REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****
UNIVERSITE DE YAOUNDE I
ECOLE NORMALE SUPERIEUR D'ENSEIGNEMENT TECHNIQUE D'EBOLOWA
DEPARTEMENT DE DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****
UNIVERSITY OF YAOUNDE I
HIGHER TECHNICAL TEACHER TREAINING COLLEGE OF EBOLOWA
DEPARTMENT OF OF COMPUTER ENGINEERING
****

Filière
Informatique Industrielle

CONCEPTION ET REALISATION D'UN SYSTEME BIOMETRIQUE UTILISANT LA RECONNAISSANCE FACIALE

Mémoire rédigé et soutenu en vue de l'obtention du
Diplôme de Professeur des Lycées d'Enseignement Technique Deuxième Grade
(DIPET II)

Par : **SAPEYA KANEDJA SOPHONIE**

Sous la direction de
Pr. NDJAKOMO ESSIANE Salomé
Maitre de conférences

Année Académique : 2019 - 2020

Dédicace

.

A ma famille

FICHE DE CERTIFICATION DE L'ORIGINALITE DU TRAVAIL

Je soussigne, SAPEYA KANEDJA SOPHONIE atteste que le présent mémoire de fin d'étude en vue de l'obtention du grade de PLET II en Génie Informatique, option Informatique Industrielle est le fruit de mes propres travaux effectués à l'Ecole Normale Supérieure de l'Enseignement Technique (ENSET) de l'université de Yaoundé 1 à Ebolowa sous la direction du professeur NDJAKOMO ESSIANE Salomé, Maître de Conférences.

Ce travail est authentique et n'a pas encore fait l'objet d'une présentation pour l'obtention d'un diplôme universitaire

Visa de l'auteur

SAPEYA KANEDJA SOPHONIE

Remerciements

Nos remerciements s'adressent :

- A madame le DIRECTEUR DE L'ENSET EBOLOWA Pr. Salomé NDJAKOMO ESSIANE superviseur et encadreur de notre mémoire, elle qui n'a ménagé aucun effort pour notre formation.
- Dr. OLLE OLLE Daniel, CHEF DE DÉPARTEMENT DU GÉNIE INFORMATIQUE, et un grand frère qui nous a apporté ses précieux conseils et son aide durant toute la période de formation.
- A M. NYATTE Membre important de notre équipe d'encadrement, enseignant à l'ENSET EBOLOWA, pour son encadrement et ces conseils.
- A Ma famille pour le soutien indéfectible dont ils ont fait part à mon égard.
- Tous les enseignants du département du génie informatique.
- A tous mes camarades de l'ENSET EBOLOWA, en particulier à ceux du département informatique filière informatique industrielle niveau 5.
- A toutes les personnes qui ont œuvré de près ou de loin dans l'accomplissement de ce mémoire.

Avant propos:

L'Ecole Normale Supérieure d'Enseignement Technique (ENSET), créé par Décret Présidentiel N° 2017/586 du 24 Novembre 2017, est un établissement d'Enseignement Supérieur relevant de l'Université de Yaoundé I. Il est situé au campus de Metykpwale dans la ville d'Ebolowa et abrite un bloc administratif, des salles de classes, un restaurant et bien d'autres.

L'ENSET a pour mission d'assurer :

- La formation des enseignants de l'Enseignement Secondaire Technique et des Conseillers d'Orientation Scolaire, Universitaire et Professionnelle ;
- La promotion de la recherche scientifique, technologique et pédagogique, ainsi que la valorisation de résultats de la recherche dans son implémentation ;
- L'appui au développement ;
- Le recyclage et le perfectionnement du personnel de l'Enseignement Secondaire Technique, des professionnels dans ses domaines de formation.

Dans le but de pouvoir perfectionner la formation de futur enseignant, il est prévu la rédaction d'un mémoire portant sur un projet réalisable d'où l'importance de ce projet : «conception et réalisation d'un système biométrique portant sur la reconnaissance faciale »

Résume :

La reconnaissance de visages est une fonction importante des systèmes de surveillance pour permettre la vérification et l'identification d'individus d'intérêt qui apparaissent dans une scène capturée par un réseau distribué de caméras. Ce projet vise à utiliser les images biométriques afin d'améliorer les performances d'authentification. Dans une première partie, nous proposons une comparaison de deux méthodes de détection du visage dans l'image. Dans une seconde partie nous nous intéressons au processus d'identification proprement dit. Une approche base sur les réseaux de neurones profond est adopté. Notre projet a été réalisé grâce à de nombreuses bibliothèque parmi lesquelles tensorflow. Notre travail nous a permis aussi de résoudre le problème de vrais jumeaux dans les systèmes de reconnaissance faciale en proposant un système embarqué de sécurisation a deux niveaux.

Abstract :

Face recognition is an important function of surveillance systems to allow verification and identification of individuals of interest who appear in a scene captured by a distributed network of cameras. This project aims to use biometric images in order to improve authentication performance. In the first part, we propose a comparison of two methods of detecting the face in the image. In a second part we are interested in the identification process itself. A deep neural network approach is adopted. Our project was carried out thanks to numerous libraries among which tensorflow. Our work has also allowed us to solve the problem of real twins in facial recognition systems by proposing an on-board two-level security system.

Table des matières

Liste des figures

Liste des tableaux

Listes des abréviations

CNN	Convolutional Neural Network
DL	Deep Learning
GPU	Graphics Processing Unit
IA	Intelligence Artificielle
LCD	Liquid Crystal Display
ReLu	Rectified Linear Unit
SVM	Support Vector Machine
ML	Machine Learning

Introduction générale :

Au Cameroun où le nombre de vol, d'arnaques et de d'escroqueries croit de jours en jours, le besoin de se protéger dans de nombreux secteurs d'activité (banques, industrie) est l'un des soucis majeurs. En plus de ces fléaux, vu le développement permanent et important de la société dans tous ces aspects, les outils de surveillance et de contrôle classique à savoir ceux relatifs à la méthode basée sur la connaissance tel que le mot de passe ou bien basée sur la possession tels que les badges, les pièces d'identités, clés, … s'avèrent inefficaces. Ces différents laissez-passer peuvent être perdus ou même volés. Dans le cas du mot de passe, celui-ci peut facilement être deviné par une autre personne. De plus ces mots de passes sont souvent archivés dans un bureau par l'organisation, or ceci est une faille certaine dans le système de sécurité.

Comment donc résoudre ces problèmes d'inefficacité des systèmes de sécurité actuelle ? comment améliorer la sécurité dans divers secteurs d'activités ? Pour pallier à ces différents problèmes d'inefficacité et de non sécurité, l'homme a fait référence à une nouvelle technique de reconnaissance qui a fait son apparition et ne cesse de croître depuis 1997 : il s'agit des contrôles d'accès par les systèmes biométriques

La biométrie est en effet une alternative aux deux précédents modes d'identification (connaissance, possession). Elle consiste à identifier une personne à partir de ses caractéristiques physiques ou comportementales. Le visage, les empreintes digitales, l'iris, sont des exemples de caractéristiques physiques. La voix, l'écriture, le rythme de frappe sur un clavier, etc. sont des caractéristiques comportementales. L'avantage principal de cette technique est que ces caractéristiques sont propres à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession. En effet, un attribut physique ou comportemental ne peut être oublié ou perdu et sont très difficiles à deviner, voler et dupliquer.

Dans ce travail, nous développerons l'un des systèmes biométriques les plus récents et les plus répandus dans le monde, et cela grâce à sa simplicité et son efficacité : un système de reconnaissance faciale simple et efficace.

Pour cela dans notre devoir nous présenterons dans une premier temps les généralités sur les systèmes biométrique et des travaux récent qui ont été fait dans notre domaine. Dans un deuxième temps nous présenterons la méthode et le matériel que nous allons utiliser pour faire notre devoir. Dans un troisième temps, nous présenterons les résultats et les interprétations

:

GENERALITES SUR LES SYSTEMES BIOMETRIQUES ET RECONNAISSANCE FACIALE

Chapitre 1

Introduction :

La protection des données est toujours une priorité pour toutes les entités économiques ou administratives surtout dans les domaines sensibles tels que la sécurité militaire et des coffres fort dans des banques, de peur qu'elles soient accessibles par des personnes malveillantes. Pour assurer cette sécurité nous utilisons les systèmes biométriques. Dans ce chapitre nous allons présenter dans un premier les différents systèmes biométriques et leur fonctionnement. Nous attarderons sur la reconnaissance faciale et les différentes techniques utilisé dans la reconnaissance faciale. Dans un deuxième temps nous ferons une synthèse de certains travaux déjà réalisé dans la reconnaissance faciale

I. Généralités sur les systèmes biométriques et reconnaissances faciales

Nous proposons dans cette section une présentation des systèmes biométriques pouvant faciliter la compréhension du travail,

I.1 les systèmes biométriques :

I.1.1-la biométrie :

La biométrie est utilisée depuis plusieurs années surtout dans le domaine de la sécurité, c'est une technologie qui consiste à identifier des personnes à l'aide d'une ou de plusieurs caractéristiques physiologiques des traits physiques particuliers qui, pour toute personne, sont uniques et permanents (empreintes digitales, visage, iris, contour de la main, etc.), ou comportementales l'analyse de certains comportements d'une personne comme le tracé de sa signature, sa démarche et sa façon de taper sur un clavier propres à chaque individu [5].

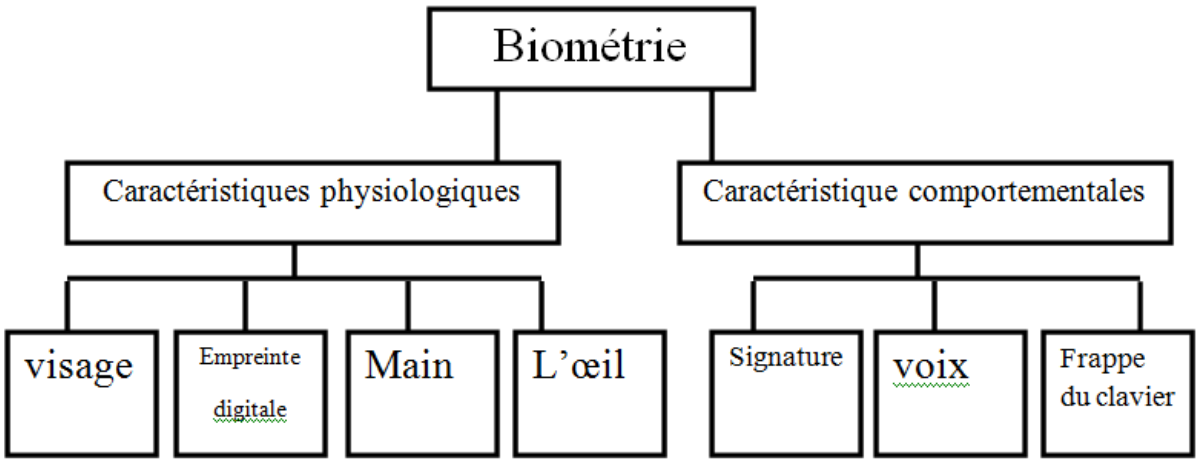


Figure 1: Classification de la biométrie [3].

Une autre définition de la biométrie est donnée par Roethenbaugh: «La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité »[6].

L'avantage de ces caractéristiques biométriques est d'être universelles, c'est-à-dire présentes chez toutes les personnes à identifier. D'autre part, elles sont mesurables et uniques, deux personnes ne peuvent posséder exactement la même caractéristique. Elles sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps. L'intérêt des applications utilisant la biométrie se résume en deux classes : faciliter le mode de vie, éviter la fraude [7].

L'utilisation de la biométrie est due aux imperfections causées par les anciennes techniques de vérification comme les mots de passe et les carte d'identité ou encore les clés qui à leur tour peuvent être perdus , volés ou encore devinés par d'autres personnes en plus aujourd'hui chacun doit se rappeler une multitude de mots de passe et avoir en sa possession un grand nombre de cartes , alors que la biométrie est immunisée contre ce genre de problèmes , elle est simple et pratique il n'y a ni carte a porté de main ni code ou mot de passe à retenir [7].

La biométrie est plus sécuritaire que les méthodes actuellement utilisées. Elle permet une identification précise et possible même sans papiers d'identification qui peuvent être contrefaits. Aussi, elle permet d'améliorer la sécurité des documents protégés biométriquement (les passeports, les contrats …etc.), donc de limiter la fraude. [6].

I.1.2. Système biométrique

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification [3]:

- L'enrôlement est une phase d'apprentissage qui consiste à recueillir des informations biométriques sur les personnes à identifier. Durant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numériques (signatures), et enfin stockées dans la base de données [3].
- Le mode de vérification (authentification) est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stocké dans la base de données du système. La vérification est réalisée via un numéro d'identification personnel, un nom d'utilisateur, ou bien une carte à puce [3].
- Le mode d'identification est une comparaison "un à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne [3].

L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés. Il existe plusieurs caractéristiques physiques uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie. Nous citons [6].

- Reconnaissance faciale
- Lecture de l'iris ou de la rétine
- L'empreinte digitale

- Reconnaissance de la voix
- Signature
- Reconnaissance du doigt
- L'ADN
- Géométrie de la main

I.1.3. Domaines d'application des systèmes biométriques

La biométrie est appliquée dans plusieurs domaines nécessitant une sécurité, tels que les contrôles d'accès physique et virtuel et l'authentification de transactions. Les applications de la biométrie peuvent être divisées en trois groupes principaux [6]:

- Applications commerciales : telles que l'ouverture de réseaux informatiques, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.
- Applications gouvernementales : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.
- Applications légales : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

I.1.4. Présentation de quelques techniques biométriques

Aucune biométrie unique ne pouvait répondre efficacement aux besoins de toutes les applications, chacune à ces forces ces limites ainsi que son type particulier d'application c'est pourquoi il existe plusieurs caractéristiques physiques uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, les techniques biométriques actuellement fonctionnelles sont très nombreuses. Elles peuvent cependant être répertoriées dans deux grandes familles [6].

I.1.4.1. Techniques d'analyse du comportement

Il s'agit d'un type de biométrie caractérisé par un trait d'attitude qui est appris et acquis au fil du temps, par exemple la dynamique de la signature, la façon d'utiliser un clavier d'ordinateur, etc. [6]. Nous citons :

- Dynamique de frappe au clavier

La dynamique de frappe au clavier est une caractéristique de l'individu, c'est en quelque sorte la transposition de la graphologie aux moyens électroniques. Christophe Rosenberger dit « C'est une technique née dans les années 1980 et qui vise à essayer d'analyser le comportement d'une personne qui tape au clavier à des fins d'authentification, elle est personnelle, et varie même avec l'âge et selon que l'on est une femme ou un homme. Comme un simple logiciel permet d'en faire l'analyse et qu'elle ne nécessite aucun autre matériel qu'un clavier » [11].

Les paramètres suivants sont généralement pris en compte : vitesse de frappe, suite de lettres, mesure des temps de frappe, pause entre chaque mot, reconnaissance de mot(s) précis. Son avantage est qu'elle est un moyen non intrusif qui exploite un geste naturel [12]

Avantage → moyen non intrusif qui exploite un geste naturel.

Inconvénient → dépendance de l'état physique de la personne (l'âge, maladies etc.).

- Signature

Chaque personne possède une signature qui lui est propre et qui peut donc servir à l'identifier. Il existe deux modes de reconnaissance : le mode statique et le mode dynamique. Le mode statique n'utilise que l'information géométrique de la signature. Le mode dynamique utilise à la fois l'information géométrique et dynamique, c'est à dire les mesures de vitesse et d'accélération. [10]

Le mode dynamique est plus riche en information que le mode statique, il est donc plus discriminant. De plus, si un imposteur veut dupliquer une signature à partir d'un exemple, il n'a pas accès à l'information dynamique. La capture se fait à l'aide d'une tablette graphique. La signature a l'avantage par rapport aux autres mesures biométriques d'être couramment utilisée

pour les transactions. Pour cette raison, la signature comme moyen d'identification est en général bien acceptée. Le problème de la reconnaissance par signature provient de la très grande variabilité qui existe entre deux occurrences de la signature d'un même individu. De plus, la signature peut être affectée par l'état de santé ou émotionnel de l'individu [10].

