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

Université Abderahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire De Fin d'Etude

En vue de l'obtention du diplôme de master professionnel en informatique

spécialité : Administration et Sécurité des Réseaux informatiques

Thème :

Reconnaissance faciale par la télésurveillance

Réalisé par :

MESROUA Djamel

REBOUH Syphax

Devant le jury composé de :

Présidente	**M^me^ S.ALOUI**	**U. A/Mira Béjaïa.**
Examinatrice	**M^me^ H.KHALED**	**U. A/Mira Béjaïa.**
Examinatrice	**M^me^ A.HOUHA**	**U. A/Mira Béjaïa.**
Promotrice	**M^me^ S.AIT KACI AZZOU**	**U. A/Mira Béjaïa.**

Béjaïa, 2017

REMERCIEMENTS

Nous adressons nos profonds remerciements à :

Nos très chers parents pour leur soutien et encouragement durant toutes nos années d'études et sans lesquels on n'aurais jamais réussi.

Nos frères et sœurs, pour leur présence, leur soutien morale et leurs encouragements.

Madame S.AIT KACI AZZOU d'avoir accepté de nous encadrer pour ce mémoire de fin d'étude, de son aide et de sa disponibilité tout au long de cette période.

Les membres du jury qui ont acceptées d'évaluer notre travail.

Mr H.BRADAI, pour son accueil durant le stage qu'on a effectué à la BADR de béjaia.

L'ensemble des enseignants qui ont contribué à notre formation.

Nos amis et toutes les personnes qui nous ont aidé de près ou de loin à réaliser ce modeste travail.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

Abréviation	**Signification**
ACP	**A**nalyse en **C**omposantes **P**rincipales
ALE	**A**gences **L**ocal d'**E**xploitation
BADR	**B**anque de l'**A**griculture et du **D**éveloppement **R**ural
CCD	**C**harged **C**oupled **D**evice
CMOS	**C**omplementary **M**etal **O**xide **S**emiconductor
CRM	**C**entre **R**égional de **M**aintenance
DEDI	**D**irection de l'**E**xploitation et du **D**éveloppement **I**nformatique
DGA	**D**irections **G**énérales **A**djointes
DM	**D**irection de **M**aintenance
DOI	**D**irections d'**O**rganisation **I**nformatique
DVR	**D**igital **V**idéo **R**ecorder
EBGM	**E**lastic **B**unch **G**raph **M**atching
EO	**E**igen **O**bject
GM	**M**élange de **G**aussiennes
GRE	**G**roupes **R**égionaux d'**E**xploitations
HDVR	**H**ybride **D**igital **V**idéo **R**ecorder
HMM	**H**idden **M**arkov **M**odels
ICP	**I**terative **C**losest **P**oint
IP	**I**nternet **P**rotocol
ARI	**A**rmée **R**épublicaine **I**rlandaise
LAN	**L**ocal **A**rea **N**etwork
LDA	**A**nalyse **D**iscriminante **L**inéaire

NVR	**N**etwork **V**idéo **R**ecorder
PAL	**P**hase **A**lternated in **L**ine
RNA	**R**éseaux de **N**eurones **A**rtif ciels
SVM	**M**achine à **V**ecteurs de **S**upport
WAN	**W**ide **A**rea **N**etwork

INTRODUCTION GÉNÉRALE

De nos jours, la vidéosurveillance est omniprésente et on la retrouve dans de nombreux secteurs d'activité (banque, transports, industrie, grande distribution, ...) ou lieux de vie (villes, immeubles de bureau, équipements collectifs, ...).

Le nombre croissant de menaces de vol ou autre a fait que la plupart des responsables d'entreprise, souhaitent accroître la sécurité, en protégeant les biens et les personnes par de la vidéosurveillance.

C'est pourquoi, notre travail consiste à doter la Banque BADR (banque agricole et du développement rurale) d'un outil qui permettra de mettre en place un système de vidéosurveillance intelligente, en intégrant un système de reconnaissance faciale qui permettra l'authentification du personnels et la reconnaissance des intrus.

Le mémoire s'articule autour de quatre chapitres :

Le premier chapitre, introduit les généralités sur la télésurveillance. Le deuxième, est consacré à un état de l'art des différentes méthodes de reconnaissance faciale utilisées. Dans le troisième chapitre, une brève description de l'organisme d'accueil est donnée. Et le dernier chapitre, présentes l'essentiel de notre travail à savoir le développement d'une application de reconnaissance faciale ainsi que les résultats d'expérimentations obtenus.

Enfin, nous terminerons par une conclusion générale où l'essentiel de notre travail est présenté ainsi que les perspectives futures.

CHAPITRE 1

TÉLÉSURVEILLANCE

Introduction

De nos jours les problèmes de sécurité se font de plus en plus ressentir (menaces terroriste, cambriolage, etc) dans notre vie quotidienne, la télésurveillance est une solution qui permet de réglé ce genre de problème, elle offre la possibilité de surveiller des individus suspect afin d'éviter d'éventuellement attentats, mettre sous surveillance sa maison pour empêcher des cambriolages ou tout simplement la télésurveillance peut servir comme outils d'authentification.

1.1 Présentation de la télésurveillance

La télésurveillance est la surveillance à distance d'un lieu, public ou privé, de machines ou d'individus. Elle est employée dans de nombreuses situations, généralement pour des raisons de sécurité.[1]

Exemple d'utilisation de la télésurveillance

- ⋆ Dans le cadre de la sécurité routière, au moyen de caméras spécialisées ou des capteurs à proximité.
- ⋆ Pour la surveillance des machines : divers capteurs permettent d'évaluer l'état de la machine, une anomalie de fonctionnement ou même un acte de malveillance serait alors détecté à distance.
- ⋆ Dans le cadre de la prévention de la délinquance (avec notamment la vidéosurveillance).

- ⋆ Pour la surveillance de lieux sensibles (banques, centrales nucléaires, etc.) et d'habitations, afin de prévenir les intrusions, les cambriolages et les actes de vandalisme.
- ⋆ Dans le cadre de la télémédecine, et en particulier pour la surveillance des patients à distance.
- ⋆ Pour la surveillance à distance des enfants et des personnes vulnérables.

1.2 Historique

1.2.1 Son apparition

La vidéosurveillance s'est développée d'abord au Royaume-Uni, en réponse aux attaques de l'IRA(Armée républicaine irlandaise en anglais Irish Republican Army). Les premières expériences au Royaume-Uni dans les années 1970 et 1980 ont conduit à des programmes de grande ampleur au début des années 1990. Ces succès conduisirent le gouvernement à faire une campagne auprès de la population, et lança une série d'installations de caméras. Aujourd'hui, les caméras au Royaume-Uni couvrent la plupart des centres villes, et de nombreuses gares et parkings. Une étude donna le chiffre approximatif de 400 000 caméras à Londres et 4 millions au Royaume-Uni au total. [1]

1.2.2 Évolution des systèmes de vidéosurveillance

La transition numérique en vidéosurveillance s'est opérée en plusieurs étapes. Amorcée avec l'apparition de l'enregistreur numérique, elle se poursuit vers une conversion totale à l'infrastructure IP, où la vidéo est transmise sur réseau intranet ou Internet de la caméra à l'écran de visionnement. Dans ce passage, l'on retrouve plusieurs systèmes hybrides, intégrant composantes analogiques et numériques. [2]

Première génération :

Le réseau TVCF analogique traditionnel : des caméras analogiques sont connectées par câbles coaxiaux (un câble par caméra) aux écrans de surveillance et, pour des fins d'archivage, à un magnétoscope qui enregistre la vidéo sur cassette. Un multiplexeur peut être utilisé pour grouper les flux vidéo de plusieurs caméras en un seul signal composite qui est transmis au magnétoscope ou à un moniteur analogique. Il permet d'afficher quatre, neuf ou 16 signaux vidéo sur un même écran, ou d'enregistrer ceux-ci sur un même système d'archivage. Aucune

compression n'est effectuée sur les signaux vidéo. Avec un magnétoscope conçu à cet effet, l'enregistrement à taux de trame (frame rate) réduit permet d'économiser de l'espace sur la bande vidéo, selon les besoins de surveillance.

Avantages :

- Les systèmes analogiques sont très fiables.
- Simple à utiliser, ils ne requièrent pas de compétences informatiques.

Inconvénients :

- La qualité de la vidéo est inférieure à celle des systèmes numériques.
- Il faut changer les cassettes fréquemment.
- Nécessite un nettoyage et un entretien régulier des magnétoscopes.
- La qualité de la vidéo enregistrée se détériore avec le temps.
- Ne permet pas le visionnement à distance, comme sur les réseaux numériques.
- Ce sont des systèmes propriétaires.

FIGURE 1.1 – Système classique CCTV

Deuxième génération :

Le système hybride le remplacement du magnétoscope à cassette par un enregistreur numérique (DVR) représente la première étape de la transition numérique en vidéosurveillance. Apparus dans les années 90, les enregistreurs numériques archivent la vidéo sur des disques durs. Comportant souvent plusieurs entrées vidéo, l'enregistreur numérique remplace à la fois le multiplexeur et le magnétoscope analogique.

Les modèles sont équipés d'un port Ethernet, permettant la connexion à un réseau et l'accès à distance à la vidéo, soit en temps réel, soit à partir de l'enregistrement. Les transmissions vidéo se font sous protocole IP à partir de l'enregistreur numérique. Ils permettent la transition vers un système hybride de vidéosurveillance sur réseau IP, tout en conservant les caméras analogiques. L'enregistreur numérique hybride (HDVR), quant à lui, peut recevoir à la fois les flux vidéo de caméras analogiques et IP. Il représente une solution efficace pour moderniser un système de vidéosurveillance en profitant des avantages des nouvelles caméras IP, tout en conservant les caméras analogiques existantes en place.

Avantages :

- Aucune cassette à changer.
- La vidéo archivée est de meilleure qualité, sans détérioration avec le temps.
- Possibilité de chercher rapidement dans les enregistrements vidéo.
- Surveillance vidéo et opération du système à distance à partir d'un PC.

