $t\_{0 }\leq t \leq t\_{n } , $step size = h, with the initial conditions.

S($t\_{0 }) $= $S\_{0 }$ $, I(t\_{0 })= I\_{0 }$, R($t\_{0 })$= $R\_{0 }$; (Warning $R\_{0 }= R\left(t\_{0 }\right)=Not the basic reproduction number)$.

The numerical solutions are obtained in equations (14), (15) and (16) [3, 10, 16, 17]:

$S\_{i+1 }=S\_{i }-h\frac{βS\_{i }I\_{i }}{N} $i=0,1,2,3,...,n-1 (14)

$I\_{i+1 }=I\_{i }+h\frac{βS\_{i }I\_{i }}{N}-hγI\_{i }$i=0,1,2,3,...,n-1 (15)

$R\_{i+1 }=R\_{i }+hγI\_{i }$i=0,1,2,3,...,n-1 (16)

where : $t\_{i+1 }=t\_{i }+h, S\_{i }=S\left(t\_{i }\right), S\_{i+1 }=S\left(t\_{i+1 }\right)=S(t\_{i }+h)$, we obtain the equations (17), (18) and (19):

$S\left(t\_{i }+h\right)=S\left(t\_{i }\right)-h\frac{βS\left(t\_{i }\right)I\left(t\_{i }\right)}{N} $ (17)

$I\left(t\_{i }+h\right)=I\left(t\_{i }\right)+h\frac{βS\left(t\_{i }\right)I\left(t\_{i }\right)}{N} -hγI\left(t\_{i }\right)$ (18)

$R\left(t\_{i }+h\right)=R\left(t\_{i }\right)+hγI\left(t\_{i }\right)$ (19)

where: $h=1, t\_{0 }=0, t\_{1 }=t\_{0 }+h=0+1=1, S\_{0 }$=$ S\left(t\_{0 }\right)=S\left(0\right), S\_{1 }$=$ S\left(t\_{1 }\right)=S\left(1\right)$, we obtain the equations (20), (21) and (22):

$S\left(t\_{1 }\right)=S\left(t\_{0 }\right)-h\frac{βS\left(t\_{0 }\right)I\left(t\_{0 }\right)}{N} $ (20)

$I\left(t\_{1 }\right)=I\left(t\_{0 }\right)+h\frac{βS\left(t\_{0 }\right)I\left(t\_{0 }\right)}{N} -hγI\left(t\_{0 }\right)$ (21)

$R\left(t\_{1 }\right)=R\left(t\_{0 }\right)+hγI\left(t\_{0 }\right)$ (22)

where: $h=1, t\_{0 }=0, t\_{1 }=t\_{0 }+h=0+1=1, S\_{0 }$=$ S\left(t\_{0 }\right)=S\left(0\right), S\_{1 }$=$ S\left(t\_{1 }\right)=S\left(1\right)$, we obtain the equations (23), (24) and (25):

$S\left(1\right)=S\left(0\right)-h\frac{βS\left(0\right)I\left(0\right)}{N} $ (23)

$I\left(1\right)=I\left(0\right)+h\frac{βS\left(0\right)I\left(0\right)}{N} -hγI\left(0\right)$ (24)

$R\left(1\right)=R\left(0\right)+hγI\left(0\right)$ (25)

**III. RESULTS**

In this part, we analyze two access control systems using facial recognition and fingerprints. In this part, we examine the decisions of two access control systems based on facial recognition and fingerprints and evaluate the performance of both access control systems [11, 12, 13].

***A. FINGERPRINTS IMPLEMENTATION***

In this part, we will implement a fingerprint-based access control system [1, 3]. It uses an embedded system under Arduino, which offers the possibility to program and configure electronic implementations. Specifically, program an electronic system to open the door automatically [1, 2, 14]. Below are some graphical interface representations of the application, as shown in (FIGURE 2) and (FIGURE 3):



**FIGURE 2. Fingerprints enrolment**



**FIGURE 3. Fingerprint Verification**

In a sample of 600 people, 300 enrolled and 300 not enrolled, our fingerprint-based single-mode access control system provided the following results: 288 true positives, 12 false negatives, 24 false positives, and 276 true negatives constitute the following confusion matrix [7], as represented in TABLE 1.

