République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Akli Mohand Oulhadj de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Mémoire de Master

en Informatique

Spécialité : *Ingénierie des Systèmes d'Information et de Logiciels*

Thème

Système de contrôle d'accès intelligent

Encadré par

— Boudjelaba Hakim

Réalisé par

— Malki Said

— Daifi Salaheddine

2020/2021

Remerciements

Nous voudrions par ce biais adresser nos sincères remerciements à dieu tout puissant dans sa grâce et sa miséricorde qui nous a accordé la santé, le temps et la force de réaliser ce travail de fin de cycle et nos remerciements à tous ceux qui ont contribué d'une manière ou d'une autre à la rédaction de ce mémoire, précisément :

Nous tenons à exprimer nos vifs remerciements à Mr Boudjelaba Hakim, de nous avoir encadré et pour ses conseils, ses motivations, sa disponibilité et sa volonté à nous aider à travers de multiples réunion.

Dédicaces

Je dédie ce travail à :

Ma Mère, ma paradis qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois a travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, mon hero qui peut être fière et trouver ici le résultat des longues années de sacrifices et de privations pour m'aider à avancer dans ma vie, merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

Mes chères frères Noureddine, Ahmed, Toufik, Abdelhakim et Mohamed.

Mes sœurs, et les filles Amina et Hanane.

Mon très cher ami Salaheddine et sa famille.

Mes chers amis Oussama, Billel, Adel et Yassine.

MALKI Saïd

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail à :

Ma Mère Rahma : "tu m'as donné la vie, la tendresse, l'amour, et le courage pour réussir

En témoignage, je t'offre ce modeste travail pour te remercier pour tes sacrifices et pour l'affection dont tu m'as toujours entourée".

Mon Père Daif : "L'épaule solide, l'œil attentif et la personne la plus digne de mon estime et de mon respect. Aucun dédicace ne saurait exprimer mes sentiment, que dieu te préserve et te procure santé et lange vie".

Mes chers Frères et Sœur : Lotfi, Zoubida, Faiza, Abdelhak et Chouaib pour leur encouragement contenu et leur soutient qu'ils trouvent ici l'expression de ma haute gratitude.

Mon très cher ami Saïd et sa famille.

Mes chers amis et à ceux qui m'aimaient : Anis, Yahia, Hamza, Djamel, Hichem, Amayasse.

Daifi Salaheddine

Abstract

Machine recognition of human face is an active and fast growing area of research due to a wide variety of commercial and law-enforcement applications including access control, security monitoring, and video surveillance. Determining automatically the identity of a person is an ongoing problem, it is necessary to recognize users in order to give them access to a building or allow them to use specific resources in order to increase security level. Our mission is to find out a new way to implement a face recognition based access controlling system using LBPH algorithms in this thesis we provide a brief overview of this growing research area and indicate the present state of art of the field.

Key words : Machine recognition, Acces control, LBPH ...

Résumé

La reconnaissance automatique des visages humains est un domaine de recherche actif et en pleine expansion en raison d'une grande variété d'applications commerciales et policières, notamment le contrôle d'accès, la surveillance de sécurité et la vidéosurveillance. Déterminer automatiquement l'identité d'une personne est un problème permanent, il est nécessaire de reconnaître les utilisateurs afin de de leur donner accès à un bâtiment ou de leur permettre d'utiliser des ressources spécifiques afin d"accroitre le niveau de sécurité. Notre mission est de trouver une nouvelle façon d'implémenter un système de contrôle d'accès basé sur la reconnaissance faciale en utilisant des algorithmes LBPH. Dans ce memoire, nous fournissons un bref aperçu de ce domaine de recherche en pleine expansion et indiquons l'état actuel de l'art dans ce domaine.

Mots clés : Reconnaissance automatique, Controle d'accès, LBPH ...

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

API	Application Programming Interface
IHM	Interface Homme Machine
SCAP	Système de Contrôle d'Accès Physique
LBPH	Local Binary Pattern Histogram
PIN	Personal Identification Number

Introduction générale

La reconnaissance biométrique est définie comme la reconnaissance automatique des individus sur la base de leurs caractéristiques comportementales ou biologiques [35].

La biométrie était à l'origine utilisée dans le cadre d'enquêtes médico-légales. Cependant, les scénarios d'application ont évolué vers d'autres aspects de sécurité et de commodité. Ce lien étroit entre les individus et les identités est utilisé pour des raisons de sécurité, comme dans les applications de contrôle des frontières et de médecine légale, ou pour des raisons de commodité, comme dans la connexion automatique et la personnalisation des maisons intelligentes.

Dans le monde d'aujourd'hui, on parle de plus en plus de l'insécurité dans divers domaines et aussi des moyens informatiques à utiliser pour contrer cette tendance. La vérification et l'identification des personnes est l'un des moyens d'assurer cette sécurité. Les humains utilisent leur système visuel pour identifier automatiquement les gens, même si le processus est complexe.

Notre travail consiste a implémenter un système qui sert a la satisfaction d'un besoin necessaire qui est la sécurtié professionnelle des individus.

Nous présentons dans ce mémoire un aperçu des tendances récentes et des efforts de recherche majeurs dans les techniques de reconnaissance biométrique. Nous avons choisi d'articuler notre étude autour de quatre chapitres principaux qui est organisée comme suit :

- Chapitre 1 : la biométrie et le controle d'accès.

  Sera consacré à la présentation générale de la biométrie. Nous présenterons le principe de fonctionnement des systèmes biométriques ainsi qu'une idée générale sur le controle d'accès.

- Chapitre 2 : généralités sur le traitement d'images.

  On va presenter les principaux concepts liés au traitement d'images d'une maniére générale.

- Chapitre 3 : Analyse et réalisation

  Nous présenterons une modélisation de notre système, son architecture globale et son principe de fonctionnement. Ainsi que la présentation de notre environement travail pour l'implémentation et la mise en oeuvre de notre système de contrôle d'accès intelligent ainsi que sa représentation graphique.

Finalement nous concluons notre travail par une conclusion générale qui englobe des perspectives envisagées.

Chapitre 1

La biométrie et le contrôle d'accès

1.1 Introduction

De nos jours, il existe trois types de sécurité ou de contrôle d'accès : La première repose sur la connaissance de la personne comme un mot de passe ou un code PIN. La deuxième est basée sur ce que possède la personne comme un badge ou une carte à puce. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. Dans le deuxiem cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé. Pour contourner cette limitation ou cette faiblesse, un autre type de sécurité a été mis au point, qui n'utilise pas les informations qu'une personne possède ou connaît, mais les informations intrinsèques à cette personne. Cette nouvelle façon d'identification est appelé Biométrie.

1.2 Les Systèmes de contrôle d'accès physique

À un niveau très basique, le contrôle d'accès est un moyen de contrôler qui entre dans un lieu et quand. La personne qui pénètre dans un lieu peut être un employé, un entrepreneur ou un visiteur, et peut marcher, conduire un véhicule ou utiliser un autre moyen de transport. L'endroit où ils entrent peut être, par exemple, une enceinte, un bâtiment, une pièce ou une armoire.

1.2.1 Définition

Quand on parle d'un SCAP, On refére à un système de sécurité électronique qui utilise un moyen d'identification tel qu'une carte d'accès, empreinte, detection des yeux, . . .pour autoriser certaines personnes à accèder à certaines zones. Et, comme il est capable d'enregistrer qui a accédé à quel endroit et à quel moment, de ce fait, il peut fournir des données précieuses pour nous aider à suivre la situation de notre site.

1.2.2 Conception du système de contrôle d'accès physique

Les fonctions du système de contrôle d'accès physique dans le cadre du système de sécurité total se situent dans les phases suivantes du processus de sécurité :[8]

- **Dissuasion :** La présence visible d'une caméra de surveillance, d'un lecteur de carte ou d'un capteur d'empreinte digitale peut dissuader une personne malveillante (voleur) qui cherche une serrure facile à crocheter.
- **Prévention :** Le système permet de déverrouiller la porte uniquement pour les personnes autorisées.
- **Appréhension :** Le système peut fournir une liste de suspects si l'on pense que l'auteur de l'infraction est un employé de l'entreprise.

1.3 Techniques de base du SCAP

Tous les SCAP utilisent trois techniques de base pour contrôler l'entrée par une porte ; Ces techniques ont été décrites comme quelque chose qu'une personne sait, qu'une personne possède, et quelque chose qu'une personne ait ou fait. Physiquement, ces trois méthodes de sécurité sont : Dispositifs à code stocké, systèmes à clé portable et systèmes à attributs physiques.[8]

Dispositifs à code stocké : Un dispositif à code enregistré est une forme électronique de serrure à combinaison, qui se manifeste généralement comme un système de contrôle d'accès à clavier. La personne qui souhaite entrer doit saisir une séquence de chiffres (qu'elle connaît), que les circuits électroniques doivent reconnaître.

Système à clé portable : Les systèmes à clé portable se présentent généralement sous la forme d'un accès par carte (que la personne possède), sur laquelle est codé un numéro qui est lu électroniquement lorsque la clé est insérée dans une fente ou une rainure. Le contrôle d'accès de proximité est une forme de système à clé portable utilisant des dispositifs qui ne doivent pas être insérés dans un mécanisme de lecture et qui peuvent être lus électroniquement à des distances allant jusqu'à plusieurs mètres.

Système à attributs physiques : Les systèmes à attributs physiques, parfois appelés systèmes biométriques, mesurent une caractéristique physique ou comportementale unique (quelque chose que la personne ait ou fait) pour pouvoir identifier une personne.

1.4 La biométrie

1.4.1 Historique

La biométrie trouve ses origines dans des procédés de reconnaissance anthropométrique [1], elle a une longue histoire, Depuis des temps immémoriaux, les gens reconnaissent leurs semblables en scrutant leur visage, leur voix et leur morphologie.

Mais même cette biométrie n'est pas nouvelle : les empreintes (la plus ancienne forme de biométrie), ont des origines très lointaines, comme les tribus de Nouvelle-Écosse qui y ont dessiné une main avec les empreintes de la paume et des doigts. Ou encore, dans l'antique Babylone où les empreintes étaient utilisées pour régler des transactions ou même en Chine où des empreintes sur des sceaux en argile ont été trouvées. Aussi, déjà au 14e siècle les Chinois utilisaient les empreintes digitales et plantaires pour distinguer les jeunes enfants des marchands.

Dans une époque plus proche, au 19ème siècle l'anthropologue français Alphonse Bertillon a conçu la première méthode scientifique d'identification biométrique largement acceptée. Le système Bertillon, le bertillonnage ou l'anthropométrie ne reposait pas sur la prise d'empreintes digitales mais sur une combinaison systématique de mesures physiques.[1]

1. la pratique consistant à prendre des mesures du corps humain et à fournir des données catégorisées.

1.4.2 Définition

La première question à laquelle on doit répondre est : qu'est-ce que la biométrie ?
La biométrie est la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu et permettant l'authentification de son identité. Au sens littéral et de manière plus simplifiée, la biométrie signifie la "mesure du corps humain".[2]

1.4.3 Caractéristiques biométriques

Pour que les caractéristiques capturées soient considérées comme des caractéristiques biométriques, elles doivent être :

- **universelles** (exister chez tous les individus),
- **uniques** (permettre de différencier un individu par rapport à un autre),
- **permanentes** (autoriser l'évolution dans le temps),
- **enregistrables** (collecter les caractéristiques d'un individu avec son accord),
- **mesurables** (autoriser une comparaison future).

1.5 Les modalités biométriques

On distingue deux catégories de technologies biométriques : les mesures physiologiques, et comportementales :[2]

1.5.1 Les mesures physiologiques

Cette modalité concerne la forme et la taille du corps, peuvent être morphologiques ou biologiques telles que :

- **Reconnaissance des empreintes :**

La reconnaissance des individus par empreintes digitales est la méthode la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanant[4].
Cette technique est disponible auprès de nombreux fournisseurs à bas prix, avec ces

appareils les utilisateurs n'ont plus besoin de taper des mots de passe, mais ont un accès instantané par le toucher.[3]

Figure 1.1 – Image d'une empreinte numérique.[49]

• **Reconnaissance faciale :**

L'identification d'une personne à partir de son visage peut se faire de plusieurs façons, comme capturer une image du visage avec une caméra ou en utilisant les modèles infrarouges du rayonnement thermique du visage.[3] Les caractéristiques considérées comme significatives pour la reconnaissance faciale sont : les yeux, la bouche et la circonférence du visage. Cette technologie est utilisée dans une variété de domaines, du contrôle d'accès physique ou logique à la surveillance, etc.[4]

Figure 1.2 – Reconaissance des visages.[50]

- **Reconnaissance de l'iris :**

Ce type de méthode de reconnaissance utilise l'iris de l'oeil, c'est-à-dire la zone colorée autour de la pupille. Les motifs d'iris, considérés comme uniques, sont obtenus à l'aide d'un système d'imagerie vidéo.

Les appareils de balayage de l'iris sont utilisés depuis de nombreuses années dans des applications d'authentification personnelle. Les systèmes basés sur la reconnaissance de l'iris ont fortement baissé leurs prix et cette tendance devrait se poursuivre.[3]

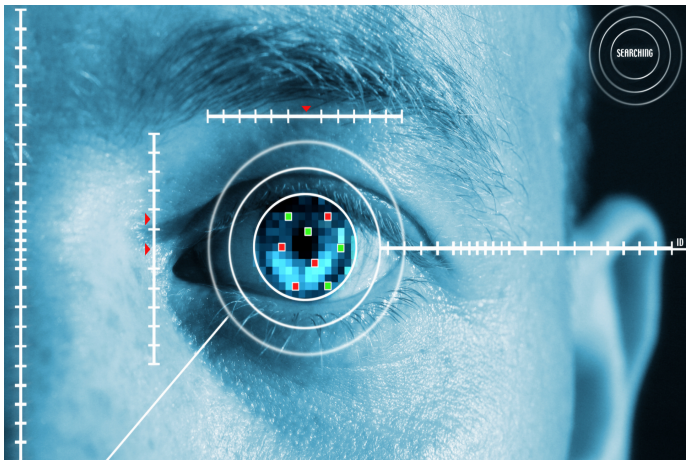


Figure 1.3 – Reconaissance de l'iris.[51]

1.5.2 Les mesures comportementales

Cette modalité est liée au changement de comportement humain au cours du temps, les plus répandues sont :

- **Reconnaissance vocale :**

La reconnaissance vocale est également appelée reconnaissance du locuteur. Au moment de l'inscription, l'utilisateur doit prononcer un mot ou une phrase dans un microphone. Ceci est nécessaire pour acquérir un échantillon de la parole d'un candidat. La reconnaissance du locuteur est l'une des technologies biométriques les mieux étudiées. La vérification est basée sur des informations relatives à la structure anatomique du locuteur, transmises par le spectre d'amplitude.[5]

Figure 1.4 – Reconaissance vocale.[52]

• **Reconnaissance de signature :**

.5cmCette technologie consiste en un stylo et une tablette d'écriture spécialisée, tous deux connectés à un ordinateur pour la comparaison et la vérification des modèles. Une tablette de haute qualité peut capturer les traits comportementaux tels que la vitesse, la pression et le timing pendant la signature. Dans la reconnaissance des signatures, l'accent est mis sur les modèles de comportement dans lesquels la signature est apposée plutôt que sur sa visibilité en termes de graphisme.[5]

Figure 1.5 – Reconaissance des signatures.[53]

1.6 Fonctionnement d'un système biométrique

Un système biométrique est un système de reconnaissance de formes qui fonctionne par l'acquisation des données biométriques à partir d'un individu à reconnaitre, puis en extrayant un ensemble de caractéristiques à partir de ces données, et comparant ces caractéristiques avec la signature dans la base de données. Un système biométrique peut comporter trois processus qui se chargent de réaliser les opérations d'enregistrement et de tests :[7]

• **Enrôlement** : les données biométriques d'une personne sont enregistrées dans la base de données biométrique du système.