Inconvénients :

- Concentration des tâches de numérisation, compression vidéo, enregistrement et réseautage dans la même machine.
- L'enregistreur numérique est un appareil propriétaire, ce qui augmente les coûts de maintenance et de mise à jour.
- Le nombre d'entrées vidéo de l'enregistreur numérique (souvent un multiple de 16) contraint l'ajout de caméras.

Les encodeurs vidéos

Sont utilisés pour convertir les signaux provenant de caméras analogiques et les transmettre en flux IP sur un réseau via un commutateur. Tout en conservant les caméras analogiques, ils permettent un passage presque complet à l'infrastructure réseau pour la vidéosurveillance, puisque que la vidéo est constamment transmise sous le protocole IP à travers le réseau.

Les encodeurs vidéo peuvent être utilisés avec les enregistreurs vidéo réseau (NVR). Ceux-ci ne peuvent traiter et enregistrer que des flux vidéo IP. Ils sont offerts sous une plateforme ouverte (un ordinateur muni d'un logiciel de gestion vidéo) ou dans un matériel propriétaire dédié. Sous cette dernière forme, l'enregistreur vidéo réseau se compare à un enregistreur numérique hybride, excepté qu'il nécessite l'usage d'encodeurs pour opérer avec des caméras analogiques.

Avantages :

- Utilisation d'ordinateurs et de matériel standards de réseau pour l'enregistrement et la gestion de la vidéo.
- Possibilité d'enregistrer à l'extérieur du site de surveillance (par exemple, centralisation des enregistrements).
- Architecture distribuée qui offre flexibilité, extensibilité (peut ajouter une caméra à la fois) et redondance (en cas de bris ou pannes).

Inconvénients :

- Gourmand en bande passante, si l'enregistrement est fait hors du site de surveillance (par ex., de façon centralisée).
- Si le réseau tombe en panne, l'enregistrement peut être interrompu.
- Si l'enregistrement centralisé n'est pas requis, l'utilisation d'enregistreurs vidéo réseau est souvent plus coûteuse que celle d'enregistreurs numériques.
- Nécessitent des calculs complexes pour déterminer le nombre de flux vidéo pouvant être supportés par le serveur, la quantité d'espace disque nécessaire à l'enregistrement, le taux de trames, le niveau de compression et d'autres facteurs liés aux capacités du réseau.

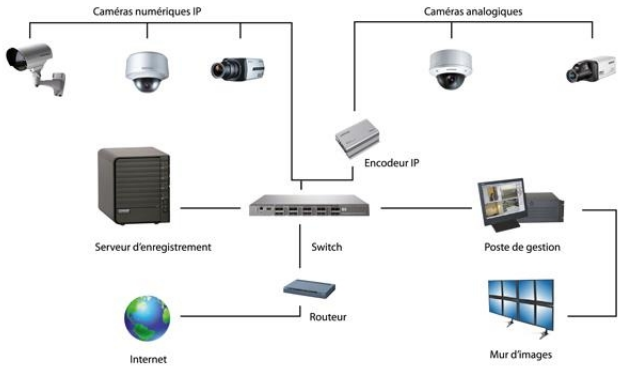

FIGURE 1.2 – Système hybride

Troisième génération :

Le tout numérique IP au sens strict, un système de vidéosurveillance est complètement IP, lorsque toutes ses composantes sont numériques et toutes les transmissions sont effectuées sous le protocole IP. Ces réseaux comprennent donc des caméras réseau, aussi appelées IP. Il s'agit de caméras intégrant leur propre encodeur. Celles-ci sont reliées, via des commutateurs réseau, à des serveurs (ordinateurs personnels), munis d'un logiciel de gestion vidéo. L'enregistrement est fait sur serveur ou sur des enregistreurs vidéo réseau propriétaires (dédiés aux tâches spécifiques d'enregistrement, d'analyse et de lecture vidéo sur IP). Les traitements sont effectués sur le serveur ou dans les périphériques. Toutefois, beaucoup de gens considèrent qu'un système de vidéosurveillance dont la vidéo est transmise sous protocole IP à partir des encodeurs, constitue un système réseau IP. Dans ces systèmes, les caméras peuvent être analogiques, en autant qu'elles soient reliées à des encodeurs.

Avantages :

- Tout est numériques (caméras, réseaux, enregistrement, accès.
- Ils peuvent inclure différents types de caméras : intelligente, mégapixel, sans fil, PTZ, panoramiques, etc.
- Ils utilisent du matériel non propriétaire.
- Ils fonctionnent avec des serveurs distribués et multiplateformes.
- La sauvegarde se fait sur réseau (NVR).
- On peut y accéder à distance, n'importe où, n'importe quand, soit d'un centre de contrôle, via Internet ou un réseau LAN ou WAN, sur un cellulaire ou un assistant numérique personnel, etc.
- Ils peuvent inclure de l'analytique vidéo.
- La vidéosurveillance sur réseau IP repose sur une infrastructure plus souple que la vidéo analogique, combinant transmission câblée et sans fil.
- L'infrastructure réseau est rapide et facilement extensible. Il n'y a pas de limite au nombre de caméras qui peuvent s'y ajouter.

Inconvénients :

- La plupart des intégrateurs et installateurs en vidéosurveillance sont issus du secteur de la sécurité physique.
- Passer d'un réseau de télévision en circuit fermé à un système de vidéosurveillance, dont les données transitent par les réseaux Ethernet ou Internet, soulève les questions de sécurité informatique.

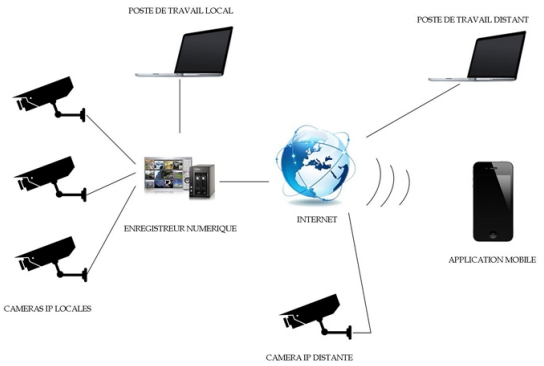

FIGURE 1.3 – Système IP

1.3 Environnement matériels et architecture des systèmes de vidéosurveillance

Dans cette section on présente les différentes composantes matérielles et logicielles, ainsi que des différentes étapes qui régissent un système de vidéosurveillance (Acquisition, Transmission, Compression, Traitement, Archivage et Affichage) [3].

1.3.1 Acquisition

La caméra est un système de prise d'images animées qui génère un signal vidéo noir et blanc ou couleur. La caméra capte la lumière pour la transformer en signal électrique. Elle se compose parfois d'un capteur d'image et d'une électronique de traitement permettant de générer le signal vidéo.

Différents types de caméras

Les caméras peuvent être de type analogiques vidéo, numériques IP ou mégapixels. Elles peuvent être installées :

- ⋆ Fixes d'intérieur, sur support, pour filmer des plans fixes avec possibilité de réglage manuel de la focale.
- ⋆ Fixes d'extérieur, sous caisson thermostaté, pour filmer des plans fixes avec possibilité de réglage manuel de la focale.
- ⋆ Sous dômes fixes, qui procurent en plus une protection de la caméra.
- ⋆ Sous dômes motorisés : le système de motorisation commande le déplacement horizontal et/ou vertical de la caméra et le zoom (PTZ).

Les caméras analogiques :

Le signal vidéo est un flux continu de données analogiques résultant du balayage vidéo du spot sur les pixels. Il correspond à 2 trames entrelacées représentant chacune la moitié de l'image [21].

- Le format de vidéo utilisé en Europe est PAL (Phase Alternated in Line) qui correspond à 625 lignes avec entrelacement 2 :1, dont 576 d'images, le reste étant des informations de régulation et de synchronisation.
- La définition des images vidéo est exprimées en lignes TV (ex : 540 lignes TV).
- Ces caméras peuvent intégrer un convertisseur de sortie vidéo/numérique pour une mise en réseau IP.

FIGURE 1.4 – Caméra analogique

Les caméras numériques (IP) :

Les informations d'images sont des paquets de données numériques (suite de bits 0/1) dont l'acquisition se fait : pour les caméras entièrement numériques (full IP), sur un capteur CCD (Charged Coupled Device) à balayage progressif où le signal lumineux reçu par chaque pixel

est codé sur plusieurs bits, avec une analyse séquentielle qui produit une image complète (il n'y plus d'entrelacement de trames) pour les caméras vidéo à sortie numérique, après un traitement du signal par un convertisseur analogique/digital qui numérise la vidéo [21].

- Le format numérique des informations est compatible réseaux IP (Internet Protocol).
- La définition des images est donnée en résolution PAL (ex : 4CIF 704 x 576 pixels, CIF176 x 144 pixels).
- La qualité nécessite des débits importants obtenus par algorithmes de compression (M-JPEG, MPEG-4, H.264).

FIGURE 1.5 – caméra numérique avec WIFI

FIGURE 1.6 – caméra numérique avec câble

Caméras mégapixels :

Les caméras megapixel utilisent des capteurs CMOS (Complementary Metal Oxide Semiconductor) qui offrent des résolutions d'images supérieures à celles des caméras numériques standard (ex : formats 0,5 - 1,3 - 2,1 et 3,1 mégapixels). Ceci permet notamment plus de détails sur les images, la couverture d'un champ de vision plus large et l'analyse intelligente d'image [21].

FIGURE 1.7 – Caméra mégapixel

Mini camera surveillance :

La mini camera surveillance est également appelée caméra espion. Habituellement, elle est de taille très petite. Elle peut être équipée d'un microphone, ce qui permet à la fois de voir ce qui se passe et d'entendre ce qui est dit. Ce type de caméra peut se dissimuler facilement dans une pièce, sous un meuble ou dans un détecteur de mouvement ou de fumée. La mini camera de surveillance : peut être filaire ou sans fil (WiFi) ; peut être reliée à un moniteur, un téléviseur, un PC (avec une carte télé), un enregistreur numérique, ...[7].

