الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Génie Biomédical

Spécialité : Imagerie Médicale

Par : BENSALAH Fayza et FADLI Nabila

Sujet

Conception d'un système d'authentification et d'identification basé sur la biométrie d'iris

Soutenu le 20 / 06 / 2022 , devant le jury composé de :

M. DJEBBARI Abdelghani	*Professeur*	Université de Tlemcen	Président
Mme. BENCHAIB Yasmine	*MCA*	Université de Tlemcen	Examinatrice
M. HADJ SLIMANE Zine-Eddine	*Professeur*	Université de Tlemcen	Encadreur

Année universitaire : 2021 /2022

Remerciement :

Nous tenons tout d'abord à remercier Dieu, qui nous a donné la force et la patience d'accomplir ce modeste travail.
Nous adressons nos remerciements aux personnes qui nous ont aidés dans la réalisation de ce mémoire.

En premier lieu, nous remercions très chaleureusement notre encadreur M. Hadj Slimane Zine Eddine pour ses précieux conseils, son soutien et sa disponibilité qui nous a fourni.

Nous remercions l'ensemble du personnel de CHU de Tlemcen pour leur accueil et leurs aides.

Nos plus vifs remerciements, nous les adressons à nos professeurs de l'imagerie médicale pour tous leurs efforts, Et aux membres de jury M. DJEBBARI Abdelghani et madame BENCHAIB Yasmine pour l'intérêt qu'ils ont porté à notre travail.

Enfin, Nous tenons à exprimer notre sincère gratitude à toute personne ayant contribué de près ou de loin à la réalisation de ce mémoire.

Dédicaces

Je dédie ce mémoire :

À mes très chers parents pour leur soutient durant toute

Ma vie et sans eux je ne serai jamais devenu

Et à mon fils AMIR qui est ma raison de vivre,

mes frères Nasreddine et Abdelhamid,

et a toute ma famille.

À mes amis d'Enfance. À mes amis d'étude

A mes amis pour leurs soutiens et leurs

Encouragements.

À tous les professeurs et enseignants qui m'ont suivi

durant tout mon cursus scolaire et qui m'ont permis

de réussir Dans mes études.

À toute personne ayant contribué à ce

travail de près ou de loin.

BENSALAH Fayza

Dédicace

Avec un immense plaisir et une joie infinie, Je dédie
ce travail à ceux qui m'ont donnés la vie,
les symboles de tendresse, qui sont sacrifiés
pour mon bonheur et ma réussite,

À ma maman et mon papa, que dieu les garde
et les protège.

À mes frères et mes chères sœurs.

À mes petits amoureux AICHA et DJAWED.

À tous mes chers professeurs,

À tous ceux qui m'aiment,

À tous ceux qui j'aime,

Je dédie ce travail.

FADLI Nabila

Résumé

La reconnaissance par l'iris est considérée comme l'une des meilleurs systèmes biométriques permettant l'identification des individus. En effet, des études ont montré que L'iris représente l'une des modalités les plus fiables et efficace pour protéger les informations classe secrètes. L'objectif de notre travail est de concevoir un système d'authentification et d'identification basé sur l'**IRIS**. Les bases de données utilisées pour les tests sont : **UBIRIS V1, UPOL, MICHE**. Dans un premier temps, un seuillage automatique est utilisé pour segmenter l'image afin de détecter les régions d'intérêts. Ensuite, nous appliquons une série d'opérations morphologiques sur l'image pour isoler l'**IRIS** et la pupille. Enfin, nous avons utilisé la méthode de la distance de Hamming pour authentifier et identifier une personne.

Mots clefs : Authentification, identification, IRIS, distance de Hamming, les operations morphologique.

Abstract

Iris recognition is considered one of the best biometric systems for identifying individuals. Indeed, studies have shown that the iris is one of the most reliable and effective ways to protect classified information. The objective of our work is to design an authentication and identification system based on **IRIS**. The databases used for the tests are: **UBIRIS V1**, **UPOL**, **MICHE**. First, automatic thresholding is used to segment the image to detect regions of interest. Then by applying a series of morphological operations on the image to isolate the **IRIS** and the pupil. Finally, we use the Hamming distance method to authenticate and identify a person.

Keywords: Authentication, identification, IRIS, Hamming distance, morphological operations.

ملخص

يعتبر التعرف على قزحية العين من أفضل أنظمة القياسات الحيوية للتعرف على الأفراد. في الواقع ، أظهرت الدراسات أن قزحية العين هي واحدة من أكثر الطرق موثوقية وفعالية لحماية المعلومات السرية. الهدف من عملنا هو تصميم نظام مصادقة و تحديد الهوية يعتمد على **قزحية العين**. قواعد البيانات المستخدمة للاختبارات هي : **UBIRIS(V1) ، UPOL، MICHE**. أولاً ، يتم استخدام العتبة التلقائية لتقسيم الصورة لاكتشاف مناطق الاهتمام. ثم من خلال تطبيق سلسلة من العمليات المورفولوجية على الصورة لعزل **قزحية العين** و بؤبؤ العين. أخيرًا، نستخدم طريقة مسافة Hamming لمصادقة و تحديد هوية الشخص.

الكلمات المفتاحية: المصادقة ، وتحديد تحديد الهوية ، قزحية العين ، مسافة Hamming، العمليات المورفولوجية.

Table des matières

II. Chapitre II : La biométrie d'iris

III. Chapitre III : Application et résultats obtenus

Liste des figures

Chapitre I :

Chapitre II :

Chapitre III :

Liste des tableaux

Liste des abréviations et Acronymes

CNIL : La Commission Nationale de l'Informatique et des Libertés

ADN: Acide DésoxyriboNucléique

ROC: Curve Receiver Operating Caracteristics curve.

FMR : Taux de fausse correspondance (false matche rate)

FNMR : Taux de fausse non-correspondance (false non-matche rate

CMC : Cumulative Match Characteristic.

TFR : Taux de faux rejet

TFA : Taux de fausse acceptation

TFA : Taux de fausse acceptation**(TFA)**

TFR : Taux de faux rejet **(TFR)**

TVA : Taux de Vraie Acceptation

TVR : Taux de Vraie Rejet

TEE : Taux d'égale erreur

DAB : distributeur automatique de billets

GAB : guichet automatique bancaire

CCD : technologie des capteurs

CMOS : technologie des capteurs

U.V. Rayons ultraviolet

I.R. Rayon infra rouge

HOG : histogramme de gradient

SVM : Séparateurs à Vaste Marge

CASIA: Institute of automation Chinese Academy of science

JPEG : acronyme utilisé pour Joint Photographic Experts Group

MMU1 : Manchester Metropolitan University

BMP : un fichier bitmap, c'est-à-dire un fichier d'image graphique

PNG : Portable Network Graphics

CCD : Charge Coupled Device

CMOS : Complementery Metal-Oxide-Semiconductor

Diode DEL : Light Imitting Diode

RVB : Rouge Vert Bleu

UBIRIS v1 : UBIRIS: A Noisy Iris Image Database

ISO : Organisation internationale de normalisation

ISO-200 : Organisation internationale de normalisation correspond donc à une faible sensibilité.

MICHE : inspiré du nom (Michel) le créateur de la base de données

MATLAB : Programme développé par la société The Math Works.

BYOD : Bring Your Own Device

UE : Emarat United

USA : United Stats of America

Introduction Générale

A l'heure actuelle, L'identification d'une personne par ses traits biométriques est devenue un sujet d'intérêt dans de nombreux pays. Ce domaine nécessite encore une grande quantité d'études avant de l'utilisé.

La biométrie est une technologie émergente qui peut résoudre certains problèmes aux anciens systèmes de vérification de l'identité, elle n'est pas vraiment récente, elle est apparu au 19ème siècle avec plusieurs modalités. Les modalités les plus employées sont : le visage, la voix, l'empreinte, la signature manuscrite, iris…etc.

Notre travail consiste à concevoir un système d'authentification (et identification) qui utiliserait l'iris comme modalité biométrique qui a un rôle très important dans l'imagerie médicale.

L'iris est un trait biométrique le plus performant pour les systèmes de reconnaissance à grandes-échelle (UE, USA…etc, utilisent ce trait biométrique).

Dans le premier chapitre on va donner une généralité sur la biométrie, sa définition, ses modalités, son principe de fonctionnement, sa fiabilité, puis on va faire une comparaison entre les différentes modalités, les systèmes multimodaux et enfin les domaines d'applications.

Dans le deuxième chapitre on va parler sur l'iris, sa définition en anatomie, on va voir la conception générale d'un système biométrique basé sur l'iris, ensuite l'état de l'art des méthodes existantes, enfin on va citer quelques méthodes de reconnaissance d'iris.

Le troisième chapitre est consacré sur notre approche (algorithme sur **Matlab**), on va citer les méthodes qu'on va utiliser dans notre système biométrique et nos résultats qu'on a obtenus, puis on va prouver la fiabilité de notre travail par le degré de correspondance.

Le quatrième chapitre contient l'interface graphique de notre application.

Problématique

En raison du grand nombre de vols et falsification documentaire et aux menaces du terrorisme ou de la cybercriminalité, aussi l'évolution logique des réglementations internationales, de nouvelles solutions technologiques sont déjà utilisés.

Parmi ces technologies, la biométrie est la méthode la plus pertinente pour reconnaître les personnes de manière fiable et rapide, en fonction de caractéristiques biologiques uniques.

Dans notre approche on va répondre à la question suivante :

Comment peut-on faire un système biométrique performant basée sur l'iris ?

Objectifs et contributions

Pour le but d'amélioration de sécurité nous avons fait un travail consiste à concevoir un système d'authentification (et identification) qui utiliserait l'iris comme modalité biométrique. La reconnaissance biométrique de l'iris est une technologie extrêmement fiable en termes de résultats car l'iris est unique et extrêmement complexe. Le degré de correspondance dans notre système atteint jusqu'à 100% qui veut dire que ce système est fiable et précis que les autres modalités.

Partie Théorique

Chapitre I

Généralité sur la biométrie

Sommaire : chapitre I

I.1. Introduction :

La reconnaissance des individus devient une approche importante dans le domaine de la sécurité et les domaines privé, professionnels et public. Elle a deux rôles essentiels :

- **L'identification** d'une personne pour établir son identité.
- **L'authentification** qui vérifie la validité de l'identité d'un individu. [1]

La biométrie fait partie dans notre vie quotidienne pour un monde plus sûr, elle peut remplacer les mots de passes et d'autres identifiants pour supprimer le doute sur l'identité, le marché des produits d'authentification et d'identification est en pleine croissance.

Dans ce chapitre, nous définirons des généralités sur la biométrie, ces principes et son fonctionnement, les modalités et leur performance, les méthodes d'évaluation d'un système biométrique. Nous présenterons quelques exemples des techniques de reconnaissance par biométrie et leurs domaines d'application et établirons un tableau général (comparatif) des modalités les plus utilisées sur terrain.

I.2. Historique :

La première utilisation d'empreinte du pouce était par les babyloniens sur une poterie d'argile pour sceller des accords commerciaux, en VIème siècle, au même moment les parents chinois de la chine antique utilisaient l'empreinte digitale de la main que celle du pied pour différencier leurs enfants. Puis les égyptiens ont fait la différence entre les commerciaux connus et les nouveaux dans le marché à l'aide des descriptions physiques, au XVIème siècle, les français utilisait la couleur des yeux pour différencier entre les prisonniers. A cause de la rapidité de la croissance des cités et les besoins de reconnaître les personnes deviennent de plus en plus importantes, l'anthropométrie est apparue au XIXème siècle. [2].

Alphonse Bertillon, est l'inventeur du premier système biométrique, appelé plus tard "système Bertillon ou Bertillonnage" en 1882. Ce système était basé sur un ensemble de mesures anthropométriques comme la longueur de la main ou la distance entre les yeux. On parle aussi de "portrait parlé". Peu pratique et insuffisamment fiable, l'empreinte

digitale s'est ensuite imposer sur le système Bertillon à partir des années 1900. Ce système d'identification, aussi appelé "système Henry" dans les pays anglo-saxons pour Edward Henry, est basé sur l'unicité et la permanence de certaines figures cutanées (boucles, arches, tourbillons).

En 1973, au Japon par Takeo Kanade ou également travaux sur l'Iris de John Daugmann. Certains traits comme le visage sont plus étudiés que d'autres car ils sont aussi utilisés par les humains pour se reconnaitre les uns les autres dans la vie de tous les jours en 1994.

Anil Jain a également proposé au début des années 2000 d'utiliser plusieurs traits biométriques afin de construite un système multimodal plus performant que les systèmes existants basés sur une seule modalité.

La biométrie est maintenant aussi étudiée depuis une dizaine d'années dans un contexte de vidéo surveillance. Le plus souvent, il ne s'agit pas d'identifier stricto sensu les individus mais d'extraire plusieurs traits sémantiques (aussi appelés biométries douces) comme la taille, le genre, la couleur des cheveux…etc.

Depuis 2010 a été lancé en Inde le plus ambitieux programme d'identité numérique au monde dénommé Aadhaar (une identité pour tous) basé sur plusieurs modalités : l'iris, l'empreinte et le visage. En France, la **CNIL** tente d'encadrer son utilisation et a publié plusieurs recommandations et autorisations ces dernières années. Il est également important de noter qu'il existe de nombreux outils informatiques pour concilier, autant que possible, nouvelles technologies, sécurité et respect de la vie privée. [3]

I.3. Définition :

Le mot biométrie signifie littéralement « mesure du vivant » et désigne dans un sens très large l'étude quantitative des êtres vivants, d'une manière plus simplifiée, la biométrie signifie la "mesure du corps humain". L'usage de ce terme se rapporte de plus en plus à l'usage de ces techniques à des fins de reconnaissance, d'authentification et d'identification, le sens premier du mot biométrie étant alors repris par le terme bio statistique.

La biométrie est la vérification de l'identité d'un individu par ce qu'elle utilise des caractéristiques physiques ou physiologiques et comportementales.

On recense trois possibilités de prouver son identité :

- De ce que l'on possède. Jusque-là, on pouvait assez aisément le faire, qu'il s'agisse de la Clé de son véhicule, d'un document, d'une carte, d'un badge.
- De ce que l'on sait, un nom, un secret ou un mot de passe.
- De ce que l'on est, son empreinte digitale, sa main, son visage.

L'utilisation de la biométrie présente de nombreux avantages dont le premier, le niveau de sécurité et de précision qu'elle garantit. Contrairement aux mots de passe, aux badges, aux documents, les données biométriques ne peuvent pas être oubliées, échangées, volées, et demeurent infalsifiables.

Le mot biométrie est une traduction du mot anglais « biometrics » qui correspond en français à l'anthropométrie, c'est une "Science qui étudie à l'aide de mathématiques (statistiques, probabilités) les variations biologiques à l'intérieur d'un groupe déterminé». [4]

Le règlement général sur la protection des données propose quant à lui une définition juridique des données biométriques, entendues comme "les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques". [5]

On trouve la biométrie dans plusieurs domaines : Anthropologie, Identification, Médecine, Agronomie. Comme montre la figure (I, 1) :

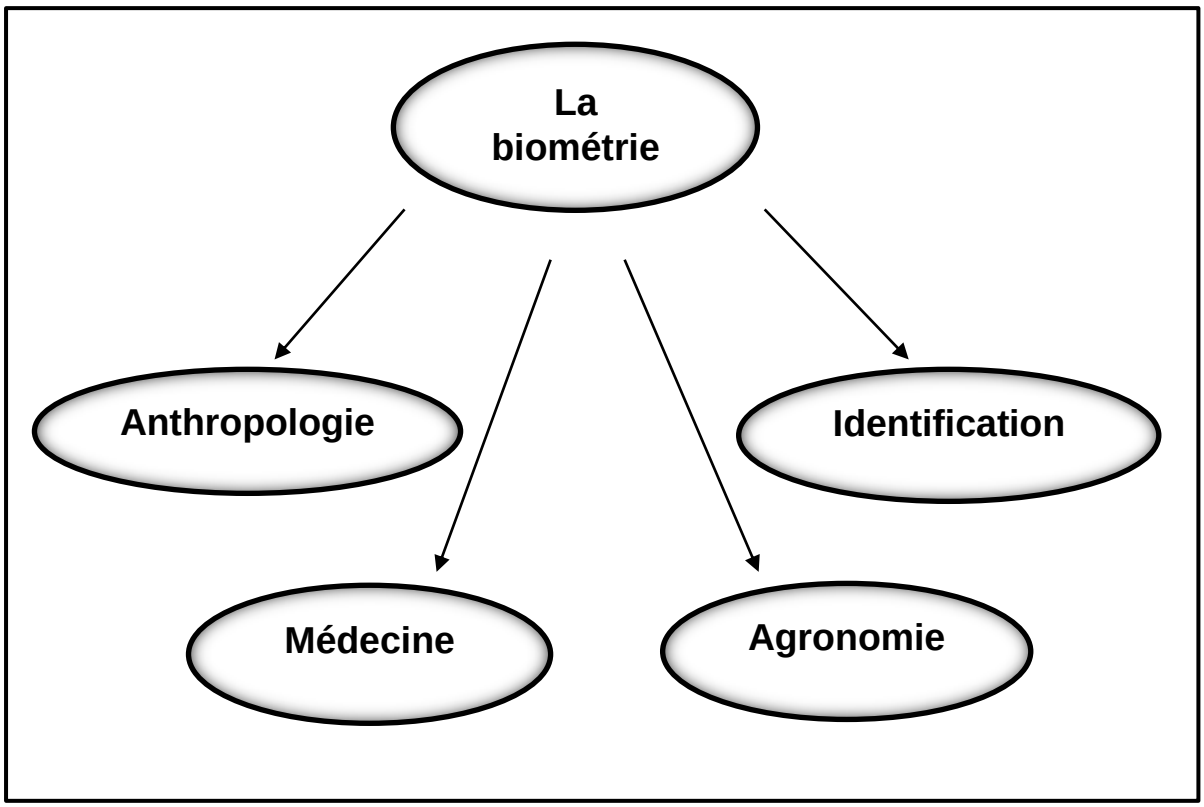


Figure (I, 1) : les différents domaines de la biométrie

I.4. Les caractéristiques de la biométrie :

On distingue deux catégories de technologies biométriques : les mesures physiologiques, et les mesures comportementales. Toutes ces caractéristiques biométriques doivent satisfaire à plusieurs critères pour être utilisables dans un processus d'identification. Elles doivent être :

- Uniques : la possibilité de deux personnes ayant les mêmes caractéristiques est minimal. Elles doivent permette la différenciation entre les individus,
- Universelles : les caractéristiques mesurées existent chez tous les individus, Stables : les caractéristiques mesurées ne changent pas au cours de temps et ne sont pas affectées par l'état de la personne tel que son état psychologique, son stress, etc.,

- Mesurables : le processus de mesure des caractéristiques peut être répété sans problème,
- Infalsifiables : les caractéristiques mesurées doivent être infalsifiables ou au moins le système biométrique doit être protégé pour identifier ces caractéristiques. [1]

I.5. Les différentes modalités biométriques :

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, et qui exploitent diverses informations biométriques à savoir : l'iris, le visage, la main, l'empreinte digitale, la voix, la signature …etc, [6]. (Figure (I, 2)). Parmi ces différentes techniques biométriques existantes on distingue trois catégories :