• **Vérification** : le système vérifie que l'identité revendiquée appartient à l'utilisateur en comparant ses caractéristiques biométriques à un modèle biométrique stocké (et associé à cette identité)

• **Identification** : le système identifie un individu en comparant sa signature avec les signatures (templates) de tous les utilisateurs dans la base de données.

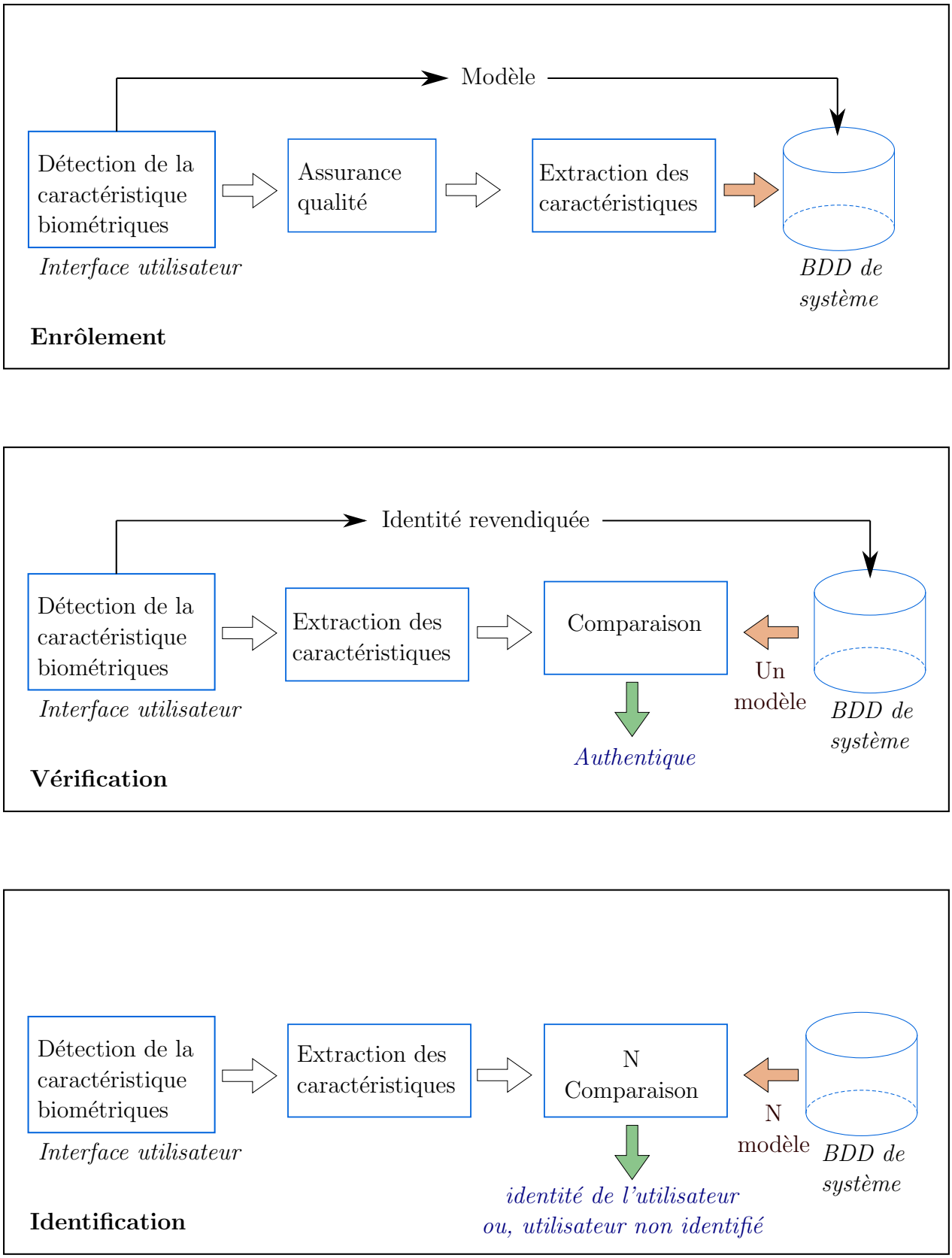


Figure 1.6 – Fonctionnement d'un système biométrique[7].

1.7 Comparaison entre les modalités

Dans le tableau ci-dessous, vous trouverez les résultats de la comparaison des solutions de reconnaissance biométrique :

Identifiant biométrique	Universalité	Distinctif	Permanente	Collectabilité	Performance	Acceptabilité	Circonvention
Empreinte	M	H	H	M	H	M	M
Géométrie de la main	M	M	M	H	M	M	M
L'iris	H	H	H	M	H	F	F
Veine de la main/du doigt	M	M	M	M	M	M	F
Visage	H	F	M	H	F	H	H
Voix	M	F	F	M	F	H	H
Signature	F	F	F	H	F	H	H

Table 1.1 – Comparaison des caractéristiques biométriques couramment utilisées. Les valeurs Hautes, Moyennes et Faibles sont désignées par H, M et F, respectivement.[27]

Cela prouve qu'aucune solution biométrique unimodale n'est capable de fournir un niveau de sécurité suffisamment élevé pour éviter le piratage. C'est pourquoi il faut utiliser une solution multimodale.

1.8 Système biométrique multimodale

Un système de reconnaissance biométrique multimodale nécessite la confirmation d'au moins deux identifiants, ce qui permet d'obtenir un niveau de précision plus élevé.

1.8.1 Définition

La multi-biométrie utilise plus d'une source d'information biométrique dans un cadre unifié afin de résoudre les problèmes rencontrés par la biométrie unimodale conventionnelle. L'approche multi-biométrique vise à améliorer la biométrie en augmentant la

précision et la robustesse aux variations intra-personnelles et aux données bruitées.

La fusion d'informations en biométrie multiple est utilisée pour construire une décision d'identification/vérification basée sur les informations collectées à partir de différentes sources biométriques.

La fusion peut se faire à différents niveaux, ce qui peut être considéré comme un compromis entre la perte d'information et l'intégrabilité.

1.8.2 Avantages des systèmes multibiométriques

Outre l'amélioration de la précision de la correspondance, les autres avantages des systèmes multibiométriques sur les systèmes unibiométriques traditionnels sont énumérés ci-dessous :[10]

1. Les systèmes multibiométriques abordent le problème de la non-universalité (c'est-à-dire la couverture limitée de la population) rencontré par les systèmes unibiométriques. Si le doigt sec d'un sujet l'empêche de s'inscrire dans un système d'empreintes digitales, la disponibilité d'un autre trait biométrique, par exemple le visage, peut faciliter l'inscription du sujet. L'existence d'une autre caractéristique biométrique, peut faciliter l'inclusion de la personne dans le système biométrique.
2. Il devient de plus en plus difficile (ce n'est pas possible) pour un imposteur d'usurper plusieurs caractéristiques biométriques d'une personne légitimement inscrite.
3. Les systèmes multibiométriques permettent également de résoudre efficacement le problème des données bruitées. Lorsque le signal biométrique acquis à partir d'un seul trait est corrompu par le bruit, la disponibilité d'autres traits (moins bruyants) peut contribuer à la détermination fiable de l'identité.
4. Un système multibiométrique peut également être considéré comme un système tolérant aux pannes, qui continue de fonctionner même si certaines données biométriques ne sont pas disponibles, ni fiables en raison d'un dysfonctionnement du capteur ou du logiciel, ou d'une manipulation délibérée de l'utilisateur. La notion de tolérance aux pannes est particulièrement utile dans les systèmes d'authentification à grande échelle impliquant un grand nombre de sujets.

1.8.3 Architecture globale des systèmes multibiométriques

Les systèmes multibiométriques comportent deux phases de processus d'identification/vérification, dont les scores de correspondance sont combinés par une règle de fusion des deux modalités, ce qui nous donne une valeur qui nous aide à prendre une décision.

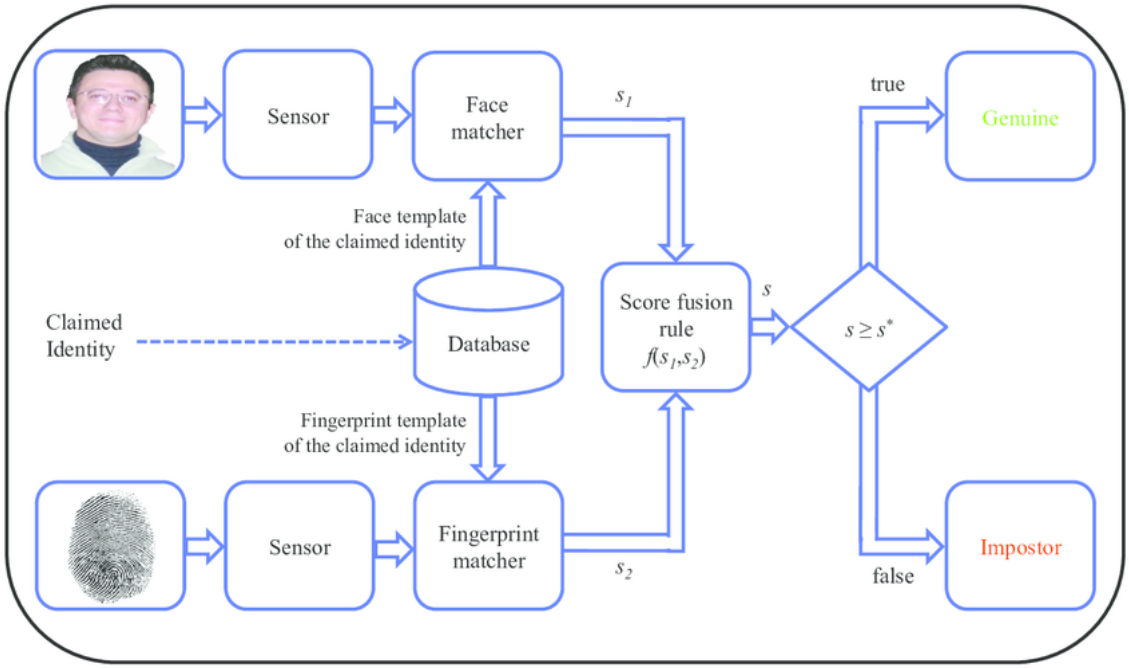


Figure 1.7 – Un système biométrique multimodale composé d'un capteur d'empreintes digitales et d'un capteur de visage.[11]

1.9 Les applications de la biométrie :

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou de déterminer l'identité d'une personne sont concernés,comme les applications bancaires, les lieux de haute sécurité comme les sièges gouvernementaux. On la trouve aussi dans des applications civiles où l'authentification des cartes de crédit, des permis de conduire et des passeports est de plus en plus courante.

Voici une liste non exhaustive des applications pouvant utiliser la biométrie pour contrôler tout accès :[6]

- **Contrôle d'accès physiques aux locaux** : Salle informatique, site sensible (service de recherche, site nucléaire, bases militaires...).

• **Contrôle d'accès logiques aux systèmes d'information** : Lancement du système d'exploitation, accès au réseau informatique, commerce électronique, transaction, tous les logiciels utilisant un mot de passe.

• **Equipements de communication** : Terminaux d'accès à internet, téléphones portables.

• **Machines et Equipements divers** : Coffre fort avec serrure électronique, distributeur automatique de billets, carte de fidélité, etc.

1.10 Conclusion

Dans ce chapitre nous avons introduit les differentes modalités biométriques, les systèmes biométriques ainsi que leurs différentes applications.

Nous avons aussi constaté que les systèmes multi-modale peut atteindre un niveau de sécurité majeur, et en plus les aventages de ces systèmes outre l'augmentation de la sécurité.

Dans le prochain chapitre, nous allons étudier et initier le traitement des images et des empreintes digitales, autant que nous avons besoin d'aller plus loin dans la reconnaissance des visages, et l'identification des empreintes digitales.

Chapitre 2

Généralités sur le traitement d'images et d'empreintes

2.1 Introduction

Le traitement de l'image est un domaine très vaste qui est devenu et devient très important au cours des dernières décennies.

Le traitement d'images numériques désigne toutes les techniques utilisées pour modifier une image numérique afin de l'améliorer ou d'en extraire des informations.

Il n'existe pas deux personnes qui ont exactement les mêmes empreintes digitales. Même des jumeaux identiques, avec un ADN identique, ont des empreintes digitales différentes. Ce caractère unique permet d'utiliser les empreintes digitales de toutes sortes de façons.

2.2 Définition de l'image

Au sens large, une image est un dessin ou une photographie. Elles transmettent de manière concise des informations sur la position, la taille et les relations entre les objets et représentent des informations spatiales que nous pouvons reconnaître comme des objets.[12] L'image est la représentation visuelle de scènes ou de personnes par différents moyens (photo, portrait, peinture, etc.). Elle peut être décrite comme une fonction de luminosité analogique continue I(x, y), définie dans une zone délimitée où x et y sont les coordonnées spatiales d'un point de l'image, et I(x, y) sa fonction d'intensité ou de

couleur.[13]

L'images numériques peuvent se décrire par un ensemble fini de valeurs entières. Si on connait cette suite de valeurs, on peut recréer une copie exacte de l'image d'origine. On peut assimiler cette suite de valeurs entières à un "code génétique" de l'image.

