**REPUBLIQUE DEMOCRATIQUE DU CONGO**

**MINISTERE DE L’ENSEIGNEMENT SUPERIEUR ET UNIVERSITAIRE**

**(MINESU)**

**UNIVERSITE CHRETIENNE BILINGUE DU CONGO**

**(UCBC)**

****

[**www.congoinitiative.org**](http://www.congoinitiative.org) **,** [**www.ucbc.org**](http://www.ucbc.org)**.**

**Conception et réalisation d’un système intelligent de détection des criminels. Cas de la ville de Beni**

**FACULTE DE SCIENCES APPLIQUEES**

**DEPARTEMENT DE GENIE INFORMATIQUE**

**Par Aganze Baraka Isaac**

**« Travail de mémoire présenté et défendu en vue de l’obtention du diplôme de licencié en génie informatique »**

**Directeur: Ir Erick Kalwana, MSc.**

**Encadreur : Ir Sage Kataliko, MSc.**

**ANNEE ACADEMIQUE : 2020 – 2021**

**Sujet** : « **Conception et réalisation d’un système intelligent de détection des criminels Cas de la ville de Beni. »**

Par

Aganze Baraka Isaac

3817

In accordance with UCBC policies, this thesis is accepted in partial fulfilment of requirements for the degree of Licencié.

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Erick Kalwana, Msc. Génie Logiciel

Directeur

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sage Kataliko, Msc. Technology

Directeur

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Felix Katimika, CT,

Doyen de la faculté des Sciences Appliquées

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Felix Katimika, CT,

SGAC chargé des recherches et documentation

**Déclaration d’honnêteté académique**

Par mon honneur, je confirme que ce présent travail scientifique intitulé :

« **Conception et réalisation d’un système intelligent de détection des criminels. Cas de la ville de Beni. »**

Est original et n'a été soumis à aucun autre collège ou institution universitaire pour le crédit universitaire. Tout texte ou digramme tiré d’un ouvrage, travail scientifique, Site Web, et autres ressources ont et utilisés et cités correctement dans les textes et dans la liste des références. Je reconnais avoir mentionné toute personne ayant porté une contribution scientifique à ce travail.

Je suis conscient que toute déclaration fausse annule ce travail et entraine des pénalités sévères selon la loi.

Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Aganze Baraka Isaac

3817

## EPIGRAPHE

*“ Seuls ceux qui sont assez fous pour penser qu’ils peuvent changer le monde y parviennent”*

***Publicité Apple “ Think Different ”, 1997***

*“Je connais tes œuvres. Voici, parce que tu as peu de puissance, et que tu as gardé ma parole, et que tu n’as pas renié mon nom, j’ai mis devant toi une porte ouverte, que personne ne peut fermer.”*

***Apocalypse 3 : 8***

## DEDICACE

A mon très cher père

A ma très chère mère

A ma très chère famille

A ma future tendre épouse et mes futurs enfants.

Je dédie ce travail

**AGANZE BARAKA Isaac**

## REMERCIEMENTS

Ce modeste travail est l’œuvre des multiples efforts, encouragements et contributions des certaines personnes pour lesquelles nous ne resterons pas indiffèrent. En guise de reconnaissance, nous tenons à témoigner nos sincères remerciements à toutes les personnes qui ont contribués de près ou de loin à l’élaboration et la réalisation de ce travail scientifique :

Nos premiers remerciements s’adressent à Dieu, Le Tout Puissant, lui qui dans sa bonté, nous a donné de la force, de l’intelligence, de la santé et nous a comblés par sa grâce et a permis que nous puissions parfaire cette œuvre, que l’honneur et la gloire lui revienne.

Nos remerciements également s’adressent à toute la communauté académique de l’Université Chrétienne Bilingue du Congo, spécialement la faculté des sciences appliquées pour nous avoir formés scientifiquement et spirituellement.

Nous adressons nos remerciements au directeur de ce travail, maitre ERICK KALWANA, et à mon encadreur maitre SAGE KATALIKO qui se sont dévoués malgré leurs multiples occupations à nous diriger, à nous encadrer pourvu que notre travail soit bien taillé.

Nos sincères gratitudes s’adressent à nos très chers parents papa BARAKA BARIHEMURA Janvier et maman RACHEL NAMWANA Benita, qui, malgré nos caprices, n’ont pas cessé de nous soutenir, des nous encouragés, de nous inculquer le sens de responsabilité et de l’amour du travail durant tout notre parcours académique. Nous remercions tous mes frères et sœurs qui se sont démenés pour la réalisation de ce travail : Armeline Baraka, Alain Baraka, Arlette Baraka, Ambroise Baraka, Aristote Baraka, Armand Baraka, Ariane Baraka, Abigaël Baraka et Aksa Baraka.

Nos remerciements s’adressent aussi aux ingénieurs Sagesse Magezi Asimwe, Vyakuno Kathe Joël, Fimbo Isohera Justin, pour nous avoir initiés dans le monde informatique et à nos camarades de l’auditoire dont nous pouvons citer : Asaka Digne, Ajaza Kimini, Bihembo Muleverwa, Jeannine Nabintu, Esther Ngangisa, Kamavu Jonas, Kakule Tsongo, Kiombwe Célestin, Ushindi Tsongo, Odette Vutegha, Jospin Mihigo, Mélanie Matofali, Claudine Winya, Pablo Tsasi, Nelson Kayisirirya, Gaspard Matuli, Kavira Safi, Kavira Salomé, Héritier Buleghe, Kizito Ngingo, Heri David, Israël Kikama, Gracieux Sivasimire, Gerlas Lungu, Erick Sawasawa, Rafiki Malimbo, Muhindo Heritier, Bénie Mapamboli.

Nous remercions particulièrement tous nos ami(e)s et familiers que nous aimons tant Laetitia Vulihwadi, Chester Makuwira, Julie Kafulubiri, Aldegonde Mumbesa, Mwenge Mumbesa, Rolande Kahashi, Victoire Matofali, Diane Kyanga, Ir Deborah Fimbo, Ir Rodriguez Nkalu, Ir James Afumba, Ir Jonathan Walux, Ir Esther Muhasa, Niya Ursule, Pierrette Ineza, Benoite Sifa, Clemence Wasyngia, Christelle Mumbesa, Benito Mafuta, Salama Muzalami, Tresor Mafika, Alice Matabishi, Josias Kikamata pour leur sincère amitié et confiance, et à qui nous devons notre reconnaissance et notre attachement.

Nous remercions People in Big Union (PBU, en sigle) qui nous a accompagnés dans notre parcours académique en donnant joie dans l’amour et l’union.

Dans l’impossibilité de citer tous les noms, nos sincères remerciements vont à tous ceux et celles, qui de près ou de loin, ont permis par leurs conseils et leurs compétences la réalisation de ce mémoire.

AGANZE BARAKA Isaac.

## SIGLES ET ABBREVIATIONS

**ADF: A**llied **D**emocratic **F**orces

**ADN: A**cide **D**ésoxyribo**n**ucléique

**ANN : A**rtificial **N**eural **N**etwork

**CNN: C**onvolutional **N**eural **N**etwork

**CRIS: C**riminal **R**ecord **I**nformation **S**ystem

**DGM: D**irection **G**enerale **de M**igration

**HCR:** **H**aut-**C**ommissariat aux **r**éfugiés

**IA: I**ntelligence **A**rtificielle

**KNN: K**-**N**earest **N**eighbors

**LBPH: L**ocal **B**inary **P**atterns **H**istograms

**PCA: P C A**

**RDC: R**epublique **D**emocratiqu**e du C**ongo

**UML: U**nified **M**odeling **L**anguage

## LISTE DES FIGURES

[Figure 1 : Différents caractéristiques biométriques : (1) rétine, (2) Iris, (3) empreintes digitales, (4) Frappe clavier, (5) ADN, (6) geste, (7) paume de main, (8) dynamique de la signature, (9) voix, (10) marche, (11) visage, (12) Oreille. 19](#_Toc81786549)

[Figure 2 Etapes de la reconnaissance faciale 21](file:///C:\Users\AMBROISE\Desktop\memoire\memoire%20aganze%20baraka%20isaac%20ok.docx#_Toc81786550)

[Figure 3 : variation des poses 22](file:///C:\Users\AMBROISE\Desktop\memoire\memoire%20aganze%20baraka%20isaac%20ok.docx#_Toc81786551)

[Figure 4 : Variation illumination. 23](file:///C:\Users\AMBROISE\Desktop\memoire\memoire%20aganze%20baraka%20isaac%20ok.docx#_Toc81786552)

[Figure 5 : exemple d'une détection de visage 23](#_Toc81786553)

[Figure 6 : Diagramme de cas d'utilisation 33](#_Toc81786554)

[Figure 7: Diagramme de cas d'utilisation du système 39](#_Toc81786555)

[Figure 8: Diagramme de cas d'activité s'authentifier 41](#_Toc81786556)

[Figure 9: Diagramme d'activité cas enrôler criminel soit présumé criminel 42](#_Toc81786557)

[Figure 10: Diagramme d'activité cas effectuer reconnaissance faciale. 43](#_Toc81786558)

[Figure 11: Diagramme de séquences cas s'authentifier 45](#_Toc81786559)

[Figure 12 : Diagramme de séquences cas enrôler criminel ou présumé criminel 46](#_Toc81786560)

[Figure 13 : Diagramme de séquences cas effectuer reconnaissance faciale 47](#_Toc81786561)

[Figure 14 : Diagramme de classe. 48](#_Toc81786562)

[Figure 15 : Diagramme de déploiement 49](#_Toc81786563)

## LISTE DES TABLEAUX

[Tableau 1: Explication du diagramme de cas d'utilisation 40](#_Toc81786855)

## RESUME

L’Est de la Republique Democratique du Congo en particulier la ville de Beni traverse une période difficile caractérisée par des tueries, des cambriolages, des assassinats, des viols, etc. Plusieurs opérations des grandes envergures ont été mises en place pour répondre à cette crise sécuritaire mais jusqu’à présent celles-ci ne donnent pas totalement les résultats escomptés non pas parce que les services sécuritaires ne font pas leur travail mais parce qu’aussi ils n’ont pas des dispositifs nécessaires pouvant les faciliter à remplir de manière efficace et avec beaucoup plus de précisions leurs missions.

En effet ces délits, contreventions, crimes sont souvent perpétrés par des personnes ayant déjà un ou plusieurs soucis avec la justice, certains sont condamné mais sans purger leurs peines, ils se retrouvent en liberté, s’évadent des prisons et plusieurs même prennent des nouvelles identités et continuent leurs activité sans se gêner.

Cette problématique nous a incité à réaliser ce présent travail celui de concevoir et réaliser un outil capable d’aider les services de sécurité dans la lutte contre la fuite des personnes recherchées par la justice soit des criminels évadés de la maison de pénitence en les identifiant par une mesure biométrique.

Différentes méthodologies sont utilisées pour atteindre l’objectif que nous nous sommes assigné dans ce travail, dont la modélisation, le prototypage, la simulation, la méthode expérimental et bien des techniques nous ont permis d’enrichir notre travail.

Nous sommes aboutis à un système intelligent de détection des criminels faisant usage de la reconnaissance faciale.

Mots clés :

## ABSTRACT

The eastern part of the Democratic Republic of Congo, in particular the town of Beni, is going through a difficult period characterised by killings, burglaries, assassinations, rapes, etc. Several large-scale operations have been put in place to respond to this security crisis, but so far these have not produced the expected results, not because the security services are not doing their job, but because they do not have the necessary devices to help them carry out their missions effectively and with much greater precision.

Indeed, these offences, offences and crimes are often perpetrated by people who have already had one or more problems with the law. Some are convicted but without serving their sentences, they find themselves free, escape from prison and many even take on new identities and continue their activities without any hindrance.

This problem has prompted us to carry out this work to design and implement a tool capable of helping the security services in the fight against the escape of people wanted by the justice system, i.e. criminals who have escaped from the house of punishment, by identifying them using a biometric measurement.

Different methodologies are used to achieve the objective that we have assigned in this work, including modeling, prototyping, simulation, experimental method and many techniques have allowed us to enrich our work.

We ended up with an intelligent criminal detection system using facial recognition.

# INTRODUCTION.

## Préambule

L'informatique pénètre peu à peu tous les domaines de notre vie quotidienne ; rares sont les activités qui ne soient aujourd'hui marquées de son sceau. Les ordinateurs calculent, écrivent, parlent et chantent. Ils sont outils de travail et moyens de recherche. [1]

Ayant pris une place considérable dans le quotidien mais aussi dans la vie d’une entreprise, l’**informatique**a connu son véritable envol en s’intégrant plusieurs domaines et secteurs entre autres social, économique, éducationnel, communicationnel, industriel, agricole, commercial, sanitaire, alimentaire ainsi que sécuritaire, … Le fait est que l’on vit aujourd’hui dans un monde où l’on ne peut ne pas se passer de l’**informatique.** [2]

Les activités déployées par le crime organisé transnational et l’argent qu’elles génèrent semblent entretenir de façon prononcée l’instabilité, l’impunité et la violence, particulièrement dans l’Est de la RDC. On recenserait encore dans l’Est de la RDC entre 6,500 et 13,000 membres actifs de groupes armés tirant profit d’activités criminelles. [3]

Depuis bien longtemps, la Province du Nord Kivu n’a cessé d’être en proie à des cas d’insécurité de toutes sortes, La population du Nord Kivu, ne cesse d’assister à une flambée des violations des droits de l’homme et des cas d’insécurité grandissante et de supporter le joug de la servitude. [4]

Depuis janvier, dans la ville et territoire de Beni, des attaques imputées au groupe armé des Forces démocratiques alliées (ADF) ont tué près de 200 personnes, en ont blessé des dizaines d’autres. « A la suite de ces attaques, environ 40.000 personnes ont été déplacées dans le territoire de Beni, dans la province du Nord-Kivu, ainsi que dans des villages voisins de la province d’Ituri », a déclaré Babar Baloch, porte-parole du HCR lors d’un point de presse à Genève. En moins de trois mois, les ADF auraient attaqué 25 villages. Selon le HCR, le groupe rebelle ougandais aurait incendié des dizaines de maisons et enlevé plus de 70 personnes. « Ces chiffres s’ajoutent aux 465 Congolais tués dans des attaques attribuées aux ADF en 2020 », a précisé M. Baloch. D’une manière générale, les attaques et les violations généralisées des droits de l’homme se poursuivent également dans d’autres parties de la province du Nord-Kivu. [5]

Sachant que la sécurité est indispensable à la vie quotidienne, car elle permet à l’individu et à la communauté de réaliser ses aspirations. L’absence de sécurité entraîne des problèmes qui se manifestent de plusieurs façons : blessures, violences, criminalité, suicides, situations de crise, sinistres, etc. Outre les inquiétudes qu’ils engendrent chez les citoyens et les citoyennes, ces problèmes génèrent aussi des conséquences individuelles, collectives et économiques importantes qui sont souvent inter reliées. [6]

Les services de sécurité devraient généralement détenir des leviers d’intervention puissants et nécessaires pour prévenir bon nombre de ces problèmes. Notre étude porte sur la conception et réalisation d’un système de reconnaissance intelligent des auteurs des crimes faisant intervenir des notions de la vision assistée par ordinateur et de l’apprentissage automatique.

