République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saâd DAHLAB, Blida

Faculté des sciences
Département d'informatique

Présenté par :

TAHAR DAHMANI Abdelkader

En vue d'obtenir le diplôme de master
Domaine : Mathématique et informatique

Filière : Informatique
Spécialité : Informatique
Option : Ingénierie de logiciel

Sujet :

Indexation et recherche d'images pour la vidéosurveillance intelligente

Promotrice : Mlle BENBLIDIA Nadjia
Encadreur : Mlle Reguieg F.Zohra
Présidente : Mme Bensettiti Souad
Examinateurs : Mlle Ameur khadidja

Laboratoire de Recherche Des Systèmes Informatique
(LRDSI)

Promotion 2013/2014

Remerciement

Tout d'abord, nous tenons rendre grâce à dieu tout puissant pour nous avoir donné le courage et la détermination nécessaire pour finaliser ce travail et le mener à terme.

On ne saurait ne pas remercier encore une fois nos parents respectifs qui, par leur amour et leur affection nous ont permis d'arriver là où nous somme aujourd'hui.

Nous remercions notre promotrice pour son aide précieuse, ces conseils avisés et ces idées riche.

Nous remercions le membre de jury pour nous avoir fait l'honneur de juger notre travail.

Nous sommes reconnaissantes à Tous nos enseignants Département informatique USDB

Nous tenons à remercier également et énormément nos amis ainsi toute personne qui nous a aidés de près ou de loin.

Merci.

Mr Abdelkader

Dédicaces

C'est avec un immense plaisir que je dédie ce travail

A mes très chers parents qui sont toutes ma vie et tout ce que j'ai de plus cher au monde, en témoignage de ma reconnaissance infinie pour ses nombreux sacrifices.

Qu'ils trouvent en ce travail la preuve de mon éternel amour et ma reconnaissance envers eux.

Que dieu les gardes et leur procure la santé et le bonheur.

Ainsi qu'à mes sœurs Souhila ,Dalila , Manel , Hadjer

a en témoignage de ma grande

affection pour eux.

A mes chers grands parents, mes tantes, mes oncles et toute ma famille.

Aussi à mes amis Sans oublier mon ami Mustapha qui a été mon acolyte dans cette épreuve et toute sa famille.

Mr : Tahar Dhmani Adelkader

Résumé

Systèmes de vidéosurveillance dans le développement aujourd'hui de plus en plus chaque jour, car une proportion croissante de la population et la nécessité d'assurer leur sécurité, il y a deux types de vidéosurveillance normale et intelligente ou automatique.

vidéosurveillance normale dépend de l'élément humain par la surveillance les caméras installée dans les lieux publics, et vidéosurveillance intelligente ou automatique s'appuyer pour identifier les personnes par le biais caractéristiques biologiques ou comportementales qui sont empreinte digitale, rétine, visage.....etc

Le but de notre travail est la réalisation un système de vidéosurveillance intelligent ou automatique basé sur la reconnaissance visage la seule personne requise, qui sont stocké dans une base de données des visages, et comparaison des ces visages avec les visages entrante par de les cameras si la comparaison est positif camera envoyé un alerte vers le serveur.

On utilise la reconnaissance visage, car le visage est la partie visible pour les Caméras contrairement empreintes digitales et la rétine. Et on utilisé l'algorithme viola et Jones pour la reconnaissance automatique des visages, elle est plus efficace que les autres algorithmes, et le taux d'erreur est faible

Ce projet est le début du développement des systèmes vidéosurveillance intelligente ou automatique.

Mots-clés: vidéosurveillance intelligente, Viola et Jones,

Abstract

Video-surveillance systems in development today growing every day, because increasing proportion of the population and the need to ensure their safety, there are two types of Video-surveillance systems normal and automatic or intelligent.

Normal surveillance depends on the human element through the surveillance cameras installed in public places. And Video-surveillance intelligent or automatic rely on to identify people through biological or behavioral characteristics which are fingerprint, retina, face……

The aim of our work is the realization of Video-surveillance systems intelligent or automatic based face recognition only person required, which are stored in a database of faces, comparison of these faces with entrant faces by the cameras if the comparison is positive camera sent a warning to the server.

We use Face Recognition, because face is visible for Cameras, unlike fingerprints and retina, and we used the viola and Jones algorithm for automatic face recognition, it is more effective than the other algorithms, and the error rate is low.

This project is the beginning of the development of intelligent video surveillance systems or automatic.

Keywords: intelligent Video-Surveillance, Viola and Jones,

ملخص

أنظمة المراقبة اليوم في التطور متزايد كل يوم لتزايد نسبة السكان وضرورة تأمين سلامتهم فظهرت انظمة مراقبة , فمنها أنظمة مراقبة عادية ومنها ذكية .العادية تعتمد على العنصر البشري في المراقبة من خلال مشاهدة شاشات الكاميرات الموضوعة في أماكن عمومية. و أما الذكية أو آلية تعتمد على التعرف على الأشخاص من خلال مواصفات خاصة بالإنسان مثل بصمة اليد, شبكية العين و الوجه.....الخ

الهدف من عملنا هو انجاز نظام مراقبة ذكي او آلي يرتكز على التعرف على الوجوه المطلوبة فقط المخزنة في قاعدة البيانات و مقرنتها بالوجوه التي التقطتها الكمرات الشبكة اذا كان تطابق , ترسل كاميرا انذار للخادم .

استخدام الوجه لتعرف لأنه هو الجزء الظاهر للكمرات عكس بصمة و شبكية العين , و استعملنا خوارزمية فيولا و جونز لتعرف على الوجه هي أكثر فعالية من خوارزميات أ خرى , تعرف على الوجه في الوقت الحقيقي وهذا مفيد للإنذار المبكر و نسبة الخطأ ضئيلة.

يعتبر هذا المشروع بداية لتطوير أنظمة المراقبة الذكية أو آلية في المستقبل.

الكلمات المفتاحية : أنظمة المراقبة ذكية ، فيولا و جونز،

Sommaire

Liste des figures

Liste des tableaux

INTRODUCTION GÉNÉRALE

Introduction générale

La sécurité est une préoccupation de plus en plus importante au sein des entreprises et commence par l'accès à l'information. Pour se prémunir contre d'éventuelles personnes indélicates, une nouvelle technique de contrôle d'accès a fait son apparition et ne cesse de croitre depuis 1997. [26]

C'est pourquoi aujourd'hui de nombreuses recherches visent à prouver l'identité d'une personne en utilisant des caractéristiques biologiques ou comportementales qui lui sont propres : rétine, empreinte digitale, forme de la main, visage, vélocité de signature ….etc. La biométrie est la science qui regroupe l'ensemble de ces travaux et dispositifs. Dans le spectre de la biométrie, la reconnaissance de visages revêt un caractère particulier de part le grand nombre de travaux qui lui sont consacrés .En effet capturer une image d'un visage, en particulier à travers une caméra 2D , C'est donc une modalité biométrique facilement tolérée par les utilisateurs, et ceci d'autant plus que les ordinateurs sont équipés de plus en plus souvent de Camera , mais les performances de la reconnaissance faciale sont toujours bien ,en deçà de ce que l'on pourrait espérer pour de telles applications. L'augmentation des taux de reconnaissance.

La diminution des reconnaissances à tort et l'accélération des temps de réponse lors de la recherche dans les grandes bases de données biométriques sont les défis auxquels doivent faire face les algorithmes actuellement développés.

Objectif :

L'objectif de notre travail est la conception et la réalisation d'un système de Vidéosurveillance intelligente. Est un segment de l'industrie de la sécurité physique. Cette dernière inclut aussi le contrôle d'accès, la détection et le contrôle d'incendies, la gestion technique de bâtiments, les systèmes assurant la sécurité des personnes et la détection d'intrusion.

La vidéosurveillance consiste à surveiller à distance des lieux publics ou privés, à l'aide de caméras, le plus souvent motorisées, qui transmettent les images saisies à un équipement de contrôle qui les enregistre ou les reproduit sur un écran. Elle capte sur image les flux de personnes pour surveiller les allées et venues, prévenir les vols, agressions et fraudes, ainsi que pour gérer les incidents et mouvements de foule.

La vidéosurveillance intelligente, est une technologie qui permet, au moyen de logiciels, d'identifier automatiquement, dans des séquences vidéo, des objets, des comportements ou des attitudes spécifiques. Elle transforme la vidéo en données qui seront transmises ou archivées

pour permettre au système de vidéosurveillance d'agir en conséquence. Il pourra s'agir d'actionner une caméra mobile, dans le but d'obtenir des données plus précises de la scène ou tout simplement, d'envoyer une alerte au personnel de surveillance pour qu'il puisse prendre une décision sur l'intervention adéquate à apporter.

Les systèmes de vidéosurveillance intelligente utilisent des algorithmes mathématiques pour détecter des objets en mouvements dans l'image et filtrer les mouvements non pertinents. Ils créent une base de données consignant les attributs de tous les objets détectés et leurs propriétés de mouvements. La prise de décision par le système ou la recherche d'événements d'intérêt dans des séquences archivées se fait à partir de règles (par ex.: si une personne traverse une limite, envoyer une alerte …….. etc.).

CHAPITRE I

Biométrie et Reconnaissance des Formes

I.1. Introduction

Depuis plusieurs années des efforts importants sont fournis dans le domaine de la recherche en biométrie. Ce phénomène s'explique en partie par la présence d'un contexte international ou les besoins en sécurité deviennent de plus en plus importants et ou les enjeux économique sont colossaux

I.2. Pour quoi utiliser la biométrie ?

La biométrie a pou l'objet d'utiliser l'informatique pour identifier une personne ou en vérifier l'identité puis d'activer les privilèges attribués à cette personne .il existe de nombreuses autres application de la biométrie qui peut être utile dés qu'une identification de l'identité automatisée est requise.

Elle sert déjà dans certains cas à remplacer l'horodateur ainsi qu'a l'inscription à des prestations sociales et la surveillance de criminels habituellement, l'authentification biométrique sert à contrôler les privilèges d'accès

I.3. Qu'est ce que la biométrie ?

La biométrie est la science qui permet d'identifier automatique un individu en se basant sur ses caractéristique physiologique ou comportementales .généralement nous distinguons deux catégories de méthodes biométrique :

-les méthodes basées sur la caractéristique physique : telle que le visage, la voix, l'iris, la rétine, la forme de la main et de l'oreille, ADN

- les méthodes basées sur la caractéristique comportementale : comme la signature, la manière de marcher ou de taper sur un clavier.

Nous pouvons constater que le domaine de la biométrie est une véritable alternative aux mots de passe conventionnels qui permet de vérifier que l'utilisateur soit bien la personne qu'il prétend être ,Cette technologie est en pleine croissance et tend à s'associer à court terme ,aux technologies actuelles comme la carte à puce , le badge , la clé ……..etc. .

Le système d'authentification biométrique suppriment les risques de Perte, d'oubli de vol ou de duplication vu qu'ils se basent sur caractères physiologique ou les traits comportementaux automatiquement reconnaissables et qui sont unique à chaque individu.

I.4. Domaine d'application de la biométrie

La biométrie est appliquée dans plusieurs domaines et ses applications dont divisées en trois groupes principaux :

- Applications Commerciales : telles que l'accès au réseau informatique, la sécurité de données électronique, le commerce électronique, l'accès à l'entèrent, le contrôle d'accès physique, le téléphone portable ……etc
- Applications de gouvernement : telle que la carte nationale d'identification, le permis du conducteur, la sécurité sociale, le passeport ……..etc
- Applications Juridiques : telle que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus ……..etc

I.5 Système Biométrique

Un système biométrique est essentiellement un système de reconnaissances de formes qui fonctionne par l'acquisition des données biométrique à partir d'un individu , puis l'extraction d'un ensemble de caractéristique à partir des données acquises et enfin la comparaison de ces caractéristiques avec la signature dans la base de données

Le système valider l'identité d'une personne en comparant les données biométriques capturées à sa propre base de données, Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (Numéro d'Identification Personnelle), d'un nom d'utilisateur, d'une carte futée, etc., et le système conduit une comparaison d'un-à-un pour déterminer si la réclamation est vraie ou fausse.

Le système identifie un individu en recherchant les signatures (Template) de tous les utilisateurs dans la base de données, Par conséquent, le système conduit à plusieurs comparaisons pour établir l'identité d'un individu, (ou échoue si le sujet n'est pas inscrit dans la base de données du système) sans devoir être soumis à réclamer une identité.

I.6. Caractéristiques Communes des Systèmes Biométriques

La caractéristique commune à des systèmes biométrique sont les suivantes :

- Universelles (exister cher tous les individus).
- Unique (permettre de différencier un individu par rapport à un autre)
- Permanentes (autoriser l'évolution dans le temps)
- Enregistrables (collecter les caractéristique d'un individu avec l'accord de celui-ci)

- Mesurables (autoriser une comparaison future)
- Et si possible infalsifiables

I.7. Typologies des systèmes biométriques

Il ya trois catégories technologique de la biométrie, la première est l'analyse biologique comme les tests portants sur sang et l'ADN . la deuxième est l'analyse comportementale qui traite la dynamique de la signature la façon d'utiliser un clavier, la manière de marcher. en dernier nous avons l'analyse morphologique qui est la plus répandue maintenant et qui traite les empreintes digitales, forme de la main , les traits de visage , la voix , dessin du réseau veineux de l'œil

I.8. Erreurs de système biométrique

Un système biométrique fait deux types d'erreurs:

- Confusion des caractéristiques biométriques de deux personnes différentes pour être de la même personne

- Confusion des caractéristiques géométriques de la même personne pour être de deux personnes différentes

Ces deux types d'erreurs se nomment respectivement « faute d'acceptation » et « faute de rejet ». Il y a une relation entre le taux « faute d'acceptation » (TFA) et le taux « faute de rejet »(TFR) dans chaque système biométrique

En fait, TFA et TFR sont des fonctions du seuil t de système; si t est diminué pour rendre le système plus tolérant aux variations et au bruit d'entrée, alors TFA augmente. D'autre part, si t est augmenté pour rendre le système plus bloqué, TFR augmente en conséquence. Le diagramme dans la **figure I.1** montre la relation entre ces deux variables [3]

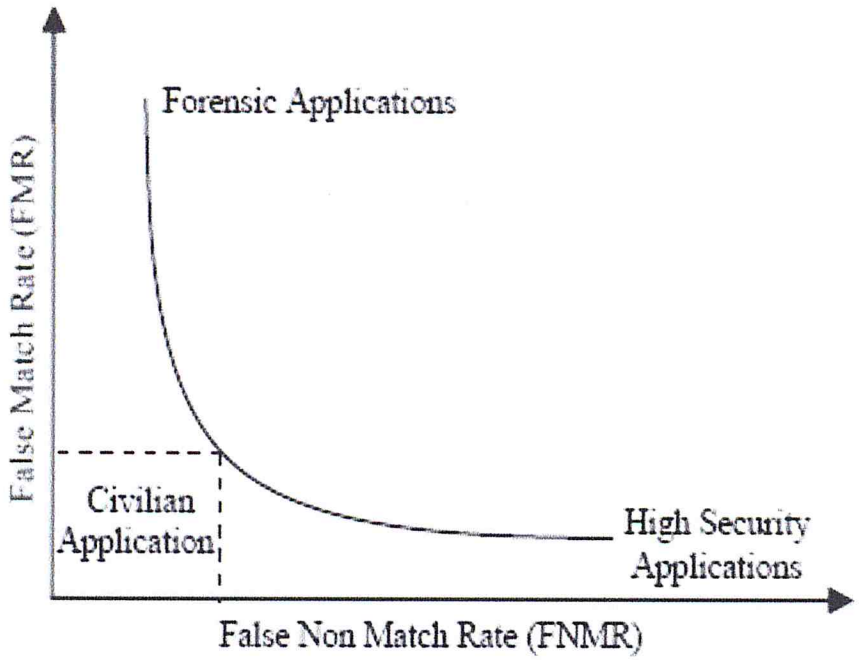


Figure I.1 : *Relation entre TFA et TFR [3]*

I.9. Comparaison les techniques biométriques

Il existe plusieurs des techniques biométriques dans la ***Figure I.2*** et elles sont utilisées dans diverses applications. Chaque technique biométrique a ses forces et faiblesses, et le choix dépend de l'application, Aucun technique biométrique répondre efficacement aux exigences de toutes les applications. En d'autres termes, aucune technique biométrique n'est optimale, La correspondance entre une technique biométrique et une application dépend du mode opérationnel de l'application et des propriétés de la caractéristique biométrique

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tableau I.1 Comparaison entre les techniques biométriques

Une brève comparaison de 9 techniques biométriques les plus utilisées ci-dessus Basées sur sept facteurs est fournie dans le tableau. L'applicabilité d'une technique biométrique spécifique dépend fortement des conditions du domaine d'application, Par exemple, il est bien connu que la technique basé sur l'empreinte digitale est plus précises que la technique basé sur la voix.

I.10.La Reconnaissance des Formes

La reconnaissance des formes s'intéresse à la conception et la réalisation des systèmes (matériels et logiciels) capables de percevoir et dans une certaine mesure d'interpréter des signaux capteurs dans le monde physique

Il s'agit donc de concevoir des systèmes automatiques ou semi-automatiques qui reconnaissent les formes qu'on leur présente

On veut reconstituer sur machine des fonctions typiquement humaines telles que

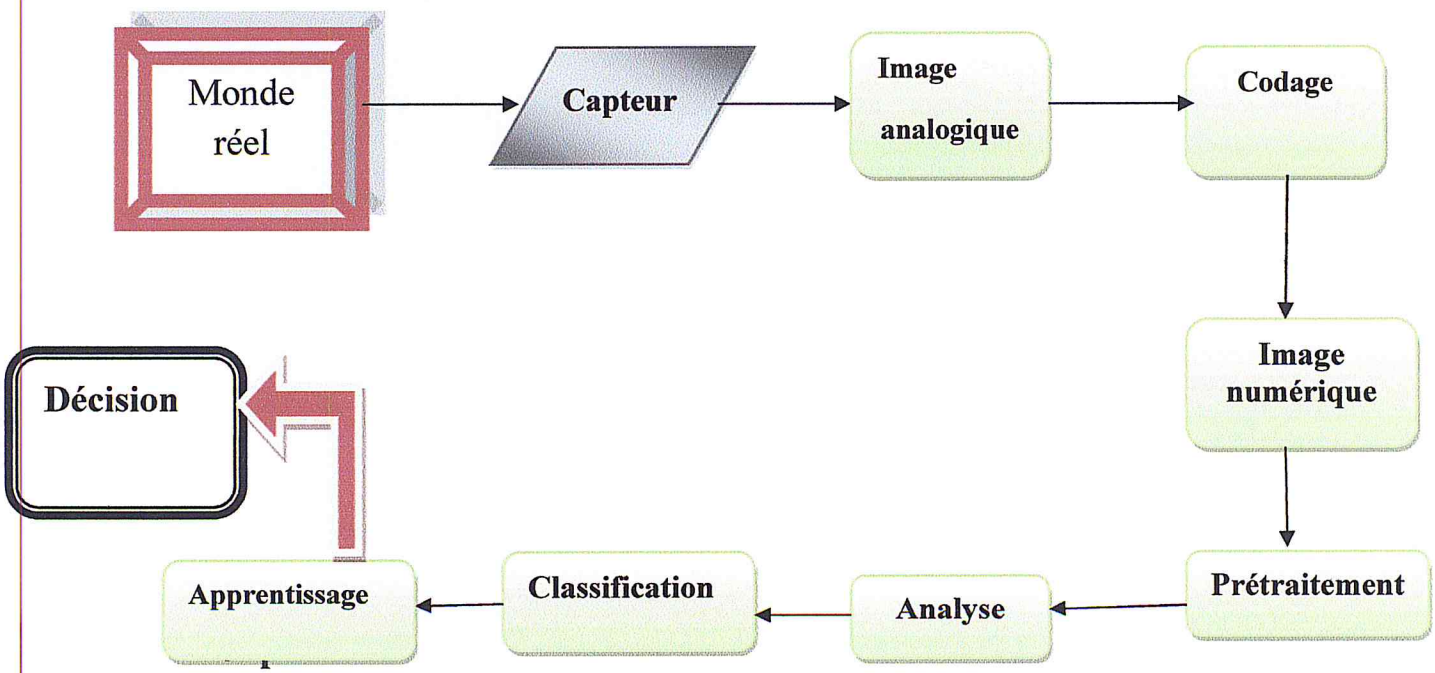
-La perception

-L'analyse

- L'interprétation

- La compréhension automatique qui relève de l'IA

I.11. Etapes de traitement d'un processus



C'est l'opération qui permet d'extraire du monde réel une représentation matricielle c'est-à-dire une image, cette opération peut être statique (Appareil photo, Scanner, etc.) ou dynamique (Caméra, Web Cam).