L'image analogique est liée à un support matériel : plaque photo, pigments de peinture et toile, par exemple. Il n'est pas possible de reproduire l'image originale à l'identique. Les copies sont nécessairement dégradées par rapport à l'original.[15]

2.3 L'image numérique

2.3.1 Définition

Il s'agit d'une image dont la surface est divisée en éléments de taille fixe, appelés pixels, ayant chacun une valeur de gris ou de couleur, qui est prise en compte par la partie correspondante de l'image réelle ou calculée à partir d'une description interne de la scène à représenter.[16]

On distingue généralement deux grandes catégories d'images .[14]

Bitmap (appelées aussi images matricielle) : sont des images pixels, c'est-à-dire un ensemble de points (pixels) contenus dans une matrice, chacun ayant une ou plusieurs valeurs décrivant sa couleur.

Vectorielles : sont des représentations de structures géométriques telles qu'un cercle, un rectangle ou un segment de cercle, de rectangle ou de segment. Ils sont représentés par des formules mathématiques (un rectangle est défini par deux points, un cercle par un centre et un rayon, une courbe par plusieurs points et points et une équation).

2.3.2 Types des images numériques

Dans ce qui suit nous donnons trois exemples d'images numériques :[17]

Image binaire : Une image binaire est une matrice rectangulaire dont les éléments sont 0 ou 1. Dans une image de ce type, les zéros sont représentés par les noirs et les uns par les blancs.

Figure 2.1 – Image binaire.

Image en niveau de gris : Dans une image en niveaux de gris que nous allons examiner, la couleur d'un pixel peut prendre des valeurs allant du noir (0) au blanc (255) en passant par un nombre fini d'étapes intermédiaires obtenues par une dégradation du noir. Le pixel est codé en un octet.

Figure 2.2 – Image en niveau de gris.

Image en couleurs : Il est obtenu en combinant les trois couleurs primaires rouge, vert et bleu (RVB). Chaque couleur est codée comme une image en niveaux de gris, avec des valeurs de 0 à 255. Pour R=G=B=0 nous avons un noir pur et pour R=G=B=255 nous avons un blanc pur. La représentation des images en couleur se fait donc soit au moyen d'une image dont la valeur de pixel est une combinaison linéaire des valeurs des trois composantes de couleur, soit au moyen de trois images différentes, dont chacune représente une composante de couleur.

Figure 2.3 – Image en niveau de gris.[21]

2.3.3 Caractéristiques d'image numérique

Comme nous l'avons vu, l'image est un ensemble structuré d'informations parmi ses propriétés nous pouvons spécifier les cractéristiques suivants :

Pixels et son voisinage

Une image numérique se compose d'un ensemble de points appelés pixels. Le pixel est le plus petit composant d'une image. Les pixels voisins sont ceux qui entourent le pixel en question (voir figure ci-dessous). Il s'agit d'une fenêtre de dimension impaire (3*3, 5*5, ...) :[14]

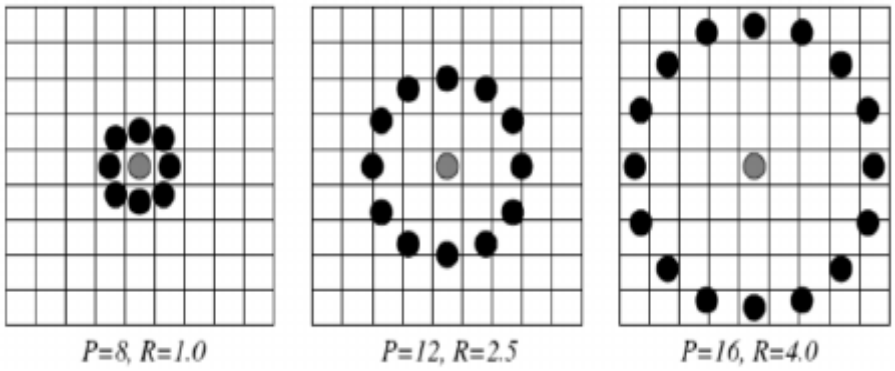


Figure 2.4 – le voisinage d'un pixel.[40]

Histogramme

L'histogramme d'une image est une représentation graphique en 2D dans laquelle X représente les différentes couleurs (par exemple (0-255) pour une image en niveaux de gris) et Y représente le nombre de répétitions de pixels de la même couleur. Dans cette représentation, un point avec les coordonnées (x,y) signifie que nous avons X pixels dans toute l'image qui ont la même couleur. que l'image entière a la même couleur Y.[17]

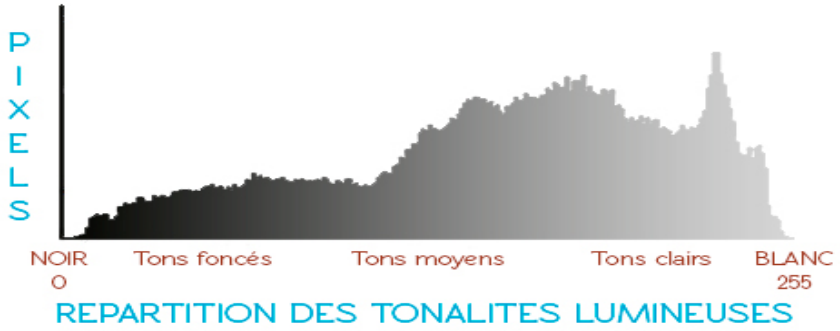


Figure 2.5 – le voisinage d'un pixel.[41]

Dimension

C'est le produit du nombre de lignes multiplié par le nombre de colonnes d'une table superposée sur l'image et dont les cellules sont les pixels de l'image. Nous obtenons le nombre total de pixels qui composent l'image.[18]

Résolution

La résolution d'une image, également appelée définition, est le nombre de pixels par unité de mesure, normalement "ppp" (points par pouce). La haute résolution d'une imprimante, d'un moniteur ou d'un scanner suppose une reproduction fidèle de l'image originale.[18]

Bruit

Le bruit dans une image est considéré comme un phénomène de fluctuations soudaines de l'intensité d'un pixel par rapport à ses voisins. intensité d'un pixel par rapport à ses voisins. Il est généré par l'éclairage de dispositifs de capteurs optiques et électroniques.[18]

Contours

Les contours représentent les limites entre les objets de l'image, ou la limite entre deux pixels dont les valeurs de gris représentent une différence significative.[18]

Luminance

La luminance est le degré de luminosité des pixels. Il est également défini comme le rapport de l'intensité lumineuse d'une surface à la surface apparente de cette surface.[18]

Contraste

Le contraste est l'opposition prononcé entre deux zones d'une image, en particulier entre les zones sombres et claires. Le contraste est défini par les niveaux de luminance de deux zones de l'image. Laissez L1 et L2 être les niveaux de luminance respectifs de deux régions adjacentes. Le contraste est défini par la relation : C = $\left(\frac{L_1-L_2}{L_1+L_2}\right)$ [18]

2.4 Traitement numérique de l'image

L'interprétation d'une image numérique implique l'analyse de l'image et l'extraction d'informations à l'aide de logiciels informatiques. Cette analyse numérique nécessite le traitement de l'image. Ces étapes de traitement sont appelées traitement numérique de l'image.

2.4.1 Définition

Le traitement d'images numériques peut être défini comme le fait de soumettre la représentation numérique d'objets (c'est-à-dire une image) à une série d'opérations afin d'obtenir le résultat souhaité.L'analyse d'images numériques est un processus qui transforme une image numérique en quelque chose d'autre qu'une image numérique, par exemple un ensemble de mesures des objets présents dans l'image. Cependant, le terme "traitement d'images numériques" est utilisé de manière large pour couvrir à la fois le traitement et l'analyse.[12]

Le traitement d'images est également un domaine de recherche important dans les domaines de l'ingénierie et de l'informatique.

Il comprend essentiellement les trois étapes suivantes :

- Importation de l'image avec un scanner optique ou par photographie numérique.
- Analyser et manipuler l'image qui comprend la compression des données et l'amélioration de l'image.
- Un résultat final qui est basé sur l'analyse d'images, ce résultat est considérer comme une sortie et qui peut être modifiée.

2.4.2 Les niveaux de traitement des images numériques

En général, il existe trois niveaux de traitement ou trois types de processus dans le traitement des images numériques, à savoir : les processus de bas, moyen et haut niveau.[20]

Le traitement de bas niveau :

Le traitement de bas niveau comprend des tâches et des opérations primitives telles que le prétraitement de l'image pour réduire le bruit, l'amélioration du contraste, la netteté de l'image, etc.
Dans ce niveau, l'entrée et la sortie sont toutes deux des images.

Exemple : Une vieille image que nous voulons améliorer.

Le traitement de moyen niveau :

Le traitement de moyen niveau implique des tâches telles que la segmentation d'images, la description d'images, la reconnaissance d'objets, etc.
Dans ce niveau, les entrées sont généralement des images mais ses sorties sont généralement des attributs d'image.

Exemple : Une image d'une chaise que nous voulons modifier pour mettre en évidence les bords.

Le traitement de haut niveau :

Le traitement de haut niveau consiste à donner un sens à un groupe d'objets reconnus. Ce processus est normalement associé à la vision par ordinateur.
Dans ce niveau, les entrées sont des attributs d'image la sortie Compréhension des images.
Exemple : Une Photo d'un suspect que nous voulons que l'ordinateur identifie.

2.4.3 Système de traitement d'image

Un système de traitement d'images se compose généralement des unités suivantes :[19]

- Un système d'acquisition et de numérisation qui permet d'effectuer l'échantillonnage et la quantification d'une image.
- Une mémoire de masse pour stocker les images numérisées.
- Un système de visualisation.
- Une unité centrale permettant d'effectuer les différentes opérations de traitement d'images.

Acquisition et numérisation :

La capture d'images est un maillon essentiel de toute chaîne de production et de création d'images. Pour manipuler une image dans un système informatique, il faut d'abord qu'elle soit lisible et manipulable par le système. La transition entre cet objet externe (l'image originale) et son image interne. La représentation interne (dans l'unité de traitement) s'effectue par un procédé de numérisation. Ces systèmes, appelés systèmes optiques, peuvent être classés en deux catégories principales : les caméras numériques et les scanners.

Visualisation :

Tout système de traitement d'images est équipé d'un dispositif d'affichage qui affiche les images. L'utilisation de différents types de rendu permet de convertir le signal numérique en un signal analogique qui peut être vu par l'œil du spectateur.

Pour cela,différents types de supports peuvent être utilisés : moniteur vidéo, plaques photographiques, impression sur papier. Dans tous les cas et pour chaque échantillon d'image numérique, on choisit un nouvel élément d'image ou pixel dont la forme est choisie de manière à reconstruire une image analogique aussi proche que possible Les erreurs introduites lors de la numérisation et de la transmission sont prises en compte.

Traitement numérique des images :

Les techniques de traitement visent à utiliser les informations contenues dans les images pour améliorer la qualité des images et les rendre plus faciles à interpréter, c'est-à-dire améliorer la qualité visuelle de l'image.

2.4.4 Domaines d'application

Le traitement d'images peut être utilisé dans un large éventail de domaines tels que :[26]

- **Robotique - Industrie**
  - Assemblage, Reconnaissance de pièces.
  - Contrôle de qualité.
  - Véhicule autonome.
- **Télé-détection**
  - Météo.
  - Cartographie.
  - Analyse des ressources terrestres.
  - Astronomie.
- **Application militaire**
  - Guidage de missile.
  - Reconnaissance (aérienne, sous-marine, etc.).

- **Imagerie médicale**
  - Tomographie.
  - Comptage (nombre de cellules).
  - Analyse des ressources terrestres.
- **Sécurité**
  - Reconnaissance (d'empreintes, visages, signatures).
  - Détection de mouvement.

2.5 La reconnaissance des visages

2.5.1 Définition

La reconnaissance faciale est un moyen de reconnaître un visage humain grâce à la technologie. Un système de reconnaissance faciale utilise la biométrie pour cartographier les caractéristiques du visage à partir d'une photographie ou d'une vidéo. Il compare ces informations avec une base de données de visages connus pour trouver une correspondance. La reconnaissance faciale peut aider à vérifier l'identité d'une personne, mais elle soulève également des problèmes de confidentialité.[42]

2.5.2 Les caractéristiques du visage utilisées

Les techniques utilisées pour la reconnaissance faciale peuvent être basées sur les caractéristiques (géométriques) ou sur les images (photométriques). La méthode géométrique s'appuie sur la forme et la position des traits du visage. Elle analyse indépendamment chacune des caractéristiques du visage, également appelées points nodaux, et génère ensuite une image complète du visage.

Les algorithmes de détection de visages commencent généralement par rechercher ***les yeux*** humains, l'une des caractéristiques les plus faciles à détecter. L'algorithme peut ensuite tenter de détecter ***les sourcils***, ***la bouche*** et ***le nez***. Lorsque l'algorithme conclut qu'il a trouvé une région du visage, il applique des tests supplémentaires pour confirmer qu'il a effectivement détecté un visage.[43][44]

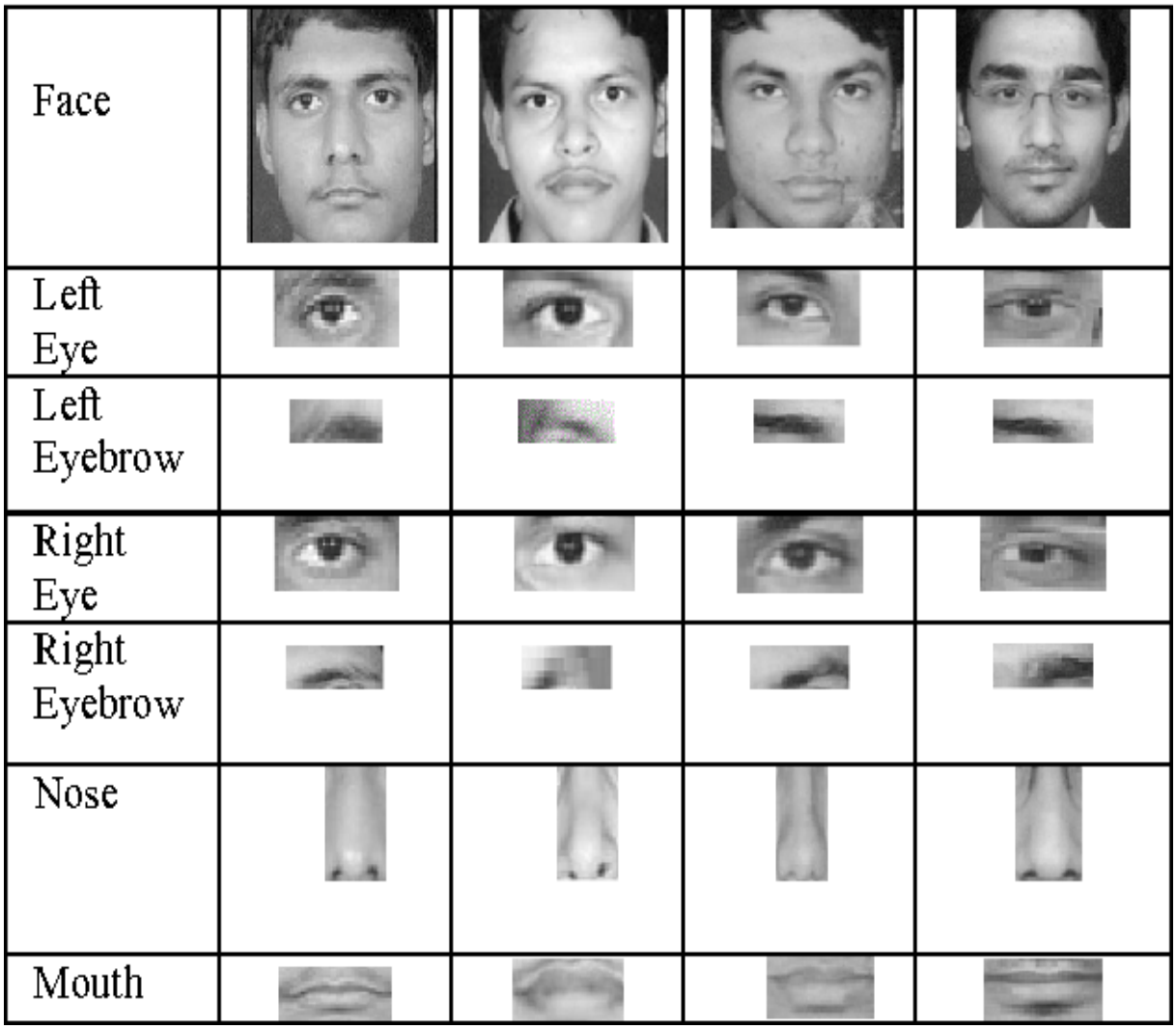


Figure 2.6 – caractéristiques faciale.[45]