## Problématique.

De nos jours, les crimes ont pris une grande ampleur dans notre pays ; l’insécurité en République Démocratique du Congo est un problème auquel il faut mettre un terme. La criminalité est toujours d’actualité et plutôt plus alarmante dans notre contrée malgré l’effectif des agents de sécurité et quelques moyens mis en leurs dispositions.

Plusieurs criminels et personnes en conflit avec la justice après avoir été incarcéré dans les maisons de pénitences planifient leurs évasions pour des multiples raisons et parfois ceux-ci y arrivent mais après ces évasions nombreux sont ceux qui ne sont pas retrouver et dans un bref délai par les services de l’ordre, les statistiques parlent d’eux même seulement 33 évadés ont été retrouvé sur un effectifs de 1335 prisonniers évadés l’année passée au mois d’octobre dans la prison de Kangbayi. [7]

Le 20 octobre 2020, Sur place à Beni, le maire de la ville parle de 110 prisonniers qui sont volontairement restés dans cette maison carcérale. Selon lui, plus de 1000 autres prisonniers ont quitté Kangbayi suite à cette attaque. Selon Modeste Bakwanamaha, les combattants ADF ont commencé par attaquer une position de l’Armée située aux alentours de la prison avant de lancer l’assaut final. [8]

En juin 2017, une autre attaque avait visé la prison de Kangbayi, 11 morts dont 8 éléments des forces de l’ordre étaient tués dans cette incursion qui avait vu 966 prisonniers prendre le large. [8]

Parfois il est déplorable de constater que certains criminels restent en liberté errant dans la nature suite à un manque de dispositif nécessaire à leur identification. Certains plus malin vont jusqu’à falsifier leurs pièces d’identité en prenant une nouvelle identité celui-ci reste en liberté tout en exerçant en toute impunité des activités illégaux en perpétrant des crimes, plusieurs arrivent à déjouer le système de contrôle à l’aéroport, les barrières routiers et les ports et parviennent à quitter le pays sans ménager aucun effort.

Cette croissance exponentielle de la criminalité dans notre contrée entraine plusieurs méfaits dont : une baisse de la qualité de vie des personnes affectées, elles deviennent non seulement plus angoissées mais elles se déplacent moins et vivent l'isolement, des pertes des vies humaines, des viols, des vols, sentiment d’insécurité collective et cela est un problème pour la gouvernance urbaine.

Au regard de toutes ces préoccupations, les questions suivantes ont attiré notre attention :

* Quel mécanisme pouvons-nous développer pour détecter un criminel ou toute autre personne recherchée par la justice ?
* Comment pouvons-nous lutter contre la fuite des personnes recherchées par la justice ?

## Hypothèses

Se basant aux questions précitées, voici ce que nous avons émis comme réponses anticipatives :

* La mise en place d’un système intelligent basée sur la vision assistée par l’ordinateur et l’intelligence artificielle serait une solution efficace pour la détection d’un criminel ou des personnes recherchées par la justice.
* Le déploiement du système de détection dans les points d’entrée (Aéroport, barrières, gares, ports) permettrait de lutter contre la fuite des personnes recherchées par la justice.

## Objectifs de la recherche

### Objectif général

L’objectif que nous visons dans ce travail est de diminuer le taux de criminalité en ville de Beni et ses environs en luttant contre la fuite des criminels ou des personnes recherchées par la justice.

### Objectifs spécifiques

Les spécificités indispensables pour atteindre l’objectif général sont les suivantes :

* Etudier les systèmes existants de reconnaissance intelligente.
* Modéliser un système intelligent basé sur la reconnaissance faciale
* Implémenter le système de détection des criminels
* Tester le système réalisé par rapport aux fonctionnalités assignées durant l’extraction des exigences du système pour ainsi tester les hypothèses.
* Plaider pour son déploiement dans la ville

## Choix et intérêt du sujet

Nous avons opté pour le choix de ce sujet nous basant à la situation de crise sécuritaire que traverse notre province plus particulièrement notre ville de Beni. La sécurité des personnes et de leurs biens est avant tout un droit garanti par l’Etat, la criminalité et l’insécurité récurrente nous ont poussé contribuer dans l’amélioration des méthodes et techniques de recherche ou repérage des criminels.

Ce travail trouve son intérêt dans plusieurs domaines dont le social, le domaine économique, psychologique, alimentaire, car la sécurité est un atout majeur pour l’épanouissement d’un peuple, les personnes sont capables d’effectuer des échanges et commerce des biens sans aucun problème car elles se sentent en sécurité et cela favorise l’élévation de l’économie et le développement de la région, lorsqu’il y a la sécurité même ceux-là qui n’accèdent pas à leur champ vont y accéder, les enfants vont à l’école, la population n’est pas traumatisée, notre pays étant un scandale géologique ; le tourisme peut reprendre ; le taux de chômage peut diminué et tout cela au profit de la population.

## Limitation et Délimitation du sujet

### Limitation

Quant au contenu, nous nous limiterons à la modélisation du système, l’enrôlement des criminels soit présumés criminels ou personnes recherchées par la justice la loi dans notre base de données, la reconnaissance faciale et la vérification de l’identité d’un criminel ou présumé criminel en fuite ou toute personne recherchée par la justice tout en retournant les informations nécessaires pour permettre de l’appréhender si et seulement si celui-ci se trouve dans une zone couverte par nos cameras à visage découvert. Tout autre aspect n’ayant pas été évoqué dans ceux cités ci-haut ne seront pas concernés par ce présent travail.

### Délimitation

* Dans le temps : le résultat de ces recherches sont entrepris de mai 2021 à octobre 2021
* Dans l’espace : nous nous sommes situés par rapport aux réalités de la province du NORD-KIVU en République Démocratique du Congo dans la ville de Beni, mais cela n’empêche que le système soit employé dans un toutes les villes de la République Démocratique du Congo.

## Audience

Notre système est conçu pour être utiliser par tous les services de sécurité de l’Etat congolais notamment ceux placés aux différents points stratégiques dont : barrières frontalières, aux aéroports, aux péages routes ; etc.

## Subdivision du travail

Hormis la partie introductive et de la conclusion, ce travail est structuré en quatre chapitres que voici :

* **Chapitre premier** « GENERALITES SUR LE TRAVAIL » : cette partie présente les différents mots clés que regorge notre travail, nous présentons le milieu d’étude, ensuite nous présentons quelques travaux déjà réalisés dans le cadre où s’inscrit le nôtre et de relever le point de démarcation. Enfin nous présentons ici les exigences logicielles de notre système.
* **Chapitre deuxième** « METHODOLOGIE ET CONCEPTION » : Ce chapitre parle de la méthodologie et techniques utilisées dans la réalisation du présent travail. Ensuite nous présentons la conception de notre système en le représentant sous formes des schémas et modèles informatiques.
* **Chapitre troisième** « IMPLEMENTATION ET PRESENTATION DES RESULTATS » : Dans ce chapitre nous parlons de l’implémentation du travail en passant par son architecture de déploiement et la présentation des outils et technologies utilisés. Ensuite, nous présentons les résultats du présent travail. Ici nous testons et présentons les fonctionnements du système conçu et implémenté.

# CHAPITRE I. GENERALITES SUR LE TRAVAIL

Ce présent chapitre nous donne un aperçu global sur les concepts-clés qui constituent le centre de notre travail. Nous présentons par la suite la revue de la littérature qui nous permet de faire connaissance des travaux similaires et recherches déjà effectués dans le cadre où s’inscrit notre travail et ainsi d’établir les bases connues, afin de s’en inspirer pour définir un cadre de recherche complémentaire, percevoir certaines implications non envisagées, éviter certaines erreurs méthodologiques identifiées dans de précédents travaux, mettre à profit certains outils utilisables pour notre propre recherche et dégager l’originalité de notre travail. Enfin nous parlons des exigences logicielles auxquelles notre système devra se soumettre.

## I.1. Définitions des concepts-clés

### I.1.1. Système

Un **s**ystème est un ensemble d'éléments interagissant entre eux selon certains principes ou règles. [9]Un système est déterminé par :

* Sa frontière, c'est-à-dire le critère d'appartenance au système (déterminant si une entité appartient au système ou fait au contraire partie de son environnement) ;
* Sa mission (ses objectifs et sa raison d'être) ;
* Ses interactions avec son environnement ;

### I.1.2. Système intelligent

Le concept de système intelligent est apparu dans les technologies de l'information en tant que type de système dérivé d'applications réussies de l'intelligence artificielle (IA)[[1]](#footnote-1). Un système intelligent est un outil qui fonctionne dans un monde complexe avec des ressources limitées, possède des capacités cognitives primaires telles que la perception, le contrôle de l'action, le raisonnement ou l'utilisation du langage, et présente un comportement intelligent complexe soutenu par des capacités telles que la rationalité, l'adaptation par l'apprentissage ou la capacité à expliquer l'utilisation de ses connaissances par introspection [10].

Les systèmes intelligents sont des machines technologiquement avancées qui perçoivent et réagissent au monde qui les entoure [11]. Un système intelligent est une machine qui intègre un ordinateur connecté à Internet qui peut collecter et analyser des données et communiquer avec d'autres systèmes.

Ces systèmes sont également caractérisés par leur capacité à apprendre par expérience, par la sécurité et la connectivité, par la capacité à s'adapter aux données actuelles et par la supervision et la gestion à distance. [12]

Deux domaines principaux au sein des systèmes intelligents : comment les machines perçoivent leur environnement et comment ces machines interagissent avec cet environnement. Une façon dont ces systèmes peuvent percevoir leur environnement est la vision. L'étude de la façon dont les ordinateurs peuvent comprendre et interpréter les informations visuelles à partir d'images statiques et de séquences vidéo a émergé à la fin des années 1950 et au début des années 1960.

Depuis, elle est devenue une technologie puissante qui est au cœur des secteurs industriel, commercial et gouvernemental du pays. [11] Les facteurs clés qui ont contribué à cette croissance sont la croissance exponentielle de la vitesse du processeur et de la capacité de mémoire ainsi que les progrès algorithmiques. [11] Le domaine des systèmes intelligents se concentre également sur la manière dont ces systèmes interagissent avec les utilisateurs humains dans des environnements physiques et sociaux changeants et dynamiques.

 Les premiers robots possédaient peu d'autonomie dans la prise de décision : ils assumaient un monde prévisible et parfumaient la ou les mêmes actions à plusieurs reprises dans les mêmes conditions. Aujourd'hui, un robot est considéré comme un système autonome capable de détecter l'environnement et d'agir dans un monde physique pour atteindre certains objectifs. [11]

#### Applications des systèmes intelligents

Les systèmes intelligents sont en passe de remplir un nombre croissant de rôles dans la société d'aujourd'hui, notamment [11] :

* Automatisation d'usine
* Robotique de terrain et de service
* Robotique assistance
* Applications militaires
* Soins médicaux
* Éducation
* Divertissement
* Inspection visuelle
* Reconnaissance des caractères
* Identification humaine à l'aide de diverses modalités biométriques (par exemple, visage, empreinte digitale, iris, main)
* Surveillance visuelle
* Transport intelligent

### I.1.3. Détection

**La** **détection** est l’action de mettre en évidence un phénomène peu perceptible à l’aide d’un détecteur. [13]

**Un détecteur** est tout appareil utilisé pour déceler la présence d’un corps, un phénomène caché ou non apparent immédiatement. [14]

### I.1.4. Criminel

**Un criminel** est toute personne coupable d’un crime [15] [qui](https://www.linternaute.fr/dictionnaire/fr/definition/qui/) [est](https://www.linternaute.fr/dictionnaire/fr/definition/est/) [condamnable](https://www.linternaute.fr/dictionnaire/fr/definition/condamnable/) [d'un](https://www.linternaute.fr/dictionnaire/fr/definition/d-un/) [point de vue](https://www.linternaute.fr/dictionnaire/fr/definition/point-de-vue/) [moral](https://www.linternaute.fr/dictionnaire/fr/definition/moral/) , [contraire](https://www.linternaute.fr/dictionnaire/fr/definition/contraire/) [aux](https://www.linternaute.fr/dictionnaire/fr/definition/local/) [lois](https://www.linternaute.fr/dictionnaire/fr/definition/loi/) [sociales](https://www.linternaute.fr/dictionnaire/fr/definition/social/).