- **Prétraitement :**

Les données brutes issues des capteurs sont les représentations initiales des données, à partir des quelles des traitements permettent de construire celles qui seront utilisé pour la reconnaissance. L'image brute peut être affectée par différents facteurs causant ainsi sa détérioration, elle peut être bruitée, c'est à dire contenir des informations parasites à cause des dispositifs optiques ou électroniques. Pour pallier à ces problèmes, il existe plusieurs méthodes de traitement et d'amélioration des images, telle que: la normalisation, l'égalisation de l'histogramme, etc.... .

- **Analyse :**

Ici il s'agit de calculer un certain nombre de caractéristiques ou paramètres, ces mesures de différentes natures (géométrique, statistique, topologique, …) servent comme les seules données représentant la forme

*C'est l'extraction de l'information pertinente

-Image : contours, coins, périmètre, connexion (point de bifurcation), concavités, surfaces, couleur, texture, ……etc.

- Parole : fréquence fondamentale, énergie harmonique, etc.

- **Classification de la forme**

Dans cette étape on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. Le choix de ces informations utiles revient à établir un modèle pour le visage, elles doivent être discriminantes et non redondantes. Ces informations seront ensuite classées, en d'autres termes, affectés à la classe la plus proche, les individus ayant des similarités sont regroupés dans la même classe. Ces classes varient selon le type de décision.

- **Apprentissage**

L'apprentissage consiste à mémoriser les modèles calculées dans la phase analyse pour les individus connus. Un modèle est une représentation compacte des images qui permet de faciliter la phase de reconnaissance mais aussi de diminuer la quantité de données à stocker en quelque sorte l'apprentissage est la mémoire du système.

CHAPITRE II

La détection de visages

II.1.Introduction

La reconnaissance faciale est une tâche que les humains effectuent naturellement et sans effort dans leurs vies quotidiennes. La grande disponibilité d'ordinateurs puissants et peu onéreux ainsi que des systèmes informatiques embarqués ont suscité un énorme intérêt dans le traitement automatique des images et des vidéos numériques au sein de nombreuses applications, incluant l'identification biométrique, la surveillance, l'interaction homme-machine et la gestion de données multimédia. La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux avances rapides dans des technologies telles que les appareils photo numériques, Internet et les dispositifs mobiles, le tout associé à des besoins en sécurité sans cesse en augmentation.

II.2. Pourquoi choisir la reconnaissance de Visage ?

La reconnaissance faciale possède plusieurs avantages sur les autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser. Parmi les six attributs biométriques considérés par *Hietmeyer* les caractéristiques faciales marquent un score de compatibilité le plus élevé dans un *système MRTD* ("*Machine Readable TravelDocuments*") ce score étant basé sur plusieurs facteurs d'évaluation tels que l'enrôlement, le renouvellement des données, les requis matériels et la perception des utilisateurs (*Figure II.1*)

Idéalement, un système de reconnaissance faciale doit pouvoir identifier des visages présents dans une image ou une vidéo de manière automatique [4]

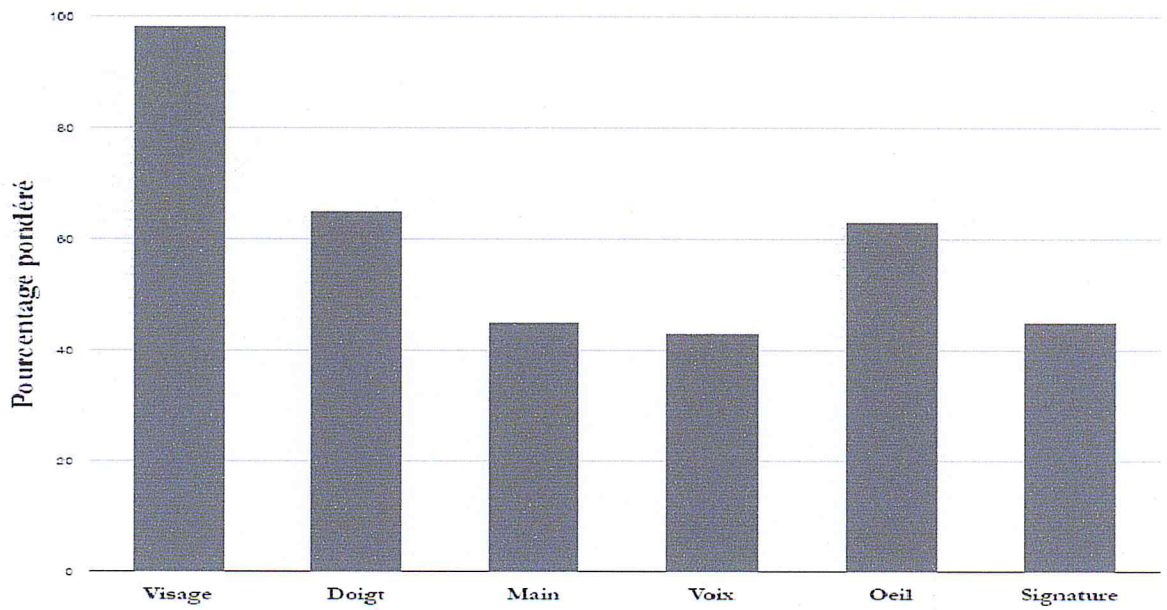


Figure II.1 : Scores de compatibilité pour différentes technologies biométriques dans un système MRTD. [4]

Le système peut opérer dans les deux modes suivants : authentification ou identification , on peut également noter qu'il existe un autre type de scénario de reconnaissance faciale mettant en jeu une vérification sur une liste de surveillance , où un individu est comparé à une liste restreinte de suspects , Le principe de fonctionnement de base d'un système de reconnaissance faciale (*Figure II.2*) , peut être résumé en quatre étapes : les deux premières s'effectuent en amont du système (« détection » et « normalisation du visage »)et les deux dernières représentent la *reconnaissance* à proprement dit (« extraction » et « comparaison des caractéristiques ») [4]

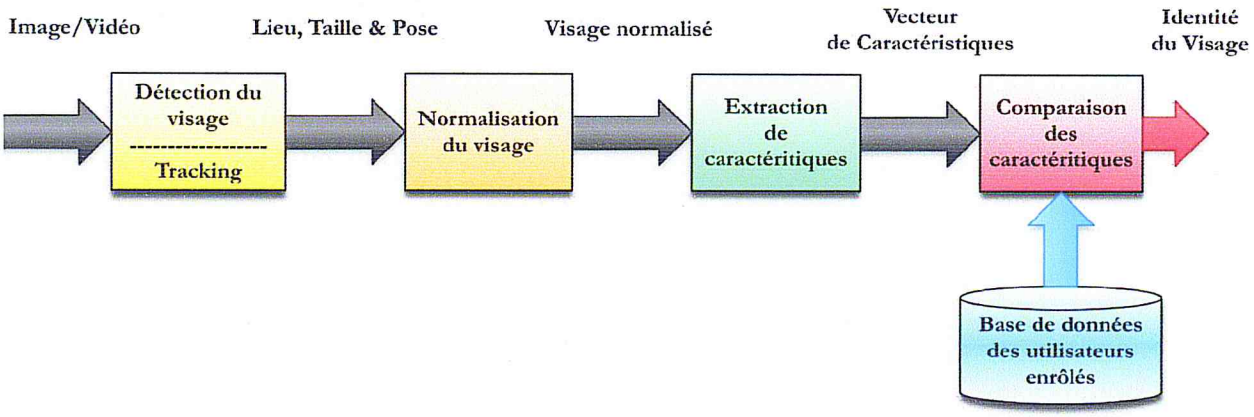


Figure II.2 Principe de fonctionnement de base d'un système de reconnaissance faciale [4]

II.3. Avantage et inconvénient de reconnaissance facial

II.3.1 Avantage

- Technologie bien acceptée par le public
- En position fixe et éclairée, les taux de reconnaissance sont effectivement très élevés.
- Technique peu coûteuse.
- Réduction des pertes financières reliées au vol d'identité

II.3.2 inconvénient

- Technologie sensible à l'environnement (éclairage, expression du visage).
- Technologie sensible au changement (barbe, moustache, chirurgie, perçage...).
- Les vrais jumeaux ne sont pas identifiés.

II.4. Le principe de la détection de visage

La détection automatique de visages prend son importance de point de vue qu'elle est à la base de la reconnaissance de visages dans une image ou dans une séquence images (vidéo) .

Le concept de base de la détection de visages est basé sur extraction des visage au travers de les séquence image (vidéo) puis à comparer chaque image de visage extraite avec une série de visages types dans un base de données

il est nécessaire que la détection de la présence ou non d'un visage dans une image soit basée sur des éléments stables et relativement descriptifs du visage humain et qui permettent ensuite de le reconnaître. Parmi ces éléments, on peut citer la forme du visage, la couleur de la peau, le contour des yeux, la forme du nez ou de la bouche... [5]

Mais en considérant des tailles, des orientations, des rotations et des éclairages différents il faudrait pouvoir comparer chaque image (visage détecté) extraite à des centaines de références. Si l'on rajoute les expressions faciales (sourires, grimaces,...), la détection de visages devient un problème difficile à traiter

-Bien que la plupart des visages soient structurellement semblables avec des caractères morphologiques communs (yeux, bouche, nez,...) placés selon une certaine configuration spatiale, il existe de grandes différences entre deux visages (forme du nez, couleur des yeux, couleur de peau,...).

- Certains caractères morphologiques peuvent être présents ou non selon les visages comme par exemple la moustache, la barbe, ...

-Certains caractères extérieurs peuvent déformer des caractères morphologiques comme par exemple le bronzage modifiant partiellement la couleur de la peau, l'âge peut modifier les rides du visage ou la couleur des cheveux, un éventuel accident peut laisser ses traces sur le visage, les lunettes,……

- Un visage peut avoir des orientations et des dimensions très différentes. Il s'y ajoute les conditions d'éclairage et la position dans l'image où certaines zones du visage peuvent être cachées soit par un objet soit par un autre visage.

- Les visages sont avant tout des structures 3D dans un espace 3D, de nombreux paramètres s'ajoutent encore au problème original : des contraintes de luminosité (dues soit à la position de la tête, soit au type d'éclairage choisi), de couleur, d'ombres et de rotations éventuelles de la tête

- La détection de visages doit être en temps réel surtout lorsque le résultat de la détection demande une réaction en temps réel comme par exemple une personne s'introduisant dans une zone très dangereuse.

Par conséquent, la détection automatique de visages dans une image reste un domaine de recherche très vaste et très riche en termes d'approches et techniques utilisées

II.4. Approches et méthodes de détection de visages

Des nombreuses méthodes de détection de visages sont apparues dans les deux dernières décennies et qui se diffèrent, aussi bien par les approches qu'elles emploient, que par les techniques d'apprentissage qu'elles utilisent. Yang et al. classifient ces techniques en quatre classes

- techniques descriptives basées sur la connaissance

- techniques basées sur l'extraction de paramètres caractéristiques invariants

- techniques basées sur la superposition de caractéristiques

- techniques basées sur l'apparence

Les techniques, basées sur l'apparence, utilisent l'analyse statistique et l'apprentissage automatique pour construire des machines capables de séparer les visages des non-visages. Les réseaux de neurones, les machines à vecteurs de support (SVM), les classificateurs Bayesiens, les modèles de Markov cachés (HMM) sont parmi les méthodes d'apprentissage automatique les plus souvent … utilisées….. ***Figure II.3*** présente les différentes approches qui utilisé dans un domaine biométrie de détection de visage [4]

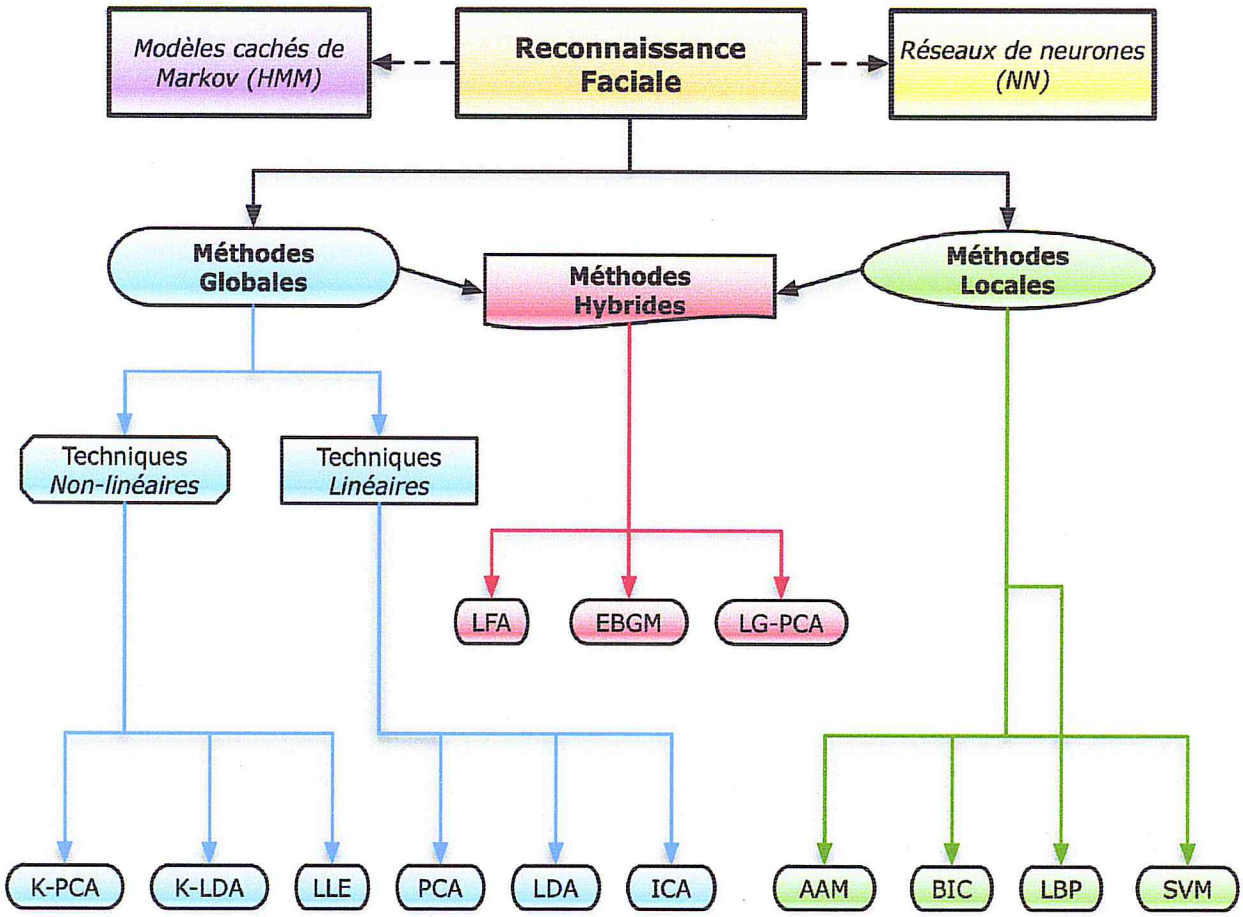


Figure II.3 Une classification des algorithmes principaux utilisés en reconnaissance faciale [4]

II.5. Les Méthodes basées sur les caractéristiques du visage

On les appelle aussi les méthodes à traits, à caractéristiques locales, ou analytiques. L'analyse du visage humain est donnée par la description individuelle de ses parties, leurs positions et de leurs relations. Ce modèle correspond à la manière avec laquelle l'être humain perçoit le visage, c'est à dire, à nos notions de traits de visage et ses parties comme les yeux, le nez et la bouche, ce qui permet de conclure la présence ou non du visage dans l'image à analyser [6]

II.5. 1. Approches basées sur la géométrie de visages

Les travaux réalisés se sont au début basés contours (les années 70) [5] ensuite la plupart des approches se sont concentrées sur l'extraction des traits du visage à partir d'une image et sur la définition d'un modèle adéquat pour représenter ce visage. Un certain nombre de stratégies ont modélisé et classé les visages sur la base de distances normalisées et angles entre points

caractéristiques : les yeux, les sourcils, la bouche, le nez,... mais peuvent être d'un niveau de détail beaucoup plus fin

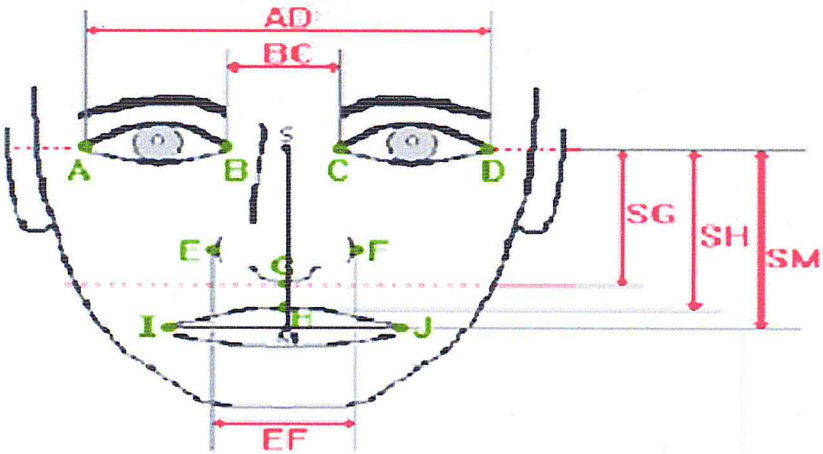


***Figure II.4**: Modèle géométrique du visage [5]*

II.5. 2. Approches basées sur la couleur de la peau :

Dans cette approche, la couleur de peau humaine a été employée comme un dispositif efficace pour la détection de visage, et les applications reliées. Bien que la couleur de peau diffère d'un individu à un autre, plusieurs études ont prouvé que la différence principale existe dans l'intensité plutôt que la chrominance , Plusieurs espaces de couleur ont été employés pour marquer des pixels de peau comprenant RVB (RGB), HSV [7]

Quoique l'information de couleur semble être un outil efficace pour identifier des secteurs faciaux, les modèles de couleur de peau peuvent échouer quand le spectre (la température corrélée de couleur) de la source lumineuse change de manière significative. En outre, les caractéristiques du dispositif d'acquisition (équilibre spécifiquement blanc) effectueront également la transformation de couleur entre l'environnement et l'image.

II.5. 3. Approches basées sur la connaissance généralisée

Dans cette approche, les algorithmes développés sont basés sur des heuristiques au sujet de l'aspect de visages. Bien qu'il soit simple de créer une heuristique pour décrire le visage humain, la difficulté principale est dans la traduction de ces heuristiques dans des règles de classification d'une manière efficace.

Yang et Huang ont employé une méthode basée sur la connaissance hiérarchique pour détecter des visages. Leur système se compose de trois règles allant du niveau général au détaillé. Cette méthode ne rapporte pas un taux élevé de détection, mais, des méthodes plus récentes ont utilisé des règles de niveaux multiples [6,11].

L'avantage de ces méthodes est qu'elles prennent en compte la particularité du visage en tant que forme naturelle à reconnaître, et un nombre réduit de paramètres en exploitant les résultats de la recherche en neuropsychologie et psychologie cognitive sur le système visuel humain. La difficulté éprouvée quand 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 .