2.5.3 Algorithmes de la reconnaissance faciale

En informatique, la reconnaissance des visages consiste essentiellement à reconnaître une personne à partir de son image faciale. Elle est devenue très populaire au cours des deux dernières décennies, principalement en raison des nouvelles méthodes développées et de la haute qualité des vidéos/caméras actuelles.[47]

Il existe différents types d'algorithmes de reconnaissance des visages, par exemple :

- **Eigenfaces (1991)**
- **Local Binary Patterns Histograms (LBPH) (1996)**
- **Fisherfaces (1997)**
- **Scale Invariant Feature Transform (SIFT) (1999)**
- **Speed Up Robust Features (SURF) (2006)**

Chaque méthode a une approche différente pour extraire les informations de l'image et effectuer la correspondance avec l'image d'entrée.

2.6 La méthode Local Binary Patterns Histograms

Le Local Binary Pattern (LBP) est un opérateur de texture simple mais très efficace qui étiquette les pixels d'une image par seuillage du voisinage de chaque pixel et considère le résultat comme un nombre binaire. Il a été décrit pour la première fois en 1994 (LBP) et s'est depuis révélé être une caractéristique puissante pour la classification des textures. Il a également été déterminé que lorsque le LBP est combiné avec le descripteur d'histogrammes de gradients orientés (HOG), il améliore considérablement les performances de détection sur certains ensembles de données.[47]

2.6.1 Entraînement de l'algorithme

Tout d'abord, nous devons entraîner l'algorithme. Pour ce faire, nous devons utiliser un ensemble de données contenant les images faciales des personnes que nous voulons reconnaître. Nous devons également définir un identifiant (il peut s'agir d'un numéro ou du nom de la personne) pour chaque image, afin que l'algorithme utilise ces informations pour reconnaître une image d'entrée et vous donner une sortie. Les images de la même personne doivent avoir le même ID. Avec l'ensemble d'entraînement déjà construit, voyons les étapes de calcul du LBPH.[47]

2.6.2 Application de l'opération LBP

La première étape de calcul du LBPH consiste à créer une image intermédiaire qui décrit mieux l'image originale, en mettant en évidence les caractéristiques du visage. Pour ce faire, l'algorithme utilise le concept de fenêtre glissante, basé sur les paramètres rayon et voisins.

L'opérateur LBP travaille avec les huit voisins d'un pixel, en utilisant la valeur du pixel central comme seuil.

Si un pixel voisin a une valeur de gris plus élevée que le pixel central (ou la même valeur de gris), un un(1) est attribué à ce pixel, sinon il reçoit un zéro(0).

Le code LBP pour le pixel central est alors produit en concaténant les huit uns ou zéros en un code binaire.[47][48]

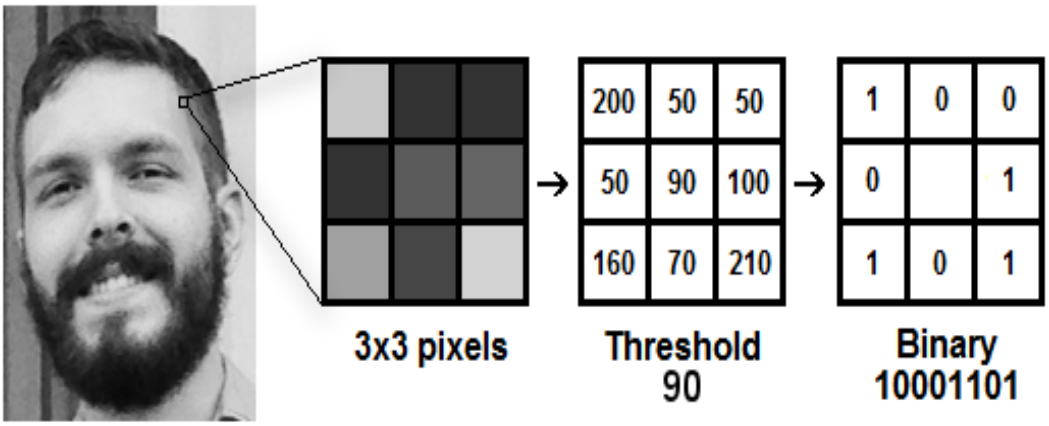


Figure 2.7 – L'opérateur original de LBP.[47]

Plus tard, l'opérateur LBP a été étendu pour utiliser des voisinages de différentes tailles. Dans ce cas, un cercle est de rayon R à partir du pixel central. P points d'échantillonnage sur le bord de ce cercle sont pris et comparés à la valeur du pixel central.

Pour obtenir les valeurs de tous les points d'échantillonnage dans le voisinage pour tout rayon et tout nombre de pixels, une interpolation (bilinéaire) est nécessaire. Pour les voisinages, la notation (P, R) est utilisée pour les voisinages. La figure 2.8 illustre quatre ensembles de voisinage pour différentes valeurs de P et R.[48]

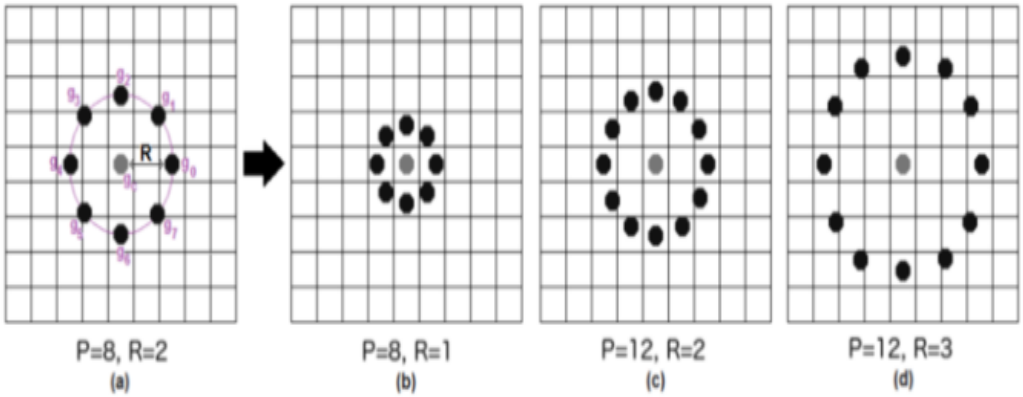


Figure 2.8 – Ensembles de voisins circulaires pour trois valeurs valeurs de P et R.[47]

Cela peut être fait en utilisant l'interpolation bilinéaire. Si un point de données se trouve entre les pixels, il utilise les valeurs des 4 pixels les plus proches (2x2) pour estimer la valeur du nouveau point de données.[47]

2.6.3 Extraction des histogrammes

Une fois que le modèle binaire local pour chaque pixel est calculé, le vecteur de caractéristiques de l'image peut être construit . Pour une représentation efficace du visage, l'image est d'abord divisée en K^2 régions.

Dans la figure 2.9, une image de visage est divisée en $8^2 = 64$ régions. Pour chaque région, un histogramme avec toutes les étiquettes possible est construit. Cela signifie que chaque case de l'histogramme représente un motif et contient le nombre de ses d'apparition dans la région. Le vecteur de caractéristiques est ensuite construit en concaténant les histogrammes régionaux pour en faire un seul grand histogramme.[48]

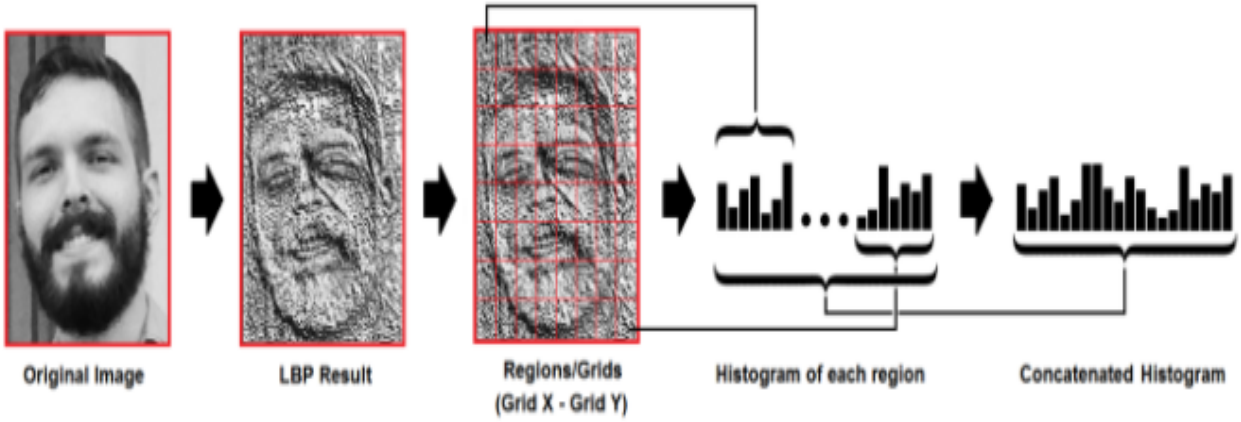


Figure 2.9 – Ensembles de voisins circulaires pour trois valeurs valeurs de P et R.[47]

2.6.4 Exécution de la reconnaissance du visage

Dans cette étape, l'algorithme est déjà entraîné. Chaque histogramme créé est utilisé pour représenter chaque image de l'ensemble de données d'entraînement. Ainsi, étant donné une image d'entrée, nous exécutons à nouveau les étapes pour cette nouvelle image et créons un histogramme qui représente l'image.

- Ainsi, pour trouver l'image qui correspond à l'image d'entrée, il suffit de comparer deux histogrammes et de renvoyer l'image dont l'histogramme est le plus proche.[47]
- Nous pouvons utiliser différentes approches pour comparer les histogrammes (calculer la distance entre deux histogrammes), par exemple : la distance euclidienne, le chi-carré, la valeur absolue, etc. Dans cet exemple, nous pouvons utiliser la distance euclidienne (qui est assez connue) basée sur la formule suivante :[47]

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

Tel que :

D : la distance.

n : le nombre des valeures de l'histogramme.

$hist1_i$: la valeur de l'histogramme de l'image d'entrée.

$hist2_i$: la valeur de l'histogramme de l'image dans la base de données.

- La sortie de l'algorithme est donc l'identifiant de l'image dont l'histogramme est le plus proche. L'algorithme doit également renvoyer la distance calculée, qui peut être utilisée comme une mesure de "confiance". Remarque : ne vous laissez pas tromper par le nom "confiance", car les confidences les plus faibles sont les meilleures car elles signifient que la distance entre les deux histogrammes est plus proche.[47]
- Nous pouvons ensuite utiliser un seuil et la "confiance" pour estimer automatiquement si l'algorithme a reconnu correctement l'image. Nous pouvons supposer que l'algorithme a réussi à reconnaître l'image si la confiance est inférieure au seuil défini.[47]

2.7 L'état de l'art de la reconnaissance des visages

Nous nous concentrons sur la reconnaissance des visages basée sur l'image. Étant donné une image prise par d'un caméra numérique, nous aimerions savoir s'il y a une personne à l'intérieur, où se trouve son visage et qui il/elle est. Pour atteindre cet objectif, nous séparons généralement la procédure de reconnaissance des visages en trois étapes : **Détection des visages**, **Pre-traitement et extraction des caractéristiques** et **Reconnaissance des visages**

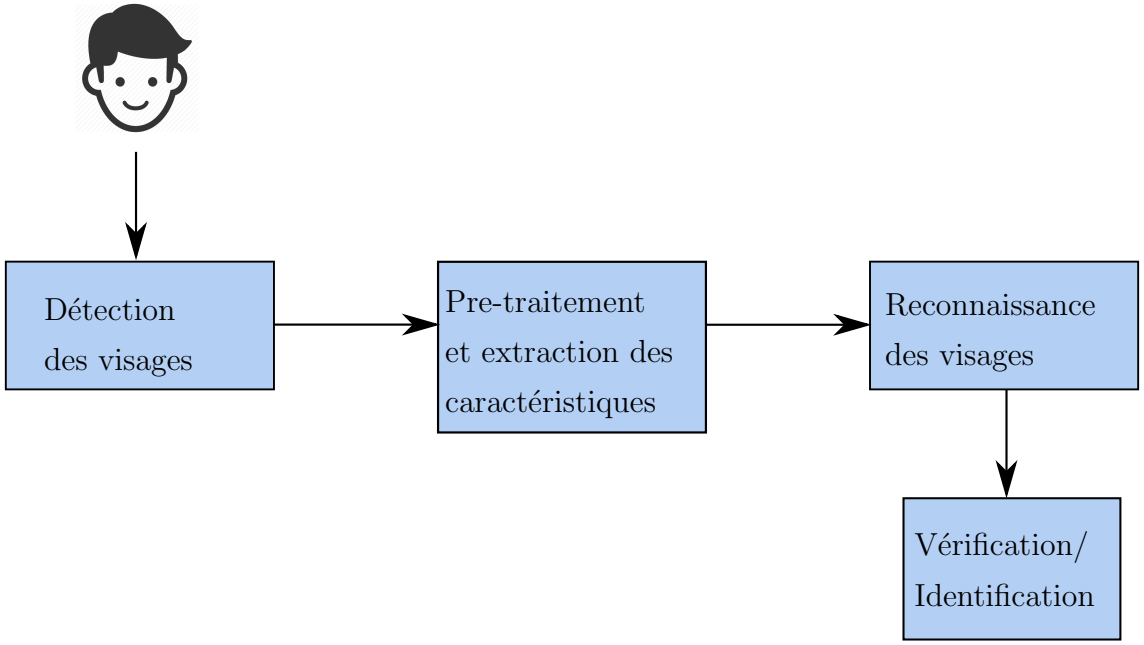


Figure 2.10 – Une structure générale de reconnaissance des visages.[36]