**Un crime** est un comportement, que ce soit par acte ou par omission, défini par la loi comme méritant une punition. Bien que la plupart des crimes nécessitent l'élément intentionnel, certains délits mineurs peuvent être commis sur la base de la responsabilité stricte même si le défendeur n'avait pas d'état d'esprit spécifique à l'égard de l'action pénale. Par exemple, les infractions de stationnement sont des crimes qui n'exigent généralement pas que les procureurs établissent une intention. [16]

### I.1.5. Généralités sur la reconnaissance faciale.

#### I.1.5.1. Aperçu globale sur la reconnaissance faciale

Depuis les années 1960, la reconnaissance faciale a été l'un des sujets de recherche les plus actifs en vision par ordinateur et en reconnaissance de formes [17] . Ces dernières années ont connu des progrès significatifs dans ce domaine grâce aux progrès de la modélisation et de technique d'analyse des visages ; des systèmes ont été développés pour la détection et le suivi des visages, mais des visages fiables [18].

Plusieurs raisons expliquent l'intérêt accru récent pour la reconnaissance faciale, notamment la préoccupation croissante du public pour la sécurité, le besoin de vérification de l'identité dans le monde numérique et le besoin de techniques d'analyse faciale et de modélisation en gestion de données multimédia. Pour mieux comprendre ce que c’est la reconnaissance faciale partons de l’illustration du cerveau humain ; nous identifions différents visages des gens tout le long d’une journée.

Cependant, lorsque nous rencontrons une personne sur notre chemin, notre cerveau cherche dans notre faculté mentale (mémoire) à savoir si la personne vue est connue ou non. C’est dans la même optique que l’ordinateur par le biais de l’intelligence artificielle et de la vision assisté par ordinateur que le visage d’un individu est localisé sur une photo ou une vidéo puis les caractéristiques de son visage sont d’abord extraites puis ensuite converties en données, et ces données peuvent ensuite être comparées avec celles de visage entré dans une base de données centralisée. [19]

#### I.1.5.2. Définition

La reconnaissance faciale est une méthode d'identification ou de vérification de l'identité d'un individu en utilisant son visage. Elle peut être utilisée pour identifier des personnes sur des photos, des vidéos ou en temps réel.

#### I.1.5.3. Système biométriques basés sur la reconnaissance faciale.

La biométrie est « l’analyse des caractéristiques physiques strictement propres à une personne ». Ces caractéristiques sont les données biométriques. Il peut s’agir par exemple des empreintes digitales, de l’iris, du visage, de la voix ou même de l’ADN[[2]](#footnote-2) d’une personne [20].

La reconnaissance biométrique fait référence à l'utilisation de différentes mesures physiologiques peuvent être morphologiques ou biologiques dans cette catégorie nous trouvons : les empreintes digitales, le visage, la forme de la main, l’œil( rétine et iris), l’ADN d’une personne et les mesures comportementales dont la reconnaissance vocale, la dynamique des signatures, la dynamique de frappe au clavier d'un ordinateur, le geste… , appelées caractéristiques biométriques, ou simplement biométrie, pour reconnaître automatiquement les individus.

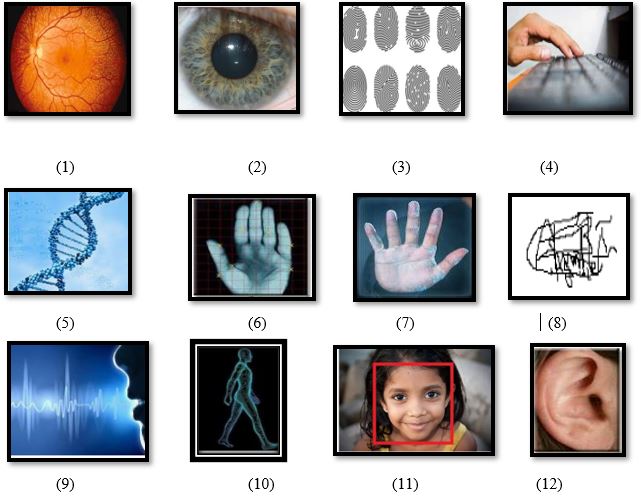


Figure 1 : Différents caractéristiques biométriques : (1) rétine, (2) Iris, (3) empreintes digitales, (4) Frappe clavier, (5) ADN, (6) geste, (7) paume de main, (8) dynamique de la signature, (9) voix, (10) marche, (11) visage, (12) Oreille.

Il sied de souligner que de tous ces systèmes d’identification, la reconnaissance faciale n’est pas la plus fiable comparée aux autres techniques de biométrie, mais elle peut être ainsi si on utilise des approches plus efficaces en plus du bon choix des caractéristiques d’identification représentant le visage en question.

Dans ce travail nous avons choisi d’utiliser un système intelligent basé sur la reconnaissance du visage car elle est une méthode passive ou discrète en matière d’identification criminelle c’est-à-dire qu’un système de reconnaissance de visages ne nécessite aucune coopération de l’individu, du genre : mettre le doigt ou la main sur un dispositif spécifique ou parler dans un microphone. En effet, la personne n’a qu’à rester ou marcher devant une caméra pour qu’elle puisse être identifiée par le système et en plus il est facile de se procurer des équipements d’acquisition, leurs utilisations est facile et leurs coûts faibles.

#### I.1.5.4. Fonctionnement d’un système de reconnaissance automatique du visage.

La **reconnaissance faciale** est une technologie de plus en plus répandue, basée sur l'intelligence artificielle, permettant d'identifier une personne sur une photo ou une vidéo en comparant son visage avec ceux sauvegardés dans une base de données. [21]

La reconnaissance automatique de visage s’effectue en trois étapes principales dont

1. La détection de visages.
2. L’extraction et normalisation des caractéristiques du visage.
3. L’identification et/ou vérification

Comme la reconnaissance faciale est aussi parmi les mesures biométriques physiologiques, celles-ci nous permettent alors d’exploiter certaines informations nécessaires relatives à l’homme ; comme déterminer son identité par exemple. [19] Le système de reconnaissance faciale est souvent une approche logicielle visant à reconnaitre une personne grâce à son visage d’une manière automatique. Cette reconnaissance peut alors prendre plusieurs aspects : déterminer à qui appartient le visage (identification), décider si oui ou non le visage est connu ou non (identification), et dans un autre cas de vérifier qu’une personne est bien celle qu’elle prétend être (authentification : dans le cadre d’un contrôle d’accès).

L’image ci-dessous illustre mieux les étapes principales de la reconnaissance faciale :

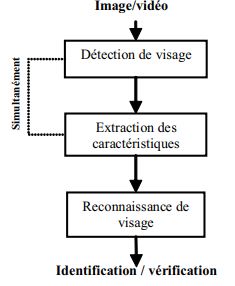


Figure 2 Etapes de la reconnaissance faciale

Dans les lignes suivantes détaillons chaque étape du système de reconnaissance faciale et nous présentons les difficultés auxquelles nous faisons face dans les systèmes de reconnaissance faciale et aussi différentes applications de ces systèmes.

La première étape dans le processus est l’acquisition de l’image. Il faut réussir à capter l'information essentielle sans bruit. La reconnaissance faciale peut être faite à l’aide des images fixes (photos) ou à partir des séquences d’images (vidéos) ou à temps réel. Notre travail traite plus de la troisième procédure celle de la reconnaissance faciale en temps réel mais cela n’exclut pas les deux précédentes, l’image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système.

Les étapes qui nous intéressent le plus se trouvent dans les paragraphes suivants :

#### La détection de visage :

La détection de visage peut se faire par détection de la couleur de la peau, la forme de la tête ou par des méthodes détectant les différentes caractéristiques du visage. Cette étape est autant plus délicate quand l'image acquise contient plusieurs objets de visage ou un fond non uniforme qui crée une texture perturbant la bonne segmentation du visage. Cette étape est dépendante de la qualité des images acquises [22]. Dans la littérature scientifique, le problème de localisation de visages est aussi désigné par la terminologie "détection de visages". Les performances globales de tout système automatique de reconnaissance dépendent amplement des performances de la détection de visages.

Plusieurs travaux de recherches ont été effectués dans ce domaine, ils ont donné lieu au développement d’une multitude de techniques allant de la simple détection du visage, à la localisation précise des régions caractéristiques du visage, tels que les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc.

Cependant, les solutions proposées jusqu’à présent sont loin d’être satisfaisantes car elles fonctionnent uniquement dans des environnements contrôlés, et par conséquent elles ne gèrent pas la variabilité des conditions d’acquisition de la vie quotidienne, notamment :   
 **La pose :** les images d’un visage changent en fonction de l’orientation de ce dernier (frontal, 45 degrés, profil). Ce nous que devons savoir ici ce que le taux de reconnaissance de visage baisse très considérablement quand des variations de pose apparaissent dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible [19].

Figure 3 : variation des poses

**La présence ou absence des composantes structurales :** les caractéristiques faciales telles que la barbe, la moustache, les lunettes causent une grande variabilité des composantes structurales du visage, notamment au niveau de la forme, la couleur et de la taille.

**Les occultations :** les visages peuvent être partiellement occultés par d’autres objets. En effet, dans une image contenant un groupe de personnes par exemple, des visages peuvent partiellement masquer d’autres visages.

**Les conditions d’illumination** : des facteurs tels que l’éclairage (distribution de la source de lumière, son intensité, son spectre) et les caractéristiques de l’appareil photographique affectent l’aspect d’un visage dans l’image acquise [23].

Figure 4 : Variation illumination.

Dans l’étape de détection, on identifie et on localise le visage dans l’image acquise au départ, indépendamment de la position, de l’échelle, de l’orientation et de l'éclairage.

Le processus de reconnaissance de visages ne pourra jamais devenir intégralement automatique s’il n’a pas été précédé par une étape de détection efficace.

Trouvons ci-dessous une image qui illustre la détection faciale

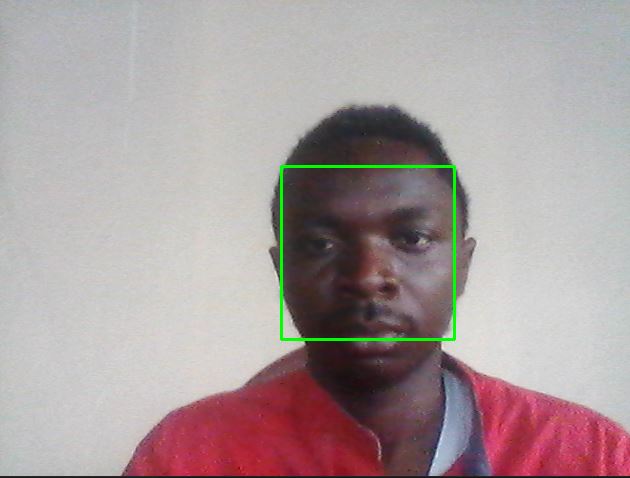


Figure 5 : exemple d'une détection de visage

#### L’extraction des caractéristiques du visage :

L’extraction des caractéristiques telles que les yeux, le nez, la bouche est une étape prétraitement nécessaire à la reconnaissance faciale. On peut distinguer deux pratiques différentes : la première repose sur l’extraction de régions entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage. La deuxième pratique extrait des points particuliers des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez. Elle est utilisée avec une méthode locale de reconnaissance et aussi pour l’estimation de la pose du visage [23].

Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. Le choix de ces informations utiles revient à établir un modèle pour le visage, elles doivent être discriminantes et non redondantes.

L’analyse est appelée indexation, représentation, modélisation ou extraction de caractéristiques. L’efficacité de cette étape a une influence directe sur la performance du système de reconnaissance de visage.

#### La reconnaissance de visage

A cette étape, chaque visage de la base est associé une signature unique qui caractérise la personne correspondante. La reconnaissance d’un visage requête est obtenue par l’extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données**.**

Ainsi, à partir de la signature numérique créé au cours de l’extraction des caractéristiques, le module de décision doit être capable d’accepter ou refuser une authentification après avoir fait la comparaison entre les nouvelles données de l’utilisateur et les différents modèles stockés dans la base de données afin de déterminer l’identité de l’usager si elle existe.

#### I.1.5.4. Principales difficultés de la reconnaissance de visage :

Le processus de la reconnaissance de visages est une grande tâche visuelle pour un humain. Bien que les êtres humains puissent détecter et identifier des visages dans une scène facilement.

Concevoir et réaliser un système automatique qui accomplit ces tâches représente un sérieux défi. Ce défi est d’autant plus grand lorsque les conditions d’acquisition des images sont très variables [24].

Il existe deux types de variations associées aux images de visages : inter et intra sujet. On parle de la variation inter sujet lorsqu’on compare le visage d’un individu à celui des autres individus tandis qu’on parle de la variation intra sujet lorsqu’on compare le visage d’un individu à lui-même. Nous devons noter que la variation inter sujet est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra sujet est plus vaste. Elle peut être attribuée à plusieurs facteurs à savoir [24] :

* La variation de la pose.
* Le changement d’illumination.
* Changement des expressions faciales.
* Influence des occultations.
* Chirurgie plastique.
* Les vrais jumeaux.

À la différence des méthodes fondées sur les empreintes digitales et l’ADN, qui ne changent pas au cours de la vie, la reconnaissance faciale doit tenir compte de ces différents facteurs.

#### I.1.5.5. Les algorithmes de détection et de reconnaissance de visage.

  La reconnaissance faciale est une technologie capable de reconnaître une personne en fonction de son visage. Il utilise des algorithmes d'apprentissage automatique qui recherchent, capturent, stockent et analysent les traits du visage afin de les faire correspondre avec des images d'individus dans une base de données préexistante. Il existe de nombreuses méthodes et techniques de reconnaissance de visages en voici quelques-unes :

* Méthodes d’apprentissage ensemblistes ;
* KNN « K-Nearest Neighbors »
* Techniques d’apprentissage supervisé et les arbres de décisions
* LBPH « Local Binary Patterns Histograms »
* Réseaux de neurone (Neural Networks, en Anglais) où nous trouvons l’apprentissage en profondeur (Deep Learning en Anglais).