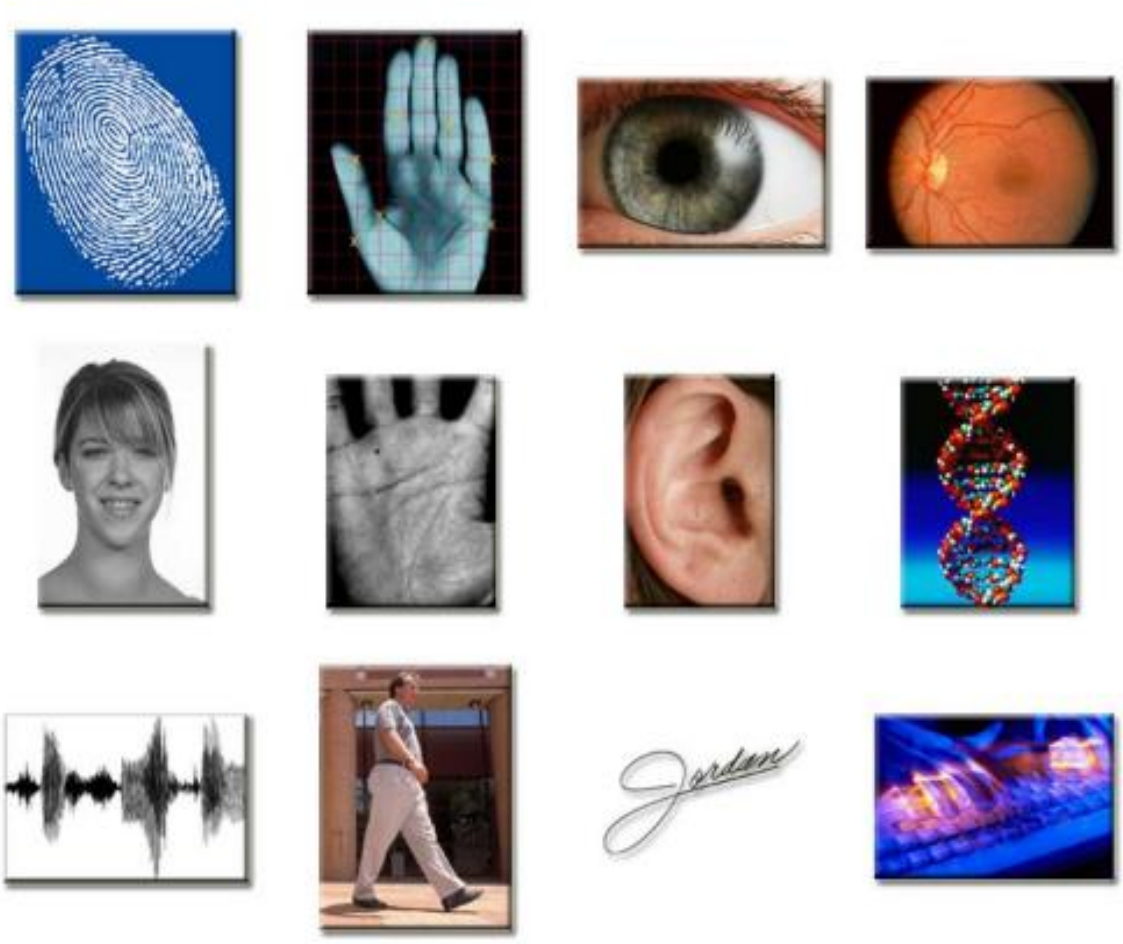


Figure (I, 2) : les différentes modalités biométriques

I.5.1. Analyse morphologique : elle se base sur les empreintes digitales, l'iris, le réseau vasculaire de la rétine ou de la paume de la main, la morphologie de la main, le poids, ainsi qu'avec les traits du visage. [6]

❖ **L'empreinte digitale :** Une empreinte digitale est le dessin formé par les lignes de la peau des doigts (Voir figure (I, 3)), des paumes des mains, des orteils ou de la plante des pieds. Ce dessin se forme durant la période fœtale. Il existe deux types d'empreintes : l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (saleté, sueur ou autre résidu déposé sur un objet) [6].

L'empreinte digitale est la caractéristique biométrique la plus utilisée dans le monde dès 1888, depuis que F. Galton découvrit la permanence et l'inaltérabilité du dessin papillaire de la naissance à la mort. Elle est utilisée depuis un siècle pour l'identification criminelle. Elle correspond à l'essentiel du marché actuel et son utilisation sera sans doute amenée à se développer. Elle possède un taux de fiabilité suffisant pour permettre d'identifier les individus dans de grandes bases de données. [7]

Figure (I,3) :l'empreinte dégitale

❖ **Le visage :** On peut identifier un individu en fonction de ses caractéristiques faciales en effectuant des mesures : écartement des yeux, arêtes du nez, commissures des lèvres, oreilles, menton (Figure (I, 4)). Ces différentes caractéristiques sont analysées par les systèmes de reconnaissance faciale et comparées à une base de données existante. Cette méthode permet d'identifier une personne ou de vérifier une identité [5].

Figure (I,4) :la biométrie de visage

❖ **L'iris :** est la zone colorée située entre le noir et le blanc [7]. L'utilisateur doit fixer l'objectif d'une caméra numérique qui balaie l'iris d'une personne d'une distance de 30 à 60 cm, et acquiert directement son dessin. (Figure (I, 5)). Elle le compare ensuite à un fichier informatisé d'identification personnelle (les systèmes de comparaison en usage aujourd'hui sont en mesure de fouiller une banque de données à la vitesse de plusieurs millions de codes iridiens par seconde). [5]

Figure (I, 5) : détail d'iris

❖ **La rétine :** La rétine est l'organe sensible de la vision, (Figure (I, 6)), pour obtenir d'une rétine il faut éclairer le fond de l'œil avec un faisceau lumineux à travers la pupille et le corps vitreux. Ce faisceau est de très faible intensité pour ne pas gêner l'utilisateur. Un système de caméra très précis vient ensuite de récupérer l'image de la rétine. [8]

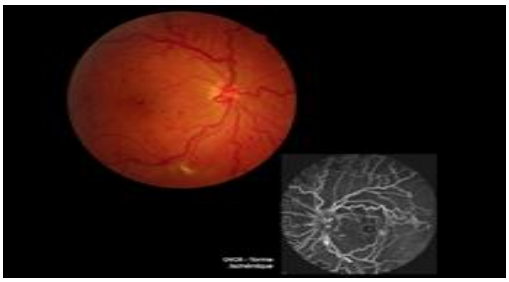


Figure (I, 6) : la rétine

I.5.2. Analyse biologique : elle utilise les caractéristiques biologiques des individus qui sont très complexes à mettre en œuvre dans un système de reconnaissance :

❖ **Reconnaissance veineuse :** On peut identifier un individu en fonction de ses caractéristiques veineuses en scannant son réseau veineux : doigts ou paume de main. (Figure (I, 7)) L'individu pose son doigt ou sa paume sur un scanner composé de leds et de caméras ce qui permet d'obtenir une empreinte veineuse unique et propre à chaque individu. Les veines sont uniques et immuables ce qui permet d'avoir une cartographie des veines identique de la naissance au décès. Les veines ne se modifient pas au cours du temps (sauf par accident comme une coupure par exemple). Cette technique récente semble prometteuse. Elle sonde par infrarouge le dessin du réseau veineux, soit du doigt, soit de la main. Les premiers produits viennent d'être mis sur le marché. Des espoirs peuvent être fondés sur cette technologie qui présente de nombreux avantages, car elle

permet de prendre une empreinte sans contact et sans laisser de trace, elle est en outre très difficile à déjouer par un imposteur [7]. Pour identifier et authentifier un individu, il suffit de comparer l'empreinte veineuse à celle enregistrée dans la base de données, cette méthode permet d'identifier une personne ou de vérifier son identité. La particularité de cette modalité est qu'elle est cachée donc elle nécessite une action volontaire de l'individu.

Figure (I, 7) : reconnaissance veineuse

❖ **L'odeur corporelle** : le vivant dépasse la machine. Même si des "nez électroniques" existent, le chien reste le plus performant pour détecter et identifier les odeurs individuelles. Mais peu de personnes sont prêtes à accepter de se faire renifler tous les matins ! Du coup, la technique est surtout utilisée dans l'agroalimentaire. [8]

❖ **L'ADN :** L'empreinte génétique est la marque biologique la plus sure du monde. Dans le cas des tests de paternité, on atteint une fiabilité de 99,999%. Mais les analyses d'ADN la (figure (I, 8)) nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel. [8]

Figure (I, 8) : l'ADN

I.5.3. Analyse comportementale : elle peut se pratiquer avec l'analyse de certains traits personnels du comportement de l'individu comme sa façon de taper sur un clavier, le tracé de sa signature, sa démarche…etc.

❖ **La démarche :** il s'agit de reconnaitre un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvement du corps…) en analysant des séquences d'images. [10]

❖ **Signature :** la biométrie par signature inclut habituellement un crayon lecteur et une tablette à digitaliser, on prit en compte la vitesse de signature et l'accélération et la pression exercée [9]. Cette solution peut présenter un intérêt en particulier dans le commerce électronique, mais il s'agit plus d'une méthode d'authentification que d'identification et malgré les progrès techniques, le risque de contrefaçon est loin d'être négligeable. [7] (Figure (I, 9))

Figure (I, 9) : reconnaissance de signature

❖ **La voix :** utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mots de passe. Un téléphone ou un microphone peut être utilisé comme dispositif d'acquisition, ce qui rend cette technologie relativement économique et facilement réalisable Cependant, elle peut être perturbée par des facteurs extérieurs comme le bruit de fond (Figure (I, 10)). [10]

La vérification vocale consiste à reconnaître automatiquement l'identité d'une personne prononçant une ou plusieurs phrases en déterminant si un locuteur est bien celui qu'il prétend être, comme un auditeur humain identifie son interlocuteur au cours d'une conversation. Pour cela, le système dispose, en entrée, d'un échantillon de parole et d'une identité proclamée. Une mesure de ressemblance est calculée entre l'échantillon et la référence du locuteur correspondant à l'identité proclamée. Si cette mesure est en-dessous d'un certain seuil, le système accepte le locuteur ; dans le cas contraire, le locuteur est considéré comme un imposteur et rejeté.

Figure (I, 10) : spectre d'un signal vocal

❖ **La dynamique de frappe** : cette modalité permet d'authentifier des individus selon leur façon de taper au clavier, ce système est peu couteux, car il ne nécessite pas de matériel d'acquisition autre que le clavier de l'ordinateur [11]. Cette technique repose sur les particularités de chaque individu lorsqu'il frappe sur un clavier, en particulier, la force avec laquelle il frappe. En l'état actuel des techniques, cette méthode peut difficilement être regardée comme une technique de haute sécurité, mais plus comme une technique de substitution à un code pour ouvrir un appareil électronique. [7]

I.5.4. Autre modalités :

❖ **La géométrie de l'oreille** : A priori, la technique serait efficace, car il n'existe pas deux formes d'oreilles identiques. Mais il n'existe encore aucune application commerciale. [10]

❖ **Biométrie fœtale :** En médecine de la biométrie correspondent à des mesures qui sont réalisées grâce à l'échographie durant la grossesse. La biométrie permet de suivre l'évolution de la croissance de l'enfant à l'intérieur de l'utérus de la maman. Au début de la grossesse cette mesure concerne essentiellement la longueur entre le crâne et le bout des fesses (on appelle cela la longueur craniocaudale). Par la suite les mesures s'effectuent au niveau de la tête : le diamètre entre les deux lobes pariétaux par exemple. Les mesures de l'abdomen et du fémur sont également recherchées. D'autres mesures peuvent également être faites comme par exemple celles des os du pied entre autres. [8]

❖ **Salive :** Chez l'être humain, elle contient aussi de nombreuses cellules provenant de la langue et des muqueuses de la bouche, ce qui la fait utiliser pour l'échantillonnage de l'ADN individu. [12]

❖ **Les ongles ou encore l'irrigation sanguine** : La technique est basée sur les stries longitudinales des ongles, qui dépendent de la structure de l'épiderme sous-jacent. On peut révéler le relief de l'ongle grâce à un interféromètre, et le cartographier. [11]

❖ **Cheveux, La taille, L'analyse des pores de la peau, La thermographie faciale...etc.**

Figure (I, 11) : quelques modalités biométriques cachés

I.6. Principe de fonctionnement :

On distingue deux types d'utilisation d'un système biométrique, on peut **identifier** une personne parmi un ensemble composé de *N* individus, le système devra alors rechercher la personne qui correspond le mieux à son observation pour **vérifier** l'identité d'une personne, le système devra simplement prendre une décision d'acceptation ou de rejet de cette personne.

Il existe deux phases dans un système biométrique, une phase d'apprentissage, appelée aussi enrôlement, et une phase de reconnaissance, ou vérification ainsi que l'autre facultatif pour l'adaptation, comme la figure (I, 12) illustre :

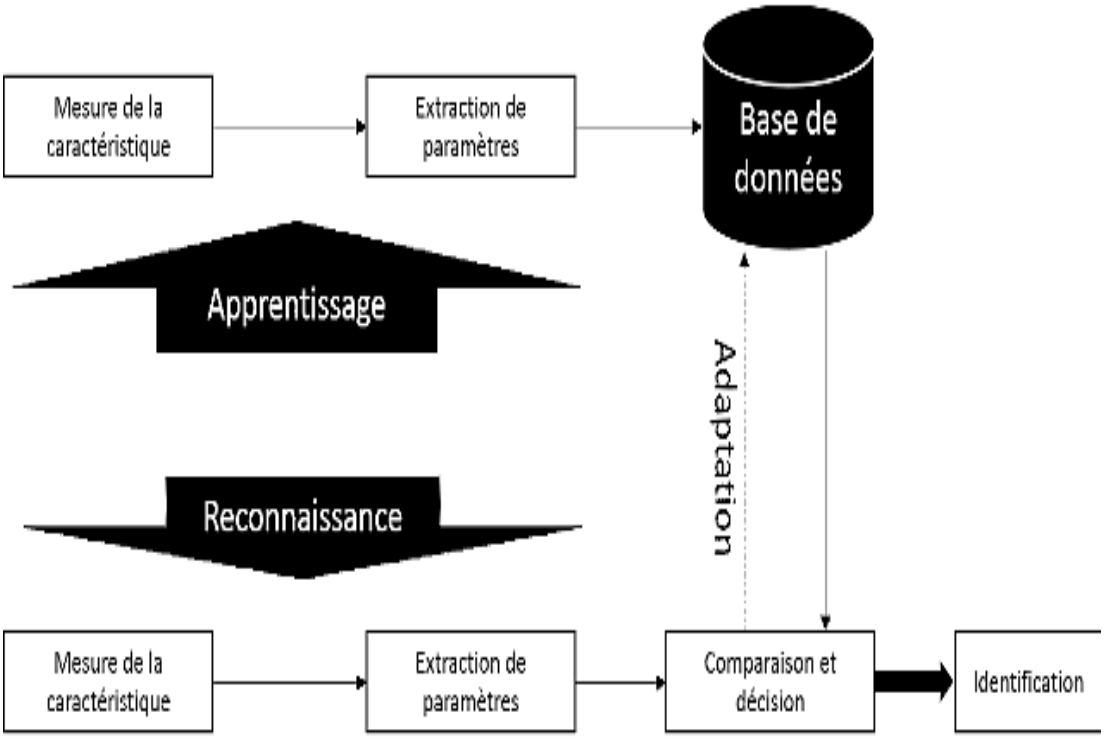


Figure (I, 12) : representation d'une architecture d'un système biometrique

I.6.1. Phase d'apprentissage :

Cette phase contient l'acquisition ou la capture de la caractéristique. Cette capture n'est stockée dans la base de données qu'après des certaines transformations lui appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle ou gabarit est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Il est à noter que la qualité du capteur peut grandement influencer les performances du système. Meilleure est la qualité du système d'acquisition, moins il y aura de prétraitements à effectuer pour extraire les paramètres du signal. [13] [14]

I.6.2. Phase de reconnaissance :

Dans cette phase, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage.

Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. [13] [14]

Cette phase se diffère selon le système utilisé (identification ou authentification) :

I.6.2.1. L'authentification :

Appelée également vérification, est le processus qui consiste à comparer les données caractéristiques provenant d'une personne, au modèle de référence biométrique de cette dernière « Template », afin de déterminer la ressemblance. Le modèle de référence est préalablement enregistré et stocké dans une base de données, dans un équipement ou objet personnel sécurisé. On vérifie ici que la personne présentée est bien la personne qu'elle prétend être [13] [14]. (Figure (I, 13))

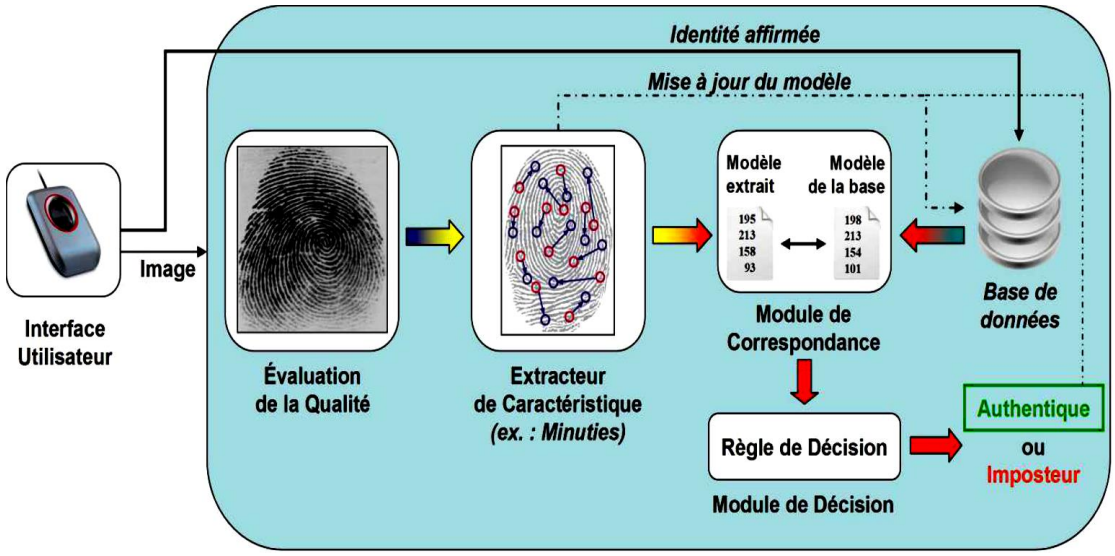


Figure (I, 13) : structure d'un système d'authentification [22]

I.6.2.2. Identification :

Consiste à déterminer l'identité d'une personne. Il s'agit de saisir une donnée biométrique de cette personne, en prenant par exemple une photo de son visage, en enregistrant sa voix, ou en captant l'image de son empreinte digitale…etc. Ces données sont ensuite comparées aux données biométriques de plusieurs autres personnes qui figurent dans une base (Voir figure (I, 14)). [13] [14]

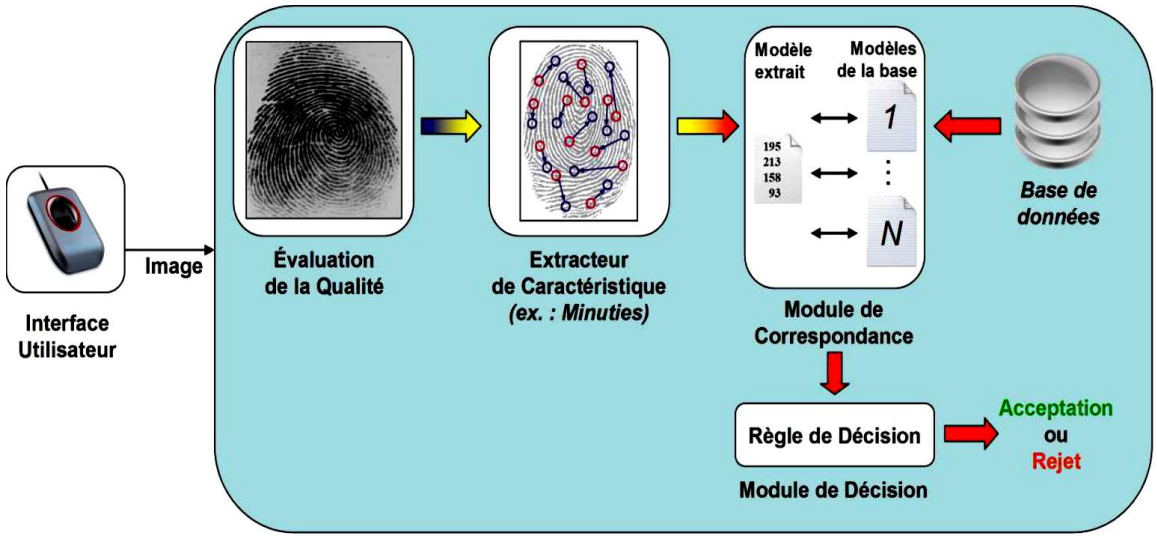


Figure (I, 14) : structure d'un système d'identification [22]

I.6.3. Phase d'adaptation :

Le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier.