2.7.1 Détection des visages

La fonction principale de cette étape est de déterminer si des visages humains apparaissent dans une image donnée, et où ces visages sont situés. Les résultats attendus de cette étape sont des patchs contenant chaque visage dans l'image d'entrée. Afin de rendre le système de reconnaissance des visages plus robuste et plus facile à concevoir, un alignement des visages est effectué pour justifier les échelles et les orientations de ces patchs.[36]

2.7.2 Pre-traitement et extraction des caractéristiques

Après l'étape de détection des visages, les patchs de visages humains sont extraits des images. L'utilisation directe de ces patchs pour la reconnaissance des visages présente quelques inconvénients. Tout d'abord, chaque patch contient généralement plus de 1000 pixels, ce qui est trop important pour construire un système de reconnaissance robuste. Les patchs de visage peuvent être pris à partir de différents alignements de caméra, avec des expressions du visage et des éclairages différents. Pour pallier ces inconvénients, des extractions de caractéristiques sont effectuées afin de regrouper les informations, de réduire la dimension et de nettoyer le bruit. Après cette étape, un patch de visage est généralement transformé en un vecteur de dimension fixe ou en un ensemble de points de repère et leurs

emplacements correspondants.[36]

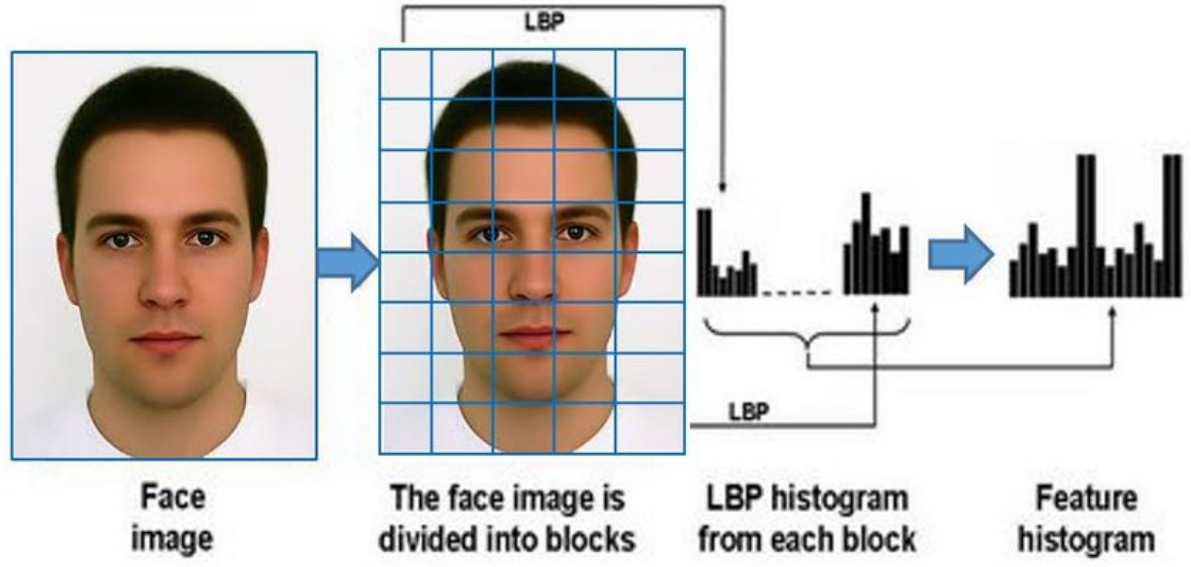


Figure 2.11 – Exctraction des caractéristiques.[46]

2.7.3 Reconnaissance des visages

Après avoir formulé la représentation de chaque visage, la dernière étape consiste à reconnaître les identités de ces visages. Afin de réaliser une reconnaissance automatique, il est nécessaire de construire une base de données de visages. Pour chaque personne, plusieurs images sont prises et leurs caractéristiques sont extraites et stockées dans la base de données. Lorsqu'une image de visage arrive en entrée, nous effectuons la détection des visages et l'extraction des caractéristiques, puis nous comparons ses caractéristiques à chaque classe de visage stockée dans la base de données.[36]

Il existe deux applications générales de la reconnaissance des visages, l'une est appelée **identification** et une autre appelée **vérification**. L'identification de visage signifie qu'étant donné une image de visage, on veut que le système dise qui il/elle est ou l'identification la plus probable ; tandis que Dans la vérification des visages, étant donné une image de visage et une supposition de l'identification, nous voulons que le système dise vrai ou faux sur la supposition.[36]

2.8 Les empreintes digitales

2.8.1 Définition

C'est le modèle formé par les lignes de la peau des doigts. Ces lignes sont uniques et immuables, ne changent pas, gardent toujours la même forme tout au long de la vie (sauf par un accident comme une brûlure), même les jumeaux qui proviennent de la même cellule Les jumeaux qui viennent de la même cellule ont des empreintes très similaires, mais pas les mêmes. Les empreintes digitales sont des motifs uniques, composés d'arêtes de friction (en relief) et de rainures (incrustées), qui apparaissent sur les balles des doigts et des pouces. Les empreintes de mains, d'orteils et de pieds sont également uniques.[22][23]

2.8.2 Classification des empreintes digitales

Les motifs des crêtes de friction sont regroupés en trois types distincts : boucles, verticilles et arcs, chacun avec des variations uniques, selon la forme et la relation des crêtes.[24]

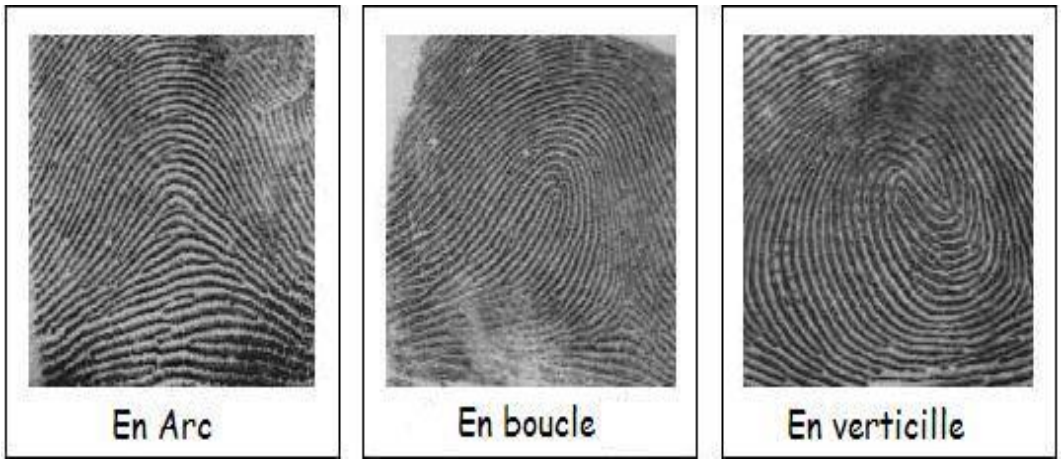


Figure 2.12 – Modèles des empreintes digitales.[39]

Les résultats de l'enquête visant à déterminer quel modèle d'empreinte digitale a disponibilité maximale dans la population humaine sont les suivants : [24]

2.8.3 Caractéristiques

Une empreinte digitale est constituée de nombreuses crêtes et vallées. Le flux continu de motifs noirs est appelé "crête" et le motif blanc entre les crêtes est appelé "vallée". Le

	Modèle	**Pourcentage**
1.	Loop	65%
2.	Whorl	30%
3.	Arch	5%

Table 2.1 – Aperçu des caractéristiques des éléments biométriques.

noyau est le point intérieur, situé en général au milieu de l'empreinte, il sert souvent de point de repère pour situer les autres minuties. Un minutieux est défini comme un point d'intérêt dans une empreinte digitale tel que comme les points de terminaison (fin de la crête) et de bifurcation points (la crête se divise en deux parties). D'autres termes sont également rencontrés : le lac, l'île, le noyau, la vallée [22][24]

Figure 2.13 – Caractéristiques d'une empreinte.[38]

2.9 Reconnaissance des empreintes digitales

Les principaux modules d'un système de vérification d'empreintes digitales sont :

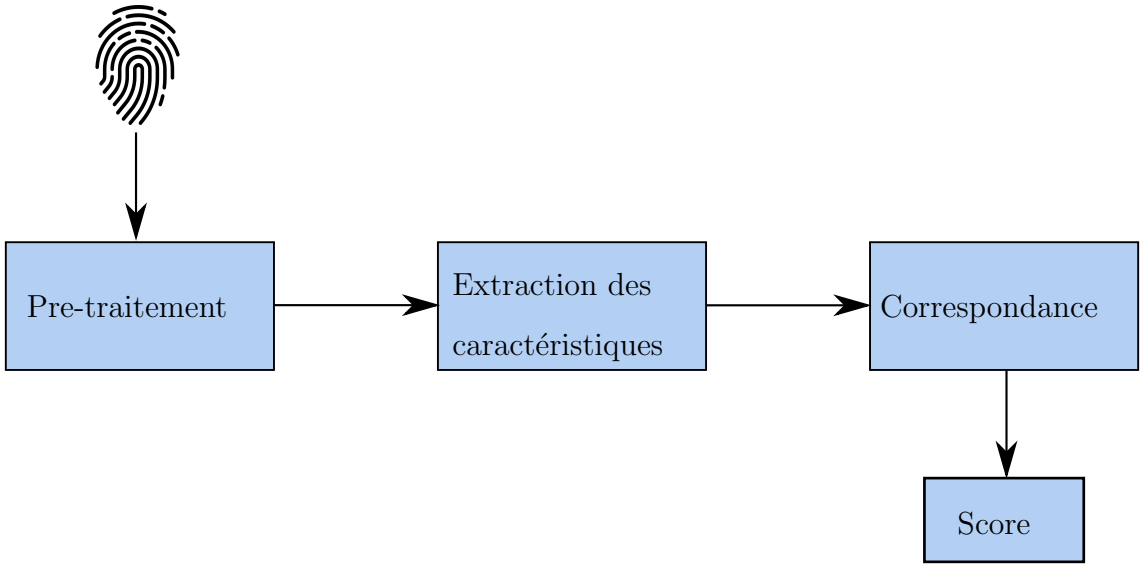


Figure 2.14 – Principaux modules d'un système de vérification des empreintes digitales

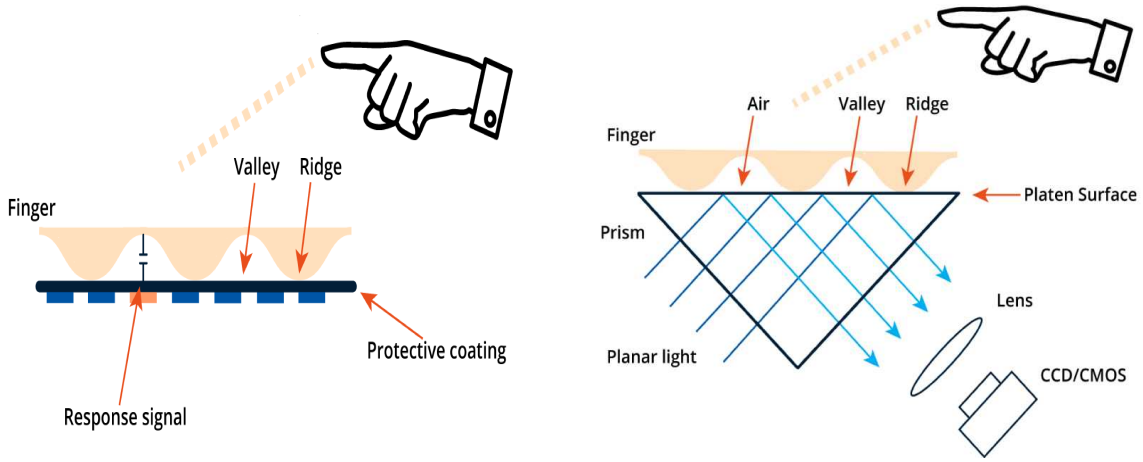
a) **L'aquisation des empreintes digitales** :

Dans laquelle l'empreinte digitale d'un individu est acquise par un capteur d'empreintes digitales pour produire une représentation numérique brute. Il existe trois familles de capteurs électroniques d'empreintes digitales basées sur la technologie de détection :[26][27]

Capteurs en silicone : Ils consistent en une matrice de pixels, chaque pixel étant lui-même un capteur. L'utilisateur place son doigt sur la surface du silicium, et quatre techniques sont généralement utilisées pour convertir l'information (crête/vallée) en un signal électrique : capacitive, thermique, champ électrique et piézo-électrique. D'autre part, les capteurs en silicium sont coûteux, de sorte que la zone de détection des capteurs à semi-conducteurs est généralement petite.[26]

Capteurs optique : Les capteurs optiques d'empreintes digitales offrent une bonne qualité d'image et une grande surface de détection, mais ils ne peuvent pas être miniaturisés, car plus la distance entre le prisme et le capteur d'image est réduite, plus la distorsion optique est introduite dans l'image acquise.[26]

Capteurs Ultrason : Des signaux acoustiques sont envoyés, capturant les signaux d'écho qui sont réfléchis à la surface de l'empreinte digitale. Les signaux acoustiques sont capables de traverser la saleté et l'huile qui peuvent être présentes dans le doigt, donnant ainsi des images de bonne qualité. D'un autre côté, les échographes sont grands et coûteux, et prennent quelques secondes pour acquérir une image.[26]



(a) Capteur en silicone **(b)** Capteur optique

Figure 2.15 – Les capteurs d'empreintes digitales les plus utilisés.[28]

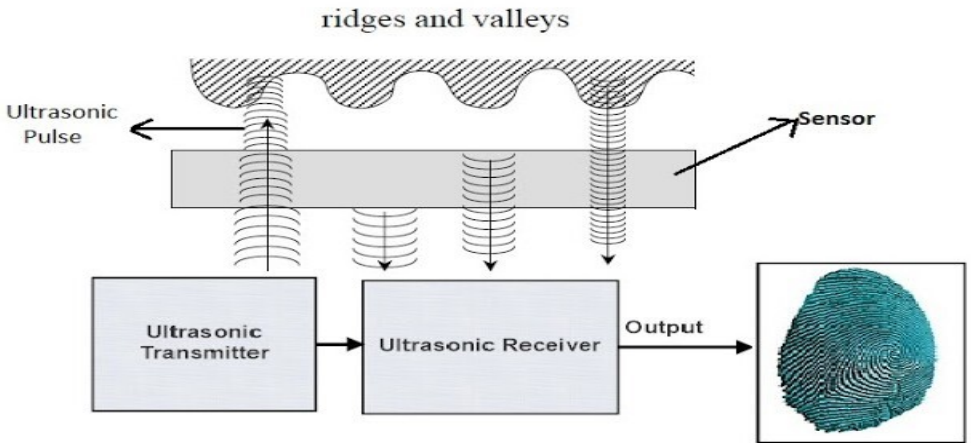


Figure 2.16 – Le capteur ultrason.[29]

b) **Prétraitement et extraction de caractéristiques** : Les algorithmes de reconnaissance d'empreintes digitales sont sensibles à la qualité des images d'empreintes digitales. L'étape de pré-traitement est un pré-traitement nécessaire avant d'exécuter les étapes suivantes. Le prétraitement consiste à lisser, à améliorer le contraste, à filtrer le domaine spatial/fréquence, etc.