FIGURE 1.8 – Caméra discrète

Webcam videosurveillance :

La webcam videosurveillance est une petite caméra connectée à un ordinateur : elle peut être intégrée au PC ou ajoutée par son utilisateur, elle affiche en direct sur l'ordinateur les images capturées [7].

La webcam videosurveillance permet deux types de videosurveillance :

1. la surveillance d'un espace situé à proximité de l'ordinateur.
2. la videosurveillance à distance : en installant sur l'ordinateur un logiciel de videosurveillance (traitement des images), on peut visualiser en temps réel et de n'importe quel point du globe ayant accès à une connexion Internet, le lieu qui est mis sous surveillance. Le logiciel enregistre les images et permet de revisualiser des séquences.

FIGURE 1.9 – Webcam

Les caméras dômes :

Les dômes procurent une protection contre l'environnement et, selon les modèles, contre le vandalisme. Ils peuvent être de type [21] :

⋆ **Dôme fixe :** la caméra a une orientation fixe de son axe optique. Cette orientation est définie à l'installation par le réglage du support de la caméra. Il est possible de régler le zoom dans l'axe de la caméra choisi.

⋆ **Dôme motorisé :** la motorisation du support de caméra permet de commander à distance le déplacement de son axe dans l'espace pour balayer un champ plus complet. Selon la caméra intégrée, le dôme fixe ou motorisé permet une utilisation :

- Jour : avec caméra couleur.
- Jour/nuit : avec caméra jour/nuit La conception du dôme et sa résistance permettront une installation en : intérieur et extérieur.

FIGURE 1.10 – Caméra dôme

Caméra de surveillance infrarouge :

— L'image capturée de nuit est en noir et blanc, de jour en couleurs.

— La caméra équipée de LED infrarouges est visible car elle émet une lumière rouge qui permet d'avoir une vision nocturne jusqu'à 100m. Certaines existent sans lumière rouge mais leur portée est beaucoup plus réduite.

— Caméra classique et projecteur halogène pour éclairer la zone à surveiller.

— Camera jour/nuit : la camera passe en mode jour ou nuit en fonction de la luminosité. ses performances se mesurent via le nombre de lux (luminosité) à partir duquel elle réagit, plus une caméra réagit à partir d'un nombre proche de 0 lux, plus elle est performante dans l'obscurité [21].

1.3.2 Transmission

La vidéo captée par les caméras de surveillance doit être transmise aux systèmes d'enregistrement, de traitement et de visionnement. Cette transmission peut se faire par câble ou à travers l'air (signaux infrarouges, transmission radioélectrique).

La vidéo filaire prédomine largement dans les systèmes de vidéosurveillance. Elle offre une plus grande bande passante et une meilleure fiabilité que les connections sans fil, à un coût inférieur. Cependant, la transmission vidéo sans fil s'impose parfois comme solution, par exemple dans le cas de surveillance de grands périmètres où l'installation de câblage s'avérerait trop coûteuse, ou lorsque les zones à surveiller sont impossibles à rejoindre par câble.

Qu'il transite par fil ou sans fil, le signal vidéo peut être analogique ou numérique. Encore aujourd'hui, la majeure partie des transmissions vidéo pour la surveillance sont analogiques. Néanmoins, les réseaux informatiques sont de plus en plus utilisés pour transporter la vidéo grâce au protocole IP. Les caméras IP peuvent se connecter directement sur ces réseaux, tandis que les flux vidéo émergeant de caméras analogiques doivent, au préalable, être numérisés par un encodeur, aussi appelé serveur vidéo, pour passer par les réseaux IP [2].

1.3.3 Compression

La vidéo numérisée représente une grande quantité de données à transmettre et à archiver. L'envoi d'une séquence vidéo peut nécessiter jusqu'à 165 mégabits de bande passante et la vidéo d'une seule caméra pour une journée peut occuper sept gigaoctets d'espace disque. C'est pourquoi la vidéo de surveillance doit être compressée grâce à des codecs, algorithmes permettant de réduire la quantité de données en supprimant les redondances, par image ou entre les trames d'une séquence, ainsi que les détails imperceptibles à l'œil humain [2].

Selon le type de compression, l'usage du processeur requis pour l'exécution du codec est plus ou moins intensif. Un compromis s'impose donc entre le taux de compression et les ressources du processeur qui sont accaparées.

Il existe deux grands groupes de standards internationaux de compression : JPEG, créés par le Joint Photographic Experts Group, et MPEG, élaborés par le Moving Photographic Experts Group. Dans le premier groupe, on retrouve les formats JPEG pour les images fixes, et MJPEG pour les séquences vidéo. Le second groupe comprend les formats MPEG-1, MPEG-2, MPEG-4 et H.26421 [4].

1.3.4 Traitement

Les systèmes de gestion vidéo opèrent les traitements des images de vidéosurveillance, tels que la gestion des différents flux vidéo, le visionnement, l'enregistrement, l'analyse et la recherche dans les séquences enregistrées. Il existe quatre grandes catégories de systèmes de gestion vidéo [2].

Enregistreur vidéo numérique (DVR) :

Appareil qui dispose d'un disque dur interne pour l'enregistrement numérique de la vidéo et d'un logiciel intégré de traitement de la vidéo. Il n'accepte que les flux provenant de caméras analogiques, qu'il numérise. Les modèles récents permettent de visionner la vidéo à distance sur ordinateur. Encore très répandus, ils laissent toutefois peu à peu leur place aux systèmes supportant la vidéo IP de bout en bout.

FIGURE 1.11 – Enregistreur DVR

Enregistreur numérique réseau (NVR) :

Conçu pour les architectures réseaux IP de vidéosurveillance, il ne peut traiter que les signaux vidéo provenant de caméras IP ou d'encodeurs.

FIGURE 1.12 – Enregistreur NVR

Enregistreur vidéo hybride (HDVR) :

Similaire à l'enregistreur numérique, mais accepte à la fois le branchement de caméras analogiques et IP. Il est possible de rendre hybrides plusieurs modèles d'enregistreurs vidéo numériques par l'ajout d'un logiciel.

Logiciel de vidéosurveillance IP :

Solution purement logicielle de gestion de la vidéo sur un réseau IP. Dans le cas de systèmes de surveillance comportant peu de caméras, un navigateur Web peut suffire à gérer la vidéo. Pour de plus gros réseaux de vidéosurveillance, un logiciel dédié de gestion vidéo doit être utilisé. Celui-ci s'installe sur un ordinateur personnel ou un serveur. Plus complexe à installer, en raison des configurations nécessaires du serveur, il offre une plus grande flexibilité pour le

choix et l'ajout de composantes au réseau de vidéosurveillance. Les logiciels de vidéosurveillance IP représentent une tendance forte en gestion vidéo, surtout dans les infrastructures comportant un grand nombre de caméras. Les plateformes ouvertes permettent d'intégrer facilement des caméras et composantes matérielles de différents manufacturiers [2].

1.3.5 Archivage

La période d'archivage des séquences vidéo varie selon les besoins de surveillance, allant de quelques jours à quelques années. En moyenne, les organisations conservent les preuves vidéo entre 30 et 90 jours. Le déploiement de vastes réseaux de caméras et l'utilisation de vidéosurveillance à haute résolution fait exploser les demandes pour les systèmes de stockage. Bien que le coût des supports d'enregistrement ait considérablement baissé dans les dernières années, l'archivage représente souvent une part importante des dépenses d'infrastructure en vidéosurveillance, en raison de la quantité toujours croissante de données vidéo à stocker.

1.3.6 Affichage

Une grande partie de la vidéo captée par les caméras de surveillance n'est jamais regardée. Elle est simplement archivée, au cas où un visionnement soit nécessaire suite à un incident. Traditionnellement, la vidéosurveillance a principalement servi comme outil d'enquête. Toutefois, dans plusieurs cas de surveillance, des agents de sécurité visionnent, en temps réel, les images provenant des caméras de surveillance. Sans nécessairement regarder toute la vidéo captée, les agents peuvent faire une revue périodique des différentes sources vidéo. La vidéo de surveillance peut être visionnée sur différents appareils. Dans de petites installations, il est possible de regarder la vidéo directement de l'enregistreur, simultanément à son enregistrement. Plus généralement, les images seront regardées à distance, sur un ordinateur ou, de façon mobile, sur un téléphone ou dispositif portable.

1.4 Les accessoires

— **Caissons de protection :** Le caisson est un boîtier qui permet de protéger la caméra et l'objectif contre les agressions de l'environnement et les conditions climatiques [3].

— **Projecteurs :** Un projecteur est une source de lumière qui permet d'éclairer une scène afin de mieux la visionner. Le spectre de lumière peut se situer dans le visible (lumière blanche) ou dans l'infrarouge. Un éclairage dans le spectre infrarouge permet une surveillance discrète puisque l'œil humain n'est pas sensible à ces longueurs d'onde [3].

— **Serveur vidéo :** Un serveur vidéo est un dispositif électronique permettant la liaison de caméras analogiques sur le réseau Ethernet – il existe aussi des serveurs une voie. Cet équipement évite de remplacer des caméras analogiques lors d'une extension ou modification d'une installation de vidéosurveillance existante [3].

— **Imprimante vidéo :** Une imprimante vidéo permet d'imprimer sur papier une image issue d'un signal vidéo noir et blanc ou couleur [3].

Conclusion

Dans ce chapitre nous avons présenté des généralités sur la télésurveillance, nous avons vu son apparition et son évolution puis nous avons énumérer les différents matériels utilisés.

Dans le prochain chapitre nous allons voir des généralités sur la reconnaissance faciales, nous pourrons voir les différentes méthodes utilisées.