Figure 2: Exemple d'une signature [13].

I.1.4. 2. Techniques d'analyse de la morphologie humaine

Il s'agit d'un type de biométrie définie par les caractéristiques physiques (empreintes digitales, forme de la main, forme du visage, dessin du réseau veineux de l'œil, la voix, etc. [4]. Nous citons :

- Empreinte digitale

Elle est définie comme la caractéristique d'un doigt, chaque personne a ses propres empreintes digitales avec l'unicité permanente. A l'heure actuelle, la reconnaissance des empreintes digitales est la méthode biométrique la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentes des points singuliers « minuties » et constituent un motif unique, universel et permanent. Les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant l'utilisation classique de l'encre et du papier. Ces capteurs sont basés sur la capture optique, thermique, électromagnétique ou sur les ultrasons [13].

L'image d'empreinte d'un individu est capturée à l'aide d'un lecteur d'empreinte digitale puis les caractéristiques sont extraites de l'image puis un modèle est créé. Si des précautions appropriées sont suivies, le résultat est un moyen d'authentification très précis [13].

Les techniques d'appariement des empreintes digitales peuvent être classées en deux catégories : les techniques d'appariement sur la détection locale des minuties et celles basées

sur la corrélation. L'approche basée sur les minuties consiste à trouver d'abord les points des minuties puis trace leurs emplacements sur l'image du doigt [13].

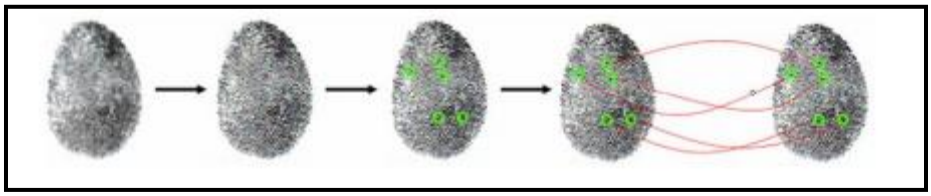


Figure 3: Le processus de reconnaissance par empreinte digitale [13].

Cette approche pose quelques difficultés lorsque l'image d'empreinte digitale est d'une qualité médiocre, car l'extraction précise des points de minutie est difficile. Par contre les méthodes basées sur la corrélation sont capables de surmonter les problèmes de l'approche fondée sur les minuties, car elles utilisent la structure globale de l'empreinte mais les résultats sont moins précis qu'avec les minuties. C'est pour cela que les deux approches sont en général combinées pour augmenter les performances du système [13].

- Voix

De tous les traits humains utilisés dans la biométrie, la voix est celle que les humains apprennent à reconnaitre dès leur plus jeune âge. Les systèmes de reconnaissance de locuteur peuvent être divisés en deux catégories : les systèmes dépendant du texte prononcé et les systèmes indépendants du texte. Dans le premier cas, l'utilisateur est tenu d'utiliser un texte fixe prédéterminé au cours des séances d'apprentissage et de reconnaissance. Alors que, pour un système indépendant du texte le locuteur parle librement sans texte prédéfini [13].

Cette dernière catégorie est plus difficile, mais elle est utile dans le cas où l'on a besoin de reconnaitre un locuteur sans sa coopération. La recherche sur la reconnaissance vocale est en plein croissance, car elle ne nécessite pas de matériel cher, puisque la plupart des ordinateurs personnels de nos jours sont équipés d'un microphone. Toutefois, la mauvaise qualité et le bruit ambiant peuvent influencer la vérification et par suite réduire son utilisation dans les systèmes biométriques. Dans un tel système, le signal est premièrement mesuré puis décomposé en plusieurs canaux de fréquences passe-bande. Ensuite, les caractéristiques importantes du signal vocal sont extraites de chaque bande. Les coefficients Cepstraux sont parmi les caractéristiques

les plus communément utilisées. Ils sont obtenus par le logarithme de la transformée de Fourier du signal vocal dans chaque bande. Finalement, la mise en correspondance des coefficients Cepstraux permet de reconnaitre la voix, dans cette étape, généralement on fait appel à des approches fondées sur les modèles de Markov cachés, la quantification vectorielle, ou la déformation temps dynamique [13].

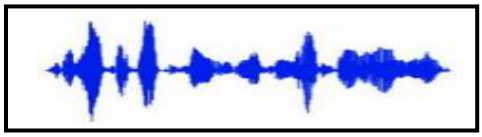


Figure 4: Spectre d'un signal voix [13].

- Iris

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification [13].

L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de l'individu est à une distance fixe et proche du dispositif de capture, ce qui limite l'utilisation de cette technologie [13].

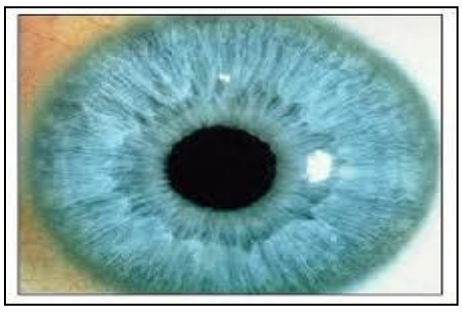


Figure 5: Détails d'une iris [13].

- Visage

Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi elle est en général très bien acceptée par les utilisateurs. Le système d'acquisition est soit un appareil photo, soit une caméra numérique pour extraire d'essentielles caractéristiques : les yeux, la bouche, le tour du visage, le bout du nez, etc.

Utiliser une caméra permet d'obtenir la forme du visage d'un individu et puis retirer certaines caractéristiques. Les caractéristiques essentielles pour la reconnaissance du visage sont : les yeux, la bouche, le tour du visage, le bout du nez, etc. Selon le système utilisé, l'individu doit être positionné devant la caméra ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont comparées au fichier référence [6].

Le logiciel doit être capable d'identifier un individu malgré les différents artifices physiques (moustache, barbe, lunettes, …)

Le visage est une biométrie relativement peu sûre. En effet, le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées, entre autres, par le maquillage, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion. La méthode de la reconnaissance du visage est sensible à la variation de l'éclairage et le changement de la position du visage lors de l'acquisition de l'image[6].

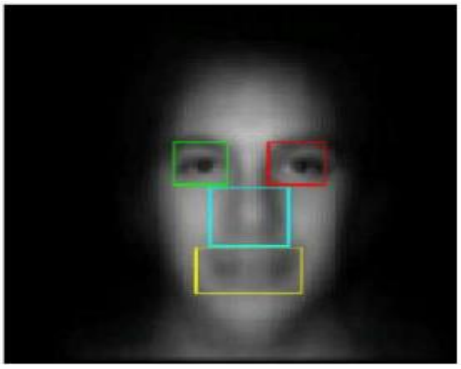


Figure 6 : Reconnaissance de visage [6].

I.1.5. Les limites de la biométrie

La biométrie présente malheureusement un inconvénient majeur ; en effet aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent [6].

I.2. La reconnaissance faciale :

I.2.1 Qu'est-ce que la reconnaissance faciale ?

La reconnaissance faciale est un procédé biométrique au même titre que la reconnaissance d'empreintes digitales, d'iris, ou vocale. Cela consiste donc à déterminer l'identité d'une personne. Le système de reconnaissance faciale est une application logicielle visant à reconnaître une personne grâce à son visage de manière automatique.

A l'aide d'algorithmes, cette application analyse toutes les caractéristiques faciales telles que l'écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton, à partir d'une image de son visage qui peut provenir à la fois d'une photo ou d'une vidéo. Donc de nombreux formats d'image peuvent être utilisés qu'ils soient statiques (JPG, bmp, png, GIF …)

Plusieurs méthodes de reconnaissance de visages ont été proposées durant ces 30 dernières années, suivant deux grands axes : la reconnaissance à partir d'images fixes et la reconnaissance à partir de séquence d'images (vidéo). La reconnaissance de visages basée sur la vidéo est préférable à celle basée sur des images fixes, puisque l'utilisation simultanée des informations temporelles et spatiales aide dans la reconnaissance.

I.2.2 Domaines de la Reconnaissance Faciale

Aujourd'hui la reconnaissance faciale est utilisée principalement pour des raisons sécuritaires. Elle peut être utilisée à des fins très diverses. Par exemple, l'authentification, le contrôle d'accès (autorisation) et la vidéo de surveillance.

Un bon exemple de l'usage des applications d'identification, est le nouveau tunnel qui est installé à Dubaï premier de ce type dans le monde. Il s'agit d'un système biométrique qui permet

aux passagers d'être identifiés en traversant un tunnel dans le but d'augmenter l'efficacité des points de contrôle de sécurité. Ils n'ont même pas besoin de montrer leur passeport. L'outil fonctionne grâce à la reconnaissance de l'iris et du visage. La procédure dure environ 15 secondes.

La reconnaissance faciale est aussi utilisée dans les Applications militaires. Un bon exemple de ce domaine est l'utilisation des lunettes de style « Robocop » munies d'une petite caméra d'une portée de 12 milles (19,3 km) par la marine américaine, la caméra peut aussi faire partie de l'optique d'un soldat sur son arme. Grâce à cet équipement, les soldats peuvent identifier des ennemis en quelques secondes sur le terrain, et cela sans réseau à large bande.

En revanche, on distingue un autre domaine d'application de ces systèmes qui est l'assistance à l'utilisateur. Les systèmes de reconnaissance faciale sont de plus en plus présents au quotidien. Ils sont par exemple utilisés sur les réseaux sociaux sur internet pour identifier quelqu'un sur une photo, sur les Smartphones pour les déverrouiller...

La nouveauté dans la reconnaissance faciale arrive grâce au développement de nouvelles caméras de type 3D. Ces caméras obtiennent de meilleurs résultats que les caméras classiques, parce qu'elles acquièrent une image tridimensionnelle de chaque visage (perspectives) pour identifier une personne lorsqu'elle passe par le portail d'authentification.

I.2.3 Historique

La reconnaissance faciale est une technique biométrique relativement récente. Si l'empreinte digitale est la technique biométrique la plus ancienne inventée en 1903 pour rechercher les criminels, la reconnaissance des visages a été développé par "Benton et Van Allen" en 1968 pour évaluer la capacité d'identification des visages non familiers. Il ne s'agit pas d'un test de reconnaissance ménisque de visages familiers ou non familiers, mais d'une épreuve consistant à apparier des photographies de visages non familiers présentés sous différents éclairages et selon des angles différents et nécessitant une bonne capacité d'intégration Visio-spatiale.

L'utilisation des techniques de reconnaissance faciale a connu un développement à grande échelle depuis le milieu des années 90, avec l'utilisation efficace de nouvelles technologies, notamment l'ordinateur et sa capacité de traitement d'images. L'utilisation de ces

techniques existe depuis qu'une machine est capable de comprendre ce qu'elle « voit » lorsqu'on la connecte à une ou plusieurs caméras, c'est à dire que les premiers essais datent du début des années 70 (Benton et Van Allen en 1968), et sont basés sur des méthodes à bases d'heuristiques, basés sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, etc. Ces méthodes sont très peu robustes, car elles font de nombreuses suppositions en se plaçant dans des cas très simples (visage de face, bonnes conditions d'illuminations, etc. L'une des premières tentatives de reconnaissance de visage est faite par TakeoKanade en 1973 lors de sa thèse de doctorat à l'Université de Kyoto.

I.2.4. Architecture générale d'un système de reconnaissance faciale

Un système de reconnaissance de visage est un système d'identification et de vérification d'individus, qui permet de vérifier si une personne appartient à la base de données du système, et de l'identifier si c'est le cas. On peut représenter les systèmes de reconnaissance par le diagramme suivant :

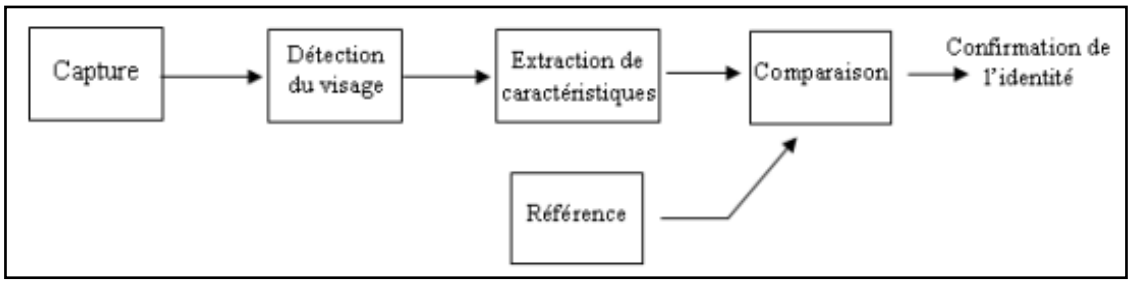


Figure 7 : Schéma générale d'un système de reconnaissance de visages [6].

- Capture : C'est la première étape dans le processus. C'est aussi l'acquisition des informations et leur transfert vers l'unité de traitement. Ça reste une étape très importante dans les systèmes de reconnaissance. En effet, avoir des images de bonne qualité en référence améliore les performances de reconnaissance. Il faut réussir à capter l'information pertinente sans bruit [17].

- Détection de visage : La détection de visage dans l'image est un traitement indispensable avant la phase de reconnaissance. En effet, le processus de reconnaissance de visages ne pourra jamais devenir intégralement automatique s'il n'est pas précédé par une étape de détection efficace [18]. Cela peut se faire par détection de la couleur de la peau, la forme de la tête, l'apparence faciale, ou par des méthodes détectant les différentes caractéristiques du visage par des descripteurs locaux (Adaboost). Après la segmentation du visage, on peut filtrer ou améliorer la qualité par des prétraitements qui sont appliqués au visage extrait. On peut effectuer des normalisations géométriques et photométriques. Ces prétraitements sont nécessaires pour éliminer ou limiter les variations de pose, uniformiser l'éclairage, minimiser l'influence de l'illumination, ainsi d'ajuster le visage pour qu'il ait une dimension particulière et qu'il soit horizontal [17].
- Extraction de caractéristiques : Le but est d'extraire les caractéristiques du visage qui peuvent le rendre à la fois différent de celui des autres personnes et robuste aux variations de la personne elle-même. C'est l'information nécessaire pour que le visage d'une personne ne ressemble pas à celui d'une autre personne et en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition [17].
- Comparaison : Selon les caractéristiques extraites précédemment, les algorithmes de comparaison diffèrent. On trouve dans la littérature plusieurs approches : calcul de distance, calcul de similarité. D'autres méthodes se basent sur la classification des caractéristiques par un seul classifieur (SVM, classifieur baysien, etc.) ou par plusieurs classifieurs [17].
- Inscription : s'il s'agit de la première fois qu'une personne est confrontée au système de reconnaissance faciale, l'image et/ou le modèle de référence peuvent être stockés sous la forme d'enregistrements en vue d'une comparaison ultérieure

I.2.5. Etat de l'art sur les techniques utilisé par la reconnaissance faciale

Plusieurs techniques de reconnaissance d'individus ont été développées au cours des dernières années. La plupart d'entre elles ont le visage comme zone d'intérêt, une tâche qui est par ailleurs un problème de reconnaissance des formes assez complexe. [15].

Les techniques les plus populaires utilisées en reconnaissance de visages, peuvent être divisées en deux groupes : les approches locales basées sur un modèle, dans lesquelles le système essaie de détecter, regrouper et reconnaitre les différents éléments constitutifs du visage tel que le nez, les yeux et la bouche, ainsi que les approches globales dans lesquelles on analyse le visage statistiquement.

I.2.5.1 Les approches globales :

Ce type d'approches utilisent le visage au complet comme source d'information, et ce
Sans segmentation de ses parties, elles se basent principalement sur l'information pixel. Ces Algorithmes s'appuient sur des propriétés statistiques bien connues et utilisent l'algèbre linéaire. Ils sont relativement rapides à mettre en œuvre mais sont sensibles aux problèmes d'éclairement, de pose et d'expression faciale. Parmi les approches les plus importantes réunies au sein de cette classe on trouve :

A. L'Analyse en Composantes Principales (ACP) / (PCA) :

L'algorithme ACP est né des travaux de MA. Turk et AP. Pentland au MIT Media Lab, en 1991[7] [14]. L'idée principale consiste à exprimer les M images de départ selon une base de vecteurs orthogonaux particuliers - les vecteurs propres – contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

Le but est d'extraire l'information caractéristique d'une image de visage, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire [7].