II.6. Les Méthodes Globale :

Cette classe regroupe les méthodes qui mettent en valeur les propriétés globales du visage. Le visage est traité comme un tout. Dans ces méthodes (« Neural Networks , Support Vecteur Machine, Principal Component Analysis, Eigen faces, Hidden Markov Model …….»), on génère une base d'exemples à partir de laquelle un classificateur va apprendre ce qu'est un visage (apprentissage). Ces systèmes sont très performants, mais très lents en phase d'apprentissage donc lourds à mettre en œuvre Parmi les approches les plus importantes réunies au sein de cette classe on trouve

II.6. 1. Approche PCA ou Les Visages Propres :

Vers la fin des années 80, Sirovich et Kirby ont développé une technique en utilisant PCA pour représenter efficacement les visages humains. Le but est de capturer la variation dans une collection d'images de visages et d'utiliser cette information pour coder et comparer les visages (en termes mathématiques : trouver les vecteurs propres de la matrice de covariance de l'ensemble des images de visages). Le nombre possible de visages propres peut être approximé en utilisant seulement les meilleurs visages propres qui correspondent aux plus grandes valeurs propres .
Plus tard, au début des années 90, M. Turc et A. Pentland ont amélioré cette technique pour l'identification de visages. Leur méthode profite de la nature distincte des poids de `Eigen faces' pour la représentation individuelle de visages [8,9].
Plus récemment, en utilisant **DFFS** (Distance From Face Space), B. Moghaddam et **A.** Pentland ont proposé un détecteur facial de dispositif qui produit des Eigen features (« Eigen eyes, Eigen nose, Eigen mouth »), qui sont obtenus à partir de divers calibres faciaux de dispositif dans un ensemble de formation .

Ensuite, ils ont développé cette technique dans un cadre probabiliste à l'aide d'un détecteur de maximum de vraisemblance qui tient compte de l'espace de visage et de son complément orthogonal pour manipuler des densités arbitraires. Comparé au détecteur de DFFS, les résultats étaient sensiblement meilleurs

L'approche PCA (Principal Components Analysis) est une manière intuitive et appropriée de construire un sous-espace pour représenter une classe d'objet dans beaucoup de cas. Cependant, pour modeler la variété dans des images de visages, PCA n'est pas nécessairement optimal. L'espace de visage pourrait mieux être représenté en le divisant en sous-classes. La plupart des méthodes qui ont été proposées sont basées sur un certain mélange de Gaussiens multidimensionnel.

II.6.2. Approches Probabilistes (Statistiques) :

Ces approches reposent essentiellement sur la théorie de décision pour résoudre les problèmes de classement et de classification, et c'est pour ça qu'ils utilisent généralement la classification fondée sur le théorème de Bayes

Colmenarez et Huang ont proposé un système basé sur l'information relative de Kullback (divergence de Kullback) pour créer des fonctions de probabilité pour les classes de Visages et de Non-Visages.

Yang et al. ont présenté une méthode pour détecter des visages humains à partir d'images en couleur. Un modèle de la couleur de peau humaine basé sur une analyse statistique multi variante est construit pour capturer les propriétés chromatiques. Ensuite, dans un autre travail, ils ont présenté une autre méthode de probabilité qui utilise un mélange d'analyseurs de facteur.

Dans une autre approche, **E.** Osuna et **al**. ont développé une méthode efficace pour former un SVM pour des problèmes à grande échelle, et l'ont appliqué à la détection de visages.

Kumar et Poggio ont, ensuite, incorporé un algorithme du SVM dans un système pour l'analyse des visages en temps réel. Ils appliquent cet algorithme du SVM sur des régions segmentées de peau dans les images d'entrée pour éviter le balayage approfondi.

W. Karam et al. ont crée, plus tard, un système de détection de visage et d'extraction de paramètres basé sur les SVM et appliqué sur des visages parlants dans des séquences vidéo. Une machine SVM est apprise sur des fenêtres après leur transformation dans le domaine D'ondelettes. Un modèle géométrique statistique est ensuite appliqué afin de lisser la sortie de la machine SVM et d'affiner la détection. Un autre modèle probabiliste sur les distances aux frontières SVM permet plus de lissage et une meilleure sélection des composantes faciales. [4,5]

Schneiderman et Kanade décrivent deux détecteurs de visage basés sur la décision de Bayes (présenté comme essai de rapport de probabilité) :

$$\frac{P(image/objet)}{p(image/non-objet)} > \frac{P(non-objet)}{p(objet)} \quad [5]$$

Si le rapport de probabilité (côté gauche) de l'équation ci-dessus est plus grand que l'autre côté, alors on décide qu'un objet (un visage) est présent à l'endroit courant.

S. Zhou et al proposent un modèle probabiliste para-métrisé par un vecteur de cheminement d'état et une variable de reconnaissance d'identité caractérisant simultanément la dynamique et l'identité des humains. Ils appellent, alors, des approches de condensation pour fournir une solution numérique au modèle. Une fois que la distribution postérieure commune du vecteur d'état et de la variable d'identité est estimée, ils la marginalisent au-dessus du vecteur d'état pour rapporter une évaluation robuste de la distribution postérieure de la variable d'identité.
Ces approches posent le problème de la complexité de calcul qui reste très élevée

II.6.3. Approches basées sur les réseaux de neurones

Cette approche repose essentiellement sur la notion d'apprentissage qui est depuis de nombreuses années au cœur de la recherche en intelligence artificielle. Puisque la détection de visages peut être comprise comme problème d'identification de modèle de deux classes (visage ou non-visage), plusieurs méthodes utilisant les réseaux de neurones ont été présentées pour la solution. Un examen des méthodes de détection de visage par réseaux de neurones La première approche basée sur un réseau de neurones, qui a donné des résultats significatifs sur des données complexes, était présentée par Rowley et al.[4]

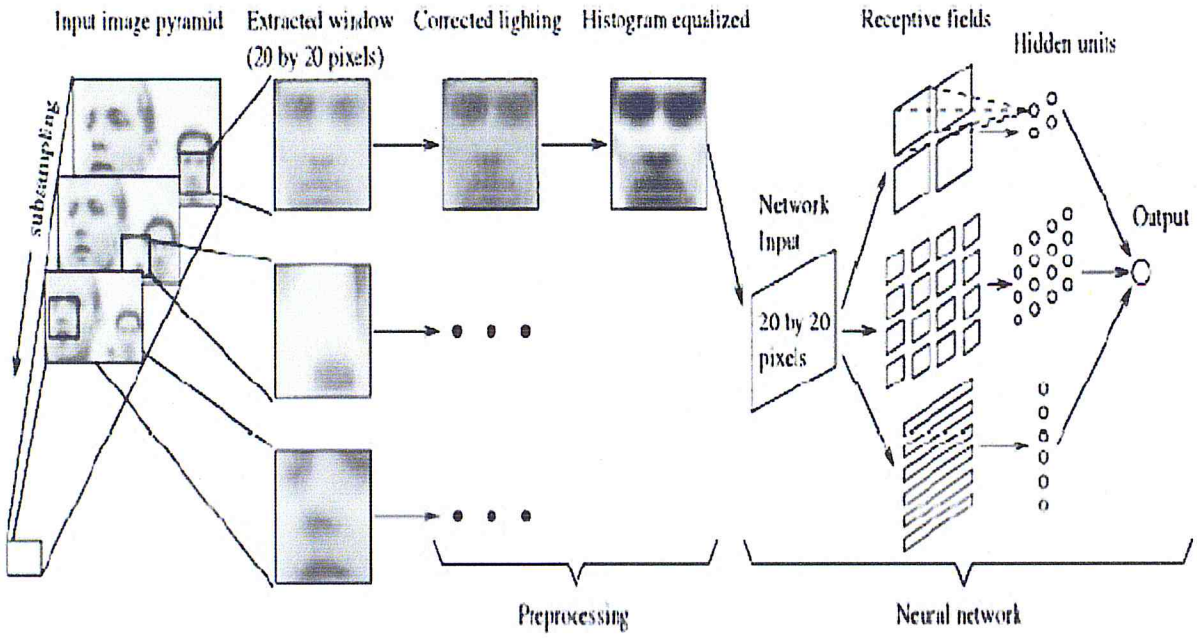


***Figure II.5**: le système de Rowley et al. (IEEE1998) [4]*

- Ce réseau de neurones est conçu pour traiter des fenêtres de 20 x 20 pixels avec une couche cachée. La fenêtre d'entrée est prétraitée par la correction d'éclairage et l'égalisation d'histogramme [4]
- L'avantage de cette approche est le gain de temps considérable. En insérant des zooms différents lors de l'apprentissage, il ne devient plus nécessaire de tester chaque dimension potentielle. Rien n'interdisant la présence d'un visage occupant toute l'image ou uniquement le un dixième dans le coin. Cependant, l'utilisation d'exemples pour apprentissage 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

II.7. Méthodes hybrides

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales

L'analyse de caractéristiques locales (**LFA**) et les caractéristiques extraites par ondelettes de Gabor (comme l'Elastic Bunch Graph Matching, EBGM), sont des algorithmes hybrides typiques. Plus récemment, l'algorithme LogGabor PCA(**LG-PCA**) effectue une convolution avec des ondelettes de Gabor orientées autour de certains points caractéristiques du visage afin de créer des vecteurs contenant la localisation et la valeur d'amplitudes énergétiques locales ; ces vecteurs sont ensuite envoyés dans un algorithme PCA afin de réduire la dimension des donnée [4]

II.8. Conclusion

Nous avons vu le principe de la détection de visages humains dans une image, ensuite nous avons présenté quelques approches à propos de ce sujet : Les méthodes basées sur les caractéristiques du visage (la géométrie du visage, la couleur de la peau, la connaissance généralisée,...) et Les méthodes globales (PCA, Approches probabilistes, réseaux de neurones...), ainsi que quelques méthodes hybrides.

La liste des méthodes présentées dans ce chapitre n'est pas exhaustive, mais constitue un aperçu de la diversité des approches qui existent pour faire la détection de visages.

CHAPITRE III

Conception et Architecture du Système de vidéosurveillance intelligente

III.1. Introduction

Le but de notre travail est la réalisation d'un système de la vidéosurveillance intelligente basé sur la reconnaissance faciale. Nous présentons dans ce chapitre d'une part l'approche viola et Jones pour la détection visage dans un temps real. Et dans Ce chapitre est consacré à la présentation différente Plateformes utilisé dans un Système Vidéosurveillance.

III.2. Méthode de Viola et Jones

La méthode la plus utilisée est une méthode de Viola et Jones , Elle est une méthode de détection d'objet dans une image numérique, proposée par les chercheurs Paul Viola et Michael Jones en 2001. Elle fait partie des toutes premières méthodes capables de détecter efficacement et en temps réel des objets dans une image, Inventée à l'origine pour détecter des visages, elle peut également être utilisée pour détecter d'autres types d'objets comme des voitures ou des avions, La méthode de Viola et Jones est l'une des méthodes les plus connues et les plus utilisées, en particulier pour la détection de visages et la détection de personnes.

En tant que procédé d'apprentissage supervisé, la méthode de Viola et Jones nécessite de quelques centaines à plusieurs milliers d'exemples de l'objet que l'on souhaite détecter, pour entraîner un classifieur. Une fois son apprentissage réalisé, ce classifieur est utilisé pour détecter la présence éventuelle de l'objet dans une image en parcourant celle-ci de manière exhaustive, à toutes les positions et dans toutes les tailles possibles.

Considérée comme étant l'une des plus importantes méthodes de détection d'objet, la méthode de Viola et Jones est notamment connu pour avoir introduit plusieurs notions reprises ensuite par de nombreux chercheurs en vision par ordinateur, à l'exemple de la notion d'image intégrale ou de la méthode de classification construite comme une cascade de classifieurs boostés [11]

III.3. Historique

Paul Viola et Michael Jones, alors employés au Cambridge Research Laboratory de la société américaine Compaq, publient la méthode qui porte leur nom pour la première fois le 13 juillet 2001 dans le journal scientifique International Journal of Computer Vision (IJCV), Les deux auteurs publient ensuite deux autres articles sur la méthode :

Une version moins détaillée, présentée à la Conférence on Computer Vision and Pattern Recognition (CVPR) en décembre 2001 et une version révisée en 2004, toujours dans IJCV.

Les caractéristiques extraites par cette méthode sont inspirées des travaux de **P**apageorgiou, **O**ren et **P**oggio, datant de 1998, qui utilisent des caractéristiques construites à partir d'ondelettes de **H**aar.

La méthode s'inspire également de précédents travaux de **P**aul Viola et **K**inh Tieu dans un autre domaine, celui de la recherche d'image par le contenu, en reprenant l'idée de sélection de caractéristiques par **AdaBoost**. Parmi les nombreuses méthodes de détection de visages publiées à l'époque, Viola et Jones considèrent en particulier celle de **R**owley- Kanade, en raison de ses excellents résultats et de sa rapidité , ils la prennent comme référence pour les comparaisons à performances équivalentes , **V**iola et **J**ones notent que la détection par leur méthode est 15 fois plus rapide que le détecteur de **R**owley-Kanade.

La méthode, considérée comme l'une des plus efficaces en détection de visage, devient rapidement un standard dans ce domaine, Les travaux de Viola et Jones sont parmi les plus utilisés et les plus cités par les chercheurs, et de nombreuses améliorations sont ainsi proposées. Leurs travaux sont également étendus à d'autres types d'objets que les visages et la méthode devient ainsi un standard en détection d'objet, La méthode est par ailleurs reconnue comme étant celle ayant eu le plus d'impact dans le domaine de la détection de visage dans les années 2000. [11]

III.4. Performances

Viola et Jones ont testé leur méthode sur la base de 130 images contenant 507 visage de face. Ils présentent leur résultat sous la forme d'une courbe **R**eceiver **O**perating **C**haracteristic . Cette courbe présente le taux de détection correct en fonction du nombre de faux positif, On remarque par exemple que pour un taux détection de 88.8%, on a eu 50 faux positifs

Comparé à d'autres méthodes de détection d'objet, celle de Viola et Jones est équivalente en terme de précision de détection, En revanche, elle est 15 fois plus rapide que la technique de **R**owley**K**anade, et 600 fois plus rapide que **S**chneiderman**K**anade [12,13]

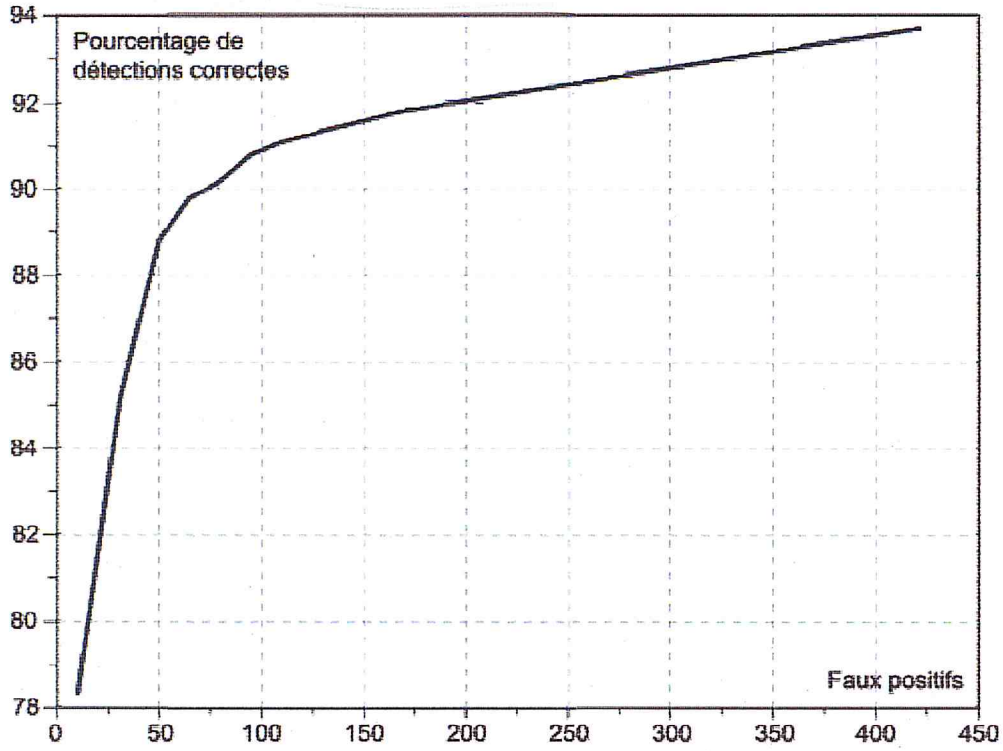


Figure III.1 pourcentage de détection correctes par la méthode de Viola et Jones [13]

III.5. Eléments de la méthode Viola et Jones

III.5.1. Image intégrale

L'algorithme se base sur les caractéristique de Haar (haar Features) pou localiser les visages présents sur une image d'entrée . dans le but d'extraire rapidement ces caractéristiques ,l'image est représentée sous forme intégrale . En effet sous cette forme l'extraction d'une caractéristique à n'importe quel endroit et à n'import quelle échelle est effectuée en un temps constant tandis que le temps de conversion vers la représentation intégrale ne remet pas en cause ce gaine de temps offert par l'utilisation de la représentation en image intégrale. la définition des caractéristique de Haar et la manière dont la représentation intégrale accélère considérablement leur extraction sont présentés ci-après pour une image en niveaux de gris.

Dans toute image une zone rectangulaire peut être délimitée et la somme des valeurs de ses pixels calculée. une caractéristique de Haar est une simple combinaison linéaire de somme ainsi obtenues.[13,14]

Plusieurs caractéristique de Haar peuvent être définies selon le nombre .les échelles, les positions et les dimensions des zones rectangulaires considérées 4 exemples sont présentés à la ***Figure III.2***

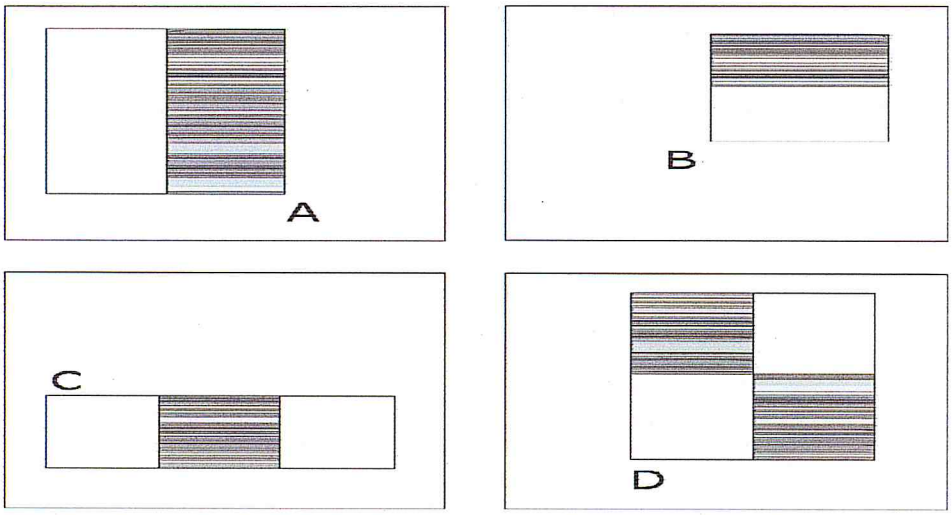


Figure III.2 Types de Haar Features utilisés par Viola et Jones [13]

La somme des valeurs des pixels appartenant aux zones encadrées claires est soustraite à la somme des valeurs des pixels appartenant aux zones encadrées sombres pour obtenir la caractéristique de Haar . Chacune des quatre caractéristique de Haar est représentée avec son cadre de détection respectif.

