Ministère de l'Enseignement Supérieur
Université de Sfax
École Nationale d'Ingénieurs de Sfax
Année : 2008

Cycle de Formation Doctorale en
Nouvelles Technologie des Systèmes
Informatiques dédiées
Mastère
No d'ordre: NTISID

MASTÈRE

présenté à

l'Ecole Nationale d'Ingénieurs de Sfax
(Département de Génie Électrique)

en vue de l'obtention

du **Diplôme de Mastère** *en*

Nouvelles Technologie des Systèmes Informatiques dédiées

par

HENTATI RAIDA

L'AUTHENTIFICATION BIOMÉTRIQUE DES PERSONNES PAR L'IRIS

soutenu le 21 juin 2008, devant la commission d'examen :

MM.	Mohamed Abid	Président
	Chokri Ben Amar	Membre
	Moncef Bousselmi	Membre

Table des matières

I Introduction générale **1**

II LES TECHNIQUES DE LA BIOMERIE ETAT DE L'ARTS **3**

II.1 Introduction 3

II.2 La biométrie 3

II.2.1 Les caractéristiques d'un système biométrique 4

II.2.2 Processus de fonctionnement d'un système d'identification ou d'authentification biométrique 5

II.2.3 Performances des systèmes biométriques 5

II.2.4 Modes d'un système de reconnaissance biométrique 6

II.2.4.1 Mode authentification 7

II.2.4.2 Mode identification 7

II.2.5 Présentation des exemples de techniques des biométries 8

II.3 Multimodalité 8

II.4 Techniques biométriques d'authentification 10

II.4.1 Empreinte digitale 10

II.4.2 Forme de main 11

II.4.3 Visage 11

II.4.4 Iris 12

II.4.5 Rétine 12

II.4.6 Signature 13
II.4.7 Frappe sur clavier d'ordinateur 13
II.4.8 Reconnaissance vocale 13
II.4.9 ADN (Acide Désoxyribonucléique) 14
II.5 Comparaison des systèmes de reconnaissance biométrique 14
II.6 Domaines d'utilisation 16
II.7 Conclusion 16

III LA RECONNAISSANCE BIOMETRIQUE PAR L'IRIS 17

III.1 Introduction 17
III.2 Les caractéristiques de l'iris 17
III.2.1 Définition 17
III.2.2 Caractéristiques de l'iris 18
III.3 Capture de l'iris 19
III.4 L'appareil de mesure de l'iris 20
III.5 Les bases de données publiques 21
III.6 Les travaux de reconnaissance par l'iris 24
III.6.1 Introduction 24
III.6.2 La technique de Daugman 24
III.6.3 Le système de Wildes 26
III.6.4 Le système Masek 27
III.6.5 Autres algorithmes 28
III.6.5.1 Algorithme de Bole et du Boashash 28
III.6.5.2 Algorithme de Kong et Zhang 29
III.6.5.3 Algorithme de L.Ma 29
III.6.5.4 Algorithme de Chin 30
III.6.5.5 Algorithme Fancourt 31

III.7 Conclusion 31

IV IMPLEMENTATION DE l'AUTHENTIFICATION BIOMETRIQUE PAR L'IRIS 32

IV.1 Introduction 32

IV.2 Système d'authentification basée sur la biométrie : l'iris 32

IV.2.1 Base d'image de test : CASIA 33

IV.2.2 Localisation de l'iris 34

IV.2.2.1 Filtrage 34

IV.2.2.2 Détection du Contour 35

IV.2.2.3 La transformée de Hough 36

IV.2.3 Extraction de signature de l'iris 38

IV.2.3.1 Normalisation 38

IV.2.3.2 Codage 39

IV.2.4 Comparaison 40

IV.3 Mesure de performance de l'algorithme :Taux d'erreur 41

IV.4 Développement d'un algorithme d'authentification par l'iris 42

IV.4.1 Localisation de l'iris 42

IV.4.2 Extraction du vecteur caractéristique 44

IV.4.2.1 Les ondelettes de HAAR 44

IV.4.2.2 Code binaire 45

IV.4.3 Prise de décision 45

IV.4.4 Mesure de taux erreur 46

IV.5 Comparaison entre les deux algorithmes 46

IV.6 Conclusion 48

Conclusion Générale 49

Bibliographie **51**

Table des figures

II.1 *Processus de reconnaissance biométrique* 5

II.2 *Courbe des variations des taux d'erreurs des différents types de taux d'erreurs en fonction du seuil de décision* 7

II.3 *Exemples de biométries* 8

II.4 *Systèmes biométriques Multimodale* 9

III.1 *La structure de l'oeil.* 18

III.2 *Les caractéristiques de l'iris.* 19

III.3 *Le système Iridien LG EOU 2200.* 20

III.4 *Exemples des systèmes Iridien.* 21

III.5 *Des exemples des images de la base de données d'iris CASIA.* 22

III.6 *Des exemples des images de la base de données d'iris MMU.* 22

III.7 *Des exemples des images de la base de données d'iris BATH.* 22

III.8 *Des exemples des images de la base de données d'iris UPOL.* 23

III.9 *Des exemples des images de la base de données d'iris UBIRIS.* 23

III.10 *Des exemples des images de la base de données d'iris ICE.* 24

III.11 *Segmentation de l'iris par la méthode intégro-différentielle[18].* 25

III.12 *Une image d'iris normalisée [18].* 26

III.13 *L'iris code généré par la méthode Daugman [18].* 26

III.14 *Processus de segmentation de l'iris par la méthode proposée par Masek [27].* 28

III.15 *L'illustration du procédé de normalisation pour deux images du même iris [27].* 28

III.16 *Traitement de S- Iris-codage* 31

IV.1 *Étapes générales du système d'identification d'iris* 33

IV.2 *Appareil-photo d'iris développé à CASIA* 34

IV.3 *Des images de l'iris de CASIA* 34

IV.4 *Filtrage de l'image :(a) Image originale (b) Image filtrée* 35

IV.5 *Détection de contour de l'image :(a) Image original (filtrée)(b)contour de Canny* 35

IV.6 *Le diagramme des étapes de localisation de l'iris* 37

IV.7 *Des exemples de location des images de l'iris de CASIA* 38

IV.8 *Des exemples de normalisation des images de l'iris de CASIA* 39

IV.9 *Courbe de FAR et FRR en fonction de nombre de sujets* 41

IV.10 *Résultats de localisation(a)Détection de pupille (b)Détection de l'iris* . . . 44

IV.11 *Les ondelettes de HAAR* 44

IV.12 *La transformé de Haar : (a)une seule itération (b) deux itérations* 45

IV.13 *La courbe de FAR /FRR en fonction de distance de Hamming* 46

Liste des tableaux

II.1 Les avantages et les inconvénients des techniques d'identification biométrique 15

III.1 Les caractéristiques des diapositives d'acquisition de l'iris 21

IV.1 Les étapes et les résultats de localisation de la pupille puis de l'iris 43

IV.2 Mesure de FAR et FRR pour les deux approches proposées 47

IV.3 Mesure le taux de reconnaissance pour les deux approches proposées 47

Chapitre I

Introduction générale

Les systèmes de sécurité traditionnels sont fondés sur la reconnaissance visuelle des individus, la possession d'une clé ou d'une carte magnétique, ou encore la connaissance d'un code ou d'un mot de passe. Toutes ces méthodes présentent des inconvénients, tels que le risque de perte , d'oubli , de vol ou de falsification. D'ou la nécessité de concevoir d'autres outils pour résoudre ses problèmes. Nous proposons comme solution les systèmes automatisés biométriques.Ces derniers évitent ces écueils tout en autorisant la reconnaissance des personnes avec grande précision. Plusieurs facteurs sont critiques pour le fonctionnement d'un système biométrique la précision, la vitesse d'acquisition, l'acceptabilité par les usagers, l'unicité de l'organe biométrique, la fiabilité et la nécessité de stockage des données. Le système d'identification doit différencier une personne autorisée d'un imposteur. Donc l'identification par biométries est introduite essentiellement pour l'amélioration des systèmes de sécurité. La popularité de la biométrie a considérablement augmenté ainsi le développement des technologies liées à la sécurité est devenu un axe stratégique majeur pour de nombreuses entreprises et états. La biométrie constite une des plus prometteuses. Les recherches actuelles s'orientent vers l'intégration de plusieurs biométries pour pouvoir apporter des garanties de performances concernant les systèmes de sécurité.

Dans ce contexte, nous avons entamé un sujet s'intéressant à l'identification biométrique. Pour cela, nous avons étudié quelques techniques biométriques tels que le visage, l'empreinte digitale, l'iris, la forme de main, la démarche, la signature, l'ADN, etc.

Ce projet a pour objectif d'étudier et d'appliquer l'une de ces biométries . Nous avons choisit l'iris. Ceci nous a amené à étudier les caractéristiques de cet organe afin d'implémenter un algorithme d'identification par l'iris.

Ce mémoire est composé de trois chapitres : dans le premier chapitre nous présenterons quelques notions nécessaires concernant le traitement des biométries ainsi qu'un état de l'art sur les biométries. Dans le second chapitre nous établisserons une étude des caractéristiques de l'iris. Ensuite nous citerons les bases de données publiées pour la recherche biométrique par l'iris. Enfin, nous présenterons les travaux faites dans ce domaine. Dans le troisième chapitre nous développerons l'approche suivie dans notre algorithme pour authentification par l'iris. Pour finir nous présenterons nos conclusions par rapport à la problématique et nous proposerons des perspectives à de nouveaux travaux de recherches dans le domaine.

Chapitre II

LES TECHNIQUES DE LA BIOMERIE ETAT DE L'ARTS

II.1 Introduction

La biométrie ou la reconnaissance biométrique est l'exploitation automatisée ou semi-automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité ; ceci suscite une attention accrue depuis les attaques terroristes du 11 septembre 2001. Les gouvernements de nombreux pays comptent de plus en plus sur la biométrie pour accroître la sécurité dans les aéroports et aux postes frontaliers et pour produire des pièces d'identité encore plus sûres. Des technologies qui font appel à la biométrie sont aussi utilisées ou mises à l'épreuve dans une foule d'applications commerciales. Dans ce chapitre nous commençons par des définitions des termes biométrie et multimodale. Ensuite nous donnons un aperçu comparatif des principales technologies biométriques qui sont disponibles et nous examinons les domaines qui s'intéressent au sujet de la sécurité et de la protection de la vie privée dans le contexte de la biométrie .

II.2 La biométrie

Nous définissons la biométrie comme une technique d'identification et d'authentification qui consiste à transformer les caractéristiques biologiques, génétiques et comportementales d'une personne telles que les empreintes digitales, l'iris, la rétine, la voix, la

forme du visage, la forme de la main, une empreinte numérique, etc [6].
Le mot biométrie venant du grec " bios " (vie) et de " métrie" (mesure), cette technique permet d'identifier l'être vivant en exploitant des parties du corps qui sont inchangeables au cours du temps. Avec la biométrie, l'identité est réduite aux caractéristiques physiques et génétiques qui confirment de l'unicité d'une personne [13].

II.2.1 Les caractéristiques d'un système biométrique

Tout être humain a des caractéristiques physiologiques et comportementales qui peuvent être utilisées comme une biométrie lorsqu'il répond aux exigences suivantes :

- Universelles : exister chez tous les individus.
- Uniques : permettre de différencier un individu par rapport à un autre.
- Permanentes : autoriser l'évolution dans le temps.
- Collectages : enregistrer les caractéristiques d'un individu avec l'accord de celui-ci.
- Mesurables : autoriser une comparaison future.

Il faut prendre en compte plusieurs autres facteurs pour savoir si l'on peut utiliser un système de reconnaissance biométrique des personnes [6], notamment :

- La performance : c'est la fiabilité et la rapidité de reconnaissance du système, les ressources requises pour obtenir la fiabilité et la rapidité de reconnaissance voulue ; et les facteurs opérationnels et environnementaux qui influent sur ses dernières contraintes du système.
- L'acceptabilité : c'est le nombre de gens acceptant l'utilisation d'une technologie de reconnaissance biométrique.
- La facilité de contournement : facilité avec laquelle le système peut être induit en erreur par des méthodes inexactes.

Les techniques biométriques peuvent être classées en trois catégories :

- Les techniques réalisées par l'analyse biologiques (ADN, sang, salive, odeur, etc.),
- Les techniques basées sur l'analyse comportementale (dynamique du tracé de signature, frappe sur un clavier d'ordinateur, etc.),
- Les techniques réalisées par l'analyse morphologique (empreintes digitales, forme de la main, traits du visage, iris, etc.)

II.2.2 Processus de fonctionnement d'un système d'identification ou d'authentification biométrique

Un système de reconnaissance biométrique se compose d'un appareil de saisie qui enregistre les caractéristiques en question et d'un logiciel qui interprète les données et détermine l'acceptabilité de la personne[13]. Les systèmes de reconnaissances biométriques fonctionnent comme suit :

- Capturer un échantillon biométrique d'un candidat ou d'une preuve biométrique,
- Extraire des données biométriques à partir de cet échantillon,
- Comparer les données biométriques avec celles contenues dans un ou plusieurs modèles de référence.
- Indiquer s'il s'agit d'une authentification de l'identité ou de l'identification qui a été réalisée.
- Prendre la décision s'il s'agit d'un client ou un imposteur.

La figure suivante représente le processus de reconnaissance biométrique [?] :

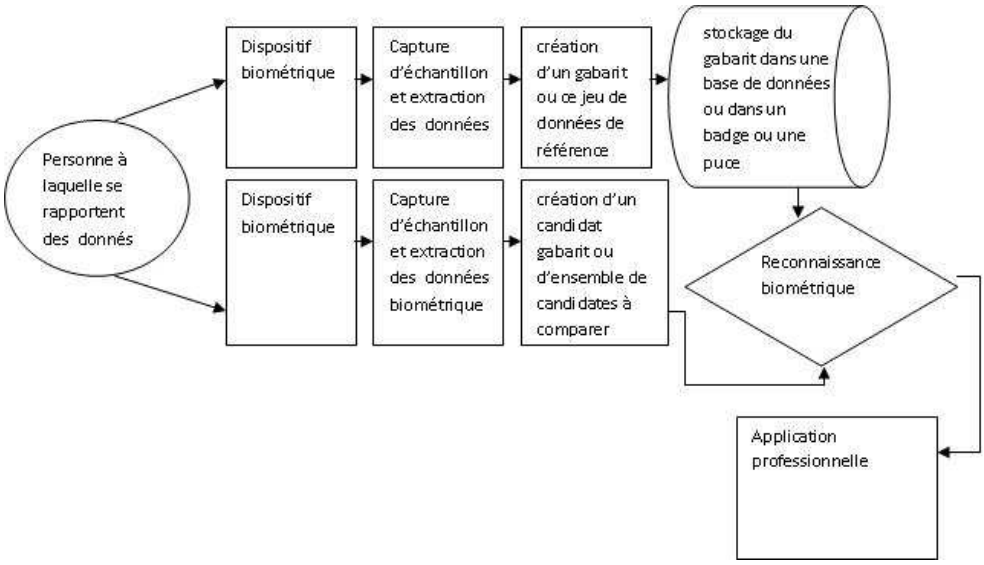


FIGURE II.1 – *Processus de reconnaissance biométrique*

II.2.3 Performances des systèmes biométriques

Etant donné que la biométrie repose sur la reconnaissance des données, la difficulté porte sur le niveau de performance du système mis en place. De ce fait il est impossible d'obtenir une coïncidence absolue (100%de similitude) entre le fichier "signature" créé lors de l'enrôlement et le fichier "signature" crée lors de la vérification. Les éléments d'origine

(image,son) utilisés pour les traitements informatiques ne pouvant jamais être reproduits à l'identique [23]. Les performances des systèmes d'authentifications biométriques s'expriment par :

- FRR : Taux de Faux Fejets (False Rejection Rate) : pourcentage de personnes rejetées par erreur.

$$FRR = \frac{NombredeFauxRejet}{Nombreclients} \tag{II.1}$$

- FAR : Taux de Faux Acceptations (False Acceptance Rate) : pourcentage d'acceptations par erreur.

$$FAR = \frac{NombreFausseAcceptation}{Nombreimposteurs} \tag{II.2}$$

- TER : Taux totale d'erreur (Total Error Rate), qui est le pourcentage de décisions erronées du système.

$$TER = \frac{NombredeFauxRejet+NombreFausseAcceptation}{Nombretotald'accs} \tag{II.3}$$

- EER : Taux d'égale erreur (Equal Error Rate), donne un point sur lequel le FAR est égal au FRR.

