An intelligent criminal detection system: A case study of Beni-town

AGANZE Baraka[*], Sage KATALIKO[**], ASAKA Digne[*]

[*] Department of Computer Engineering, Christian Bilingual University of Congo,
[**] Department of Information Technology, AMA University,

DOI: 10.29322/IJSRP.11.11.2021.p11961
http://dx.doi.org/10.29322/IJSRP.11.11.2021.p11961

***Abstract*-**The central prison in Beni usually gets attacked, and most of the prisoners take the opportunity to escape. This situation enhances the level of criminality in Beni. This research paper presents an intelligent criminal detection system. We use a face recognition mechanism to detect criminals who escape from the prisons and other wanted people. The objective of the following research paper is to reduce the crime rate in the town of Beni and its surrounding by combatting the flight of criminals or wanted people. We advocate so that the system may be installed in airports, entry points and some public places.

***Index Terms*-** : Beni, criminals, wanted, face recognition, airport

I. INTRODUCTION

In October 2020 the central prison in the town of Beni which is located in the Democratic Republic of Congo was attacked by an armed group. Statistics show that only 33 escapees were found out of a total of 1335 escaped prisoners [1]. This article presents an intelligent criminal detection system.

In recent studies [2], Alireza Chevelwalla et al designed a criminal face recognition system. The purpose was to identify criminals during investigations. The authors of the study stored criminal images in a database with their details. Next, the stored images were segmented into four slices: forehead, eyes, nose and lips. The slices were stored in a database. Finally, eyewitnesses should select the slices on the screen so that the facial image can be retrieved from the database. One drawback we notice in their system is that they need eyewitnesses to gather the segmented image and to see if the image matches an image already registered in the database; this can lead to inaccuracy and false results but also to delays in the investigations and in the capture of the criminal.

Sometimes it is deplorable that some criminals remain at large due to a lack of the necessary means of identification. Some of the escaped criminals take a new identity by falsifying their ID cards. As a result, the criminals remain at large while carrying out illegal activities with impunity, committing new crimes. Many of them even manage to bypass the control system at the airport, roadblocks and ports, and manage to leave the country without any effort.

Thus, we present an intelligent system based on computer vision and we believe that it is an effective solution for the detection of a criminal or people who are wanted by the courts. We advocate for its deployment at entry points (airports, barriers, railway stations, ports) to fight against the flight of wanted persons.

The objective of this work is to reduce the crime rate in the town of Beni and its surroundings by combating the flight of criminals or people wanted by the courts.
This paper first discusses Artificial intelligence and the use of facial recognition systems. Second we design the system using the Unified Modeling Language. After the design, we present the results.

II. OVERVIEW OF ARTIFICIAL INTELLIGENCE

Marvin Lee Minsky, in 1956, defined artificial intelligence as “the science of making machines do things that would require intelligence if done by men” [3]. Artificial intelligence involves implementing a number of techniques that allow machines to mimic some form of real intelligence. Artificial intelligence is capable of performing tasks intelligently without being explicitly instructed and it is also capable of thinking and acting rationally and humanely.

Categories of artificial intelligence

There are two main types of artificial intelligence: *weak artificial intelligence* and *strong artificial intelligence*. These two concepts were coined by John Searle in order to differentiate the performance levels in different kinds of AI machines.

A. Weak artificial intelligence

Weak AI is used in simple tasks. It's a fairly limited intelligence by its functions because it only works with a succession of algorithms programmed by humans to simulate intelligence. This is the most common form of AI available in today's industries. Weak AI cannot function beyond what is assigned to the system. Indeed, it is trained to perform a single specific task.

B. Strong artificial intelligence

Strong AI, which is still a futuristic idea, is based on the analysis of a concrete situation (evolutionary algorithm, neuron system). It’s looking for a real autonomy; for researchers, the robot with a

strong AI would have a real consciousness and would experience feelings. Moreover, his reasoning must be close to that of the human being, it is the ambitious dream of many researchers to reach this stage.