Présenté comme tel , le calcul d'une caractéristique de Haar demande à chaque fois l'accès aux valeurs de tous les pixels contenus dans les zones rectangulaires considérées Cela devient vite contraignant temporellement dés que les caractéristique de Haar sont définies par des zones rectangulaires de grandes dimensions , l'image intégrale permet de surmonter ce problème en rendant constant le temps de calcules d'une caractéristique de Haar à n'importe quelle échelle . L'image intégrale est représentée mathématiquement par [13]

$$ii(x,y) = \sum_{x' \leq x, y' \leq y} i(x',y')$$

$$\forall \quad 0 < x \leq width, 0 < y \leq height$$

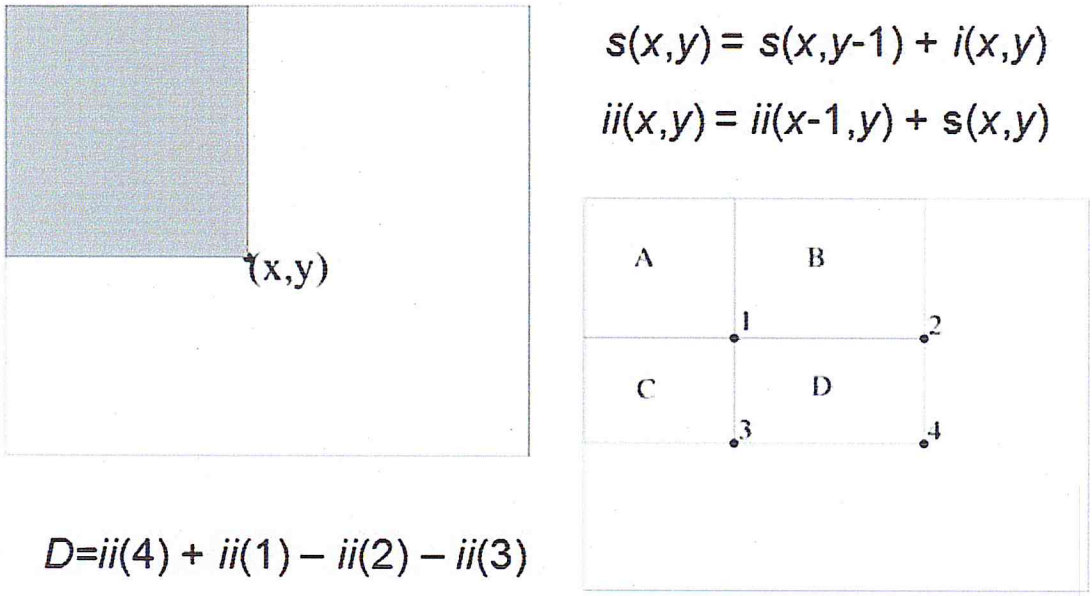


Figure III.3 : Intégrale Image [13]

Où i(x , y) est l'image d'origine et i(x',y') l'image sous sa nouvelle représentation .Ainsi chaque pixel a pour valeur la somme des valeurs des pixels compris dans le rectangle défini par le coin supérieur gauche de l'image et lui-même.

Le calcul de la somme des valeurs des pixels appartenant à une zone rectangulaire s'effectue donc en accédant seulement à quatre pixel de l'image intégrale : soit un rectangle ABCD dont les sommets sont nommés dans le sens des aiguilles d'une montre en commençant par le sommet supérieur gauche et soit x la valeur sous la représentation intégrale d'un sommet X du rectangle ($X \in \{ A,B,C,D \}$).

la somme des valeurs des pixels appartement à ABCD est quelle que soit sa taille , donnée par C-B-D+A.

Une caractéristique de Haar étant une combinaison linéaire de tels rectangles ABCD son calcule se fait alors en un temps indépendant sa taille [13]

III.5.2. Algorithme d'apprentissage basé sur Adaboost

Pour localiser les visages sur l'image d'entrée, cette dernière par une fenêtre de dimension déterminée. la fenêtre parcourt l'image et son contenu est analysé pour savoir s'il s'agit d'un visage ou non, comme dit plus haut , les caractéristique de Haar sont extraites pour effectuer la classification et de ce fait la représentation intégrale de l'image accélère l'analyse . mais pour une fenêtre 24 x24 pixels il y a 45396 caractéristiques de Haar , les traiter toutes prendrait beaucoup

trop de temps pour une application en temps réel .pour surmonter ce problème , une variante de la méthode de Boosting Adaboost est utilisée

Ci-dessous Adaboost est brièvement présenté suivi de sa variante qui constitue le deuxième apport du travail de Viola & Jones .

Adaboost est une méthode d'apprentissage permettant de « Booster »les performances d'une classifieur quelconque nommé « classifieur faible » . l'idée est de faire passer les candidats à classifier à travers plusieurs classifieurs faibles ,chacun étant entrainé en portant plus d'attention sur les candidats mal classifiés par le classifieur précédent.

Pour arriver à ce résultat des poids sont associés aux échantillons du set d'entrainement (x_i,y_i) : i= (1,…….,m), tout d'abord de manière équilibrée : [15]

$$w_i^0 = \frac{1}{m}$$

Pour i=1,…….,m le 0 exposant indique qu'il s'agit des poids initiaux ensuite le premier classifieur faible est entraine comme suit :

$$h^0 = \text{argmin } h_j \in H \in_j$$

Avec l'erreur $\in_j = \sum_{i=0}^{m} w_i^0 \delta(y_i - h_j(x_i))$ et H l'ensemble des classifieurs faibles puis la nouvelle génération de poids w_i^1 sont créés tels qu'ils accordent plus d'importance aux échantillons mal classifiés par h_0 ensuite un nouveau classifieur h_1 est entrainé puis de nouveaux poids w_i^2 sont générés et ainsi de suite . enfin après T itérations le classifieur fort H(x) est obtenu :

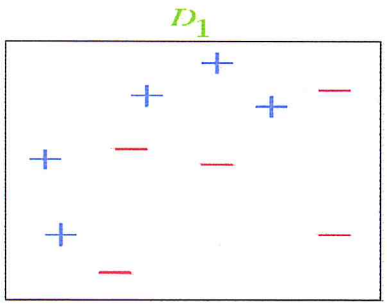
$$H(x) = \text{sign}\left(\sum_{t=1}^{T} \alpha_t h_t(x) - \theta\right) \quad [15]$$

Avec $\alpha = \frac{1}{2} ln \frac{1-\varepsilon t}{\varepsilon t}$ et θ un seuil à déterminer. chaque classifieur fort est donc constitué d'un nombre T de classifieurs faibles

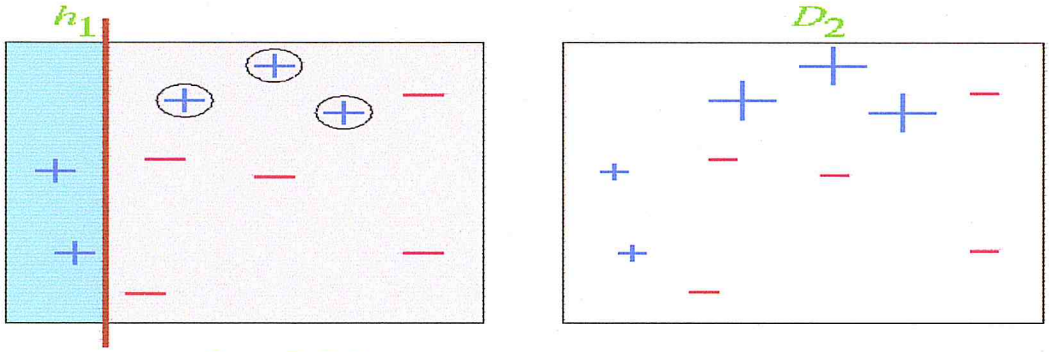
Adaboost sert donc à booster une classifieur déjà existant et à priori chaque classifieur faible possède le même espace d'entrée . dans la variante d'Adaboost de Viola et Jones , les cllassifieurs

faibles $h_j \in H$ ont pour entrée une caractéristique de Haar différente . Adaboost s'apparente alors à une sélection de caractéristiques (Feature selection). Cette variante d'Adaboost est utilisée lors de l'apprentissage pour sélectionner les caractéristique de Haar les plus à même de détecter un visage et permet ainsi de surmonter le problème du nombre élevé de caractéristique de Haar existant pour une de recherche .

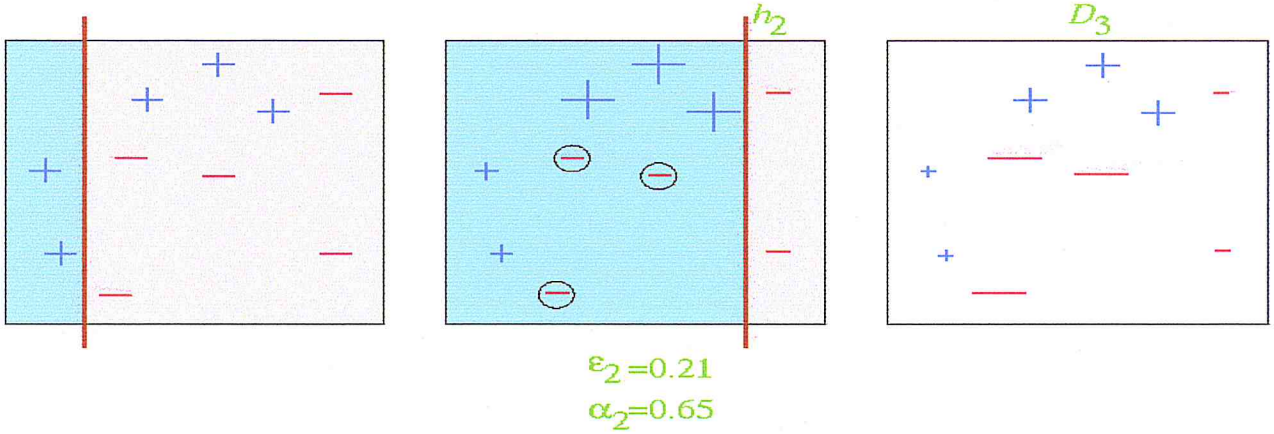
- **Exemple de Boosting**

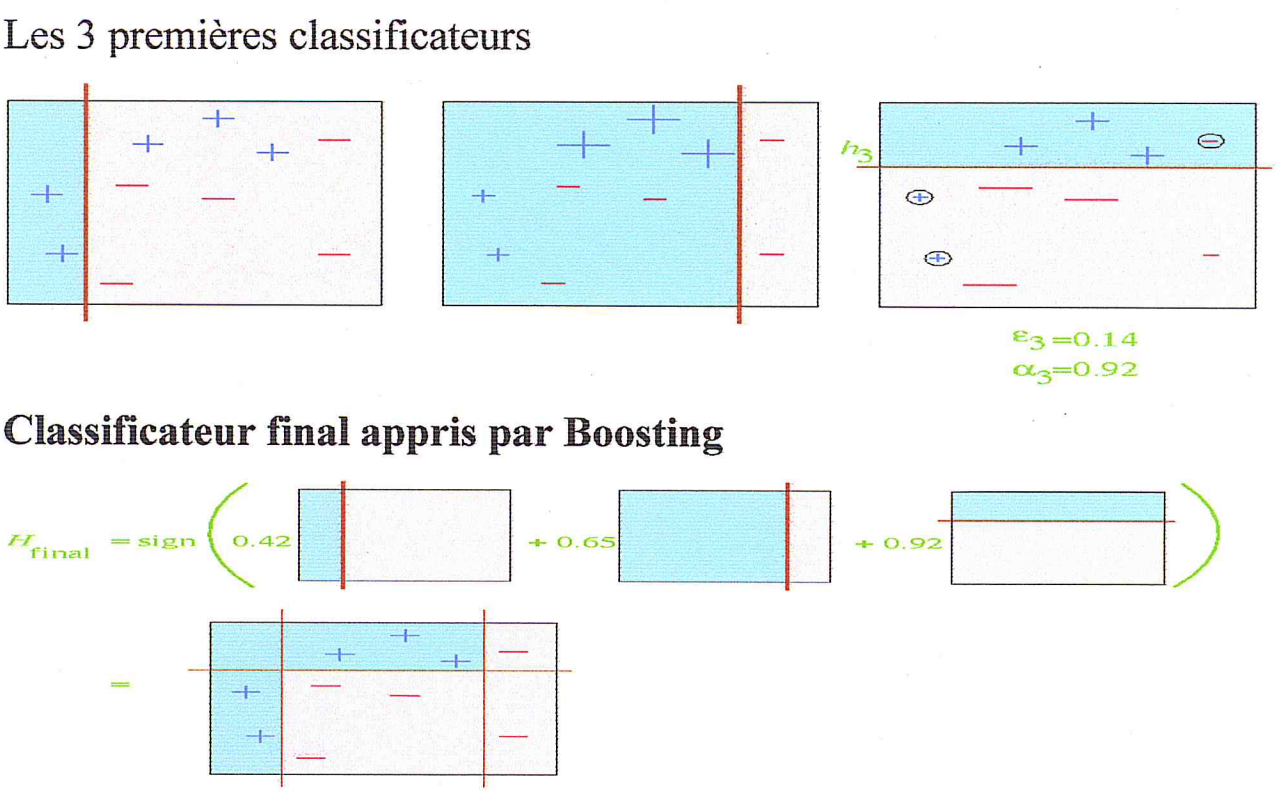


Premier classificateur



Les 2 premières classificateurs





III.5.3. Cascade de classifieurs

L'idée de base derrière le concept de cascade est que parmi l'l'ensemble des candidats, c'est-à-dire l'ensemble des états de la fenêtre de recherche, une partie peut être éliminée sur base de l'évaluation de seulement quelque caractéristique de Haar .une fois cette élimination effectuée, les candidats restants sont analysés par classifieurs plus complexes (utilisant plus de caractéristique de Haar) demandant un plus grand temps de traitement . en utilisant plusieurs « étages » de ce type , le processeur évite d'effectuer des analyses lourdes en temps de calcul sur des échantillons pour lesquels il est rapidement possible de se rendre compte qu'ils sont négatifs .le processus de classification apparait alors comme une cascade de classifieurs fort de plus en plus complexes où à chaque étage les échantillons classifiés négatifs sont sortis tandis que les échantillons classifiés positifs sont envoyée aux classifieurs suivants [13]

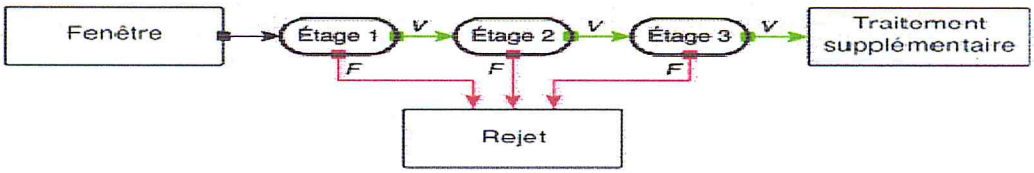


Figure III.4 : Illustration de l'architecture de la cascade [13]

les fenêtres sont traitées séquentiellement par les classifieurs, et rejetées immédiatement si la réponse est négative (F)

Si le premier étage rejette un faux négatif, c'est un gros problème car il ne sera jamais récupéré par la cascade . autrement dit c'est un visage qui ne sera pas détecté par contre , si le premier étage transmet un faux positif il pourra toujours être éliminé aux étages suivants de la cascade . ce petit raisonnement permet de mettre en évidence que les premiers nœuds constitutifs de la cascade peuvent se permettre d'avoir un taux de faux positifs élevés (de l'ordre de 40-50%) mais doivent absolument assurer un taux de détection maximum.

Ce concept permet donc à l'algorithme de consacrer son temps à de longues analyses complexes uniquement lorsque cela en vaut la peine. il s'agit à nouveau d'un mécanisme qui accélère la vitesse d'exécution de la méthode proposée par Viola et Jones [13,14]

III.6. Limites et extensions de la méthode de Viola et Jones

La méthode de Viola et Jones pose des problèmes dans certains cas particuliers, comme par exemple les visages de coté, ou de biais (tournés à 45°). L'augmentation des caractéristiques pseudo Haar de 4 à 14 en 2002 permet de connaître plus de schéma, L'utilisation d'images intégrales, d'histogrammes de gradients orientés, des motifs binaires locaux. de la covariance de région ont permis d'augmenter les performances de la méthode depuis sa première parution.

Les chercheurs ont également étudiés l'utilisation de variantes de l'algorithme de Boosting, notamment RealBoost, qui en plus de la classification produit des indices de confiance à valeurs réelles. Pour améliorer la méthode en detection de visage de coté, Viola et Jones ont proposés une amélioration, qui consiste à apprendre une cascade dédiée pour chaque orientation de vue.

L'utilisation d'arbre de décision permet de parcourir les espaces des cascades avec une bonne complexité algorithmique. [13]

III.7. vidéo sur IP

La vidéo sur IP – souvent appelée IP-Surveillance dans le cadre d'applications spécifiques de vidéosurveillance, de sécurité et de contrôle distant – est un système permettant à ses utilisateurs de visualiser et d'enregistrer des images vidéo via un réseau IP (LAN/WAN/Internet).
À la différence des systèmes analogiques, la vidéo sur IP utilise le réseau informatique plutôt qu'un système de câblage point-à-point pour transmettre les informations, dans une application de vidéo sur IP, les flux d'images vidéo numériques peuvent être transférés n'importe où dans le monde via un réseau IP câblé ou sans fil. [16]

III.7.1. Sécurité et vidéosurveillance

Grâce à ses fonctions avancées, la vidéo sur IP s'avère particulièrement indiquée pour les applications de sécurité et de vidéosurveillance, La souplesse des techniques numériques renforce la capacité à protéger les personnes, les biens et les propriétés.

III.7.2. Contrôle distant

La vidéo sur IP permet aux utilisateurs d'obtenir à tout instant des informations sur une opération en cours, et de la suivre en temps réel. Cette caractéristique en fait une technologie idéale pour assurer le contrôle des installations, des personnes et des locaux, sur place ou à distance. Citons quelques exemples d'applications distantes : le contrôle de la circulation, le contrôle des lignes de production ou le contrôle des points de vente.

Les principaux marchés verticaux bénéficiant des systèmes vidéo sur IP sont les suivants :

- **Environnements scolaires :** Applications de sécurité, vidéosurveillance et contrôle distant des cours de récréation, des couloirs, des halls d'école et des classes, et sécurisation des bâtiments.
- **Transport :** Contrôle distant des gares et des voies ferrées, des autoroutes et des aéroports.
- **Secteur bancaire :** Applications courantes dans les locaux des banques, et sécurisation des appareils automatiques.
- **Domaine public :** à des fins de surveillance, pour assurer la sécurité des lieux publics.
- **Commerces :** Vidéosurveillance et contrôle distant afin de faciliter et d'optimiser la gestion des magasins.
- **Secteur industriel** : Surveillance des processus industriels, des systèmes logistiques, des systèmes de gestion des entrepôts et de contrôle des stocks. [16]

III.8. Qu'est-ce qu'un logiciel de gestion vidéo ?

Un logiciel de gestion vidéo fonctionnant sur un serveur Windows ou Unix/Linux est un outil qui permet de gérer les images vidéo, de les analyser et de les enregistrer. Tout un ensemble de logiciels permettent de répondre aux demandes des utilisateurs

Pour visualiser simultanément plusieurs caméras, un logiciel de gestion vidéo spécifique est nécessaire, Sous leur forme la plus simple, des logiciels permettent l'affichage en direct, l'enregistrement et la consultation des séquences vidéo.[16]

III.9. Systèmes de vidéo sur IP avec caméras réseau

Une caméra réseau associe une caméra et un ordinateur. Permettant la numérisation et la compression vidéo, elle est en outre équipée d'un connecteur réseau. La vidéo est acheminée par réseau IP via les commutateurs réseau. Pour être enregistrée sur un PC/serveur standard à l'aide d'outils de gestion vidéo. [16]

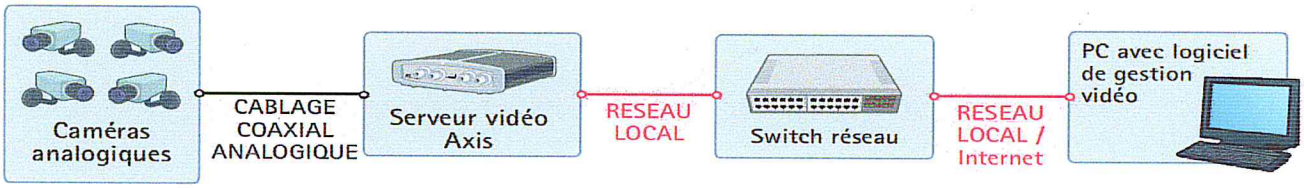


***Figure III.5** : architecture de vidéosurveillance*

III.10. Plates-formes matérielles

Il existe deux types de plates-formes pour la gestion vidéo sur IP : les plates-formes utilisant un serveur PC et les plates-formes utilisant un enregistreur vidéo sur IP.