En fait, les taux d'erreurs FAR et FRR, définis plus haut, varient d'une manière inverse par rapport au seuil. Dans le cas d'un score de similarité, plus le seuil de décision augmente, plus le taux de FRR augmente et plus le taux de FAR diminue. Afin de visualiser ces variations, il est possible de tracer en fonction du seuil les trois taux d'erreurs. La Figure 2 montre un exemple d'une telle courbe. On peut remarquer que dans les zones où le seuil est faible le taux de fausses acceptations est grand et celui de faux rejets est faible, et inversement dans les zones où la valeur du seuil est grande. A chaque valeur du seuil correspond une valeur particulière de FAR et une autre de FRR. Ce choix induit un fonctionnement particulier du système et est appelé par conséquent point de fonctionnement. Plusieurs points de fonctionnement particuliers sont utilisés pour comparer des systèmes biométriques entre eux. Donc ces taux d'erreur dépendent d'un seuil qui est fixé en fonction du degré de sécurité souhaité par l'application. Ce valeur peut varier considérablement d'une application à une autre.

II.2.4 Modes d'un système de reconnaissance biométrique

Un système de reconnaissance biométrique peut fonctionner en mode vérification ou en mode identification.

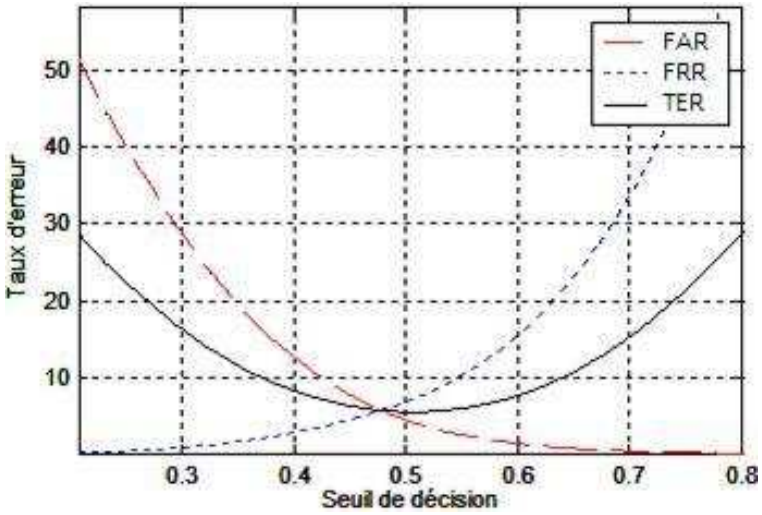


FIGURE II.2 – *Courbe des variations des taux d'erreurs des différents types de taux d'erreurs en fonction du seuil de décision*

II.2.4.1 Mode authentification

Il s'agit une comparaison individuelle (1-1) : le système vérifie l'identité de la personne. Il valide son identité en comparant les données biométriques saisies aux gabarits biométriques de la personne entreposés dans la base de données du système (ou sur une carte à puce portée par la personne). La vérification de l'identité est habituellement utilisée pour l'identification catégorique, lorsque l'on veut éviter que plusieurs personnes utilisent la même identité[**?**].

II.2.4.2 Mode identification

C'est une comparaison collective (1-N) : le système reconnaît une personne en examinant tous les gabarits dans le système à la recherche d'un appariement. Etant donné que de nombreuses comparaisons doivent être effectuées en mode identification, un appariement accidentel ou des appariements multiples sont possibles. L'identification est un élément crucial pour des applications comme les listes de surveillance, pour lesquelles le système détermine si le gabarit biométrique d'une personne se trouve dans sa base de données[**?**].

II.2.5 Présentation des exemples de techniques des biométries

La plus part des techniques biométriques sont actuellement utilisées par les applications de sécurité. Chacune a ses avantages et ses inconvénients, le choix d'une technique se fait suivant le type d'application. La figure suivante montre la diversité des techniques biométriques utilisé dans plusieurs domaines, lesquels ne seront pas tous abordés dans ce rapport.

FIGURE II.3 – *Exemples de biométries*

II.3 Multimodalité

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'aux applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles [35]. Afin d'améliorer la sécurité des systèmes précédents, une première solution consiste

à intégrer la biométrie avec l'identification basée sur une connaissance ou une possession. Cette méthode permet d'améliorer la sécurité du système, mais elle possède des faiblesses inhérentes à l'identification basée sur une connaissance ou une possession. La multimodalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique [25]. Par performance, nous entendons à la fois la précision du système mais aussi son efficacité, plus particulièrement en mode identification [23]. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer partie de cette complémentarité afin d'améliorer la performance globale du système. De ce fait la multimodalité est la combinaison de plusieurs modalités biométriques permettant d'augmenter les performances globales, de diminuer les taux d'erreur et d'impossibilité de captage. Dans ce cas, le couplage de plusieurs modalités paraît une voie prometteuse qui reste à valider [1]. Actuellement il devenue possible de numériser, stocker et retrouver des formes biométriques et de les traiter par ordinateur. Les travaux dans [30] le système biométrique multimodal est développé en utilisant le visage, l'empreinte digitale, l'iris et la signature, illustré dans la figure suivante.

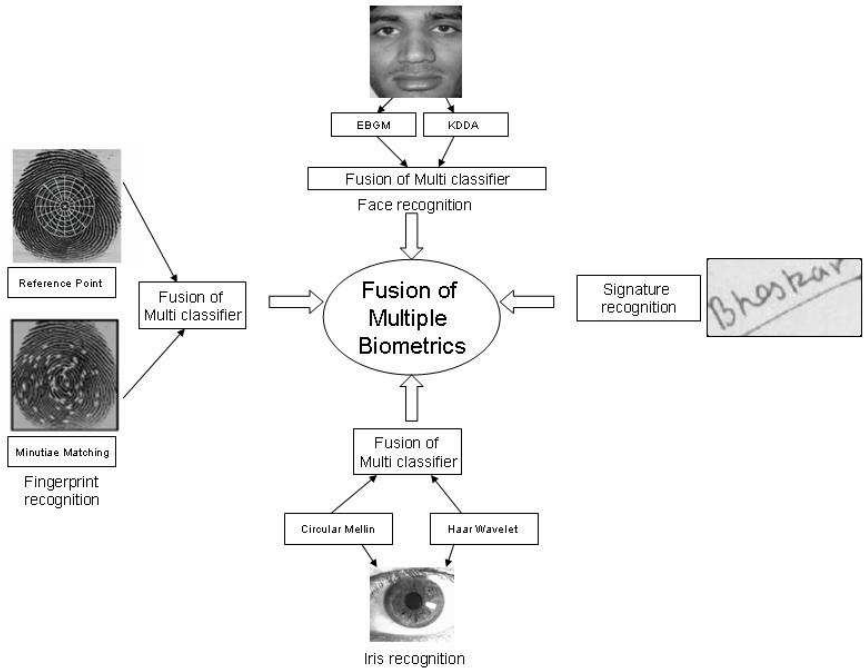


FIGURE II.4 – *Systèmes biométriques Multimodale*

Dans l'identification de visage, l'image de visage d'entrée est identifiée en utilisant l'algorithme élastique de graphique de groupe. La vérification d'empreinte digitale, est basée sur les filtres de Gabor. Dans l'identification d'iris, l'image d'entrée est localisée

en trouvant la pupille et l'iris ensuite en utilisant la combinaison de l'ondelette de Haar et de l'opérateur circulaire de Mellin. Dans la vérification de signature, le vecteur de dispositif se compose des dispositifs globaux et locaux de l'image de signature et puis en utilisant la distance euclidienne pour la comparaison. Les modules basés sur les différentes biométries renvoient une valeur de nombre entier après comparaison entre des vecteurs de base de données et de dispositif de question. Toutes les fusions sont faites au niveau du classificateur. Les points finaux sont produits en employant la somme de la technique de points aux points assortis de niveau qui sont passés au module de décision.

II.4 Techniques biométriques d'authentification

Il existe une variété de technologies de reconnaissance biométrique, soit sur le marché, soit à l'étape de la recherche et de développement. Les technologies les plus courantes servent à la reconnaissance des empreintes digitales, du visage, de l'iris et de la main ou des doigts. Les technologies moins fréquemment utilisées s'appuient sur la reconnaissance des images rétiniennes, la démarche et la vérification dynamique de la signature.

II.4.1 Empreinte digitale

La reconnaissance d'empreintes digitales est la technique biométrique la plus ancienne et la plus mature. Elle a été développée vers la fin du 19ème siècle par Alphonse Bertillon, fondateur de la police scientifique en France [5]. Cependant, les empreintes digitales représentent une mesure biométrique assez mal acceptée par les utilisateurs à cause de l'association qui est souvent faite avec la criminologie. Plusieurs méthodes sont employées pour reconnaître les empreintes digitales : localisation des minuties, analyse spectrale à l'aide d'ondelettes, traitement de textures, etc. La méthode de la localisation des minuties : ne retient que l'emplacement des minuties les plus pertinentes. Elle est peu sensible aux déformations des doigts entre plusieurs vérifications (doigts plus ou moins appuyés sur le capteur). Le traitement de textures des paramètres issus de certaines propriétés de la texture des empreintes (orientation, fréquence, etc.) sont comparés. Cette méthode permet un traitement très rapide, et donc un temps de réponse très court. Il existe bien d'autres méthodes, mais elles ne sont pas divulguées par les entreprises qui les développent pour un souci de propriétés intellectuelles.

II.4.2 Forme de main

La reconnaissance s'effectue à partir de la géométrie de la main dans l'espace (3D) : longueur des doigts, largeur et épaisseur de la paume, dessins des lignes de la main. Au moment de la capture de l'image, la personne pose sa main sur une platine où les emplacements du pouce, de l'index et du majeur sont matérialisés et comparés à la base de donnée. On extrait environ quatre vingt dix caractéristiques. Cette biométrie est toutefois sujette aux modifications de la forme de la main liées au vieillissement [34].

II.4.3 Visage

La reconnaissance faciale se base sur les caractéristiques significatives du visage. Il existe plus de 60 critères fondamentaux. Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire l'ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc. On évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne. Il existe plusieurs variantes de la technologie de reconnaissance du visage. Quatre méthodes de base sont utilisées par les fabricants de systèmes biométriques : Eigenface, l'analyse de points particuliers, les réseaux de neurones et le traitement automatique de visage.
La première a été développée est celle de "Eigenface". Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière [32]."Le traitement automatique du visage "est une technologie rudimentaire, elle caractérise les visages par des distances et des proportions entre des points particuliers comme les yeux, le nez les coins de la bouche. Aussi éprouvé que les autres technologies, le traitement automatique de visage est la plus efficace dans des situations de capture d'image avec peu d'éclairage. "l'analyse points particuliers "est la technologie d'identification faciale la plus largement utilisée. Cette technologie se rapproche de Eigenface, mais elle est capable de s'adapter à des changements d'aspect facial (sourire, froncer des sourcils,...). Et " Les réseaux de neurones "permettent en théorie de mener à une capacité accrue d'identification dans des conditions difficiles de capture. Les réseaux de neurones emploient un algorithme pour déterminer la similitude entre des captures d'images de visage et des gabarits. En employant le plus possible de captures et de gabarits.

II.4.4 Iris

L'iris présente une texture très détaillée et unique dont les caractéristiques permettent de reconnaître une personne. Les systèmes automatisés de reconnaissance de l'iris sont relativement récents Ces systèmes illuminent l'iris avec une lumière proche de l'infrarouge (inoffensive pour l'oeil) et en prennent une photo au moyen d'une caméra numérique de grande qualité. Les motifs aléatoires de l'iris sont alors encodés en termes mathématiques et les codes ainsi produits sont comparés de manière statistique à un ou à plusieurs gabarits. La méthode employée pour la caractérisation d'un iris est celle brevetée par John Daugman [19]. Après la numérisation de l'image de l'oeil, l'algorithme va déterminer le centre de la pupille et la zone où se trouve l'iris. Puis sur deux secteurs angulaires, l'algorithme y découpe des bandes de taille régulière et en génère un gabarit (IrisCode) à partir de l'analyse locale de la texture de l'iris. La taille des bandes varie en fonction de la dilatation de la pupille. Cette technique permet de s'affranchir du degré de dilatation de la pupille. Avec le même nombre de bande sur une pupille très dilatée, on retrouve le même motif que sur l'oeil avec une dilatation normale de la pupille. La seconde étape consiste à extraire les paramètres caractéristiques de l'iris. La plupart du temps, on utilise une transformée par ondelette. La dernière étape consiste à prendre la décision d'accepter ou de rejeter selon le résultat de la phase de comparaison.

II.4.5 Rétine

Cette mesure biométrique est plus ancienne que celle utilisant l'iris. La mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), qui effectue ensuite un balayage de la rétine. Il est physiquement impossible d'effectuer une mesure rétinienne à une distance de 30 cm ou plus sur un sujet mobile comme on peut le voir dans certains films. Cette méthode requiert des sujets coopératifs et entraînés. Cette technique se base sur le fait que le schéma et le dessin formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'oeil) est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut ainsi fournir jusqu'à 400 points caractéristiques du sujet, que l'on peut comparer aux 30 à 40 points fournis par une empreinte digitale [21]. Les difficultés liées à la capture de l'image d'une rétine sont autant psychologique que médicale et technique. Pour obtenir une image d'une rétine, il est nécessaire d'éclairer le fond de l'oeil à l'aide d'un faisceau lumineux ; à travers la pupille et le corps vitreux. Ce faisceau est de très faible intensité pour ne pas gêner l'utilisateur ; il est sans danger et de plus faible intensité que sur les dispositifs ophtalmologiques. Un système de caméra très précis vient ensuite récupérer l'image de la rétine. Des lecteurs de

rétine sont disponibles, et permettent d'obtenir un très haut niveau de sécurité.