La plupart des systèmes de reconnaissance des empreintes digitales utilisent des minuties comme caractéristiques des empreintes digitales. La plupart des systèmes de reconnaissance d'empreintes digitales utilisent les détails de l'empreinte.

Un extracteur minutia recherche les extrémités des crêtes et des branches dans les empreintes digitales. Si les crêtes sont bien déterminées, l'extraction minutieuse est une tâche relativement simple.

Cependant, dans la pratique, il n'est pas toujours possible d'obtenir une carte de crête parfaite. Par conséquent, la performance des algorithmes actuellement disponibles pour l'extraction minutiae dépend fortement de la qualité des images des empreintes digitales.[33]

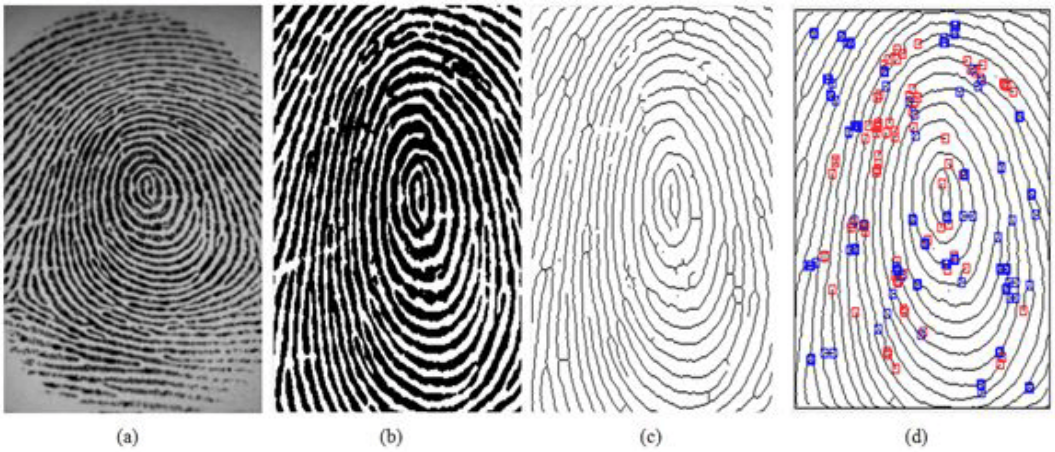


Figure 2.17 – Étapes de l'extraction des caractéristiques d'une empreinte digitale.[37]

(a) - Exemple d'image d'empreinte digitale.

(b) - Après le prétraitement de l'image de l'empreinte digitale en (a).

(c) - Après (b) l'opération morphologique de l'empreinte digitale dans (a).

(d) - L'extraction des minutiae de l'empreinte digitale.

c) **Mise en correspondance** : L'identification automatique basée sur les empreintes digitales nécessite de recouper les empreintes digitales d'entrée avec un grand nombre d'empreintes digitales dans une base de données (par exemple, la base de données du FBI contient plus de 200 millions).Afin de réduire le temps et la complexité de la recherche, il est souhaitable de classer ces empreintes digitales de manière précise et cohérente, de sorte que l'empreinte digitale d'entrée n'ait à être comparée qu'à un sous-ensemble des empreintes digitales de la base de données.[33][34]

Les modèles des utilisateurs autorisés du système biométrique, également appelés clients, sont généralement stockés dans une base de données. Les clients peuvent revendiquer une identité et leurs empreintes digitales peuvent être comparées aux empreintes digitales stockées.

2.10 Conclusion

Dans ce chapitre nous avons définit c'est quoi une image numérique, une empreinte et leur types ainsi que leur caractéristiques. On a donné une définition des systèmes de traitement d'images et leur domaines d'application.

Dans le prochain chapitre, nous parlerons de la conception et de la mise en œuvre de notre application ainsi que du matériel utilisé pour réaliser ce projet.

Chapitre 3

Analyse et réalisation

3.1 Introduction

Dans le cadre d'accroitre la sécurité et améliorer les systèmes de suivi dans différentes entreprises, et après l'analyse des besoins on a décidé que notre travail consistera a implémenter une approche de suivi assistée par la reconnainsance faciale.

l'application est développé avec python en utilisant différentes librairies pour la détéction des images : openCV , LBPH

Ce dernier chapitre est consacré aussi l'implementation et la réalisation de notre application.

Une application simple d'utilisation, conçu pour faciliter l'ajout des employés de l'entreprise ainsi que l'ajout des images des visages pour la reconnaisaance faciale.

l'identification via empreinte est une perspective très importante pour l'amélioration de rendement de notre système.

L'evaluation de système de détection des visages se fait d'une manière générale comme suit :

- Capture de l'image depuis la caméra de surveuillance
- Traitemnt LBPH et extraction des visages
- Comparaison des visages extraits avec ceux qui sont enregistrés dans la base de données
- Avoir le resultat de comparaison et l'affichage

3.2 Architecture de notre système

Dans notre projet, nous voulons concevoir et réaliser un système de contrôle d'accès intelligent basé sur la reconnaissance faciale standard, simple d'utilisation et facilement configurable pour s'adapter aux différents besoins des entreprises pour accroitre leur niveau de sécurité.

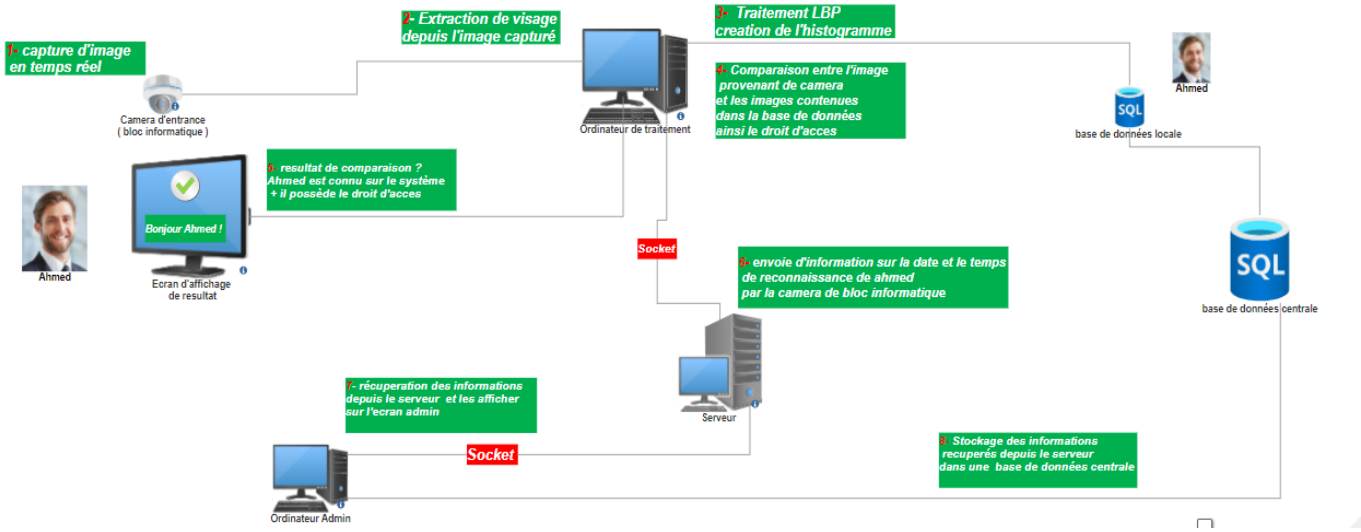


Figure 3.1 – Architecture de notre système de contrôle d'accès intelligent

3.2.1 Diagramme de classes

Apres une analyse des besoins pour notre systeme, ce diagramme de classe peut élaborer comment le système va être implementé au sein d'une entreprise quelconque.

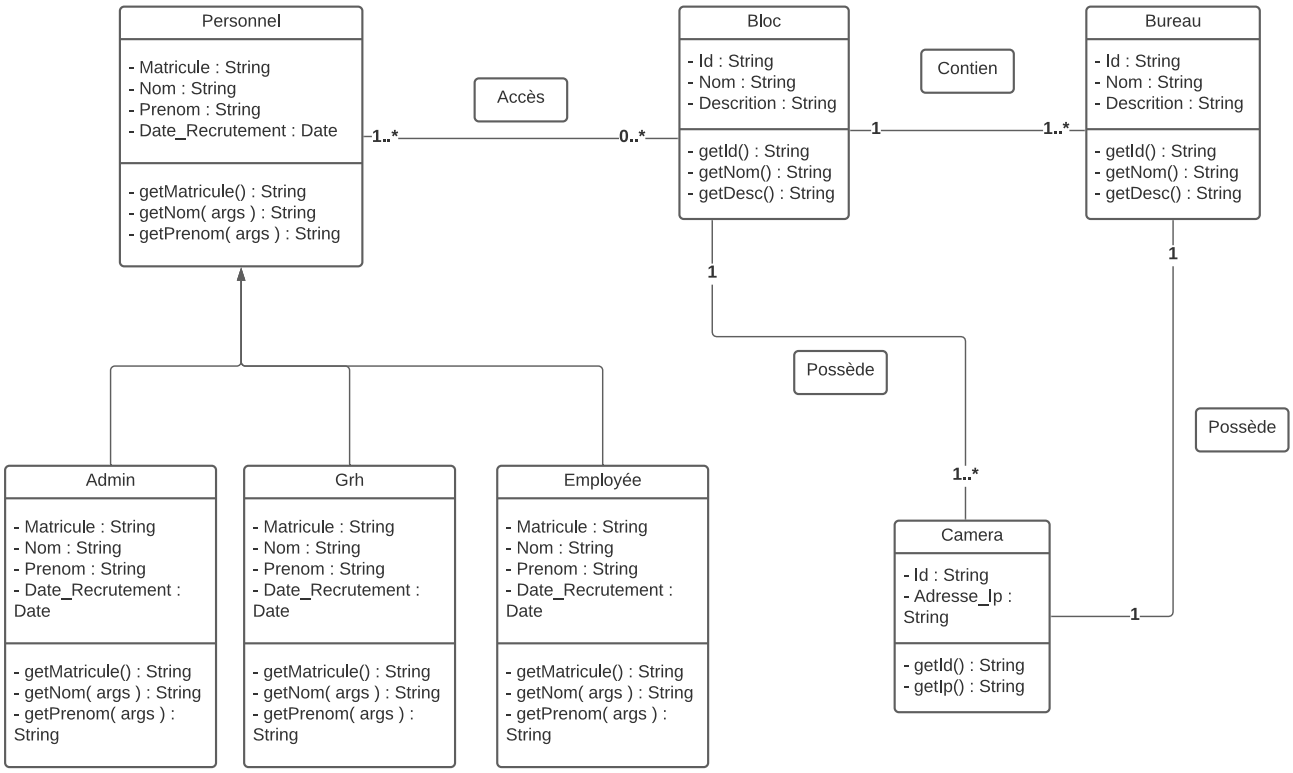


Figure 3.2 – Principaux modules d'un système de vérification des empreintes digitales

Depuis ce diagramme de classe on deduit que :

* l'administrateur, éditeur et employé sont de personnel de l'entreprise
* Chaque employé peut acceder a plusieurs blocs, selon les droits d'accès définis par l'administrateur. (dans le cas ou y a un visiteur, ce dernier aura pas l'acces au blocs, cela justifie la cardinalité 0..*)
* chaque bloc possède une ou plusieurs caméras.

par consequent un administrateur est un employé qui possède les droit d'accès à tous les blocs.

3.2.2 Diagramme de cas d'utilisation

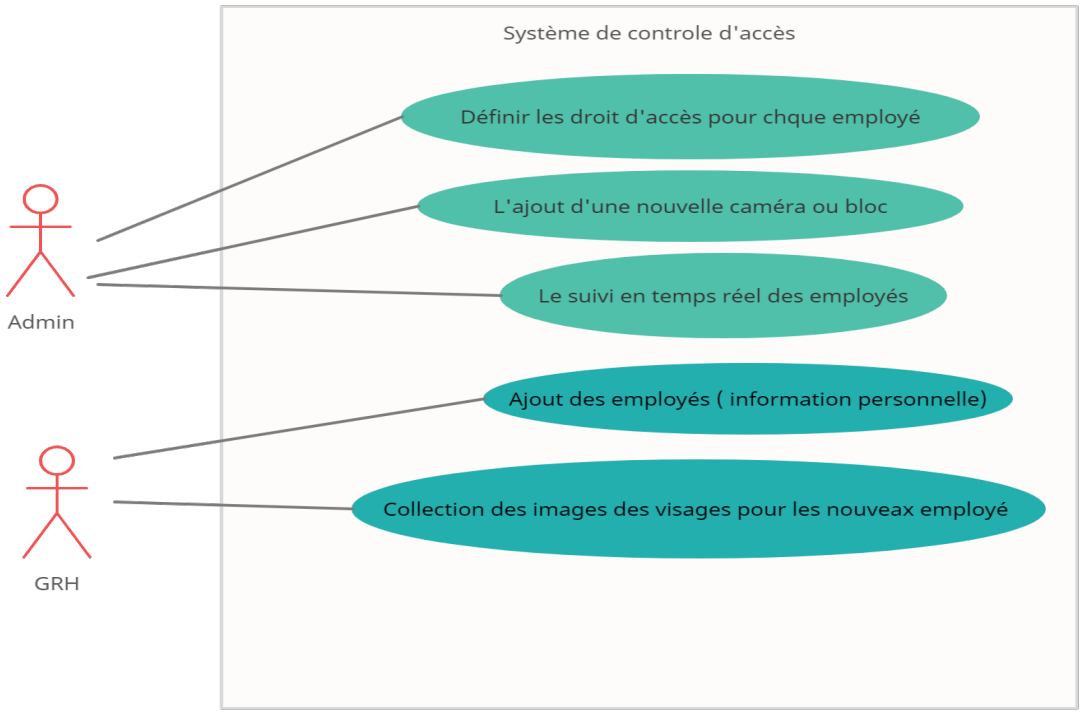


Figure 3.3 – Diagramme de cas d'utilisation pour le système de controle d'accès intelligent

* l'administrateur va avoir un tableau de board sur lequel il peut définir les droit d'accès de chaque employé ainsi que le suivi en temps réel de n'importe quel employé en cas de besoin. exemple : un employé E est en train d'accèder a un bloc B (camera en temps réel)
* l'editeur sert a collecter les informations nécessaires pour alimenter le système de controle d'accès incluant les images des visages de chaque employé

3.2.3 Flux d'information

L'elaboration de diagramme de flux d'information se fait comme suit :

Phase d'entrainement :

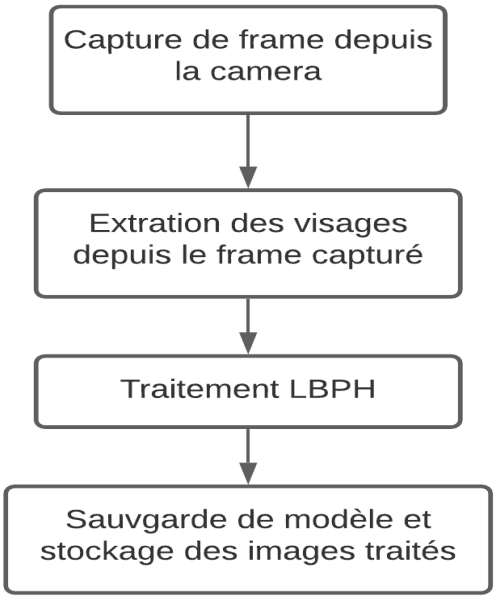


Figure 3.4 – Flux d'information lors de la phase d'entrainement.