En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage. Donc, la ACP ne nécessite aucune connaissance à priori sur l'image et se révèle plus efficace lorsqu'elle est couplée à la mesure de distance, mais sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale [15].

Remarque : Le fait que l'on peut construire un sous-espace vectoriel en ne retenant que les meilleurs vecteurs propres, tout en conservant beaucoup d'informations utiles, fait du ACP un

algorithme efficace et couramment utilisé en réduction de dimensionnalité où il peut alors être utilisé en amont d'autres algorithmes.

B. L'Analyse Discriminante Linéaire (ADL) / (LDA) :

L'algorithme LDA est né des travaux de Belhumeur et al. De la Yale University (USA), en 1997[16]. Il est aussi connu sous le nom de « Fisherfaces ». Contrairement à l'algorithme ACP, celui de la ADL effectue une véritable séparation de classes. Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe.

La ADL analyse les vecteurs propres de la matrice de dispersion des données, avec pour objectif de maximiser les variations entre les images d'individus différents (interclasses) tout en minimisant les variations entre les images d'un même individu (intra-classes).

Cependant, lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, il est difficile d'appliquer la ADL qui peut alors faire apparaître des matrices de dispersions singulières (non inversibles). Afin de contourner ce problème, certains algorithmes basés sur la ADL ont récemment été mis au point (les algorithmes ULDA, OLDA, NLDA) [7] [16].

C. Les réseaux de neurones (RNA) :

Les réseaux de neurones artificiels ou RNA sont des assemblages fortement connectés d'unités de calcul. Chacune des unités de calcul est un neurone formel qui est, en soi, une formulation mathématique ou un modèle très simplifié d'un neurone biologique. Les RNA ont de très grandes capacités de mémorisation et de généralisation.

On classe généralement les réseaux de neurones en deux catégories : les réseaux faiblement connectés à couches que l'on appelle des réseaux « feedforward » ou réseaux directs et les réseaux fortement connectés que l'on appelle des réseaux récurrents. Dans ces deux configurations, on retrouve des connexions totales ou partielles entre les couches. Les réseaux de neurones peuvent être utilisés tant pour la classification, la compression de données ou dans le contrôle de systèmes complexes en automatisme. Cette approche repose essentiellement sur la notion d'apprentissage qui est depuis de nombreuses années au cœur des recherches en intelligence artificielle [15]. L'idée est d'identifier à partir d'exemples un visage (ici une

personne). De manière plus formelle, l'apprentissage du réseau a pour but l'extraction des informations pertinentes à l'identification.

L'avantage de ce modèle est le gain de temps considérable. Cependant, l'utilisation d'exemples pour apprendre apporte le risque de ne pouvoir résoudre que des situations déjà rencontrées, où un phénomène de sur-apprentissage qui spécialiserait le réseau uniquement sur les exemples connus sans généraliser [15].

D. Machine à Vecteurs de Support (SVM) :

C'est une technique qui a été proposée par V.Vapnik en 1995, elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion,… ect). L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à des classes différentes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [19] [20].

Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la fonction de classement séparant les classes tels que :

- Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyperplan.

- La plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

Depuis son introduction dans le domaine de reconnaissance de formes, plusieurs travaux ont montré l'efficacité de cette technique, principalement en traitement d'images.

E. Mélange de gaussiennes (GMM) :

C'est une nouvelle approche qui a été proposé par Conrad SANDERSON et al, elle consiste à transformer les images de départ en plusieurs vecteurs de coefficients DCT, puis modéliser leur distribution selon une combinaison linéaire de plusieurs gaussiennes qui vont représenter un modèle d'une personne [21].

Cette technique est venue pour améliorer les performances des HMM, elle a prouvé une efficacité surprenante surtout en matière de précision et de temps d'exécution.

F. L'approche statistique et l'approche probabiliste :

Cette approche repose essentiellement sur la théorie de décision pour résoudre les problèmes de classement et de classification. Pour cela on utilise généralement la classification fondée sur le théorème de Bayes. L'approche probabiliste utilise un mélange d'analyseurs de facteurs pour détecter les visages humains. L'inconvénient c'est qu'elle pose le problème de la complexité de calcul qui est très élevée [15].

I.2.5.2 Les approches locales :

On les appelle aussi les méthodes à traits, à caractéristiques locales, ou analytiques. Ce type consiste à appliquer des transformations en des endroits spécifiques de l'image, le plus souvent autour de points caractéristiques (coins des yeux, de la bouche, le nez, ...). Elles nécessitent donc une connaissance a priori sur les images [15].

L'avantage de ces méthodes est qu'elles prennent en compte la particularité du visage en tant que forme naturelle à reconnaître, en plus elles utilisent un nombre réduit de paramètres et elles sont plus robustes aux problèmes posés par les variations d'éclairement, de pose et d'expression faciale [20],[7]. Mais leur difficulté se présente lorsqu' il s'agit de prendre en considération plusieurs vues du visage ainsi que le manque de précision dans la phase "extraction" des points constituent leur inconvénient majeur [20]. Parmi ces approches on peut citer :

a. Hidden Markov Models (HMM):

Les modèles de Markov cachés (HMM) sont utilisés depuis plusieurs années pour la détection et la reconnaissance du visage. Différentes variantes ont également été proposées mais celle des (Embedded HMM) génère des résultats supérieurs aux méthodes HMM de base [22]. Reposant sur certains coefficients de la transformée en cosinus discrète (DCT) comme source d'observations, les Embedded HMM constituent un algorithme de reconnaissance très performant. Or, les temps d'exécution des phases d'apprentissage et de test sont relativement élevés, nuisant donc à son utilisation en temps réel sur d'immenses banques d'images [22].

b. Eigen objects (EO):

Basés sur les mêmes principes théoriques que la méthode des « EigenFaces » abordée à la section précédente, les « EigenObjects » visent cette fois certaines parties bien précises du visage. La personne peut par exemple être reconnue uniquement grâce à ses yeux. Pour réaliser l'apprentissage, un module de ce type doit tout d'abord procéder à une ACP des yeux contenus dans la banque de visages. L'espace des yeux (eye space) ainsi construit pourra alors servir au processus de reconnaissance qui est identique à celui utilisé pour les « EigenFaces ».

c. Elastic Bunch Graph Matching (EBGM):

Dans cette approche, on localise des points caractéristiques (coins des yeux, de la bouche, nez, etc.) à partir d'une image de visage, cette localisation peut se faire manuellement ou automatiquement à l'aide d'un algorithme [1]. Un treillis élastique virtuel est ensuite appliqué sur l'image de visage à partir de ces points.

Chaque point représente un nœud labellisé auquel on associe un jeu de coefficients d'ondelettes complexes de Gabor, appelés Jet. Pour effectuer une reconnaissance avec une image test, on fait une mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

La caractéristique de l'EBGM c'est qu'il ne traite pas directement les valeurs de niveaux de gris des pixels d'une image de visage, ce qui lui confère une plus grande robustesse aux changements d'éclairement, de pose et d'expression faciale. Cependant il est plus difficile à implémenter que les méthodes globales [7].

d. L'appariement de gabarits :

L'appariement de gabarits (Template Matching) est une technique de comparaison des images, son principe est simple. En effet, elle permet l'extraction et la construction des descripteurs des points d'intérêts de l'image, ces descripteurs sont très robustes et fiables et permettent une représentation fidèle de l'image en se basant sur son contenu. En plus on peut permettre une meilleure représentation à notre image par translation et rotation sans perte d'information grâce aux invariants de Hu [2].

I.2.5.3 Les approches hybrides :

Plusieurs techniques peuvent parfois s'appliquer afin de résoudre un problème de reconnaissance des formes. Chacune d'entre elles possède évidemment ses points forts et ses points faibles qui, dans la majorité des cas, dépendent des situations (pose, éclairage, expressions faciales, etc.). Il est par ailleurs possible d'utiliser une combinaison de classificateurs basés sur des techniques variées dans le but d'unir les forces de chacun et ainsi pallier à leurs faiblesses.

I.2.7. Avantages et inconvénients de la reconnaissance de visages

Plusieurs facteurs rendent la modalité visage attractive pour une utilisation à grande échelle, elle est acceptable par les personnes vues que c'est une partie apparente du corps, facilement vérifiable par n'importe quel opérateur pour avoir une décision, intrusive en raison de la vérification aisée. De plus, les capteurs d'images sont moins chers sur le marché [6]. En dépit de ses avantages, elle présente des inconvénients qui influent sur la qualité de la reconnaissance. On peut citer les aspects suivants :

- Changement d'illumination.
- Expressions faciales.
- Présence ou absence des composantes structurales, telles que : la barbe, la moustache et les lunettes.
- Les vrais jumeaux qui ont le même indicatif d'AND

II. Etude des travaux antérieurs :

1. SOUHILA GUERFI ABABSA (2008) : université de Evry val d'essone

Dans son travail de thèse, SOUHILA avait mené une étude sur l'authentification des individus à l'aide de la reconnaissance faciale. Utilisant la méthode ACP, son étude avait pour objectif de concevoir un système d'authentification de visage simple et efficace. Il est arrivé au résultat en développant une technique 2D de reconnaissance de visage basé sur l'analyse en composant principal qui prend en entrée, non pas l'image entière du visage, mais les « imageries » correspondant aux trois régions de caractéristique de visage (le nez, la bouche et les yeux) et a réussi a démontré que cette technique donnait des taux de reconnaissance aussi bon que l'image complète

2. Walid Hizem (2009) : Université pierre et marie currie de France

Dans son travail de thèse, Walid a mené une étude sur les capteur intelligent pour la reconnaissance faciale. Etant beaucoup plus intéressé par les problèmes liés à la lumière dans le domaine de la reconnaissance faciale, dans le travail, Walid s'est fixé comme objectif une solution capable d'éliminer le problème de luminosité. Pour y arriver, Walid a utilisé l'illumination active avec deux méthodes d'acquisition : la première avec un capteur CMOS différentiel, la seconde une acquisition avec réduction de temps d'exposition et un flash synchrone à la période d'acquisition. Ainsi comme résultat, il a mise au point une caméra CCD permettant d'avoir des images de bonne qualité en proche infrarouge et à moindre coût en éliminant la variation d'illumination

3. MURHULA KABI Grâce (2017) : Institut supérieur pédagogique de Bukavu

Dans son travail, MURHULA grâce a mené une étude sur la conception et la réalisation d'une application de gestion des présences des agents basé sur la technologie biométrique de reconnaissance faciale. Dans son mémoire, son objectif est d'utilisé une technique de reconnaissance faciale qui serait très rapide et robuste afin que son système fonctionne en temps réel. Pour cela elle a utilisé une librairie de reconnaissance faciale appelé « luxand FaceSdk » qui dispose d'un outil « Tracker API » qui simplifie la reconnaissance en temps réel, WampServer et un IDE NetBeans et un api gratuit pour la production des rapports en java

4. Kalghoum ANWAR (2011) : Institut supérieur d'informatique et gestion de Kairouan de Tunisie

Dans son travail portant sur la réalisation d'une application de gestion des présences via reconnaissance faciale, Kalghoum s'est fixé l'objectif de faire l'étude, la conception et la mise en œuvre d'un système informatisé de gestion des présences via une technologie de reconnaissance faciale pour la société SIERREN en Tunisie. A l'aide du duo JAVA-Access, il avait mis au point un système qui permettrait à l'agent que lorsqu'il arrive au travail, il se présente devant l'ordinateur, on lui capture la photo afin de pointer la présence. Signalons que l'auteur n'a pas été claire sur la méthodologie.

5. M. BELAHCENE-BENATIA mébarka (2014) : revue de science des matériaux

Dans son article, Mébarka avait le but de concevoir un système d'authentification d'identité qui serait facile et peu couteux dans l'implémentation utilisant le visage humain. Cette étude mené avec la méthode ACP et la classification avec les réseaux des neurones avait pour objectif de minimiser le TEE (taux d'erreur égale) afin de renforcer les capacités d'une application de reconnaissance faciale. Mébarka aboutit aux résultats selon lesquels en utilisant la classification il a un taux d'erreur égale (TEE=11.5%) sur la base de données de 40 sujets avec un TFA (taux de fausse Acceptation) égale à 9% et un TFR (taux de faux rejet) égale à 15.32%. En faisant la classification avec les réseaux de neurones, TFA= 5% ; TFR=57 pour une base de données de 60 sujets et avec la normalisation TFA=12 et un TFR=23 pour la même base de 60 sujets

6. BERREDJEM Achref (2019) : Université de Guelma en Algérie

L'objectif suivi par BERREDJEM propose une démarche qui consiste à améliorer la performance de l'identification biométrique via l'empreinte FKP par plusieurs méthodes avec un ensemble d'opération. Pour cela, il fait le choix de la méthode LPQ et LBP qu'il applique à sa base de données. Les résultats qu'il obtient sont très intéressant car : il arrive a un taux de reconnaissance acceptable. Ce qui rend son système fiable. Malgré les résultats obtenue, force est de constater que dans son devoir il ne prend pas en compte l'évaluation de la performance en deux phases la vérification et l'identification en utilisant une base de données de grande taille. Il n'intègre pas d'autres traits biométriques pour augmenter la précision de son système.

7. BOUDJELAL Sofiane (2010) : UMMTO en Algérie

C'est avec la méthode Eigenface que BOUDJELAL Sofiane a sur un système de reconnaissance faciale. Son travail avait pour objectif de mettre en place un système qui permet la reconnaissance d'un individu et le contrôle d'accès. Pour cela, il a fini par développé une application qui malgré de bon résultat qu'elle a apporté, il souligne un problème de pose et d'éclairage restent des challenges qui susciterons des efforts au niveaux des chercheurs

8. Serge KOMANDA BASEMA (2010) : ISP/BUKAVU

Cet auteur a mené une étude sur l'étude des personnes par reconnaissance des visages pour la sécurité d'une institution bancaire. L'objectif de ce travail était d'offrir à la banque un

système de contrôle par caméra de surveillance et ces dernières assistées par une application de détection et reconnaissance faciale (reconnaissance des visages) afin que les figures capturées puissent subir de suivi en cas d'espionnage, d'escroqueries et de braquages. En utilisant la méthode des eigenfaces et opencv, il est arrivé à un résultat de mise en place d'une application de reconnaissance faciale qui ne s'est limité qu'au stockage des images sur le disque dur.

9. MESROUA Djamel REBOUH Syphax (2017) : Université Abderahmane Mira de Béjaïa

Suite aux besoins d'identifier une personne ayant par exemple commis un délit en milieu professionnel(banque) ; Le travail réalisé par MESHOUA porte sur l'intégration d'un système de reconnaissance faciale à la télésurveillance. Pour cela, il crée une base de données grâce un script python, effectue un apprentissage puis une détection du visage. La reconnaissance est effectué grâce à la méthode ACP utilisant l'algorithme Eigenfaces et le logiciel permettant le traitement d'images est opencv. Des tests ont été effectués sur plusieurs images, et les résultats sont satisfaisants. Malgré ces résultats, il n'utilise pas un système embarqué et la détection d'intru ne se fait pas à temps réels

10. Mr. GHALI Ahmed (2015) : UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN MOHAMED BOUDIAF

Dans son mémoire, Mr. GHALI Ahmed travail sur la reconnaissance faciale dans le but de vérifier l'identité d'une personne à partir de son image. Dans ce travail, la transformation en ondelettes discrète DWT est utilisée comme une étape de prétraitement, l'analyse en composantes principales (ACP) est utilisée pour jouer un rôle clé dans la fonction d'extraction et les SVM sont utilisés pour lutter contre le problème de la reconnaissance des visages. Il illustre le potentiel de SVM sur la base de données de visages ORL de Cambridge, qui se compose de 400 images de 40 personnes, contenant tout un haut degré de variabilités dans l'expression, posons, et les détails du visage. Les SVM qui ont été utilisées dans son travail comprennent le linéaire (LSVM), Polynomial (PSVM), et fonction à base radiale (RBFSVM). Il a obtenu un taux de reconnaissance très élevée égale à 97,9 dans la base des images d'ORL.