II.4.6 Signature

La signature est peu utilisée mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents électroniques, rapports, contrats). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo . Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc. C'est à dire tout ce qui peut permettre d'identifier une personne de la façon la plus sure possible quand on utilise une donnée aussi changeante que la signature [28]. La méthode d'identification utilise les modèles cachés de Markov comme classificateurs. L'image de signature doit passer par les étapes suivantes : le filtrage permettant d'enlever le bruit. la correction de l'inclination de la feuille dans le module de balayage. La binarisation du graphique. Le centrage l'image de signature. Et l'application de l'algorithme. L'extraction de dispositif caractéristique. Le vecteur obtenu contient 300 éléments[10]

II.4.7 Frappe sur clavier d'ordinateur

Les frappes au clavier représentent une des méthodes d'identification qui est influencée par plusieurs contraintes ; tout d'abord, selon le texte que l'on tape et, de manière plus générale selon sa nature, on aura tendance à modifier sa façon de taper au clavier[21]. Ces techniques sont assez satisfaisantes mais restent néanmoins statistiques. Ensuite, le facteur comportemental entre en jeu, et ce facteur va être-lui- différent pour chaque individu. Les facteurs sont à peu près identiques à ceux évoqués précédemment : ce sont les durées entre frappes, la fréquence des erreurs, la durée de la frappe elle-même, etc. La différence se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux, soit dynamiques et statistiques (comparaison continuelle entre l'échantillon et la référence).

II.4.8 Reconnaissance vocale

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux parce qu'ils représentent une combinaison de facteurs comportementaux (vitesse, rythme, etc.) et physiologiques (tonalité, âge, sexe, fréquence, accent, harmoniques, etc.). Ils ne sont en général pas limitables. L'intérêt de cette tech-

nique est l'authentification lors des communications téléphoniques ou sur Internet [3].
Nous pouvons néanmoins décrire un système standard de la façon suivante : Le signal acoustique est, dans un premier temps, analysé afin d'en extraire des paramètres. Ces paramètres résultent, entre autres, d'une analyse spectrale du signal (coefficients de prédiction linéaires ou bancs de filtres).
Les paramètres servent ensuite à l'élaboration éventuelle d'un modèle et sont introduits dans un classifieur qui permettra de déterminer l'identité du locuteur. De nombreuses techniques sont utilisées pour réaliser ce classifieur. On peut citer entre autre : les réseaux de neurones, les champs de Markov cachés, les mélanges gaussiens, la quantification vectorielle, etc.

II.4.9 ADN (Acide Désoxyribonucléique)

La technique d'identification par analyse de l'ADN est connue sous le nom d'empreintes génétiques. La technique des empreintes génétiques est notable dans son principe et très performante. Quand elle est associée à la technique d'amplification génique, elle comporte de vastes possibilités d'application. Les empreintes génétiques sont plus performantes pour une exclusion d'identité ou de parenté, que pour affirmer une relation d'identité entre deux prélèvements ; se posent, d'une part, les problèmes d'interprétation de la comparaison de l'emplacement des bandes, et, d'autre part, la connaissance de la fréquence d'un profil de répartition de ces bandes dans la population générale [20]. Actuellement, le temps requis pour une analyse et le coût associé à celle-ci restreignent son utilisation dans des domaines autres que celui de l'identification judiciaire. Cependant, ce procédé biométrique fait l'objet de recherche intensive puisqu'il représente la technologie d 'identification par excellence avec une marge d'erreur au dessous des autres moyens biométriques.

II.5 Comparaison des systèmes de reconnaissance biométrique

Certaines techniques de reconnaissance biométrique sont disponibles sur le marché. Le tableau suivant décrit les avantages et les inconvénients des neuf identifiants biométriques les plus utilisés.

Technique	Avantage	Inconvénient
Empreinte digitale	ergonomie Coût Facile de mise en place	Laisse des traces relativement Variable Acceptabilité moyenne
Forme de la main	Très ergonomique Bonne Acceptabilité	Assez chère Perturbation possible par des blessures
Visage	Bonne Acceptabilité Coût	Très Variable Peu fiable : réligon Psychologie Vulnérable aux attaques
Iris	Grande fiabilité Pérennité	Assez chère Enregistrement assez contraignant
Rétine	Grande fiabilité Pérennité	très chère Enregistrement très contraignant
Signature	Ergonomie	fiabilité Dépend de l'état émotionnel de l'homme
Frappe au clavier	Mise en ouvre rapide	Dépend de l'état physique de l'homme Utilisation des claviers d'un format différents AZERTY, QWERTY
Voix	Bonne acceptabilité Pérennité	Relativement Variable Peu fiable
ADN	Pérennité Grande fiabilité	assez chère

TABLE II.1 – Les avantages et les inconvénients des techniques d'identification biométrique

II.6 Domaines d'utilisation

La biométrie permet d'associer à une personne une identité. Elle est utilisée dans plusieurs types d'applications. Ces systèmes pourraient s'appliquer dans les secteurs suivants [?].

- Les systèmes de sécurité militaire.
- L'accès à des pièces de travail spéciales, comme des chambres stériles, chambres blanches, pour les entreprises qui travaillent dans des secteurs de hautes technologies.
- L'accès au secteur administratif des banques où les données de travail sont confidentielles. La sécurité y est assurée par des cartes magnétiques d'accès et pour l'utilisation des ordinateurs par un code généré par une seconde carte.
- Empêcher ou autoriser l'accès à certaines zones dans des prisons ou des administrations pour éviter les attentats.

II.7 Conclusion

Dans ce chapitre nous avons présenté le principe d'un système de reconnaissance biométrique en décrivant ces caractéristiques, ces modes, ces moyens et ces performances. L'arrivée de la biométrie a engendré de grands espoirs dans l'industrie mondiale. Il devient important de concevoir dès aujourd'hui des architectures de systèmes robustes. De ce fait, ces systèmes se heurtent à plusieurs problèmes tel que le bruit qui peut attaquer l'échantillon, les effets de vieillissement qui peuvent produire des changements physionomiques importants ainsi les accidents. Les différentes techniques biométrique ont été brièvement décrites, En mettant l'accent sur leurs avantages et inconvénients. Dans la suite de ce travail nous allons nous intéresser à l'une de ce technique biométrique, en occurrence le sujet d'authentification biométrique par l'iris.

Chapitre III

LA RECONNAISSANCE BIOMETRIQUE PAR L'IRIS

III.1 Introduction

Le système de reconnaissance par l'iris permet d'effectuer une identification sûre et rapide d'une personne. Cet organe interne du corps humain, visible de l'extérieur est reconnu être le plus précis et efficace pour la discrimination, tout en étant le moins intrusif pour l'utilisateur lors de la reconnaissance d'une identité proclamée. En conséquence, ce dispositif trouvera des applications dans tous les domaines mettant en application des systèmes de sécurité. Il apparaît ainsi que le dispositif de reconnaissance par l'iris ne se limite pas au seul domaine de la surveillance, mais aussi des applications dans le domaine médical où il peut apporter au spécialiste des éléments non négligeables dans l'appréciation d'une pathologie Dans ce qui suit nous allons détailler les différentes caractéristiques de l'iris ainsi que les phases de son acquisition. Nous décrivons les bases de données publiques disponibles selon leurs caractéristiques et leur importance. Enfin nous donnons un aperçu sur ce domaine.

III.2 Les caractéristiques de l'iris

III.2.1 Définition

L'iris est situé dans l'humeur aqueuse, il est entouré par le blanc de l'oeil et la pupille qui est située en son centre, la cornée se trouve devant lui et le cristallin derrière. L'iris

correspond donc à la partie colorée de l'oeil et c'est cette partie qui nous intéresse au niveau de la reconnaissance biométrique [36]. La formation de l'iris pour un oeil humain

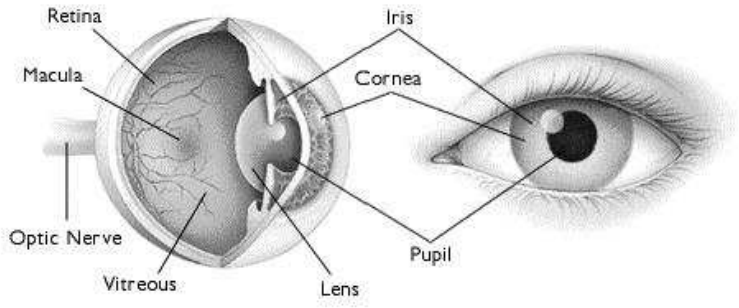


FIGURE III.1 – *La structure de l'oeil.*

commence au troisième mois de gestation. Les structures qui créent les éléments distinctifs sont terminées lors du huitième mois et la pigmentation se poursuit dans les premières années suivant la naissance [2].

III.2.2 Caractéristiques de l'iris

On recèle environ 244 caractéristiques pour un motif. En effet, la texture de l'iris ou ce que l'on appelle le motif de l'iris, comprend de nombreuses caractéristiques. Celles les plus souvent utilisées dans la biométrie, sont la collerette (on l'appelle ainsi car elle forme le dessin d'une collerette autour de la pupille), les tâches pigmentaires (comme les tâches de rousseur ou les grains de beauté), les cryptes (ce sont des petits creux), la couronne ciliaire (ou zone ciliaire, enchevêtrement de tubes fins formant un petit renflement), les sillions ou la pupille qui eux sont contrôlés suivant leur taille [**?**]. Ces éléments de l'iris restent fixe, ils ne varient que très peu durant toute une vie : chaque motif est stable et unique (la probabilité de similitude est de 1 sur 10 puissance 72). De plus, le motif de l'iris n'est pas relié aux gènes, c'est-à-dire à l'ADN, cela signifie que ce n'est pas en fonction des gènes du père et de la mère que le motif de l'iris est formé contrairement à la couleur des yeux. Donc deux individus, même s'ils sont frères, peuvent avoir la même couleur mais jamais le même motif. Par ailleurs, les vrais jumeaux non plus ne sont pas confondus, il y a assez de caractéristiques dans l'iris pour que l'on puisse les distinguer. L'organe iridien est relativement à l'abri des lésions. S'agissant d'un tissu interne, l'iris est protégé par la cornée et l'humeur aqueuse. Étant donné que ces deux barrières sont transparentes, l'iris peut être facilement identifié à plus d'un mètre. On peut donc facilement photographier l'iris[31].

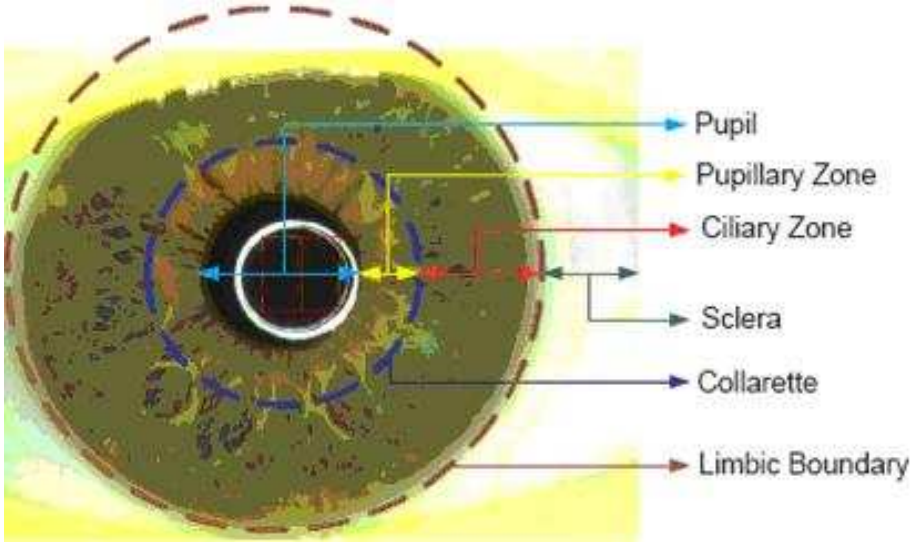


FIGURE III.2 – *Les caractéristiques de l'iris.*

III.3 Capture de l'iris

Etant donné que l'iris occupe une petite surface, le matériel utilisé actuellement pour l'observer ne permet pas une étude précise au niveau des éléments du motif :on a seulement les contours macroscopiques. Ce problème reste temporaire car la précision des capteurs augmente de plus en plus.

L'utilisateur doit fixer l'objectif d'une caméra numérique qui balaie l'iris d'une personne d'une distance de 30 cm à 60 cm, et acquiert directement son dessin. Elle le compare ensuite à un fichier informatisé d'identification personnelle (les systèmes de reconnaissance en usage aujourd'hui sont en mesure de fouiller une banque de données nationale à la vitesse de 100 000 codes iridiens par seconde)[16]. Or, l'iris est un organe sensible, sa taille est petite et il est obscurci par les cils, les paupières ou les lentilles de contacts. De plus, elle est variable et les utilisateurs ont tendance à bouger. Il est donc assez difficile d'avoir une bonne image de l'iris, il faut que ce soit rapide, précis et qu'il n'y ait pas de lumière pouvant se refléter sur l'oeil.

La prise de vue de l'iris est effectuée le plus souvent par une caméra (caméra CCD monochrome 640 x 480) employée avec une source de lumière de longueur d'ondes comprise entre 700 et 900 nm, invisible pour les humains[3]. D'autres systèmes emploient une caméra à large vision qui permet la localisation des yeux sur le visage, puis une autre caméra avec une vision étroite prend des images des yeux (il y a une plus grande résolution) avec un

capteur classique et une objective macro. Les différentes contraintes, en particulier de l'éclairage, impose une proximité entre le capteur et l'oeil (30 à 60 cm), car plus l'oeil est éloigné plus il y a de problèmes. Il faut également tenir compte des reflets ponctuels, du non uniformité de l'éclairage, et des images de l'environnement qui se reflètent sur l'iris. On utilise alors un éclairage artificiel (diodes DEL) infrarouge, tout en atténuant le plus possible l'éclairage ambiant.

III.4 L'appareil de mesure de l'iris

Parmi les appareils utilisés pour l'acquisition de l'image on cite le système iridien LG EOU2200 présenté par la figure . Dans cet appareil, il existe un rectangle au milieu utilisé pour aider les gens à placer leurs yeux dans l'emplacement exigé. Il y a 3 lumières infrarouges, l'un se trouve au sommet, le deuxième à gauche, et l'autre à droite. La personne qui va faire le test s'installe devant l'appareil-photo, et regarde dans le rectangle de l'appareil. La distance entre l'oeil et le système doit être fixée. Si la distance n'est pas appropriée, le système fournit un signal vocal avec " déplacer vous en avant un peu " ou "déplacer vous en arrière un peu " pour guider la personne à ajuster sa place. Le système permet l'acquisition de trois images à un seul coup. Chacune des trois images emploie un des trois illuminateurs infrarouges (qui sont indiquées par les trois points rouges de la figure ci-dessous [37].

FIGURE III.3 – *Le système Iridien LG EOU 2200.*

La figure suivante présente d'autres appareils d'acquisition d'iris [**?**].