Some subsets of Artificial Intelligence

There are many subsets of AI but this article presents two of them. Let's find below various subsets of artificial intelligence:

- Machine learning
- Machine vision

A. Machine Learning

Machine Learning is an artificial intelligence technology that allows computers to learn without having been explicitly programmed for this purpose [5]. To learn and grow, however, computers need data to analyze and train on.
Machine learning can be subdivided into three types:

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

Supervised learning:
Supervised learning is a type of machine learning in which machine learns from labeled data and then predict the output. A supervised learning agent needs to find out the function that matches a given sample set.
Supervised learning further can be classified into two categories of algorithms: **Classifications**, **Regression**

Unsupervised learning:
Unsupervised learning is associated with learning without supervision or training. In unsupervised learning, the algorithms are trained with data which is neither labeled nor classified. In unsupervised learning, the agent needs to learn from patterns without corresponding output values.
Unsupervised learning can be classified into two categories of algorithms: **Clustering, Association rules**

Reinforcement learning:
Reinforcement learning is a type of learning in which an AI agent is trained by giving some commands, and on each action, an agent gets a reward as a feedback. Using these feedbacks, agent improves its performance.
Reward feedback can be positive or negative which means on each good action, agent receives a positive reward while for wrong action, it gets a negative reward.
Reinforcement learning is of two types: **Positive Reinforcement learning**, **Negative Reinforcement learning**

Deep Learning:
Deep Learning is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks [6]. Deep Learning concepts are used to teach machines what comes naturally to us humans. Using Deep Learning, a computer model can be taught to run classification acts taking image, text, or sound as an input.

B. Machine vision

Machine vision (computer vision) is a field of study that seeks to enable computing systems to understand and process digital photographs, videos, displays etc. and behave as if they have a vision just as other living beings have [6]. The goal of computer vision is to draw inferences from visual sources and apply it towards solving a real-world problem such as image classification, videos and traffic analysis, face recognition, etc.

Face recognition

Recent years have seen significant progress in this area due to advances in modeling and face analysis techniques; systems have been developed for face detection and tracking, but reliable faces [7]. There are several reasons for the recent increased interest in facial recognition, including growing public concern for security, the need for identity verification in the digital world, and the need for facial analysis and modeling techniques in multimedia data management.
Automatic face recognition is done in three main steps

1. Face detection.
2. Extraction and normalization of facial features.
3. Identification and/or verification

Image acquisition is very essential in a facial recognition system. It's necessary to succeed in capturing essential information without noise. Facial recognition can be done using images (photos) or from image sequences (videos) or in real time.
The process of face recognition is a great visual task for a human. While humans can detect and identify faces in a scene easily, designing and building an automatic system that accomplishes these tasks is a serious challenge. This challenge is all the greater when the conditions for acquiring images are highly variable [8].
Here are some face recognition difficulties:

- The variation of the pose.
- The change of enlightenment.
- Change in facial expressions.
- Influence of occultations.
- Plastic surgery.
- Identical twins.

III. DESING OF THE SYSTEM

Modeling is the representation of a system in the easiest way to understand. It consists in creating a simplified representation of a problem: the model, which is an abstract and simplified representation (which excludes certain details), of an entity (phenomenon, process, system, etc.) of the real world in order to describe, explain or predict it. With model it is possible to simply represent a problem, a concept and simulate it. We used UML to model our system. Modeling opened us up to implementing our

system. Two UML diagrams help us to understand the system: the use case diagram and the activity diagrams.

1) Use case diagram

To first understand the features of the system, we present the use case diagram.