Soulignons ici que nous détaillons l’apprentissage en profondeur (Deep Learning) car nous allons nous servir de lui pour faire la reconnaissance faciale.

##### L’algorithme d’apprentissage en profondeur (Deep Learning).

L’apprentissage en profondeur est une phase avancée de l'apprentissage automatique qui utilise principalement des réseaux de neurones pour l'apprentissage et la prédiction de données. C'est un groupe d'algorithmes différents.

Ceux-ci sont utilisés pour concevoir un système généralisé complexe qui peut prendre tout type de problèmes et faire des prédictions. Il utilise le graphe profond avec de nombreuses couches de traitement, composées de nombreuses couches linéaires et conversion non linéaire.

Les réseaux de neurones convolutifs (CNN) sont le type le plus courant de méthode d'apprentissage en profondeur pour la reconnaissance faciale. L’avantage principal des méthodes d'apprentissage en profondeur est qu'elles peuvent être entraînées avec de grandes quantités de données pour apprendre une représentation du visage qui est robuste aux variations présentes dans la formation des données.

De cette façon, au lieu de concevoir des fonctionnalités spécialisées qui sont robustes à différents types de variations intra sujet (par ex. éclairage, pose, expression faciale, âge, etc.), les CNN peuvent les apprendre à partir des données d'entraînement.

Le principal inconvénient de la profondeur méthodes d'apprentissage est qu'ils doivent être formés avec des de grands ensembles de données qui contiennent suffisamment de variations pour généraliser à échantillons invisibles [25]. Dans le présent travail nous allons utiliser « **Face Recognition Library** » qui est une librairie qui nous permet de reconnaitre et manipuler les visages en python ; cette librairie a été construite en utilisant la reconnaissance de pointe de **Dlib** qui est une boîte à outils C++ moderne contenant des algorithmes d'apprentissage automatique et des outils permettant de créer des logiciels complexes en C++ pour résoudre des problèmes du monde réel. Il est utilisé à la fois dans l'industrie et dans les universités dans un large éventail de domaines, notamment la robotique, les appareils embarqués, les téléphones mobiles et les grands environnements informatiques haute performance.

#### Quelques applications de la reconnaissance faciale.

Depuis son invention dans les années 70, la **reconnaissance faciale** a progressé à pas de géant. Elle s'impose aujourd'hui comme la plus naturelle des mesures biométriques [26]. Les applications de reconnaissance faciale sont subdivisées en trois catégories majeures :

* **La sécurité**: La reconnaissance faciale a deux fonctions : l'identification et l'authentification. Aujourd’hui nous trouvons son application dans les systèmes des contrôles d’accès, l’exemple de nos smartphones avec l’application « Face ID », le contrôles dans les aéroports et aux frontières, retrouver des personnes disparues, application de la loi, les recherches indexées ; etc.
* **La santé :** Dans le domaine sanitaire la reconnaissance faciale trouve son application dans des hôpitaux qui l’utilise pour améliorer le soin aux patients. Les prestataires de soins de santé sont en train de l’utilisation de la reconnaissance faciale pour accéder aux dossiers des patients, simplifier leur enregistrement, détecter les émotions et la douleur et même pour identifier certaines maladies génétiques.
* **Le commerce** : les services bancaires pour l’utilisation de la reconnaissance faciale en replacement des cartes bancaires ou des signatures, en marketing et publicité pour l’amélioration de l’expérience des consommateurs, etc.

## I.2. Revue de la littérature

Ce point se focalise sur quelques travaux des chercheurs qui ont traité ce thème dans le domaine de lutte contre l’insécurité vue que nous ne sommes pas le premier à aborder la question de la sécurité et des systèmes intelligents faisant usage de la reconnaissance faciale.

Nous présentons le sujet de recherche de chaque chercheur, leurs préoccupations de départ, les objectifs de leur recherche et les résultats de leurs travaux pour enfin ressortir le point de démarcation qui existe entre notre travail et ces derniers.

1. **Londres teste la reconnaissance faciale en temps réel pour débusquer des criminels**

Dans son article, Victoria Beurnez [27] présente le lancement du système de la police de reconnaissance faciale en temps réel dans le quartier de londrès. Le but de ce système est d’anticiper de potentiels crimes tels que l’agression par arme à feu et blanche, les violences sexuelles sur les enfants. Il servira aussi à protéger les populations les plus vulnérables.

Parlant de sa fonctionnalité, cette reconnaissance faciale fonctionne en comparant l’actuelle liste des surveillances et les visages des gens présents dans la zone surveillée pour comparer un visage avec l’existant, le système procède par la mesure des points essentiels de chaque visage incluant la distance entre les yeux, le nez, la bouche et la mâchoire pour afin créer un schéma utile. Après si deux visages correspondent, une alerte sera directement envoyée à la police.

1. **Conception et réalisation d’un système d’enregistrement et vérification des informations judiciaires liées à la personne : Cas de la ville de Beni**

Fimbo Vakali Déborah [9], dans son travail de mémoire présenté en vue de l’obtention du diplôme de licence en faculté des sciences appliquées / département de génie informatique, a traité sur le problème de savoir comment on peut limiter les opérations de fraude liées aux pièces d’identité dans le territoire de Beni , mais aussi savoir par quel moyen on peut rendre la tâche facile aux services de sécurité pour trouver les évadés des prisons et les infracteurs, en fin comment rendre disponible les casiers judiciaires des citoyens aux services de sécurité pour s’assurer que ces derniers sont irréprochables.

Elle a pensé que mettre en place un système informatique qui contient toutes les informations reliées à chaque numéro national serait une solution pour résoudre le problème de circulation des fausses pièces d’identité, mais aussi un système d’alerte qui enverra les avis de recherches avec les identités des évadés et celles des personnes en fuite dans tous les services de sécurité, et faciliter l’accès aux casiers judiciaires.

C’est sur base de ces hypothèses que l’auteur s’est fixé comme objectif de proposer une solution plus efficace de contrôle pour s’assurer qu’il n’y a pas fraude des évadés dans notre pays précisément dans la ville de Beni mais aussi aider les services de sécurité à les retrouver grâce à l’information judiciaire qui sera fournie par son système.

Elle a finalement interconnecté les services de sécurité et le parquet pour permettre l’échange des informations ; elle a réalisé une application mobile connecté au système pour permettre aux agents de sécurité de faire le contrôle sur l’authenticité de la carte d’électeur lorsqu’il y a évasion dans une prison, elle a aussi établi une base des données qui contiendra les informations judiciaires.

Dans son travail l’auteur s’est limité à la vérification des casiers judicaires par carte d’identité or cela ne suffit pas avec l’évolution et l’avancée de la nouvelle technologie car une pièce d’identité est facilement piratable au point où nous ne saurons distinguer le vrai de la fausse. En effet plusieurs contraintes sont constatés telle que la perte de la carte ou soit l’oubli de la carte d’identité.

**III. Identification biométrique par le visage et l’oreille**

Ben Othmane Imene et Djaala Ines[28]dans leur travail de mémoire se sont intéressés à deux modalités biométriques, qui sont le visage et l’oreille, c’est ainsi qu’ils proposent la méthode des faces propres PCA pour réaliser le système de reconnaissance de visage.

Dans la partie du système de reconnaissance d’oreille humain, ils ont proposé une approche d’extraction des caractéristiques géométriques basées sur un prétraitement par des filtres avec une classification basée sur les réseaux de neurones artificiel ANN.

Dans ce travail ils ont étudié l’identification des personnes en employant des images faciales ; la méthode de faces propres a été testée sur une base de données qui a été créé à partir de la base de données standard de visage face, ils ont aussi utilisé une méthode qui se base sur l’analyse en composantes principales. C’est une méthode de comparaison simple méthode des distances euclidiennes entre les vecteurs représentant les images pour déterminer la personne la plus favorable pour réduire la dimension des images.

**IV. Etude et réalisation d’un système de détection des auteurs d’un crime à partir des emprunts digitaux.**

KAKULE ISUKA Victoire, dans son travail [29] s’est fixé l’objectif d’étudier et réaliser un système de détection des auteurs d’un crime à partir des empreintes digitales.

Il envisage que la conception d’un système qui pourrait détecter les empreintes digitales sur un bien matériel, et le prélèvement des empreintes digitales sur un bien après intrusion permettrait d’identifier l’auteur.

La finalité de ce travail, est la confirmation des hypothèses émises dans l’introduction de ce travail, à cette optique où les empreintes digitales ont été utilisées et intégrées dans l’investigation criminel.

Dans ce travail l’auteur fait usage d’une autre modalité biométrique qui est celle de l’empreinte digitale pour détecter les criminels, une méthode efficace dans l’investigation ou la recherche des criminels cependant l’auteur n’a pas envisagé une technique qui permettrait de traquer ce dernier s’il décide d’échapper aux institutions judiciaires.

**V. Criminal Face Recognition System**

Pour Alireza Chevelwalla, Ajay Gurav, Sachin Desai, Prof. Sumitra Sadhukhan [30] leur système vise à identifier les criminels dans tout service d'enquête. Dans leur système, ils stockent les images de criminels dans sa base de données ainsi que ses détails, puis ces images sont segmentées en quatre tranches-front, yeux, nez et lèvres. Ces images sont à nouveau stockées dans un autre enregistrement de base de données afin de rendre le processus d'identification plus facile. Des témoins oculaires sélectionneront les tranches qui apparaissent à l'écran et en l'utilisant il récupère l'image du visage de la base de données. Ainsi ce système fournit un environnement très convivial à la fois pour l'opérateur et le témoin oculaire pour identifier facilement le criminel, si le casier judiciaire existe dans la base de données.

Nous saluons le travail qu’a abattit ces auteurs néanmoins une faille que nous remarquons dans leurs systèmes ce qu’ils ont besoin des témoins oculaires des faits pour ainsi rassembler l’image segmentée et voir si l’image correspond à une image déjà enregistrer dans la base de données ce qui pourrait conduire à une imprécision et à des faux résultats mais aussi des retards dans les enquêtes et dans la capture du criminel,

**VI. Computerized Crime Tracking System**

Rashmi, Amrutha et Manu Prakash [31], Dans leur travail, l’objectif de leur système est de faciliter la police de traquer les criminels dans un laps de temps, les autorités gouvernementales ont constaté l’insécurité dans la partie Nord du Nigeria causée par le groupement séculier.

Ils ont abouti à un système d’enregistrement d’information criminelle (CRIS : Criminal Record Information System). Qui est un système de suivi du crime qui aide les agents de sécurité à déterminer les sites de crime potentiels en examinant des critères complexes apparemment sans rapport et en les affichant tous dans une interface. Traditionnellement, ces activités ont été soutenues par du papier et un stylo. Les policiers par ce système ont maintenant la capacité pour générer immédiatement un rapport de crime directement pertinent à la situation critique.

**VII. La reconnaissance faciale fait son chemin dans les aéroports**

Dans son article publié le dimanche 20 octobre 2019, la radiotélévision Belge Francophone [32], nous explique comment la reconnaissance faciale est le sésame d'un aéroport du futur au parcours passager fluidifié : un simple regard vers un capteur permet de franchir toutes les étapes, de l'enregistrement à l'embarquement. Dans cet aéroport de demain, le passager présentera à une borne son passeport dont la photographie sera recoupée avec les données biométriques de son visage saisies par un capteur à l'enregistrement, au dépôt des bagages, au contrôle à la frontière et enfin à l'embarquement.

Tout en reconnaissant les apports qu’offrent les travaux susmentionnés, il convient de donner quelques éléments qui différencient ce travail des autres : il se focalise sur la détection des personnes recherchés par la justice à partir de la reconnaissance faciale et de visualiser le résultat qui est une alerte après toute reconnaissance.

## I.3. Spécifications d’exigences logicielles

Dans cette section de notre travail nous décrivons le comportement externe de notre système. Cette partie nous offre un aperçu global décrivant le fonctionnement de notre système et les caractéristiques des utilisateurs de notre système.

### Perspective du logiciel

Notre application de détection des criminels ou des personnes en conflit avec la loi sera dotée d’une base de données contenant les informations nécessaires sur un criminel ou la personne recherchée par la justice comme son identité complète, ses différentes images, son casier judiciaire, la punition, la date de son arrestation ou son emprisonnement et la date de sa libération ensuite l’application sera en mesure de faire la reconnaissance des visages si le criminel en fuite se présente dans un champs qui permettra la capture de son visage afin de l’identifier s’il correspond ou pas. Si la personne correspond ou est trouvée dans la base de données l’application devra être capable d’alerter les services de sécurité pour que celui-ci soit appréhendé par les services habiletés.