CHAPITRE 2

RECONNAISSANCE FACIALE

Introduction

Dans un monde où la sécurité des individus est devenue un souci majeur, le besoin de se protéger augmente jour après jour. En effet, vu le développement permanent et important de la société dans tous ces aspects, les outils de surveillance et de contrôle classique à savoir ceux relatifs à la méthode basée sur la connaissance tel que le mot de passe ou bien basée sur la possession (les badges, les pièces d'identités, clés, ...) s'avèrent inefficaces.

En effet, ces différents laissez-passer peuvent être perdus ou même volés. Dans le cas du mot de passe, celui-ci peut facilement être oublié par son utilisateur ou bien deviné par une autre personne.

Pour pallier à ces différents problèmes, la solution et l'utilisation des caractéristiques physiques des individus pour les identifier et la reconnaissance faciale et un excellent moyen pour le réalisé.

2.1 Historique

La reconnaissance faciale automatique est un concept relativement nouveau. Le premier système semi-automatisé de la reconnaissance faciale a été développé dans les années 1960, il nécessite à l'administrateur de localiser les yeux, les oreilles, le nez et la bouche sur la photo et de saisir les distances calculées et les ratios à un point de référence commun, qui ont ensuite été comparés aux données de référence [16].

Dans les années 1970, Goldstein et al [17] ont utilisé 21 marqueurs spécifiques tels que la

couleur des cheveux et l'épaisseur de la lèvre pour automatiser la reconnaissance. Le problème avec ces deux premières solutions, c'est que les mesures et les emplacements ont été calculés manuellement.

En 1988, Kirby et Sirovich [18] ont appliqué l'analyse en composantes principales (ACP), une technique standard de l'algèbre linéaire. Cela a été considéré en quelque sorte comme une étape importante car elle a montré qu'au moins une centaine de valeurs ont été nécessaires pour coder convenablement et avec précision une image alignée et normalisée.

En 1991, Turk et Pentland [19] ont découvert que lorsque vous utilisez la technique Eigenfaces (ACP), l'erreur résiduelle peut être utilisée pour détecter un visage dans une image, une découverte qui a permis la reconnaissance faciale automatique en temps réel.

Bien que l'approche était quelque peu limitée par des facteurs environnementaux, elle a néanmoins créé un intérêt significatif pour promouvoir le développement des technologies de la reconnaissance faciale automatique. Cette technologie a été mise en essai en janvier 2001 lors de la finale du championnat de football américain SUPER BOWL en capturant des images de surveillance puis comparées à une base de données numérique [20].

Aujourd'hui la reconnaissance faciale est utilisée dans plusieurs domaines, par exemple dans des lieux publiques pour détecter des personnes qui pourront nuire, ou encore comme moyen d'authentification aux sites sensibles ...

2.2 Processus de reconnaissance faciale

La reconnaissance faciale de visage s'effectue en trois étapes principales :

2.2.1 Détection de visage

La détection de visages est la première étape dans le processus de reconnaissance faciale. Son efficacité a une influence directe sur les performances du système de reconnaissance de visages. Il existe plusieurs méthodes pour la détection de visages, certaines utilisent la couleur de la peau, la forme de la tête, l'apparence faciale, alors que d'autres combinent plusieurs de ces caractéristiques [8].

Les méthodes de détection de visages peuvent être subdivisées en quatre catégories :

2.2.1.1 Approches basées sur les connaissances acquises

Ces méthodes se basent sur la connaissance des différents éléments qui constituent un visage et des relations qui existent entre eux. Ainsi, les positions relatives de différents éléments clés tels que la bouche, le nez et les yeux sont mesurées pour servir ensuite à la classification visage ou non visage.

Le problème dans ce type de méthode est qu'il est difficile de bien définir de manière unique un visage. Si la définition est trop détaillée, certains visages seront ratés tandis que si la description est trop générale, le taux de faux positifs montera en flèche [12].

2.2.1.2 Approches basées sur le « Template-matching »

La détection des visages se fait à travers un apprentissage d'exemples standards de visages ou d'images frontales contenant des visages. La procédure se fait en corrélant les images d'entrées et les exemples enregistrés (gabarits) et le résultat donne la décision finale soit de l'existence ou non d'un visage. On trouve 2 types de corrélation suivant le type des gabarits [11] :

— Faces de visages prédéfinies (predefined face template).
— Modèles déformables (Deformable Template).

2.2.1.3 Approches basées sur l'apparence

La différence entre cette méthode et "Template matching" est que les modèles (Template) sont lus à partir des images d'apprentissage qui doivent être représentatives et faites à différentes positions du visage.

Généralement l'approche basée sur l'apparence se base sur des techniques d'analyse statistiques (pourcentage d'existence des modèles dans l'image) et d'apprentissage automatique pour trouver des caractéristiques significatives des visages et des non visages.

Pour l'approche suivante il existe plusieurs méthodes où chacune d'entre elles se base sur une des caractéristiques du visage ou plus précisément une partie de visage qui peut être interprétée sous le cadre probabiliste [11].

2.2.1.4 Approches basées sur des caractéristique invariantes

Ces approches sont utilisées principalement pour la localisation de visage. Les algorithmes développés visent à trouver les caractéristiques structurales existantes même si la pose, le point de vue, ou la condition d'éclairage changent. Puis ils emploient ces caractéristiques invariables

pour localiser les visages. Nous pouvons citer deux familles de méthodes appartenant à cette approche : Les méthodes basées sur la couleur de la peau, et les méthodes basées sur les caractéristiques de visage, elles consistent à localiser les cinq caractéristiques (deux yeux, deux narines, et la jonction nez/lèvre) pour décrire un visage typique [8].

2.2.2 Extraction de caractéristiques du visage

L'extraction des caractéristiques telles que les yeux, le nez, la bouche est une étape prétraitement nécessaire à la reconnaissance faciale. On peut distinguer deux pratiques différentes :

La première repose sur l'extraction de régions entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage.

La deuxième pratique extrait des points particuliers des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez. Elle est utilisée avec une méthode locale de reconnaissance et aussi pour l'estimation de la pose du visage [8].

Par ailleurs, plusieurs études ont été menées afin de déterminer les caractéristiques qui semblent pertinentes pour la perception, la mémorisation et la reconnaissance d'un visage humain. Par exemple, les caractéristiques pertinentes rapportées sont : les cheveux, le contour du visage, les yeux et la bouche. Cette étude a également démontré le rôle important que joue le nez dans la reconnaissance faciale à partir des images de profil. En effet, dans ce cas de figure, il est évident que la forme distinctive du nez est plus intéressante que les yeux ou la bouche [9] [10].

2.2.3 Reconnaissance du visage

De nos jours, le visage peut être utilisé pour identifier une personne dans une base mais il est plus communément utilisé pour vérifier l'identité. Il s'agit alors de déterminer si une identité réclamée est correcte ou fausse. Pour la vérification des visages, ce processus est effectué en comparant un modèle du demandeur (une ou plusieurs images de test), avec un modèle stocké (une ou plusieurs images de référence) [14].

Dans ce qui suit nous allons détaillée les déférentes techniques utilisée pour la reconnaissance de visage, à savoir les techniques de reconnaissance 2D et 3D.

2.2.3.1 Techniques de reconnaissance de visage 2D

On distingue trois catégories de méthodes [13] : les méthodes globales, les méthodes locales et les méthodes hybrides.

Les méthodes globales : Le principe de ces approches est d'utiliser toute la surface du visage comme source d'information sans tenir compte des caractéristiques locales comme les yeux, la bouche, ...L'une des méthodes la plus largement utilisée pour la représentation du visage dans son ensemble est l'ACP. Les algorithmes globaux s'appuient sur des propriétés statistiques bien connues et utilisent l'algèbre linéaire. Ils sont relativement rapides à mettre en œuvre, mais sont sensibles aux variations d'illumination, de pose et d'expression faciale. Parmi les approches les plus importantes réunies au sein de cette classe on trouve :

- ⋆ L'Analyse en Composantes Principales (PCA ou Eigen Faces),
- ⋆ L'Analyse Discriminante Linéaire (LDA),
- ⋆ Machine à Vecteurs de Support (SVM),
- ⋆ Les Réseaux de Neurones (RNA),
- ⋆ Mélange de Gaussiennes (GMM),
- ⋆ Modèle Surfacique du Visage (3D),
- ⋆ L'approche statistique et probabiliste.

Avantages :

— Le problème de la reconnaissance faciale automatique est transformé en un problème d'analyse de sous–espaces de visages, pour lequel de nombreuses méthodes statistiques existent.

— Les méthodes globales sont souvent applicables à des images basses résolutions ou de mauvaises qualités.

Inconvénient :

— Il est nécessaire de disposer de suffisamment de données représentatives des visages.

— Il n'y a pas d'a priori sur le physique d'un visage.

— Ces méthodes ne sont robustes qu'à des variations limitées (pose, illumination, expression).

Les méthodes locales : On les appelle aussi les méthodes à traits, géométriques, à caractéristiques locales, ou analytiques. Ce type consiste à appliquer des transformations en des endroits spécifiques de l'image, le plus souvent autour des points caractéristiques (coins des yeux, de la bouche, le nez, ...), l'énergie sera accordée aux petits détails locaux évitant le bruit engendré par les cheveux, les lunettes, les chapeaux, la barbe, etc. Mais leur difficulté se présente lorsqu'il s'agit de prendre en considération plusieurs vues du visage ainsi que le manque de précision dans la phase "extraction" des points constituent leur inconvénient majeur. Précisément, ces méthodes extraient les caractéristiques locales de visage comme les yeux, le nez et la bouche, puis utilisent leur géométrie et/ou l'apparence comme donnée entrée du classificateur. On peut distinguer deux pratiques différentes :

La première repose sur l'extraction de régions entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage.

La deuxième pratique extrait des points particuliers des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez. Parmi ces approches on peut citer :

- ⋆ Modèles de Markov Cachés (Hidden Markov Models (HMM)),
- ⋆ L'Algorithme Elastic Bunch Graph Matching (EBGM),
- ⋆ Eigen Object (EO),
- ⋆ L'appariement de gabarits.