L'adaptation est donc nécessaire pour maintenir voire améliore la performance d'un système utilisation après utilisation. L'adaptation peut se faire en mode supervisé ou non-supervisée mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré - estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance

du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non - supervisée peut poser problème en cas d'erreurs du module de reconnaissance. L'adaptation est quasi indispensable pour le les caractéristiques non permanentes comme la voix [13] [14].

I.7. Les modes du système biométriques :

I.7.1. Système unimodal : Les systèmes uni-modaux doivent faire face à divers défis tels que le manque de secret, la non-universalité des échantillons, l'étendue du confort et de la liberté de l'utilisateur tout en traitant avec le système, les attaques d'usurpation d'identité sur les données stockées, etc. Certains de ces défis peuvent être relevés en utilisant un système biométrique multimodal. [15]

I.7.2. Système multimodale : Le système biométrique multimodal possède tous les modules conventionnels d'un système unimodal (la figure (I, 15)) illustre les différents modules du système multimodal :

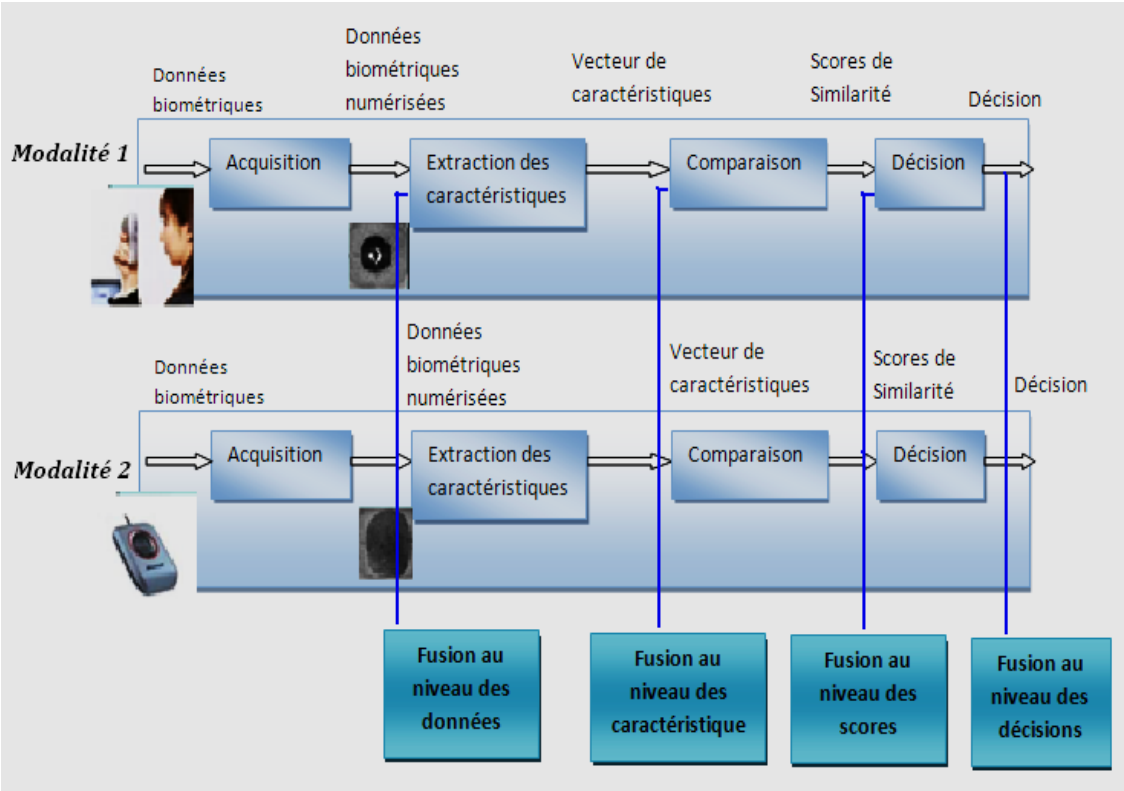


Figure (I, 15) : système biométrique multimodal

➢ **Les formes de la multimodalité :**

Il existe cinq forme sont :

- **Multi-capteurs** : utilisation de plusieurs capteurs pour acquérir la même modalité.
- **Multi-instances** : utilisation de plusieurs instances de la même biométrie.
- **Multi-algorithmes** : utilisation de plusieurs algorithmes traitent la même image acquise.
- **Multi-échantillons** : utilisation de plusieurs échantillons différents de la même modalité.
- **Multi-biométries** : plusieurs biométries différentes. [16]

➢ **Les modules conventionnels de la biométrie unimodale et multimodale :**

Le tableau suivant (Tableau (I, 1)) : montre les modules conventionnels du système unimodal et les niveaux de la fusion du système multimodale :

Les niveaux :	**Unimodal :**	**Multimodal :**
Module de capture	**Utilise un seul capteur.**	**Utilise deux ou plusieurs capteurs. (ex : caméra infrarouge caméra a lumière visible).Utilise un algorithme ou une combinaison d'algorithmes.**
Extraction des fonctionnalités	**Extraction de caractéristiques pertinentes.**	**La classification Différents vecteurs de caractéristiques sont combinés. Appliquant différents algorithmes d'extraction de caractéristiques aux mêmes données brutes.**

Module de décision	**On peut fusionner les deux module (module de décision avec le module de rang) et on appelle : Module de comparaison.**	**chaque sous-système biométrique complète de manière autonome les processus d'extraction.**
Module de rang	***Identification : comparaison de l'image capturée avec une base de données enregistrée.** ***Authentification ; comparaison de l'image capturé avec une image dans la base de donnée.**	**La fusion au niveau des rangs consiste à combiner les rangs d'identification obtenus à partir de plusieurs données biométriques unimodales. Il consolide un rang qui est utilisé pour prendre la décision finale.**
Module de score	**Acceptation ou rejet**	**La combinaison des scores d'appariement fournis par les différents systèmes. Les techniques de fusion au niveau du score sont divisées en deux ensembles principaux : les règles fixes (ET, OU, majorité, maximum, minimum, somme, produit et règles arithmétiques) et les règles entraînées (somme pondérée, produit pondéré, discrimination linéaire de Fisher, discrimination quadratique, logistique)**

Tableau (I, 1) : comparaison entre la biométrie unimodal et multimodal

I.8. Test de fiabilité du système biométrique :

La fiabilité d'un système biométrique se mesure généralement à l'aide d'une courbe **"**caractéristique de la performance d'un test**"** ou **"**courbe **ROC"** indiquant son :

❖ **Taux de faux positifs** (**FMR**) : par rapport à une galerie d'échantillons biométriques, Le taux de faux positifs est la fréquence à laquelle des échantillons biométriques de différentes sources sont incorrectement considérés comme originaires d'une même source.

❖ **Taux de faux négatifs** (**FNMR**) : est la fréquence à laquelle des échantillons d'une même source sont incorrectement considérés comme originaires de sources différentes.

❖ Un système biométrique performant se caractérise par des résultats rapides et un faible taux de faux positifs et de faux négatifs, la fiabilité d'un système est égale au point de la courbe ROC dont l'emplacement est fonction du "seuil" de correspondance appliqué.

♦ Un seuil de correspondance élevé réduit le taux de faux positifs mais augmente le taux de faux négatifs (plus de sécurité, moins de commodité).

♦ Un seuil de correspondance faible réduit le taux de faux négatifs mais augmente le taux de faux positifs (plus de commodité, moins de sécurité ; voir la figure (I, 16). Un grand nombre de données (ex : plus d'empreintes digitales) et des échantillons de grande qualité (très réguliers) sont nécessaires pour les identifications, contrairement aux vérifications [17]. Il est important de reconnaître que la fiabilité des systèmes biométriques dépend largement de la nature des données biométriques du système. Chaque galerie de données biométriques par rapport à laquelle est effectuée une comparaison d'échantillons donnera une courbe ROC (Curve **(Receiver Operating Caracteristics curve)** qui représente l'évolution du FRR en fonction du FAR. L'étude de cette courbe permet de déterminer les performances d'un système biométrique de fiabilité différente. (Figure (I, 16) explique la fiabilité du système : [18]

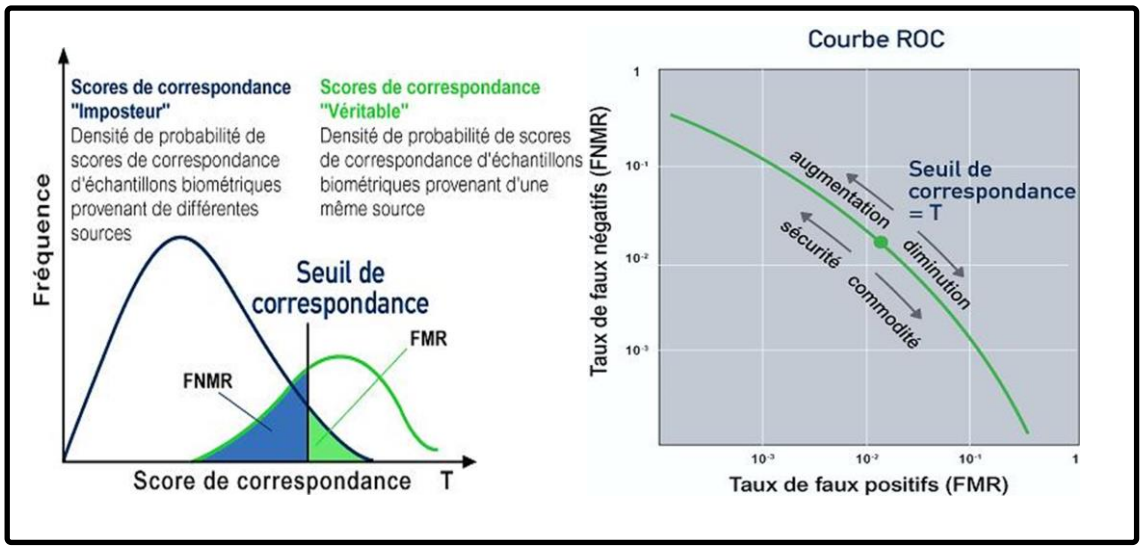


Figure (I, 16) : courbe ROC pour un système de recherche correspondance biométrique et un ensemble de données

Dans le cas d'un système utilisé en mode identification, on utilise ce que l'on appelle une courbe CMC (pour "Cumulative Match Characteristic" en anglais). La courbe CMC (Figure (I, 17)) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée…etc, On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible. [19]

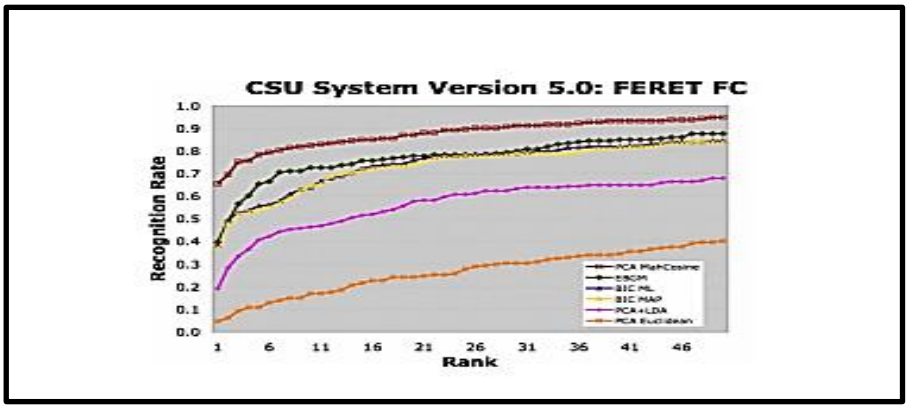


Figure (I, 17) : courbes CMC du CSU System 5.0 pour le "FERET Probe Set FC" et pour différents algorithmes de reconnaissance faciale

Le meilleur moyen de prédire le comportement d'un système biométrique lors d'un déploiement en situation réelle consiste donc à tester ses performances sur des données pour lesquelles il n'a pas été expressément entraîné.

❖ **Taux de faux rejet (TFR)** : la probabilité qu'un utilisateur connu soit rejeté par le système biométrique.

❖ **Taux de fausse acceptation (TFA)** : indique la probabilité qu'un utilisateur inconnu soit identifié comme étant un utilisateur connu.

Ce taux définit la sécurité du système biométrique. [17]

♦ **Fausse Acceptation** : Événement ayant lieu lorsqu'un système biométrique accepte une personne alors qu'elle n'est pas dans sa base d'utilisateurs. Cet événement doit être le plus rare possible pour assurer la sécurité d'un système biométrique.

♦ **Faux Rejet** : Événement ayant lieu lorsqu'un système biométrique refuse une personne alors qu'elle est dans sa base d'utilisateurs. Cet événement est souvent dû à une mauvaise acquisition des données biométriques et est perçu comme une gêne par l'utilisateur.

❖ **TFA - Taux de fausse acceptation(TFA)** : C'est la probabilité qu'un utilisateur inconnu soit identifié comme étant un utilisateur connu. Ce taux définit la sécurité du système biométrique. En anglais " False Accept Rate (**FAR**) " c'est la probabilité qu'un utilisateur non reconnu mais qui est accepté par le système (le pourcentage d'acceptation d'un imposteur). Le calcule de ce taux est comme suite :

$$\mathbf{FAR} = \frac{\text{Nb de } \mathbf{FA}}{\text{Nb imposteurs}} \qquad \mathbf{(I, 1)}$$

❖ **TFR - Taux de faux rejet (TFR) :** la probabilité qu'un utilisateur connu soit rejeté par le système biométrique. Ce taux définit en partie le confort d'utilisation du système biométrique. En anglais "False Rejection Rate (FRR) " concerne la probabilité qu'un utilisateur connu soit rejeté (le pourcentage de faux de rejet d'un utilisateur légitime). Sa formule est donnée comme suite :

$$\mathbf{FRR} = \frac{\text{Nb de } \mathbf{FR}}{\text{Nb de clients}} \qquad \mathbf{(I, 2)}$$

Les erreurs que l'on peut faire sont de deux sortes :

FR= (False Rejection) rejeter faussement un client

FA= (False Acceptation) accepter faussement un imposteur

❖ **Taux de Vraie Acceptation (TVA) :** le taux d'acceptation d'utilisateurs de façon justifiée.

❖ **Taux de Vraie Rejet (TVR) :** le taux d'imposteurs qui peuvent être rejetés par le système.

❖ **TEE - Taux d'égale erreur** : Donne un point pour lequel le **TFA** est égal au **TFR**.

❖ **Temps de réponse** : Période temporelle requise par un système biométrique pour retourner une décision sur l'authentification d'un échantillon biométrique. [17]

❖ **Échec à l'enrôlement** : Événement ayant lieu lorsqu'une personne ne réussit pas à s'enrôler. Ceci inclut les cas où la personne ne peut pas fournir l'échantillon biométrique demandé, les cas où la qualité de l'échantillon est insuffisante,

❖ **Taux d'échec à l'enrôlement** : Evaluation statistique de la partie de la population ne pouvant pas être enrôlée sur un système donné. Ce taux dépend de la méthode de capture, du capteur et de l'algorithme utilisé ainsi que des caractéristiques de la population étudiée.

❖ **Gabarit** (en anglais **Template)** : Modèle initial créé au cours de l'enrôlement. Modèle mathématique décrivant certaines caractéristiques physiques ou comportementales d'un individu. On comparera par la suite les demandes de reconnaissance à ce modèle.

❖ **Matching** : Procédé mathématique permettant d'effectuer la comparaison de deux échantillons biométriques [17]

❖ **Modèle de référence** : Donnée représentant une caractéristique biométrique d'un individu utilisé par un système biométrique pour permettre la comparaison avec des échantillons soumis a posteriori biométrique.

❖ **Seuil de décision** : L'acceptation ou rejet d'une donnée biométrique dépend du passage du score de correspondance au-dessus ou au-dessous du seuil. Ce dernier est ajustable pour rendre le système biométrique plus ou moins strict, cela dépend des éléments requis par tout système application biométrique

❖ **Seuil de rejet** : Score minimum en dessous duquel un algorithme biométrique rejettera une authentification/identification.

❖ **Seuil d'acceptation** : Score au-dessus duquel un algorithme biométrique acceptera une authentification/identification. [17]

I.9. Comparaison des différentes modalités biométriques :

Chaque modalité biométrique a ses bienfaits et ses inconvénients. Le tableau suivant (I, 2) est un tableau comparatif entre ces différentes modalités biométriques :

	Biométriques	Fiabilité	Coût	Taille de l'échantillon	Stabilité sur du long terme
	Reconnaissance faciale	Faible	Elevé	Large	Faible
	Iris	Elevée	Elevé	Petite	Moyenne
	Empreintes digitales	Elevée	Faible	Petite	Elevée
	Réseau veineux du doigt	Elevée	Moyen	Moyenne	Elevée
	Reconnaissance vocale	Faible	Moyen	Petite	Faible

Redsen Consulting – Avril 2018

Tableau (I, 2) : tableau comparatif entre les modalités biométriques

Il montre que la biométrie d'iris et celle de l'empreinte digitale et de Réseau veineux du doigt sont les plus fiables (fiabilité). L'iris et la reconnaissance faciale sont plus couteux que les autres modalités. La taille d'échantillons de l'iris, de reconnaissance vocale et l'empreinte digitale est petite par contre les autres modalités (sont : large ou moyen). L'empreinte digitale et la reconnaissance du réseau veineux du doigt ont stabilité du long terme que l'iris, reconnaissance faciale et la reconnaissance vocale. [20]

I.10. Les domaines d'applications biométriques :

L'évolution des technologies biométriques (maturité technique, coûts en baisse) permet aux professionnels qui œuvrent dans les domaines de la sécurité et de la sûreté de déployer des solutions qui bénéficient d'une plus-value technique et commerciale accrue.

Les différents domaines dans lesquels s'exercent ces professionnels sont :

- **Les transports :** contrôle des titres de transport**.**
- **La gestion des accès logiques :** PC, serveurs, bases de données**.**
- **Le verrouillage des équipements de communication :** téléphones portables.
- **Le verrouillage des véhicules** : clef de contact, boîte à gants [21]
- **Sécurité biométrique :** La technologie biométrique est plus accessible que jamais auparavant, prête à apporter une sécurité améliorée et une plus grande commodité à tout ce qu'il faut protéger.
- **Contrôle frontalier / Aéroports :** Contrôle des frontières par identification biométrique dans les aéroports est un domaine clé d'application pour la technologie biométrique. [21]
- **Biométrie résidentielle :** Les innovations récentes en matière de mobilité et de connectivité ont créé une demande de biométrie dans les foyers et les poches des consommateurs, (Exp : Les Smartphones avec capteurs d'empreintes digitales, la reconnaissance faciale et vocale),
- **Biométrie financière :** L'identification financière, la vérification et l'authentification dans le commerce contribuent à rendre les opérations bancaires, les achats et la gestion des comptes plus sûrs, pratiques et responsables [21]. La sécurisation des transactions : banque, finance, Internet (distributeur automatique de billets : **DAB**, guichet automatique bancaire : **GAB**, terminaux de paiement). [21]
- **Biométrie de la santé :** La biométrie offre non seulement une sécurité et une commodité partout où elle est déployée, mais dans certains cas elle apporte une organisation accrue. Dans le domaine de la santé, cela est particulièrement vrai. Les

dossiers de santé sont quelques-uns des documents personnels les plus précieux, et les médecins ont besoin d'y accéder rapidement. [21]

- **Justice :** La technologie biométrique et la justice ont une histoire très longue, et de nombreuses innovations très importantes en matière de gestion d'identité ont suscité cette relation bénéfique. Aujourd'hui, la biométrie légale est vraiment multimodale ; l'empreinte digitale, la reconnaissance faciale et la reconnaissance vocale jouent tous un rôle crucial dans l'amélioration de la sécurité publique et l'identification des personnes recherchées.