#### Fonctionnalités du produit

Avant d’effectuer n’importe quelle opération, le système prévoit une partie d’authentification pour l’administrateur et l’utilisateur du système. L’administrateur qui est le commissaire de la police judiciaire se charge d’enregistrer une personne recherchée par la justice soit un détenu en récoltant ses identités et toutes ses informations judiciaires ; il a la capacité de modifier une information d’un détenu, peut aussi le supprimer du système, il sera assigné la tache de gérer le compte utilisateur c’est-à-dire qu’il peut créer un utilisateur, le modifier et si nécessaire le supprimer aussi. L’utilisateur du système qui est un agent de la DGM ou un agent de la police sera chargé d’effectuer la reconnaissance faciale et visualiser le résultat si la personne est connue ou pas dans la base des données, ainsi pour toute personne ayant été reconnue le système lancera une alerte pour que la personne soit saisie par les services sécuritaires. La figure ci-dessous décrit très clairement les taches de chacun de l’administrateur et l’utilisateur simple :

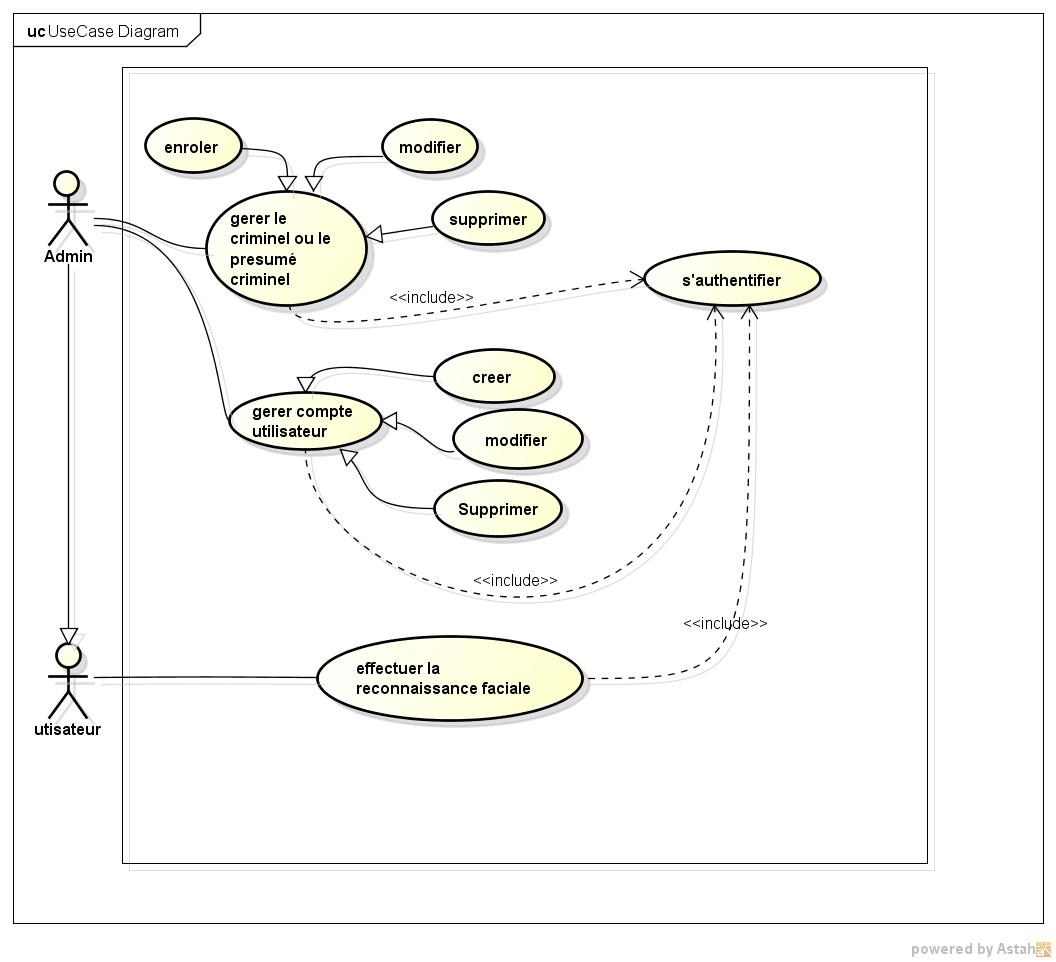


Figure 6 : Diagramme de cas d'utilisation

#### Caractéristiques des utilisateurs

Cette application sera utilisée par les agents de sécurité ayant des notions préliminaires en informatique.

#### Dépendances et suppositions

Pour son bon fonctionnement, notre application ne dépendra d’aucun système externe ni encore moi d’un API.

#### Fonctionnalités reportées à une version ultérieure

Vu que les fonctionnalités sont limitées à celles déjà prescrites dans la première version de notre application, nous comptons dans une version ultérieure étendre les champs d’action du système à la gestion des prisons en y ajoutant les fonctionnalités telles que lancer une alerte en cas d’évasion d’une prison, lancer un avis de recherche ; dans les versions ultérieures nous comptons intégrer un module d’investigation des crimes en utilisant nos cameras pour enregistrer toutes les scènes du crime et faciliter la traque des malfrats.

### Performance

Des nombreuses conditions réelles affectent la performance d’un système de reconnaissance faciale cependant en dépit de tous ses aspects notre système sera en mesure de supporter la reconnaissance des plusieurs visages à la fois et cela en temps réel.

### Fiabilité

Le système devra être disponible vingt-quatre heures sur vingt-quatre. L’administrateur et / ou l’utilisateur se connectent en temps voulu, et le nombre de fois qu’ils veulent selon leurs disponibilités au service à condition qu’ils aient le droit d’accès. En cas, de panne ou de faille, une équipe de maintenance devra être prête pour le dépannage. L’équipe de la maintenance pourra prendre quelques heures de correction en cas de disfonctionnement.

### Sécurité

L’identité d’une personne enregistrée dans la base de données est l’une des informations de plus sensible. Nous ne pouvons-nous permettre d’exposer ces données de peur qu’elles soient falsifiées ce qui peut nous mener à l’imprécision, à perte de données, aux menaces, … L’application devra être développée de manière à limiter les risques liés à la sécurité des données. Notons qu’une authentification est requise pour avoir accès au système.

### Portabilité

Notre application est une plateforme hébergée sur un serveur distant. Seuls l’administrateur et l’utilisateur peuvent y accéder avec un système d’exploitation et un terminal de leur choix à condition que ce dernier se connecte dans le même réseau que le serveur applicatif et s’authentifie avec succès.

Dans ce chapitre, nous avons donné un aperçu général sur les concepts clés de notre travail. Nous avons passé en revue les travaux de nos prédécesseurs dans le but d’en dégager l’originalité de notre travail enfin nous avons parlé des exigences logicielles qui a décrit le fonctionnement de notre application ce qui nous permet d’entamer la partie suivante celle de la méthodologie appliquées et modélisation de notre système.

# CHAPITRE II. METHODOLOGIE ET CONCEPTION DU SYSTEME

Apres un aperçu global sur les concepts clés de notre système, ce chapitre consiste à décrire scrupuleusement les méthodes et les techniques utilisées afin de résoudre le problème posé. De même, ce chapitre nous permet de mettre au clair les détaillé la conception du système

## II.1 Méthodologies et techniques

### II.1.1 Méthodes

La méthode désigne un ensemble ordonné de manière logique de principes, règles, d’étapes, qui constitue un moyen pour parvenir à un résultat [33]. En effet la méthode est très importante car elle permet de mener de manière plus efficace une étude ou la résolution d'un problème. La méthodologie est cette systématisation de l'étude, indépendamment du thème à étudier lui-même. Pour pouvoir vérifier et confirmer la véracité des hypothèses posées dès le début du travail nous avons suivis certaines méthodes scientifiques dont :

#### A. La modélisation.

**La modélisation** est la représentation d'un système de façon la plus facile à appréhender. Elle consiste à créer une représentation simplifiée d'un problème : le modèle, qui est une représentation abstraite et simplifiée (qui exclut certains détails), d’une entité (phénomène, processus, système, etc.) du monde réel en vue de le décrire, de l’expliquer ou de le prévoir. Grâce au modèle il est possible de représenter simplement un problème, un concept et le simuler.

Notons que la modélisation est constituée de deux étapes essentielles :

* L'analyse, c'est-à-dire l'étude du problème dans le but de le comprendre profondément,
* La conception, soit la mise au point d'une solution au problème. Le modèle constitue ainsi une représentation possible du système pour un point de vue donné.

En d’autres termes, concrètement un modèle est une représentation simplifiée de la réalité en vue de réaliser un traitement moyennant un ordinateur. Nous avons fait usage du langage UML pour modéliser notre système. La modélisation nous a ouvert à l’implémentation de notre système.

#### B. Simulation.

La simulation consiste à décrire le résultat d’un phénomène, comme s’il est réel, d’après futuraTech, la simulation informatique, ou simulation numérique, est une série de calculs effectués sur un ordinateur et reproduisant un phénomène physique. Elle aboutit à la description du résultat de ce phénomène, comme s'il s'était réellement déroulé [34]. Nous nous sommes servis de cette méthode pour simuler la base des données des personnes en conflit avec la loi ou des criminels considérant que ceux-ci ont déjà été enrôler d’avance.

#### C. La méthode d’expérimentation

La méthode expérimentale consiste à tester la validité d'une hypothèse, en reproduisant un phénomène (souvent en laboratoire) et en faisant varier un paramètre [35]. Pour vérifier notre hypothèse nous sommes passés à son expérimentation. Cette méthode nous a permis de tester la performance de notre système nouvellement implémenté.

### II.1.2 Techniques

Par techniques de recherches, on sous-entend un ensemble particulier de procédés permettant d'obtenir un résultat déterminé. Spécialisé, qui relève d'un domaine ou activité. En effet une technique constitue l’ensemble des moyens mis en œuvre en vue d’atteindre un but. En fin d’enrichir ce travail lors de son élaboration voici quelques techniques dont nous avons fait usage :

#### A. La technique documentaire

Cette méthode nous a aidé dans l’enrichissement de notre travail car elle nous a permis de consulter plusieurs archives des travaux scientifiques qui ont un trait de ressemblance avec le nôtre. Nous avons ainsi consulté quelques thèses, mémoire, article et nous y avons tiré certaines informations nécessaires qui sont d’une façon ou d’une autre intervenues dans la rédaction tout comme dans l’implémentation de notre système.

#### B. La technique d’interview

Nous avons eu des échanges avec certaines autorités de service de sécurité locale de Beni et le parquet. Ces dernières nous ont présenté les problèmes auxquels ils font face dans leur métier : l’absence d’un système informatique lors de la recherche des criminels a beaucoup attiré notre attention.

## II.2 Conception du Système avec UML

En Ingénierie, la conception est une étape de création d’un projet dont le but est de créer un système répondant à des nécessités présentées lors de l’analyse d’un problème posé [36].

Pour la modélisation de notre système nous utilisons UML qui est un langage de modélisation Par ailleurs, nous nous basons sur les trois vues de modélisation avec UML pour mieux modéliser notre système dont la vue fonctionnelle, la vue dynamique et enfin la vue statique.

### II.2.1 Vue fonctionnelle

La vue fonctionnelle donne un aperçu sur le fonctionnement du système à modéliser. Nous nous servons du diagramme de cas d’utilisation pour illustrer le fonctionnement du système.

#### Diagramme des cas d’utilisation

En anglais (use case Diagram), décrit, sous forme d’actions et de réactions, le comportement d’un système du point de vue d’un utilisateur il permet de définir les limites du système et ses relations avec l’environnement [37].

Il constitue la première étape de l’analyse UML en :

* Modélisant les besoins des utilisateurs.
* Identifiant les grandes fonctionnalités et les limites du système.
* Représentant les interactions entre le système et ses utilisateurs.

Les cas d’utilisation permettent d’exprimer le besoin des utilisateurs d’un système, ils sont donc une vision orientée utilisateur de ce besoin au contraire d’une vision informatique [38]. Le diagramme de cas d’utilisation sert donc à modéliser « à quoi » sert le système en organisant les interactions possibles avec les acteurs. Celui-ci se base sur 3 principaux concepts que voici : acteurs, cas d’utilisation et liens entre les acteurs et les cas d’utilisation et entre les acteurs eux-mêmes.

Dans notre cas notre système comprend deux acteurs principaux dont :

* **L’administrateur** : celui-ci est le maitre du système. Il gère le criminel ou la personne recherché par la justice, il a le pouvoir d’enrôler, modifier, supprimer ce dernier et gère aussi l’utilisateur c’est-à-dire qu’il a la capacité d’enregistrer, modifier ou supprimer un utilisateur, dans notre cas l’admin hérite de tout ce que fait l’utilisateur, avant d’effectuer toutes tâches, il lui est demandé de s’authentifier dans le système.
* **Utilisateur** : c’est un acteur qui effectue la reconnaissance faciale et visualise le résultat une fois de plus il faudra que celui-ci s’authentifie avant de pose toute action dans le système.