Avantages :

- Le modèle créé possède des relations intrinsèques bien définies avec les visages réels.
- Les modèles créés peuvent prendre en compte explicitement les variations telles que la pose, l'illumination ou les expressions. La reconnaissance est ainsi plus efficace dans le cas de fortes variations.
- La connaissance a priori sur les visages peut être intégrée aux modèles afin d'améliorer leur efficacité.

Inconvénient :

- La construction du modèle, reposant souvent sur la détection de points caractéristiques faciaux, peut être laborieuse.
- L'extraction des points caractéristiques peut être difficile dans le cas de variations de pose, d'illumination, d'occlusion . . .
- Les images doivent être de relativement bonne qualité, et/ou être de résolution suffisante afin de pouvoir extraire les points caractéristiques.

Les méthodes hybrides : Plusieurs approches ont été proposées pour la reconnaissance de visages, sauf qu'aucune d'elle n'est capable de s'adapter aux changements d'environnements tels que la pose, expression du visage, éclairage, etc. La robustesse d'un système de reconnaissance peut être augmentée par la fusion de plusieurs méthodes. Il est par ailleurs possible d'utiliser une combinaison de classificateurs basés sur des techniques variées dans le but d'unir les forces de chacun et ainsi pallier à leurs faiblesses. Les techniques hybrides combinent les deux méthodes précédentes pour une meilleure caractérisation des images de visages.

2.2.3.2 Techniques de reconnaissance de visage 3D

Les techniques de reconnaissance 3D de visage peuvent être regroupées en trois catégories principales [13] : approches basées modèle, approches 3D et approches 2D + 3D.

Approches modèles : Ces approches construisent, à partir des points 3D, des modèles de visages qu'elles utilisent par la suite pour la reconnaissance. L'ensemble des visages est représenté par un espace vectoriel. Les points 3D des modèles de visages générés sont représentés par leurs coordonnées cylindriques définies par rapport à un axe vertical.

Approches 3D : Elles sont subdivisées en deux catégories : les approches basées surface qui utilisent la géométrie de la surface du visage et les approches holistiques 3D.

⋆ **Approches surface :** Dans ce cas, le problème de la reconnaissance 3D de visage est celui de l'alignement de deux surfaces 3D qui modélisent les deux visages à apparier. L'algorithme généralement utilisé est l'algorithme du plus proche voisin itéré, ou ICP (Iterative Closest Point). Il consiste en une optimisation alternée d'appariements et de transformations. Ainsi, à partir d'une transformation initiale, les deux étapes suivantes sont réitérées :

— Mise en correspondance (plus proche voisin) : on apparie chaque primitive du modèle transformé avec la primitive la plus proche dans la scène.
— recalage : la transformation (translation + rotation) est généralement calculée aux sens des moindres carrés, surtout si l'on travaille avec des points. Si l'on possède une information d'incertitude, on peut l'utiliser dans les étapes terminales pour affiner la

solution.

⋆ **Approches holistiques 3D :** Les techniques holistiques comme l'ACP ont été largement utilisées dans la reconnaissance faciale 2D. Plus récemment, ces techniques ont été aussi étendues aux données 3D de visage.

⋆ **Approche géométrique ou locale 3D :** Par rapport aux approches « holistiques », les techniques d'identification 3D du visage basées sur les caractéristiques faciales locales de type géométriques restent relativement peu développées. Elle a aussi mis en avant le besoin de comprendre et d'utiliser les propriétés discriminantes des caractéristiques locales du visage afin de concevoir des techniques efficaces de reconnaissance 3D de visage.

Approches 2D + 3D Il s'agit de techniques qui combinent des données 2D et 3D sur le visage pour améliorer les performances et la robustesse de la reconnaissance. Récemment, plusieurs approches basées sur ce principe ont été développées.

La décision multi-modale peut être résumée comme suit : dans un premier temps, les images d'entrée 2D (2D probe) et 3D sont appariées avec les images des galeries 2D et 3D respectivement. Ceci permet d'obtenir deux ensembles de N distances dans deux espaces différents, l'espace facial 2D et l'espace facial 3D. N est la taille de la galerie d'images. Les distances 2D et 3D sont additionnées, et l'image qui donne la plus petite somme est sélectionnée.

Le résultat de l'approche multi-modale est obtenu en utilisant une somme pondérée des distances dans les espaces de visage 3D et 2D. Une étude a démontré, grâce à l'utilisation de l'ACP sur les images 2D et 3D, que les données faciales 3D fournissent des performances biométriques bien meilleures que les données faciales 2D. Par ailleurs, les auteurs ont démontré aussi que la combinaison des données faciales 2D et 3D permet d'augmenter d'une manière significative les performances de la reconnaissance [15].

Conclusion

Dans ce chapitre nous avons vu les différentes méthodes utilisées pour faire de la reconnaissance faciale, nous allons présenter les avantages et les défauts de ces méthodes, nous avons constaté que les méthodes globales sont les plus adéquates pour le travail que nous allons effectuer, par le fait que les méthodes globales sont souvent applicables à des images basses résolutions ou de mauvaises qualités.

CHAPITRE 3

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Introduction

A fin de pouvoir cerner au mieux notre étude et être plus objectif dans cette exposition du plan de sécurité de la BADR nous avons pris comme échantillons le GRE de Bejaïa qui fait partie du territoire de compétence du CRM de Bejaia où nous avons eu l'honneur d'effectuer notre stage de mise en situation professionnelle. Avant de s'intéresser aux menaces aux quelles est affrontée et aux différentes démarches sécuritaires de la BADR, nous avons jugé nécessaire d'avoir une vue globale sur les valeurs de son système informatique ainsi répondre à la première question qu'on doit se posé avant d'entamer quelconque démarche visant la sécurité informatique ; que devons nous protéger ?

Puis en dernier lieu, nous proposerons un système qui dois améliorer la sécurité de la BADR.

3.1 Historique et évolution

La Banque de l'Agriculture et du Développement Rural est issue de la restructuration du secteur des banques par les pouvoirs publics engagée en Mars 1982, héritant 140 agences de la banque nationale d'Algérie étendues ce jour à plus de 290 et 41 Groupes Régionaux d'Exploitations (G.R.E). Constituant des éléments fondamentaux de différenciation qui lui confèrent une place de choix dans la stratégie de développement institutionnel et financier tracée par les pouvoirs publics, elle est classée depuis plusieurs années comme l'une des premières banques en Algérie. Crée pour répondre à une nécessité économique, née d'une volonté politique afin de restructurer le système agricole, assurer l'indépendance économique du pays et relever

le niveau de vie des populations rurales.

Tout en demeurant le principal partenaire financier du monde agricole et de la pêche, la BADR a étendu son réseau d'activité à d'autres secteurs. Elle est devenue la banque universelle la plus impliquée dans le financement du développement économique ou elle a entamé depuis l'an 2000 un plan de modernisation à même de la hisser aux normes internationales. Elle dispose aujourd'hui d'une informatique de pointe et travaille à l'intégration des nouvelles technologies de l'information. Elle a introduit en septembre 2001 le concept de banque assise qui s'est étendu sur l'ensemble de son réseau à la fin 2008.

3.2 Missions et objectifs de la BADR

3.2.1 Ses principales missions sont :

- ⋆ Le traitement de toutes les opérations de crédit, de change et de trésorerie.
- ⋆ L'ouverture de comptes.
- ⋆ La réception des dépôts à vue et à terme.
- ⋆ La participation à la collecte de l'épargne.
- ⋆ La contribution au développement du secteur agricole.
- ⋆ L'assurance de la promotion des activités agricoles, agro-alimentaires, agro-industrielles et artisanales.
- ⋆ Le contrôle avec les autorités de tutelle de la conformité des mouvements financiers des entreprises domiciliées.

3.2.2 Ses objectifs :

- ⋆ L'augmentation des ressources aux meilleurs coûts et rentabilisation de celles-ci par des crédits productifs et diversifiés dans le respect des règles.
- ⋆ La gestion rigoureuse de la trésorerie de la banque tant en dinars qu'en devises.
- ⋆ L'assurance d'un développement harmonieux de la banque dans les domaines d'activités la concernant.
- ⋆ L'extension et le redéploiement de son réseau.
- ⋆ La satisfaction de ses clients en leurs offrant des produits et services susceptibles de répondre à leurs besoins.
- ⋆ L'adaptation d'une gestion dynamique en matière de recouvrement.

⋆ Le développement commercial par l'introduction de nouvelles techniques managériales telles que le marketing, et l'insertion de nouvelles gammes de produits.

3.3 Organigramme de la BADR

L'organisme dispose de différentes directions comme le montre la figure 3.1, nous avons eu l'honneur de préparer notre stage au centre régional de maintenance informatique.