11. Khayati Mouna, Mestiri Makram, Hamrouni Kamel, Daoudi Mohamed (2016) : Ecole national d'ingénieurs de Tunis

Dans cet article, ils travaillent sur la détection de visage et la reconnaissance de visage par une caméra de profondeur. Pour cela ils proposent un Framework appelé la Kinect pour la détection en temps réel et l'identification du visage. Ce Framework est utilisé pour la reconnaissance faciale 3d et se divise en 6 parties : ils commencent par capturer des images 3D de profondeurs via le capteur infrarouge, et des images RVB, une reconstruction du nuage de points est alors appliquée. Ils appliquent ensuite une mise en correspondance 2D/3D afin de retrouver les textures de chaque pixel de l'image 3D. Il localise le visage par association des deux images 2D et 3D. après extraction Il utilise les diffèrent filtres afin d'améliorer la qualité du nuage de point capturé. Il obtient un system de détection de visage

12. VARUN JAIN (2011) : université de Grenoble

VARUN JAIN a orienté son étude sur la reconnaissance des émotions à partir du visage. Son travail avait pour objectif de développer des méthodes et des techniques permettant d'inférer l'état affectif d'une personne à partir des émotions des informations visuelles, c'est-à-dire l'analyse des expressions du visages. Dans ses démarches, il avait utilisé l'approche Gaussienne Multi-échelle en tant que scripteur d'image pour l'estimation de la pose de la tête, pour la détection de sourire, puis aussi pour la mesure de l'affect. En plus de cette approche, il avait tout de même utilisé l'analyse en composant principal pour la réduction de la dimensionalité et les machines à support des vecteurs pour la classification et les régressions. Lors de ces expérimentations, Varun JAIN a constaté que dans le cas d'un éclairage partiel du visage, les dérivées gaussiennes multi-échelles ne fournissaient pas une description d'image suffisamment discriminante. Pour résoudre ce problème il avait combiné des dérivées Gaussiennes avec des histogrammes locaux de types LBP (Local Binary pattern). Avec cette combinaison il avait obtenu des résultats à la hauteur de l'état de l'art pour la détection de sourire dans la base d'image GENKI qui comporte des images de personnes trouvées « dans la nature » sur internet, et avec la difficile « extended YaleB database ».

13. DIALLO Nene Adama Dian(2019) : Université de Guelma en Algérie

Dans son mémoire, DIALLO a orienté son étude sur les expressions faciales. La méthode qu'il a utilisée est le réseau des neurones convolutif. Il utilise comme bibliothèque opencv pour le traitement d'image, matplolib qui est une bibliothèque de traçage pour le langage de programmation python, keras qui permet d'interagir avec le réseau de neurones profond ; pandas qui est une bibliothèque open source sous licence BSD fournissant des structures de données de hautes performances et faciles à utiliser. Malgré de bon résultat nous constatons qu'il met en perspectives de travailler avec les modèles déjà entrainés tels que VGG-face

Tableau 1 : synthèse des résultats

N°	Auteurs	Méthode	Principaux résultats
1	SOUHILA GUERFI ABABSA (2008)	ACP	Développement d'une technique 2D de reconnaissance de visage basé sur l'analyse en composant principal qui prend en entrée, non pas l'image entière du visage, mais les « imageries » correspondant aux trois régions de caractéristique de visage (le nez, la bouche et les yeux)
2	Walid Hizem (2009)	Acquisition avec réduction du temps	Il a mise au point une caméra CCD permettant d'avoir des images de bonne qualité en proche infrarouge et à moindre coût en éliminant la variation d'illumination
3	MURHULA KABI Grâce (2017)	luxand FaceSdk	Son objectif est d'utilisé une technique de reconnaissance faciale qui serait très rapide et robuste afin que son système fonctionne en temps réel.
4	Kalghoum ANWAR (2011)	Méthode non spécifiée dans le travail	Une application de gestion des présences pour la société SIERREN

5	M.BELAHCENE-BENATIA mébarka (2014)	Analyse en composants principal et la classification avec le réseau des neurones	Application de reconnaissance faciale avec un TEE=11.5%
6	BERREDJEM Achref (2019)	LPQ et LBP	BERREDJEM propose une démarche qui consiste à améliorer la performance de l'identification biométrique via l'empreinte FKP
7	BOUDJELAL Sofiane (2010)	Eigenfaces	Développement d'une application de reconnaissance faciale
8	Serge KOMANDA BASEMA (2010)	Eigenfaces et comparatives	Une approche d'identification des individus
9	MESROUA Djamel REBOUH Syphax (2017)	ACP	; Le travail réalisé par MESHOUA porte sur l'intégration d'un système de reconnaissance faciale à la télésurveillance.
10	Mr. GHALI Ahmed (2015)	ACP et SVM	Ahmed travail sur la reconnaissance faciale dans le but de vérifier l'identité d'une personne à partir de son image
11	Khayati Mouna, Mestiri Makram, Hamrouni Kamel, Daoudi Mohamed (2016)	Framework Kinect	Ils travaillent sur la détection de visage et la reconnaissance de visage par une caméra de profondeur

12	VARUN JAIN (2011)	L'approche Gaussienne Multi-échelle et ACP	Lors de ces expérimentations, Varun JAIN a constaté que dans le cas d'un éclairage partiel du visage, les dérivées gaussiennes multi-échelles ne fournissaient pas une description d'image suffisamment discriminante. Pour résoudre ce problème il avait combiné des dérivées Gaussiennes avec des histogrammes locaux de types LBP (Local Binary pattern).
13	DIALLO Nene Adama Dian (2019)	Réseaux de neurones convolutif	Il a orienté son étude sur les expressions faciales.

III. Discussion :

Après avoir feuilleter quelques travaux sur la reconnaissance faciale, nous avons eu comme initiale impression que presque tous les projets ont utilisé la méthode Eigenfaces, ACP ou encore SVM. Pour la réalisation de leurs projets. Or, comme nous l'avons dit plus haut dans la revue de littérature théorique, la contrainte de temps dans ces méthodes est plus considérable par rapport aux réseaux des neurones, ceci étant nous proposons dans un premier temps une solution plus rapide. En plus de ce problème de rapidité les méthodes de Eigenfaces tout comme les SVM sont trop sensible aux problèmes de pose, d'expression faciale et de luminosité. Cela étant, notre deuxième apport est de proposé une approche basée sur 128 points du visage afin de renforcer la robustesse de la reconnaissance.

Par rapport aux travaux de monsieur Serge KOMANDA BASEMA qui a trav aillé dans un sujet presque similaire au notre par rapport à son titre ; son système permettait d'offrir à la banque un système de contrôle par caméra de surveillance et ces dernières assistées par une application de détection et reconnaissance faciale (reconnaissance des visages) afin que les figures capturées puissent subir de suivi en cas d'espionnage, d'escroqueries et de braquages. Un apport de notre projet par rapport à ce projet est d'offrir non plus une application permettant

la reconnaissance faciale, mais un système embarqué qui sera connecté à une application androïde permettant de renforcer la sécurité du système et la facilité d'utilisation de notre projet

En prenant les travaux de DIALLO Nene Adama Dian en 2019 qui utilise les réseaux de neurones convolutif pour la détection des expressions faciales, nous constatons que celui-ci malgré les résultats qu'il obtient met en perspectives de travailler avec un modèle déjà entrainées tels que VGG16. Bien que nous ne fassions pas dans la détection des expressions faciales comme monsieur DIALLO, un apport à notre travail serait d'utilisé ce modèle déjà entraîné VGG16 qui est complexe dans l'utilisation afin d'obtenir de meilleur résultat

En plus de tous ce qui a été dit plus haut dans les inconvénients(limites) de la reconnaissance faciale, nous ne pouvons pas distinguer les vrais jumeaux : une originalité donc de notre système est de résoudre ce problème en proposant un premier niveau de sécurité par code et ensuite un deuxième niveau de sécurité avec la reconnaissance faciale.

Enfin tous les articles utilisant la reconnaissance faciale sont faits avec le microcontrôleur Raspberry pi qui est une solution vraiment plus ergonomique. Nous dans notre projet nous proposons une reconnaissance faciale utilisant une solution didactique basé sur le microcontrôleur Arduino

Conclusion partielle :

A la fin de ce chapitre où notre propos était de présenter la généralité sur les systèmes biométrique et la reconnaissance faciale, nous avons décrit les systèmes biométriques existants dans un premier temps, dans un deuxième temps nous avons présenté les systèmes à reconnaissance faciale et dans un troisième temps nous avons montré les travaux qui ont déjà été menés dans le domaine de reconnaissance faciale et de la biométrie. Après avoir présenté ces quelques travaux, nous avons ensuite exhibé l'originalité de notre travail par rapport à ces travaux déjà accomplis. Comme nous l'avons évoqué en introduction générale, l'objectif de notre travail est de réalisé un système biométrique de reconnaissance faciale. Ainsi, nous allons donc dans le prochain chapitre décrire la méthode et présenter les matériaux nécessaire a la réalisation de notre projet

:

MATERIEL ET METHODES

Chapitre 2

Introduction

Dans ce chapitre nous allons tout d'abord présenter de façon détaillé la méthodologie que nous avons suivie pour la réalisation de l'application qui nous permettra d'identifier une personne. Le programme de reconnaissance faciale sera codé en python. Il utilisera une bibliothèque openCV pour le traitement des images recueillit grâce à une caméra. L'algorithme utilisé dans notre projet est le réseau de neurone de convolution. Enfin nous présenterons tous les outils qui ont permis la réalisation de notre projet.

I- Cahier de charge fonctionnel :

Le cahier des charges fonctionnel (CdCF) est un document formulant le besoin, au moyen de fonctions détaillant les services rendus par un produit et les contraintes auxquelles il est soumis. Le cahier des charges vise à définir et à faire valider les spécifications d'un produit ou d'un service à réaliser. Ici il s'agit de cahier des charges fonctionnel, formulant le besoin au moyen de fonctions détaillant les services attendus et les contraintes auxquelles le produit à fournir est soumis.

I.1- Le concept général et les principaux services attendus

I.1.1 Mise en situation

a) Formulation du besoin

Assurer la sécurité des biens et des personnes à travers système embarqué, pour garder ou préserver la confidentialité et la restriction des accès dans les salles à accès réduites

b) Les clients, utilisateurs et usagers potentiels

- Les clients

Les clients peuvent toutes personnes, femmes et les hommes. Le client étant celui qui réalise l'acte d'achat de notre application

- Les utilisateurs et les usagers

Les utilisateurs sont tout d'abord des personnes qui décident d'acquérir le logiciel. Il Ya lieu de souligner que tout comme dans les entreprises ou des structures nous avons des cadres, il est important de séparer les cadres ou usagers particuliers des usagers normaux pouvant être admis à accéder à l'application

I.2- Contexte du projet

Etudes déjà effectuées en amont de l'élaboration du Cahier des Charges Fonctionnel

Avant de constituer le Cahier des Charges Fonctionnel, deux études sont effectuées pour mieux saisir le besoin du client potentiel.

- Une étude de marché : dégager les fonctions de service

L'étude de marché permet d'analyser la demande et de répondre au mieux aux attentes du client. Pour satisfaire le client, il faut dégager les fonctions principales[1] répondant au besoin.

Dans notre cas, pour répondre au besoin, il faut travailler sur les fonctions suivantes :

- Eviter une confusion entre les individus
- Prendre en compte les jumeaux dans la reconnaissance faciale
- Permettre l'ouverture et la fermeture de la porte en temps réel
- Être simple d'utilisation
- Être léger
- Être peu encombrant
- Être esthétique

- Permettre la surveillance à distance par le propriétaire de l'application ou le gérant d'entreprise

➢ **Enoncer le besoin :**

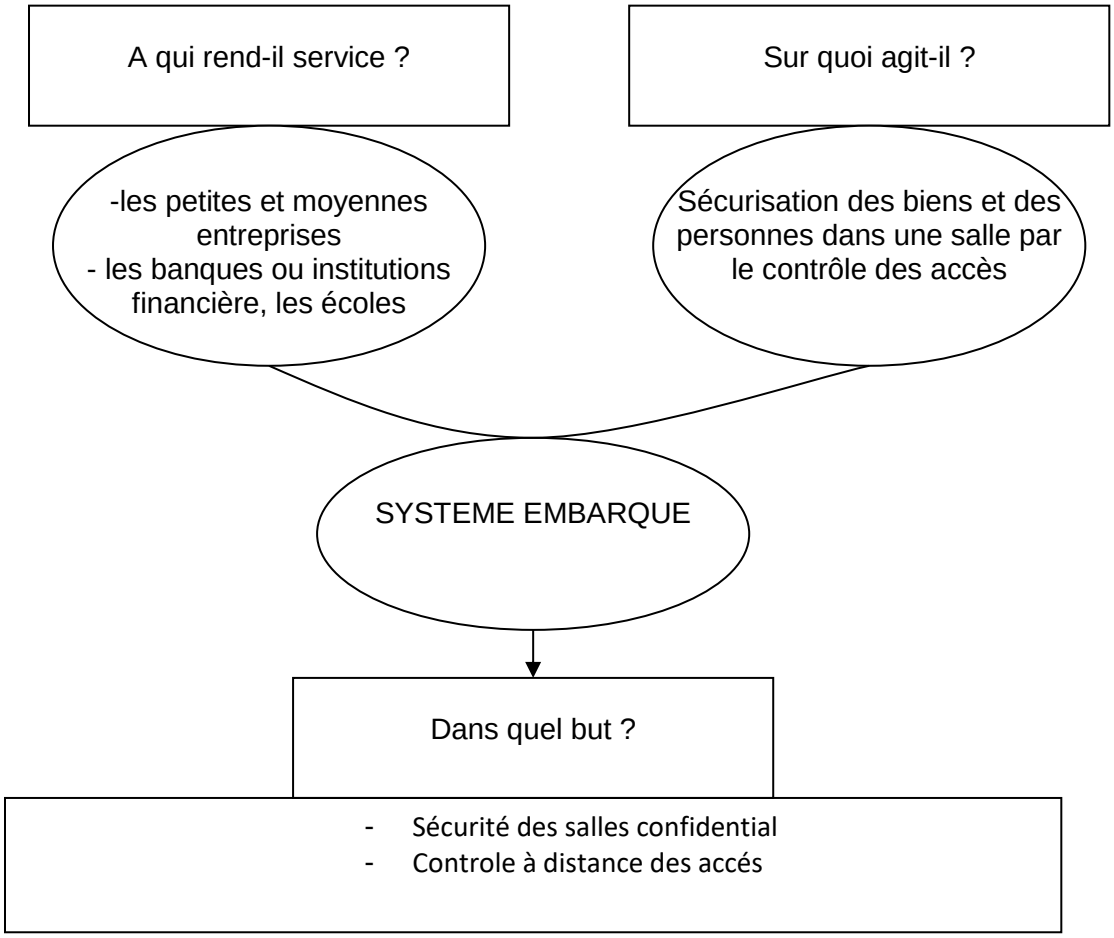


Figure 8 Diagramme bête à corne

➢ **Valider le besoin**

- À qui le produit rend-il service ?

Le système embarqué s'adresse aux utilisateurs désirant assurer la sécurité et la sureté des biens et des personnes désireux d'accéder à une salle d'accès restreinte. Le consommateur doit avoir

un produit répondant à toutes ses attentes : il doit être léger, utilisable en tout lieu et doit pouvoir être esthétique.

- Sur quoi agit-il ?