**TABLE 1**

**Individuals distributed in the confusion matrix**

|  |  |  |
| --- | --- | --- |
|  | E+ | E- |
| S+ | 288 | 12 |
| S- | 24 | 276 |

Following this result, fingerprint recognition can be used to evaluate the performance of the access control system and can be represented graphically with curves as follows:

where $β=0,2; γ=0,1 and N=600$

Initial conditions: S($0) $= 564 for fingerprint recognition $, I\left(0\right)=$36 for fingerprint recognition, R($0)$= 0 for both systems. To find : S($t) $= ? $, I\left(t\right)= ?$, R($t)$= ? (for t<217 days). Given $β=0,2 and γ=0,1$ ; $R\_{0}= \frac{β}{γ}=\frac{0,2}{0,1}=2>1,$ we obtain the result of the SIR model using fingerprint recognition as follows in (TABLE 2):

**TABLE 2**

**Result of the SIR model by fingerprints**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ti | S(ti) | I(ti) | R(ti) | S+I+R |
| 0 | 564 | 36 | 0 | 600 |
| 1 | 557.232 | 39.17  | 3.60 | 600 |
| 2 | 549.96 | 42.53  | 7.52  | 600 |
| 3 | 542.16  | 46.07 | 11.77  | 600 |
| 4 | 533.84  | 49.79  |  16.38  | 600 |
| 5 | 524.98  | 53.67  | 21.36  | 600 |
| 6 |  515.58  | 57.69  |  26.72  | 600 |
| 7 | 505.67  | 61.84  |  32.49  | 600 |
| 8 | 495.25 | 66.08  | 38.68  | 600 |
| 9 | 484.34  | 70.38 | 45.28  | 600 |
| 10 | 472.97 | 74.70  | 52.32  | 600 |
| ... | ... | ... | ... | ... |
| 215 | 106.46  |  0.00  | 493.54  | 600 |
| 216 | 106.46 | 0.00 | 493.54 | 600 |

Following this result, fingerprint recognition can be used to evaluate the performance of the access control system and can be represented graphically with curves as follows (FIGURE 4).

**FIGURE 4. Graphical output of the SIR model by fingerprints**

***B. FACIAL RECOGNITION IMPLEMENTATION***

In this part of our work, we use an embedded system under the Arduino which gives us the possibility to realize an access control system based on facial recognition systems and to parameterize our programming and electronic achievements. More precisely, it programs electronic systems. Doors open automatically without human intervention [14, 15]. Below are some graphical interface representations of the application, as shown in (FIGURE 5) and (FIGURE 6).



**FIGURE 5. Facial recognition enrolment**



**FIGURE 6. Facial recognition verification**

In a sample of 600 individuals, 300 of whom were registered and 300 non-registered, our single-mode input/output monitoring system using face recognition obtained the following results. The 270 true positives, 30 false negatives, 48 false positives, and 252 true negatives make up the following confusion matrix [7], as follows in (Table 3):

**TABLE 3.**

**Individuals distributed in the Confusion Matrix**

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

Based on these results, we can evaluate the performance of the two systems and represent them graphically as follows:

Where $β=0,2; γ=0,1 and N=600$. Initial conditions: S($0) $= 522 for face recognition$, I\left(0\right)= 78 $for face recognition, R($0)$= 0 for both systems. To find : S($t) $= ? $, I\left(t\right)= ?$, R($t)$= ? (for t<217 days). Given $β=0,2 and γ=0,1$ ; $R\_{0}= \frac{β}{γ}=\frac{0,2}{0,1}=2>1,$ we obtain the result of the SIR model using facial recognition as follows in (TABLE 4).