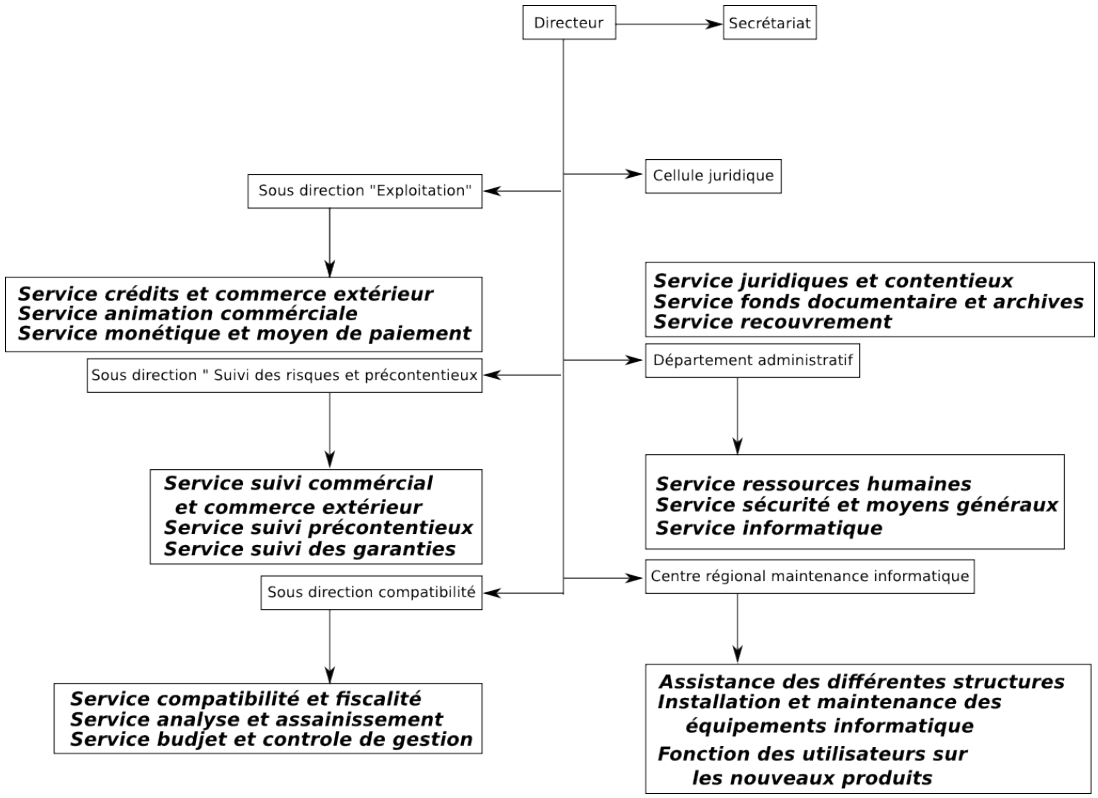

FIGURE 3.1 – Organigramme de la BADR.

3.3.1 Présentation de la direction de la maintenance

La direction de maintenance dit aussi (DM), c'est la deuxième direction après la direction de l'exploitation et du développement informatique (D.E.D.I). Qui appartiennent tout deux à la DGA (Informatique, Comptabilité et Trésorerie).

S'occupant de la gestion du parc informatique et consommable de la BADR, la direction de maintenance est consultée par les moyens généraux pour l'achat du matériel et chargée d'élaborer des cahiers de charge, aussi les formations de maîtrise des nouveaux logiciels. Elle a pour mission le suivi de l'activité informatique et l'assistance des Centres Régionaux de Maintenance.

3.3.2 Les structures de la Direction de Maintenance

Elle se compose de structures internes et de structures décentralisées :

3.3.2.1 Les structures internes :

Sont organisées comme suite :

- **Le Centre Gestion du Parc Informatique :** Considéré comme l'une des structures internes de la direction de maintenance, il est chargé de gérer le parc informatique et le consommable, de mettre aussi en place un système de gestion adéquat des équipements de la maintenance.
- **Le Laboratoire Central :** C'est le site central de la maintenance informatique, chargé également de l'approvisionnement et la gestion des pièces de rechanges, de la documentation technique, l'assistance au Centres Régionaux, mais aussi la maintenance des équipements installés au niveau des structures centrales.

3.3.2.2 Les structures décentralisées :

Appelées aussi CRM (Centre Régional de Maintenance), prend en charge la maintenance, la formation, la mise en place des produits et toutes formes d'assistance, en relation avec les informaticiens des Groupes Régionaux d'Exploitation.

Dirigé par un chef de centre nommé par la direction générale sur proposition du directeur de la direction de maintenance. Le centre de maintenance dépend sur le plan hiérarchique et technique directement de la DOI (Direction D'organisation Informatique), et pris en charge administrativement par le GRE (Groupe Régional d'Exploitation) qui l'abrite, au quel il rendra également compte de son activité à titre d'information.

3.3.3 Les missions du Centre Régional de Maintenance

Chargé de l'assistance et de la maintenance des structures sises au niveau de son territoire de compétence et l'assistance des informaticiens GRE. La direction de maintenance peut appeler à tout moment le personnel des centres régionaux de maintenance pour effectuer des missions en dehors de leur territoire, comme elle intervient pour assurer le support en tant qu'organe central pour les contrôles et les inspections techniques.

Le technicien prend contact avec la structure appelante pour un diagnostique de la panne signalée, on pourra avoir trois cas :

1. Dépannage (intervention) à distance.

2. Déplacement du technicien sur le site.
3. Envoi de l'équipement vers le Centre Régional de Maintenance.

La panne signalée peut être réglée à distance après l'intervention des techniciens. Dans le cas échéant, le technicien se déplace sur le site concerné par la panne et établit un rapport d'intervention technique, visé par les deux parties (technicien et responsable de la structure), pour le compte de la direction de la maintenance.

Au niveau du laboratoire central, a la réception des équipements transmis par les structures vers la DM, le chef de département d'équipement informatique et consommable enregistre les références des équipements reçus sur le registre approprié et les oriente vers la sous direction concernée pour prise en charge.

3.4 Les ressources informatiques de la BADR

Représentée dans les quarante huit wilayas du pays avec plus de trois cent structures, la BADR dispose d'un parc informatique impressionnant, un des plus importants au niveau national et le plus grand dans son secteur.

Le GRE de Bejaia comme chaque structure de la BADR que ce soit un autre GRE, une ALE, une inspection ou une direction centrale, dispose d'une salle informatique aménagée spécialement pour le fait, d'un réseau électrique ondulé indépendant et un générateur, elle abrite aussi les serveurs, l'armoire de brassage, les équipements de télécommunication, les onduleurs, l'imprimante arrière guichet et les équipements de vidéo surveillance. Tandis que les postes de travail qui se composent en générale d'une unité centrale, d'un écran et d'une imprimante, évidement d'une prise ondulée, une de réseau et une autre téléphonique, sont répartis sur les différents services selon l'activité. On notera aussi que chaque siège possède en moyenne une quinzaine de postes, ajoutons à cela les GAB (Guichet Automatique Bancaire) dont dispose plus de 100 ALE.

En plus du serveur d'exploitation et de sécurité cité auparavant, les postes de travail du GRE de Bejaia sont au nombre de dix huit et répartis sur les différents services.

3.5 Télésurveillance à la BADR

La BADR dispose d'un système de télésurveillance qui peut être consulté après un délit, le tableau 3.1 représente les différents matériels utilisés pour la vidéo surveillance de la BADR. le tableau englobe les caméras, les moniteurs de surveillance, les enregistreurs ainsi que les différent accessoires utilisé pour la télésurveillance.

Désignation	Référence
Caméra couleur CCD 1/3 HAD Day/night à objectif A/iris vari 2,8-13 mm focal (exterieur) et caisson ventilé et thermostatée	LG SCB5000
Caméra couleur CCD 1/3 HAD Day/night (intérieur) avec objectif A/iris v/focal 2,5-08 mm	LG LCB5000
Moniteur couleur 21 TFT-LCD	SAMSUNG
Moniteur couleur 19 TFT-LCD	SAMSUNG
Enregistreur multiplexeur numérique DVR 16 canaux	SAMSUNG
Disque dur 1 To	SAMSUNG
Onduleur 03 Kva On Line	UPS
Vidéophone avec gache	UPS
Câble alimentation souple 3*1,5 mm	ORMALIS
Câble coaxial vidéo K*6	K*6-500
Gaine flexible ignifuge 32 mm	ORMALIS
Goulotte blanche 20*40	ORMALIS
Accessoires de connections et de raccordements	ENS

TABLE 3.1: Matériels de la télésurveillance à la BADR

3.6 Problématique et proposition

3.6.1 Problématique

Durant notre stage, nous avons constaté que la banque dispose d'un système de vidéosurveillance qui pourrait être consulté après un délit ou un problème qui survient au sein de la banque. La question qui se pose c'est comment identifier la personne responsable du délit ou du problème en question ?

3.6.2 Proposition

La solution que nous proposons pour remédier au problème cité dans la problématique, est d'utilisé un système de reconnaissance faciale, ce système peut même être utilisé comme moyen d'authentification pour permettre aux employés d'accéder aux endroits légitimes.

Conclusion

Nous avons présenté dans ce chapitre l'organisme d'accueil, nous avons détaillé le fonctionnement de la direction de la maintenance, de cela une problématique à la quelle nous avons proposé une solution à la fin de ce chapitre.

Dans le prochain chapitre nous allons présenté la méthode et les outils que nous utiliserons pour implémenter le programme de reconnaissance faciale, ainsi que les résultats obtenus durant les tests effectués à l'aide de notre programme.

CHAPITRE 4

RÉALISATION ET EXPÉRIMENTATION

Introduction

Notre but est de pouvoir réaliser un système de vidéosurveillance, qui permet de reconnaître les personnes responsables d'un délit ou bien tout simplement d'authentifier la personne en question.

Pour cela, nous allons présenter la méthodologie qu'on a suivie pour résoudre notre problème.

4.1 Méthodologie de travail

Pour la réalisation de notre travail, nous avons suivi les étapes d'un processus de reconnaissance des formes à savoir :

— Création de la base de données,

— Apprentissage

— Détection du visage

— Reconnaissance et identification de la personne.

4.1.1 Création de la base de données

Pour faire de la reconnaissance, nous avons besoin d'une base de données des personnes à reconnaître. Dans cette optique, nous avons choisi d'enregistrer les images des personnes à reconnaître dans une base de données qui sera utilisée pour l'identification.