- **Contrôle d'accès logique :** Le contrôle d'accès logique est un domaine d'application majeur pour la technologie biométrique. Lorsque nous disons : « Il est temps de tuer le mot de passe », c'est la technologie dont nous parlons. Qu'il s'agisse de sécuriser les applications sur votre Smartphone, d'accéder à un email de travail ou de permettre une politique BYOD efficace.
- **Biométrie mobile :** Les solutions de biométrie mobile vivent à l'intersection de la connectivité et de l'identité. Elles intègrent soit une ou plusieurs modalités biométriques à des fins d'authentification ou d'identification, et profitent de la portabilité des Smartphones, des tablettes, et d'autres types d'ordinateurs de poche.
- **Temps et pointage :** Des solutions biométriques pour la gestion du temps existent pour suivre les mouvements du personnel, avoir un rapport précis sur les heures de travail de chacun, et optimiser le rendement des ressources humaines. Et ce en installant une pointeuse biométrique au niveau des entités, sociétés, entreprises et autres organismes. [21]
- **La gestion de titres identitaires :** carte nationale d'identité, permis de conduire, carte de séjour.
- **L'immigration :** contrôle aux frontières. [21]

I.11. Conclusion :

Dans ce chapitre, nous avons montré c'est quoi la biométrie, les différentes technologies biométriques et les domaines d'applications de ces techniques, ainsi les performances de système biométrique, bien que certaines technologies biométriques sont utilisées pour identifier des individus.

Dans le chapitre suivant on va présenter une technique spécifique qui est la technique de la biométrie basée sur l'iris.

Chapitre II

La biométrie d’iris

Sommaire : chapitre II

II.1. Introduction :

Il existe plusieurs modalités biométriques dans le monde qui diffèrent les unes des autres en termes de performance, de sécurité, de confort et de simplicité d'utilisation. La reconnaissance des personnes à partir des images d'iris est considérée comme étant parmi les meilleures technologies biométriques

Ce chapitre est consacré à la définition de l'iris et ses caractéristiques, à l'architecture d'un système d'authentification et d'identification ainsi que les méthodes de reconnaissance de l'iris.

II.2. Anatomie de l'œil :

L'œil, une sphère complexe ou globe oculaire, est une structure creuse de forme globalement sphérique. Il se compose de tuniques, d'un cristallin et de liquides. La tunique externe est la sclérotique, tissu conjonctif dense et peu vascularisé. Son rôle est la protection de l'œil. C'est le blanc de l'œil, elle est entourée d'une membrane très fine et transparente, appelée conjonctive. Du côté antérieur, cette sclérotique est remplacée par la cornée, transparente qui permet l'entrée des rayons lumineux dans le globe oculaire. Elle est plus riche en fibres nociceptives : le contact avec un objet induit le clignement et la sécrétion lacrymale, deux fonctions de protection. (Voir la Figure(II,1).

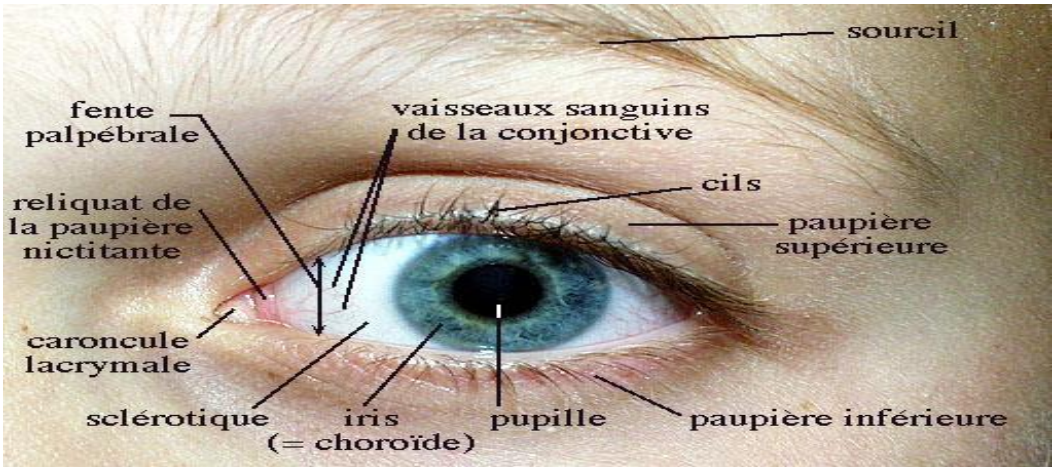


Figure (II, 1) : les composants de l'œil

La cornée est composée de cinq couches différentes :

- Epithélium cornéen : 32 micromètres d'épaisseur, cellules se renouvelant rapidement. L'éclat du regard est lié à la régularité de la surface épithéliale, et à l'intégrité du film de larmes ;
- Membrane de Bowman : couche de transition de 12 micromètres, nature conjonctive ;
- stroma : très épais (400 microns), 90 % de l'épaisseur de la cornée. Tissu conjonctif très spécifique. Il contient de l'eau, des substances organiques, du collagène. Tous ces éléments sont présents dans des règles qui assurent la transparence ;
- Membrane de Décimètre: 6 micromètres ;
- Endothélium : de 6 micromètres, membrane interne, fragile et fine. La qualité et la quantité de ces cellules varient avec l'âge et des altérations y surviennent à partir de 65 ans.

La tunique vasculaire au milieu est formée de trois parties : la choroïde, le corps ciliaire et l'iris :

- La choroïde est une membrane pigmentée en brun par des mélanocytes. Elle constitue une chambre noire, elle est très vascularisée ;
- Le corps ciliaire est formé de muscles lisses qui modifient la forme du cristallin et permettent l'accommodation ;
- L'iris est la partie colorée de l'œil. Composé de muscles lisses, il permet de contrôler la taille de la pupille (ouverture centrale de l'œil) et donc la quantité de lumière (diaphragme de l'œil).

Le champ de vision est la portion d'espace que nous voyons, il comprend une partie de vision monoculaire et une partie de vision binoculaire. La pupille est un trou circulaire au milieu de l'iris qui est le diaphragme de l'œil. Il règle la quantité de lumière entrante et sa taille varie en fonction de la lumière. Quand le diamètre est petit, la profondeur du champ augmente, et il y a moins d'imperfection au niveau de l'image perçue. Son diamètre en lumière normale se situe aux alentours de 3 et 6 mm, le phénomène de l'augmentation du diamètre de la pupille se nomme « mydriase », et sa diminution « myosis ». Chez l'être humain la pupille est circulaire, ce n'est pas le cas chez les animaux.

- Il y a une mydriase bilatérale lors d'une excitation d'un nerf sensitif (ouïe, vue, odorat), dans l'obscurité, lors de coma ou de mort, chez les diabétiques, les épileptiques et également chez les usagers de drogues dérivées des amphétamines.

- Une mydriase unilatérale s'installe à la suite d'un glaucome ou d'un décollement de la rétine.
- Un myosis bilatéral apparaît lors d'une luminosité abondante, d'un clignement de l'œil, lors du passage de la vision de loin à la vision rapprochée et chez les usagers de dérivés morphiniques.
- Un myosis unilatéral se forme quand il y a une présence d'un corps étranger dans l'œil, lors d'une kératite (inflammation de la cornée) ou encore à la suite d'une paralysie des voies optiques.

La transmission des informations obtenues sur la rétine vers le cerveau est opérée par le nerf optique. Toutes les fibres optiques issues des cellules visuelles convergent vers un point précis de la rétine (la pupille). En ce point débouche aussi le réseau veineux et artériel de la rétine. Les fibres optiques se rejoignent toutes là pour former un câble : le nerf optique. Il mesure 4 mm de diamètre et 5 cm de long. Il y a un nerf optique par œil. Les deux nerfs se croisent dans une zone appelée chiasma optique. À cet endroit s'entrecroise une partie seulement des fibres selon la figure (II, 2). [1]

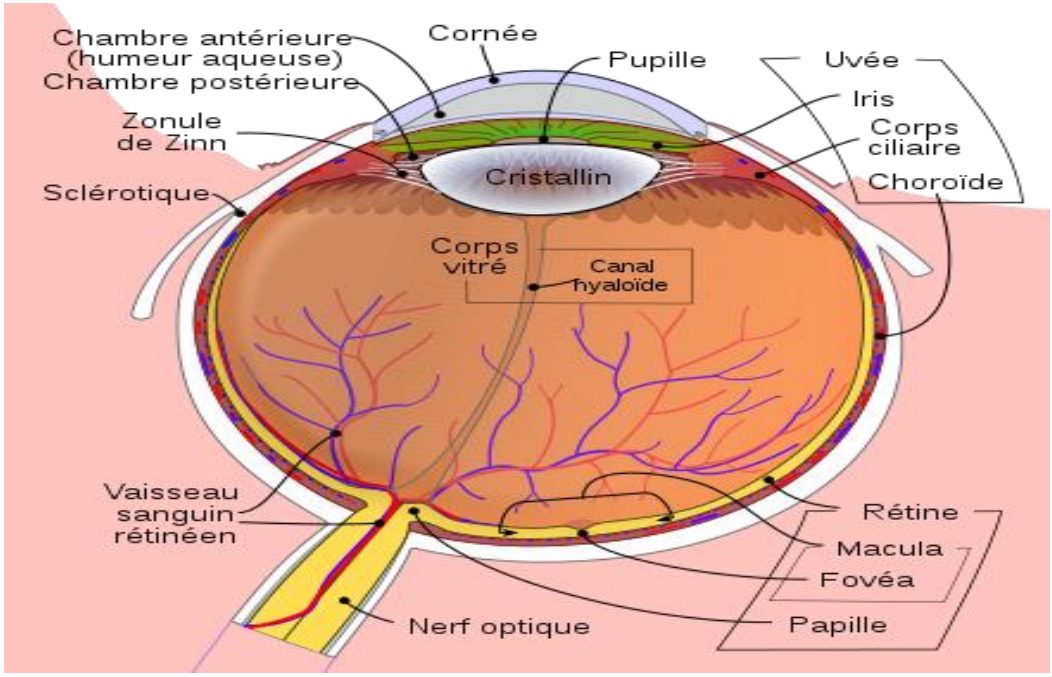


Figure (II, 2): anatomie de l'œil

II.3. Définition de l'iris :

En grec le mot 'IRIS 'désigne : Arc-en-ciel, spectre des couleurs ; reflets, teintes imitant les couleurs de l'arc-en-ciel.

L'Iris (nom masculin) est un genre de plantes vivaces à rhizomes ou à bulbes de la famille des Iridacées. Le genre Iris contient 210 espèces et d'innombrables variétés horticoles. [1]

On anatomie de l'œil c'est un disque coloré de la partie antérieure de l'œil, visible à travers la cornée, placé devant le cristallin et percé en son centre d'un orifice à diamètre variable.

La pupille, C'est une ouverture circulaire à diamètre variable obtenue par un ensemble de lamelles réglables, utilisée comme élément de diaphragme ou comme cache [2]. Il se dilate ou se contracte par réflexe naturel pour adapter l'œil à son environnement lumineux. Chaque iris est unique et les variantes possibles de couleurs sont infinies. [3]

La couleur de l'iris est déterminée par la quantité de mélanine qu'elle contient. Cette affection est caractérisée par une sensibilité exagérée de l'œil à la lumière ; de là une contraction spasmodique de l'iris, quelquefois avec occlusion complète de la pupille, de sorte que les personnes nyctalopes voient très-bien pendant la nuit, mais cessent de voir pendant le jour. [4]

II.4. L'historique de la biométrie par l'iris :

Les premières traces d'une proposition d'utilisation du motif de l'iris comme moyen de reconnaissance remontent à un manuel d'ophtalmologie écrit par James Doggarts et datant de 1949. On dit même que l'ophtalmologiste Frank Burch en avait émis l'idée dès 1936. [4]

Durant les années 80, l'idée reparut dans différents films de James Bond (Never Say Never Again, 1993), mais elle restait du domaine de la science-fiction. Ce n'est donc qu'en 1987 que deux ophtalmologistes (Aran Safir et Leonard Lom) déposèrent un brevet sur cette idée et demandèrent à John Daugman (enseignant à cette époque à l'université de

Harvard) d'essayer de trouver un algorithme d'identification basé sur le motif de l'iris. Cet algorithme a été breveté en 1994. Il est la base de tous les systèmes de reconnaissance d'iris actuels. La personne qui cherche à se faire identifier doit simplement fixer l'objectif d'une caméra qui récupère instantanément le dessin de son iris.

L'iris est un motif très dense et qui n'est pas dicté par les gènes. Chaque œil est unique. Dans toute photographie de l'iris, on compte plus de 200 variables indépendantes, ce qui fait une probabilité très faible de confondre 2 individus. On doit cette méthode à quelques ophtalmologues qui ont remarqué dès les années 80, que la couleur de l'iris peut varier, mais rarement son motif. Cette méthode d'identification évoluera certainement avec le temps, probablement autant que les empreintes digitales, au moins autant que l'évolution des caméras Pour capturer l'image de cette membrane colorée, pas besoin d'éclairer la rétine. [4]

Par contre, l'éclairage de l'iris pose un problème de reflets, on utilise souvent un éclairage artificiel (diodes DEL) calibré tout en atténuant le plus possible l'éclairage ambiant. L'éclairage est d'autant mieux toléré qu'il peut être infrarouge, peu visible pour l'œil. Le système peut être trompé à partir d'une photo ou d'une lentille de contact reproduisant l'iris de la personne dont on souhaite usurper l'identité. Mais la résolution demandée est très importante (distance iris / caméra faible, évolution rapide de la technologie des capteurs CCD/CMOS). [4]

De plus il est possible de repérer, par filtrage, que l'iris présenté et constitué d'une suite régulière de points et non d'un motif varié. Enfin, il existe de nombreuses techniques qui permettent de s'assurer que l'iris présenté est humain (ou très ressemblant) :

- Si l'on fait varier l'éclairage, le diamètre de la pupille varie. Les temps de latence et vitesse de variation sont mesurables.
- Il est possible d'éclairer des U.V. à l'I.R. et d'observer les images obtenues. L'œil est opaque dans l'IR lointain (proche du thermique) ainsi qu'aux UV.

Ainsi, il semble difficile de fabriquer un faux iris complet (variations de la pupille, réactivité à l'IR…)

La biométrie par l'iris est une des technologies (avec la rétine) qui assure un haut niveau de sécurité.

L'iris procure une unicité très élevée (1 sur 10 puissance 72) et sa stabilité est étendue jusqu'à la mort des individus, d'où une fiabilité extraordinaire. [4]

II.5. Les caractéristiques de l'iris :

La formation de l'iris pour un œil humain 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 : la formation de l'iris est chaotique, on a donc des motifs avec de fortes variabilités. 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 taches 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 fixes, 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 (Acide Désoxyribonucléique), 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 parents, 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, qui n'est pas pourtant exposé à d'éventuels dommages. Cependant comme 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 et l'iris est suffisamment varié pour qu'il ne soit pas indispensable de recueillir toutes les informations qu'il contient. [5] (voir la figure (II, 3)).

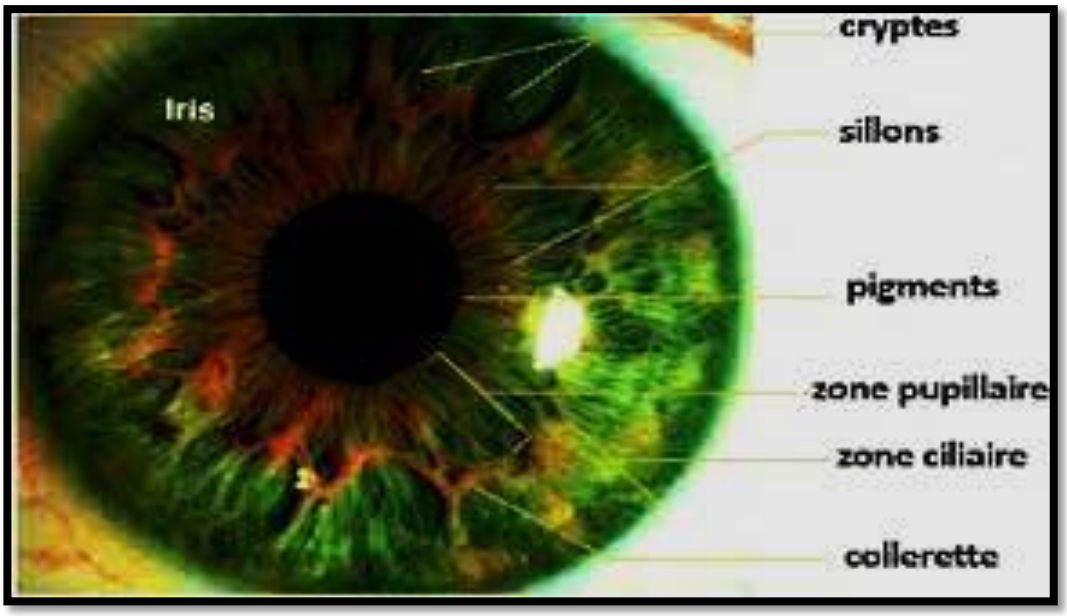


Figure (II, 3) : Les composants de l'iris

II.6. L'état de l'art :

De nombreuses recherches ont été suggérées dans la littérature pour révéler les principaux éléments de l'iris et pour faire des systèmes performants et précis et fiables.
Nous mentionnerons quelques-unes des œuvres que nous avons rencontrées au cours de nos recherches :

1. EN janvier 2022, Thukral, A., & al. Ils utilisent des méthodes d'extraction de caractéristiques des filtres Gabor et des bacs HOG (histogramme de gradient) et des machines à vecteurs de support (SVM) comme classificateur dans le mécanisme conçu qui peut aider à détecter les attaques d'impression de l'iris à différents niveaux de sécurité, et de manière efficace et conviviale. Le résultat de cette approche est capable de fonctionner avec de très bonnes performances sous différents systèmes biométriques (multi-

biométrique) et pour divers scénarios de spoofing, mais il offre également une haute sécurité contre certaines attaques non spoofing (multi-attaques). [6]

2. En 2021, Labati, R. D & al. Ont présenté un ensemble de données d'images publiques appelé I-SOCIAL-DB (Iris Social Database). Cet ensemble de données est composé de 3 286 régions oculaires, extraites de 1 643 images de visage haute résolution de 400 individus, collectées sur des sites Web publics. Pour chaque région oculaire, un expert humain a extrait les coordonnées des cercles se rapprochant des limites intérieure et extérieure de l'iris et a effectué une segmentation pixel par pixel des contours, des occlusions et des réflexions de l'iris. Cet ensemble de données est la première collection d'images oculaires provenant de sites Web publics et de médias sociaux, et l'une des plus grandes collections d'images oculaires segmentées manuellement dans la littérature. Ils ont proposé une analyse qualitative des échantillons, un ensemble de protocoles de test et de chiffres de mérite, et des résultats de référence obtenus à l'aide d'algorithmes de segmentation et de reconnaissance de l'iris accessibles au public. On conséquence, ils ont donné un nouvel outil de test à la communauté de la recherche biométrique. [7]

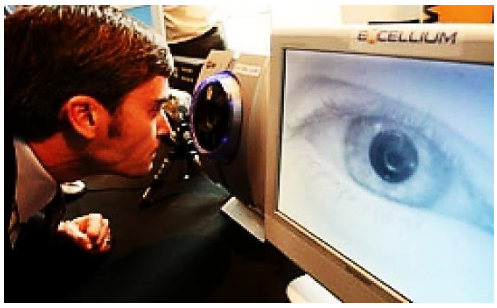
3. En 2022, Phillips, S., & al. Ils ont présenté une étude qui compare non seulement les résultats de systèmes entraînés avec des images frontales par rapport à des images hors angle, mais également les résultats d'images avec un nombre élevé de pixels dans la texture de l'iris par rapport à des images avec un faible nombre de pixels(dans la texture de l'iris c'est-à-dire péri-oculaire ou oculaire).Ils ont étudié les effets de l'angle du regard et de la distance à la caméra sur la reconnaissance en utilisant différentes tailles et angles d'images. À l'aide de réseaux de neurones convolutés. Ils ont formé et testé la méthode proposée avec un ensemble de données d'iris hors angle avec 11 000 images. [8]