Les solutions utilisant une plate-forme avec serveur PC fonctionnent sur un matériel 'standard', dont les composants physiques ont été sélectionnés avec soin, de manière à offrir des performances optimales. Avec ce type de solution, il est possible d'optimiser les composants standard, notamment en augmentant les capacités de stockage, en ajoutant de l'espace externe ou des postes de traitement supplémentaires, ou en exécutant des logiciels supplémentaires en parallèle à l'application vidéo, tels que des outils pare-feu ou antivirus.

Ce qui distingue le plus une solution serveur PC d'une solution utilisant un enregistreur vidéo sur IP, est le fait que l'enregistreur vidéo sur IP se présente dans un boîtier physique où les fonctions de gestion sont préinstallées. Par définition, l'enregistreur est dédié à l'enregistrement, l'analyse et la lecture des séquences vidéo sur IP, toute autre application résidante étant exclue. L'enregistreur est en effet 'verrouillé' pour les seuls usages réservés, toute adaptation qui permettrait d'ajouter de nouvelles fonctionnalités étant généralement impossible.[16]

III.10.1. Plateformes utilisant les serveurs PC

Comme indiqué précédemment, les solutions utilisant une plate-forme serveur PC fonctionnent sur un matériel 'standard', dont les composants physiques ont été sélectionnés de manière à offrir des performances optimales compte tenu de la destination du système – par exemple le stockage indépendant ou les systèmes à double processeur.

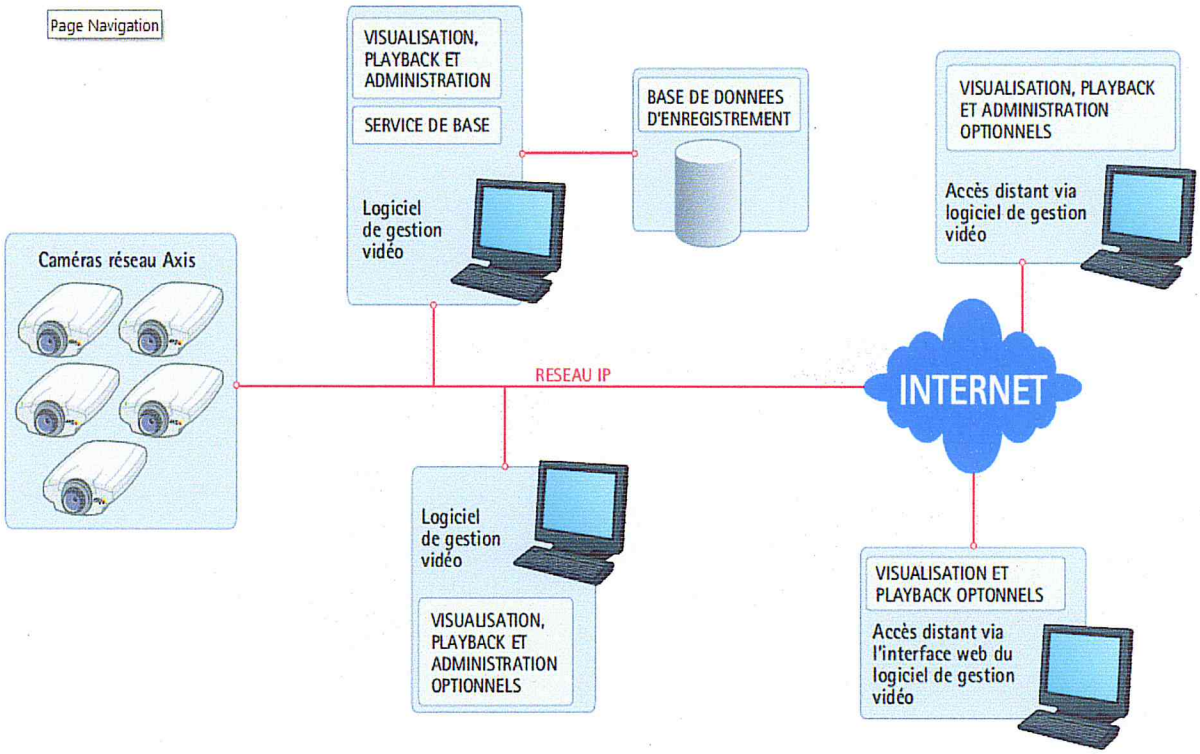


Figure III.6 : Plateformes les serveurs PC

III.10.2. Plateformes utilisant les enregistreurs vidéo sur IP

Les enregistreurs vidéo sur IP présentent certaines similitudes avec les enregistreurs numériques Digital Video Recording (DVR) en termes d'enregistrement et de lecture. Mais alors que l'enregistreur numérique est en réalité un système hybride, capable de prendre en charge les caméras analogiques et de stocker les images vidéo dans un format numérique sur disque dur, l'enregistreur vidéo sur IP, en revanche, est un système 100% numérique, qui reçoit des images ou des flux vidéo numériques via le réseau, et les enregistre sur disque dur également au format numérique. Certains enregistreurs numériques possèdent une interface réseau rudimentaire, permettant la visualisation à distance. Un enregistreur vidéo sur IP n'a ni écran ni clavier dédié. Toutes les fonctions d'affichage et de gestion ont lieu à distance via un PC sur le réseau.

Un enregistreur vidéo sur IP est conçu pour offrir des performances optimales pour une ou plusieurs caméras, mais ses capacités d'extension sont inférieures à celles des plates-formes utilisant un serveur PC. L'enregistreur vidéo sur IP convient donc pour les environnements de plus petite taille, lorsque le nombre de caméras reste dans les limites des capacités de l'enregistreur. Un avantage, en revanche, est que les plates formes utilisant un enregistreur vidéo sur IP sont moins difficiles à installer que les plates-formes avec serveur PC [16]

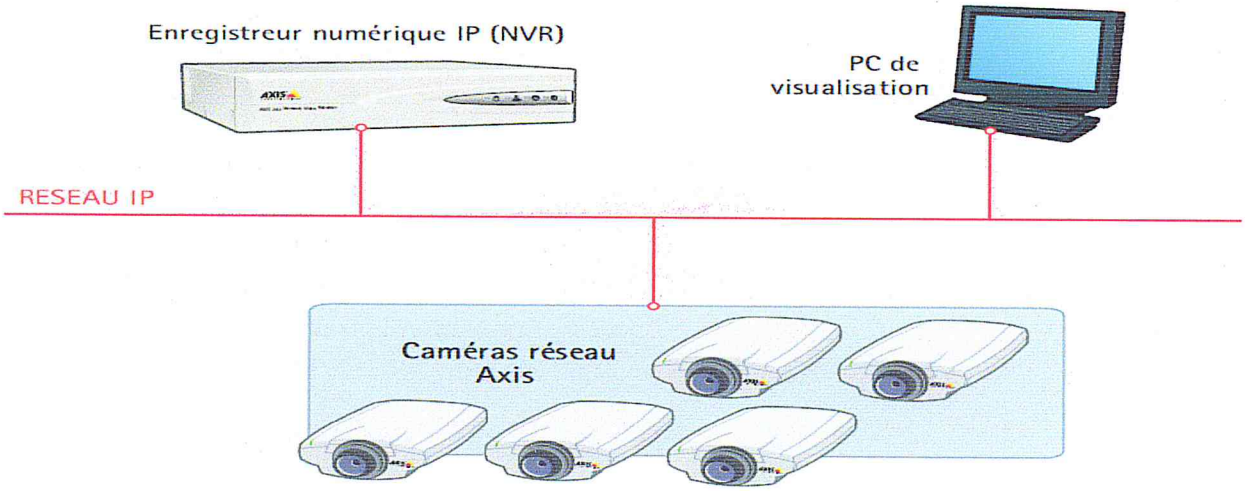


Figure III.7: Plateformes enregistreurs vidéo sur IP

III.11.Vidéosurveillance intelligente :

L'analytique vidéo aussi appelée vidéosurveillance intelligente, est une technologie qui permet, au moyen de logiciels, d'identifier automatiquement, dans des séquences vidéo, des objets, des comportements ou des attitudes spécifiques. Elle transforme la vidéo en données qui seront transmises ou archivées pour permettre au système de vidéosurveillance d'agir en conséquence. Il pourra s'agir d'actionner une caméra mobile, dans le but d'obtenir des données plus précises de la scène ou tout simplement, d'envoyer une alerte au personnel de surveillance pour qu'il puisse prendre une décision sur l'intervention adéquate à apporter.

Les systèmes de vidéosurveillance intelligente utilisent des algorithmes mathématiques pour détecter des objets ou en mouvements dans l'image et filtrer les mouvements non pertinents. Ils créent une base de données consignant les attributs de tous les objets détectés et leurs propriétés de mouvements. La prise de décision par le système ou la recherche d'événements d'intérêt dans des séquences archivées se fait à partir de règles (par ex.: si une personne traverse une limite, envoyer une alerte ….) [16,17]

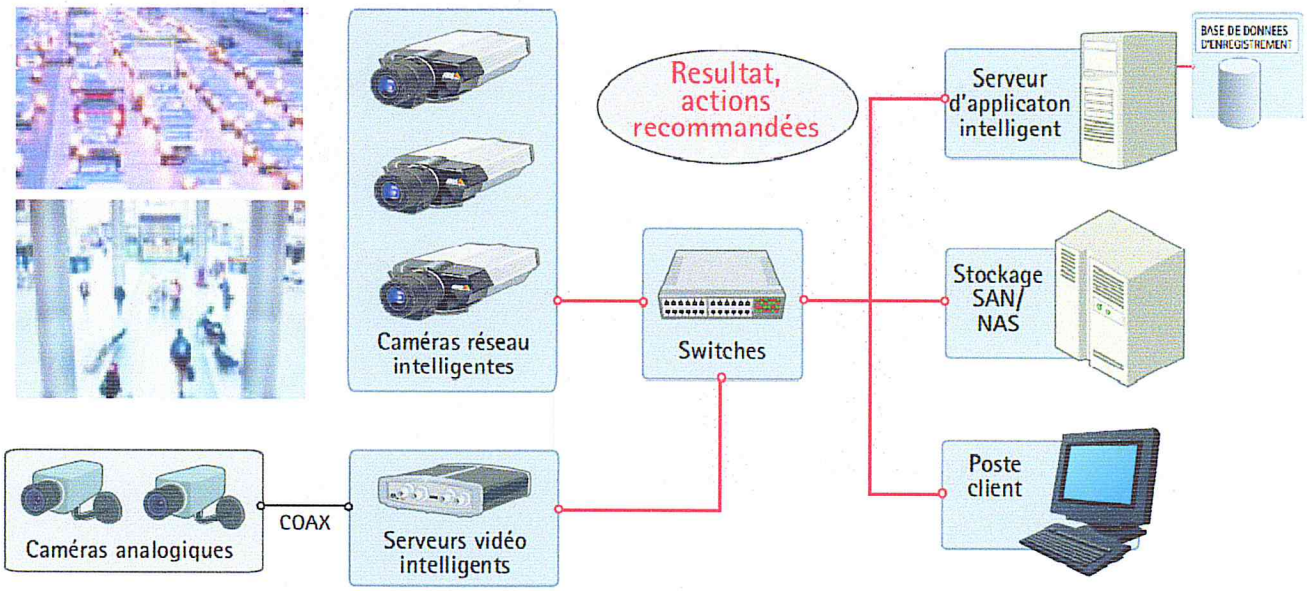


***Figure III.8**: architecture de vidéosurveillance* intelligente

III.12. Méthodes de transmission des données

III.12.1. Les adresses IP

Une adresse IP (adresse de protocole Internet) est un numéro unique permettant aux équipements de s'identifier et de communiquer entre eux sur les réseaux utilisant la norme liée au protocole Internet. Une adresse IP se compose de quatre nombres, séparés par un point. Elle se subdivise encore en une partie réseau et une partie hôte, la séparation entre ces deux parties étant déterminée par la longueur du masque réseau ou du préfixe. Un masque réseau 255.255.255.0 signifie par exemple que les 3 premiers octets constituent l'adresse réseau et le dernier octet l'adresse hôte. La longueur du préfixe est une autre façon de marquer la séparation. Ainsi, dans l'adresse de l'exemple précédent, la longueur du préfixe est de 24 bits (soit 192.36.253.80/24).

III.12.2. Les protocoles de transport destinés à la vidéo sur IP

Le protocole le plus courant pour la transmission des données sur réseaux informatiques est la suite TCP/IP. TCP/IP sert de "transporteur" pour de nombreux autres protocoles, en particulier pour le protocole HTTP (Hyper Text Transfer Protocol) qui permet de consulter les pages des serveurs dans le monde entier via Internet. Les protocoles TCP/IP et les ports utilisés dans le cadre de la vidéo sur IP Les protocoles les plus courants dans le cadre de la transmission des flux vidéo sur IP et leurs numéros de ports correspondants comme la *Figure* IV.*4*

L'IP utilise deux protocoles de transport : le protocole TCP (Transmission Control rotocol) et le protocole UDP (User Datagram Protocol). Le protocole TCP offre un canal de transmission fiable, qui repose sur la notion de connexions ; il prend en charge le processus de séparation de volumes de données importants en paquets plus petits, adaptés à la configuration physique du réseau, et veille à ce que les données envoyées à un bout parviennent bien à l'autre bout. Quant au protocole UDP, il s'agit d'un protocole dit "sans connexion", qui ne garantit pas la livraison physique des données envoyées et laisse donc à l'application le soin de vérifier et de contrôler les erreurs.
En général, le protocole TCP est utilisé lorsque la fiabilité de la communication a priorité sur la latence du transport. La fiabilité obtenue par retransmission peut cependant causer des délais importants. UDP ne permettant pas, en revanche, la retransmission des données perdues, il ne produit dès lors pas non plus de délais supplémentaires. [16]

Protocole	Protocole de transport	Port	Utilisation courante	Utilisation en vidéo sur IP
FTP File Transfer Protocol	TCP	21	Transfert de fichiers sur Internet/intranet	Transfert d'images ou de vidéo de la caméra réseau/serveur vidéo vers un serveur FTP ou une application
SMTP Simple Mail Transfer Protocol	TCP	25	Protocole pour l'envoi de messages e-mail	Une caméra réseau/serveur vidéo peut envoyer des images ou notifications d'alarme à l'aide de son client e-mail intégré
HTTP Hyper Text Transfer Protocol	TCP	80	Utilisé pour le web, par ex. pour accéder à des pages de serveurs web	La manière la plus courante pour transmettre des flux vidéo d'une caméra réseau/serveur vidéo. L'appareil de vidéo sur IP agit comme un serveur web, rendant la vidéo disponible à l'utilisateur ou au serveur applicatif
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	TCP	443	Utilisé pour accéder à des pages web de façon sécurisé à l'aide de l'encryptage	La transmission vidéo sécurisée depuis les caméras réseau/serveurs vidéo peut aussi être utilisée pour authentifier la caméra à l'aide des certificats numériques X.509
RTP Real Time Protocol	UDP/TCP	Non défini	Format de paquets avec encryptage RTP pour fournir de l'audio et de la vidéo sur Internet. Souvent utilisé dans les sytèmes de media streaming ou de vidéoconférence.	Une méthode courante pour transmettre des flux de vidéo sur IP MPEG. La transmission peut être individuelle (unicast) ou multiple (multicast)
RTSP Real Time Streaming Protocol	TCP	554	Utilisé pour configurer et contrôler les sessions multimédia par RTP	

***Figure III.9**: protocole et les ports utilisés dans le système vidéo surveillance*

III.13. Sécurité des réseaux

Il existe plusieurs façons de sécuriser un réseau ainsi que les communications entre différents réseaux et clients. En réalité, tout peut être contrôlé et sécurisé : depuis les données envoyées sur le réseau jusqu'à l'utilisation qui est faite du réseau et son accessibilité.

III.13.1 Sécurisation des transmissions

Assurer la sécurité des transmissions, c'est un peu comme faire appel à un transporteur pour livrer des documents importants d'une personne à une autre. Quand le transporteur arrive chez l'expéditeur, celui-ci lui demande de décliner son identité, suite à quoi, l'expéditeur décide s'il a bien affaire à la bonne personne et s'il peut lui faire confiance. Si tout semble en ordre, la missive scellée lui est remise pour livraison au destinataire. Du côté du destinataire, une même procédure d'identification a lieu, suite à quoi le sceau peut être vérifié et enfin défait. Une fois le transporteur reparti, le destinataire ouvre la missive et en extrait le document pour prise de connaissance.
Une communication sécurisée se crée de la même manière. Elle se déroule selon trois étapes distinctes :

- **Authentification** : Cette première étape doit permettre à l'utilisateur ou au périphérique de s'identifier sur le réseau ou l'hôte distant. Pour ce faire, certaines données d'identité sont communiquées au réseau ou au système, comme par exemple un code d'utilisateur et un mot de passe, un certificat X509 (SSL), et le recours à la norme 802.1x.
- **Autorisation :** L'étape suivante consiste à autoriser et à accepter l'authentification, c'est-à-dire à vérifier si la machine est bien celle qu'elle prétend être. On vérifie à cet effet l'identité donnée par rapport aux informations contenues dans la base de données ou dans une liste d'identités réputées correctes et approuvées. Au terme de l'autorisation, la machine est totalement connectée et opérationnelle dans le système.
- **Confidentialité :** La dernière étape consiste à appliquer le degré de confidentialité souhaité. Pour ce faire, la communication est cryptée afin que les données ne puissent être utilisées ou lues par personne d'autre. Selon le type de déploiement et de chiffrement utilisé, il peut arriver que le recours au cryptage nuise assez fortement aux performances. La confidentialité peut être assurée de plusieurs façons. [16]

III.14. Client /serveur

Dix ans après son apparition le client serveur est devenu l'architecture d'applications la plus prisée, ***Figure III.10*** illustre sa popularité croissante .En fait, il applique un gigantesque aux applications monolithique des site centraux pour répartir les charges de traitement entre client et serveurs.

La manière dont étaient conçues et bâties les applications jusqu'ici en a été révolutionnée, et la facilité d'utilisation désormais offerte aux utilisateurs finaux a répondu à leurs attentes .
Le client /serveur a entrainé dans son sillage , la création d'une énorme industrie logicielle dominée par des géants comme baan , Informix ,Lotus , Microsoft ,Novell ,Oracle , PeopleSoft ,SAP, Sun et Sybase .Superstars de la première époque du client serveur ces entreprises forment aujourd'hui le nouvel establishment de l'informatique [22]

Même si cela peut surprendre une révolution silencieuse est en marche au sein même de la révolution client /serveur la ***Figure III.10*** montre en effet que la technologie client /serveur est en train de passer s'une structure originelle à 2 niveaux à une architecture à 3 niveaux l'impact de ce changement sera plus important encore que l'évolution initiale des applications monolithiques vers le client /serveur . Ce courant vers le modèle à 3 niveaux a été initié par la nécessité d'utiliser la technologie client /serveur pour les grands applications des entreprise, l'Internet, les intranet, les objets distribués et les composants propulsent aujourd'hui la structure à 3 niveaux au cœur du client /serveur

Le client à 3 niveaux est donc devenu la forme dominante de l'informatique et le modèle à 3 niveaux la forme dominante du client /serveur.