Pour cela nous avons utilisé un script python [25] pour la création du fichier *nosPhotos.txt* qui est présenté dans la figure 4.1.

```
if __name__ == "__main__":

    if len(sys.argv) != 2:
        print "usage: create_csv <base_path>"
        sys.exit(1)

    BASE_PATH=sys.argv[1]
    SEPARATOR=";"

    label = 0
    for dirname, dirnames, filenames in os.walk(BASE_PATH):
        for subdirname in dirnames:
            subject_path = os.path.join(dirname, subdirname)
            for filename in os.listdir(subject_path):
                abs_path = "%s/%s" % (subject_path, filename)
                print "%s%s%d" % (abs_path, SEPARATOR, label)
            label = label + 1
```

FIGURE 4.1 – Script python pour la création du fichier *nosPhotos.txt*

Dans un terminal linux, nous exécutons le script avec la commande suivante pour obtenir le fichier *nosPhotos.txt* :

python create_csv.py nosPhotos/ >> nosPhotos.txt

La figure 4.2 représente une partie du fichier *nosPhotos.txt.* où :

```
72 nosPhotos/s3/17 (autre copie).jpg;90
73 nosPhotos/s3/5 (autre copie).jpg;90
74 nosPhotos/s3/8.jpg;90
75 nosPhotos/s3/4 (autre copie).jpg;90
76 nosPhotos/s2/18 (autre copie).jpg;92
77 nosPhotos/s2/13 (copie).jpg;92
78 nosPhotos/s2/20.jpg;92
79 nosPhotos/s2/3 (autre copie).jpg;92
80 nosPhotos/s2/1 (copie).jpg;92
81 nosPhotos/s2/1.jpg;92
82 nosPhotos/s2/3 (copie).jpg;92
83 nosPhotos/s2/21 (copie).jpg;92
84 nosPhotos/s2/20 (copie).jpg;92
```

FIGURE 4.2 – une partie des chemins des images.

— **NosPhotos/s3/** =>> représente le répertoire où se trouvent les images de la troisième personne.
— **1.jpg** =>> représente le nom de l'une des images.
— **90** =>> représente le label.

4.1.2 Détection de visage

Une fois que la base de données est créée, nous allons passer à la détection de visage et pour cela, nous avons exploité la bibliothèque opencv [26] qui offre différentes fonctions de détection de visage dans des poses frontales ou de profil, détection des yeux, détection des corps .... Le détecteur de visage examine chaque pixel de l'image et le classifie comme appartenant à un visage ou non.

Dans notre cas nous allons exploiter le programme *haarcascade_frontalface_alt2.xml* qui est le plus adapté pour notre travail, car il permet de détecter l'individu en exploitant son visage de face. La figure 4.3 montre la détection du visage en utilisant la fonction *haarcascade_frontalface_alt2.xml*.

FIGURE 4.3 – La détection du visage.

4.1.3 Reconnaissance faciale

Une fois le visage détecté, il reste à le reconnaître.

Pour la reconnaissance faciale nous avons décidé, d'utiliser la méthode des eigenfaces, qui permet de déterminer les caractéristiques d'un visage. Ces caractéristiques seront ensuite exploitées pour la recherche de l'individu dans la base de données

4.1.3.1 Description d'Algorithme (eignefaces) : qu'est-ce que c'est Eigenface ?

Les eigenfaces sont un ensemble de vecteurs propres utilisés dans le domaine de la vision artificielle afin de résoudre le problème de la reconnaissance du visage humain. Le recours à des

eigenfaces pour la reconnaissance a été développé par Sirovich et Kirby (1987) et utilisé par Matthew Turk et Alex Pentland pour la classification de visages. Cette méthode est considérée comme le premier exemple réussi de technologie de reconnaissance faciale [22].

Reconnaissance par Eigenfaces

La méthode de reconnaissance faciale Eigenfaces emploie la technique de l'analyse en composante principale, qui marque une différence notable avec les méthodes plus classiques, appelées méthodes locales, qui se basent sur les particularités du visage analysé, et dont les défauts résident dans son manque de précision, ainsi que sa sensibilité aux informations qui ne sont pas pertinentes. La méthode des eigenfaces est qualifiée de globale, puisque l'ensemble du visage est alors analysé.

De manière simple, nous visons la diminution de la dimension de l'espace dans lequel nous allons travailler, et nous pourrons alors simplifier les données à notre disposition et leur interprétation.

L'algorithme ACP, PCA en anglais (Principal Composent Analysis) est né des travaux de M.A. Turk et A.P. Pentland au MIT Media Lab, en 1991 [24]. Cet algorithme s'appuie sur des propriétés statistiques bien connues et utilise l'algèbre linéaire. Il est relativement rapide à mettre en œuvre mais il reste sensible aux problèmes d'éclairement [23], de pose et d'expression faciale.

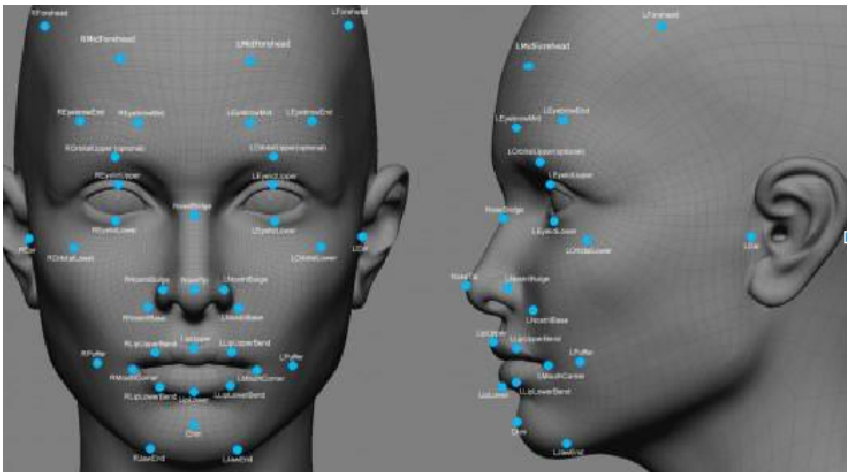

FIGURE 4.4 – La technique de l'analyse en composante principale

L'idée principale consiste à exprimer les **M** images d'apprentissage selon une base de vecteurs orthogonaux particuliers, contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du

visage. Nous voulons extraire l'information caractéristique d'une image de visage, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire. En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage [24].

4.1.3.2 Comment reconnaître une personne ?

Pour reconnaître une personne, nous procédons en deux étapes :

Première étape : Apprentissage

Dans cette phase, chaque personne est identifiée par son label (numéro affecté à l'image dans la base de données) et sa photo.

En premier lieu nous allons créer un modèle avec la fonction **Ptr<FaceRecognizer> model = createEigenFaceRecognizer()**, par la suite nous allons appliquer l'apprentissage sur ce modèle en utilisant la fonction *train* de cette façon **model->train(images, labels)** les résultats sont sauvegardés dans le fichier *eigenfaces.yml*.

Le fichier *eigenfaces.yml* contient les caractéristiques des visages qui seront utilisées pour l'identification.

Deuxième étape : Reconnaissance

Une fois l'apprentissage fait nous chargeons le fichier *eigenfaces.yml* avec la fonction *load* de cette façon **model->load("eigenface.yml")**, nous rappelons que ce fichier contient les caractéristiques des personnes qui se trouvent dans la base de données, par la suite nous allons faire la prédiction c-à-d avec la ligne de code suivante **model->predict(visageRedimenssionner,label,confic** la fonction *predict* va prédire si la personne est bien dans la base de données ou pas, et pour cela, la fonction utilise le label comme preuve de la présence ou de l'absence de la personne.

Et pour terminer la reconnaissance nous comparons le label que l'algorithme a trouvé avec le label que nous avons déclaré pour chaque personne. Si les labels correspondent, alors la personne est reconnue sinon la personne n'est pas reconnue.

4.2 Résultats d'expérimentation

Avant de présenter les résultats que nous avons obtenus, nous allons tout d'abord présenter la base de données que nous avons utilisé, c-à-d les personnes qu'on essaiera d'identifier grâce au programme.

Dans le but de tester le programme de reconnaissance faciale nous avons pris deux personnes pour les tests, nous avons enregistré dix photos de profil de deux personnes différentes. Ces images vont nous servir comme base de données d'apprentissage. La figure 4.5 représente un exemple des images d'une personne que nous avons prise.

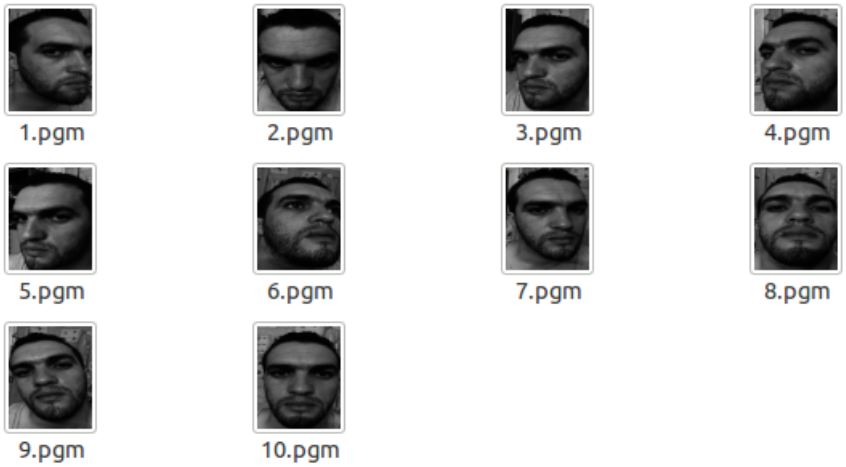

FIGURE 4.5 – Un exemple des images qu'on a prise.

Les images doivent être prises sous différents angles, et avec différentes postures.

Nous avons expérimenté notre travail sur différents types d'image pour tester sa capacité à identifier les personnes.

Notre travail a été donc testé sur des images de personnes sans et avec artifices.

L'expérimentation a été sur des images :

- De personnes portant une barbe.
- De personnes avec lunettes ou casquette.
- De personnes dans différentes conditions d'illumination.
- De personnes selon différentes postures.

4.2.1 Identifier quelqu'un avec barbe et sans barbe

Pour notre premier test, nous allons identifié une personne avec une barbe. Par la suite nous allons essayer d'identifier la même personne sans sa barbe. Les résultats du test sont présentés dans la figure 4.6 .