Il agit directement sur une porte permettant la sécurisation des biens ou des personnes grâce à deux niveaux de sécurité

II- Méthode utilisé pour l'implémentation de notre reconnaissance

II.1 – principes de fonctionnement de la reconnaissance faciale :

- Tout d'abord, une IA trouve le visage dans l'image (avec l'algorithme Haar Cascade)
- Puis le visage est découpé et déformé pour être recentré et réaligné par rapport à l'image : c'est le Dlib Shape Predictor qui peut faire ça
- Ensuite une IA analyse l'image et en donne 128 nombres qui la représentent, via un réseau de neurones convolutifs : VGG Face
- Enfin, la dernière IA cherche dans notre base de données quelle est la personne la plus « proche » de ce vecteur
-

II.2- méthodes utilisé pour la reconnaissance faciale :

II.2.1- description du réseau de neurones de convolution :

L'opération de convolution va se faire en plusieurs étapes à savoir :

a) L'opération de convolution :

Dans sa forme la plus générale, la convolution est une opération sur deux fonctions d'argument réel. Elle fonctionne comme un extracteur de caractéristiques des images. Une image est passée à travers une succession de filtres, ou noyaux de convolution, créant de nouvelles images appelées cartes de convolutions. Certains filtres intermédiaires réduisent la résolution de l'image par une opération de maximum local. Au final, les cartes de convolutions sont mises à plat et concaténées en un vecteur de caractéristiques, appelé **code CNN.**

Nous obtenons une nouvelle fonction qui fournit une estimation lisse de la position du vaisseau spatial :

$$s(t) = \int x(a)w(t-a)da$$

L'opération de convolution est généralement désignée par un astérix :

$$s(t) = (x * w)t$$

Si on suppose maintenant que x et w sont des entiers, on peut définir la convolution discrète :

$$s(t) = (x * w)(t) = \sum_{a=-\infty}^{\infty} x(a)w(t-a)$$

La convolution est le cœur du réseau de neurones convolutif, comme vous vous en doutez. À l'origine, une convolution est un outil mathématique (on parle de produit de convolution) très utilisé en retouche d'image, car il permet d'en faire ressortir l'extraction des caractéristiques à partir des images d'entrées, afin d'appliquer un bon filtre. En fait, une convolution prend simplement en entrée une image et un filtre (qui est une autre image), effectue un calcul, puis renvoie une nouvelle image (généralement plus petite).

- Bien qu'il existe plusieurs types d'opération de convolution nous pouvons dire que nous allons utilisé l'opération de convolution de base
- Fonctions d'activation : Une fonction d'activation est une fonction mathématique appliquée à un signal en sortie d'un neurone artificiel. Il dérive de l'équivalent biologique qui signifie "potentiel d'activation, lorsque le seuil de stimulation aura été atteint entraîne une réponse du neurone. Son but principal est de pouvoir permettre aux réseaux de neurones d'apprendre des fonctions plus complexes qu'une simple régression linéaire, car le simple fait de multiplier les poids d'une couche cachée est juste une transformation linéaire : □ Rectified Linear Unit (ReLU) : Elle est utilisée après chaque opération de convolution, ou toutes les valeurs de pixels négatifs sont mises à zéro. Le but de ReLU est d'introduire la non-linéarité dans notre CNN, puisque la

b) Couche de pooling

Une architecture atypique d'un réseau convolutif se compose de trois types de couches différentes. D'abord une couche convolutive pour générer un ensemble d'activations linéaires ensuite, on les fait passer à travers une couche d'activation non linéaire telle que Rectified Linear Unit (ReLu), enfin on utilise la fonction pooling

- Il permet de réduire progressivement la taille des représentations afin de réduire la quantité de paramètres et de calcul dans le réseau et, par conséquent, de contrôler également le sur-apprentissage.
- Il permet l'invariance aux petites translations
- Utile lorsqu'on préfère savoir si une caractéristique est présente plutôt que la région de sa présence.
- Plusieurs types de pooling diffèrents (MAX pooling (très populaire), AVG pooling)

Après avoir extrait les caractéristiques des entrées, on attache à la fin du réseau un perceptron ou bien un MLP. Le perceptron prend comme entrée les caractéristiques extraites et produit un vecteur de N dimensions ou N est le nombre de classe ou chaque élément est la probabilité d'appartenance à une classe. Chaque probabilité est calculée à l'aide de la fonction softmax dans le cas où les classes sont exclusivement mutuelles.

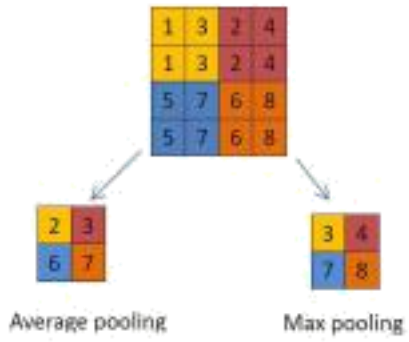


Figure 9: (à gauche) Average pooling, (à droite) Max Pooling

Ainsi dans notre cas, Le traitement d'images à travers l'extraction des caractéristiques et la segmentation en séquence d'entrée des images RGB se fait automatiquement à travers les couches de convolution et de pooling de nos modèles.

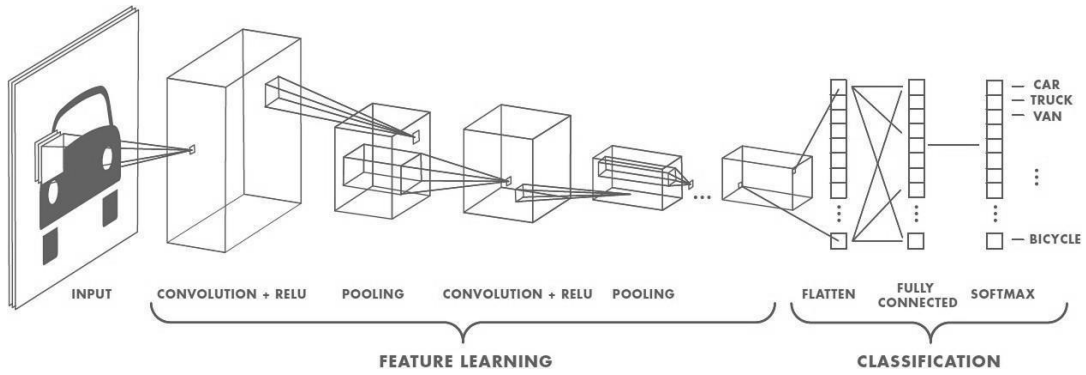


Figure 10: Apprentissage des fonctionnalités

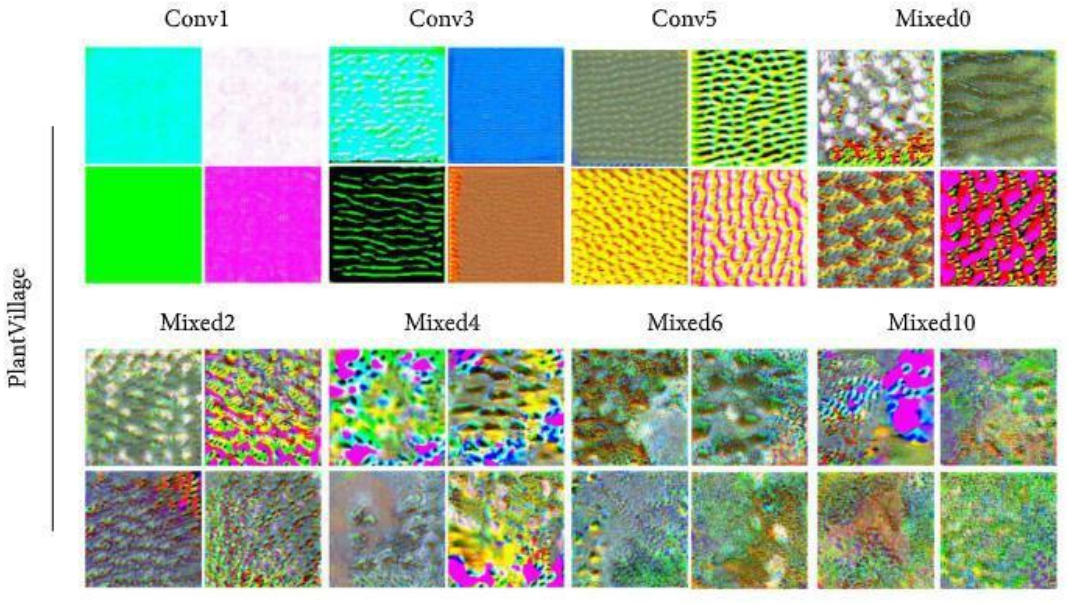


Figure 11:Visualisation des fonctionnalités.

II.2.2- implémentation de la reconnaissance faciale :

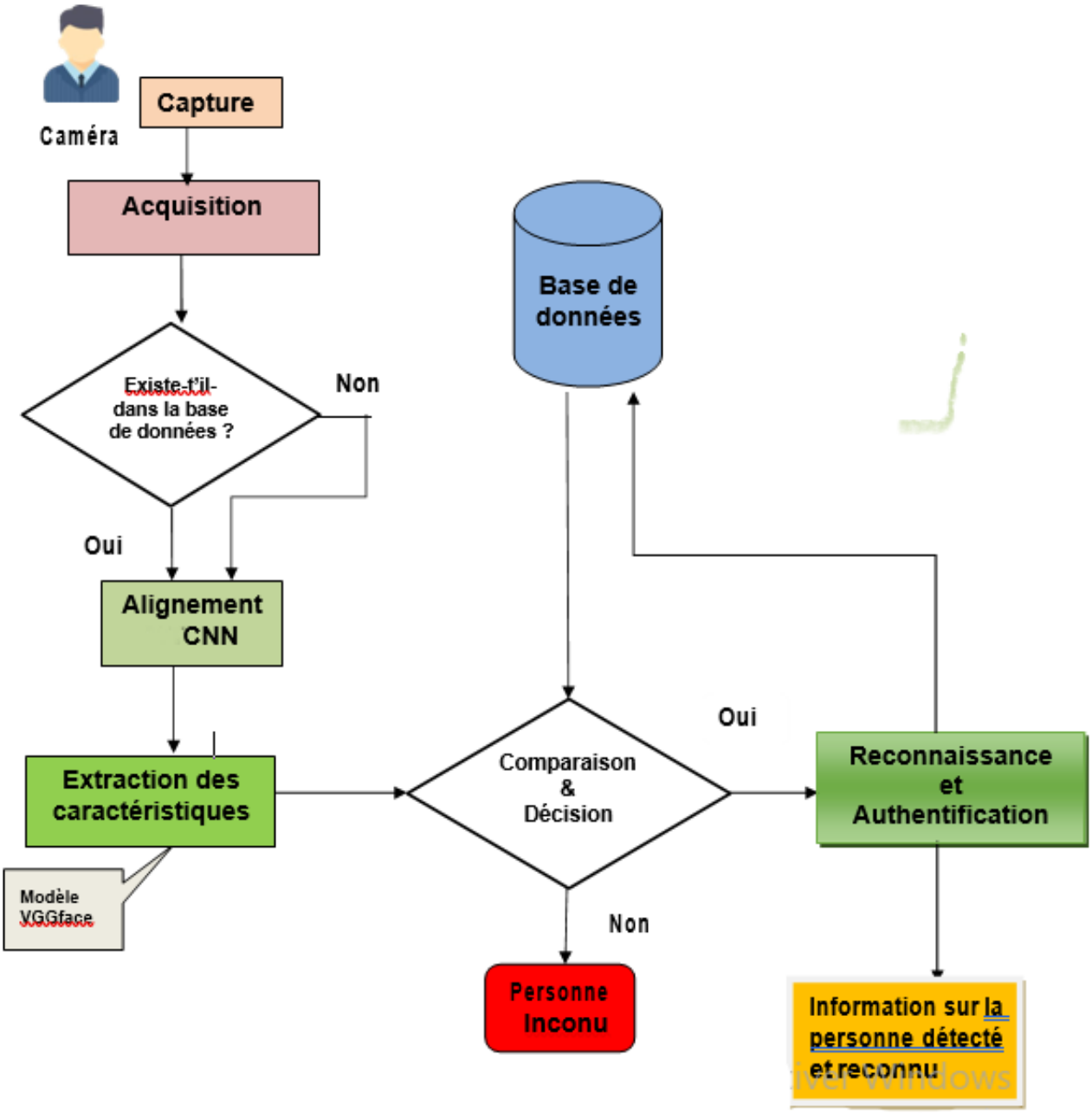


Figure 12: étape de la reconnaissance faciale

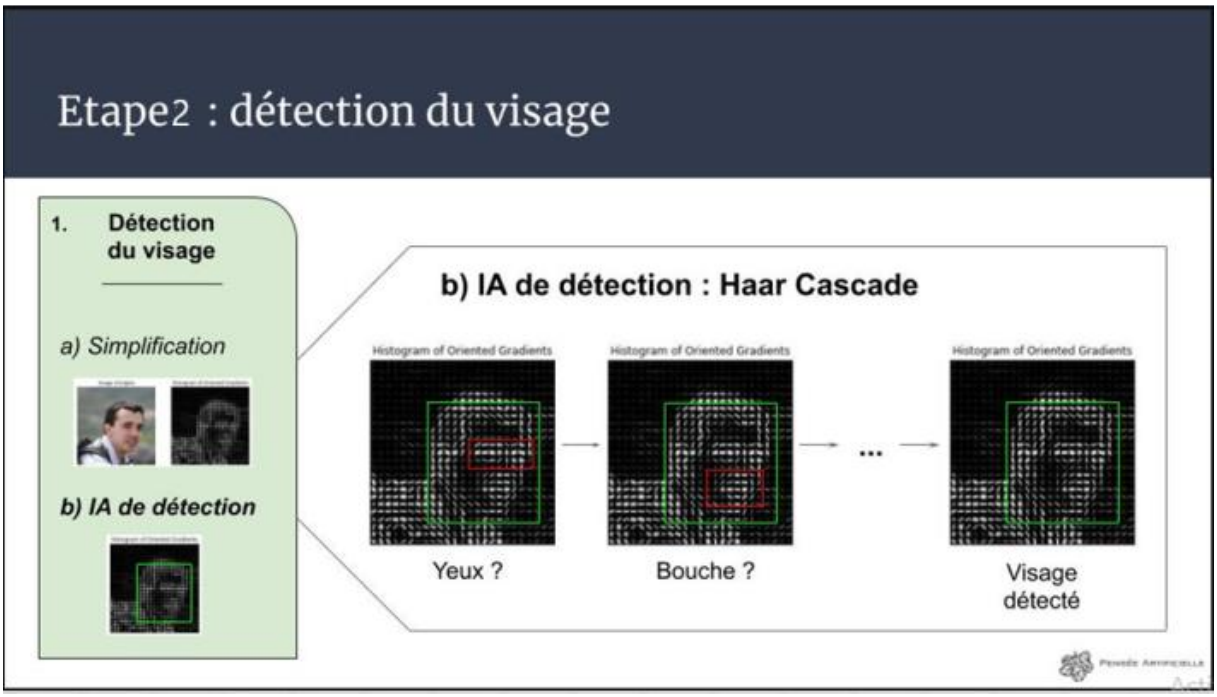
a- Capture

Cette étape consiste acquérir les informations (images) et les transférer vers l'unité de traitement. Elle est une étape très cruelle dans les systèmes de reconnaissance. En effet, avoir des images de bonne qualité en référence améliore les performances de

reconnaissance. Il faut réussir à capter l'information pertinente sans bruit. Il existe plusieurs types de capteurs pour l'acquisition du visage qui se classe selon leur mode de fonctionnement, leurs domaines de sensibilité spectrale et leur mode d'acquisition. On trouve sur le marché les capteurs classiques d'image à 2D tels que : les CCD (Couple charged device) ou CMOS pour capturer des images dans le spectre visible et/ ou proche-infrarouge, ou les capteurs thermiques qui permettent une acquisition dans l'infrarouge. Il existe des capteurs qui nous donnent une image avec l'information 3D, cela se fait par des scanners 3D, où la mesure de la profondeur est réalisée grâce à un rayon laser balayant la scène ou par stéréo vision. Chaque type de capteur présente des avantages et des inconvénients. Dans la reconnaissance de visage on peut utiliser les capteurs 3D par exemple pour s'affranchir des problèmes de pose. Mais leur prix excessif ne permet pas une utilisation à grande échelle. Les capteurs en proche infrarouge sont utilisés pour éliminer les problèmes de l'illumination (Walid Hizem ; 2009, p.10). Dans le cadre de ce travail, nous avons effectué nos tests de capture avec la webcam de notre ordinateur pour les premiers tests et enfin la caméra de notre téléphone ;

b- détection du visage dans une image

Après avoir capturé l'image contenant un visage, la deuxième étape consiste à l'extraire de l'image. Cette deuxième étape est cruciale, et c'est celle qu'il manquait à Woodrow Bledsoe pour que sa première IA de reconnaissance faciale soit autonome !