FIGURE III.4 – *Exemples des systèmes Iridien.*

Le Tableau suivant montre les caractéristiques des diapositives d'acquisition de l'iris

Dispositif d'acquisition	Procédé d'acquisition	Les caractéristiques	Taux de faux acquisition
LG IrisAccess 3000 EOU	dans des séquences séparés	capture intuitive	0.69%
OKI IrisPass-WG	dans des séquences séparées	Utilisation facile	0.32%
Panasonic BM-ET300	dans la même séquence	Utilisation difficile	0.42%
IG-H100	dans la même séquence	rapide et souple	0.06%

TABLE III.1 – Les caractéristiques des diapositives d'acquisition de l'iris

III.5 Les bases de données publiques

Il y a six bases de données de l'image de l'iris (yeux) disponibles au public pour les recherches biométrique par l'iris. les bases se sont : CASIA, MMU , BATH , UPOL ,UBIRISet ICE [31].

La base de données CASIA (Institute of Automation, Chinese Academy of Sciences) est plus utilisée. Cependant, ses images incorporent peu de types de bruit, presque exclusivement raconté avec paupière et obstruction des cils.

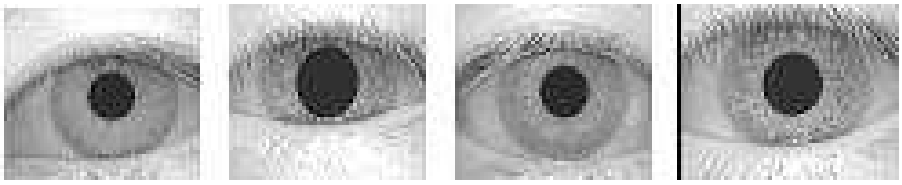


FIGURE III.5 – *Des exemples des images de la base de données d'iris CASIA.*

Les images des iris de la base de donnné MMU été développées par l'université Multimédia. Cette base contient 450 images capturées par l'appareil (LG IrisAccessR 2200). Elles sont fortement homogènes et leurs facteurs de bruit sont reliés à l'obstruction d'iris par des paupières et des cils [31].

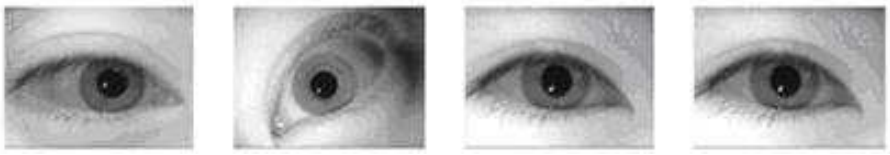


FIGURE III.6 – *Des exemples des images de la base de données d'iris MMU.*

L'université de Bath a développé un système de capture d'iris permettant d'acquérir des images de haute qualité. 2000 images d'iris de 50 personnes . Les européens et les asiatiques sont représentés dans cette base. Puisque la capture a été faite en mode très contrôlé, la qualité des images d'iris est très bonne et la résolution dépasse largement les résolutions des autres bases disponibles. Pour la base de donné UBATH, la résolution des images disponible est de 1280*960 [2].

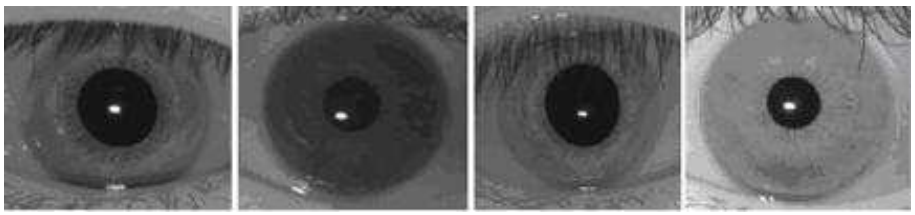


FIGURE III.7 – *Des exemples des images de la base de données d'iris BATH.*

UPOL est une base de données d'iris qui contient 384 images de 64 sujets européens. Les iris ont été acquis par le capteur TOPCON TRC50IA connecté à la caméra SONY DXC-950P 3CCD. La base est propre, la qualité des images est très bonne sans aucune occlusion des paupières et des cils. Les images sont acquises en couleur au format PNG

avec la résolution 768*576 [2].

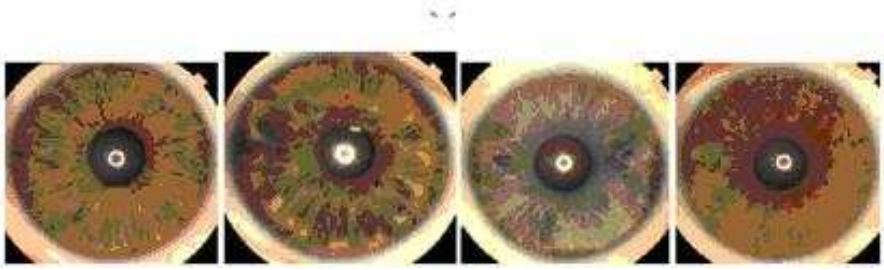


FIGURE III.8 – *Des exemples des images de la base de données d'iris UPOL.*

UBIRIS est une base de données qui a été pensée pour tester la robustesse des algorithmes de reconnaissance d'iris aux différents types de dégradations de qualité d'images d'iris. Dans ce but, plusieurs variations des conditions d'acquisition et diverses dégradations des images (illumination, contraste, réflexion, dé focus et occlusion) ont été introduite dans cette base de données. Elle contient 1877 images de résolution 400x300 de 241 personnes capturées en deux sessions. Puisque le mode d'acquisition choisi était la lumière visible, les images sont aussi disponibles en couleur sous deux résolutions possibles : 800x600 et 200x150. Le grand point faible de cette base de données est qu'elle a été acquise en lumière visible et ne peut donc être utilisée pour évaluer des systèmes développé sur des images en infrarouge [2].

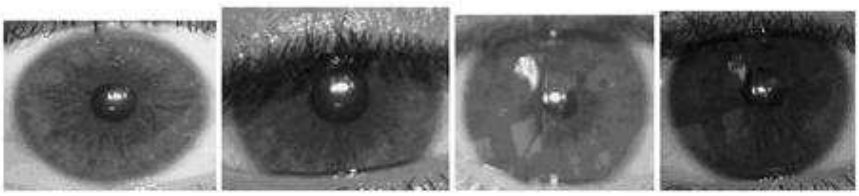


FIGURE III.9 – *Des exemples des images de la base de données d'iris UBIRIS.*

Le National Insitute of Standards and Technology (NIST) a mis à disposition des chercheurs sa base ICE 2005. La base contient 2953 images de 132 personnes acquises par la caméra dédiée LG2200. Dans la plupart des cas l'iris gauche et droit sont acquis en même temps. Cette base de données est une sous partie d'une base plus large de plus de 25094 images. La base contient plusieurs variations intra classe et différents types de dégradation. En effet les images peuvent être occultées par les paupières et les cils. Le niveau de flou et le niveau de flou de bougé sont largement supérieurs à ceux présents

dans les autres bases précédemment citées [37].

FIGURE III.10 – *Des exemples des images de la base de données d'iris ICE.*

III.6 Les travaux de reconnaissance par l'iris

III.6.1 Introduction

L'identification biométrie par l'iris a été proposée par Bertillon dès 1885 .il a utilisé la couleur de l'iris, pouvant être évaluée qualitativement par examen direct ou photographique et quantitativement par la colorimétrie [29]. Cependant cette identification chromatique n'est pas suffisante car il n'y a environ que cinquante couleurs d'iris discriminables, et elles changent avec l'âge, la pathologie irienne et sous l'effet de certains médicaments. Il est donc préférable d'utiliser pour l'identification la structure anatomique de l'iris. Selon l'idée proposée par Burch en 1936et Doggarts en 1949 [4]. L'application pratique fut réalisée par Flom et Safir en 1987 [4] puis elle a été développée par divers chercheurs comme Wildes et en 1994 [33], Boles en 1997 [7] et concrétisée par les travaux et les algorithmes de Daugman [15].

III.6.2 La technique de Daugman

Le travail le plus important dans l'histoire de la biométrie par l'iris est celle de Jean Daugman. Ce dernier a décrit un système opérationnel d'identification d'iris. L'approche de Daugman devient un modèle standard de référence pour développer des travaux dans la biométrie d'iris. En outre, presque tous les systèmes de la technologie biométrique par l'iris commerciaux existant sont basés sur de Daugman.
D'après Jean Daugman la clef de l'identification de l'iris est l'échec du test de l'indépendance statistique qui inclut beaucoup de degrés de liberté. Ce test est réussi quelque soit les " phase codes " pour deux yeux différents, mais il peut être seulement en échec quand la " phase code " de l'oeil est comparée avec une autre version de lui-même [33].

L'algorithme de Daugman [15][18][14][17]est l'algorithme d'identification de l'iris le plus connu. L'iris est modélisé en tant que deux cercles, qui ne sont pas nécessairement concentriques. Chaque cercle est défini par trois paramètres (r, x_0, y_0), où (x_0, y_0)) définit le centre d'un cercle de rayon r. dans cet algorithme, il emploie une opération intégrale/différentielle pour déterminer les valeurs des trois paramètres circulaires. Il recherche la valeur maximale du rayon r qui est donné par l'équation suivante :

$$max_{(r,x_0,y_0)}|G_\sigma(r) * \frac{\partial}{\partial r} \oint \frac{I(x,y)}{2\Pi r} ds| \tag{III.1}$$

Où I(x, y) est l'image de l'oeil, r le rayon du cercle que l'on est en train de chercher, $(2\Pi r)$ est employé pour normaliser l'intégrale, $G_\sigma(r)$ est une fonction gaussienne de lissage. $*$ signifie l'opération de convolution. L'opérateur effectue donc la différence entre la moyenne des gradients calculés sur deux cercles de rayons r et r+1. Le cercle qui maximise cette différence est le cercle recherché.
Les paupières sont modélisées par des arcs paraboliques. Un opérateur intégro-différentielle décrit dans l'équation 4 est également utilisé pour placer les paupières supérieures et inférieures. Dans ce cas l'intégrale est calculée au-dessus d'un arc parabolique au lieu d'un arc circulaire. Les régions détectées pour les paupières sont exclues de l'image de l'iris. L'image segmentée de l'iris est normalisée et convertit les coordonnées cartésiennes de l'image aux coordonnées polaires.
Un filtre 2D de Gabor est utilisé pour encoder l'image de l'iris à un code binaire de longueur 256 octets. Dans la partie sortante, la distance de Hamming est employée pour indiquer la similitude de deux codes d'iris. Plus la distance de Hamming est petite plus que le résultat est meilleur. Un seuil est utilisé pour déterminer si les codes de deux iris appartiennent à la même personne. Daugman a obtenu la valeur (FAR) égale à 1 dans 4 millions d'image avec un (FRR) égale à zéro.

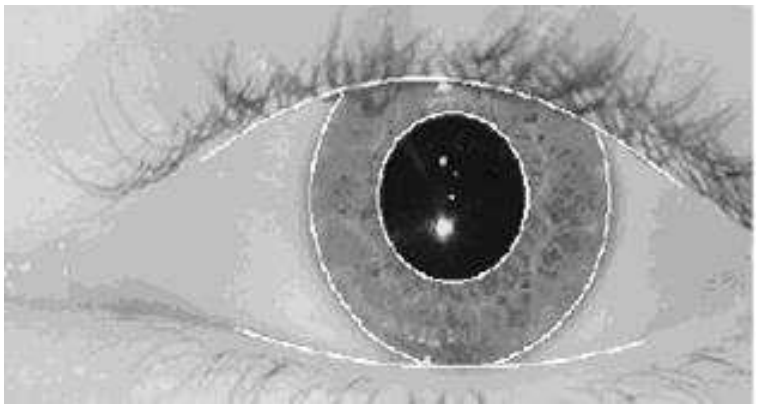


FIGURE III.11 – *Segmentation de l'iris par la méthode intégro-différentielle[18].*

FIGURE III.12 – *Une image d'iris normalisée [18].*

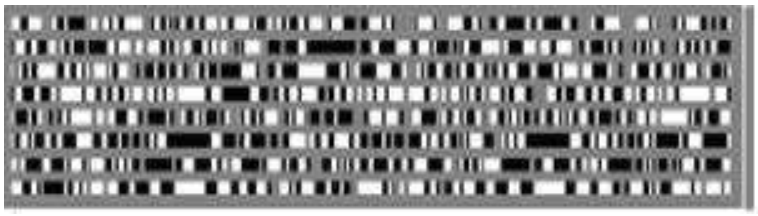


FIGURE III.13 – *L'iris code généré par la méthode Daugman [18].*

III.6.3 Le système de Wildes

Wildes décrit un système de biométrie d'iris développé aux laboratoires de Sarnoff qui emploie une technique différente de celle de Daugman.
Le système de Wilde [33] eest un système d'identification de l'iris. Il utilise la transformée de gradient de Hough pour détecter les deux bornes circulaires d'un iris. Il inclut deux étapes : d'abord il détecte un contour binaire en utilisant un filtre gaussien. Ensuite, il analyse l'espace circulaire de Hough pour estimer les trois paramètres d'un cercle (r, x_0, y_0). Un espace de Hough est défini par l'équation suivante :

$$H_{(x_c,y_c,r)} = \sum_{j=1} h_{(x_j,y_j,x_c,y_c,r)} \tag{III.2}$$

avec

$$h_{(x_j,y_j,x_c,y_c,r)} = \begin{cases} 1 & siC_{(x_j,y_j)} \in h_{(x_c,y_c,r)} \\ 0 & sinon \end{cases}$$

Avec (x_j, y_j) est un pixel du contour.

Les valeurs(x_c, y_c, r)sont les valeurs maximales dans $H_{(x_c,y_c,r)}$ et choisies en tant que vecteur de paramètre pour la borne circulaire. Dans le modèle de système de Wildes les paupières sont détectées en tant qu'arcs paraboliques. Les paupières supérieure et inférieure sont détectées en utilisant la transformé de Hough. Son principe est semblable à celui décrit ci-dessus. La seule différence est qu'elle vote pour les arcs paraboliques au lieu des cercles.
Le système de Wildes emploie la décomposition du pyramide de Laplace pour encoder la

texture de l'iris.
Il utilise la corrélation normalisée pour déterminer la similarité entre deux codes d'iris. La décision finale est obtenue d'un discriminant linéaire Fisher qui est basé sur la force de chaque bande de fréquence. Une exactitude de vérification de 100% a été réclamée en testant 600 images d'iris (60 iris différents)[11].