III.14. 1. Présentation de l'architecture d'un système Client /Serveur

De nombreuses applications fonctionnent se ;on un environnement client /serveur , cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur , un machine généralement très puissante en termes de capacités d'entrée –sortie , qui leur fournit des services , ces services sont des programmes fournissant des données telle que l'heure , des fichiers , connexion ……etc. [19]

Les services sont exploité par des programmes appelés programmes clients s'exécutant sur les machines clientes , on parle ainsi de client (client FTP (File transport Protocol) , client de messagerie ,……) lorsque l'on désigne un programme tournant sur un machine cliente , capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP , il s'agit de fichiers tandis que pour le client de messagerie , il s'agit de courrier électronique) .

III.14. 2. Avantages de l'architecture Client /Serveur

Le modèle Client /Serveur est Particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité ses principaux atouts sont

- **des ressource centralisées :** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction
- **une meilleure sécurité :** car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **une administration au niveau serveur :** les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés [19]
- **un réseau évolutif :** grâce à cette architecture, il est possible se supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure

III.14.3. Inconvénients du modèle Client / Serveur :

L'architecture Client /Serveur a tout de même quelque lacunes parmi lesquelles :

- **Un coût élevé** dû à la technicité du serveur.
- **Un maillon faible :** le serveur est le seul maillon faible du réseau Client /Serveur étant donné que tout le réseau est architecturé autour de lui, Heureusement, le Serveur a une grand tolérance aux pannes.
- **Fonctionnement d'un système Client /Serveur**

Un système client /serveur selon le schéma suivant :

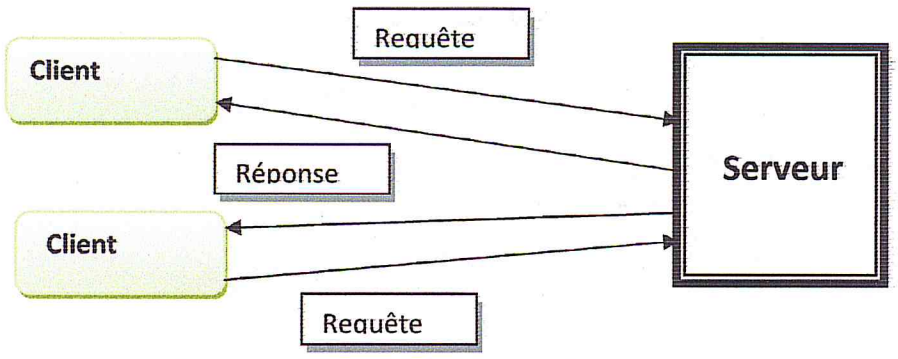


Figure III.11 : Architecture Client /Serveur

- Le Client émet une requête vers le serveur grâce à son adresse IP(Internet Protocol) et le port , qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répand à l'aide de l'adresse de la machine cliente et son port.

III.14.4. Architecture Mainframe

Les premiers réseaux informatique étaient architecturés autour d'un ordinateur central, appelé « mainframe »

Le mainframe représente ainsi un ordinateur central de grand puissance chargé de gérer les sessions utilisateurs des différents terminaux qui lui étaient reliés , grâce à cette architecture , il est ainsi possible de consolider , c'est –à-dire de gérer de manière centralisée l'ensemble des applications métiers de l'entreprise .

Cependant, dans le modèle mainframe, la performance du système tout entier repose sur les capacités de traitement de l'ordinateur centrale, c'est la raison pour laquelle ce modèle est parfois qualifié « d'informatique lourde » par ailleurs dans un environnement mainframe les terminaux du réseau ne peuvent voir que le serveur central [19]

III.14.5. Présentation de l'architecture à 2 niveaux

L'architecture à deux niveau (aussi appelée architecture 2-Tier , Tier : signifiant rangée en an anglais [20]) caractérise les système client / serveur pour lesquels le client demande une ressource et le serveur la lui fournit directement , en utilisant ses propres ressource . Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.

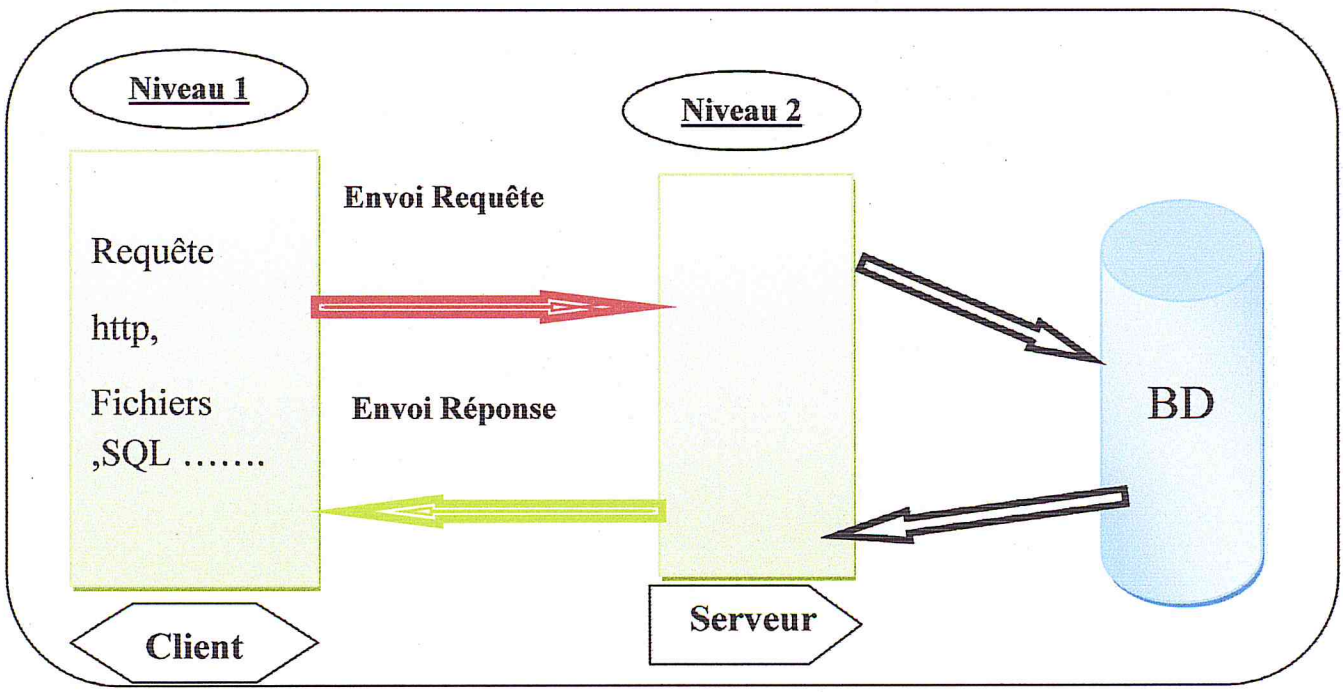


Figure III.12 : Architecture à deux niveaux

III.14.6. Présentation de l'architecture à 3 niveaux

Dans l'architecture à 3 niveaux (appelée architecture 3-tier) , il existe un niveau intermédiaire , c'est –à-dire que l'on a généralement une architecture partagée entre :

1- Un client , c'est-à-dire l'ordinateur demandeur de ressources ,équipée d'une interface utilisateur (généralement un navigateur Web) chargée de la présentation
2- Le serveur d'application (appelé également **middleware) ,** chargé de fournir la ressource mais faisant appel à un autre serveur
3- Le serveur de données , fournissant au serveur d'application les données dont il a besoin [20]

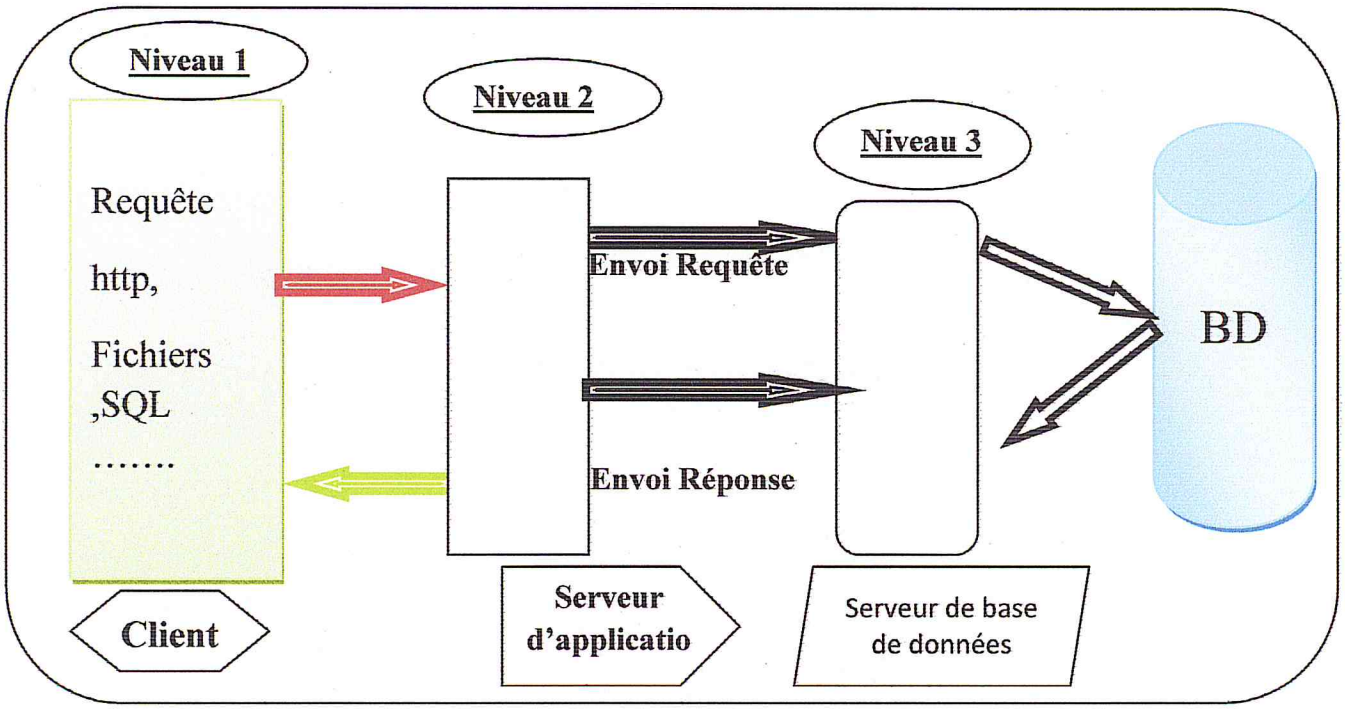


Figure III.13 : Architecture à trois Niveaux

Etant donné l'emploi massif du terme d'architecture à 3 niveaux, celui-ci peut parfois désigner aussi les architectures suivantes :

- Partage d'application entre client, serveur intermédiaire, et serveur d'entreprise
- Partage d'application entre client, serveur d'application et serveur de base de données d'entreprise

III.14.7. Comparaison des deux types d'architecture à 2 et 3 niveaux :

L'architecture à deux niveau est donc une architecture Client / Serveur dans laquelle le serveur est polyvalent c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client .

Dans l'architecture à trois niveau par contre , les applications au niveau sont délocalisées , c'est-à-dire que chaque serveur est spécialisé dans un tâche (serveur web/ serveur de base de données par exemple) .L 'architecture à trois niveau permet :

- Une plus grand flexibilité / souplesse
- Une sécurité accrue car la sécurité peut être définie indépendamment pour chaque service et à chaque niveau
- De meilleures performances, étant donné le partage des tâches entre les différents serveurs

III.14.8. L'architecture multi niveaux :

Dans l'architecture à 3 niveau , chaque serveur (niveau 2 et 3) effectue une tâche « une service » spécialisée .un serveur peut donc utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service . par conséquent , l'architecture à trois niveaux est potentiellement une architecture à N niveaux [21]

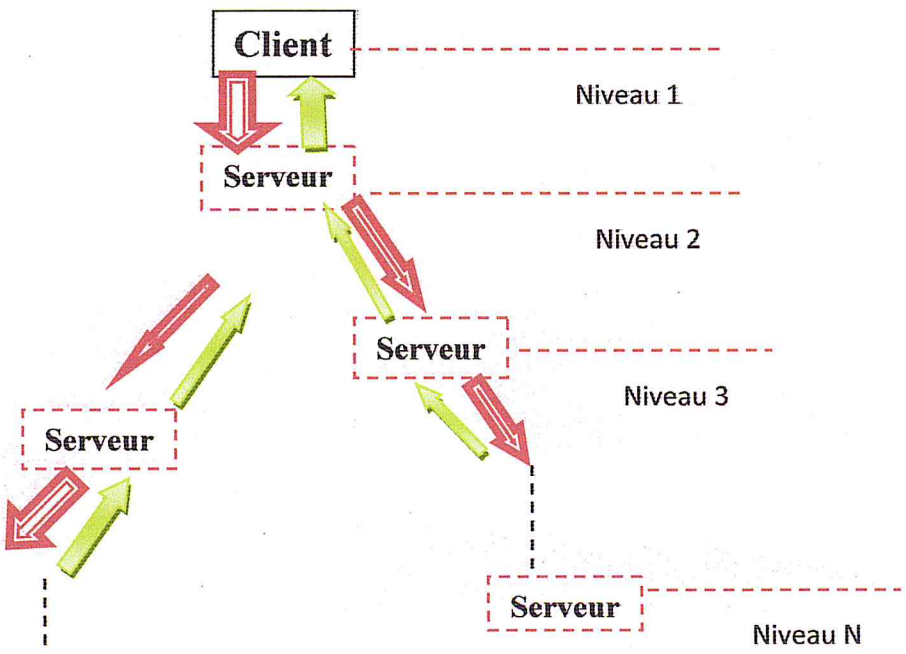


Figure III.14 : Architecture à multi-niveaux

III.14.9. Différents types de clients

- **Client lourd :** Le terme « client lourd » (en anglais « Fat Client » ou « Heavy client ») par opposition au client léger , désigne une application client graphique exécutée sur le système exploitation de l'utilisateur .un client lourd possède généralement des capacités de traitement évoluées et peut posséder une interface graphique sophistique néanmoins ,ceci demande un effort de développement et tend à mêler la logique de présentation (interface graphique) avec la logique applicative (les traitement).

Ce type d'application étant généralement installé sur le système d'exploitation de l'utilisateur , une nouvelle version doit être installée afin de al faire évoluer . pour y remédier , les éditeurs d'applications lourdes les dotent généralement d'une fonctionnalité exécutée au lancement de l'application , permettant de vérifier sur un serveur distant si une version plus récente est disponible et le cas échéant propose à l'utilisateur de la télécharger et de l'installer [19]

- **Client léger :** Le terme « client léger » (parfois « client pauvre » , en anglais « thin client ») par opposition au client lourd , désigne une application accessible via une interface web (en HTML) consultable à l'aide d'un navigateur web ,où la totalité de la logique métier est traitée de coté du serveur .pour ces raisons , le navigateur est parfois appelé client universel

L'origine du terme lui-même provient de la pauvreté du langage HTML (Hyper Text Markup Language) , qui ne permet de faire des interfaces relativement pauvres en interactivité si ce n'est par le biais du langage javascript

Le fait que l'essentiel des traitements soit réalisé du coté du serveur et que l'interface graphique soit envoyée au navigateur à chaque requête permet une grand souplesse de mise à jour .En contrepartie l'application doit s'affranchir des différances d'interprétation du code HTML par les différents navigateurs et l'ergonomie de l'application possède un champ réduit [19]

- **Client riche** : Un client riche est un compromis le client léger et le client lourd . L'objectif du client riche est donc de proposer une interface graphique , décrite avec une grammaire de description basé sur la syntaxe XML (eXtended Markup language) permettant d'obtenir des fonctionnalités similaire à celles d'un client lourd (glisser déposer , onglets , multi fenêtrage , menus déroulants

Les client riche permettent ainsi de gérer l'essentiel des traitement du coté du serveur les données sont ensuite transmises dans un format d'échange standard utilisant la syntaxe XML, puis interprétés par le client riche [19]

III.15. conception et Modélisation :

III.15.1 UML : outil de modélisation

Nous utilisons UML Comme langage Efficace pour modéliser notre Système

- III.15.2 Diagrammes de cas d'utilisation

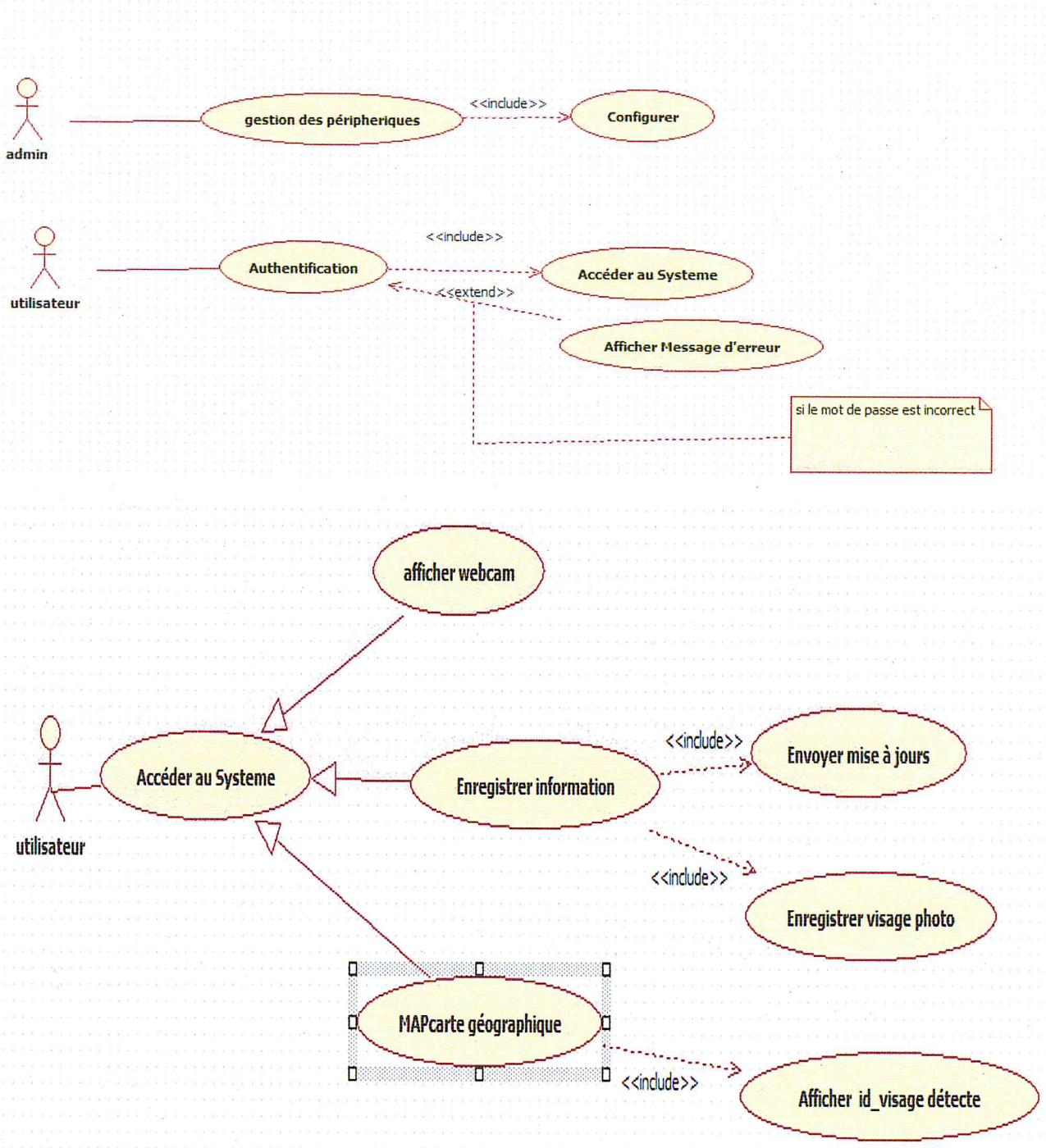


Figure III.15: **Diagramme de cas d'utilisation d'un système vidéosurveillance**

- **Description du diagramme de cas d'utilisation**

cas d'utilisation	Description
Gestion du périphérique	Gestion des caméra installation des caméras et ip des ces caméras
Mise à jour	Droit d'Access à la base de données ajouter supprimer modifier
Configuration	Configuration des adresse ip des caméra
Accéder au système	Accéder au système si la vérification si la opération réussie
Afficher message d'erreur	Afficher message d'erreur opération fausse
Afficher webcam	afficher tout les caméras qui sont connecte avec le serveur
Envoyer mise à jour	Envoyer la mise à jours des nouveaux visage vers visage à toutes les caméras
Enregistrer visage photo	Envoyer la mise à jours des nouveaux visage vers tout les caméra
MapCarte géographique	Afficher la localisation dans un carte géographique des visages détectés
Afficher id-visage détecte	Affiche tous les visages détecté par id personne et le temps de détection

Tableau III.1. Description du diagramme de cas d'utilisation

III.15.3 Scenarios et diagramme de séquences

Analyse

L'analyse permet de lister les résultats attendus, en terme de fonctionnalités, de performance, de robustesse, de maintenance,… etc.