D'après notre schéma, dans cette étape nous devons :

- Convertir l'image en niveaux de gris
- Appliquer l'algorithme HOG (Histogram of Oriented Gradients) pour simplifier l'image
- Envoyer cette image à l'algorithme Haar Cascade qui s'occupera de trouver les visages

En effet nous convertissons ces images en niveaux de gris pour la préparation des données d'entrées car l'algorithme est entraîné à trouver les images en niveaux de gris. Il est donc hors de question de lui fournir des images en couleur car il ne s'en sortira pas aussi bien.

Pour le Haar Cascade, nous utilisons la version fournie directement par OpenCV. Nous commençons donc par charger notre fichier haarcascade et par le configurer en indiquant comment il doit fusionner les visages qu'il identifie (en effet, il va trouver plusieurs fois le même visage en décalant simplement sa zone de quelques pixels) :

```
        if len(faces) > 0:
            # Draw a rectangle around the faces
            for (x, y, w, h) in faces:
                cv2.rectangle(image, (x, y), (x+w, y+h), (0, 25
            (x, y, w, h) = faces[0]
            center_x = x+w/2
            center_y = y+h/2
            height, width, channels = im.shape
            b_dim = min(max(w,h)*1.2,width, height)
            box = [center_x-b_dim/2, center_y-b_dim/2, center_x
            box = [int(x) for x in box]
            # Crop Image
            if box[0] >= 0 and box[1] >= 0 and box[2] <= width
                crpim = im[box[1]:box[3],box[0]:box[2]]
                crpim = cv2.resize(crpim, (224,224), interpolat
                print("Found {0} faces!".format(len(faces)))
                return crpim, image, (x, y, w, h)
    return None, image, (0,0,0,0)
```

Puis dans un second temps on va tracer des rectangles autour de tous les visages trouvés et on va découper l'image autour du premier. Puis découper tous les visages et les traiter en parallèle, rien ne vous en empêche (à part la puissance de votre ordinateur).

```python
def auto_crop_image(image):
    if image is not None:
        im = image.copy()
        # Load HaarCascade from the file with OpenCV
        faceCascade = cv2.CascadeClassifier("haarcascade_fronto

        # Read the image
        gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)

        # Detect faces in the image
        faces = faceCascade.detectMultiScale(
            gray,
            scaleFactor=1.1,
            minNeighbors=5,
            minSize=(30, 30)
        )
        faces = faceCascade.detectMultiScale(gray, 1.2, 5)
```

Grâce à cette méthode, on est donc en mesure de trouver tous les visages qui sont dans une image, de les encadrer, puis de découper l'image autour du premier (le plus en haut à gauche) pour procéder aux traitements suivants.

c- découpage et déformation du visage

On vient à l'instant de découper le visage qui était dans notre image. Haar Cascade centrant ses zones autour des visages, ces derniers sont automatiquement centrés et bien alignés s'ils se tiennent bien face à la caméra. Nous n'avons donc rien de particulier à faire ici, et si vous voulez retrouver le Dlib Shape Predictor (qui déforme les visages). Dans notre cas puisque, nous fonctionnons sur un CPU nous n'allons pas utiliser dlib shape predictor mais plutôt un autre algorithme permettant d'exercer la déformation du visage comme le fais aussi le Dlib Shape Predictor

d- Analyse du visage(extraction des caractéristique) : phase d'apprentissage

Dans cette section nous attaquons le cœur de la reconnaissance faciale qui va nécessiter beaucoup de code. En effet, pour la phase d'apprentissage nous allons utiliser le modèle prédéfinit VGG face. Le modèle VGG-face permet de classer les images en 1000 catégories d'Object entre autres le visage humain. Ce réseau utilise une taille d'image en entré de 224*224*3. La valeur de 3 spécifie le nombre de canaux de couleur qui indique que le traitement s'effectue sur des images en RVB. L'architecture de VGG-face est illustré par le schéma ci-dessous :

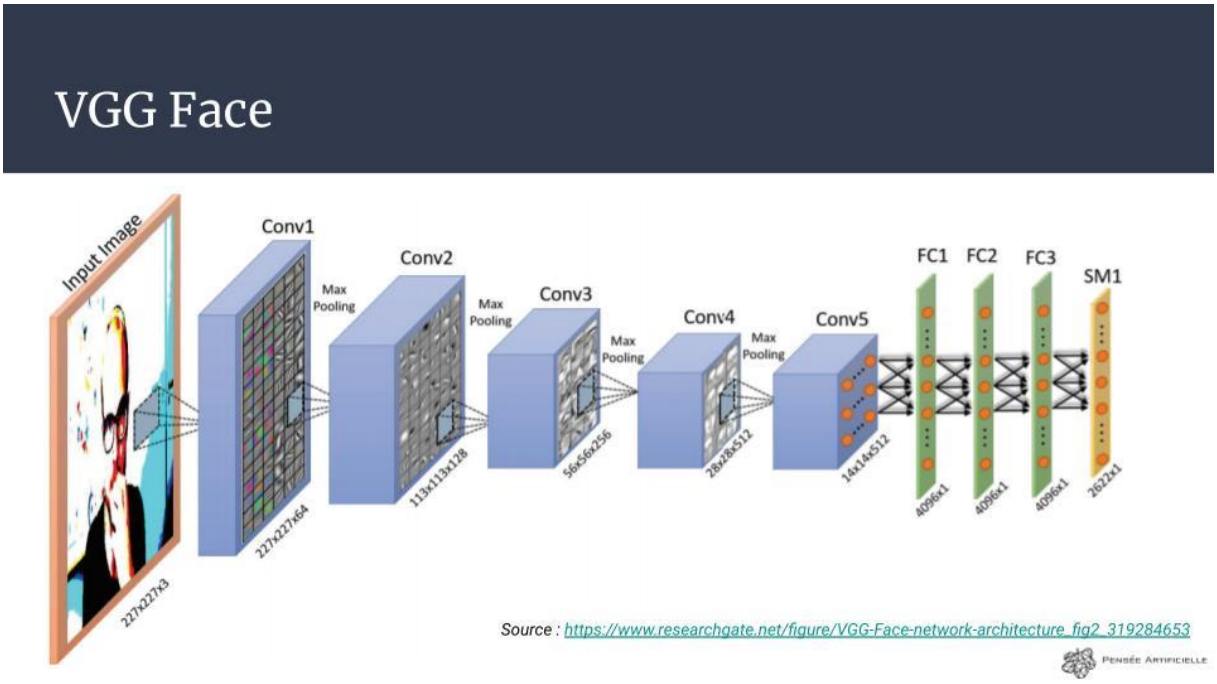


Figure 13: structure du réseau convolutif VGG face

Chaque couche de convolution utilise des filtres de taille 3*3, déplacés avec un pas de 1 pixel. Le nombre de filtres varie selon le « bloc » dans lequel se trouve la couche. De plus, un paramètre de biais est introduit dans le produit de convolution pour chaque filtre. Chaque couche a pour fonction d'activation une ReLU. Autrement dit, il Ya toujours une couche de correction ReLU après une couche de convolution. L'opération pooling est réalisé avec des cellules de taille 2*2 pixels et un pas de 2 pixels. Les deux premières couches entièrement connectées calculées sont des vecteurs de taille 4096, et sont chacune suivies d'une couche ReLU. La dernière couche entièrement connectée renvoie le vecteur de probabilités de taille 1000(le nombre de classes). De plus, ces trois couches utilisent un paramétre de biais pour chaque élément du vecteur en sortie.

Bien que le modèle VGG-face soit déjà un modèle déjà entraîné, il est important pour nous de le reprogrammé

Nous allons tout d'abord charger le modèle VGG face. Elle se fait en deux phases :

- Construction du modèle de réseau convolutif qui est identique à VGG
- Chargement des poids de toutes les variables du réseau, qui sont sauvegardées dans vgg-face.mat, et que l'on applique au modèle que l'on a réécrit

e- trouvons maintenant le vecteur le plus proche dans la base de données :

Elle va se faire en deux étapes. Tout d'abord nous allons chargé notre base de donnée

```
def generate_database(folder_img = "images"):
    database = {}
    for the_file in os.listdir(folder_img):
        file_path = os.path.join(folder_img, the_file)
        try:
            if os.path.isfile(file_path):
                name = the_file.split(".")[0]
                img = cv2.imread(file_path)
                crpim, srcimg, (x, y, w, h) = auto_crop_image(img)
                vector_image = crpim[None,...]
                database[name] = featuremodel.predict(vector_image)[0,:]
        except Exception as e:
            print(e)
    return database
```

- On parcourt le dossier /images
- Pour chaque image trouvée, on extrait le visage

- Puis on réalise une prédiction dessus (i.e. on génère un vecteur de 128 nombres grâce à notre CNN)
- Et on stocke ce vecteur dans un dictionnaire qui va représenter notre base de données !

Il ne reste plus qu'à faire :

```
db = generate_database()
```

Pour générer les vecteurs de toute notre base.

Cherchons dans la base de données à qui appartient l'image

Dernière étape de notre reconnaissance faciale, on dispose d'une base de données de vecteurs et l'on cherche celui qui est le plus proche du vecteur issu de la caméra.

Plusieurs méthodes sont possibles :

- Utiliser un algorithme de Machine Learning, qui va par exemple grouper les vecteurs dans l'espace (on parle de clustering) ou construire une frontière qui va les séparer les uns des autres (avec Support Vector Machine notamment)
- Ou alors, calculer soit la distance entre les vecteurs soit l'angle entre les vecteurs (solution que nous allons privilégier) et dire que deux vecteurs sont proches si leur angle est faible

III. Outils nécessaires à la réalisation de notre projet :

III.1- le software :

III.1.1 – Tensorflow :

Elle est une bibliothèque open-source développée par l'équipe Google Brain qui l'utilisait initialement en interne. Elle implémente des méthodes d'apprentissage automatique basées sur le principe des réseaux de neurones profonds (deep learning)

Figure 14: logo de tensorflow

I.1.2- keras :

Keras est une bibliothèque open source écrite en python et permettant d'interagir avec les algorithmes de réseaux de neurones profonds et de machine Learning, notamment Tensorflow et Theano. Elle a été initialement écrite par François Chollet.

Figure 15: logo de Keras

I.1.3- nympy

Est une bibliothèque permettant d'effectuer des calculs numériques avec Python. Elle introduit une gestion facilitée des tableaux de nombres, des fonctions sophistiquées (diffusion), on peut aussi l'intégrer le code C / C ++ et Fortran.

I.1.4 opencv

Est une bibliothèque proposant un ensemble de plus de 2500 algorithmes de vision par ordinateur spécialisé dans le traitement d'images, accessible au travers d'API pour les langages C, C++, et Python. Elle est distribuée sous une licence BSD (libre) pour les plateformes Windows, GNU/Linux, Android et MacOS, nous avons utilisé cette bibliothèque pour la détection du visage à partir des images introduites.

Figure 16 : Logo opencv

I.1.5- haarcascade_frontalface_default.xml

Une cascade de Haar est frontalement un classificateur utilisé pour détecter des objets particuliers à partir de la source. L'haarcascade_frontalface_default.xml est une cascade haar conçue par opencv pour détecter la face frontale. Une cascade Haar fonctionne en formant la cascade sur les milliers d'images négatives avec l'image positive superposée. La cascade de Haar est capable de détecter des caractéristiques de la source

I.1.6- SciPy

SciPy : réservée aux calculs scientifiques, dont le traitement du signal (on s'en servira surtout pour la 4e partie de recherche dans la base de données)

III.2- le hardware

Pour la réalisation de notre projet nous allons faire un montage comprenant :

a. La carte de commande et de contrôle : c'est le microcontrôleur Arduino méga 2560

Tout d'abord, nous devons revenir à l'origine d'Arduino. Elle est une carte électronique programmable est utilisée comme microcontrôleur pour la conception et le contrôle de composants électroniques, mécaniques, domotiques ou robotiques. En effet, grâce à Arduino, vous pouvez créer des systèmes amateurs ou professionnels intelligents, tels que des systèmes de contrôle pour divers composants de la maison. Grâce à Arduino, vous pouvez aussi utiliser votre smartphone comme télécommande, par exemple pour allumer ou éteindre les lumières de la maison, ou pour atténuer ou augmenter les volets électriques, régler la température et la distance de la maison en contrôlant le chauffage, etc.

Les cartes Arduino ont plusieurs modèles telles que la Arduino UNO R3, la plus connu et utiliser, ajoutons aussi la Arduino Nano. Mais l'Arduino Méga est le modèle le plus perfectionné et puissant de la célèbre carte électronique. Elle permet d'effectuer un maximum

d'actions et délivre un potentiel tel, qu'il est possible de se pencher sur les montages les plus lourds et gourmands en code. Cette carte peut être utilisée par les amateurs confirmés, mais est principalement destinée aux experts qui pourront en faire un usage plus professionnel. La carte dispose d'un brochage spécifique par rapport aux autres cartes. Par rapport à d'autres cartes, la carte a une disposition de broches spécifique. Cela le rend incompatible avec certains composants.

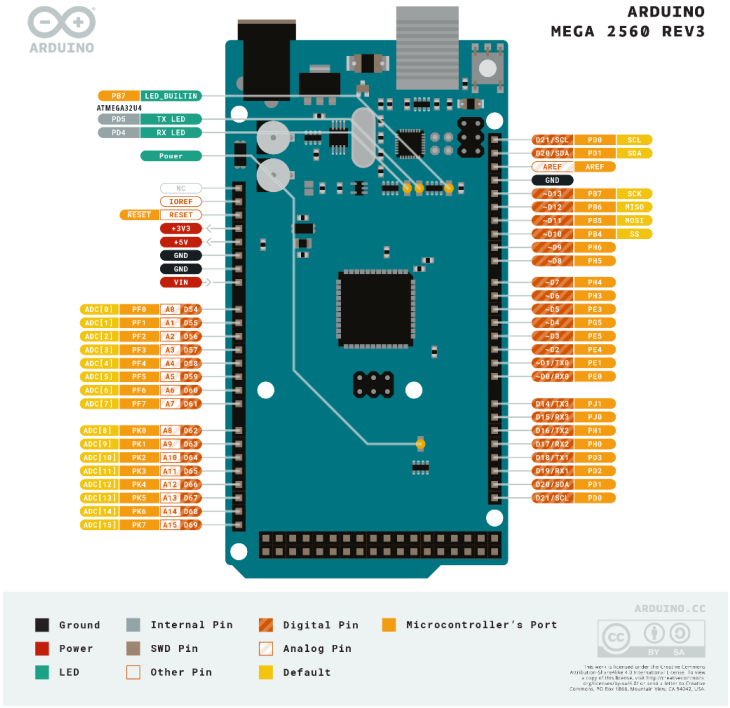


Figure 17: Représentation schématique de la MEGA

La carte Arduino MEGA 2560 est une carte à microcontrôleur basée sur un ATMEGA2560 et qui dispose de :

- 54 Broches numériques d'entrées/sorties dont 14 peuvent être utilisées en sorties PWM (largeur d'impulsion modulée),

- 16 entrées analogiques (qui peuvent également être utilisées en broches entrées/sorties numériques),
- 4 UART (port série matériel),
- Un quartz 16Mhz,
- Une connexion USB,
- Un connecteur d'alimentation jack,
- Un connecteur ICSP (programmation « in-circuit »),
- Un bouton de réinitialisation (Reset).