**TABLE 4**

**Result of the SIR model using facial recognition**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ti | S(ti) | I(ti) | R(ti) | S+I+R |
| 0 | 522 | 78 | 0 | 600 |
| 1 | 508.428 | 83.77 | 7.80 | 600 |
| 2 | 494.23 | 89.59 | 16.18 | 600 |
| 3 | 479.47 | 95.39 | 25.14 | 600 |
| 4 | 464.22 | 101.10 | 34.68 | 600 |
| 5 | 448.58 | 106.63 | 44.79 | 600 |
| 6 | 432.64 | 111.91 | 55.45 | 600 |
| 7 | 416.50 | 116.86 | 66.64 | 600 |
| 8 | 400.27 | 121.40 | 78.33 | 600 |
| 9 | 384.07 | 125.46 | 90.47 | 600 |
| 10 | 368.01 | 128.97 | 103.01 | 600 |
| ... | ... | ... | ... | ... |
| 215 | 93.92 | 0.00 | 506.08 | 600 |
| 216 | 93.92 | 0.00 | 506.08 | 600 |

Based on this result, which allows us to evaluate the performance of our face recognition system, we can graphically represent it with the following graph (FIGURE 7):

**FIGURE 7. Graphical output of the SIR model using facial recognition**

From all the tests performed, we can say that the determination of the fingerprint recognition system is better than the determination of the facial recognition system [14].

**IV. DISCUSSION**

Compared with the work of Sharif [18], which consisted of The Effectiveness of Online Video Marketing on Facebook Using Susceptible-Infected-Recovered (SIR) Mode, our approach was to show that the effectiveness of biometric access control systems can also be evaluated using SIR models. On the other hand, if we look at the work of Mangata [14], which consists of comparative studies between a facial recognition system and a fingerprint recognition system for access control, our approach in this work proves that the results obtained by fingerprints are better than the results obtained by facial recognition, using the SIR model. Some of the limitations and weaknesses of this study are: (a) the SIR model without demographic data is a simplified version of the epidemic dynamics, which does not account for factors such as birth, death, migration, age structure, and heterogeneity of the population. These factors may affect the transmission and recovery rates of the biometric systems, as well as the basic reproduction number, (b) the study only considers two single-mode biometric systems, namely facial recognition and fingerprint recognition, and does not compare them with other biometric modalities or multimodal systems, which may have different performance and robustness, (c) the study does not provide any details on how the facial recognition and fingerprint recognition systems were implemented, such as the algorithms, databases, hardware, and software used, which may affect the reproducibility and validity of the results.

The current page is research that evaluates the performance of two biometric access control systems using facial recognition and fingerprints by the Susceptible-Infected-Recovered (SIR) model, which is used in epidemiology12. The implication of this study is: (a) it shows that the SIR model can be applied to assess the effectiveness of biometric systems in terms of false acceptance and false rejection rates, which are important metrics for security and usability, (b) it demonstrates that the fingerprint recognition system is more efficient than the facial recognition system, according to the SIR model, which means that it has lower false acceptance and false rejection rates, and thus higher accuracy and reliability, (c) it provides a novel and interdisciplinary approach to combine biometrics, embedded systems, and mathematical modeling to solve real-world problems in access control and identity verification.

**V. CONCLUSION**

In this work, we use the Euler method to evaluate the effectiveness of two single-mode access control systems based on facial recognition and fingerprints and solve the Susceptible-Infected-Recovered model without demographic data. To evaluate these access control systems, we implemented two biometric authentication systems based on fingerprint and facial recognition. The system can interact with Arduino-based embedded systems to automatically open doors without human intervention. In a sample of 600 people, 300 enrolled and 300 not enrolled, two simple access control systems each provided the following results: The facial recognition system had 270 true positives, 30 false negatives, 48 false positives, and 252 true negatives, while the fingerprint recognition system had 288 true positives, 12 false negatives, 24 false positives, and 24 true negatives, making 276. These results gave us two confusion matrices. Based on these two confusion matrices, we were able to exploit the false rejection rates and false acceptance rates to correct for these inconveniences using the SIR model, i.e., 78 infected individuals for the facial recognition system, compared to 36 infected individuals for the fingerprint recognition system which we projected over 216 days, i.e. one academic year (six working days multiplied by 4 weeks, for 9 months). In this paper, when comparing the two biometric systems mentioned above, we did not take into account the imprecision of the sensors but rather the positive or negative results of the tests performed. According to all the tests and calculations, the results show that the fingerprint recognition system is more efficient than the facial recognition system, according to the SIR model without demographic formulation.