III.6.4 Le système Masek

Masek a étudié en 2003 l'application d'une ondelette Log-Gabor et a constaté qu'elle présentait de bonnes qualités d'analyse dans le cas de l'iris. Le système Masek est un système "Open -Source" de reconnaissance des personnes par l'iris [27].
Le système inclue un module de segmentation basé sur la transformée de Hough qui permet de localiser la pupille, l'iris, les paupières et les cils. Le système est composé aussi d'un module de normalisation basé sur la méthode de normalisation pseudo polaire. Un troisième module du système est celui de la reconnaissance où un filtrage 1D de Log-Gabor est effectué sur 4 niveaux pour coder la phase de Gabor selon le procédé de codage 4 quadrants. La distance de Hamming est finalement employée dans le dernier module pour la prise de décision. Le système Masek segmente l'image de l'iris de la manière suivante :
(i) L'étiquetage des points de contours se fait par l'utilisation de l'algorithme de détection de Canny. Les gradients verticaux seuls sont utilisés pour détecter la frontière Iris-blanc de l'oeil alors que les gradients verticaux et horizontaux sont équitablement pondérés pour détecter les points de frontières de la pupille.
(ii) La détection de la frontière extérieure de l'iris se fait avant celle de la frontière intérieure.
(iii) La détection des paupières est effectué en cherchant des droites sur les parties hautes et basses du disque de l'iris, détecté en utilisant la transformée de Hough. La paupière est modélisée par une droite horizontale obtenue à partir de la droite détectée par la transformée de Hough de la manière suivante : on recherche les points d'intersection du cercle de l'iris et de la droite puis on trace la droite horizontale qui passe par le point le plus bas (si nous voulons détecter la paupière du haut) ou le point le plus haut (si nous voulons détecter la paupière du bas).
(iv) Les cils et les reflets sont simplement détectés par seuillage de l'image sur les niveaux de gris, montre un iris segmenté par la procédure proposée par Masek.

(a) image originale,(b) iris détecté par la transformée de Hough,(c) modélisation des paupiéere par les deux droites horizantales (d) résultat finale de la détection de l'iris.
La figure suivante montre un iris normalisé par la procédure proposée par Masek.

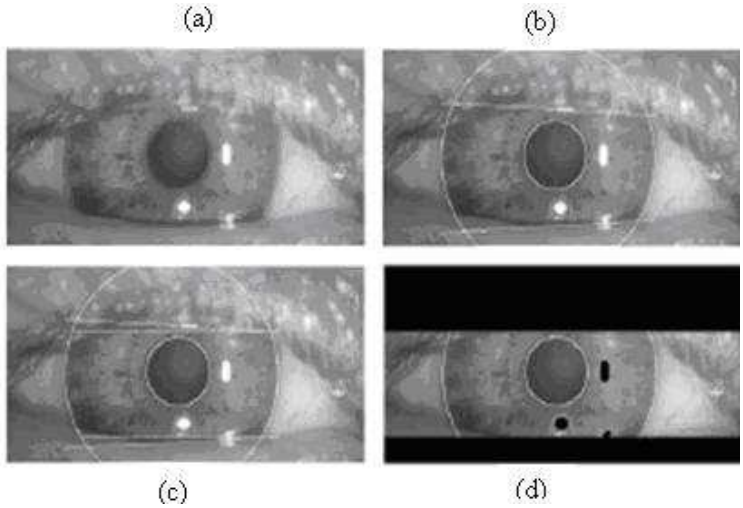


FIGURE III.14 – *Processus de segmentation de l'iris par la méthode proposée par Masek [27].*

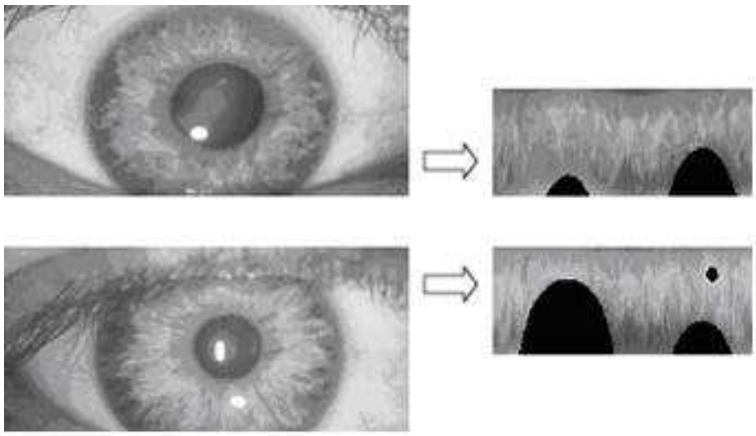


FIGURE III.15 – *L'illustration du procédé de normalisation pour deux images du même iris [27].*

III.6.5 Autres algorithmes

III.6.5.1 Algorithme de Bole et du Boashash

L'algorithme de Bole et du Boashash [7] extrait un ensemble de signaux unidimensionnels de l'image d'iris en utilisant les valeurs de l'intensité d'un ensemble de contours circulaires centrés dans le centre de la pupille, qui est localisé en utilisant des techniques de détection de bord. L'ensemble des signaux unidimensionnels est alors encodé en utilisant la transformation " zero crossing " dans différents niveaux de résolution. Pour calculer la dissimilitude globale entre deux codes d'iris, on utilise la moyenne de la dissimilitude à

chaque niveau de résolution. Une exactitude de vérification de 100%a été enregistrée avec 11 images d'iris.

III.6.5.2 Algorithme de Kong et Zhang

Kong et Zhang [33] ont proposé une segmentation de cil et de réflexion dans leur algorithme. Tout le système est développé en se basant sur l'algorithme de Boles et Boashash [24] avec l'ajout d'un modèle de segmentation de cil et de réflexion. La segmentation de l'iris est implantée en utilisant des approches d'ajustement de courbe. Des cils sont sous-classifiés en deux types. Les cils séparables et les cils multiples. Des cils séparables sont segmentés en utilisant un filtre de Gabor. Les cils multiples sont segmentés en vérifiant si la variance de l'intensité d'une espace donnée est plus petite qu'un seuil. Les réflexions peuvent être distinguées comme de forte réflexion et de faible réflexion. Les réflexions fortes sont détectées en plaçant un seuil pour la valeur de l'intensité, et les faibles réflexions sont détectées en utilisant un modèle statistique sur distribution d'intensité. Ils ont utilisé quatre types d'ondelettes 1-D (chapeau Mexican, les ondelettes de Haar, Shannon, et Gabor) pour extraire les caractéristiques de l'iris. La dissimilitude entre un pair de codes d'iris est mesuré par la norme L1 définie par :

$$d(X,Y) \quad = \quad \sum_{k=1}^{n} |X_k - Y_k| \tag{III.3}$$

X et Y sont deux pixels des codes d'iris et n est la taille du code. Kong et Zhang ont réclamé un taux d'erreur égale (EER) de 11%, qui a été réduit à 3% en utilisant leur modèle de segmentation de cil et de réflexion. L'ensemble de données de test se compose de 238 images d'iris (48 iris).

III.6.5.3 Algorithme de L.Ma

Dans l'algorithme proposé par Ma [26], les images d'iris sont projetées dans les directions verticales et horizontales pour estimer le centre de la pupille. Ceci ce qui permet de réduire le temps pour rechercher les bornes d'iris. Après la normalisation de l'iris localisé, le contraste d'image est mis en valeur en faisant la soustraction de l'illumination estimée. En faisant extraire l'iris, un filtre modulé par une fonction sinusoïdale symétrique circulaire est utilisé. Au lieu d'utiliser la totalité de l'image d'iris, on utilise la région d'intérêt contrainte qui est dans l'espace tout proche de la pupille car dans cet espace la texture de la pupillaire est plus abondante. En utilisant ceci, on évite le bruit de paupière et de cil. La représentation de l'iris est un vecteur caractéristique de longueur 1.536 bits. Un

discriminant linéaire de Fisher est employé pour réduire la dimension du vecteur caractéristique. L'algorithme a été testé sur l'ensemble de données de la version 1 de CASIA. Le rapport d'identification est 99.43%, le FAR est 0.001% tandis que le FRR est 1.29%. Dans l'étape de classification un réseau neurologique de propagation (NN : Neuron Nets) est utilisé. Dans l'étape de segmentation, la région de pupille est d'abord détectée avec une méthode linéaire de seuil, ensuite on utilise la chaîne de code Freeman [16]. Puis un filtre de contraste est appliqué à l'image pour mettre en valeur la différence d'intensité dans l'image d'iris. La borne d'iris est décidée en contrôlant les valeurs d'intensité d'une ligne horizontale passant par le centre de pupille détecté. L'étape de la segmentation de cette approche n'a pas eu beaucoup de succès. L'exactitude de la segmentation est 78.6Dans le NN, il y a trois couches : une couche d'entrée, une couche cachée et une couche de sortie. La couche d'entrée correspond au vecteur caractéristique de l'iris. Le nombre d'unités d'entrée est égal à la longueur du vecteur caractéristique de l'iris. Le nombre d'unités de sortie est égal au nombre de sujets impliqués dans les expérimentations. Le nombre de noeuds cachés est égal à la moitié du nombre de noeuds d'entrée. Pour réduire la complexité de calcul, ils ont employé une décomposition singulière de valeur (SVD) et le composant indépendant d'nalyse (ICA) pour réduire la longueur des vecteurs d'iris, et par suite réduire le nombre d'unités d'entrée du NN. Les résultats expérimentaux montrent que l'utilisation d'ICA fonctionne mieux en utilisant le SVD. Le taux d'identification dans l'ensemble de données de CASIA est 92.1% quand on utilise ICA pour diminuer la longueur de vecteur d'entrée à 50

III.6.5.4 Algorithme de Chin

Chin et al [8] a proposé l'utilisation d'un " S-iris encodant " qui est généré du produit intérieur de la sortie d'un filtre 1D log Gabor et des nombres pseudo-aléatoires secrets. Dans la phase de segmentation : un contour de l'image est généré en utilisant un détecteur de contour de Canny. Un transformé de Hough circulaire est utilisée pour obtenir les bornes de l'iris. La transformé de Hough linéaire est utilisé en excluant les bruits de paupière et de l'oeil. Ensuite la partie de l'iris isolée est normalisé dans un rectangle avec une résolution de 20x240 pixels en utilisant le modèle rubber sheet de Daugman[15]. Puis le code de l'iris final est généré du produit intérieur de la sortie d'un filtre 1D log de Gabor et les nombres pseudo aléatoires secrets. Dans la phase de comparaison, on utilise la distance de Hamming pour indiquer la dissimilitude entre une paire de codes d'iris[12]. Une vérification exacte de 100% est reportée en testant dans l'ensemble de données d'image d'iris CASIA version 1.0. la figure suivant montre les phases de l'algorithme de Chin .

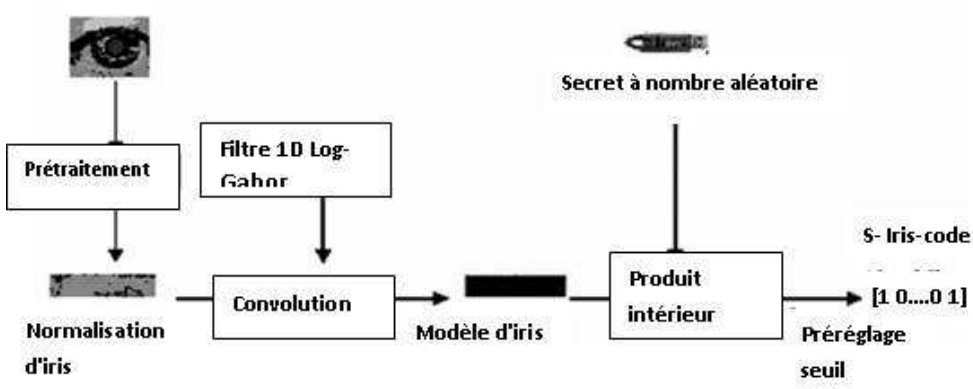


FIGURE III.16 – *Traitement de S- Iris-codage*

III.6.5.5 Algorithme Fancourt

Fancourt[9]a étudié le problème de l'identification d'iris en utilisant les images acquises à une distance plus que 10 mètres. Les images ont été capturées à l'aide d'un télescope. Les images ont une résolution de 640x480. Ils utilisent L'algorithme de segmentation automatique [11]. Ils ont aussi employé une segmentation manuelle " bootstrap" à la segmentation automatique. La similitude entre l'image de test et l'image de référence est mesurée par le coefficient de corrélation moyenne à travers les sous-blocs avec une taille de 12x12 Pixel. Ils ont testé l'algorithme sur deux bases de données d'iris avec aucuns sujets communs. Il y a 50 sujets (50 iris) dans la base de données I, et 200 sujets (247 iris) dans la base de données II.

III.7 Conclusion

Dans ce chapitre nous avons introduit les propriétés importantes de l'iris à prendre en compte lors de la conception d'un système d'identification par l'iris. Les exigences de performances sont au terme de flexibilité, de coût, de fiabilité et de temps d'exécution. Nous avons étudié plus en détail les algorithmes de l'identification par l'iris. En mettant l'accent sur les travaux de Daugman, ainsi que la technique de Wilde et d'autres approches d'identification par l'iris. Nous avons constaté que l'approche de Wilde pour la localisation de l'iris utilise un algorithme simple et facile à mettre en ouvre . L'approche retenue consiste à utiliser la transformée de Hough pour la localisation le filtre de Gabor et la transformée de Haar pour extraction le codes de l'iris et la distance de Hamming pour la comparaison et prendre la décision d'acceptation ou de rejet. Le développement de cette approche faire l'objet du chapitre suivant.

Chapitre IV

IMPLEMENTATION DE l'AUTHENTIFICATION BIOMETRIQUE PAR L'IRIS

IV.1 Introduction

La reconnaissance biométrique par l'iris est l'un des moyens les plus performants pour identifier une personne. En effet, des études biologiques ont montré que les profils et les courbes présents dans un iris garantissent son unicité. Ce travail consisté donc à développer un système complet et fiable de reconnaissance s'appuyant sur cette propriété, depuis l'acquisition de l'image, jusqu'à la recherche dans une base de données existante en passant par la codification. Le premier objectif est d'élaborer un système de reconnaissance biométrique par l'iris qui fonctionne sur une base de données existante (CASIA) et ne présentant pas ou peu de défauts (images infrarouges, pas de reflets sur l'image, etc.). Ensuite, nous allons mesurer les performances de l'algorithme en termes de taux d'erreur. Nous finirons par des interprétations des résultats trouvés.

IV.2 Système d'authentification basée sur la biométrie : l'iris

Un système complet d'identification d'iris peut être composé de quatre étapes : acquisition de données, segmentation, codage et comparaison.

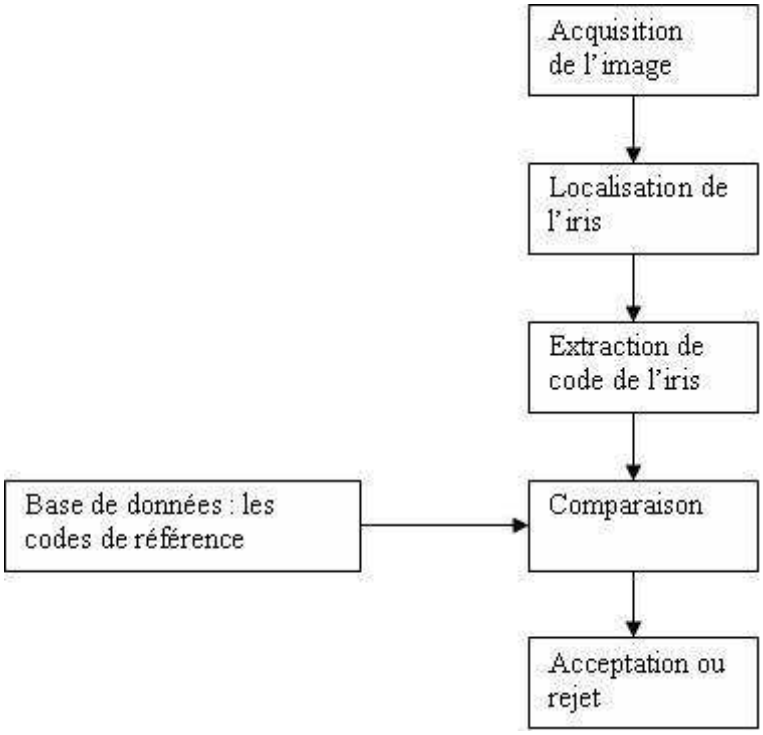


FIGURE IV.1 – *Étapes générales du système d'identification d'iris*

IV.2.1 Base d'image de test : CASIA

Dans notre travail, nous allons utiliser la base de données d'images de l'iris CASIA version 1.0[22] cette base contient un nombre total de 756 iris (yeux) de 108 sujets (7 images différentes pour chaque sujet). Les images de chaque classe sont prises à partir de deux sessions (un mois d'intervalle entre les deux sessions). Chaque image de l'iris est à niveau de gris, codée sur 8 bits avec une résolution de 320x280.