4. En 2022, Zambrano, J. E & al. Ils ont proposé une méthode de reconnaissance rapide de l'iris qui nécessite une seule opération d'appariement et est basée sur des modèles de classification d'images pré-entraînés en tant qu'extracteurs de caractéristiques. Leur approche utilise les filtres des premières couches des réseaux de neurones convolutés comme extracteurs de caractéristiques et ne nécessite pas d'ajustement pour les nouveaux ensembles de données. Étant donné que leurs caractéristiques sélectionnées extraites de couches convolutionnelles codent la surface de l'iris, elles ont l'avantage de ne pas être limitées à des positions spatiales spécifiques, il n'est pas nécessaire d'effectuer un processus de décalage de bits dans l'étape d'adaptation, éliminant un nombre important de calculs. De plus, pour atténuer l'effet produit par la bordure de masque dans les images en feuille de caoutchouc, nous proposons de filtrer les tenseurs de carte de caractéristiques en masquant leurs canaux et en sélectionnant les caractéristiques les plus pertinentes. Leur méthode a été évaluée sur les ensembles de données accessibles au public CASIA Iris Lamp et CASIA Iris Thousand, et a montré une amélioration significative à la fois en termes de précision et de temps de correspondance. [9]

II.7. Conception générale d'un système de reconnaissance par l'iris:

Un système de reconnaissance de l'iris est un système automatique de reconnaissance de formes qui se peut composer de plusieurs étapes comprenant :

- **L'acquisition :**



L'iris sera capturé et stocké sous forme d'image [10]. L'acquisition s'effectue généralement avec une caméra monochrome dans le domaine du proche infrarouge. Idéalement, le diamètre de l'iris au sein de l'image acquise doit être approximativement compris entre 200 et 300 pixels pour s'assurer d'un minimum de détail au cœur même de l'iris. [11] L'image d'iris se fait avec une caméra, soit avec une caméra infrarouge ou une caméra à lumière visible. Comme la montre La figure (II, 4) :

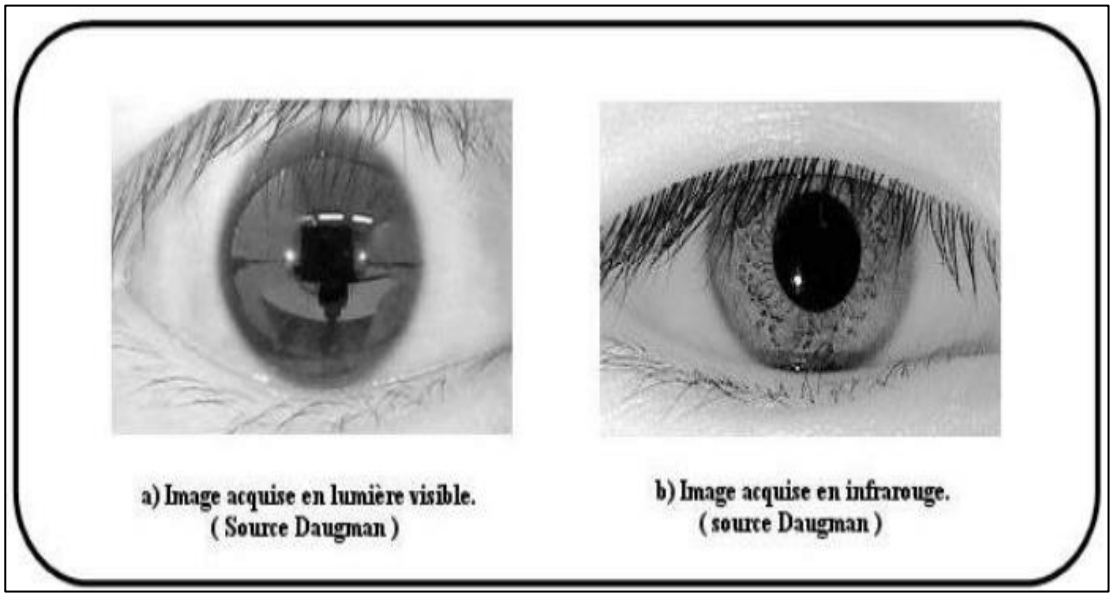


Figure (II, 4) : Image d'iris capturée par une caméra infrarouge et une caméra à lumière visible.

- **La segmentation :**

Après l'acquisition de l'image, l'iris doit être isolé. Dans un premier temps, une série d'opération d'amélioration de l'image peuvent être appliquée. Ces opérations de prétraitement sont de type filtrage passe haut, amélioration du contraste et égalisation d'histogramme et seuillage automatique…etc.

Leurs buts sont de rehausser la qualité globale de l'image pour appliquer ensuite les opérations de segmentation de l'iris.

La segmentation de l'iris sera ainsi définie par l'ensemble de traitement nécessaire pour extraire l'iris se son milieu environnant : pupille, blanc de l'œil, paupières, cils et réflexions spéculaires. Elle est considérée comme l'étape la plus difficile du système de reconnaissance et son degré de fiabilité affecte très signifiant la performance du système.

Deux grandes approches existent dans la bibliographie de ce processus. Elles sont basées sur des approximations circulaires ou elliptiques, ou sur la détection par des contours en forme libre tels que les contours actifs et les méthodes statistiques. [12]

- **La normalisation:**

L'iris est un disque percé à l'intérieur par un autre disque plus petit, la pupille. Les deux cercles que constituent les frontières de l'iris avec le blanc de l'œil, ainsi que les frontières de la pupille avec l'iris ne sont pas parfaitement concentriques.
De plus, avec les contractions et les dilatations de l'iris ainsi que la variation des distances d'acquisition entre les personnes et l'objectif, la taille du disque de l'iris n'est pas toujours constante.

La normalisation permet de transformer le disque irrégulier de l'iris en une image circulaire de taille constante.

- **L'extraction des caractéristiques d'iris:**

C'est l'extraction des caractéristiques pertinentes de l'image normalisée de l'iris des points, des vecteurs ou des coefficients caractéristiques de la personne.

- **L'encodage :**

Dans cette étape, l'iris est bien segmenté et normalisée. L'encodage consiste à extraire de l'iris les caractéristiques les plus discriminantes et les plus pertinentes, nécessaires et utiles pour son identification. Des filtres de type passe-bande, des ondelettes, et d'autres outils peuvent ainsi être utilisés. Le résultat obtenu peut être gardé dans des valeurs réelles ou peut être quantifié en valeurs discrètes. Le processus de l'encodage de l'iris résulte finalement en un profil d'iris représentant la signature de l'iris. Ce profile est unique pour chaque iris, insensible aux variations de dimensions ou aux rotations crées lors de l'acquisition de l'iris et sera utilisé ensuite pour la classification de l'iris. (Cette étape n'est pas nécessaire). [10] [13]

- **La comparaison:**

Les caractéristiques acquises sont comparées avec les caractéristiques stockées dans une base de données et à partir du résultat de cette comparaison une décision est prise, cette étape est un élément clef du traitement [10]. voir la figure (II, 5).

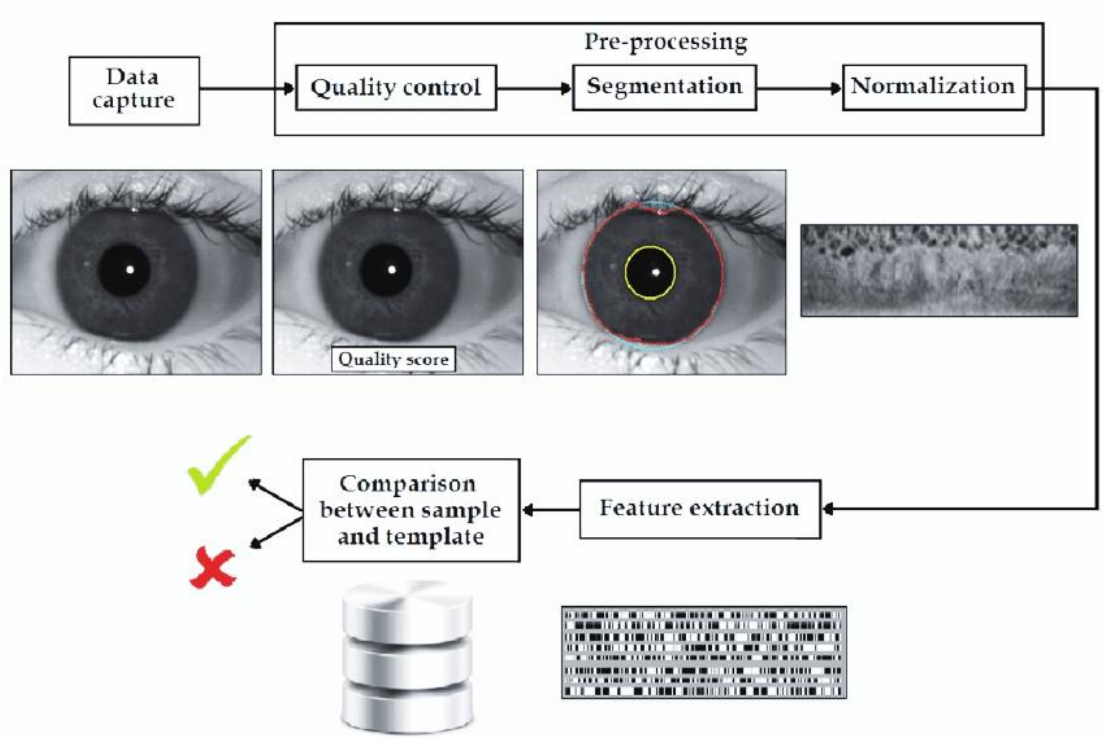


Figure (II, 5) : les étapes d'un système de reconnaissance d'iris.

En général, la vérification biométrique consiste deux étapes : inscription (enrôlement) et authentification.

Durant l'inscription, la biométrie de l'utilisateur est capturée (acquisition) et les caractéristiques extraites (Template ou signature) sont sauvegardées sur une base de données.

Durant l'authentification, la biométrie de l'utilisateur est de nouveau capturée et les attributs extraits sont comparés avec ceux qui existent déjà dans la base de données pour déterminer la correspondance.

L'enregistrement spécifique choisit pour la comparaison est déterminé en fonction de l'identité acclamée par l'utilisateur. (Voir la Figure (II, 6)).

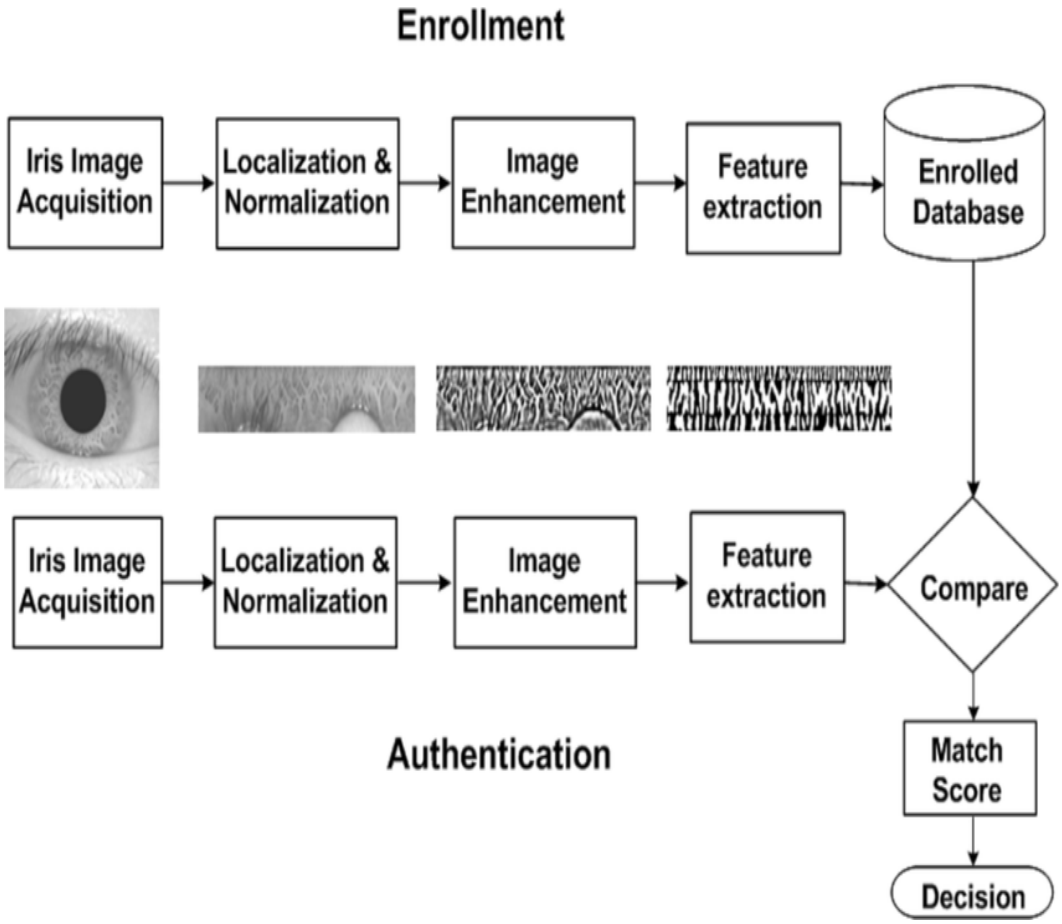


Figure (II, 6) : l'identification et l'authentification d'un système biométrique d'iris.

II.8. Quelques méthodes existantes de reconnaissance par l'iris:

Il y'a plusieurs méthodes pour reconnaître l'iris, parmi ces méthode on cite les suivantes:

II.8.1. La transformée de Hough:

L'iris est utilisé comme référence pour l'étude des marques biométriques uniques chez les personnes. L'analyse de la façon d'extraire les informations caractéristiques de l'iris représente un défi fondamental dans l'analyse d'images, en raison des implications qu'elle présente : détection d'informations pertinentes, schémas de codage des données…etc. Pour

cette raison, dans la recherche d'extraction d'informations utiles et caractéristiques, des approximations ont été proposées pour son analyse.

Cette transformée aide à trouver des géométries primitives dans les iris, qui sont utilisées pour caractériser chacun d'eux.

La transformée de Hough consiste à construire un espace paramétrique de structures géométriques régulières. Les zones maximales de cet espace désignent les régions avec une forte probabilité de trouver ces structures. Diverses investigations ont montré qu'il est possible de détecter des figures différentes.

Depuis, ont été mises en œuvre pour la reconnaissance et la segmentation de l'iris. Cette tâche peut être facilitée si sa morphologie circulaire est prise en compte et si les images sont correctement préparées avant de passer à la phase de traitement.

L'utilisation de la morphologie des objets circulaires envisageant différentes conditions dans l'acquisition, ainsi que l'obstruction possible avec des objets entourant l'iris. Des techniques de traitement d'images numériques sont utilisées telles que : transformation en niveaux de gris, négatif et binarisation.

Cette méthode est appliquée pour la détection des bords et des circonférences, respectivement [14]. (Voir la figure (II, 7))

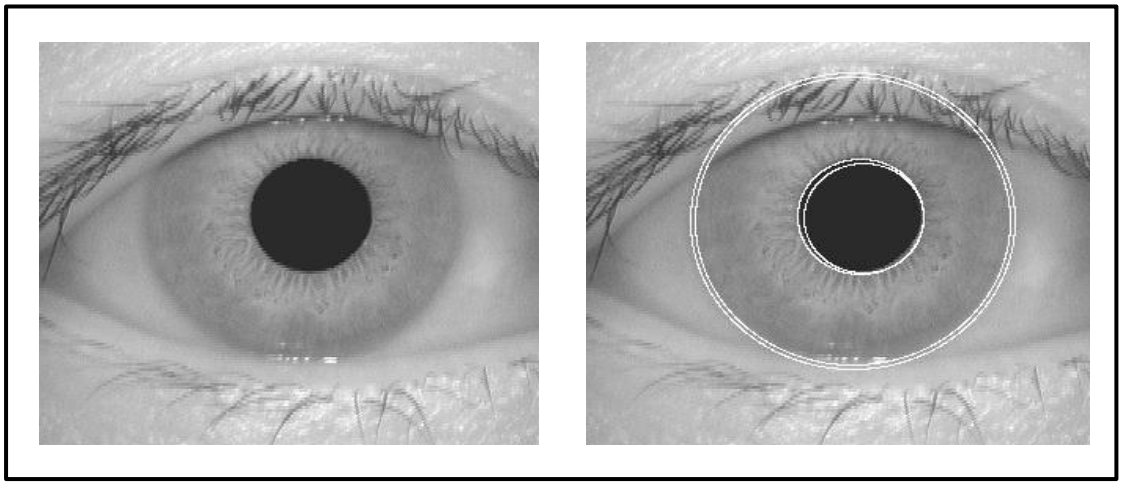


Figure (II, 7) : Notre essai du transformée de Hough
de la base de données Casia V1

II.8.2. Filtre Canny :

En 1986, John Canny a proposé un filtre ou un détecteur en traitement d'image pour détecter les contours, cet algorithme a trois critères sont les suivants :

1) Une bonne détection : un faible taux d'erreur dans la signalisation des contours,
2) Une bonne localisation : minimiser les distances entre les contours détectés et les contours réels.
3) LA clarté de la réponse : une seule réponse par contour et pas de faux positifs.

- **Réduction du bruit :**

Avant de détecter les contours il est nécessaire de réduire le bruit de l'image originale la réduction du bruit c'est l'élimination les pixels isolés qui pourraient induire de fortes réponses lors du calcul du gradient, conduisant ainsi à de faux positifs.

Un filtrage **gaussien** 2D est utilisé, l'opérateur de convolution est le suivant :

$$\mathbf{G}(\mathbf{x},\mathbf{y}) = \frac{\mathbf{1}}{\mathbf{2\pi\sigma^2}}\ e^{\left(-\frac{\mathbf{x^2+y^2}}{\mathbf{2\sigma^2}}\right)} \qquad \textbf{(II, 1)}$$

Et un exemple de masque 5 * 5 discret avec $\boldsymbol{\sigma} = \mathbf{1.4}$

$$\mathbf{h} = \frac{\mathbf{1}}{\mathbf{159}} \begin{bmatrix} \mathbf{2} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{2} \\ \mathbf{4} & \mathbf{9} & \mathbf{12} & \mathbf{9} & \mathbf{4} \\ \mathbf{5} & \mathbf{12} & \mathbf{15} & \mathbf{12} & \mathbf{5} \\ \mathbf{4} & \mathbf{9} & \mathbf{12} & \mathbf{9} & \mathbf{4} \\ \mathbf{2} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{2} \end{bmatrix} \qquad \textbf{(II, 2)}$$

Le filtre est de taille plus réduite que l'image filtrée. Plus le masque est grand, moins le détecteur est sensible au bruit et plus l'erreur de localisation grandit.

- **Gradient d'intensité :**

Pour retourner l'intensité des contours il faut appliquer un gradient, l'opérateur utilisé permet de calculer le gradient suivant les directions X et Y, il est composé de deux masques de convolution, un de dimension 3 × 1 et l'autre 1 × 3 :

$$|\mathbf{Gx}| = [-\mathbf{1}\ \ \mathbf{0}\ \ \mathbf{1}] \quad ; \quad \mathbf{Gy} = \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \\ -\mathbf{1} \end{bmatrix} \qquad \textbf{(II, 3)}$$

La valeur du gradient en un point est approximée par la formule:

$$|\mathbf{G}| = |\,\mathbf{Gx}\,| + |\,\mathbf{Gy}\,| \qquad \textbf{(II, 4)}$$

Et la valeur exacte est:

$$|\mathbf{G}| = \sqrt{\boldsymbol{Gx^2} + \boldsymbol{Gy^2}} \qquad \textbf{(II, 5)}$$

Les orientations des contours sont déterminées par la formule :

$$\boldsymbol{\theta} = \pm \mathbf{arctan}\,\frac{\mathbf{Gy}}{\mathbf{Gx}} \qquad \textbf{(II, 6)}$$

Finalement on obtient une carte des gradients d'intensité en chaque point de l'image accompagnée des directions des contours.