L'analyse répond donc à la question « *que faut-il faire ?* » et a pour but de se doter d'une vision claire et rigoureuse du problème posé et du système à réaliser en déterminant ses éléments et leurs interactions.

Définition d'un scénario [23]

Un scénario représente un ensemble ordonné de messages échangés par des objets. On parle ici d'objet au sens large : instance de classe d'analyse ou instance d'acteur.
Les échanges de messages entre objet peuvent être représentés en UML dans une sorte de diagramme complémentaire appelé diagramme de séquence.

Définition du diagramme de séquence [24]

Un diagramme de séquence est une représentation séquentielle du déroulement des traitements et des interactions entre les éléments du système et / ou de ses acteurs.

Les diagrammes de séquences permettent de représenter des collaborations entre objets selon un point de vue temporel, on y met l'accent sur la chronologie des envois de messages.
Dans ce qui suit nous allons présenter les diagrammes de séquence afin de formaliser les scénarios des cas d'utilisation vus précédemment. Nous allons voir le système comme un ensemble d'objet en interaction.

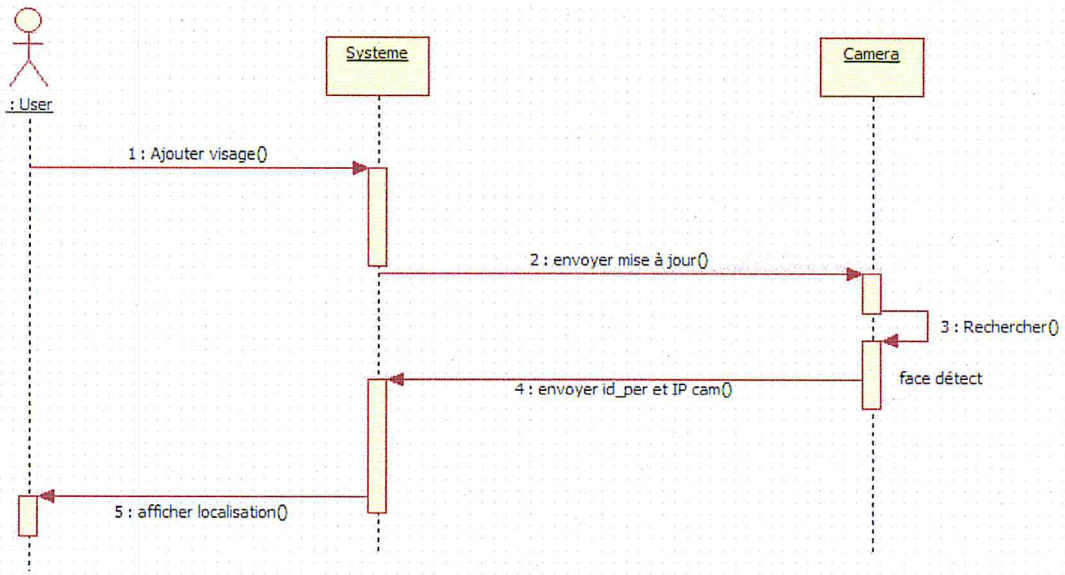


Figure III.16. Diagramme de séquence d'un système vidéosurveillance

III.15.4. Diagramme de classe

Les diagrammes de classes présentent un ensemble d'éléments de modèle statiques, leur contenu (structure interne) et leurs relations aux autres éléments. [25]

Une classe représente la description abstraite d'un ensemble d'objets possédant les mêmes caractéristiques. Un attribut est un camp de classes, c'est-à-dire un type d'information contenu dans la classe.

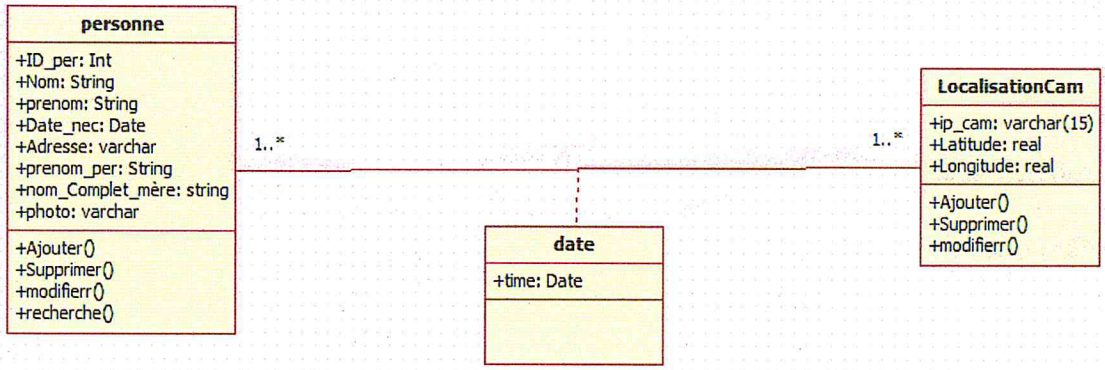


Figure III.17. Diagramme de classe

- **Descriptions des données des classes**

Nom de classe	Identifient	Attribut	Type
LocalisationCam	IP_cam	Ip_cam	varchar
		Latitude	Real
		Longitude	Real

Nom de classe	Identifient	Attribut	Type
Date		time	Date

Nom de classe	Identifient	Attribut	Type
Personne	ID_per	ID_per	int
		Nom	String
		prénom	String
		Date_nec	Date
		Adresse	varchar
		prenom_per	String
		Nom_complet_mer	String
		Photo	varchar

Tableau III.2 : Descriptions des données

III.16. Conclusion

Dans ce chapitre, nous avons présenté le travail selon deux partie, dans la première partie on a abordé la méthode de viola et jones pour la détection du visage et les éléments de la méthode et la architecture de vidéosurveillance intelligente. La seconde partie présente l''étude conceptuelle qui nous a permis de mettre en évidence les étapes nécessaires pour la création de l'application vidéosurveillance intelligente. Cette étude nous a permis aussi de mettre en évidence les différentes classes du système.

Dans le chapitre suivant, nous allons implémenter et mettre en œuvre ce que nous avons proposé dans l'étude conceptuelle de notre système.

CHAPITRE VI

Implémentation

IV.1. Introduction

Après avoir présenté dans le chapitre précédent la modélisation UML de notre application. L'objectif de ce chapitre est de présenter notre logiciel

Nous commençons ce chapitre par la présentation de l'environnement matériel et logiciel que nous avons utilisé pour atteindre notre objectif

IV.2. Environnement de développement

IV.2.1. Environnement logiciel

IV.2.1.1 La structuration de données (SQL Serveur)

Un serveur de bases de données stocke les données dans des tables séparées plutôt que de tout rassembler dans une seule table. Cela améliore la rapidité et la souplesse de l'ensemble. Les tables sont reliées par des relations définies, qui rendent possible la combinaison de données entre plusieurs tables durant une requête. [26]

IV.2.1.2 Le langage de programmation choisi (Visual Studio C#)

C sharp est un langage orienté objet de type sécurisé et élégant qui permet aux développeurs de générer diverses applications sécurisées et fiables qui s'exécutent sur le .NET Framework. Vous pouvez utiliser le langage C# pour créer entre autres des applications clientes Windows, des services Web XML, des composants distribués, des applications client-serveur et des applications de base de données. Visual C# fournit un éditeur de code avancé, des concepteurs d'interfaces utilisateur pratiques, un débogueur intégré et de nombreux autres outils pour faciliter le développement d'applications basées sur le langage C# et .NET Framework.

IV.2.1.3 Library Opencv

Opencv (Open Computer Vision) est un librairie Open source qui comporte un certain nombre des algorithmes et des exemples des codes pour la vision ordinateur cette librairie vise a simplifier la conception d'applications d'idées à la vision en temps réel , la reconnaissance de contours , la segmentation .....etc , le fait qu'elle soit Open Source signifie qu'elle est très évolutive puisque le développement de nouvelles fonctions , nouveaux algorithmes , sont réalisée par une vaste communauté ,par ailleurs OpenCv est bâti sur IPL (Intel Image Processing library) dont elle reprend le format d'images (IPL image) ainsi qu'un certain nombre de fonctions de filtrage , ... ,elle implémente également un certains nombres d'algorithmes exclusifs . la librairie rajoute également un certain nombre de notions telles que la gestion des espaces couleurs **RGB** .

OpenCv est composé de quatre grands blocs de fonctions.

- **CXCore** comporte les fonctions de base d'OpenCv (fonctions de dessin, de gestion des points .....)
- **CV** comporte les fonctions principales du traitement de l'image : un certain nombre de fonctions de filtrage , ainsi que les fonctions de calibration ,appariement .....
- **HighGui** comporte les fonctions de gestion des interfaces graphique celle-ci sont simplifiée et permettent principalement la création de fenêtres graphique dans lesquelles seront affichées des images ou des flux des images (vidéo) [27]
- **CvCam** contient un certain nombre de fonctions de gestions de WebCams ,utiles pour ouvrir des flux vidéo .

Notons par ailleurs que la librairie fonctionne sous Windows, Linux, Androïde , et est adaptée pour les langages c++, c# , java , Python.

Library OpenCV offre:

- Traitement d'images

Elle propose la plupart des opérations classiques en traitement bas niveau des images - lecture, écriture et affichage d'une image, calcul de l'histogramme des niveaux de gris ou d'histogrammes couleurs, lissage, filtrage, segmentation en composantes connexes [27]

- Traitement vidéos

Cette bibliothèque s'est imposée comme un standard dans le domaine de la recherche parce qu'elle propose un nombre important d'outils issus de l'état de l'art en vision des ordinateurs tels que

- lecture, écriture et affichage d'une vidéo (depuis un fichier ou une caméra)
- détection de visages par la méthode de **Viola** et **Jones**
- cascade de classifieurs Boostés
- détection de mouvement
- poursuite d'objets par mean-shift ou Camshift « Tracking»

- Algorithmes d'apprentissage

Certains algorithmes classiques dans le domaine de l'apprentissage artificiel sont aussi disponibles :

K-means , AdaBoost , Réseau de neurones artificiels **RNA** , Machine à vecteurs de support **SVM** , Estimateur (statistique)

- Calculs Matriciels

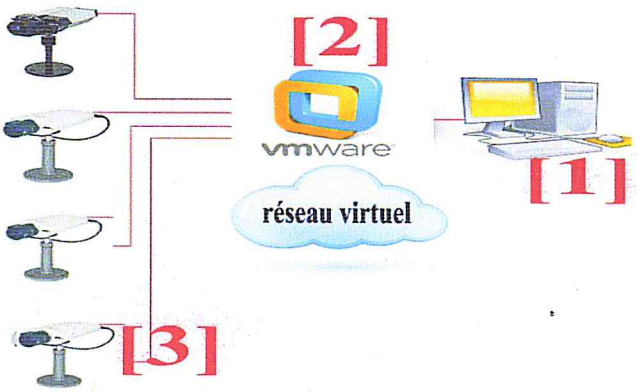
OpenCV l'accent a été mis sur les matrices et les opérations sur celles-ci. En effet, la structure de base est la matrice. Une image peut être considérée comme une matrice de pixel. Ainsi, toutes les opérations de bases des matrices sont disponibles,

IV.2.1.4 VMware Workstation

VMware créer un environnement clos dans lequel sont disponibles un, deux, quatre ou huit (vSphere) processeur(s), des périphériques et un BIOS virtuel.

VMware Workstation est reconnu pour sa large prise en charge de systèmes d'exploitation, son environnement utilisateur riche, son ensemble complet de fonctionnalités et ses hautes performances. VMware Workstation est conçu pour les professionnels qui utilisent des machines virtuelles

IV.2.2. Environnement Matériel



1:pc
2: VMware Workstation
(réseau virtuelle)
3: Camera

Figure IV.*1* : Environnement Matériel

IV.3. L'interface graphique :

Le système vidéosurveillance se compose de deux applications application serveur et application client qui Capture des images de caméra et les envoie au serveur .

Application Serveur : reçoit les vidéo en ligne et si une caméra détecte un visage d'un personne est tenue Caméra envoyer l'ID au Serveur, à la réception ID le serveur affiche ID de ce personne et la localisation de camera qui envoyer le message dans un carte géographique le système lance un alerte à l'utilisateur.

IV.3.1 LOGIN

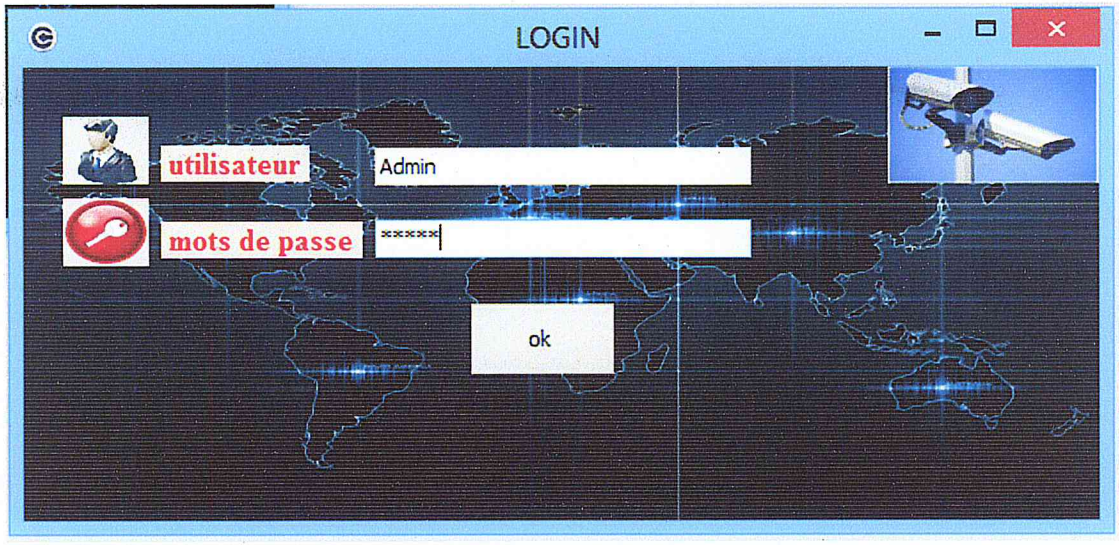


Figure* IV.*2 : Interface LOGIN Système vidéosurveillance

C'est l'interface qui permet d'accéder au contenu du système vidéosurveillance l'utilisateur entre son nom d'utilisateur et son mot de passe si la vérification est réussie le système ouvre l'interface principale. Sinon un message d'erreur indiquera la vérification a échoué.

IV.3.2 l'interface principale

L'interface principale il se compose à trois « tabPage »

IV.3.2 .1.En ligne Cam

1L'interface qui contient tout les caméras qui connecté avec le serveur et affiche dans un

1	Les web came en Ligne
2	Liste panel affiche toute Les adress ip des camera
3	Traitement Vidéo pour la reconnaissance le visage du fichier video « mp4,wmv,avi.... »

Tableaux IV.1 : En ligne Cam

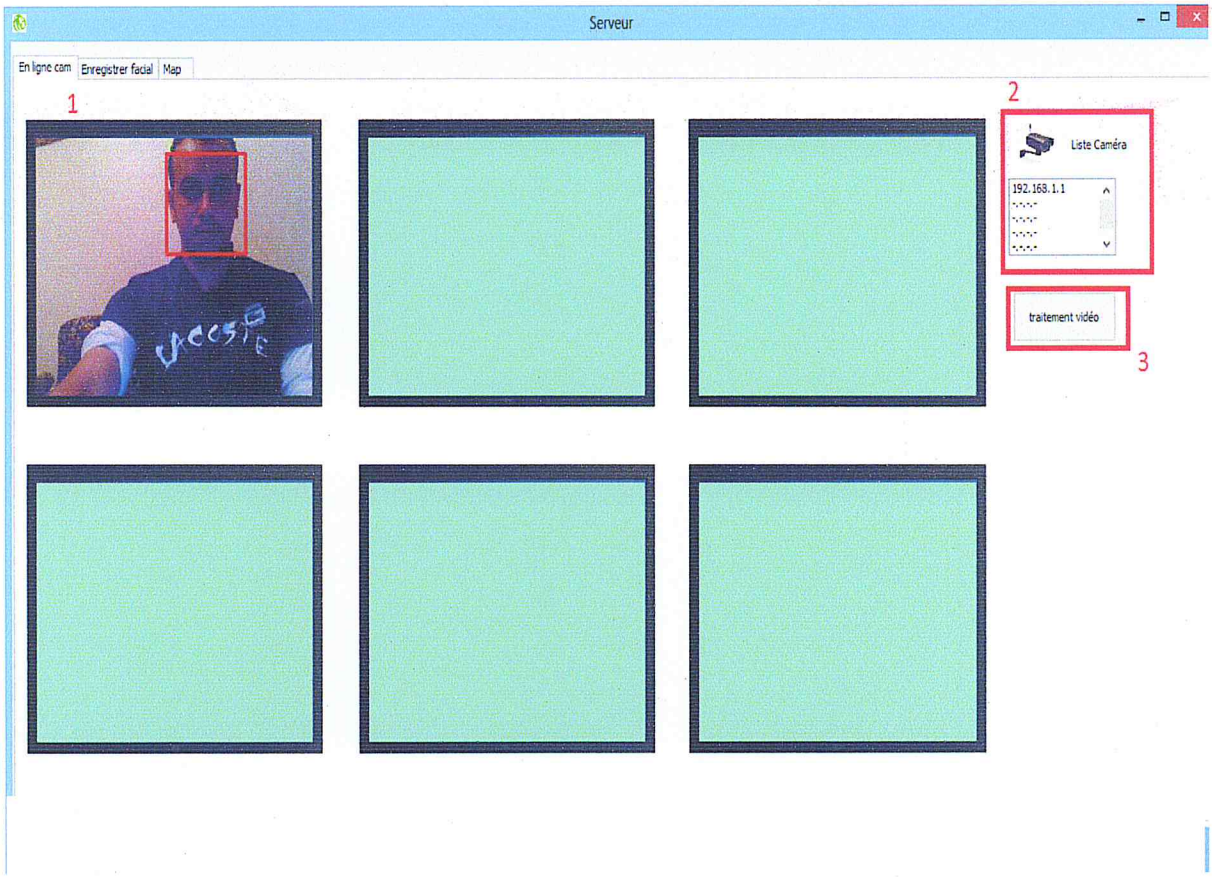


Figure IV.*3 : Interface* En ligne Cam

IV.3.2 .2. Traitement Vidéo

Fonction de cette bouton si on souhaite traitement un fichier vidéo « Mp4, AVI, Wmv »