Cette base a été utilisée par les travaux de recherches sur la reconnaissance de l'iris développé par le Laboratoire national de la reconnaissance des formes de la Chine. Dans chaque image, la région de pupille a été modifiée manuellement de sorte qu'elle contienne une région circulaire d'un constant niveau d'intensité. Les iris deviennent donc très visibles et ils sont de bon contraste.
Les images ont été capturées par la caméra de la figure suivante :

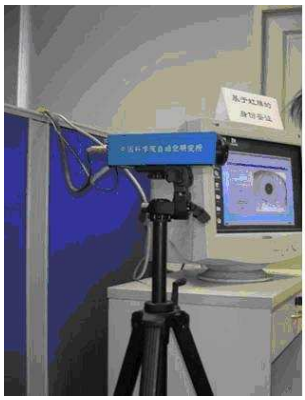


FIGURE IV.2 – *Appareil-photo d'iris développé à CASIA*

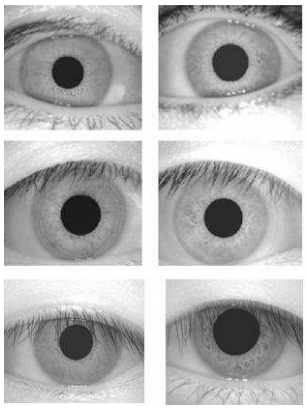


FIGURE IV.3 – *Des images de l'iris de CASIA*

IV.2.2 Localisation de l'iris

La première étape du procédé de traitement de l'image d'un oeil est de localiser la pupille et l'iris. On doit suivre les étapes de prétraitement suivantes : filtrage, détection de contour, transformée de Hough.

IV.2.2.1 Filtrage

Pour diminuer l'effet du bruit qui présent dans les images de l'iris, nous avons utilisé un filtre médian. Pour éliminer les cils nous avons utilisé le même filtre tout en augmentant la fenêtre de filtrage pour rendre l'image un peu floue ce qui permettre d'écraser la couleur noir des cils et il ne retenir que la couleur noir correspondant uniquement à la pupille. La figure suivante montre une image d'oeil originale et l'image après le filtrage :

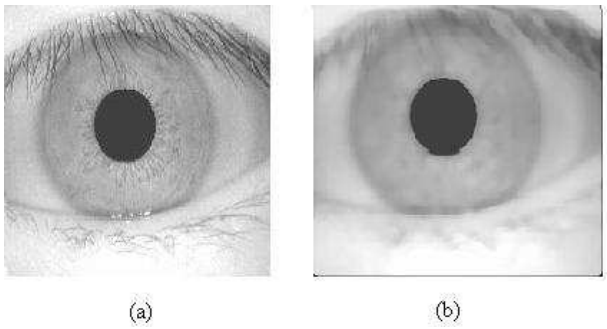


FIGURE IV.4 – *Filtrage de l'image :(a) Image originale (b) Image filtrée*

IV.2.2.2 Détection du Contour

La détection du contour permet d'obtenir une information primordiale sur l'image analysée. Les contours vont permettre de caractériser les formes qui se trouvent dans l'image. Dans une image, un contour peut être vu comme une variation locale de l'intensité des niveaux de gris. plusieurs méthodes de détection de contour peut être utilisé, dans notre travail nous avons utilisé le filtre de Canny pour la première partie et le détecteur de Sobel pour la deuxième partie. Les figures suivantes montrent le contour de Canny d'une image d'oeil.

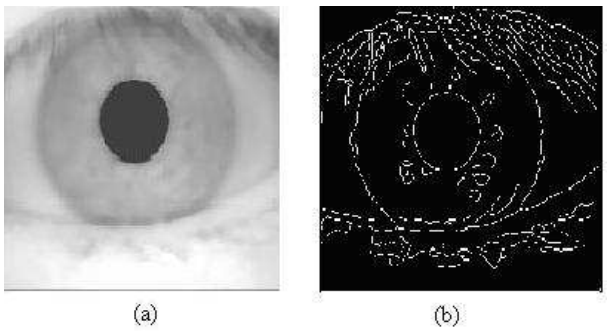


FIGURE IV.5 – *Détection de contour de l'image :(a) Image original (filtrée)(b)contour de Canny*

Le filtre de Canny nous permet d'obtenir une image dont les contours sont en blanc sur un fond noir.

IV.2.2.3 La transformée de Hough

La transformée de Hough permet la détection des droites, des cercles ou des ellipses dans une image. Le principe général de la transformée de Hough est d'établir une projection entre l'espace de l'image et un espace de paramètres représentatifs de la forme recherchée.
Dans ce travail nous nous intéressons à la détection du cercle. Le principe de base de la détection des cercles est très simple : on dessine les contours de l'image et pour tous les points appartenant aux contours, on dessine dans l'accumulateur un cercle de rayon R. Si l'on cherche à détecter un cercle de rayon R, le point de l'accumulateur ayant reçu le plus de suffrage sera le centre du cercle recherché .
Avantages de cette méthode : nous pouvons détecter un cercle même s'il est partiellement caché ou même si l'image est très bruitée si l'on connaît le rayon du cercle recherché, d'où la rapidité et la robustesse de cette méthode.
Inconvénients de cette méthode : ce traitement nécessite de connaître approximativement le rayon du cercle recherché.
Tout d'abord, il faut générer l'image des contours à partir de l'image d'iris originale ; pour cela, on emploie un algorithme classique en traitement d'images ("détection des contours de Canny"), qui représente les bords des formes géométriques présentes dans l'image à partir des dérivées des valeurs d'intensité.
Une fois l'image des contours est générée, la transformée de Hough prend chacun des points représentés et dessine un cercle ayant ce point comme centre avec un rayon passé en argument. Tous les cercles tracés sont comptabilisés dans "l'espace de Hough", de telle façon que le point dans l'espace où se croisent le plus grand nombre de cercles est choisi comme étant le centre du cercle à rayon donné recherché. Donc le traitement consiste à la découverte de la méthode de détection des cercles on sélectionne un intervalle de rayon possible et le programme trouve le cercle le plus adapté.Cependant, nous sommes partis d'estimations disponibles pour la base de données CASIA version 1.0, qui indique que les valeurs de rayons de pupille et de l'iris à utiliser se trouvent dans l'intervalle de 28 à 75 pixels et dans l'intervalle de 80 à 150 respectivement.

Au cours de processus de localisation de l'iris nous cherchons le paupière inférieur ,le paupière supérieur, la pupille et enfin nous détectons iris.

Le diagramme suivant illustre les principales étapes localisation de l'iris.

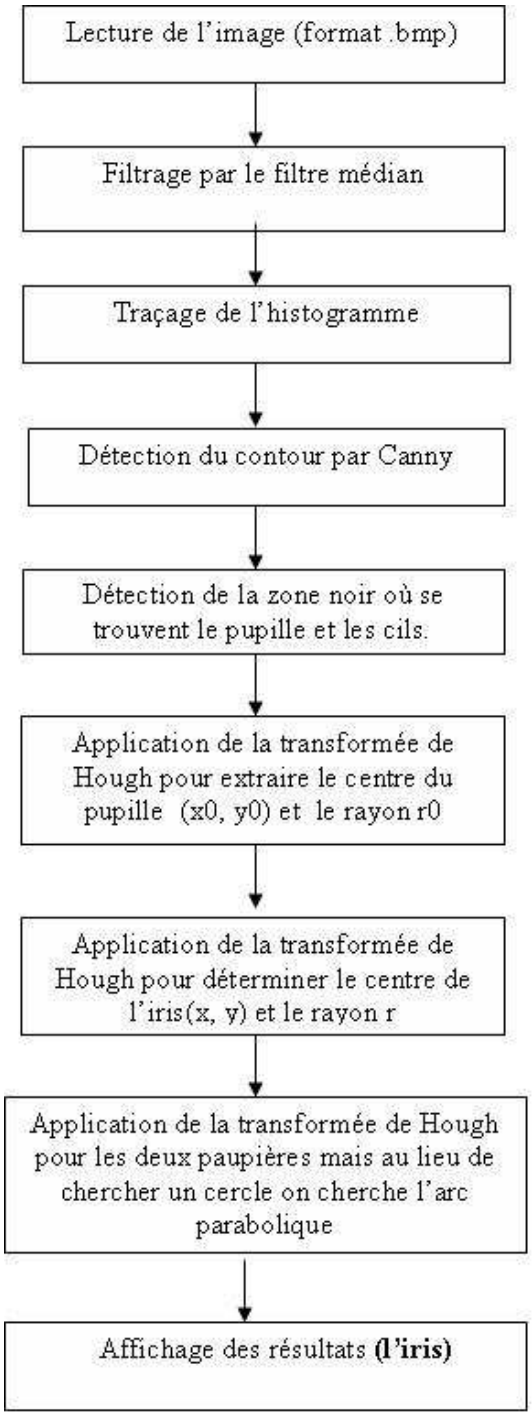


FIGURE IV.6 – *Le diagramme des étapes de localisation de l'iris*

La figure suivante montrent des exemples d'extraction de l'iris.

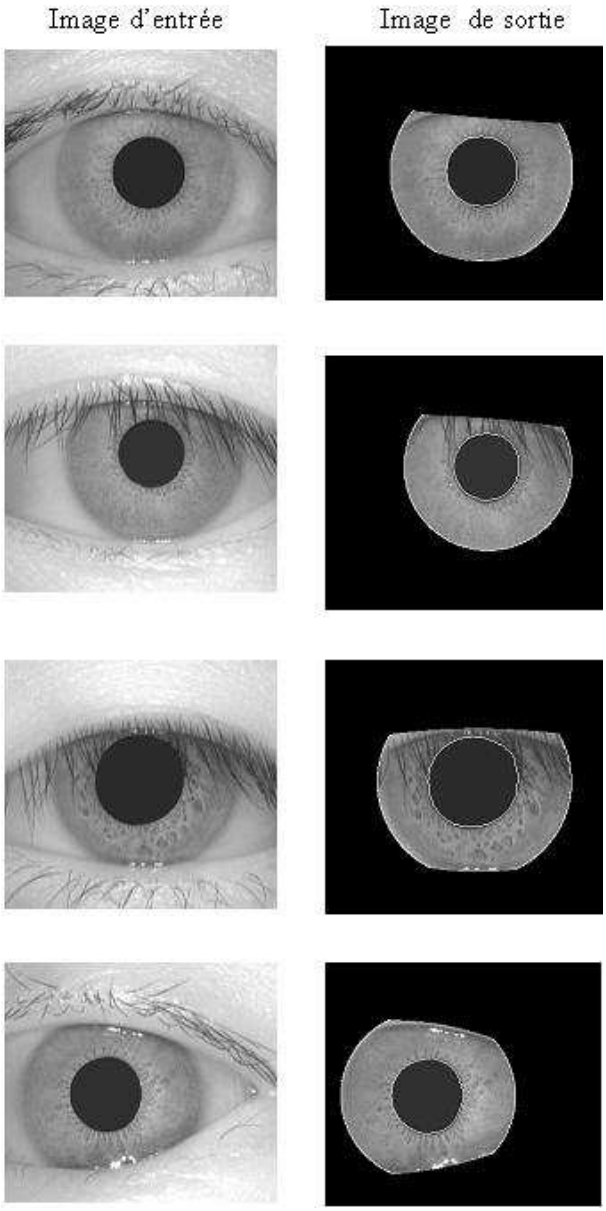


FIGURE IV.7 – *Des exemples de location des images de l'iris de CASIA*

IV.2.3 Extraction de signature de l'iris

IV.2.3.1 Normalisation

La taille de la pupille peut changer selon la variation de l'illumination. Cette déformation de l'iris peut causer l'interférence avec les résultats de l'assortiment du modèle. Pour réduire cette interférence, l'iris détecté devrait être tracé dans un bloc rectangulaire de texture de taille fixe. On fait une On réalise une transformation pseudo polaire ; c.-à-d une transformation l'image de l'iris I(x,y)) en coordonnés polaires I(ρ,θ). En utilisant les

équations suivantes :

$$\theta \in [0\ 2\pi]\rho \in [0\ 1]I(x(\rho,\theta),y(\rho,\theta)) \rightarrow I(\rho,\theta) \tag{IV.1}$$

$$x(\rho,\theta) = (1-\rho)x_p + \rho x_p(\theta) \tag{IV.2}$$

$$y(\rho,\theta) = (1-\rho)y_p + \rho y_p(\theta) \tag{IV.3}$$

$$x_p(\theta) = x_{p0}(\theta) - r_p\cos(\theta) \tag{IV.4}$$

$$y_p(\theta) = y_{p0}(\theta) - r_p\sin(\theta) \tag{IV.5}$$

$$x_i(\theta) = x_{i0}(\theta) - r_i\cos(\theta) \tag{IV.6}$$

$$y_i(\theta) = y_{i0}(\theta) - r_i\sin(\theta) \tag{IV.7}$$

où rp et ri sont respectivement le rayon de la pupille et l'iris, ($x_p(\theta)$, $y_p(\theta)$) et ($x_i(\theta)$, $x_i(\theta)$) sont les coordonnées de la pupille et de l'iris et de direction theta. La valeur detheta appartient à [0 2π],ρ appartient à [0 1] . Le résultat de la normalisation des images est montré dans la figure suivante :

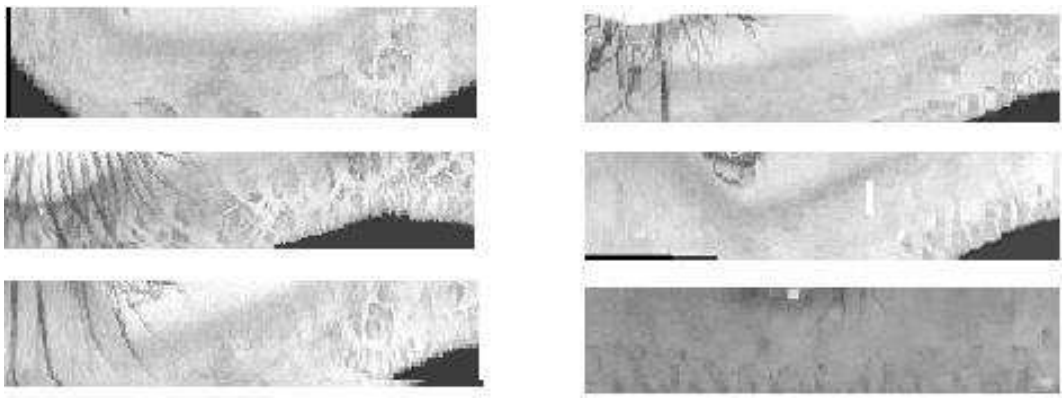


FIGURE IV.8 – *Des exemples de normalisation des images de l'iris de CASIA*

IV.2.3.2 Codage

Il nous reste maintenant à extraire de l'image les informations qui nous intéressent et vont nous permettre de caractériser un iris. L'ensemble de ces informations est appelé code de l'iris. Le calcul de ce code de l'iris s'effectue par l'intermédiaire des ondelettes de Gabor .