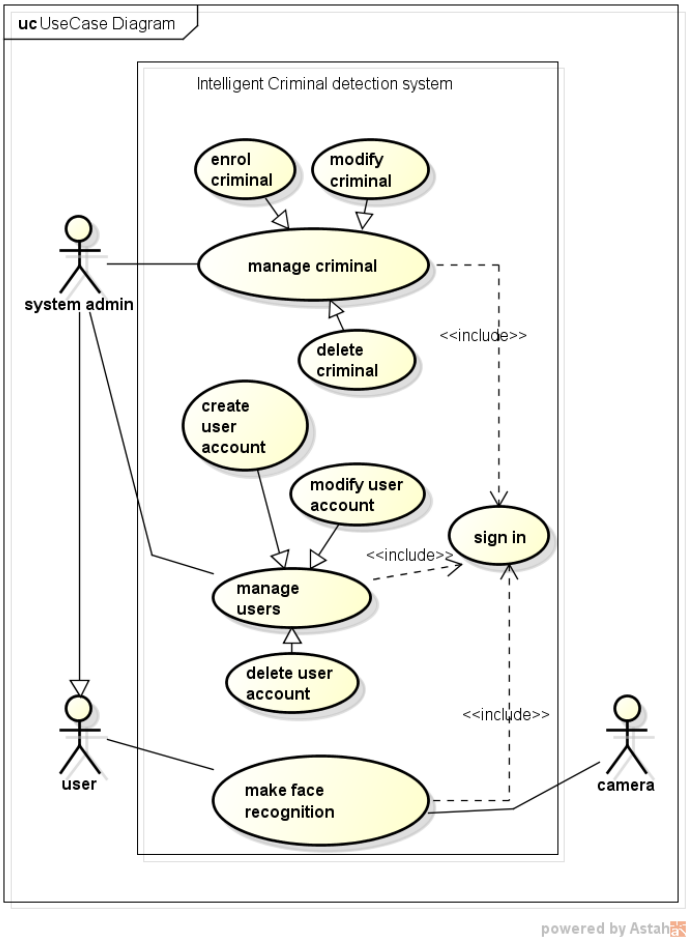

Figure 1: Use case diagram

The use case diagram presents the features of the system. The bellow table describes the different use cases (features).

Use case	Actor	Description	requirements
Manage criminal	System admin	This features is about managing a criminal. By managing a criminal we mean enroling the criminal, modifying its details or deleting the records	Being authenticated
Manage users	System admin	This features is about managing user accounts By managing user accounts we mean creating user accounts, modifying user accounts or deleting user accounts	Being authenticated
Make face recognition	• System admin (primary actor) • Camera (secondary actor)	Here the system recognizes faces of people in order to chek if the person is wanted by the courts	

To understand the most important features of the system, we need do describe them with the help of activity diagrams.

2) Enrolement activity diagram

The following activity diagram gives a clear description about the enrolement use case. Enrolment is done when the criminal is arrested and judged by the courts. Its identities and photos need to be taken so that in case he escapes, his face may be easily recognized by the system. These are the different activies for the enrolment:

(1): The system administrator requests the enrolment form
(2): The interface displays the enrolment form
(3): The system administrator fills and submit the enrolment form
(4): The submitted form is checked for validation
(5): The camera starts capturing images
(6): Image processing
(7): Signature extraction
(8): store data : Here we store the identity of the criminal and the signature of the image, for future use