Voici le diagramme de cas d’utilisation de notre système :

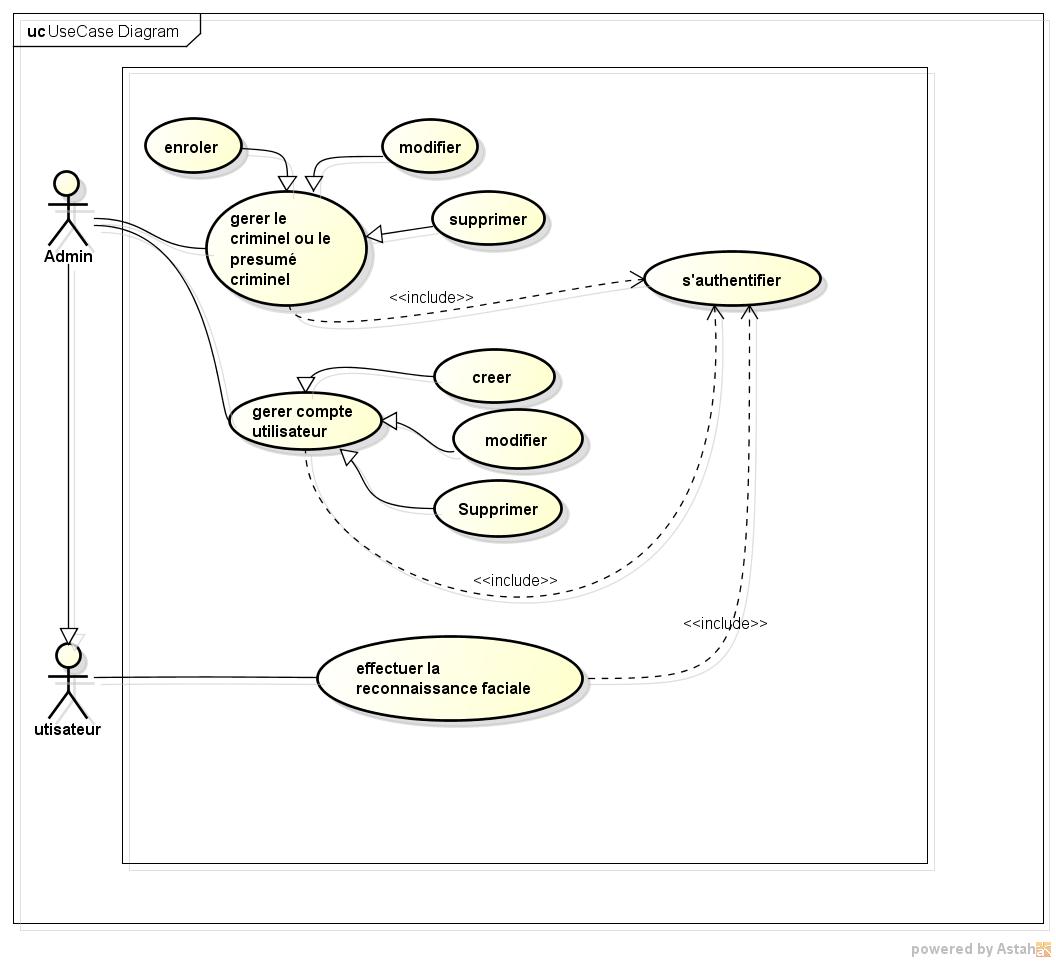
**Le diagramme de cas d’utilisation illustré ci-dessus trouve son explication dans le tableau ci-après :

Figure 7: Diagramme de cas d'utilisation du système

Dans le tableau ci-dessous trouvons une explication brève du diagramme de cas d’utilisation de notre système représenté dans la figure ci-dessus :

|  |  |  |  |
| --- | --- | --- | --- |
| Cas d’utilisation | Objectif | Précondition | Acteurs |
| S’authentifier | Se connecter au système | Être agent de services de sécurité et avoir un compte actif | Administrateur et Utilisateur |
| Gérer un criminel soit une personne recherchée par la justice | Lister personnes recherchées par la justice | Être agent de service des sécurités et être connecté au système | Administrateur |
| Gérer compte utilisateur | Identifier les utilisateurs | S’authentifier en tant qu’administrateur | Administrateur |
| Effectuer la reconnaissance faciale | Vérifier si la personne n’est pas recherchée par la justice | Être connecté et être un agent de sécurité | Administrateur et Utilisateur |

Tableau 1: Explication du diagramme de cas d'utilisation

### II.2.2 Vue dynamique

La vue dynamique va nous permettre de montrer le comportement du système, les interactions des objets et leur évolution dans le temps. La vue dynamique d'un modèle UML décrit l'aspect comportemental du modèle. La dynamique d'un système peut impliquer deux typologies déférentes de changements dans l'instance symbolique du modèle : les changements d'états d'objets individuels, provoqués par le déclenchement d'événements et l'exécution consécutive d’actions ; et des changements dans l’état général du système (dus par exemple à la création et à la destruction d'objets) [38].Cette vue comprend plusieurs diagrammes. Cependant dans ce travail nous présentons :

#### Diagrammes d’activités

Un diagramme d'activité fournit une vue du comportement d'un système en décrivant la séquence d'actions d'un processus [39]. Il permet ainsi de représenter graphiquement le comportement d'une méthode ou le déroulement d'un cas d'utilisation [38]. Dans ce travail, nous détaillons trois diagrammes d’activités pour trois cas d’utilisations dont :

* **Le cas d’utilisation s’authentifier :**

La figure ci-dessous est une représentation du diagramme d’activité du cas s’authentifier :

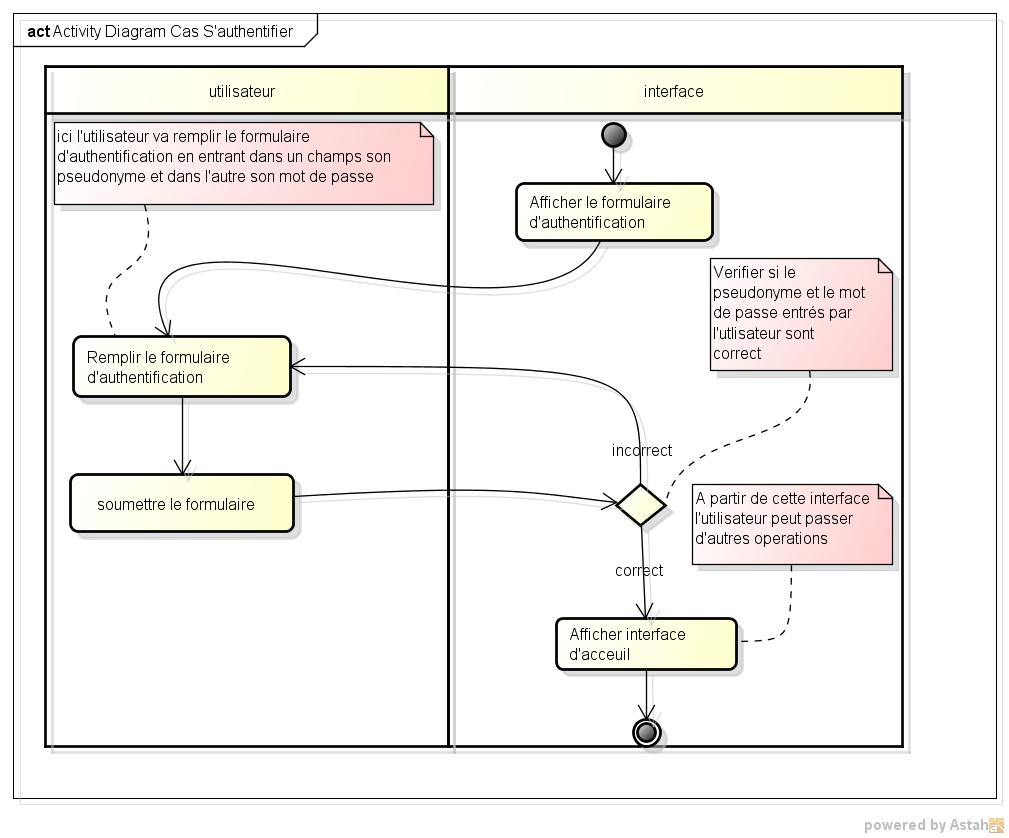


Figure 8: Diagramme de cas d'activité s'authentifier

**Explication du diagramme** : Après avoir été enregistré comme utilisateur, l’authentification est obligatoire pour utiliser le système. C’est ainsi qu’un utilisateur saisit d’abord son pseudonyme et son mot de passe et le soumettre avant d’effectuer toute opération. Cette action déclenche une vérification du pseudonyme et du mot de passe, s’ils sont corrects alors, il est authentifié alors l’interface d’accueil s’ouvre et c’est à partir de cette dernière que l’utilisateur peut passer d’autres opérations. Dans le cas contraire, l’utilisateur n’est pas authentifié et le système lui renvoie à l’étape de remplir le formulaire.

* **Le cas d’utilisation enrôler une personne recherchée par la justice :**

Nous représentons dans la figure suivant le diagramme d’activité du cas enrôler un criminel ou un présumé criminel soit une personne recherchée par la police

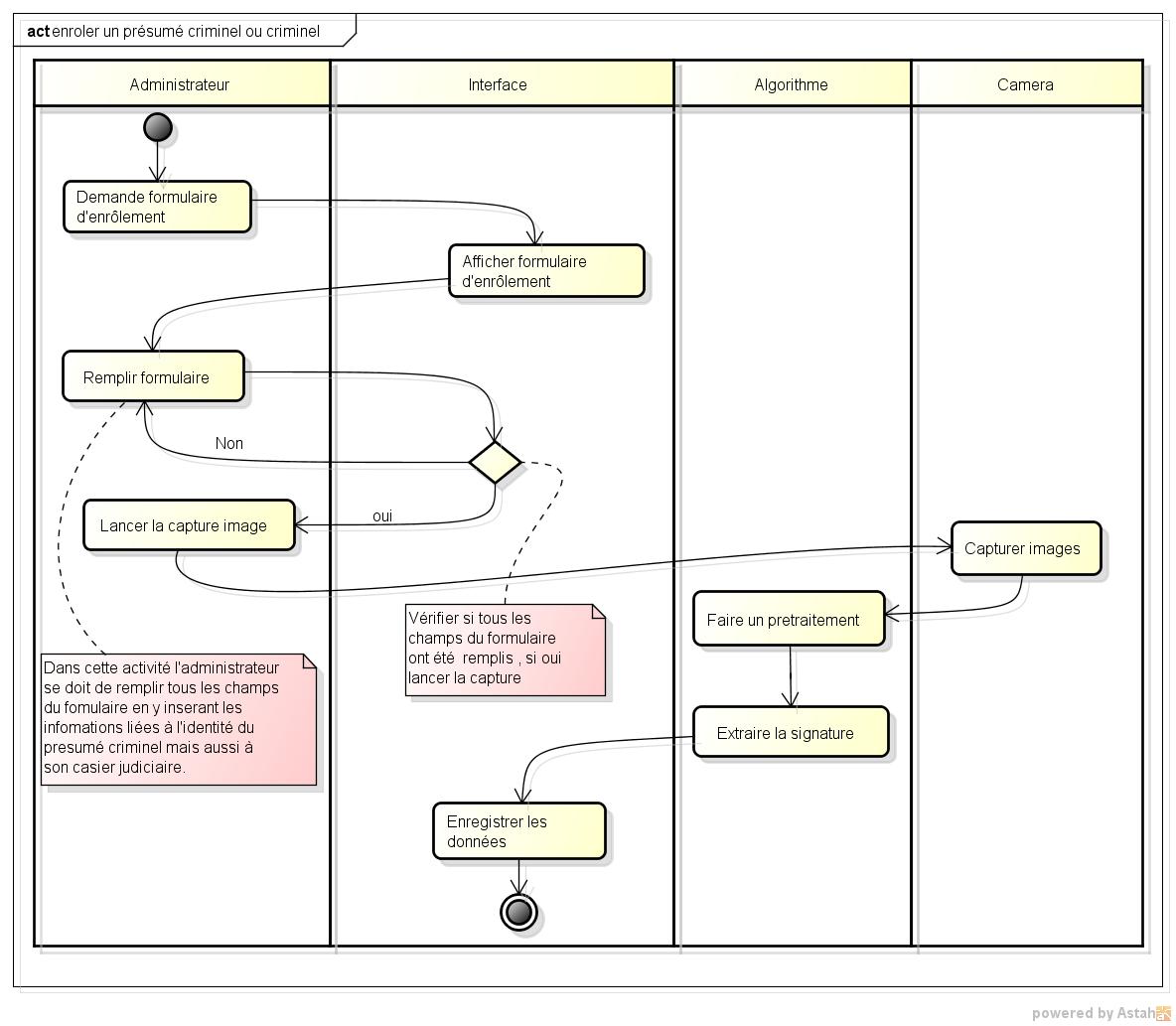


Figure 9: Diagramme d'activité cas enrôler criminel soit présumé criminel

**Explication du diagramme**: Dans ce diagramme l’administrateur du système fait une demande d’un formulaire d’enrôlement aussitôt que le système lui présente un formulaire d’enrôlement celui-ci le remplit en y entrant toutes les informations du criminel ou du présumé criminel soit d’une personne recherchée comme son identité, son casier judiciaire et son adresse si ces informations sont remplies correctement, l’administrateur va lancer la capture des images pendant que la capture sera en train d’être faite par la caméra, l’algorithme se chargera d’y appliquer des certains prétraitements , en extraire la signature numérique puis l’enregistrer.