Sa fiche Technique est la suivante :

Microcontrôleur	ATMEGA2560
Tension de fonctionnement	5V
Tension d'alimentation (Recommandée)	7-12V
Tension d'alimentation (Limites)	6-20V
Broches E/S numériques	54 (dont 15 disposent d'une sortie PWM)
Broches d'entrées analogiques	16 (utilisables en broches E/S numériques)
Intensité max. disponible par broche E/S (5V)	40 mA (ATTENTION : 200mA cumulé pour l'ensemble des broches E/S)
Intensité maxi disponible pour la sortie 3.3V	50 mA
Intensité maxi disponible pour la sortie 5V	Fonction de l'alimentation utilisée - 500 mA max. si port USB utilisé seul
Mémoire Programme Flash	256 KB dont 8 KB sont utilisées par le bootloader
Mémoire SRAM (mémoire volatile)	8 KB
Mémoire EEPROM (mémoire non volatile)	4 KB
Vitesse d'horloge	16 MHz
LED_BUILTIN	13
Longueur	101.52 mm

Largeur	53.3 mm
Poids	

b. Le clavier

c. Un afficheur LCD

Pour afficher les informations de consommation du client, nous avons opté pour l'utilisation d'un écran LCD 16×2. Et notre écran pour des facilités de branchements utilisera un bus I2C.

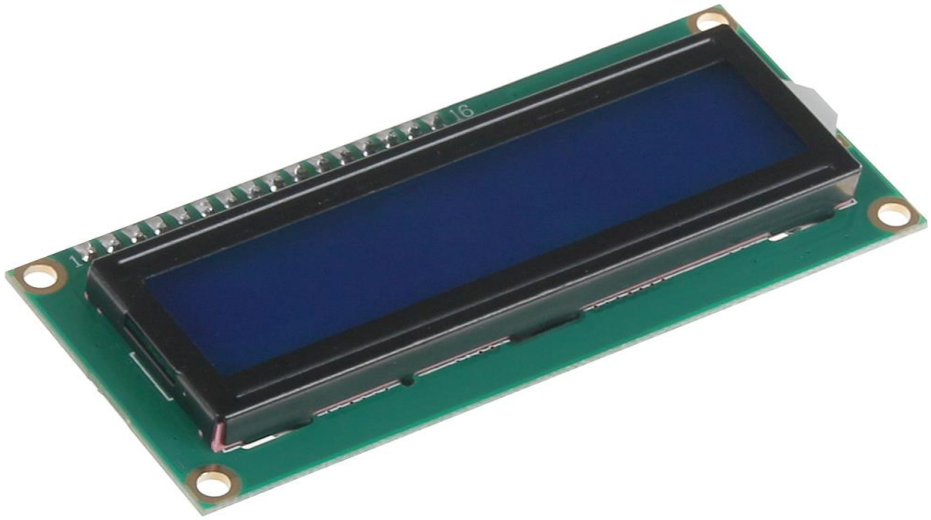


Figure 18: Afficheur LCD 16×2

Sa fiche technique est la suivante :

- Alimentation : 5 Vcc
- Interface I2C (adresse 0x27)
- Caractères blancs sur fond bleu
- Contraste ajustable via potentiomètre
- Dimensions : 80 x 38 x 18 mm

d. Le Relay DC/12V

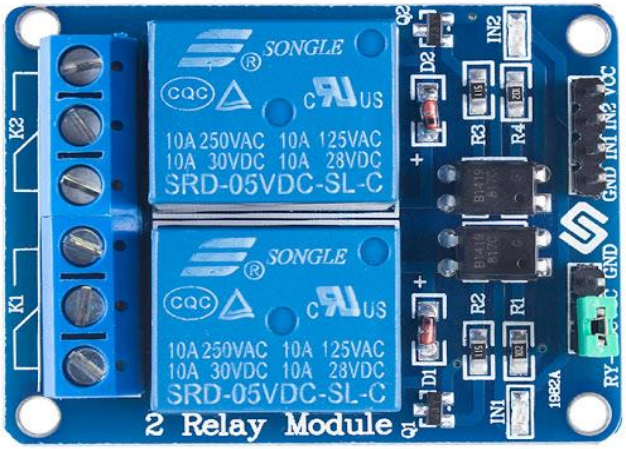


Figure 19: Relai 2 Modules

Sa fiche technique est la suivante :

- Sortie maximale du relais : DC 30V / 10A, AC 250V / 10A
- Dimensions : 50,6 x 38,8 x 19,3 mm
- Poids : 30g

e. Un ordinateur portable qui sera connecté avec la carte Arduino méga. Voici les caractéristiques de notre machine :

RAM	4GB
Processeur	2.10GHZ
Modèle du système	HP Probook

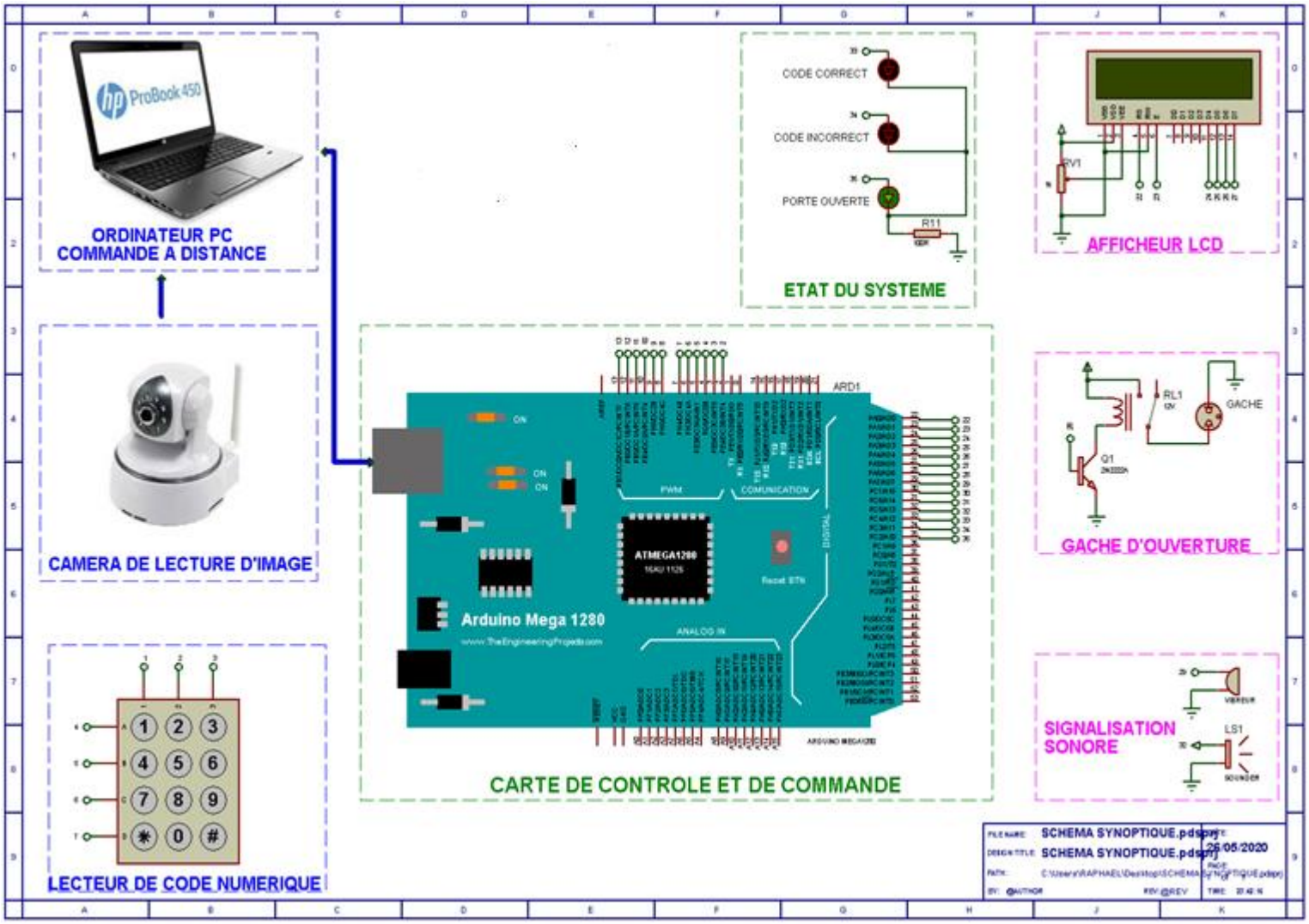


Figure 9 : synoptique de mon mémoire

Conclusion partielle :

A la fin de ce chapitre ou notre propos était de dégager les différentes méthodes utilisées dans la reconnaissance faciale, il en ressort que la méthode utilisée pour notre reconnaissance faciale est la méthode par le réseau de neurone convolutif qui se fait en plusieurs étapes. Après cela nous avons dit nous avons cité tous les outils utilisé pour la réalisation de notre projet de reconnaissance faciale. Dans le prochain chapitre nous allons présenter les différents résultats que nous avons obtenu dans la réalisation de notre projet

RESULTATS ET INTERPRETATION

Chapitre 3

Introduction :

Après avoir présenté la méthode utilisée pour la reconnaissance faciale. Il est important de présenter dans un premier temps les interfaces et dans un deuxième temps les résultats obtenus et de les interpréter

I. Présentation des différentes interfaces :

a. Interface de connexion

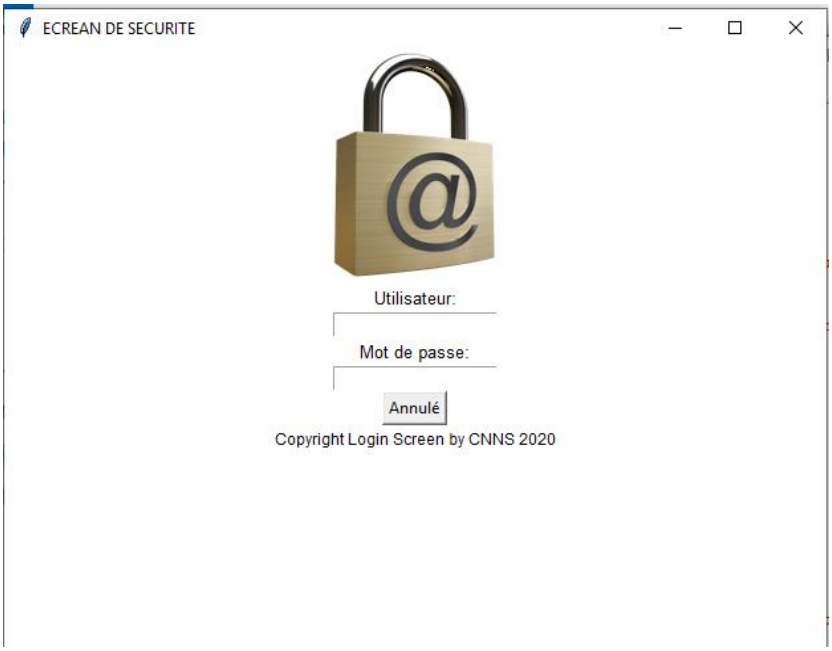


Figure 20: interface de connexion

b. Interface d'accueil :

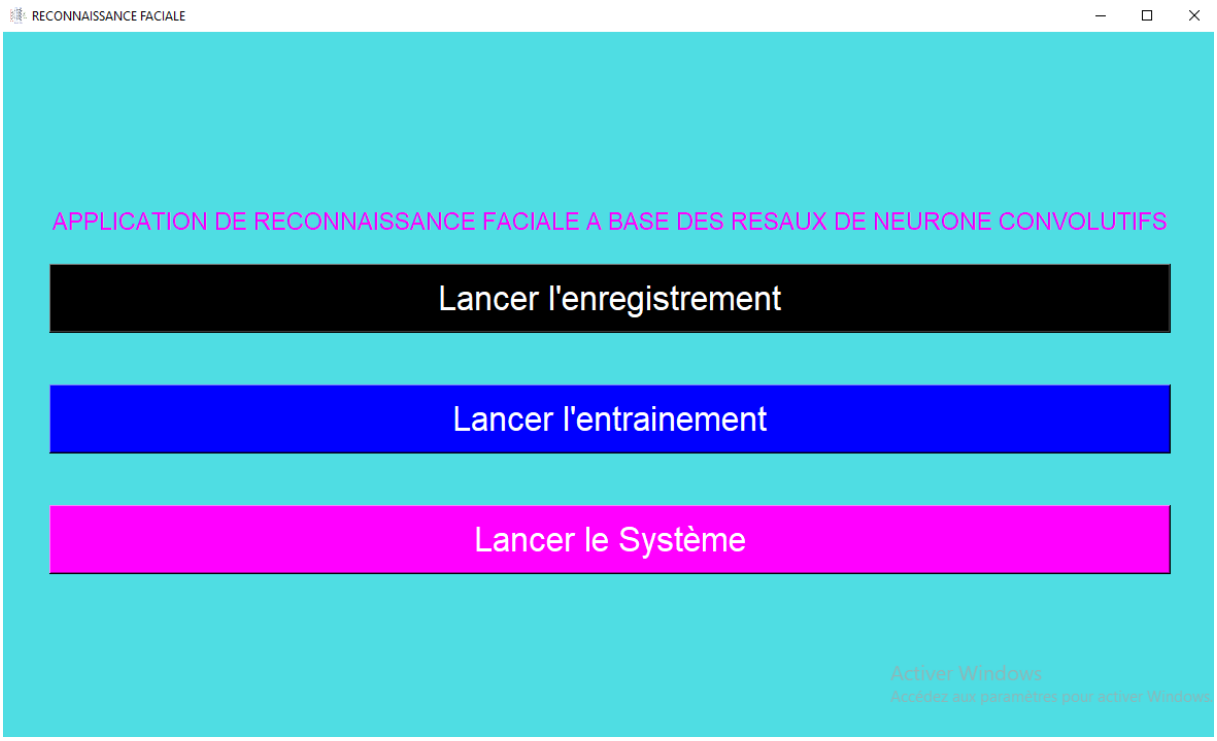


Figure 21: interface d'accueil

Cet interface contient un bouton permettant de faire l'enregistrement d'une nouvelle personne ; un bouton permettant de faire l'entrainement des données enregistrés et un dernier bouton permettant de lancer l'identification de la personne

II. Résultats d'expérimentation :

a. Notre jeu de données

Avant de présenter les résultats que nous avons obtenus, nous allons tout d'abord présenter la base de données que nous avons utilisé, c-a-d les personnes qu'on essaiera d'identifier grâce au programme. Dans le but de tester le programme de reconnaissance faciale nous avons pris deux personnes pour les tests, nous avons enregistré 300 photos de profil de six personnes déférentes. Ces images vont nous servir comme base de données d'apprentissage. Voici un exemple des images des personnes d'une personne que nous avons prise :

Figure 22: exemple de photos que nous avons pris de la première personne

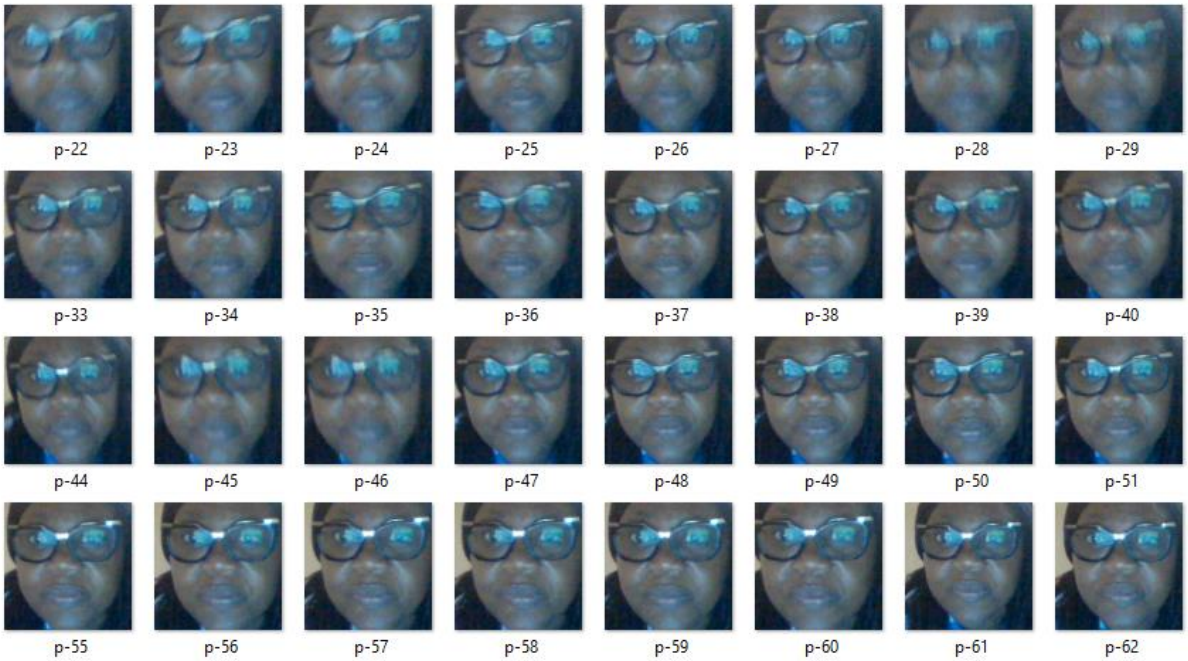


Figure 23: image de la deuxième personne prise

Notre travail a été donc de tester sur des images des personnes :