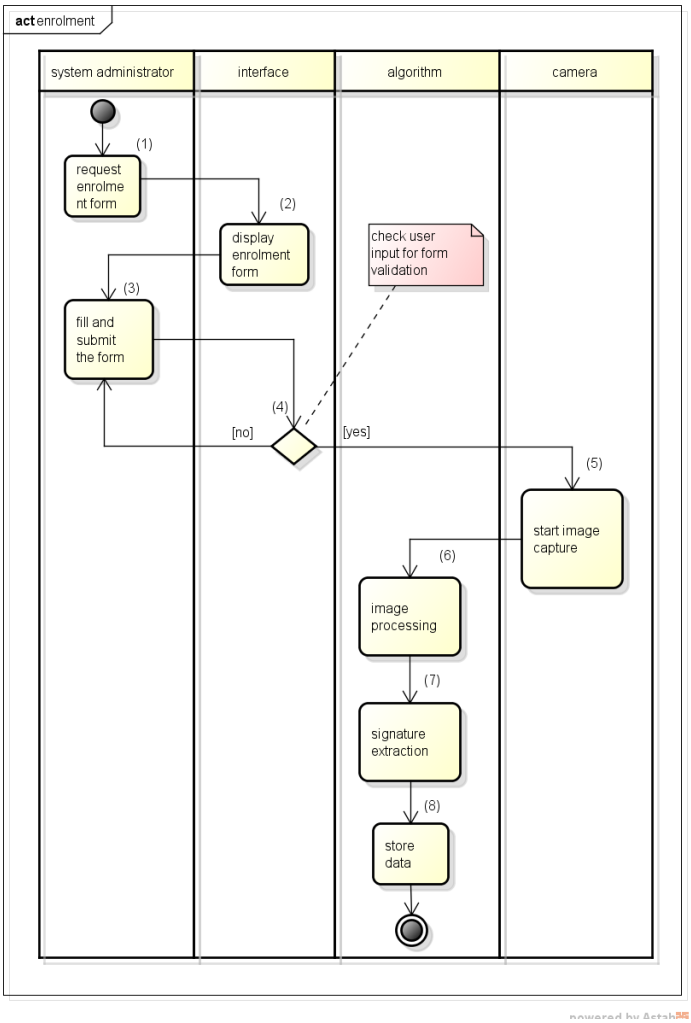

Figure 2: Criminal enrolment activity diagram

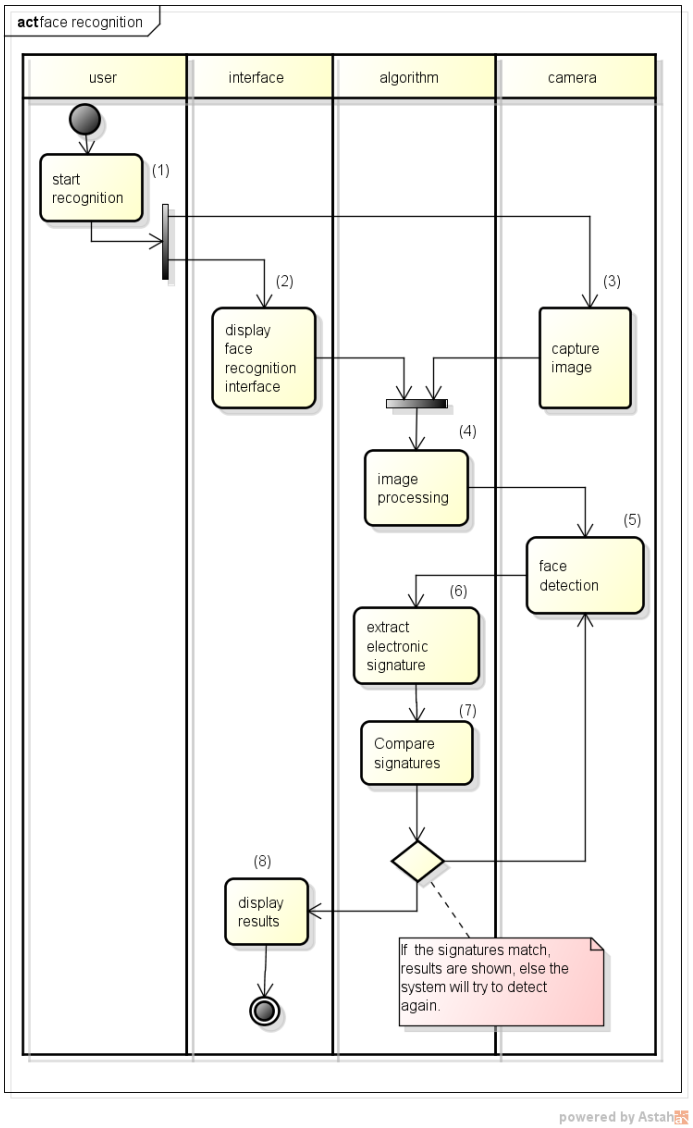

Figure 3: Face recognition activity diagram

3) Criminal detection activity diagram

The following activity diagram gives a clear description about the face recognition use case. Criminal detection is done when someone faces the cameras. The face's signature is compared with the already known signatures. If there is a match, the application users are notified for further operations. The following are the different activies for the criminal detection use case:

(1): start recognition
(2):display face recognition interface
(3):capture image
(4):image processing
(5): face recognition
(6):extract electronic signature
(7): compare signatures : signatures are compared. If there is a match, the results are displayed (8), otherwise the system continues to make recognition

IV. RESULTS AND ANALYSIS

1) System architecture

The architecture of the system is made with different blocs:

- **Remote server**: In this machine we deploy the database and the business logic of the application. The application is written in Python, using the opencv library for image processing
- We have different **sites** where we install IP cameras. The cameras are connected to the router with a control station and a modem. A control station is a thin client used to display notifications. A modem is used to provide Internet connection to the materials.