* **Le cas d’utilisation effectuer la reconnaissance faciale.**

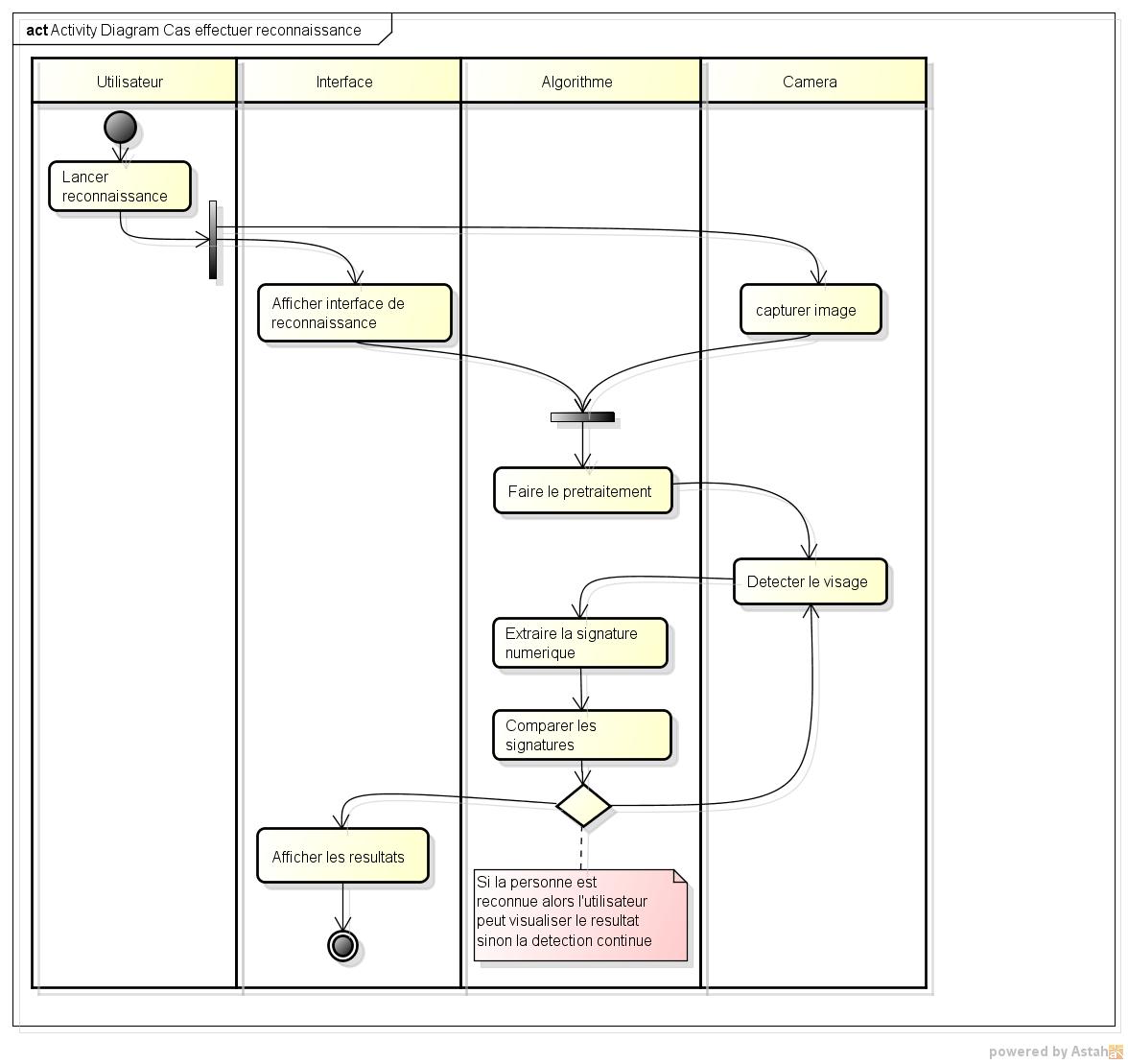
La figure ci-dessous est une représentation du diagramme d’activité du cas s’authentifier :

Figure 10: Diagramme d'activité cas effectuer reconnaissance faciale.

**Explication du diagramme**: Dans ce diagramme l’utilisateur lance la reconnaissance par un bouton ce qui permet d’initialiser la caméra et de l’ouvrir ensuite une fenêtre va s’afficher et c’est le début de la reconnaissance des visages.

* **Faire les prétraitements :** cette activité consiste à convertir l’image qui a était capturée de BGR en RGB [[3]](#footnote-3) car l’algorithme que nous utilisons, emploi le RGB.
* **Détecter le visage :** Dans cette activité le système au travers la caméra va détecter tous les visages humains grâce à la méthode **face\_locations[[4]](#footnote-4),** c’est une méthode qui a été entrainé pour détecter rien que les visages dans la librairie face\_recognition.
* **Extraire la signature numérique :** Dans cette partie l’algorithme va assigner à toutes les images capturées une signature numérique c’est-à-dire une valeur numérique**.**
* **Comparer les signatures :** Ensuite vient la comparaison de la valeur numérique pendant la reconnaissance avec celle de la base de données recueillie au cours de l’enrôlement avec un seuil de tolérance inférieur ou égal à 0.6.
* **Afficher les résultats :** ici l’utilisateur sera entrain de visualiser le résultat sur son écran et en cas d’une personne recherchée trouvé ; le système renvoi une alerte.

#### Les diagrammes de séquences

Le diagramme de séquence affiche les évènements par ordre chronologique ; en d’autres termes, il nous permet de décrire comment les objets (instances) échangent les messages dans un ordre particulier [38].

Pour les 3 diagrammes d’activités, voici les trois diagrammes de séquences y afférant.

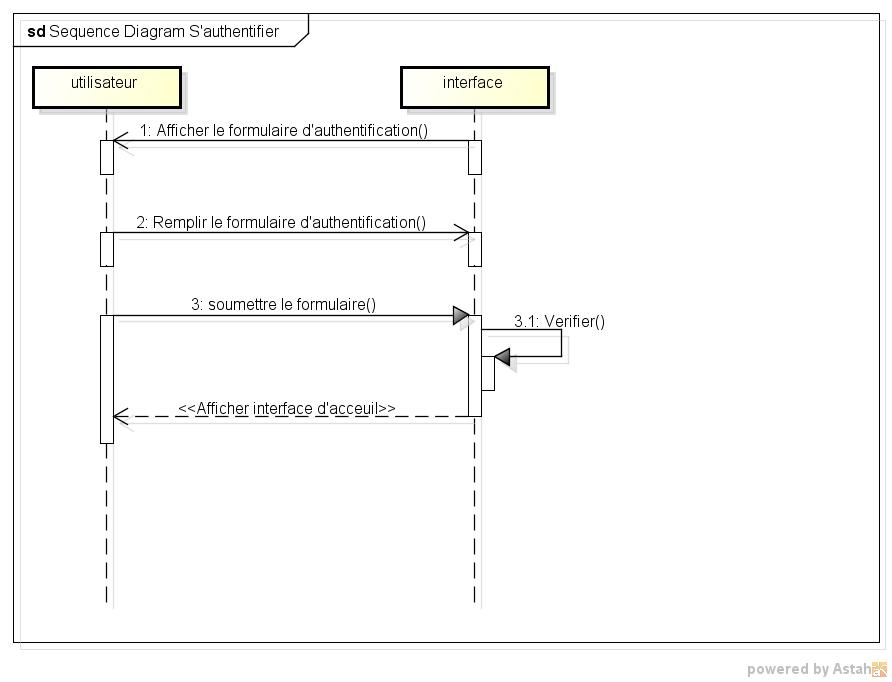
* Cas s’authentifier

Figure 11: Diagramme de séquences cas s'authentifier

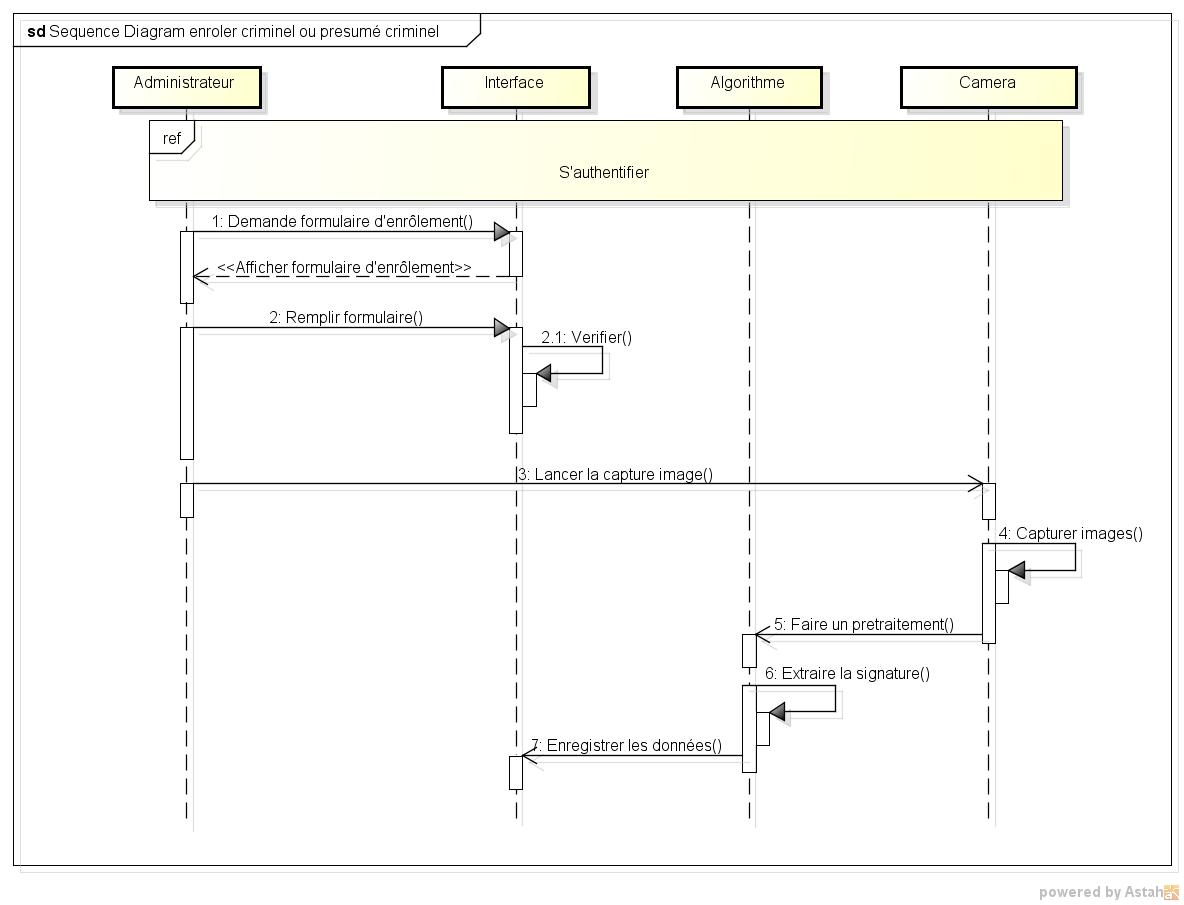
* Cas enrôler un criminel ou présumé criminel

Figure 12 : Diagramme de séquences cas enrôler criminel ou présumé criminel

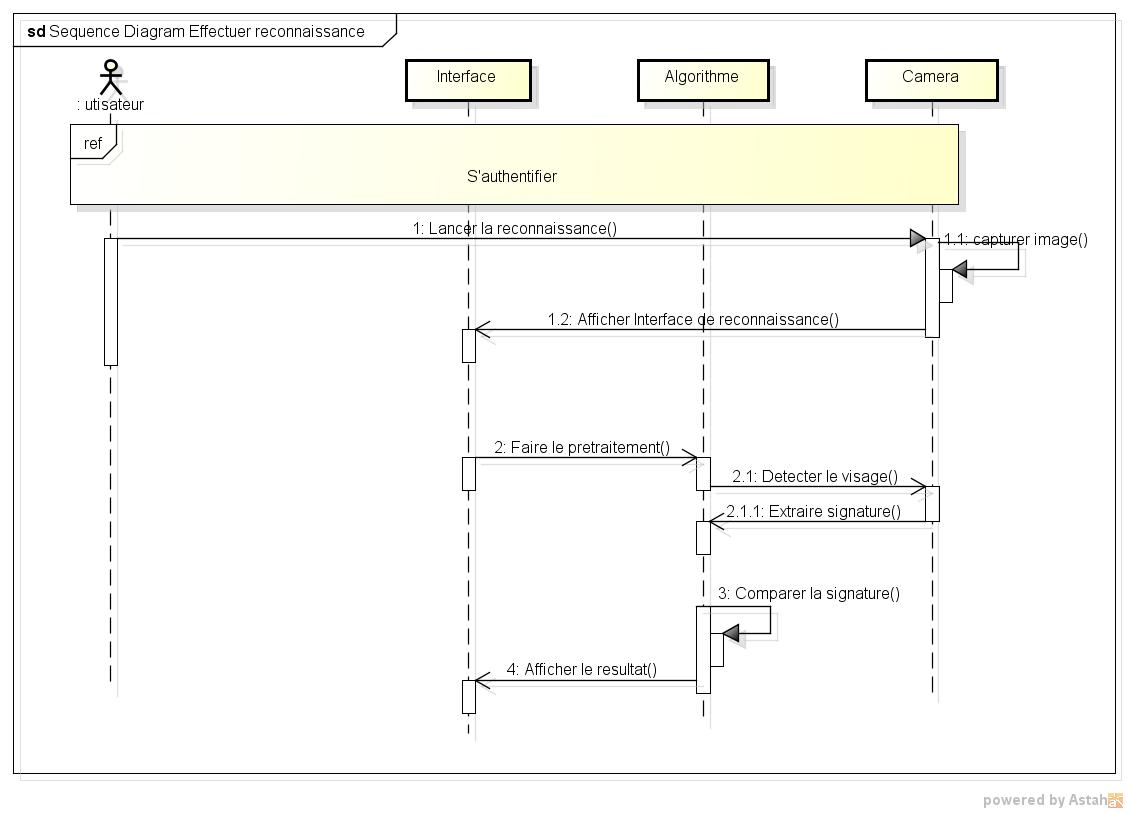
* Cas effectuer reconnaissance faciale.

Figure 13 : Diagramme de séquences cas effectuer reconnaissance faciale

### II.2.3 Vue statique

La vue statique modélise les concepts du domaine d'application, qui est affiché dans les diagrammes de classes, ainsi nommés, car leur objectif principal est la description des classes. Une classe est la description d'un concept du domaine d'application ou de la solution d'application [38]. Cette vue comprend plusieurs diagrammes comme le diagramme de déploiement, le diagramme d’objets, le diagramme de classe, dans ce présent travail, nous présentons le diagramme de classe.

#### A. Diagramme de classes

Les diagrammes de classes décrivent clairement la structure d’un système particulier en modélisant ses classes, ses attributs, ses opérations et les relations entre ses objets [40]. Le diagramme de classe montre un système du point de vie structure interne contrairement au diagramme de cas d’utilisation qui montre un système du point de vue des acteurs, il permet donc de fournir une représentation abstraite des objets du système qui vont interagir entre eux pour réaliser les cas d’utilisation [38].