Les ondelettes de Gabor sont un type de fonctions, qui de la même façon que la transformée de Fourier ou la DCT, permettent une représentation fréquentielles d'un signal, ou, dans le cas présent, d'une image. Les ondelettes de Gabor sont un type d'ondelettes particulier qui sont en fait formées de fonction gaussiennes modulées par des sinusoïdes

complexes. La formule 2D d'ondelettes de Gabor est donnée par l'équation suivante :

$$H = \int_{\rho}\int_{\phi} \exp^{-iw(\theta_0-\phi)} \exp^{-} \frac{(r_0-\rho)^2}{\alpha^2} exp^{-} \frac{(\theta_0-\phi)^2}{\beta^2} I(\rho\phi)\rho d\rho d\phi \qquad \text{(IV.8)}$$

On effectue donc la transformée en ondelettes de l'image grâce à la formule ci-dessous, que l'on applique localement sur l'image :

$$h_{\{Re,im\}} = sgn_{\{Re,im\}} \int_{\rho}\int_{\phi} \exp^{-iw(\theta_0-\phi)} \exp^{-} \frac{(r_0-\rho)^2}{\alpha^2} exp^{-} \frac{(\theta_0-\phi)^2}{\beta^2} I(\rho\phi)\rho d\rho d\phi \qquad \text{(IV.9)}$$

Où sgn est : 1 si l'élément correspondant de H est plus grand que zéro, 0 si l'élément correspondant de H est égal à zéro et -1 si l'élément correspondant de H est moins que zéro.
Cette formule nous permet d'extraire des informations sur la phase, et plus précisément de savoir dans quel quadrant du plan complexe se situe la phase de la zone considérée. L'opération est répétée localement sur toute la surface de l'iris afin d'extraire 2048 bits d'information (cette valeur de 2048 bits fut choisie à l'origine en se basant sur la quantité d'information enregistrable sur une bande magnétique de carte de type carte bancaire ou carte de téléphone).

IV.2.4 Comparaison

L'authentification par l'iris est réalisée par comparaison précise entre une image de test, celle de l'individu à authentifier et toutes les images d'une base de données préétablie : celles avec lesquelles l'individu testé doit être rapproché. La décision authentification se tournera vers l'image de la base de données reconnue comme étant la plus proche en termes d'information de l'image de test. On applique la distance de Hamming pour comparer deux signatures de l'iris. La distance de Hamming donne le nombre de bits qui sont identiques entre deux séquences de bits. En utilisant la distance de Hamming entre deux séquences de bits, on peut décider si les deux modèles ont été générés à partir de la même lentille ou à partir de lentilles différentes.
La distance de Hamming HD entre deux séquences binaires X et Y est définie comme la somme de désaccord bits (somme des OU-exclusif entre X et Y) par rapport à N (nombre total de bits dans le modèle) ; l'expression de cette distance est donnée par l'équation suivante :

$$HD = \frac{1}{n}\sum_{j=1}^{n} X_j \bigoplus Y_j \qquad \text{(IV.10)}$$

Avec N=2048, X_j et Y_j sont deux codes de d'iris.
Chaque région de l'iris produit un modèle binaire qui est indépendant de celui produit par une autre lecture de l'iris ; d'autre part, deux codes d'iris produits par le même individu sont fortement corrélés.

IV.3 Mesure de performance de l'algorithme :Taux d'erreur

Lorsqu'on souhaite évaluer les caractéristiques d'un système biométrique de nombreux critères peuvent êtres pris en compte. Dans l'idéal, on désire un algorithme proposant un taux d'acceptation fausse (FAR) nul, avec un taux de faux Rejet (FRR) est nul, et avec un taux de reconnaissance de 100%.Nous rappelons que le FAR est le taux auquel un imposteur est inexactement accepté en tant que authentifié et FRR est évalué tel qu'un authentifié est rejeté.John Daugman, a effectué des essais sur un nombre très grand de modèles d'iris (jusqu'à 3 millions d'images d'iris) et il a déduit que la distance maximale de Hamming qui existe entre deux iris appartenant à la même personne est 0.32[15]. Dans notre travail, nous avons adopté cette constations et notre décision est la suivante :

- Si le HD <= 0.32 alors c'est la même personne.
- Si HD > 0.32 alors c'est une personne différente.

La courbe suivante représente les taux de faux d'acceptation et le taux de faux rejet en fonction du nombre de gabarits.

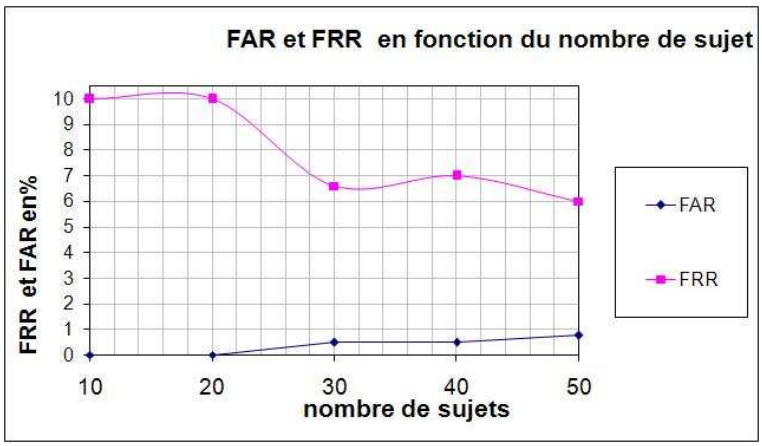


FIGURE IV.9 – *Courbe de FAR et FRR en fonction de nombre de sujets*

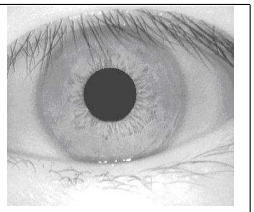
D'après la courbe ci-dessus nous remarquons si le nombre de gabarits augmente le FAR augmente, par contre FRR diminue car dans ces types des systèmes il est impossible de faire diminuer les deux types d'erreurs en même temps. C'est l'une des raisons qui a motive l'introduction de la multimodalité puisqu'il est possible de diminuer les deux types d'erreur à la fois. Ces erreurs peuvent être expliquées par :un mauvais éclairage, l'occlusion par les paupières, les bruits ou le positionnement inadéquat d'oeil. la première phase de la détection de l'iris donnent différents forme de l'iris. Ensuite nous faisons le codage de l'iris, la mauvaise localisation de l'iris entraine des erreurs sur les codes.Il serait donc intéressant de remédier à cette limite en affinant les traitements de la première phase afin d'augmenter leurs précisions

IV.4 Développement d'un algorithme d'authentification par l'iris

Dans la deuxième partie nous avons utilisé l'outil Microsoft Visual C++ pour développer des algorithmes pour la localisation de l'iris basé sur la transformée de Hough. Ensuite nous développons un algorithme basé sur la transformée des ondelettes de Haar et nous finissons par une comparaison entre deux codes d'iris en utilisant la distance Hamming.

IV.4.1 Localisation de l'iris

Le tableau ci-dessous montre les étapes de localisation de la pupille puis de l'iris ainsi que le résultat de chaque étape.

Chargement de l'image	
Filtrage par le filtre de Sobel	

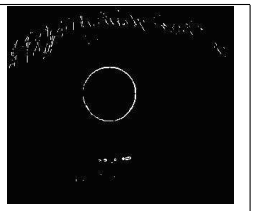
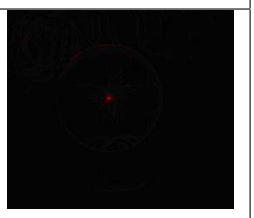
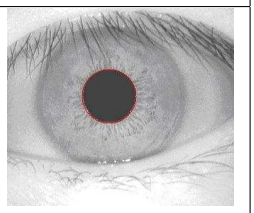
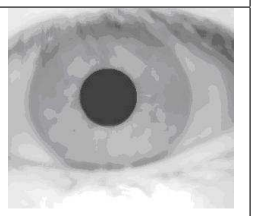
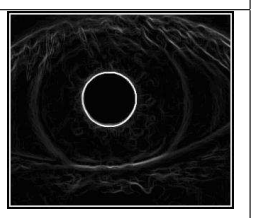
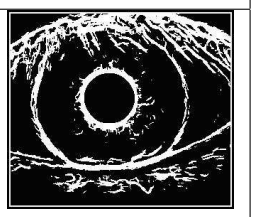
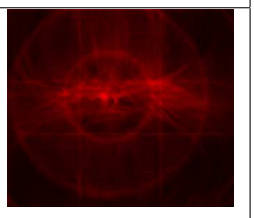
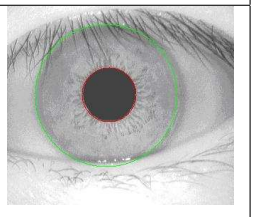
Seuillage	
extraire le centre et de le rayon la pupille	
Dessin du cercle trouvé (pupille)	
Filtrage par le filtre Median	
Filtrage par le filtre de Sobel	
seuillage	
pour déterminer le centre et le rayon de l'iris	
Dessin du cercle trouvé (l'iris)	

TABLE IV.1 – Les étapes et les résultats de localisation de la pupille puis de l'iris

Extraction de l'iris elle se fait selon les étapes :
la soustraction des pixels appartient à la zone noire (les pupilles et les cils).
stockage des pixels dans une autre matrice (mat-out1).
stockage dans autre matrice (mat-out) des pixels qui se trouvent à l'intérieur du cercle de coordonnées (x0, y0) et de rayon r obtenus à partir des résultats de la transformée de Hough.
Reconstruction e l'image de sortie (l'iris uniquement).

le résultats de l'Extraction de l'iris est la suivante

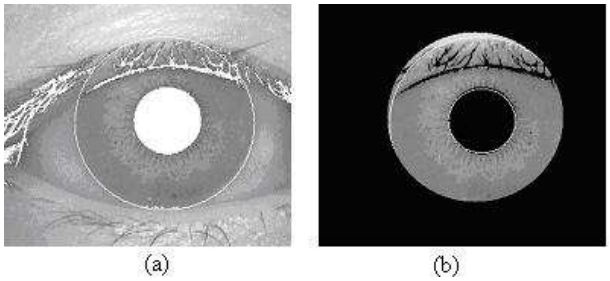


FIGURE IV.10 – *Résultats de localisation(a)Détection de pupille (b)Détection de l'iris*

IV.4.2 Extraction du vecteur caractéristique

IV.4.2.1 Les ondelettes de HAAR

Cette étape est responsable d'extraire les modèles de l'iris en tenant compte de la corrélation entre les pixels adjacents. Nous avons employée les ondelettes de Haar. L'ondelette de HAAR est illustrée dans la figure suivante : Les ondelettes est une famille d'outils

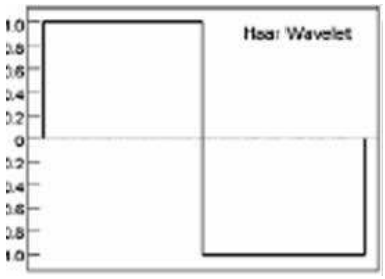


FIGURE IV.11 – *Les ondelettes de HAAR*

d'analyse qui permettent de décomposer l'image en quatre sous-images représentant les basses fréquences et les hautes fréquences dans les directions horizontales, verticales et

diagonales. Cette décomposition est généralement représentée comme présenté dans la figure suivante :

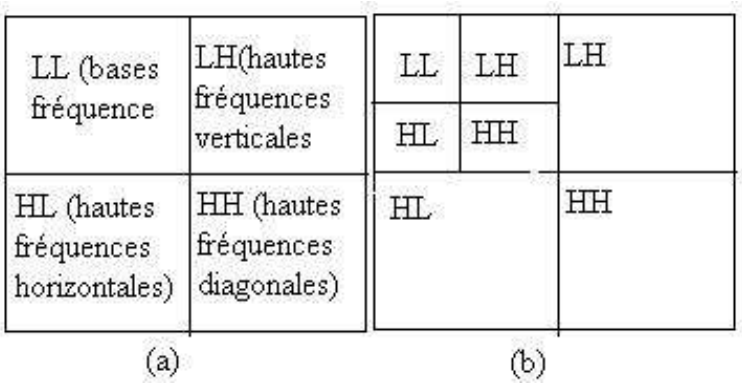


FIGURE IV.12 – *La transformé de Haar : (a)une seule itération (b) deux itérations*

IV.4.2.2 Code binaire

III est très important de représenter le vecteur obtenu dans un code binaire parce qu'il est plus facile de trouver la différence entre deux codes binaires qu'entre deux vecteurs de nombre. En fait, les vecteurs booléens sont toujours plus faciles à comparer et manipuler. Puisque chaque coefficient a une valeur réelle allant de -1,0 à +1,0, le vecteur caractéristique est quantifié de manière à ce que toute valeur positive est représentée par 1, et toute valeur négative est représentée par 0. Il en résulte un modèle biométrique compact. En d'autres termes, si on considère " Coef " le coefficient du vecteur caractéristique d'une image, la quantification convertit le vecteur caractéristique en code binaire selon les équations suivantes :

- Si Coef(i) >= 0 alors Coef(i)= 1.
- Si Coef(i)< 0 alors Coef(i)= 0.

IV.4.3 Prise de décision

L'étape finale dans l'authentification est la comparaison des codes d'iris. La comparaison est basée sur la distance de Hamming entre le vecteur de dispositif d'entrée et les vecteurs de caractéristique dans la base de données. Le choix d'un seuil adéquat permettre de décider si la personne est un authentifié ou un imposteur.