– Extraction des images depuis la camera a chaque unité de temps

– Extraction des visages depuis les images capturées pour forger un jeu d'images d'entrainement

– Classification LBP (local binary pattern) et la création de modèle

– Sauvgarde de modèle et stockage des images dans les contenaires de visages dans la base de données

Phase de test :

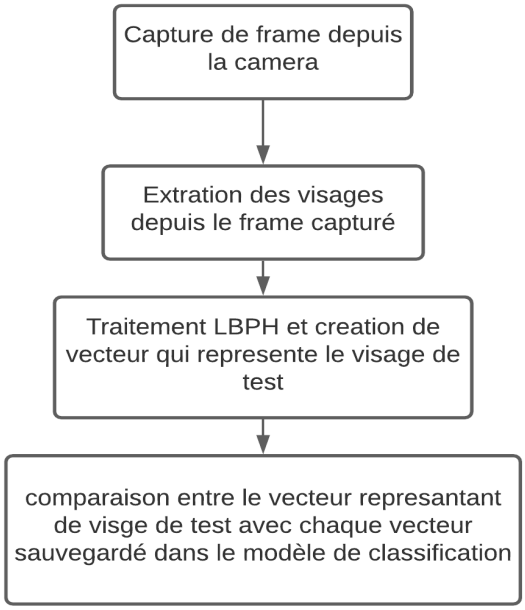


Figure 3.5 – Flux d'information lors de la phase de test.

– Extraction des visages depuis le frame de la camera

– Creation d'un vecteur représantant le visage de test

– Comparaison entre le vecteur généré et chaque vecteur du modèle déjà créé

– Si il y a une correspondance alors les visages sont identiques

3.2.4 Architeture globale

L'application de reconnaissance faciale sera utilisée par 3 type d'utilsateur dans l'entreprise : (Admin , gestionnaire de ressource humaines , employé / visiteur)

- Gestionnaire de ressources humaines :

  il a pour objectif d'ajouter les nouveaux employés au système et de créer les modèle de reconnaissance faciale correspondant à chaque nouveau employé qui seront ensuite utilisés par notre système pour l'identification.

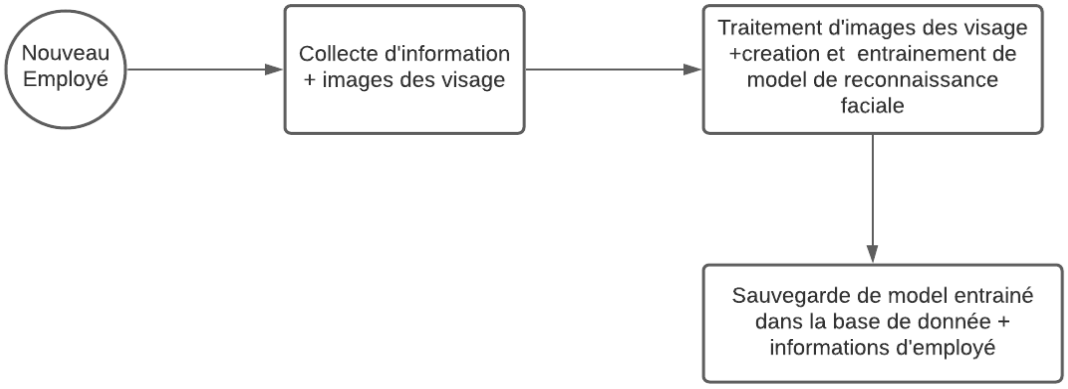


Figure 3.6 – Processus d'enregistrement de nouveaux employés

- Admin :

  son role est de définir les droit d'accès pour le personnel de l'enrtreprise, ainsi le suivi de ces derniers

  exemple : un employé dans le bloc de parking il a le droit d'acceder au bloc GRH mais pas l'administration .

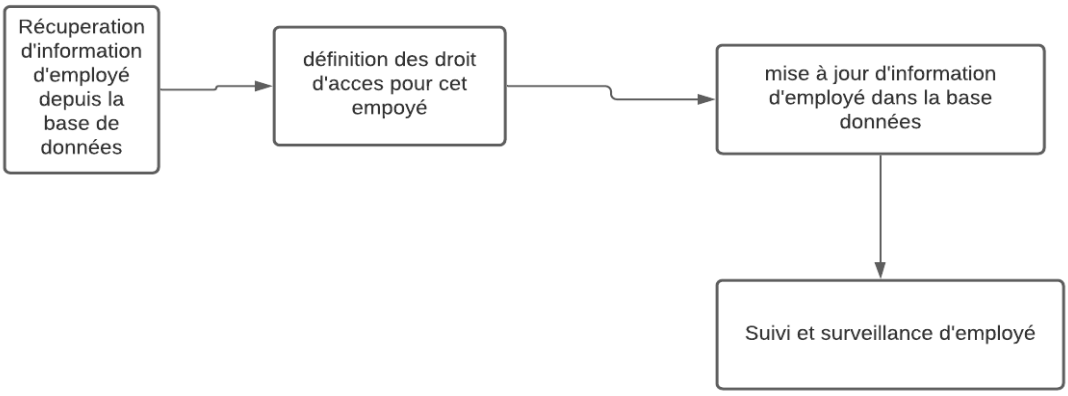


Figure 3.7 – Processus de définition des droits d'acces pour l'employé

- Employé /visiteur :

  c'est l'entité essentiel dans la phase de la reconnaissance faciale. l'employé doit se presenter devant une camera qui va capter son visage puis le comparer a chaque visage dans notre jeu d'entrainement si elle existe une correspondance ça va retourner un resultat positif, négatif sinon.

  Le système de sécurité va agir selon le resultat retourné lors de la reconnaissance

faciale, exemple (ouvrir une porte si la personne est reconnue et si elle a le droit d'acces prédifini)

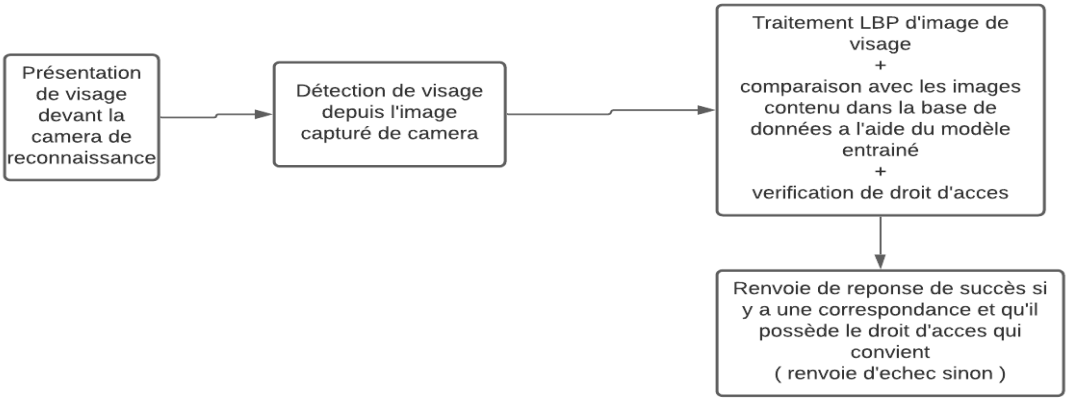


Figure 3.8 – Processus de controle d'acces d'un employé

PS : un administateur c'est un employé qui possède tout les droits d'acces a n'importe quel site de l'entreprise .

L'architecture d'un système de controle d'accès assisté par reconnaissance faciale tourne autour d'un modèle distribué d'un réseau des composants interconnectés pour faciliter la distribution d'information entre différentes entitées

3.3 Espace de travail

3.3.1 Materiel

On a utilisé deux ordinateurs pour avoir une simple comparaison entre les resultats obtenus lors d'evaluation sur chacun des ordinateurs :

- Ordinateur 1 : processeur Intel quad core, 4 thread en parallele avec une fréquence 2.16 Ghz, 8 GB RAM.
- Ordinateur 2 : processeur Intel core i5, 4 thread en parallele avec une fréquence 2.30 Ghz, 8 GB RAM.

  En comparant les deux résultats obtenus on deduit que :

  – Le temps pris pour la détection des visages sur l'ordinateur 2 est inférieur par rapport à l'ordinateur 1.

– La qualité d'image de la camera de l'ordinateur joue un role important pour avoir une meilleure précision

3.3.2 Logiciel

Python

Language de programmation qui sert a donner non seulement une facilité lors d'ecriture de code grace a sa syntaxe simplifié, python est dédié pour le domaine de machine learning grace a des bibiliothèque prédéfinies.

openCV

OpenCV (Open Source Computer Vision Library) est une bibliothèque open source de vision par ordinateur et d'apprentissage automatique.

OpenCV a été construit pour fournir une infrastructure commune pour les applications de vision par ordinateur et pour accélérer l'utilisation de la perception artificielle dans les produits commerciaux. Étant un produit sous licence BSD, OpenCV permet aux entreprises d'utiliser et de modifier facilement le code.

La bibliothèque compte plus de 2500 algorithmes optimisés, ce qui inclut un ensemble complet d'algorithmes de vision par ordinateur et d'apprentissage automatique classiques et de pointe. Ces algorithmes peuvent être utilisés pour détecter et reconnaître des visages, identifier des objets, classer des actions humaines dans des vidéos, suivre les mouvements de la caméra, suivre des objets en mouvement, etc.[30]

Pycharm

Pycharm est un IDE (Integrated Developpement Environement) qui offre la saisie intelligente la mise en évidence des erreur et des correctifs rapides.

Pycharm offre aussi une console python qui aide au déploiement de code écrit

PyQT designer

Qt Designer est l'outil Qt permettant de concevoir et de réaliser des interfaces graphiques utilisateur (GUI) avec des widgets Qt. Vous pouvez composer et personnaliser vos

fenêtres ou vos boîtes de dialogue de manière WYSIWYG (what-you-see-is-what-you-get), et les tester en utilisant différents styles et résolutions.[31]

SQLite

SQLite est une bibliothèque en langage C qui implémente un moteur de base de données SQL petit, rapide, autonome, très fiable et complet.

SQLite est le moteur de base de données le plus utilisé dans le monde.

3.4 Interface graphique

Notre application possède 4 interfaces simples selon le role d'utilisateur dans l'entreprise .

- interface pour connexion / login

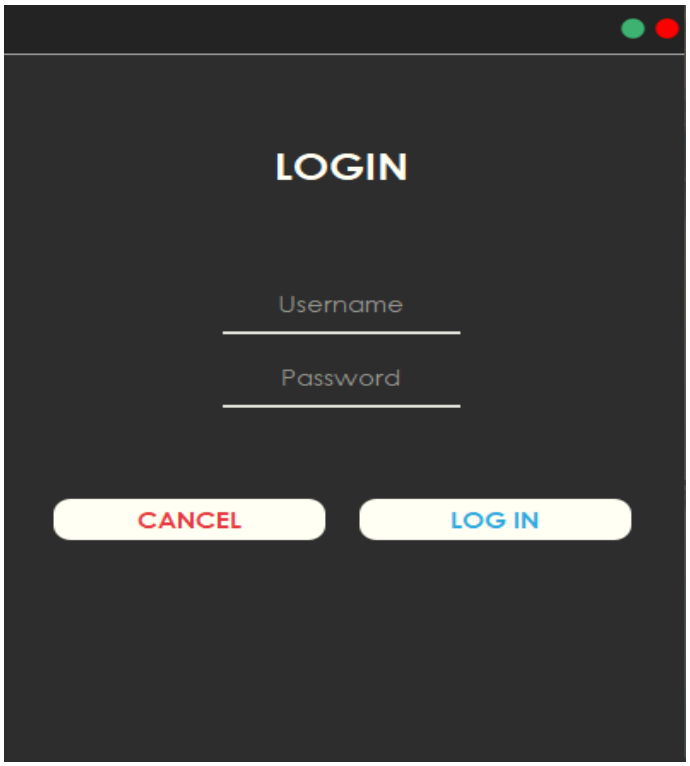


Figure 3.9 – interface de connexion à l'application.

une simple interface là ou on peut definir le type d'acces a l'application lors de connexion : que ce soit (admin , editeur , ou simple utilisateur)

- interface admin : ou l'administrateur pour définir les droit d'accès

Figure 3.10 – interface de l'administrateur.

l'administrateur aura l'interface qui sert a lui donner la main pour manipuler les droit d'acces aux differents sites pour chaque employé, comme il a une partie où il peut recevoir les notifications de la part des cameras de reconnaissance pour un but de suivi.(figure 3.10)

- interface GRH : exemple d'un gestionnaire de ressources humaines où il peut enregistrer un nouveau employé ainsi ses images de visage

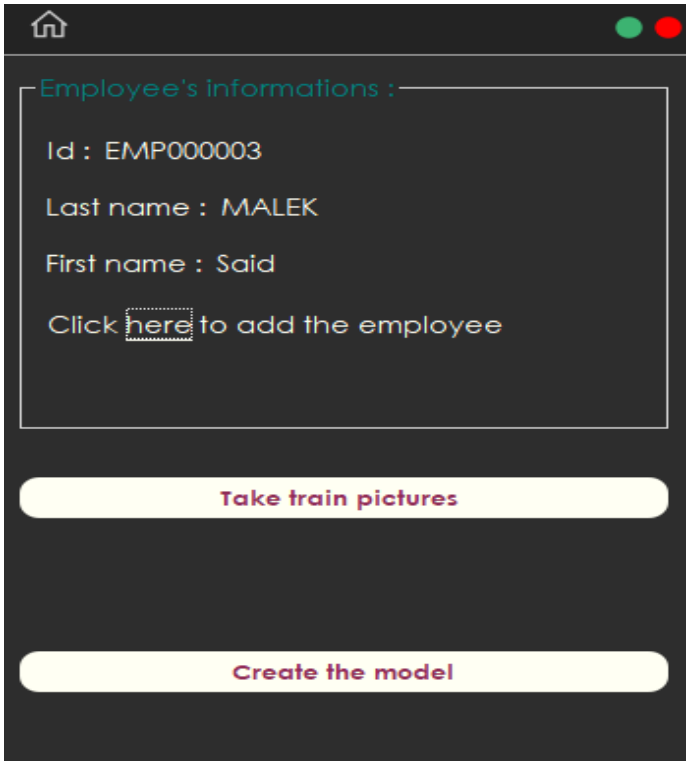


Figure 3.11 – Interface de l'éditeur ou gestionnaire de resources humaines.