- **Suppression de non maxima :**

Une forte intensité indique une forte probabilité de présence d'un contour. Cette intensité n'est pas suffisante pour dire que le point correspond à un contour ou non. Les points correspondant à des maximas locaux sont considérés comme correspondant à des contours, Un maximum local est présent sur les extrema du gradient, c'est-à-dire là où sa dérivée selon les lignes de champs du gradient s'annule.

- **Seuillage des contours :**

Le seuillage à hystérésis faire la différenciation des contours sur la carte générée, ce seuillage nécessite deux seuils : un haut ou un bas. Ces deux seuils seront comparés à l'intensité du gradient de chaque point.

Pour chaque point, si l'intensité de son gradient est :

❖ Inférieur au seuil bas, le point est rejeté ;

❖ Supérieur au seuil haut, le point est accepté comme formant un contour ;

❖ Entre le seuil bas et le seuil haut, le point est accepté s'il est connecté à un point déjà accepté.

Si en suivi toutes les étapes citées, l'image obtenue est binaire avec d'un côté les pixels appartenant aux contours et les autres. Les deux paramètres principaux déterminant le temps de calcul et l'acuité de l'algorithme sont la taille du filtre gaussien et les deux seuils.

Le filtre utilisé pour réduire le bruit a une influence directe sur le comportement de l'algorithme. Si le filtre est :

✓ De petite taille : il produit un effet de flou moins prononcé, ce qui permet la détection de petites lignes bien marquées.

✓ De taille plus grande produit un effet de flou plus important, ce qui permet de détecter des contours moins nets, par exemple celui d'un arc-en-ciel.

✓ Seuils : l'utilisation de deux seuils au lieu d'un améliore la flexibilité mais certains problèmes propres au seuillage demeurent. Ainsi,

- Un seuil trop bas : peut conduire à la détection de faux positifs.
- Un seuil trop haut : peut empêcher la détection de contours peu marqués mais représentant de l'information utile.

Actuellement, Il n'existe pas de méthode générique pour déterminer des seuils produisant des résultats satisfaisants sur tous les types d'images. Il existe des méthodes statistiques permettant d'obtenir automatiquement une valeur du seuil haut convenable, la valeur du seuil bas étant un pourcentage du seuil haut. [15]

Figure (II, 8) : Filtre de Canny

II.8.3. Décomposition en ondelettes de Haar :

En traitement d'image, les ondelettes orthogonales sont très utilisées car elles conduisent à des calculs rapides. Le signal est décomposé en une approximation et un détail dans le cas d'un signal d'une dimension (1D), en deux dimensions (2D), l'image est décomposée en une approximation et trois détails (horizontal, diagonal et vertical).En utilisant les ondelettes de Haar illustrées dans la figure (II, 9) {une fonction de base pour extraire les caractéristiques de la région de l'iris}. [16]

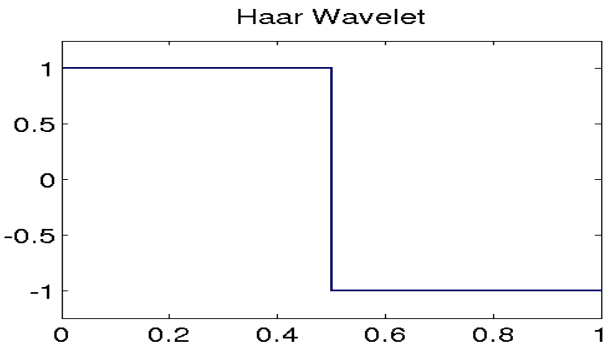


Figure (II, 9) : Les ondelettes de Haar

II.8.4. Filtre de Gabor :

Représente un filtre de Gabor linéaire sensible aux textures avec une longueur d'onde et une orientation spécifiées. On peut utiliser la fonction Gabor pour créer un seul filtre Gabor ou une banque de filtres Gabor.

Une banque de filtres est un ensemble de filtres représentant des combinaisons de multiples longueurs d'onde, d'orientations et d'autres paramètres facultatifs. Par exemple, si vous spécifiez deux longueurs d'onde et trois orientations, la banque de filtres Gabor est composée de six filtres pour chaque combinaison de longueur d'onde et d'orientation. Pour appliquer un filtre Gabor ou une banque de filtres Gabor à une image, utilisez la fonction « imgaborfilt ». [17]

II.8.5. La méthode Daugman :

Daugman a proposé une méthode de détection de l'iris dans l'image de l'œil. Il l'a détecté au moins les pixels formants la frontière entre l'iris et la pupille, et la sclérotique par la méthode d'opérateur intégro-différentiel.

Il a aussi développé une méthode pour normaliser la forme de l'iris «Rubber Sheet » qui décrite comme une tentative d'étendre le disque de l'iris comme du caoutchouc, elle est nommé pseudo-polaire grâce à des cercles d'iris et de pupille qui n'ont pas le même centre. En plus, il a utilisé un banc des filtres de Gabor qui permet d'extraire des informations pertinentes relatives à la texture d'image de l'iris normalisé. [18]

On explique les étapes de cette méthode par :

- **L'opérateur intégro-différentiel :**

L'expression suivante explique la proposition de la méthode de détection de l'iris, de la pupille et des paupières:

$$\mathbf{Max}_{(r,x0,y0)} \left| G_\sigma(r) * \frac{\partial}{\partial} \phi_{(r,x0,y0)} \frac{I(x,y)}{2\pi r} ds \right. \qquad \textbf{(II, 7)}$$

I (x, y): est l'image de l'œil

r: le rayon du cercle que l'on est en train de chercher

G_σ (r): est une fonction gaussienne de lissage

L'opérateur faire 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, il est appliqué de manière itérative avec un degré de lissage afin d'atteindre une détection précise. Il a détecté Les paupières de la même façon, il utilise des rayons très grands et des arcs de cercles. [19]

La méthode intégro-différentielle est une généralisation de la méthode de la transformée de Hough, elle utilise une image gradient et rechercher un contour géométrique bien défini. Puis elle utilise l'image gradient sans seuillage.

Par contre, elle est plus sensible aux bruits parce qu'ils rendent les gradients très forts et engendre la moyenne du gradient fausse sur un cercle et attirer le contour vers leurs positions.

- **Méthode pseudo-polaire :**

La dilatation et la contraction de la pupille rendre la forme de l'iris irrégulière, au fait des changements non linéaires de la texture de l'iris. A chaque pixel de l'iris dans le domaine cartésien lui est assigné un correspondant dans le domaine pseudo polaire suivant la distance du pixel par rapport aux centres des cercles et l'angle qu'il fait avec ces centres. [20]

La transformation se fait comme suite :

$$x(r,\theta) = (1-r)\, x_p(\theta) + r x_s(\theta)$$
$$y(r,\theta) = (1-r)\, y_p(\theta) + r y_s(\theta) \qquad \textbf{(II, 8)}$$

$\boldsymbol{x_p(\theta)}$**:** représente l'abscisse du point de la frontière détectée de la pupille dont le segment qui passe par ce point et le centre de la pupille fait un angle θ avec une direction choisie.

$\boldsymbol{y_p(\theta)}$**:** représente l'ordonné de ce même point.

$\boldsymbol{x_s(\theta)}$**:** représente les coordonnées des points obtenus par le même principe mais sur le contour de l'iris.

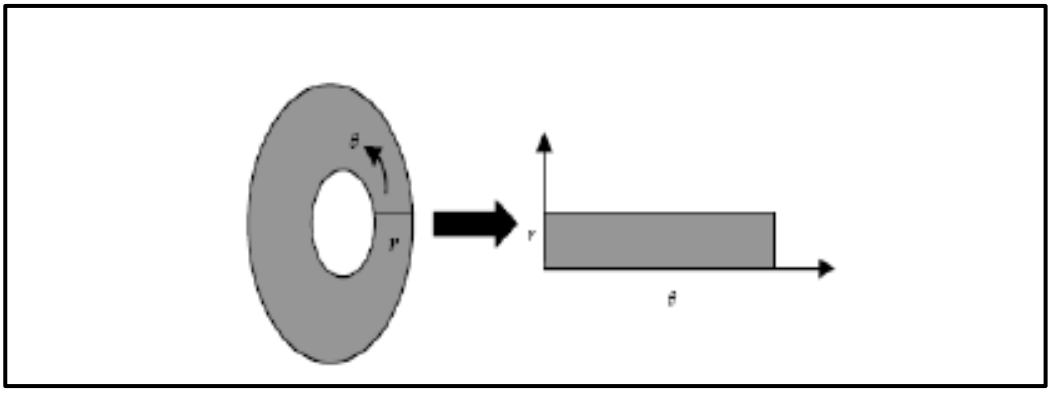


Figure (II, 10) : transformée pseudo polaire

II.8.6. La morphologie mathématique :

Le filtrage morphologique repose sur la morphologie mathématique, basée sur une description ensembliste des images.

Les opérateurs morphologiques privilégient la notion de forme plutôt que l'information sur l'amplitude des signaux. Ils s'appliquent aussi bien aux images binaires (deux niveaux : blanc ou noir) qu'aux images monochromes (en niveaux de gris), en utilisant son histogramme pour choisir un seuil adéquat.

L'image binaire est obtenue par une numérisation dont la quantification ne comporte que deux niveaux de reconstruction, elle est une image pour laquelle les pixels (m, n) n'ont que deux valeurs de luminance L (m, n) possibles, notées conventionnellement 0 (fond) et 1 (formes). [21]

On définit donc les formes 'X' comme étant l'ensemble des points 'P' d'affixe 'p', appartenant au support 'S'de l'image, tel que la luminance en ces points soit égale à 1 :

$$X = \{ p \in S \,/ L(p) = 1 \} \qquad \textbf{(II, 9)}$$

- **Filtrage morphologique:** Les opérateurs morphologiques travaillent aussi sur le voisinage local de chaque pixel. La forme de ce voisinage est appelé élément structurant. Pour les filtres linéaires ou médians, on peut utiliser des éléments structurants de taille et de forme variée.

- **L'élément structurant:** est un ensemble de pixels à 1. Le point O de coordonnées (0, 0).

- **La dilatation:** consiste à déplacer l'élément structurant sur chaque pixel de l'image, et à regarder si l'élément structurant touche la structure d'intérêt, la formule de la dilatation est :

$$\mathbf{A \circ B} \triangleq (\mathbf{A} \ominus \mathbf{B}) \oplus \mathbf{B} \qquad \textbf{(II, 10)}$$

- **L'érosion:** est l'opération inverse, qui est définie comme une dilatation du complémentaire de la structure. Elle consiste à chercher tous les pixels pour lesquels l'élément structurant centré sur ce pixel touche l'extérieur de la structure. Le résultat est une structure rognée, sa formule est la suivante :

$$\mathbf{A} \oplus \mathbf{B} \triangleq \left\{ \mathbf{z} \mid \left(\widehat{\mathbf{B}} \right)_{\mathbf{z}} \cap \mathbf{A} \neq \varnothing \right\} \qquad \textbf{(II, 11)}$$

- **La fermeture morphologique** : est une dilatation suivie d'une érosion. La fermeture a pour effets :

✓ de faire disparaître les trous de petite taille dans les structures.

✓ De connecter les structures proches. (Lissage du contour de A).

Sa formule est:

$$\mathbf{A} \ominus \mathbf{B} \triangleq \{ \mathbf{z} \mid (\mathbf{B})_{\mathbf{z}} \subseteq \mathbf{A} \neq \varnothing \} \qquad \textbf{(II, 12)}$$

- **L'ouverture morphologique** : est une érosion suivie d'une dilatation. L'ouverture a pour effets :

✓ de faire disparaître les petites particules (dont la taille est inférieure à celle de l'élément structurant)

✓ de séparer les grosses particules aux endroits où elles sont plus fines.

Sa formule est:

$$\mathbf{A} \bullet \mathbf{B} \triangleq (\mathbf{A} \oplus \mathbf{B}) \ominus \mathbf{B} \qquad \textbf{(II, 13)}$$

- **Segmentation avec opérateurs morphologiques :** On appelle segmentation d'une image l'opération consistant à séparer une image en un ensemble de régions disjointes deux à deux, et dont l'union recouvre l'image d'origine. On distingue deux types d'approches pour la segmentation : contour ou région. Il faut isoler le ou les contours des objets d'intérêt, le résultat se présente en général sous la forme d'un ensemble de chaînes de pixels, et des traitements additionnels sont souvent nécessaires pour associer les contours aux objets d'intérêt, et à identifier des régions de pixels homogènes au sein de l'image, le critère d'homogénéité peut être l'intensité, la couleur, ou même la texture locale, le résultat se présente soit sous la forme d'une image binaire, ou d'une image étiquetée, chaque étiquette ou label correspondant à une région. [21]

II.9. Conclusion :

Dans ce chapitre nous avons cité quelques méthodes biométriques de reconnaissance, des problèmes qui en découlent et les caractéristiques d'iris, nous avons également présenté la structure globale d'un système de reconnaissance d'iris et les performances de ce système.

Dans la suite de ce travail nous allons détailler notre contribution dans le cadre de la proposition d'une nouvelle méthode biométrique d'iris, et résoudre quelques problèmes des méthodes de reconnaissance d'iris existantes.

Partie Pratique

Chapitre III : Application et résultats obtenus

Sommaire : Chapitre III

III.1. Introduction :

La reconnaissance de l'iris est une des applications biométriques les plus performantes côté résultat.

Le système de reconnaissance de l'iris est un système biométrique qui est basé sur plusieurs méthodes grâce à des bases de données disponibles.

Dans ce chapitre, nous présenterons les méthodes que nous avons utilisées dans notre programmation qui incluent le prétraitement de l'image de l'iris, la segmentation automatique, la normalisation et nous avons fait la comparaison dimensionnelle dans la dernière étape.

III.2. Présentation des bases de données des images d'iris :

Pour obtenir des images plus précises et crée une base de données performante, cela nécessite un long temps, un travail acharné et en plus d'une recherche continue pour atteindre la taille de base de données d'images requise et les informations importantes et suffisantes qu'elle contient. Pour cela, les chercheurs ont pu collecter des images d'iris de qualité et en faire une base de données valable pour leur traitement et la possibilité de les utiliser comme référence, par exemple la base de données **: CASIA V1.0**, **UBIRIS v1**, **UPOL**…etc.

III.2.1. Base de données CASIA (version 1.0) :

Les bases de données d'images d'iris CASIA se compose de 756 images d'iris d'intensité 320*280 de 108 yeux capturées à l'aide d'un capteur développé en interne. Les images sont stockées sous forme de fichiers « .JPEG » au niveau de gris de 8 bits, sept images sont capturées pour chaque œil au cours de deux sessions, trois lors de la première session et quatre lors de la seconde session. [1]

On a quelques images de cette base de données dans la (figure III, 1) :

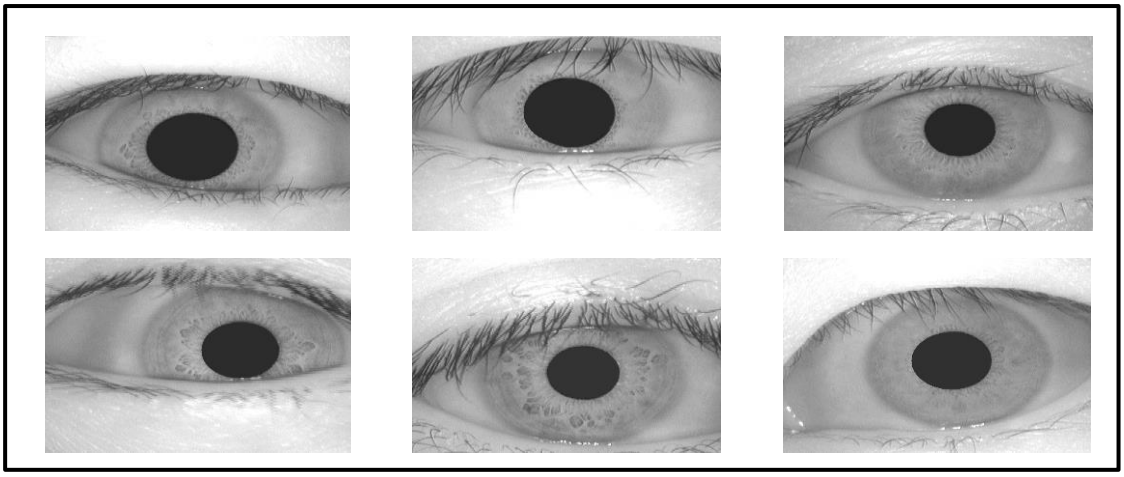


Figure (III, 1): des images de base de données CASIA V1.0

III.2.2. Base de données MMU :

La base de données de l'Université multimédia (MMU1) est une base de données publique composée des images oculaires pour les modèles de formation du système de présence biométrique basé sur IRIS. Les motifs IRIS pour chaque œil sont uniques pour chaque individu, ce qui est utile pour identifier un individu.