**REFERENCES**

1. Aliouche, S., & Chetibi, H. E. (2021). Reconnaissance biométrique des personnes par la caractérisation de la rétine (Doctoral dissertation, Université jijel).
2. Bagal, D. K., Rath, A., Barua, A., & Patnaik, D. (2020). Estimating the parameters of susceptible-infected-recovered model of COVID-19 cases in India during lockdown periods. *Chaos, Solitons & Fractals*, *140*, 110154.
3. Bonazza, P. (2019). Système de sécurité biométrique multimodal par imagerie, dédié au contrôle d’accès (Doctoral dissertation, Bourgogne Franche-Comté).
4. Dhanwant, J. N., & Ramanathan, V. (2020). Forecasting covid 19 growth in india using susceptible-infected-recovered (sir) model. *arXiv preprint arXiv:2004.00696*.
5. Duan, H., & Nie, W. (2022). A novel grey model based on Susceptible Infected Recovered Model: A case study of COVD-19. *Physica A: Statistical Mechanics and its Applications*, *602*, 127622.
6. Forgács, P., Libál, A., Reichhardt, C., Hengartner, N., & Reichhardt, C. J. O. (2022). Using active matter to introduce spatial heterogeneity to the susceptible infected recovered model of epidemic spreading. *Scientific Reports*, *12*(1), 11229.
7. Gurova, S. M., Gurov, T., & Karaivanova, A. (2020, December). Scalability study of MPI algorithm for a predator-prey model with SEIRS epidemic disease. In *AIP Conference Proceedings* (Vol. 2302, No. 1, p. 030001). AIP Publishing LLC.
8. Hassan, S. A., Teoh, Y. K., Nasir, D. S. M., & Sharil, N. S. (2022). Simulation of COVID-19 Trend in Selangor via SIR Model of Infectious Disease. *Journal of Computing Research and Innovation*, *7*(2), 294-303.
9. Kahina, O., & Ania, Z. (2019). Contrôle d’accès à base d’empreinte digitale (Doctoral dissertation, Université Mouloud Mammeri).
10. Liu, R., Pisco, A. O., Braun, E., Linnarsson, S., & Zou, J. (2022). Dynamical systems model of RNA velocity improves inference of single-cell trajectory, pseudo-time and gene regulation. *Journal of Molecular Biology*, *434*(15), 167606.
11. Mangata, B. B., Nakashama, D. I., Muamba, D. K., & Christian, P. B. (2022). Implementation of an access control system based on bimodal biometrics with fusion of global decisions: Application to facial recognition and fingerprints. Journal of Computing Research and Innovation, 7(2), 43-53.
12. Mangata, B. B., Muamba, K., Khalaba, F., Parfum, B. C., & Mbambi, K. (2022). Parallel and Distributed Computation of a Fingerprint Access Control System. Journal of Computing Research and Innovation, 7(2), 1-10.
13. Mangata, B. B., Mbambi, K., Muamba, K., & Khalaba, F. (2022). Modeling and implementation of an automatic Access control system for secure permises using facial recognition. Journal of Computing Research and Innovation, 7(2), 11-22.
14. Mangata, B. B., N’kashama, D. I., Christian, P. B., & Muamba, D. K. (2022). COMPARATIVE STUDIES BETWEEN A FACIAL RECOGNITION SYSTEM AND A FINGERPRINT RECOGNITION SYSTEM FOR ACCESS CONTROL. IJISCS (International Journal of Information System and Computer Science), 6(2), 69-75.
15. Mangata, B. B., Eugène, M. M., Nzambi, B. M., Maheshe, C. B., & Christian, P. B. (January 2022)**.** PERFORMANCE EVALUATION OF A SINGLE-MODE BIOMETRIC ACCESS CONTROL SYSTEM. Journal of Research in Engineering and Applied Sciences, Volume 7, Issue 1, 270-275
16. Meng, Q., & Jiang, X. (2022, September). A Simple Numerical Solution Framework for Ordinary Differential Equations Based on Reduced MIPS Instructions. In *2022 IEEE 4th International Conference on Circuits and Systems (ICCS)* (pp. 53-59). IEEE.
17. Saeedian, M., Khalighi, M., Azimi-Tafreshi, N., Jafari, G. R., & Ausloos, M. (2017). Memory effects on epidemic evolution: The susceptible-infected-recovered epidemic model. *Physical Review E*, *95*(2), 022409.
18. Sharif, N., Bidin, J., Ku Akil, K. A., & Mazlan, S. F. (2022). The effectiveness of online video marketing on Facebook using Susceptible-Infected-Recovered (SIR) model. *Journal of Computing Research and Innovation (JCRINN)*, *7*(2), 54-65.
19. Shoaib Arif, M., Raza, A., Abodayeh, K., Rafiq, M., Bibi, M., & Nazeer, A. (2020). A numerical efficient technique for the solution of susceptible infected recovered epidemic model. *Computer Modeling in Engineering & Sciences*, *124*(2), 477-491.
20. Srivastava, H. M., & Günerhan, H. (2019). Analytical and approximate solutions of fractional-order susceptible-infected-recovered epidemic model of childhood disease. *Mathematical Methods in the Applied Sciences*, *42*(3), 935-941.
21. Teoh, Y. K., Hamdan, N. F., Hasan, S. A., Ariffin, A. F., & Mahat, A. (2022). Application of Susceptible-Infected-Removed Model with Vital Dynamics for COVID-19 Outbreak in Malaysia. *Journal of Computing Research and Innovation*, *7*(2), 82-87.
22. Televnoy, A., Ivanov, S., Zudilova, T., & Voitiuk, T. (2021, January). Neural ODE Machine Learning Method with Embedded Numerical Method. In *2021 28th Conference of Open Innovations Association (FRUCT)* (pp. 451-457). IEEE.
23. Veeresha, P., Ilhan, E., Prakasha, D. G., Baskonus, H. M., & Gao, W. (2022). A new numerical investigation of fractional order susceptible-infected-recovered epidemic model of childhood disease. *Alexandria Engineering Journal*, *61*(2), 1747-1756.
24. Wang, P., Li, Y., Yu, P., & Zhang, Y. (2021). The analysis of urban flood risk propagation based on the modified susceptible infected recovered model. *Journal of Hydrology*, *603*, 127121.
25. Wang, W., Liu, Q. H., Zhong, L. F., Tang, M., Gao, H., & Stanley, H. E. (2016). Predicting the epidemic threshold of the susceptible-infected-recovered model. *Scientific reports*, *6*(1), 1-12.