Cette interface est dédiée pour le gestionnaire des ressources humaines dans l'entreprise qui veut implementer notre système, incluant les informations necessaires d'employé ainsi que la possibilité de capturer des images du visage de l'employé pour forger un jeu d'image d'entrainement, l'entrainement du modèle créé ainsi la sauvgarde de ce dernier dans la base de données.(figure 3.11)

- interface employé/visiteur : pour afficher le resultat de la reconnaissance

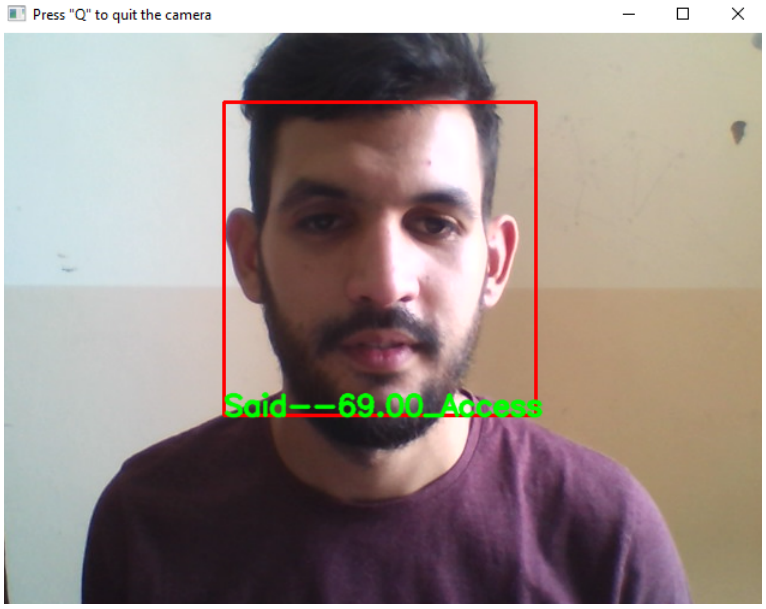


Figure 3.12 – Interface de test en cas d'accès autorisé .

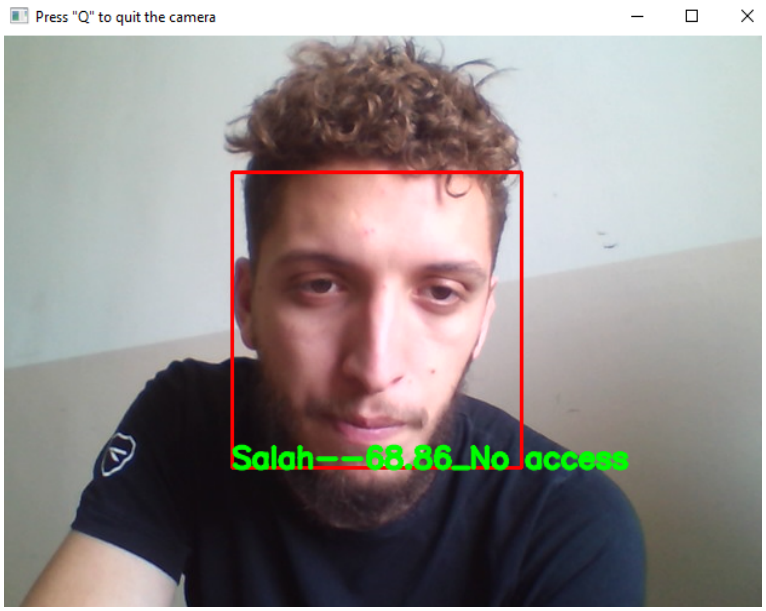


Figure 3.13 – Interface de test en cas d'accès non autorisé .

lors de la reconnaisance faciale d'un employé en entrée, il doit se presenter devant la camera pendant une unité de temps 4 à 8 secondes, le système va le reconnaitre, il va extraire les droit d'acces pour voir si il a la possibilté d'acceder au site contenaire de caméra.

PS : la qualité d'images d'entrainement ainsi de test joue un role important pour avoir une bonne précision (webcam dans notre cas)

Conclusion générale et perspectives

Ce travail rentre dans le cadre du projet de fin d'etdue pour l'obtention du diplôme de master en informatique dans la spécialité Ingénierie des Systèmes d'Information et Logiciel. Ce mémoire représente une concrétisation de cinq années d'études.

L'objectif de notre travail a consisté dans le développement d'un système de controle d'accès intelligent basé sur la reconnaissance faciale. Ce projet inclut toutes les étapes de la conception et de réalisation de notre application par le formalisme UML et la mise en œuvre des bases de données avec le SGBD SQLite. Ensuite l'implémentation des requêtes SQL pour la manipulation des données et enfin l'exécution de l'application sous l'environnement de programmation pycharm qui nous a permis de développer et de tester le système.

Ceci nous a permis d'avoir une bonne expérience et améliorer nos connaissances concernant le domaine de machine learning et aussi ça nous a permet de nous faire une idée sur le domaine professionnel.

La réalisation de ce système n'est pas bornée car y aura des perspectives dans les versions prochaines comme l'assistance par identification des empreintes, assistance par reconnaissance de voix, a long terme y aura une assistance par identification de l'iris .

Bibliographie

[1] **Guardware Systems Ltd., Fingerprint Recognition : History of Fingerprinting** [en ligne], https ://www.biometrie-online.net/images/stories/dossiers/technique/empreintes/History_of_Fingerprinting.pdf (dernière consultation 28 Avr 2021)

[2] **La biométrie, au service de l'identification et l'authentification.** [en ligne], https ://www.thalesgroup.com (dernière consultation 29 Avr 2021)

[3] **M. Sayed, F. Jradi** Biometrics : Effectiveness and Applications within the Blended Learning Environment- Vol.5, No.5, 2014

[4] **S. BOUDJELAL**, "Détection et identification de personne par méthode biométrique ", Mémoire de magister en électronique, Université de Tizi Ouzou, 2014

[5] **K. Saeed**, New Directions in Behavioral Biometrics, 2017.

[6] **S. Akrouf**, "Une Approche Multimodale pour l'Identification du Locuteur", Thèse de doctorat, université Ferhat Abbas Sétif, 2011.

[7] **N. Damer**, Application-driven Advances in Multi-biometric Fusion, [Ph.D. Thesis] - 2018

[8] **Dan M. Bowers**, Physical Access Control, 83-05-10.1

[9] **Why you should use multimodal biometric verification** [en ligne], https ://towardsdatascience.com (dernière consultation 15 MAI 2021)

[10] **Arun Ross**, An introduction to multibiometrics, West Virginia University, Morgantown, WV 26506 USA

[11] **A multimodal biometric system made up of a fingerprint and a face sensor** [en ligne], https ://www.researchgate.net (dernière consultation 23 MAI 2021)

[12] **unit 10 characteristics of digital collection remote sensing images** [En ligne], http ://www.egyankosh.ac.in/bitstream/123456789/39539/1/Unit-10.pdf (dernière consultation 20 MAI2021)

[13] **BENAMROUZ S, KETTANE S.** Segmentation d'image par les méthodes adaptives basées sur les matrices de cooccurrences. Université d'UMMTO, 2009

[14] **HOUASSINE C.** Segmentation d'images par une approche biomimétique hybride ,memoire de magister, universite m'hamed bougara- BOUMERDES 2012

[15] **Image numérique et image analogique.** [En ligne] docplayer.fr (dernière consultation 20 MAI 2021)

[16] **AKROUR Nawal,CHABI Lilia .** bioseg :une plateforme évolutive pour le développement d'approches biomimétique en segmentation d'image. E.S.I, Algérie.2008.2009

[17] **BENRAMDENE S.** utilisation des systemes d'informations geographiques pour la mesure de la surface, MEMOIRE MASTER EN Télécommunication, universite abou bekr belkaid tlemcen 2016

[18] **BENAMROUZ S. KETTANE S.** Segmentation d'images par méthode adaptative basée sur les matrices de cooccurrences. Memoire de master. Université Mouloud MAAMRI de Tizi-ouzou 2009

[19] **BENFRIHA S. HAMEL A.** Segmentation d'image par Coopération région-contours. Mémoire Master Professionnel Université KasdiMerbah-Ouargla 2016.

[20] **Image processing levels** [En ligne] https ://www.asquero.com (dernière consultation 22 MAI 2021)

[21] **Le pingouin** [En ligne] https ://www.jaitoutcompris.com (dernière consultation 25 MAI 2021)

[22] **MATALLAH A. BABAHADJ A.**
Système de controle d'acces physique. Mémoire Master 2017.

[23] **Principles of Fingerprint Analysis.** [En ligne] http ://www.forensicsciencesimplified.org (dernière consultation 25 MAI 2021)

[24] **Chandana . Surendra Y . Mathuria M .**
Fingerprint Recognition based on Minutiae Information. Volume 120 – No.10, June 2015

[25] **Understanding fingerprints** [En ligne] http ://www.abovetopsecret.com (dernière consultation 25 MAI 2021)

[26] **Petrovska-Delacrétaz D. Chollet G. Dorizzi B.** Guide to Biometric Reference Systems and Performance Evaluation

[27] **Maltoni D. Maio D. Jain A. Prabhakar S.** Handbook of Fingerprint Recognition. Springer, 1040 New York (2003)

[28] **The benefits of fingerprint identification** [En ligne] https ://www.argustrueid.com (dernière consultation 2 JUN 2021)

[29] **Fingerprint sensors are going ultrasonic** [En ligne] https ://www.3dincites.com (dernière consultation 2 JUN 2021)

[30] **openCV définition** [En ligne]
https ://opencv.org/about/ (17 JUN 2021)

[31] **PyQT designer définition** [En ligne]
https ://doc.qt.io/qt-5/qtdesigner-manual.html (17 JUN 2021)

[32] **Algorithme LBPH, C'est Quoi ?** [En ligne]
https ://iq.opengenus.org/lbph-algorithm-for-face-recognition/ (19 JUN 2021)

[33] **BENCHENNANE I.** Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus. Thèse de doctorat 2016.

[34] **Detect the guilty, protect the innocent** [En ligne]
https ://www.thalesgroup.com (dernière consultation 25 JUN 2021)

[35] **INTERNATIONAL ORGANIZATION FOR STANDARDIZATION** ISO/IEC 2382-37 :2012 : Information technology Vocabulary Part 37 : Biometrics. Standard, ISO/IEC TC JTC1 SC37 Biometrics, Dec. 2012.

[36] **CHAO W-L.** Face Recognition, GICE, National Taiwan University

[37] **Geetha S. Mariluthu K. Hafizul Islam SK. Mohammad MH.** A Lightweight Machine Learning-based Authentication Framework for Smart IoT Devices. Article in Information Sciences · August 2019

[38] **La biométrie : un nouveau moyen de sécuriser et rendre plus rapide nos paiements ?** [En ligne]
http ://depgbcreteil.blogspot.com (dernière consultation 02 JUL 2021)

[39] **Analyse d'une empreinte digitale** [En ligne]
https ://tpedoisneau.wixsite.com (dernière consultation 02 JUL 2021)

[40] **Nombre P de pixels en fonction du rayon R du voisinage considéré.** [En ligne]
https ://www.researchgate.net/ (dernière consultation 23 JUL 2021)

[41] **histogramme-photo** [En ligne]
https ://apprendre-la-photographie.net/ (dernière consultation 23 JUL 2021)

[42] **Facial recognition defined** [En ligne]
https ://us.norton.com/ (dernière consultation 15 AOUT 2021)

[43] **Rajiv Desai** FACIAL RECOGNITION (TECHNOLOGY) December 3, 2018.

[44] **face detection** [En ligne]
https ://searchenterpriseai.techtarget.com/ (dernière consultation 18 AOUT 2021)

[45] **Facial feature extraction and textual description** [En ligne]
https ://www.semanticscholar.org/ (dernière consultation 18 AOUT 2021)

[46] **Face description with local binary patterns** [En ligne]
https ://www.researchgate.net/ (dernière consultation 18 AOUT 2021)

[47] **Face Recognition : Understanding LBPH Algorithm** [En ligne]
https ://towardsdatascience.com/ (dernière consultation 20 OCT 2021)

[48] **Md. Abdur Rahim, Md. Najmul Hossain, Tanzillah Wahid Md. Shafiul Azam** Face Recognition using Local Binary Patterns Vol 13 Issue 4 Version 1.0 Year 2013

[49] **Fingerprint Recognition System** [En ligne]
https ://teachingonlineblog.blogspot.com/ (dernière consultation 23 OCT 2021)

[50] **Progress on regulating facial recognition** [En ligne]
https ://blogs.microsoft.com/ (dernière consultation 23 OCT 2021)

[51] **UnionCommunity's iris recognition system** [En ligne]
https ://www.icon-uk.net/ (dernière consultation 23 OCT 2021)

[52] **Clubhouse confirms security breach, deploys new safeguards** [En ligne]
https ://www.neowin.net/ (dernière consultation 23 OCT 2021)

[53] **The Power of a Signature in a Digital World** [En ligne]
https ://platform.keesingtechnologies.com/ (dernière consultation 23 OCT 2021)