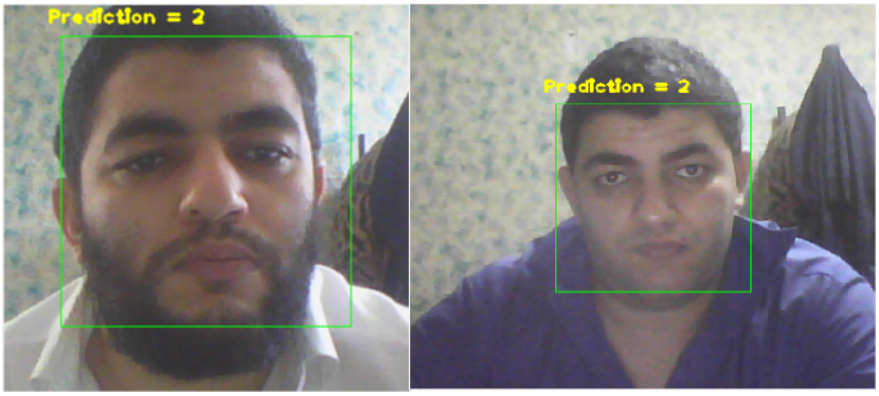

FIGURE 4.6 – Identification de personne avec et sans barbe

Dans la figure, nous remarquons le carré vert qui représente la détection du visage par le programme, ainsi que la prédiction qui est égale à 2, qui représente le label que nous avons donné à la personne dans notre base de données, ce qui démontre que le programme a bien reconnu l'individu avec ou sans barbe.

4.2.2 Identifier quelqu'un qui porte des lunettes de vue

Pour le deuxième test, nous allons essayer d'identifier un individu sans et avec lunettes de vue. La figure 4.7 montre le résultat du test.

FIGURE 4.7 – Identifier quelqu'un qui porte des lunettes de vue

Dans ce deuxième test notre individu s'appelle *Syphax*, nous remarquons sur la figure que le programme l'a bien reconnu avec des lunettes et sans lunettes. Le programme a bien réagit et a identifié une personne qui porte un artifice.

4.2.3 Identifier quelqu'un dans des conditions d'illumination (éclairage) différentes

Le troisième test est consacré au niveau d'éclairage dans la pièce, nous avons essayer d'identifier deux personnes différentes en faisant variés le niveau de luminosité, et pour cela on procède en quatre étapes :

— Éclairer les visages des deux personnes de front.

— Éclairer les visages des deux personnes du coté gauche.

— Éclairer les visages des deux personnes du coté droit.

— Identifier les deux personnes sans éclairage.

La figure 4.8 représente les résultats des trois premier tests, nous constatons que les deux personnes ont bien été identifié.

FIGURE 4.8 – Identification avec différentes illumination

Pour le test sans éclairage la figure 4.9 montre que le test a échoué.

FIGURE 4.9 – Identification sans illumination.

Sur l'image de droite la personne a été bien identifié, par contre sur l'image de gauche la personne n'a pas été identifié, le programme ne fonctionne pas dans des conditions d'illumination réduite.

Le programme identifie les personnes dans de bonne conditions d'illumination, mais en revanche des que les conditions ne sont pas satisfaisantes le programme n'arrive pas a reconnaître la personne.

4.2.4 Identifier une personne dans différentes postures

Dans le quatrième test on allons nous intéresser aux différentes postures que prend l'individu , et pour cela nous allons essayer d'identifier l'individu sous trois postures différentes.

— Identifier une personne qui lève la tête.

— Identifier une personne qui baisse la tête.

— Identifier une personne qui tourne la tête.

La figure 4.10 montre les résultats des trois testes, nous constatons que la personne a bien été identifié, le programme réagit bien aux différentes poses.

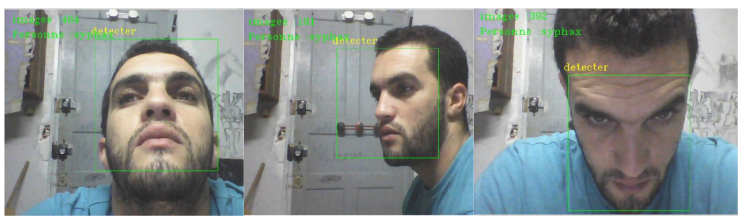

FIGURE 4.10 – Identification dans différentes postures

Conclusion

L'expérimentation de notre travail a donné des résultats satisfaisant pour des images existantes dans la base de données, que ce soit dans des postures différentes, avec ou sans barbe, avec ou sans artifice.

Par contre le programme de reconnaissance nécessite de bonne condition d'illumination.

CONCLUSION GÉNÉRALE

La reconnaissance faciale joue un rôle très important dans la vidéosurveillance, elle permet de reconnaître les intrus et d'authentifier le personnel d'une entreprise ou d'une banque.

Dans ce travail, nous avons réalisé un outil de reconnaissance faciale pour la vidéosurveillance intelligente. La réalisation de ce projet nous a permis de maîtriser :

— Les concepts de base des vidéosurveillances.

— Les outils de traitements d'images.

— Les méthodes de reconnaissance faciales.

Nous avons donc développé, un outil qui permet de reconnaître une personne, pour cela nous avons suivi le processus de reconnaissance des formes à savoir :

— Création de la base de données.

— Apprentissage.

— Détection d'une personne et reconnaissance de cette dernière.

L'outil a été validé à l'aide de tests sur des personnes vues de faces, de profils et avec ou sans accessoires ; et les résultats obtenus sont concluants en matière de reconnaissance.

Perspectives futures :

— Intégrer l'outil développé dans une application réelle de vidéosurveillance pour l'authentification.

— Adjonction des systèmes de télésurveillance à un centre de contrôle de sécurité.

— Détection d'intrus en temps réels.

BIBLIOGRAPHIE

[1] F.Mohamed et al. le système rapace. vidéo surveillance à distance. rapport de projet TER. univérsité de Montpelier 2. 2011.

[2] V.Gouaillier, A.Fleurant. la vidéosurveillance intelligente : promesses et défis. rapport de veille technologique et commerciale. CRIM. mars 2009.

[3] L.Beddiaf. vidéosurveillance principe et technologies. DUNOD. Paris 2008.

[4] F.Nilsson. Intelligent Network Video : Understanding Modern Video Surveillance System. Boca Raton : CRC Press, 2009.

[5] J.Honovich. Security Manager's Guide to Video Surveillance. Version 2.0, IPVideoMarket.info, Novembre 2008.

[6] Axis Communications, H.264 video compression standard. New possibilities within video surveillance. Document technique. 2008.

[8] S.Guerfi. authentification d'individus par reconnaissance de caractéristique biométriques liées aux visages 2D/3D, thèse doctorat, univérsité d'Evry-val d'Essonne, France, 2008.

[9] V.Bruce. Recognizing faces. Lawrence Erlbaum Associates, London, U.K,1988.

[10] W.Shepherd. et al. Studies of cue saliency, in : G.M. Davies, H.D. Ellis, J.W. Shepherd (Eds.), Perceiving and Remembering aces, Academic Press, London, UK, 1981.

[11] M.Zrelli, implémentation d'une méthode de détéction et suivi de visage en temps réel, Ecole royale militaire Bruxelles royaume de la Belgique, 2006/2007.

[12] Cheng-Chin. et al. A novel method for detecting lips, eyes and faces in real time. Real-Time Imaging, 9(4) : 277-287, 2003.

[13] M.Belahcene, authentification et identification en biométrie, univérsité de Biskra, Algérie 2013.

[14] A. Melakh, reconnaissance des visages en condition dégradées, thèse de doctorat, univérsité d'Evry-val d'Essonne, France 2009.

[15] Y.Wang. C.Chua, and Y. Ho. Facial feature detection and face recognition from 2D and 3D images. Pattern Recognition Letters, 23 :1191–1202, 2002.

[16] K.Bouchra, Mise au point d'une application de reconnaissance facial, univérsité de Tlemcen, 2013.

[17] A.J.Goldstein. L.D.Harmon and A.B.Lesk, Identification of Humman Faces, Proc.IEEE, May 1971, vol.59, No. 5, 748-760.

[18] L.Sirovich and M.Kirby, A Low -Dimensional Procedure for the Characteri- zation of Human Faces, J. Optical Soc. Am. A, 1987, vol.4, No. 3, 559-524.

[19] M.A.Turk and A.P.Pentland, Face Recognition using Eigenfaces, Proc. IEEE, 1991, 586-591.

[20] National Science and Technology Concil (NSTC). Comittee on Technology. Face Recongnition. 7 Aout 2006, 10p.

[21] S.Bennaouche, étude et réalisation d'un système de vidéo de surveillance à distance, univérsité de Béjaia 2014.

[23] M.Turk and A.Pentland. Eigenfaces for recognition. Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71–86, 1991.

[24] A.S.Tolba. A.H.El-Baz and A.A.El-Harby, Face Recognition : A Litera- ture Review, INTERNATIONAL JOURNAL OF SIGNAL PROCESSING VOLUME 2 NUMBER 2 2005 ISSN 1304-4494.

WEBOGRAPHIE

[7] https ://videosurveillance.ooreka.fr/comprendre/caméra-de-surveillance

[22] https ://labiometrie.wordpress.com/2017/02/12t/reconnaissance-faciale/

[25] https ://openclassrooms.com/courses/apprenez-a-programmer-en-python

[26] https ://openclassrooms.com/courses/introduction-a-la-vision-par-ordinateur

Résumé

Le travail réalisé porte sur l'intégration d'un système de reconnaissance faciale à la télésurveillance.

Pour cela nous avons créée une base de donnée, effectuer un apprentissage puis une détection du visage.

Finalement, la reconnaissance est effectué grâce à la méthode ACP, des tests ont été effectués sur plusieurs images, et les résultats sont satisfaisants.

Mots-clés : Reconnaissance faciale, ACP, Apprentissage, télésurveillance.

Abstract

The work carried out involves the integration of a facial recognition system with remote monitoring.

For this we created a database, to carry out an apprenticeship and then a detection of the face.

Finally, the recognition is carried out using the PCA method, tests have been carried out on several images, and the results are satisfactory.

Keywords : Facial Recognition, PCA, Learning, Remote Monitoring.