IV.4.4 Mesure de taux erreur

Pour le choix du seuil nous donnons la courbe de FAR et FRR en fonction de distance de Hamming :

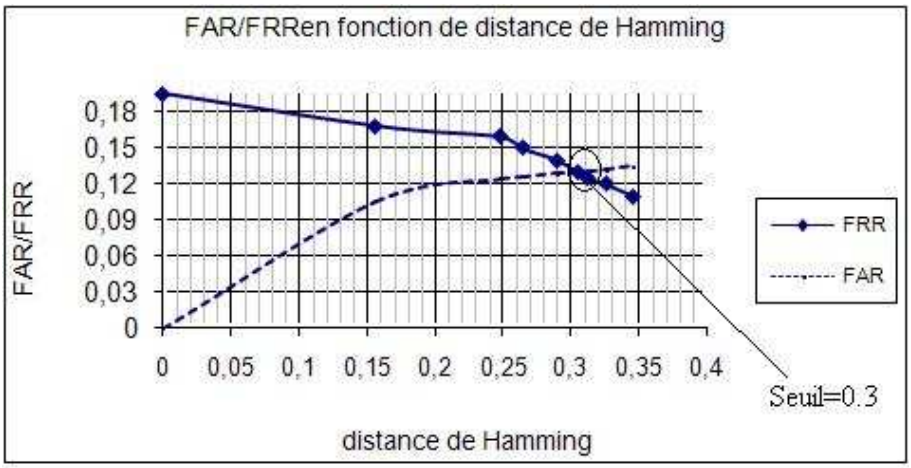


FIGURE IV.13 – *La courbe de FAR /FRR en fonction de distance de Hamming*

Le point d'intersection des deux courbes présente le seuil choisi dans notre cas le seuil est de 0.3 Plus le seuil de décision est bas, plus le système acceptera d'utilisateurs légitimes mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision est élevé, plus le système rejettera d'imposteurs mais plus il rejettera aussi d'utilisateurs légitimes. Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps.
C'est l'une des raisons qui a motive l'introduction de la multimodalité dans laquelle il est possible de diminuer les deux types d'erreur à la fois.

La décision si ces deux images appartiennent à la même personne ou non dépend du résultat suivant :

- Si le HD <= 0.3 alors c'est la même personne.
- Si HD > 0.3 alors c'est une personne différente.

IV.5 Comparaison entre les deux algorithmes

Dans le tableau suivant nous montrons une comparaison entre les ondelettes de Haar et les ondelettes de Gabor.

	Les ondelettes Haar		Les ondelettes Gabor	
Nombre de sujet	FRR((%))	FAR((%))	FRR((%))	FAR((%))
10	14. 5	18.5	0	10
15	13.00	16.00	0	10
20	10.50	15.5	0	10
25	7.5	12.6	0.14	7
30	7	8	0.14	6.6

TABLE IV.2 – Mesure de FAR et FRR pour les deux approches proposées

Le tableau ci-desssus présente les valeurs mesurées pour le FAR et FRR. On constate que dans l'approche basée sur les ondelettes de Haar les valeurs de FAR n'évoluent pas de la même façon que le FRR, bien que ces deux derniers aient des valeurs supérieures à ceux mesurées pour la première approche. Ceci nous amène à déduire que les ondelettes de Gabor sont plus efficaces que celle de Haar . Pour mesurer le taux de reconnaissance nous utilisons l'équation suivante.

$$Tauxdereconnaissance \quad = \quad 100 - \frac{FRR + FAR}{2} \tag{IV.11}$$

Dans le tableau suivant nous calculons le taux de fiabilité de nos algorithmes.
le tableau montre que les ondelettes de Gabor sont plus fiables que les ondelettes de Haar.

	Taux de reconnaissance(%)
Les ondeletes de Gabor	95,64
Les ondelettes de Haar	87.57

TABLE IV.3 – Mesure le taux de reconnaissance pour les deux approches proposées

Dans ce travail, nous avons traité l'authentification biométrique par l'iris : Nous avons employé, deux méthodes. Transformations des ondelettes de Gabor et Transformations des ondelettes de Haar pour extraire le vecteur caractéristiques iris. Nous avons trouvé que le transformé des ondelettes de Gabor donne meilleure exécution à celle de Haar. En second lieu, la transformation par ondelettes de Haar a été employée pour optimiser la dimension des vecteurs de dispositif afin de réduire la durée de la transformation. Les résultats de l'expérimentions, nous sommes convaincus que le système proposé dans le premiers partie est plus performant en terme de fiabilité.

IV.6 Conclusion

Dans ce chapitre, nous avons présenté deux méthodes de reconnaissance par l'iris. La premiere utilise la transformée de Hough dans la phase de segmentation, la transformé des ondelettes de Gabor dans la phase d'extraction de gabarit et la distance de Hamming dans la phase de prendre de décision. La deuxième méthode, consiste à modifier la phase d'extraction de gabarit et utiliser le transformé des ondelettes de Haar. Nous avons présenté une mesure de la performance des deux approches tout en calculant le taux de fausse acceptation et de faux rejet nous avons conclue que la première est plus performante en terme de fiabilité dont le taux d'erreur inferieur a la deuxième méthode. Mais celle-ci présente un vecteur caractéristique dont le nombre de bit est inferieur à la premier ce qui nous permet de gagner en terme d'espace mémoire de stockage et vitesse d'exécution .Pour conclure on peut dire que la détection et la reconnaissance biométrique d'individus demeurent des problèmes complexes, malgré les recherches actives actuelles. Il y a de nombreuses conditions réelles difficiles à modéliser et prévoir qui limitent les performances systèmes actuels en termes de fiabilité et temps réels.

Conclusion Générale

Les systèmes de reconnaissance biométrique sont des dispositifs de sécurité intuitifs. Certaines personnes s'opposent carrément à leur utilisation. Cependant, d'autres personnes sont d'avis qu'ils peuvent être nécessaires dans certains cas, à condition de prendre des mesures de sécurité et de juridiques appropriées qui sont en place pour protéger les renseignements personnels de nature délicate .

Dans ce travail nous nous sommes intéressés à l'identification biométrique par l'iris. Il s'agit de l'un des moyens les plus performants pour identifier une personne. En effet, des études biologiques ont montré que les profils et les courbes présents dans un iris garantissent son unicité. De plus l'iris contient des caractéristiques qui assurent la fiabilité et précisons du système base sur la reconnaissance par l'iris ce qui montre les performances de cette biométrie par rapport aux autres.

En premier temps nous avons établi une étude sur les principes de base de la reconnaissance par iris comme le traitement d'images, la reconnaissance de forme et la transformation par ondelettes, etc, afin de proposer un système complet de reconnaissance biométrique par l'iris.

En deuxième temps nous avons donné un état de l'art sur la reconnaissance biométrique par l'iris. Nous avons présenté différents travaux à savoir l'approche de DAUGMAN qui est la plus connue dans ce domaine, l'approche de WILDES et autres approches. Chaque approche a ses caractéristiques en termes de fiabilité et précision. Ensuite, nous avons proposés notre approche pour l'authentification de l'iris. Deux méthodes ont été testées. Dans la première méthode, nous avons utilisé la transformée de Hough, pour la détection de cercle, les ondelettes de Gabor pour le codage et la distance de Hamming pour la comparaison. Dans la deuxième méthode, nous avons suivi le même processus pour la localisation. Mais dans l'extraction de vecteur caractéristique nous avons appliqué la

transformée de Haar. Les deux méthodes ont été testées sur la base de données CASIA version 1.0.

Pour les deux approches nous avons calculé le taux de fausse acceptation et de faux rejet nous avons constaté que la première est plus performante en terme de fiabilité car le taux d'erreur inferieur à la deuxième méthode. Cependant celle-ci présente un vecteur caractéristique dont le nombre de bit est inférieur à la premiére ce qui nous permet de gagner en terme d'espace mémoire de stockage.

Pour conclure, la reconnaissance biométrique de l'individu demeure des problèmes complexes, malgré les recherches actives actuelles. Il y a de nombreuses conditions réelles, difficiles à modéliser et prévoir, qui limitent les performances systèmes actuels en termes de fiabilité et temps réels.

Comme perspective, nous proposons d'une part d'étendre l'algorithme développé, soit en ajoutant autre technique biométrique pour obtenir un système multimodale pour avoir des systèmes plus performants en termes de fiabilité de sécurité, soit en exécutant en temps réel. D'autre part, l'implémentation d'un tel algorithme sur une technologie cible afin de profiter des performances fournies par cette technologie.

Bibliographie

[1] Bernadette DORIZZI . Éditorial biométrie multimodale. In *GET/INT 9 rue Charles Fourier 91011 Evry, France Carmen GARCIA-MATEO E.T.S.I. de Telecomunicación Campus Universitario 36310 Vigo, Spain.*

[2] Emine Krichen . Thèse de doctoratreconnaissance des personnes par liris en mode degrade. 4 octobre 2007.

[3] J. P. Campbell . Speaker recognition : A tutorial. In *",Proceedings of the IEEE.*, volume Vol. 85, No. 9, p. 1437-1462.

[4] Lalita Acharya . Division des sciences et de la technologie. Le 11 septembre 2006.

[5] Pierre Piazza . La fabrique bertillonienne de lidentité. In *Labyrinthe, Thèmes,*, volume 33-50.

[6] Arun Ross et Salil Prabhakar. Anil K. Jain. *An Introduction to Biometric Recognition.*

[7] W. Boles and B. Boashash. A human identification technique using images of the iris and wavelet transform. . *IEEE Transactions on Signal Processing*, 1998.

[8] A. Jin C. Chin and D. Ling. *EHigh security iris verification system based on random secret integration.* PhD thesis, Computer Vision and Image Understanding,, May 2006.

[9] K. Hanna Y. Guo R. Wildes N. Takahashi C. Fancourt, L. Bogoni and U. Jain. Iris recognition at a distance. In *In The Proceedings of International Conference on Audio- and Video-Based Biometric Person Authentication*, 2005.

[10] Travieso C.M. Morales C.R. Ferrer M.A Camino, J.L. Signature classification by hidden markov model. security technology. In *Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference*, 1999.

[11] T. Camus and R. Wildes. Reliable and fast eye finding in close-up images. In *In The Proceedings of International Conference on Pattern Recognition*, 2002.

[12] Andrew Teach B.Jand David Ngo.C.L Chong Siew CHIN. *Tokenised discretisation in iris verification.* PhD thesis, faculty of information science and technologiy (FIST) ?MULTIM.

[13] Ravi Das. An introduction to biometrics. *Military Technology*, p. 20 à 27., juillet 2005.

[14] J. Daugman. *Demodulation by complex-valued wavelets for stochastic pattern recognition.* PhD thesis, International Journal of Wavelets, Multiresolution and Informa-tion Processing.

[15] J. Daugman. high confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1993.

[16] J. Daugman. *Statistical richness of visual phase information : Update on recognizing persons by iris patterns.* PhD thesis, International Journal of Computer Vision, 2001.

[17] J. Daugman. *The importance of being random : Statistical principles of iris recognition. Pattern Recognition.* 2003.

[18] J. Daugman. Biometric personal identification system based on iris analysis. Technical report, No. 5,291,560, 1994.

[19] J. Daugman and C. Downing. *UDemodulation, predictive coding, and spatial vision.* PhD thesis, J. Opt. Soc. Amer. A, 1995.

[20] Comité Consultatif National d'Ethique pour les sciences de la vie et de la santé . Avis relatif à la diffusion des techniques d'identification par analyse de l'adn (techniques des empreintes génétiques). décembre 1989.

[21] http ://www.biometrie online.net/. Master's thesis.

[22] Chinese Academy of Sciences. CASIA iris image database. http ://www.sinobiometrics.com Institute of Automation. 2004.

[23] R. Duin J. Matas. J. Kittler, M. Hatef. On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence,*, Vol. 20,n°3, p. 226 239, 1998.

[24] W. Kong and D. Zhang. *Detecting eyelash and reflection for accurate iris segmentation.* International Journal of Pattern Recognition and Artificial Intelligence, 2003.

[25] S. Pankanti . L. Hong, A. Jain. *Can Multibiometrics Improve Performance ?* PhD thesis, Oct 1999.

[26] Y. W L. Ma, T. Tan and D. Zhang. Personal identification based on iris texture analysis. *IEEE Transactions on Pattern Analysis and Machine Intel- ligence.*, 1999.

[27] P. Kovesi L. Masek. Matlab source code for a biometric identification system based on iris patterns. In *The University of Western Australia. http ://www.csse.uwa.edu.au/pk/studentprojects/libor*, 2003.

[28] J. Kharroubi S. Salicetti B.Dorizzi G. Chollet . M. Fuentes, D. Mostefa. *Verification de l'identite par fusion de donnees biometriques :signatures en-ligne et parole.* PhD thesis, 2002.

[29] LANTHONY P. Colorimétrie de l'oeil humain. il : iris. biom hum et anthropol. *A system for automated iris recognition. IEEE publications*, 1994.

[30] Hunny Mehrotra Anil Kumar Kaushik . Phalguni Gupta, Ajita Rattani. Multimodal biometrics system for efficient human recognition. In *Dept. of Computer Science and Engineering, Indian Institute of Technology Kanpur 208016, India bDept. of Information Technology, New Delhi 110003, India.*

[31] Hugo Pedro Martins Carric¸o Proenc¸a. Towards non-cooperative biometric iris recognition. In *University of Beira Interior Department of Computer Science*, October 2006.

[32] S. Sirohey . R. Chellappa, C. Wilson. Human and machine recognition of faces. In *A Survey, Proceedings of IEEE,*, volume Mai 1995, Vo. 83, p.705 740,.

[33] S. C. Hsu R. J. Kolczynski J. R. Matey R. P. Wildes, J. C. Asmuth and S. E. McBride. *Automated, noninvasive iris recognition system and method.* U.S. Patent, No. 5,572,596,.

[34] Sanchez-Avila C. Gonzalez-Marcos . Sanchez-Reillo, R. Biometric identification through hand geometry measurements. Oct 2000.

[35] P. Verlinde. Une contribution à la vérification multimodale de lidentité en utilisant la fusion de décision. 1999.

[36] Biométrie Wiki Vulnerabilite.com.

[37] M.S. Xiaomei Liu, B.S. these optimizations in iris recognition. In *of the University of Notre Dame Graduate Program in Computer Science and Engineering Indiana*, November 2006.

Résumé

L'iris est l'une des plus performantes modalités biométriques qui a plusieurs avantages. L'iris est le seul organe interne humain visible de l'extérieur, il est stable durant la vie d'une personne et il est caractérisé par une texture unique. Dans notre projet, nous proposons deux approches d'authentification biométrique par l'iris en exploitant les images de la base de donnée internationale CASIA version 1.0. Dans la première approche nous avons utilisé la transformé de Hough, pour la détection de l'iris, les ondelettes de Gabor pour le codage et la distance de Hamming pour prendre la décision. Dans La deuxième approche nous avons suivi les même étapes sauf que nous avons utilisé les ondelettes de Haar au lieu des ondelettes de Gabor. L'implémentation des algorithmes est réalisée en mettant en oeuvre leurs fiabilité ; les résultats expérimentaux des deux approches sont comparés pour dégager la performance de nos algorithmes .

Mots-clés: authentification, biométrie, iris, transformé de Hough, ondelettes de Gabor, ondelettes de Haar.

Abstract

The iris is one of the most accurate biometric modalities that have several advantages. It is the only internal organ of the body which is externally visible and highly stable through lifetime. It is characterized by a chaotic unique texture structure. In our project, we propose two approaches of iris authentication biometric by exploiting the images of the international data base CASIA version 1.0. In the first approach we used transformed of Hough for the detection of the iris, the wavelets of Gabor for coding and the Hamming distance to make the decision. In The second approach we made the same steps except we used the wavelets of Haar. The implementation of the algorithms is made by implementing reliability ; the experimental results of the two approaches are compared to release the performance of our algorithms.

Keywords: authentication, biometrics, iris, transformed of Hough, wavelets of Gabor, wavelets of Haar.