Cette base de données se compose de 450 images chacune d'IRIS gauche et droit de 320*240 pixels au format « .BMP » en niveaux de gris 24 bits, toutes les images ont été utilisées dans les expériences [2]. (Voir la figure (III, 2))

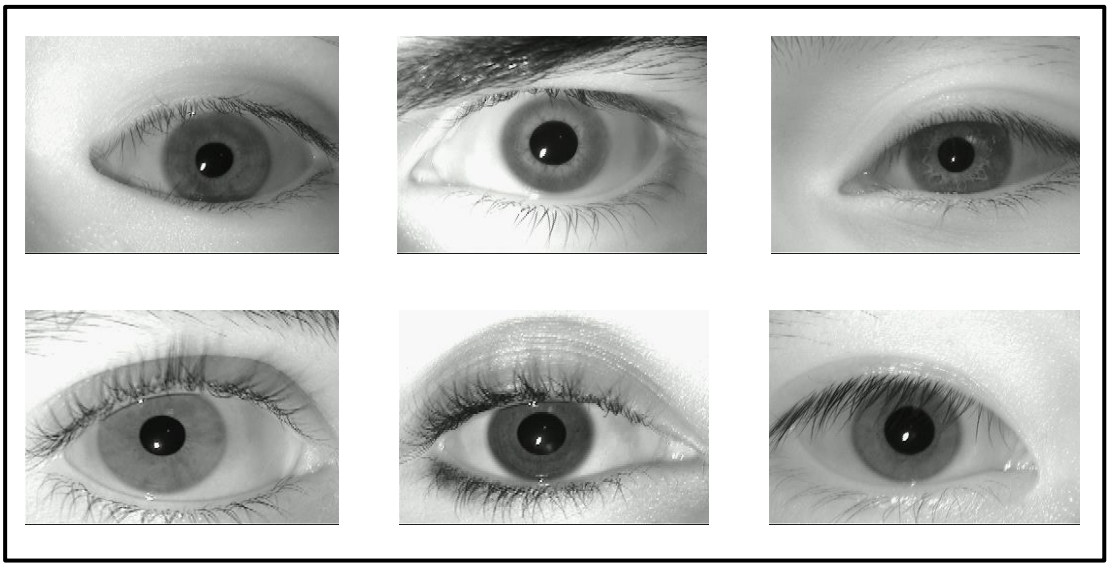


Figure (III, 2): des images de base de données MMU

III.2.3. Base de données UPOL :

Cette base de données contient 384 images d'iris, à gauche on a 192 images et aussi à droite. Les images sont : 24 bits - RVB, avec 576*768 pixels, d'un format de fichier « .PNG ». Les iris ont été scannés par un dispositif optique TOPCON TRC50IA connecté à une caméra SONY DXC-950P 3CCD [3]. **(**Figure (III, 3))

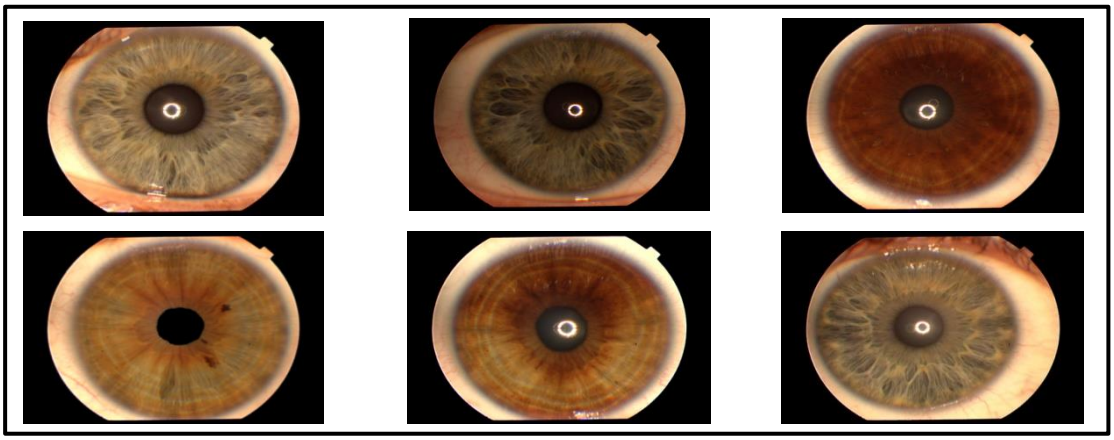


Figure (III, 3): des images de base de données UPOL

III.2.4. Base de données UBIRIS v1 :

La base de données UBIRIS v1 est composée de 1877 images collectées après de 241 personnes, en deux sessions distinctes. Elle a été prise par des paramètres: l'appareil photo Nikon E5700, logiciel E5700v1.0, Les couleurs RVB, distance focale 71 mm, temps d'exposition 1/30 sec, vitesse ISO ISO-200, images Largeur 2560 pixels, hauteur 1704 pixels, résolution horizontale 300 dpi, résolution verticale 300 dpi, profondeur de bits 24 et d'un Format JPEG [4]**. (**Figure (III, 4))

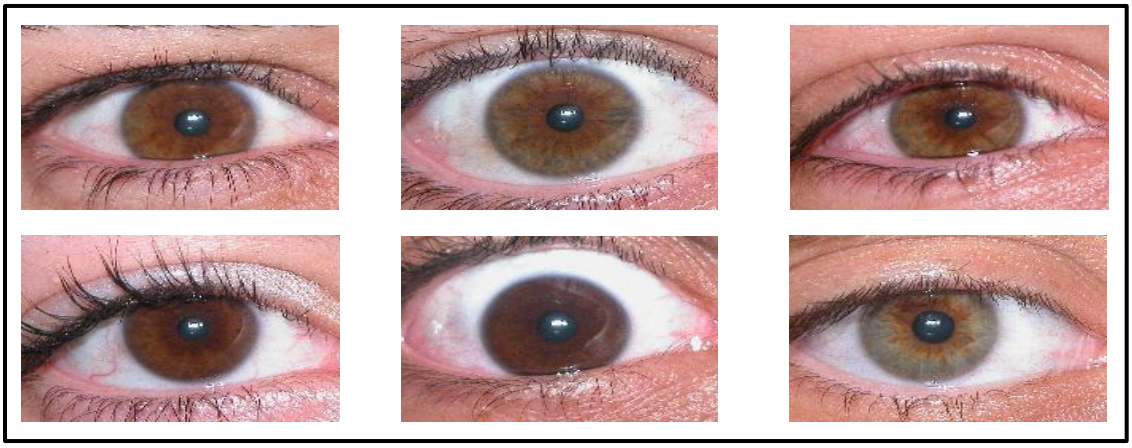


Figure (III, 4): des images de base de données UBIRIS v1

III.2.5. Base de données Miche:

La base de données MICHE c'est un ensemble de données biométriques sur l'iris capturé dans des paramètres non contrôlés à l'aide d'appareils mobiles. [5][6]

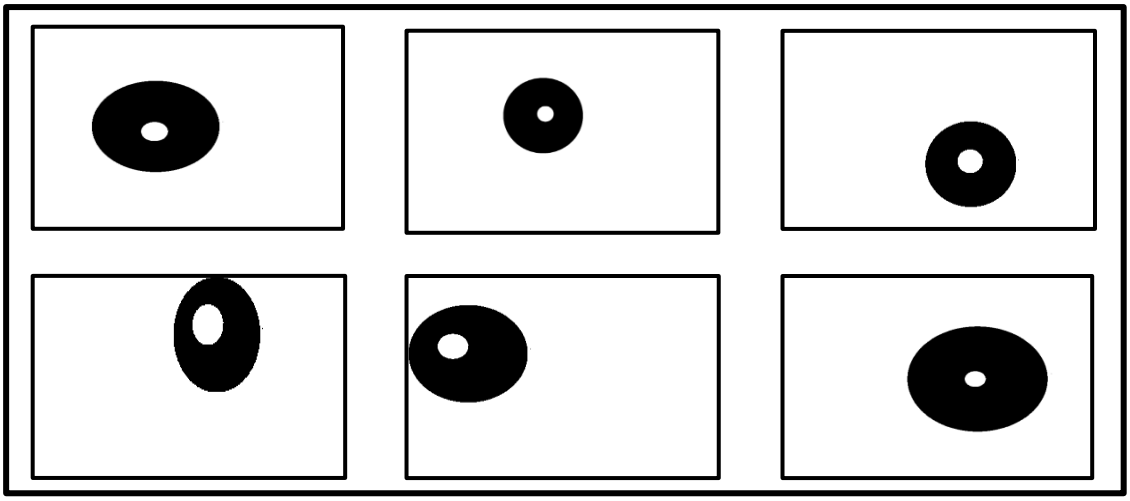


Figure (III, 5): des images de base de données MICHE

III.3. Présentation de l'application:

Nous présenterons la plate-forme logicielle que nous avons implémentée sous l'environnement **MATLAB®15.0** qui montre le principe du système complet de reconnaissance d'iris, ainsi qu'une explication des différentes tâches que nous avons réalisées dans le cadre de ce travail depuis le prétraitement, jusqu'à la recherche dans une base de données.

III.3.1. Le programme MATLAB :

MATLAB est un langage de programmation de type facile à apprendre, il permet de décrire certaines opérations de manière non procédurale et d'obtenir rapidement des résultats à partir de courts programmes. Développé par la société The Math Works.

Ce programme est utilisé à des fins de calcul numérique, il permet d'utiliser des algorithmes et ses résultats sous forme des courbes, des données ou des images.

III.3.2. Application sur UBIRIS v1 et UPOL et MICHE:

A l'aide du **MATLAB,** nous avons effectué quelques opérations (l'acquisition, segmentation et normalisation) pour découvrir l'iris en utilisant les trois bases de données: **UBIRIS v1** et **UPOL** et **MICHE**.

III.3.2.1. L'acquisition d'image de l'iris:

On commence par l'acquisition, c'est-à-dire capter l'œil par un capteur puis entrer l'image de l'iris dans le programme en utilisant la commande "imread" qui consiste à déterminer l'iris.

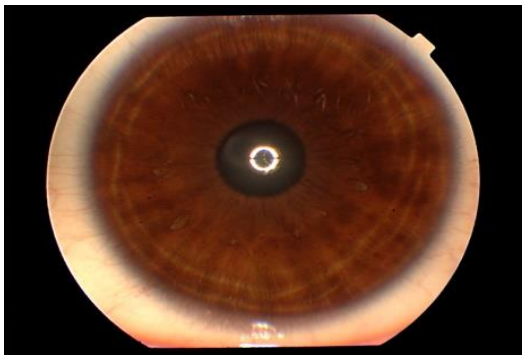


Figure (III, 6): image d'entrée de base de données UPOL

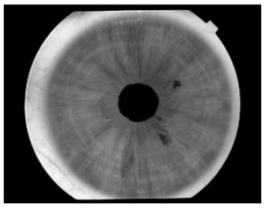
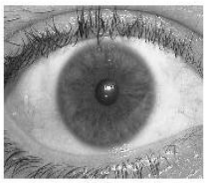
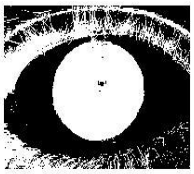
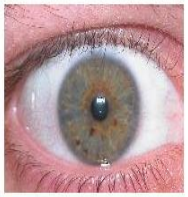
Figure (III, 7): image d'entrée de base de données UBIRIS V1

III.3.2.2. La segmentation:

Cette méthode permet de détecter les régions de l'iris, elle compose de deux étapes :

❖ La première étape: changer l'image de l'iris en niveau de gris par la commande "rgb2gray"

❖ La deuxième étape: trouver le seuil automatiquement en utilisant la commande "graythresh", c'est une technique de binarisation d'image, elle consiste à transformer une image en niveau de gris à une image dont les valeurs de pixels ne peuvent avoir que la valeur 1 ou 0. On parle alors d'une image en noir et blanc. Voir le tableau suivant:

Image originale de l'iris	Image au niveau de gris	Image segmentée
		
		
		
		

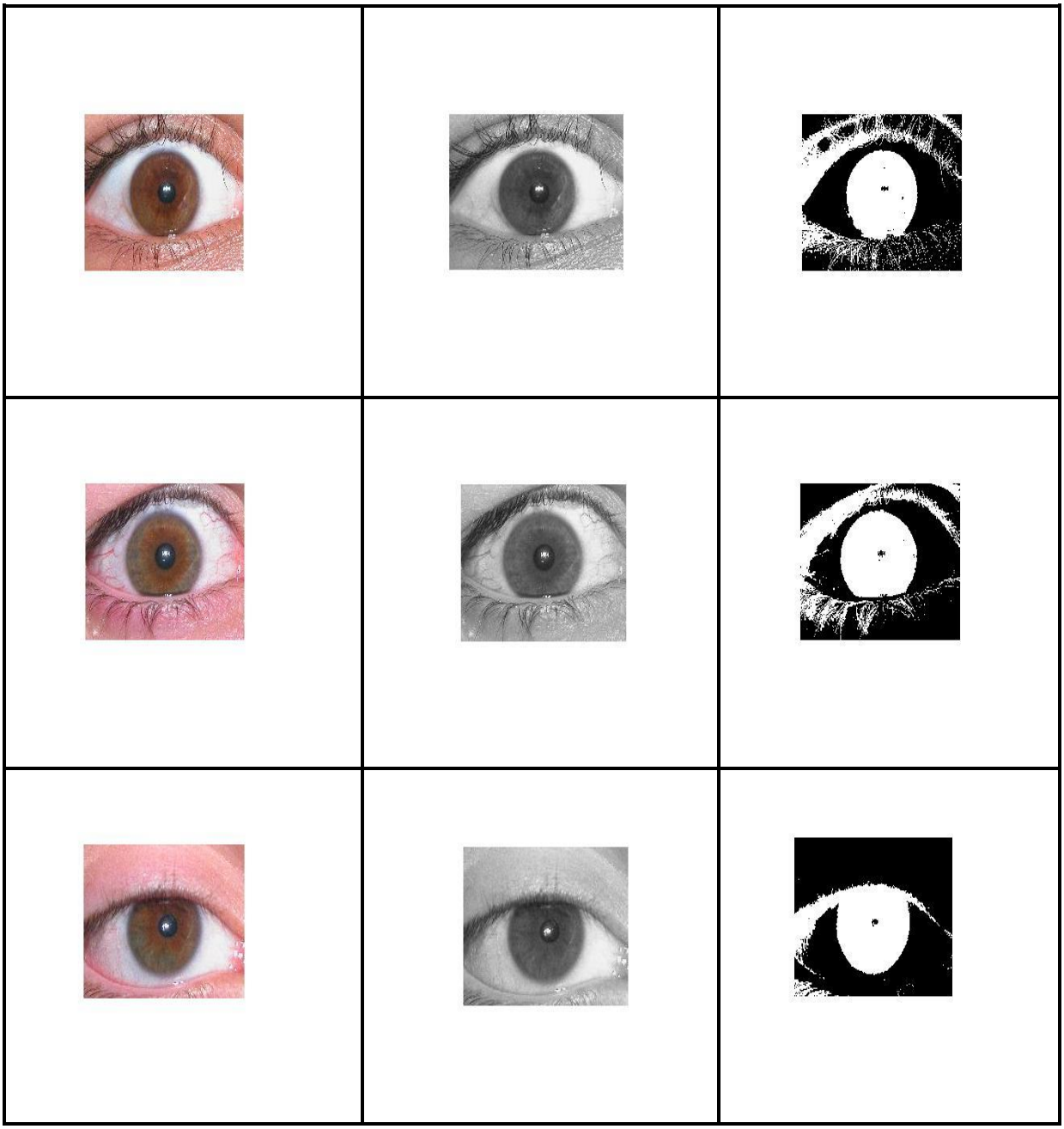


Tableau (III, 1): des images représentants les étapes de la segmentation d'iris De base de données UBIRIS v1

III.3.2.3. La normalisation:

La normalisation est une partie de traitement d'image, de but d'isolé et régler les cercles d'iris et la pupille, où le capteur détecte le centre de la pupille puis on faire un remplissage par une dilatation d'une façon circulaire pour atteindre la forme de la pupille, ainsi qu'une

chaque base de données utilise méthode différente. En utilisant la méthode morphologique par les étapes suivantes:

→Pour la base de données UPOL on utilise:

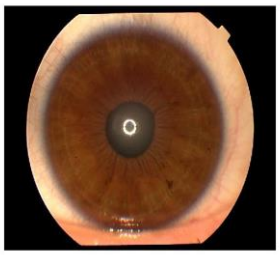
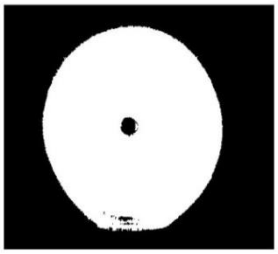
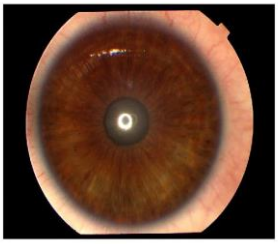
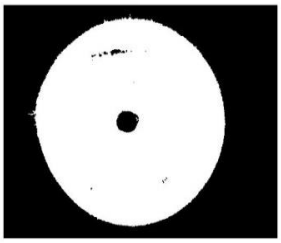
❖ "imclearborder" pour supprimer les structures lumineuses dans l'iris et les objets qui l'entourent.

❖ "bwareaopen" pour supprimer les petits objets de l'image binaire.

❖ "imdilate" pour dilater la pupille.

❖ "imerode" pour éroder l'image avec un élément structurant morphologique "strel".

❖ Faire la fonction inverse de l'image érodée.

Image originale de l'iris (UPOL)	**Image avec reflets**	**Image normalisée**
		
		
		

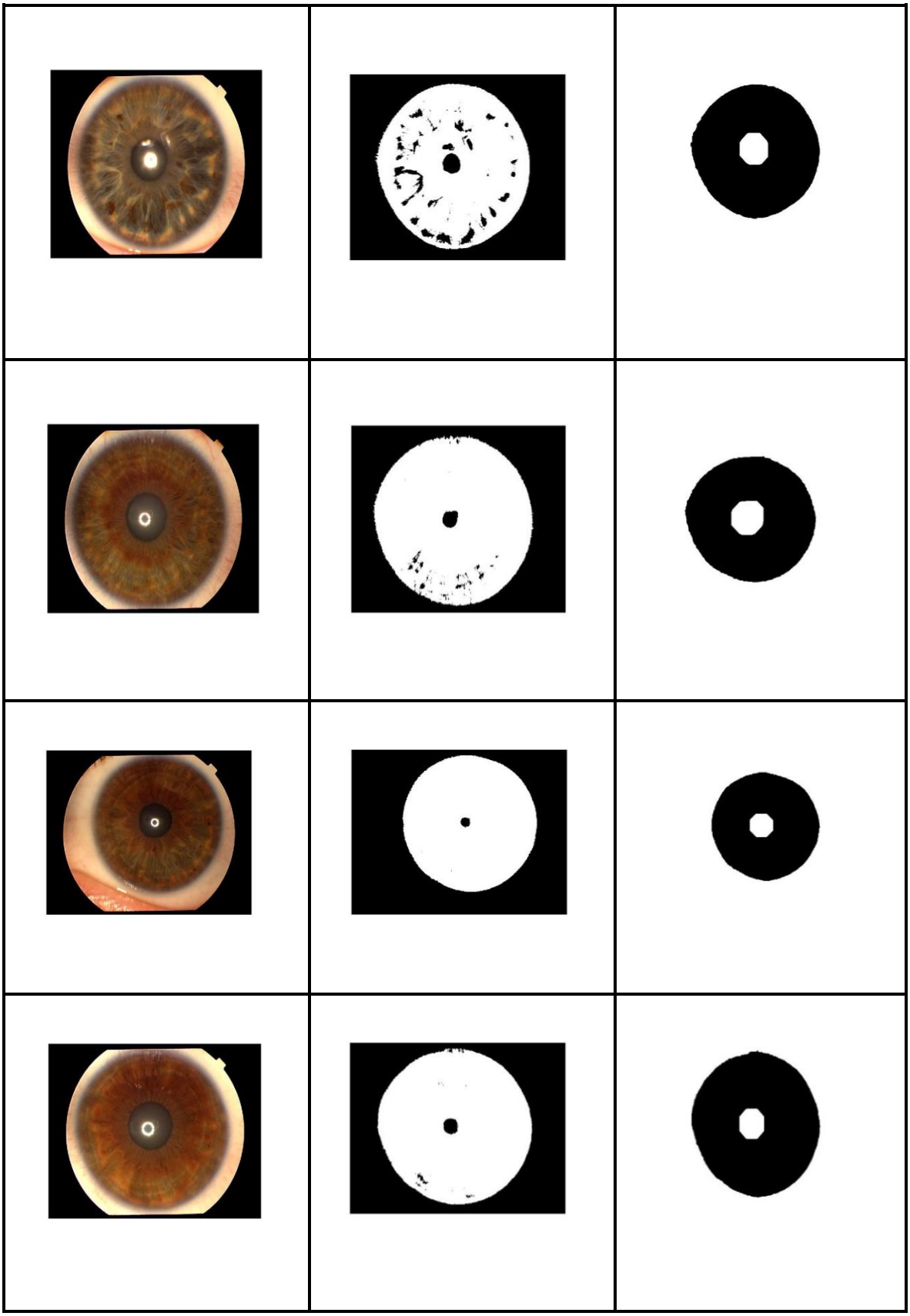


Tableau (III, 2): des images représentants les étapes de la normalisation d'iris de base de données UPOL.

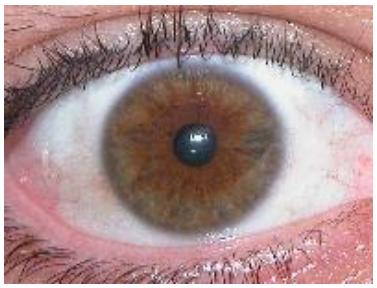
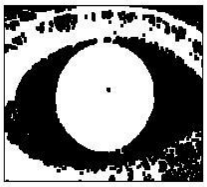
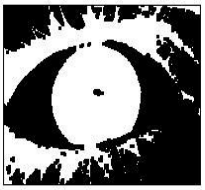
→Pour la base de données UBIRIS V1 on utilise:

❖ "bwmorph" pour faire des opérations morphologiques sur l'image binaire, effectue une fermeture morphologique sur l'iris et la pupille.

❖ "imerode" pour éroder l'image avec un élément structurant morphologique "strel".

❖ "imdilate" pour dilater la pupille.

❖ Inverser l'image dilatée.