|  |  |
| --- | --- |
| RSG | Bopatriciat BOLUMA MANGATA received his B.Sc., and M.Sc. degree in Computer Science from University of Kinshasa, D.R.Congo, in 2015 and 2022 respectively. He is currently a teaching assistant and Ph.D. Student at the Department of Mathematics, Statistics and Computer Science, Faculty of Science and Technology, University of Kinshasa. His research interests include artificial intelligence, and distributed systems.¶ |
|  | Odette SANGUPAMBA MWILU. Doctor in Computer Science. University Professor. Dean of the Faculty of Computer Sciences at the Catholic University of Congo. Her research focuses on Information Systems, Business Intelligence and Cloud Computing. She teaches courses in computer analysis methods, relational database, distributed database, database administration, database techniques, business intelligence systems, and Internet of Things and cloud computing. |
|  | Patience Ryan Tebua. Bachelor in Computer Engineering \*UNIKIN\* (class 2017-2018). Cybersecurity Analyst \*I-CSSI\* (class 2022) , Teaching Assistant and Researcher at the Catholic University of Congo (Faculty of Computer Sciences) (Since 2021). Research area: IT- Security and Auditor, Cybersecurity, Blockchain, Penetration testing, etc. |
|  | Mate Landry Gilgen, born in Kinshasa in 1988, graduated in computer science from UNIKIN in January 2013, graduated from UPN in February 2021 and is currently a PhD student in computer science, computer engineering orientation at UPN. Computer science teacher in several higher education institutions in DRC and computer science researcher. |