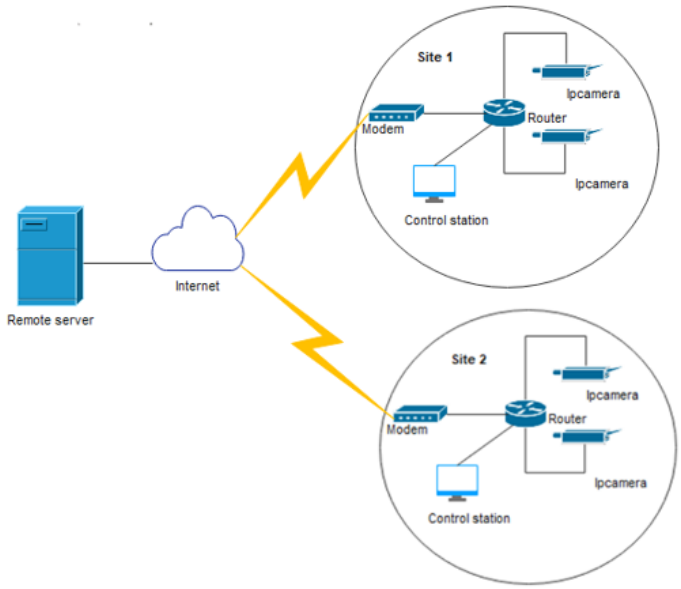

Figure 4: System architecture

2) Results and Performance evaluation of the algorithm

The tests have been done using a laptop with the following characteristics:

- Model: HP NOTEBOOK-15-da0072na
- Hard drive: 1TB
- CPU: Intel® Core ™ i5-8250U 1.60 GHZ 1.80 GHZ
- RAM: 4GB

The algorithm used for classification is evaluated using the following confusion matrix.

n=100	Predicted: NO	Predicted: YES	
Actual no	TN=40	FP=0	40
Actual yes	FN=1	TP=59	60
	41	59	

The following performance metrics give a clear idea about the performance:

$$\text{Accuracy}=\frac{TP+TN}{n}=\frac{59+40}{100}=\frac{99}{100}=0.99=99\%$$

$$\text{Misclassification rate}=\frac{FP+FN}{n}=\frac{0+1}{100}=0.01=1\%$$

$$\text{True positive rate (Recall)}=\frac{TP}{actual\ yes}=\frac{59}{60}=0.98=98\%$$

$$\text{False positive rate}=\frac{FP}{actual\ no}=\frac{0}{40}=0=0\%$$

$$\text{True negative rate}=\frac{TN}{actual\ no}=\frac{40}{40}=1=100\%$$

$$\text{Precision}=\frac{TP}{predicted\ yes}=\frac{59}{59}=1=100\%$$

The following graphic gives a clear understanding.

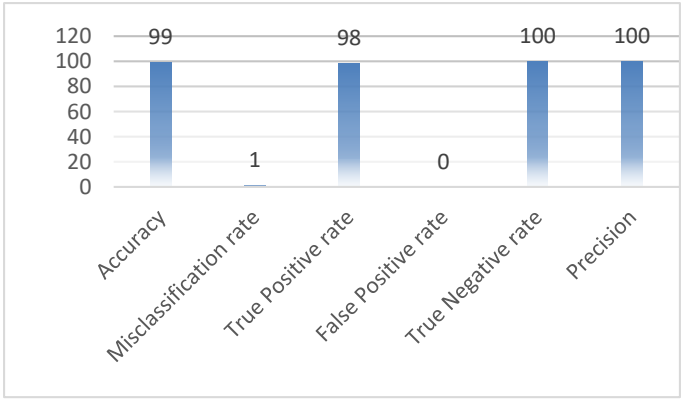

Figure 5: Performance analysis

- With the accuracy, we understand how often the classifier is correct. With 99% of accuracy, the result is correct.
- With the misclassification rate, we understand how often the classifier is wrong. With 1% of misclassification rate, we can realize that the result is acceptable.
- With the true positive rate, we want to understand how often the classifier predicts yes when it is actually yes. The result here is 98%.
- With the false positive rate we want to understand how often the classifier predicts yes when it is actually no. the graphic shows that the false positive rate is 0%, and it is perfect.
- With the true negative rate we want to understand how often the classifier predicts no when it is actually no. the rate here is 100%.
- Finally we have the precision. This metric tells us how often it is correct when the classifier predicts yes. The precision here is 100%.