Dans la figure suivante trouvons le diagramme de classe de notre système :

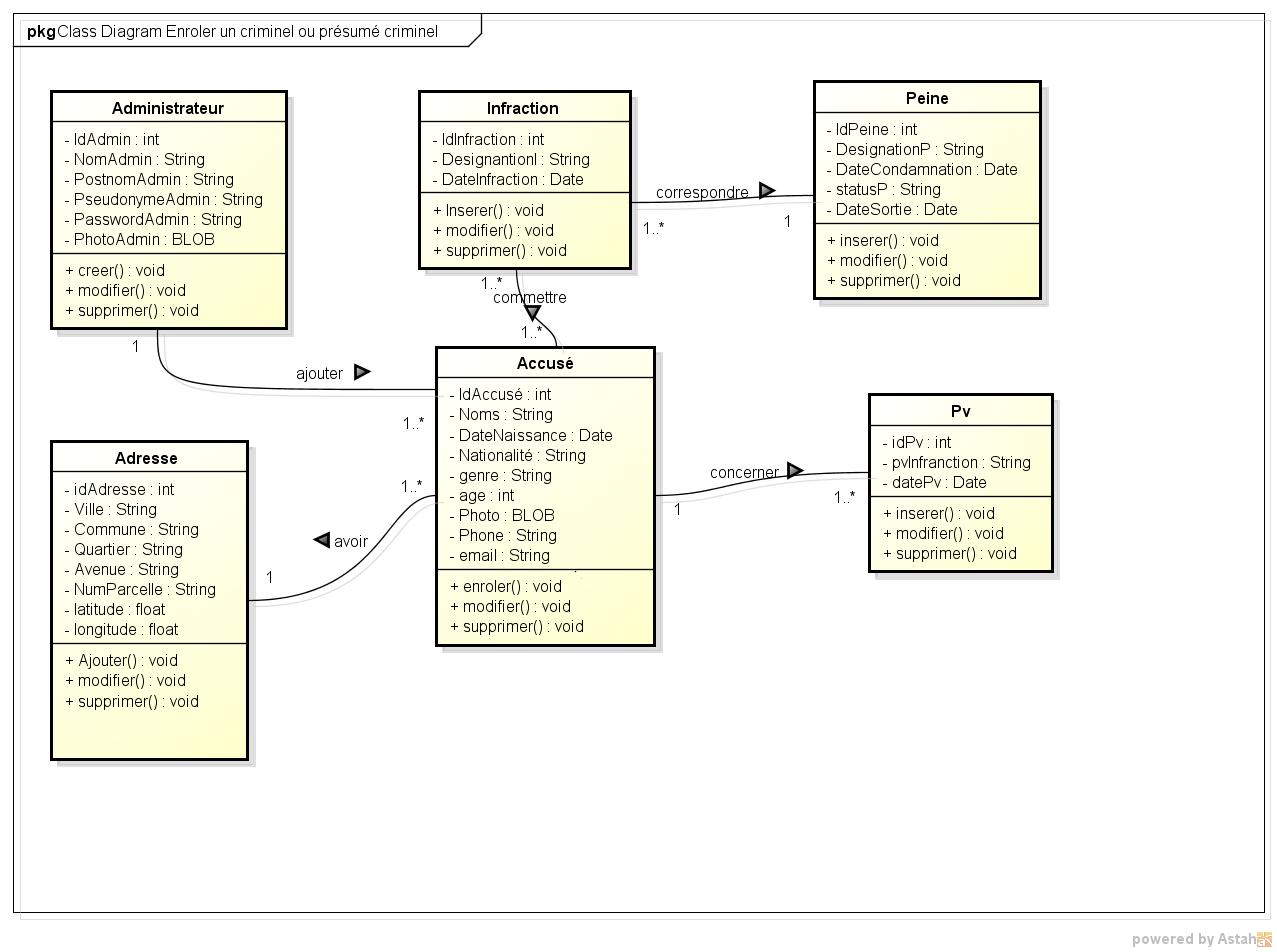
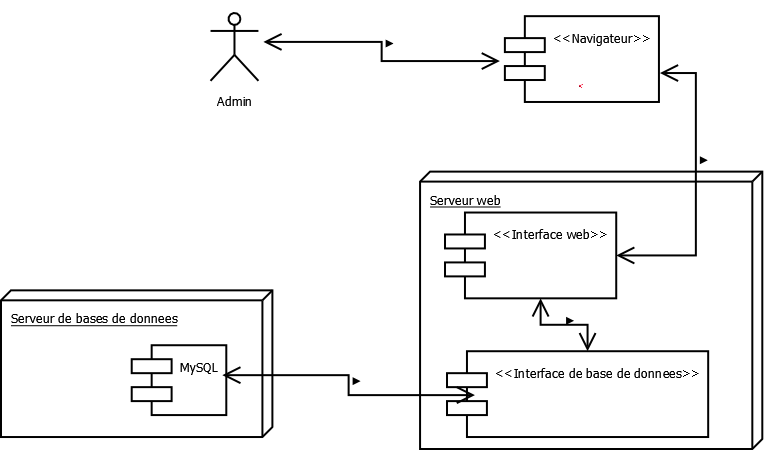


Figure 14 : Diagramme de classe.

**Explication du diagramme :** Notre diagramme de classe contient 6 classes comme vu dans la figure ci-dessus. La classe **Administrateur** qui contient les attributs et les méthodes nécessaires correspondants à l’administrateur ; la classe **Criminel** qui contient l’identité du présumé criminel ou du criminel ; la classe **Adresse** qui va nous servir à enregistrer l’adresse de la personne recherchée, la classe **Infraction** elle nous sert à enregistrer tous les délits, toutes les contreventions et tous les crimes commis par une personne ; une classe **Peine** qui a pour attributs les sanctions prévues pour chaque infraction se trouvant dans le dossier de la personne et enfin une classe **Pv** qui se charge de stocker le PV de toutes les accusations du présumé criminel.

#### B. Diagramme de déploiement.

Un diagramme de déploiement décrit la disposition physique des ressources matérielles qui composent le système et montre la répartition des composants sur ces matériels. Chaque ressource étant matérialisée par un nœud, le diagramme de déploiement précise comment les composants sont répartis sur les nœuds et quelles sont les connexions entre les composants ou les nœuds.

Figure 15 : Diagramme de déploiement****

### II.2.4 Base de données

On appelle base de données toute collection de données ou d'informations spécialement organisée pour une recherche et une extraction rapide par ordinateur. Les bases de données sont structurées de manière à faciliter le stockage, la récupération, la modification et la suppression de données conjointement avec diverses opérations de traitement de données.

La création d’une base de données normalisée se fait suivant les étapes suivantes :

* + Niveau conceptuel
  + Niveau relationnel
  + Niveau physique

Au niveau conceptuel, en UML, nous avons le diagramme de classes (voir figure 14)

#### Modèle Relationnel

Pour constituer notre base des données, nous allons passer du diagramme de classe UML vers un modèle relationnel de tables en se basant sur certaines règles de transformation qui dépendront bien des multiplicités ou cardinalités maximales des associations entre les classes. On distingue trois familles d’associations :

* **Un-à-plusieurs** : ici il faut ajouter un attribut de type clé étrangère dans la relation fils de l’association. L’attribut portera donc le nom de la clé primaire de la relation père de l’association. La relation père est celle où on trouve une cardinalité égale à 1 et la relation fils est celle où on trouve une cardinalité plusieurs. Pour se rappeler facilement de cette règle, on la décrit de la manière suivante : la clé primaire du père migre dans la relation fils.
* **Plusieurs-à-plusieurs et n-aires** : ici l’association (classe-association) devient une relation dont la clé primaire est composée par la concaténation des identifiants des entités (classes) connectés à l’association.
* **Un-à-un :** si les deux relations minimales sont égales à un, il est préférable de fusionner les deux entités (classes).

En respectant les règles de transformation, voici l’illustration de notre modèle relationnel :

**ADMINISTRATEUR** [idAdmin, nomAdmin, postnomAdmin, pseudoAdmin, passwordAdmin, photoAdmin]

**ACCUSE** [idAccuse, #idAdmin, #idAdresse, nomsAccuse, genre, age, nationalite, photo, phone, email]

**ACCUSE\_INFRACTION** [#idAccuse, #idInfraction]

**INFRACTION [**idInfraction, #idPeine designationI, dateInfraction**]**

**Pv [**idPv, # idAccuse, pvInfraction**]**

**PEINE [**idPeine, designationP, dateCondamnation, statusP, dateSortie**]**

**ADRESSE** [idAdresse, ville, commune, quartier, avenue, cellule, numParcelle, longitude, latitude]

Dans ce chapitre, nous avons premièrement présenté les méthodes et techniques que nous avons utilisées pour la réalisation de ce présent travail ensuite nous avons présenté quelques diagrammes qui nous ont guidés dans le processus de la conception et qui nous ont ainsi permis de réaliser une représentation du système que nous avons implémenté et présenté dans le chapitre qui suit.

# CHAPITRE III. IMPLEMENTATION ET PRESENTATION DU SYSTEME

Après conception du système dans le chapitre précèdent, ce présent chapitre est consacré à la présentation de l’architecture du système, à la présentation des technologies et outils utilisés lors de son implémentation ; par la suite nous présentons certaines vues des interfaces du système et enfin nous effectuons le test en présentant les résultats issus du fonctionnement du système.

## III.1. Architecture du système

## III.2. Technologies et outils utilisés

## III.3. Présentation des résultats

# CONCLUSION GENERALE

Table des matières

[EPIGRAPHE iv](#_Toc82003972)

[DEDICACE v](#_Toc82003973)

[REMERCIEMENTS vi](#_Toc82003974)

[SIGLES ET ABBREVIATIONS vii](#_Toc82003975)

[LISTE DES FIGURES viii](#_Toc82003976)

[LISTE DES TABLEAUX ix](#_Toc82003977)

[RESUME x](#_Toc82003978)

[ABSTRACT xi](#_Toc82003979)

[INTRODUCTION. 12](#_Toc82003980)

[0.1. Préambule 12](#_Toc82003981)

[0.2. Problématique. 1](#_Toc82003982)

[0.3. Hypothèses 2](#_Toc82003983)

[0.4. Objectifs de la recherche 3](#_Toc82003984)

[0.4.1. Objectif général 3](#_Toc82003985)

[0.4.2. Objectifs spécifiques 3](#_Toc82003986)

[0.5. Choix et intérêt du sujet 3](#_Toc82003987)

[0.6. Limitation et Délimitation du sujet 4](#_Toc82003988)

[0.6.1. Limitation 4](#_Toc82003989)

[0.6.2. Délimitation 4](#_Toc82003990)

[0.7. Audience 4](#_Toc82003991)

[0.8. Subdivision du travail 4](#_Toc82003992)

[CHAPITRE I. GENERALITES SUR LE TRAVAIL 6](#_Toc82003993)

[I.1. Définitions des concepts-clés 6](#_Toc82003994)

[I.1.1. Système 6](#_Toc82003995)

[I.1.2. Système intelligent 6](#_Toc82003996)

[I.1.3. Détection 8](#_Toc82003997)

[I.1.4. Criminel 8](#_Toc82003998)

[I.1.5. Généralités sur la reconnaissance faciale. 8](#_Toc82003999)

[I.2. Revue de la littérature 18](#_Toc82004000)

[I.3. Spécifications d’exigences logicielles 22](#_Toc82004001)

[A. Perspective du logiciel 22](#_Toc82004002)

[B. Performance 25](#_Toc82004003)

[C. Fiabilité 25](#_Toc82004004)

[D. Sécurité 25](#_Toc82004005)

[E. Portabilité 25](#_Toc82004006)

[CHAPITRE II. METHODOLOGIE ET CONCEPTION DU SYSTEME 27](#_Toc82004007)

[II.1 Méthodologies et techniques 27](#_Toc82004008)

[II.1.1 Méthodes 27](#_Toc82004009)

[II.1.2 Techniques 28](#_Toc82004010)

[II.2 Conception du Système avec UML 29](#_Toc82004011)

[II.2.1 Vue fonctionnelle 29](#_Toc82004012)

[II.2.2 Vue dynamique 31](#_Toc82004013)

[II.2.3 Vue statique 38](#_Toc82004014)

[II.2.4 Base de données 40](#_Toc82004015)

[CHAPITRE III. IMPLEMENTATION ET PRESENTATION DU SYSTEME 42](#_Toc82004016)

[III.1. Architecture du système 42](#_Toc82004017)

[III.2. Technologies et outils utilisés 42](#_Toc82004018)

[III.3. Présentation des résultats 42](#_Toc82004019)

[CONCLUSION GENERALE 42](#_Toc82004020)

1. Intelligence artificielle : est un ensemble de théories et de techniques développant des programmes informatiques complexes capables de simuler certains traits de l'intelligence humaine (raisonnement, apprentissage…). En termes simple l’IA est un concept visant à **donner aux machines la capacité de raisonner comme un être humain**. [↑](#footnote-ref-1)
2. ADN : signifie [acide](https://www.futura-sciences.com/sciences/definitions/chimie-acide-750/) désoxyribonucléique, et constitue la [molécule](https://www.futura-sciences.com/sciences/definitions/chimie-molecule-783/) support de l'information génétique [héréditaire](https://www.futura-sciences.com/sante/definitions/medecine-hereditaire-2713/). [↑](#footnote-ref-2)
3. RGB : est **un mode colorimétrique utilisé en informatique et qui permet de coder une couleur.** Le sigle RGB signifie Red-Green-Blue en anglais. On emploie aussi le terme RVB (pour Rouge-Vert-Bleu en français). Il s'agit donc d'un procédé utilisé par défaut pour l'affichage des couleurs sur un écran (ordinateur, appareil photo numérique, télévision...). [↑](#footnote-ref-3)
4. https://www.programcreek.com/python/example/111024/face\_recognition.face\_locations [↑](#footnote-ref-4)