- Portant une barbe afin d'ouvrir le système
- Portant des lunettes afin d'ouvrir le système

b. Apprentissage :

Après la phase d'enregistrement c'est la deuxième étape de notre système.

```
[array([[133, 135, 138, ...,  79,  69,  65],
        [134, 139, 140, ...,  98,  91,  86],
        [141, 143, 143, ...,  89,  87,  94],
        ...,
        [ 95,  91,  84, ..., 161, 162, 163],
        [101,  97,  95, ..., 160, 161, 162],
        [106, 107, 105, ..., 158, 159, 159]], dtype=uint8)
 array([[157, 158, 160, ..., 177, 171, 168],
        [158, 158, 160, ..., 176, 181, 188],
        [158, 161, 162, ..., 177, 194, 195],
        ...,
        [ 45,  45,  50, ..., 161, 158, 150],
        [ 42,  42,  44, ..., 161, 157, 152],
        [ 38,  40,  41, ..., 164, 161, 144]], dtype=uint8)
 array([[129, 128, 128, ...,  55,  58,  59],
        [127, 128, 129, ...,  55,  56,  56],
        [128, 128, 130, ...,  55,  55,  55],
        ...,
        [163, 159, 152, ...,  93,  85,  82],
        [167, 165, 156, ...,  95,  86,  82],
        [166, 165, 145, ...,  90,  84,  80]], dtype=uint8)
 ...
 array([[139, 112,  95, ...,  92,  93,  94],
        [131, 110, 107, ...,  92,  92,  94],
        [144, 123, 115, ...,  92,  92,  92],
        ...,
        [ 95,  93,  92, ..., 123, 127, 126],
        [ 97,  96,  94, ..., 122, 125, 127],
        [ 97,  96,  96, ..., 121, 124, 127]], dtype=uint8)
 array([[150, 147, 146, ...,  87,  89,  93],
        [152, 149, 146, ...,  86,  87,  90],
        [150, 148, 145, ...,  88,  91,  91],
        ...,
        [109, 108, 107, ..., 117, 120, 120],
        [109, 109, 107, ..., 117, 117, 121],
        [110, 110, 109, ..., 118, 116, 122]], dtype=uint8)
 array([[141, 109,  93, ...,  94,  96,  99],
        [137, 107,  86, ...,  93,  93,  99],
        [134, 116,  91, ...,  93,  94,  98],
        ...,
        [ 96,  94,  92, ..., 132, 131, 131]
```

Figure 24: contenu de la figure de sortie de l'apprentissage

Le nombre d'époques est le nombre de fois où le modèle parcourt les données. Plus nous avons d'époques, plus le modèle s'améliorera, jusqu'à un certain point. Ensuite, le modèle cessera de s'améliorer à chaque époque. La figure suivante représente notre modèle qui entraîne les données, puis les valide. Une époque est le nombre de fois que le modèle s'entraîne sur l'ensemble de nos données.

c. Identification

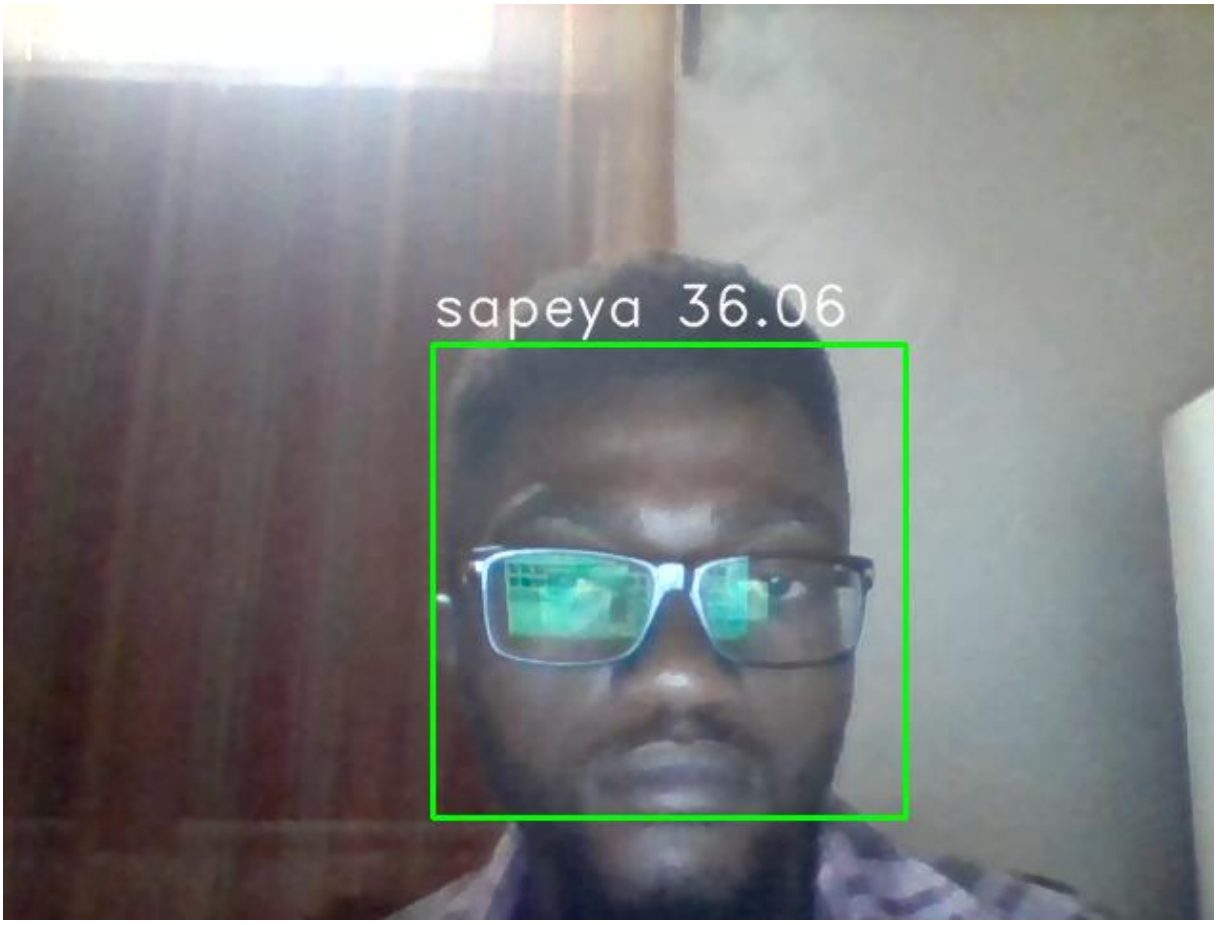


Figure 25: identification d'une personne devant le système

Figure 26: fausse prédiction

Les résultats obtenus sur le taux d'entrainement de la perte représenté dans le tableau cidessous nous ont donné 1.2742

Et les résultats sur la perte nous ont donné un taux de 0.3451

Figure 27: bonne prédiction

Les résultats obtenus sur les données tests représentés dans le tableau ci-dessous nous ont donné un taux de 0.8903. Et les résultats sur les données d'entrainement nous ont donné un taux de 0.6124.

Comparaison aux travaux déjà existants :

Tableau 2: tableau comparatif avec certains travaux[7]

Modèle	**Trainning accuracy**	**Validation accuracy**
SVM	43.36%	38.61%
CNN	72.25%	63.86%
CNN	90.11%	67.68%
CNN	89,03%	61 ,24%

Conclusion partielle :

Arrivé au terme de notre chapitre où notre propos était de présenter les différents résultats et de les interpréter, il en ressort que le taux de prédiction du réseau de neurone de convolution est bien meilleur que celui des support vector machine. La sécurité aujourd'hui étant primordiale aux jours d'aujourd'hui bénéficie donc d'un système plus fiable et plus sécurisé. Le travail étant donc terminé dans ce chapitre nous allons dans la prochaine section donné une conclusion tout en illustrant les perspectives

Conclusion générale :

La reconnaissance faciale joue un rôle très important dans la vidéosurveillance, elle permet de reconnaître les intrus et d'authentifier le personnel d'une entreprise ou d'une banque. Dans ce travail, nous avons réalisé un outil de reconnaissance faciale pour réduire l'accès dans les salles restreinte. La réalisation de ce projet nous a permis de maîtriser :

- Les outils de traitement d'images
- Les réseaux de neurones profond (réseaux de neurones de convolution)
- La programmation Arduino, python

Nous avons donc développé, un outil qui permet de reconnaître une personne en deux phases (code et reconnaissance faciale), pour cela nous avons suivi le processus de reconnaissance des formes à savoir :

- Création de la base de données
- Apprentissage
- Saisit du code qui lui est donné
- Détection d'une personne et identification de cette dernière

Nous prévoyons en perspectives de faire un système autonome qui n'est pas branché à la machine, d'utiliser une caméra rapide à la place de la webcam afin de pouvoir améliorer le rendu

MEMOIRES :

ASSUMANI NABONIBO [2014], conception et mise en œuvre d'un système de trois-tiers de gestion d'un parc informatique cas de la SNEL, mémoire inédit, ISC/KINSHASA

BOUDJELLAL Sofiane (2010), Détection et identification des personnes par la méthode biométrique, mémoire, inédit, UMMTO

Kalghoum ANWAR (2011), réalisation d'une application de gestion des présences via la reconnaissance faciale, mémoire, inédit, institut supérieur d'informatique et de gestion de Kairouan, Tunisie

PHITOS MBAA (2014), conception et realisation d'une plateforme d'e-learning : cas de l'institut supérieur de commerce de kinshasa, mémoire inédit, ISC/KINSHASA

Serge KOMANDA BASEMA (2010), l'identification des personnes par reconnaissances de visages pour la sécurité d'une institution bancaire, mémoire, inédit, ISP/Bukavu

Berredjem Achref [2019], La reconnaissance des individus par leur empreinte des articulations des doigts, mémoire, inédit, Guelma

MESROUA Djamel REBOUH Syphax [2017], Reconnaissance faciale par la télésurveillance, mémoire, inédit, Université Abderahmane Mira de Béjaïa

Mr. GHALI Ahmed [2015] : AMELIORATION DE LA RECONNAISSANCE PAR LE VISAGE, mémoire, inedit, ORAN MOHAMED BOUDIAF

SOUHILA GUERPI ABABSA (2008), Authentification d'individus par la reconnaissance de caractéristiques biométriques liés aux visages 2D/3D, thèse de doctorat en sciences de l'ingénieur, Université EVRY Val d'Essone

Khayati Mouna,Mestiri Makram,Hamrouni Kamel ,Daoudi Mohamed(2016): détection et reconnaissance du visage par une caméra de profondeur, Ecole national d'ingénieurs de Tunis

Walid Hizem (2009), capteur intelligent pour la reconnaissance de visage, thèse de doctorat en électronique et informatique, Université pierre et marie currie de France

Reference bibliographiques :

[1] Arca S, Campadelli P, Lanzarotti R., «A Face Recognition System Based On Automatically Determined Facial Fiducial Points», Article 2005 de Pattern recognition p 432-443, 2005

[2] Yessaadi Sabrina et M. T. Laskri. "Un modèle basé Templates Matching/Réseau de neurones pour la reconnaissance des visages humains" P2. Groupe de recherche en intelligence artificielle, Département d'informatique, Université d'Annaba, 2005

[3] A. Bettahar, S.Fathi, Extraction des caractéristiques pour l'analyse biométrique d'un visage, Mémoire de Master académique, Ouargla, 5 / 06 / 2014

[5] http://www.gemalto.com/france/gouv/inspiration/biometrie,consulté le 08/03/2016]

[6] H.Daoui et A.Elomar et Bentaouza Meriem Chahinez , Identification de personne grâce à la reconnaissance faciale par la géométrie du visage et la classification, mémoire de master, Mostaganem, 2014/2015.

[7] Nicolas MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL et Amara AMARA "Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie" P1-11. Institut Supérieur d'Electronique de Paris (ISEP), département d'Electronique, 2006.

[8] S. Liu and M. Silverman, « A practical Guide to Biometric Security Technology », IEEE Computer Society, IT Pro-Security, January-February 2001.

[9] A.K .Jain, L. Hong et S. Pankanti, « Biometrics: PromisingFrontiers for Emerging Identification Market », Communications d'ACM, Février 2000, pp. 91-98.]

[10] F. Perronnin et J.-L. Dugelay, « Introduction à la Biométrie : Authentification des Individus par Traitement Audio-Vidéo », l'Institut Eurocom, Département des Communications Multimédia, Revue Traitement du Signal, Vol. 19, No. 4, 2002.

[11] Futura High-Tech », http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/informatique-frappe-clavier-outil-biometrique-prometteur-41010/, Consulté le 29 Décembre 2014 à 10h27.

[12] Commission Technique de Sécurité Physique, « Techniques de Contrôle d'Accès par Biométrie », Dossier Technique, Club de la Sécurité des Systèmes d'Information Français, Juin 2003.

[13] S. Boudjellal, « Détection et Identification de Personne par Méthode Biométrique », Mémoire de Magister en Electronique, Option : Télédétection, Université Mouloud Mammeri, Tizi-Ouzou, Soutenu le 06 Juin 2012.

[14] TURK M. A. et PENTLAND A. P.: Face recognition using eigenfaces. IEEE Comput. Sco. Press, p. 586-591, June 1991

[15] Moad Benkiniouar, Mohamed Benmohamed. "Méthodes d'identification et de reconnaissance de visages en temps réel basées sur AdaBoost" Article P2-3,2005

[16] K. Etemad, R. Chellappa, Discriminant Analysis for Recognition of Human Face Images, Journal of the Optical Society of America A, Vol. 14, No. 8, August 1997, pp.1724-1733

[17] W.Hizem, « Capteur Intelligent pour la Reconnaissance de Visages », Thèse de Doctorat, Option : Informatique/Electronique, Institut National des Télécommunications et Université Pierre et Marie Curie, Paris, 2009].

[18] A. Chaari, « Reconnaissance de Visages par Réseaux d'Ondelette de Gabor », Thèse de Doctorat, Discipline : Automatique, Génie Informatique, Traitement du Signal et des Images, Université Lille 1, France, Université Sfax, Tunisie, Soutenue le 08 Décembre 2009.

[19] W.Zhao, R.Chellappa, P.J.Phillips, « ACM Computing Surveys », Vol. 35, No. 4, December 2003, pp. 399–458

[20] G. Guo, S.Z. Li, K. Chan, Face Recognition by Support Vector Machines, Proc. of the IEEE International Conference on Automatic Face and Gesture Recognition, 26-30 March 2000, Grenoble, France, pp. 196-201

[21] Fabien Cardinaux, Conrad Sanderson, and Samy Bengio "User Authentication via Adapted Statistical Models of Face Images", In the IEEE Transaction on Signal Processing. Vol. 54, Issue 1, Jan 2006, Pages: 361-373

[22] A.V. Nefian, M.H. Hayes III, Hidden Markov Models for Face Recognition, Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP'98, 12-15 May 1998, Seattle, Washington, USA, pp. 27212724