Pour la reconnaissace visage dans ce fichier

1	Ouvrir un fichier média
2	Play fichier média
3	Tableaux pour Affiche les id des visages détectés
4	Affiche carré rouge si visage dans la base de donnée sinon affiche carré vert

Tableaux IV.2 : Traitement vidéo

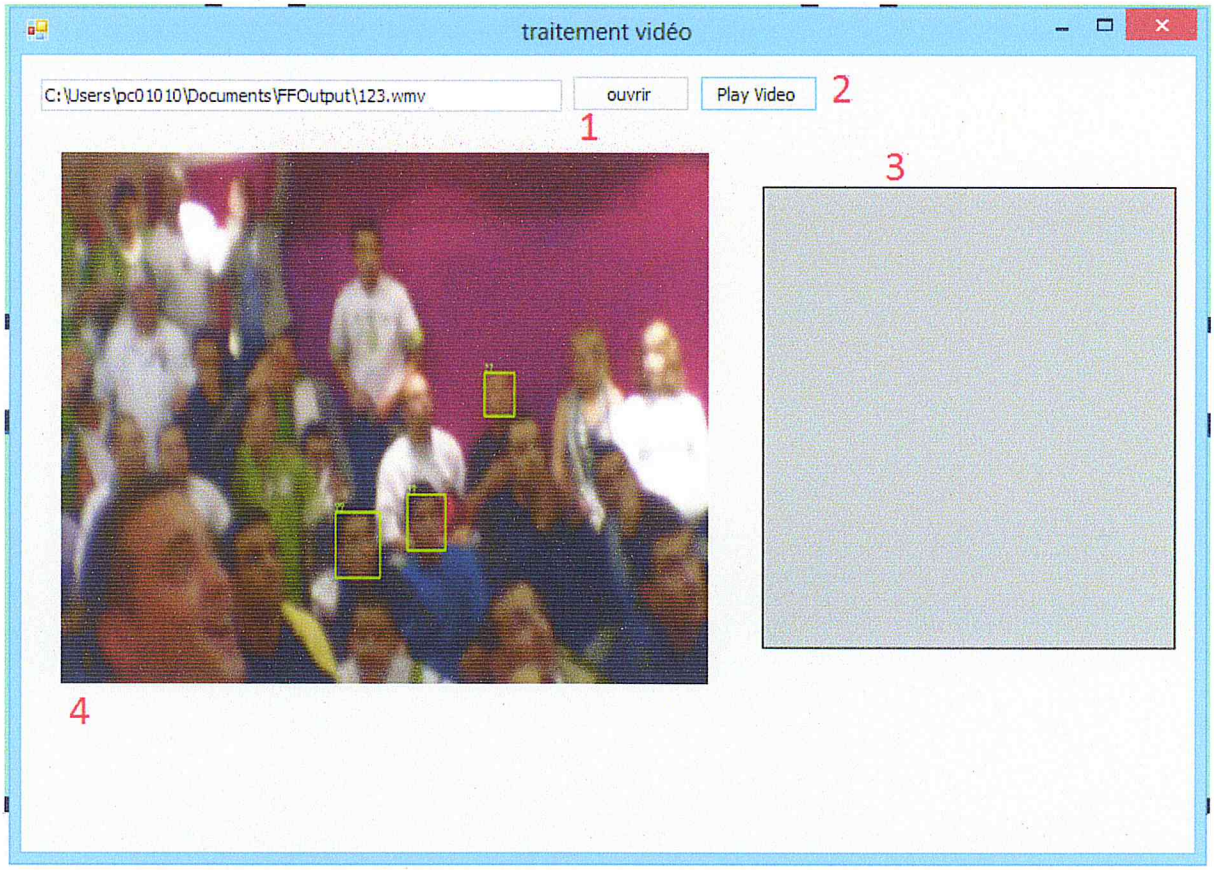


Figure IV.*4 : Interface traitement vidéo*

IV.3.2 .3. Enrigistre Facial

Dans ce « tabPage » on saisir le visage des personnes pour rechercher Des ces personnes, et envoyer la mise à jour pour toutes les webcams.

1	Ouvrire l'image de personne
2	Affiche le visage du personne
3->8	Les informations personne
9	Ajouter à la base de données
10	envoyer la mise à jour pour toutes les webcams

Tableaux IV.3 : Enrigistre Facial

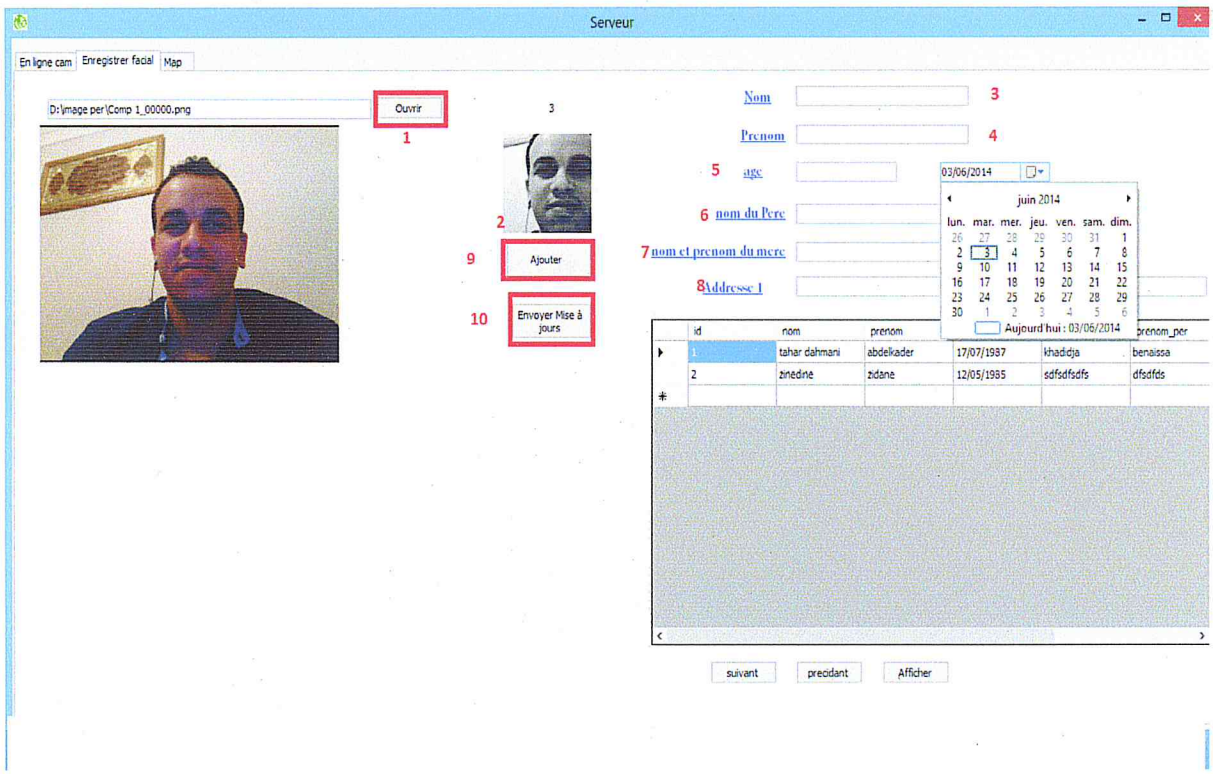


Figure *IV.5* : *Enrigistre Facial*

IV.3.2 .4. MAP

Dans ce map le systéme affiche tous les visage détect par ip_camera et la localisation géographique dans un map et le id de visge détecté .

1	Latitude de caméra
2	Longitude de caméra
3	Ip-camera
4	Ok pour ajouter un nouvelle cameras aux un base de donnée
5	obtention les Latitude et Longitude pour 1 et 2
6	Affiche les markers dans un map par date
7	Button pour afficher les id dans un tableaux par date et recherche les informations de ce id (nom prénom …..)

Tableaux IV.4 : MAP

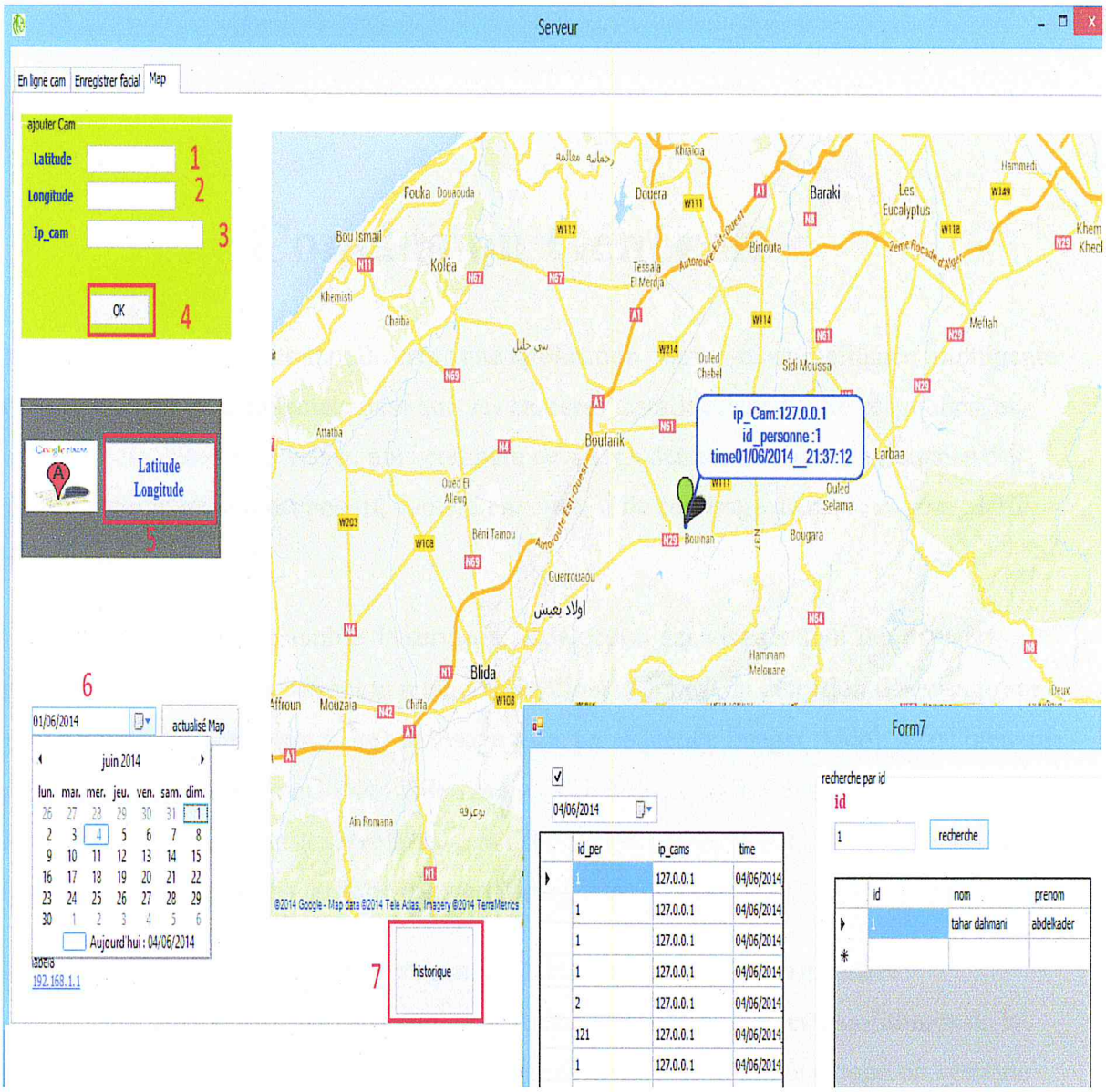


Figure *IV.5* : MAP

IV.4.Conclusion

Dans ce chapitre nous avons présenté brièvement l'environnement de programmation. Nous avons aussi décrit l'interface du système vidéosurveillance avec toutes les fonctionnalités qu'elle permet d'accomplir.

Bibliographie

[1]A. Belaid et Y. Belaid – RdF : méthodes et application– (Bibliothèque 14)

[2] http://www.biometrique.fr/biometrique.htm [En ligne]

[3] Biométrie pour l'Identification http://www.ifi.auf.org/site_data/rapports/tpe-promo10/tipe-dang_hoang_vu.pdf

[4] Reconnaissance Biométrique par Fusion Multimodale , Thèse présentée pour obtenir le grade de Docteur de l'Ecole Nationale Supérieure des Télécommunications : Spécialité : Signal et Images

[5] L.Carminati : *Détection et suivi de visage par Support Vector Machine robustes aux changements d'echelle*, Thèse du Centre National de la Recherche Sientifique.

[6] M. Benkiniouar, M. Benmohamed : *Méthodes d'identification et de reconnaissance de visages en temps réel basées sur AdaBoost*, Novembre 2005

[7] F. Boray Tek: *Face detection using learning networks*, A thesis from the middle east technical university, June 2002

[8] A Pentland, B. Moghaddam, and T. Strarner. *View-based and modular eigenspaces for face recognition*. IEEE Proc. of Int. Conf. on Computer Vision and Pattern Recognition, pages 84-91, 1994.

[9] M.turk , A.pentland EigenFcae for recognition ‚Journal Of Conitiv Neurocience Vol3 N01 1991 p.71.86

[10] S.-H. Lin, S.-Y. Kung, and L.-J. Lin. *Face recognition/detection by probabilistic decision based neural network*. IEEE Trans. Neural Networks, 8:114-132, 1997.

[11] E. Hjelmas et B. K. Low, Face Detection: A Survey , *Computer Vision and Image Understanding*, volume 83, pages 236-274, 2001.

[12] Paul Viola, Michael Jones Rapid Object Detection using a Boosted Cascade of Simple , Accepted Conference on Computer Vision and Pattern Recognition 2001

[13] http://fr.wikipedia.org/wiki/M%C3%A9thode_de_Viola_et_Jones [En ligne]

[14] M. Van Wambeke Reconnaissance et suivi de visages et implémentation en robotique temps-réel 2009

[15] P.Van Viet Détection de visages 2D dans des poses frontales et non-frontales 2010

[16] Guide technique de la vidéo sur IP. [En ligne] www.axis.com , http://www.concept-telecom.fr/doc/techguide.pdf

[17] Conception d'un système de vidéosurveillance intelligente pour l'IMT http://www.fresnel.fr/perso/derrode/poly/Rapport_PT_CRS.pdf

[18]Philippe Junnemann Client Serveur : les raisons du succès par Addison wesley France 1995

[19] Robert Orfali ,Dan Harkey , Jeri Edwards Client /serveur :guide de survie publié par internationale Thomson publ. France 1995

[20] Alain Lefebvre L'architecteur client /serveur Aspects techniques enjeux stratégique publier par Armand Colin 1995

[21] D.Dromard ,D.Seret architecteur des réseaux publier par Pearson Education .France 2006

[22] IF -457 –EX 3 Bibliothèque 14 client /serveur à 3 niveaux En Pratique

[23] Site officiel de Java, «Définition d'un scénario de diagramme de séquence» [Enligne]http://www.istantic.com/v2/programmation/Java/Generalites/Generalites.html

[24] Site officiel d'éclipse, «Définition de diagramme de séquence» [En ligne] http://www.eclipse.org .

[25] Site officiel des objets, «Définition de diagramme de classe » [En ligne] http://support.objecteering.com/objecteering6.1/help/fr/objecteering_uml_modeler/diagrams/class_diagrams.html.

[26] Techniques Contrôle d'accès par Biométrie http://www.clusif.asso.fr/fr/production/ouvrages/pdf/controlesaccesbiometrie.pdf

ANNEXe

A.1. Qu'est-ce qu'un réseau ?

C'est un ensemble de matériels et de logiciels permettant à des équipements de communiquer entre eux.

L'objectif d'un réseau est le partage des ressources matérielles (disques durs, imprimantes) et des ressources logicielles (Fichiers, applications).

Les réseaux regroupent un ensemble hétérogène d'architectures, du filaire au sens-fil, du LAN au WAN

A.2. Topologies de réseaux

Les principales topologies de réseaux existantes :

- en étoile
- en bus
- en anneau
- maillé

Ces éléments de base sont combinés pour former des réseaux complexes

A.3.Commutation.

Manière de faire passer l'information de l'émetteur au récepteur

- Commutation de circuits
- Commutation de paquets
- Commutation de cellules

A.3.1 Commutation de circuit

Utilisée sur le réseau téléphonique, RNIS, GSM

- Création d'un circuit physique reliant les deux se extrémités lors de l'établissement de la connexion
- Elle est adaptée au transport de la voix
- Contrainte de temps de transmission (téléphonie : isochronie et écho)
- Inconvénient : le circuit est occupé pendant la communication, qu'il soit utilisé ou non

A.3.2. Commutation de paquets

- L'information est découpée en paquets qui sont transportés de point en point à l'autre extrémité du réseau
- La commutation de paquets est utilisée sur les réseaux locaux, Internet, Frame Relay, GPRS
- Elle est adaptée au transport des données

A.3.2. Commutation de cellules

- Utilisée par ATM (Asynchronous Transfer Mode)
- Cellule de taille Fixe 53 octets (5 d'en-tête + 48 de données)
- Temps de commutation très faible par rapport au temps de propagation du signal
- Permet d'introduire des notions de qualité de service
- Utilisée principalement sur les liens d'interconnexion ou dans des applications multimédia

A.4. Mode avec / sans connexion

- **Mode connecté :** toute transmission doit être précédée d'une demande de connexion réussie
  - permet de contrôler proprement la transmission : Authentification des intervenants, contrôle de Flux
  - trois phases : établissement de la connexion, transfert des données, coupure de la connexion
  - Les Ressources mobilisées ne sont pas forcément utilisées
- **Mode non connecté :** pas de négociation entre les intervenants (ni contrôle de Flux ou d'erreur) bon pour des envois de messages courts

A.5. Mode d'envoi des informations

- **Unicast :** point à point ; une source, une destination. C'est le cas général

- **Multicast** : multidiffusion une source, des destinations multiples, Permet d'atteindre plusieurs correspondants à la fois, utilisé dans certaines applications

- **Broadcast** : multidiffusion ; une source, toutes les cibles possibles (en général, toutes les machines d'un réseau local)

A.6. Le Modèle OSI

A.6.1.OSI: Open Systems interconnection

C'est une classification des problèmes à résoudre dans un réseau il comporte 7 couches

Application
Présentation
Session
Transport
Réseaux
Liaison de données
Physique

Modèle OSI

- **Couche Physique**
  - Couche basse (électronique ou optique)
  - Circulation des bits d'information (0/1)
  - Fibre optique : lumière
  - Cuivre : paire torsadée, ondes électriques
  - Ondes radio : Wifi, BLR, satellite
  - Matériels passifs : répéteurs, ponts
  - Matériels actifs : commutateurs

- **Couche Liaison de données**
  - Transmission des données en « trames », en séquence
  - Gestion Des acquittements, détection des erreurs, régulation du trafic

- **Couche Réseau**
  - Permet d'établir, maintenir et libérer des connexions
  - Gère l'acheminement des paquets (adressage, routage de point en point)
  - Interconnecter des réseaux hétérogènes

- **Couche Transport**
  - Transporter les données de manière transparente entre deux systèmes
  - Fournit un service de bout en bout, avec le contrôle d'infor mations et la qualité de service
  - TCP, UDP

- **Couches Session, Présentation**
  - Session : organise et structure le dialogue entre applications : dans les deux sens en même temps ou chacun son tour, synchronisation
  - Présentation : fournit à l'application une abstraction de la représentation des données

- **Couche Application**
  - Ce que voit l'usager
  - Liaison Entre la pile réseau de la machine et les programmes
  - Fournit des éléments et services de base aux applications : routines system, communication interprocessus, accès aux protocoles et aux services sur le réseau

A.7. Encapsulation entre couches

- Une couche offre un ensemble de services à la couche immédiatement au-dessus
- Chaque passage à la couche inférieure ajoute son en-tête
- Chaque passage à la couche supérieure enlève les informations propres à la couche du dessous