3) Screen shots

The following screen shots give a view about how the system proceeds with criminal detection.

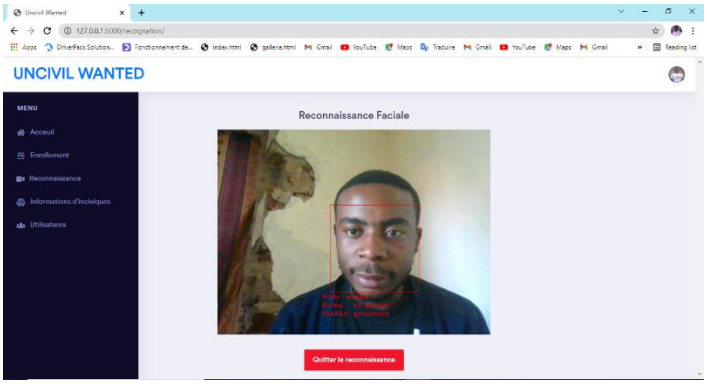

Figure 6: criminal detection

V. CONCLUSION AND FUTURE SCOPE

The security of the population of Beni and their property being above all a right guaranteed by the Congolese state, the recurrent criminality and insecurity in this area are a major concern. Security is a crucial asset for the development of the population and in the practice of their daily activities, this is the reason why we were pushed to contribute to the improvement of the methods and techniques of research of an uncivilized person on the run or wanted by justice.

In this study, we have proposed an intelligent system for criminal detection in Beni town. The objective of this work is to reduce the crime rate in the town of Beni and its surroundings by combating the flight of criminals or people wanted by the courts. We advocate for the deployment of this system of detection in various entry points (Airport, barriers, stations, ports).

In the future, the route tracing of the detected person, the indication of the area where the detection took place and the sending of messages (containing the information of the detection as for example: time and geographical coordinates) to the assigned services could be added among the functionalities of this system.

REFERENCES

[1] Radio Okapi, "Evasion de la prison de Beni : fouille systématique des usagers de la route Butembo-Goma," 21 10 2020. [Online]. Available: https://www.radiookapi.net/2020/10/21/actualite/societe/evasion-de-la-prison-de-beni-fouille-systematique-des-usagers-de-la.

[2] A. G. S. D. P. S. S. Alireza Chevelwalla, «Criminal Face Recognition System,» *International Journal of Engineering Research & Technology (IJERT)*, 2015.

[3] D. M. Aaron., «"Marvin Minsky",» *Encyclopedia Britannica*, 5 August 2021.

[4] B. L, «lebigdata.fr,» 3 february 2021. [En ligne]. Available: https://www.lebigdata.fr/machine-learning-et-big-data. [Accès le 8 november 2021].

[5] v. advani, «mygreatlearning.com,» 19 october 2021. [En ligne]. Available: https://www.mygreatlearning.com/blog/what-is-artificial-intelligence/#WhatisArtificialIntelligence. [Accès le 11 November 2021].

[6] S. Z. L. &. A. K. Jain, Handbook of Face Recognition, Springer London Ltd; 2nd ed. 2011 édition (22 août 2011), 2011, p. 699.

[7] A. NADJETTE, «Mise au point d'une application de reconnaissance faciale,» Université Mohamed Khider-BISKRA, BISKRA, 2020.

[8] I. c. education, «ibm.com,» 2 july 2020. [En ligne]. Available: https://www.ibm.com/cloud/learn/natural-language-processing. [Accès le 8 november 2021].

AUTHORS

First Author – AGANZE BARAKA, BSc. Computer Engineering, CHRISTIAN BILINGUAL UNIVERSITY OF CONGO. E-mail: aganzebaraka003@gmail.com
Second Author – SAGE KATALIKO, MSc. Information Technology, PhD scholar at AMA University.
E-mail: kkataliko@gmail.com
Third Author – ASAKA Digne, BSc. Computer Engineering, CHRISTIAN BILINGUAL UNIVERSITY OF CONGO.E-mail address:dignemerveille@gmail.com