Image originale de l'iris (UBIRIS)	Image avec reflets	Image normalisée
		
		
		

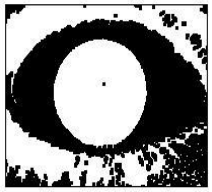
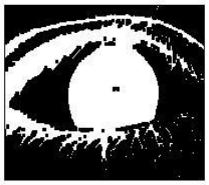
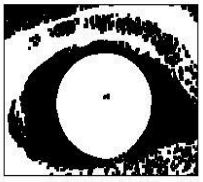
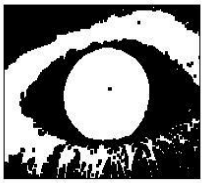
		
		
		
		

Tableau (III, 3): des images représentants les étapes de la normalisation d'iris de base de données UBIRIS v1.

III.3.2.4. La comparaison:

On applique la méthode de la comparaison entre les images normalisées des bases de données suivantes: **UBIRIS V1**, **UPOL** et **MICHE,** de deux iris revient à comparer leurs vecteurs signatures, en utilisant la distance de hamming pour faire la vérification et l'identification d'iris avec:

$$\mathbf{HD} = \frac{|\,(\mathbf{code\ A} \otimes \mathbf{code\ B}) \cap \mathbf{mask\ A} \cap \mathbf{mask\ B}\,|}{|\,\mathbf{mask\ A} \cap \mathbf{mask\ B}\,|} \qquad \textbf{(III, 1)}$$

Où code A et code B sont deux codes calculés à partir de deux images d'iris par le procédé précédemment décrit et mask A et mask B représentent leurs masques associés. Littéralement la distance de Hamming calcule le nombre de bits différents et valides pour les deux iris entre le code A et le code B. Plus la distance de Hamming est faible, plus les deux codes se ressemblent. Une distance 0 correspond à une parfaite correspondance entre les deux images alors que deux images de personnes différentes auront une distance de Hamming dans l'intervalle]0 ; 1] [7]. Les figures ((III, 8) et (III, 9)) montre notre résultat de comparaison:

1)

- ✓ Classe =1
- ✓ Résultat =Oui
- ✓ hd = 0
- ✓ Distance = même iris.
- ✓ Alors, c'est un même iris d'une même personne.

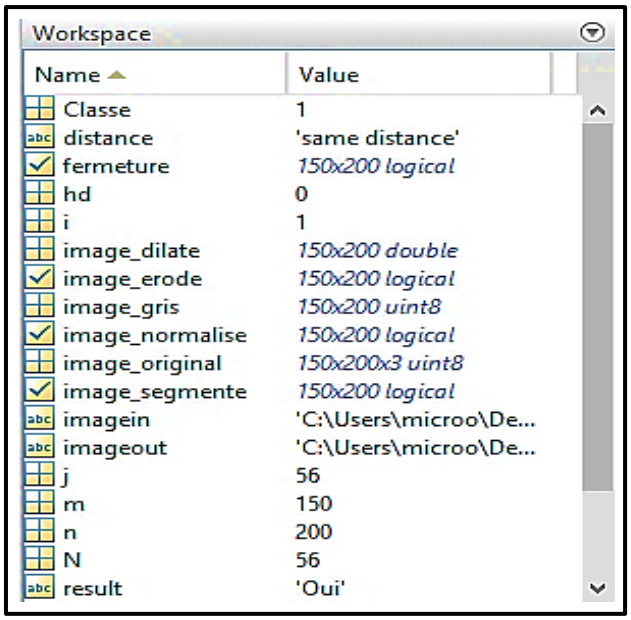


Figure (III, 8):résultat de même distance d'iris

2)

✓ Classe =0

✓ Résultat =Non

✓ hd = 0.0333

✓ Distance = différente iris.

✓ Alors, c'est un différend iris, n'est pas d'une même personne.

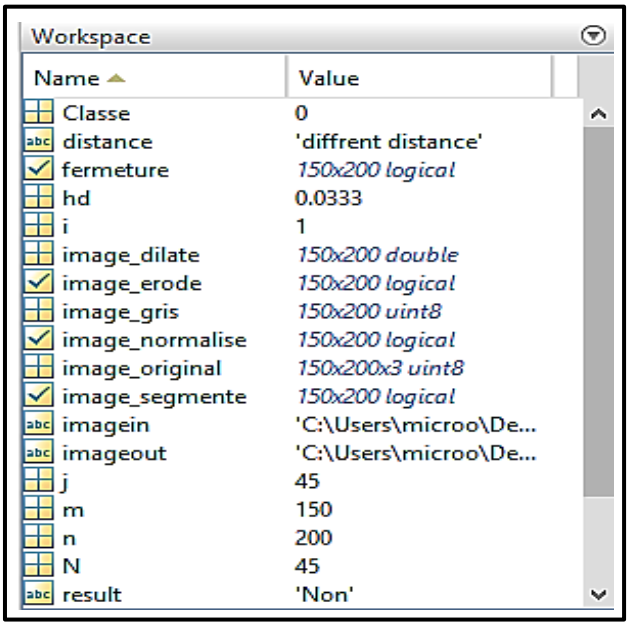


Figure (III, 9): résultat de différente distance d'iris

III.3.2.4.1. La vérification:

→ D'une personne par apport à d'autre:

- Le résultat sera « Non » et la distance ne sera pas égale à zéro.

→ D'une même personne:

- Le résultat sera « Oui » et la distance sera égale à zéro d'une même cotée d'iris soit la gauche ou la droite.
- Le résultat sera « Non » pare ce que la distance entre l'iris du l'œil gauche n'est pas la même par apport à l'une de la droite.

III.3.2.4.2. L'identification:

→ Pour identifier une personne nous avons utilisé la méthode suivante :

- Nous avons créé une nouvelle base de données à travers des images régulières que nous les avons acquises
- Nous avons inséré l'image d'iris d'une personne
- A l'aide de la distance de hamming, le programme va comparer cet iris avec tous les iris qui sont dans la base de données (degré de correspondance)

- Enfin, nous avons remarqué si la personne était parmi ces personnes ou non par la distance qu'elle sera égale 1 (existe) ou 0 (n'existe pas).

III.4. Quelques problèmes lors l'acquisition des images d'iris :

➢ **Le mouvement de la paupière :** naturellement l'œil est toujours en mouvement, ce mouvement des paupières peut obstruer les parties pertinentes de l'iris, spécialement dans ses extrêmes supérieures et inférieures de l'image d'iris.

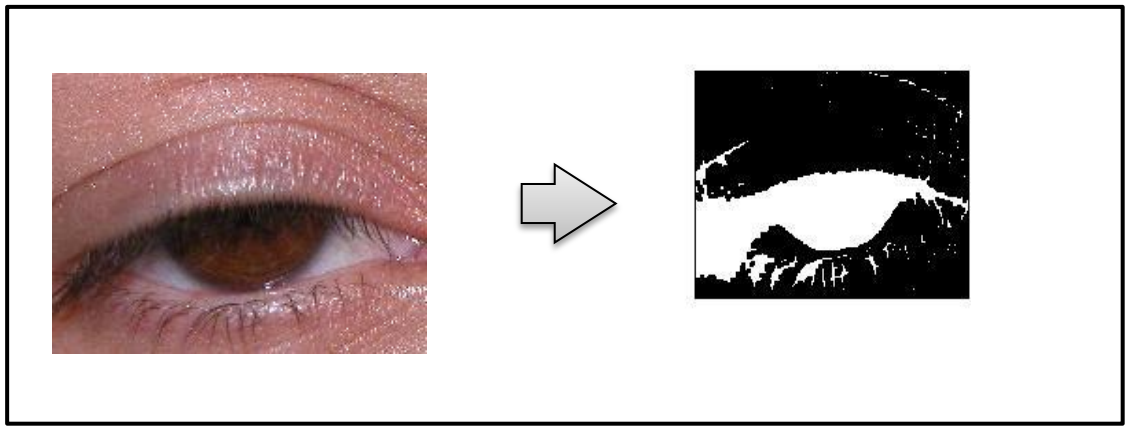


Figure (III, 10): image d'un mouvement de la paupière

➢ **Les cils :** Les cils peuvent apparaitre comme une ligne très mince et sombre dans la région de l'iris ou un petit fragment. Ils génèrent une région uniforme et sombre. (plus la présence de mascara).

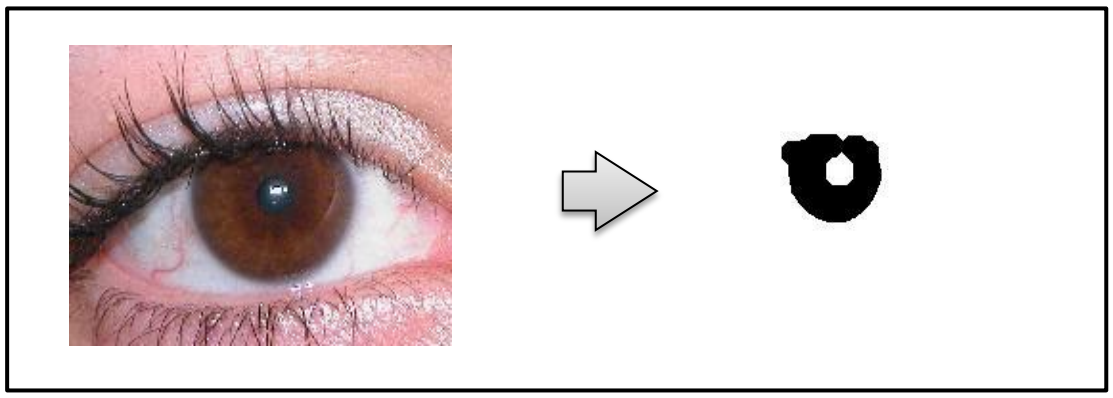


Figure (III, 11): image des cils obstrués

➢ **Mouvement de la tête :** capture des images qui ne sont pas alignées avec la direction du capteur. Cette tentative de reconnaissance biométrique de ce genre d'images donne des fausses acceptations parce que les images capturées ne sont pas d'iris.

➢ **La réflexion d'éclairage :** L'éclairage naturel d'environnements et la réflexion de la source de lumière artificielle à proximité de l'objet peuvent être un bruit, ils peuvent localiser dans des parties de l'iris, ce sont des valeurs d'intensité proche du maximum.

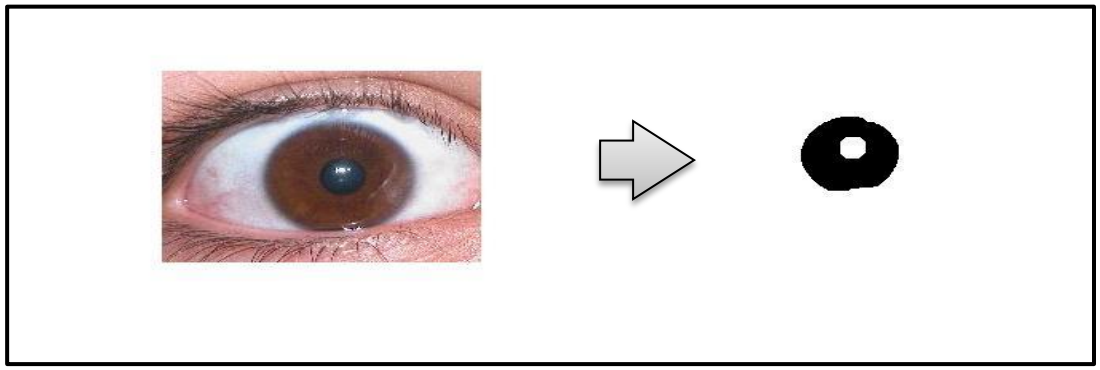


Figure (III, 12): image de réflexion d'éclairage

➢ **Les lunettes:** les personnes qui portent des lunettes ou les lentilles.

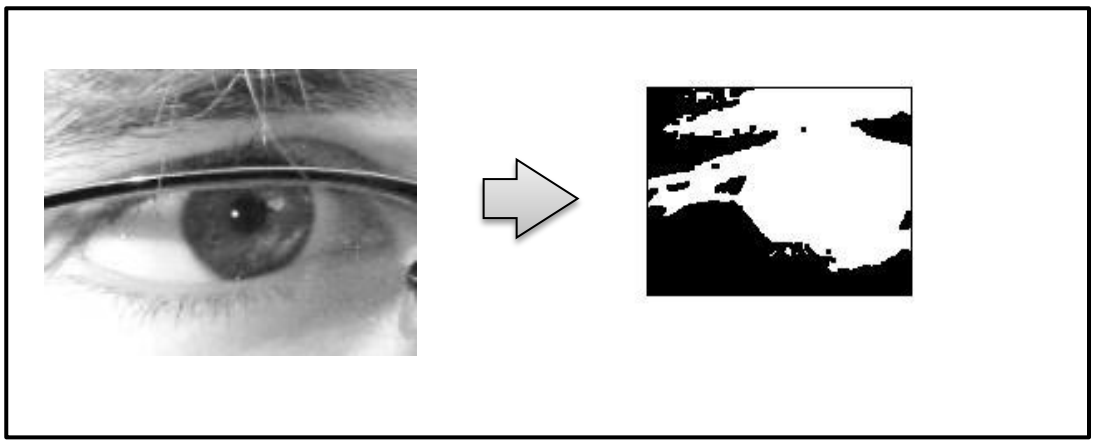


Figure (III, 13): image avec lunettes

➢ **Le floue d'image :** Lors de la capture de l'image, beaucoup de pièces mobiles produisent le flou.

➢ **Considération de la pupille comme un bruit appartenant à l'iris** : si la segmentation de frontières de pupille/iris n'est pas exacte, certaines parties de pupille sont considérées comme un bruit dans l'ris. [10]

➢ **Capture de l'image d'iris :** Lors du mouvement du corps, la caméra peut capturer exclusivement des parties de l'iris, ce qui réduit la quantité d'informations, ou peut capturer l'iris aves des parties du visage.

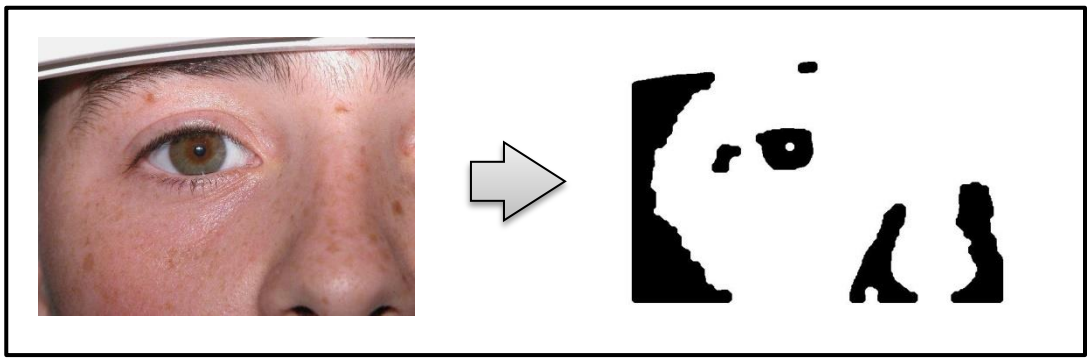


Figure (III, 14): image des parties du visage

III.5. Les maladies de l'iris d'œil:

Il existe plusieurs maladies d'iris, certains n'obstruent plus à la reconnaissance d'iris et certains oui, à cause de ces dernières le système ne répond jamais. [8]

Parmi ces maladies, nous citons les suivantes:

Rougeur d'iris: c'est l'apparition et la formation de vaisseaux sanguins anormaux autour de l'iris de l'œil, à cause de la rétinopathie ou l'occlusion veineuse rétinienne. Cette maladie n'influe pas à notre système biométrique.

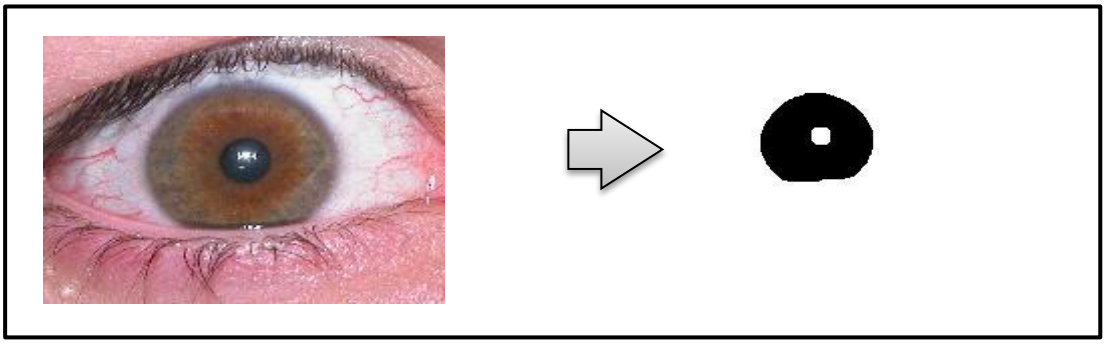


Figure (III, 15): image avec Rougeur d'iris

Et Voici quelques maladies qui peuvent obstruent la reconnaissance d'iris:

- **Absence d'iris:** il y'a des personnes qui n'ont pas d'iris depuis la naissance. C'est la disparition des tissus de l'iris, et donc la taille de la pupille est très grande et de forme irrégulière.
- **Déformation de l'iris:** est une disparition d'une partie de l'iris, elle apparaît sous la forme d'une tache en elle, afin que l'œil apparaisse comme ayant deux pupilles, ou elle peut apparaître une fente noire sur les bords de la pupille. Et ses causes sont génétiques.
- **Hétérochromie des deux iris:** La couleur de l'iris est formée en fonction de la quantité de pigment de mélanine qu'il contient, et elle apparaît dans des couleurs sombres telles que le noir ou le marron ou apparaît dans des couleurs claires telles que le vert, le bleu ou le miel. Dans certains cas, la soi-disant hétérochromie des deux iris se produit, ce qui conduit à une couleur différente de l'iris à l'iris de l'autre œil, ou la maladie peut apparaître sous la forme de la présence de plus d'une couleur dans l'iris lui-même.
- **Cancer de l'iris, kystes de l'iris, atrophie de l'iris.**

III.6. Les résultats:

La distance de Hamming est considérée l'un des performances qui évalue notre système de reconnaissance d'iris, son résultat est sous forme des chiffres entre 0 et 1. Cette méthode a l'avantage de calculer la distance entre les iris d'une façon rapide et fiable, jusqu'à 100%, ce pourcentage est considéré comme un meilleur résultat. Les codes de Hamming sont très faciles et meilleur à la correction et la détection d'erreurs sur un seul bit. L'existence d'un des obstacles qu'on a déjà cité peut changer le résultat de notre approche même si l'iris d'une même personne, on peut résoudre ce problème par l'intelligence artificielle « Deep learning » qui prend plusieurs positions de la vue d'une personne, puis les enregistrent (enroulement) pour les reconnaître comme une seule personne, on peut aussi résoudre le problème de floutage par un capteur de bonne qualité et l'influence de lumière extérieur par l'isolation de l'utilisateur.

Dans notre travail on a transformé ces chiffres à des pourcentages pour les comparer avec des résultats précédents des personnes qui ont déjà fait le thème de la biométrie d'iris. Le tableau (III, 4) montre la transformation de la distance de Hamming en pourcentage:

Seuil	Classe	Résultat	Distance de hamming	Pourcentage %
0	**1**	**Même iris (Accept)**	**0**	**100%**
ailleurs	**0**	**Différente iris (Rejet)**	**0.0333**	**3.33%**
			0.28	**28%**
			0.5	**50%**
			1	**0%**

Tableau (III, 4): la distance de Hamming en pourcentage

III.7. Conclusion:

Dans ce chapitre, nous avons présenté la conception et la validation de notre travail. Nous avons commencé par une introduction suivie par la description des bases de données publiques de l'iris. Et on a présenté l'application de notre approche. Ensuite, nous avons validé notre contribution sur les bases de données **UBIRIS v1** et **UPOL** et **MICHE**. Puis, on a établi les différentes étapes qu'on suivit dans notre programmation et notre utilisation de la morphologie mathématique. Quelques problèmes et quelques maladies de l'iris on a aussi cité. Enfin, Nous avons utilisé la distance de Hamming pour faire la comparaison.

Le système biométrique d'iris est un système robuste et efficace grâce aux résultats obtenus de notre travail qui sont pertinents et fiables.

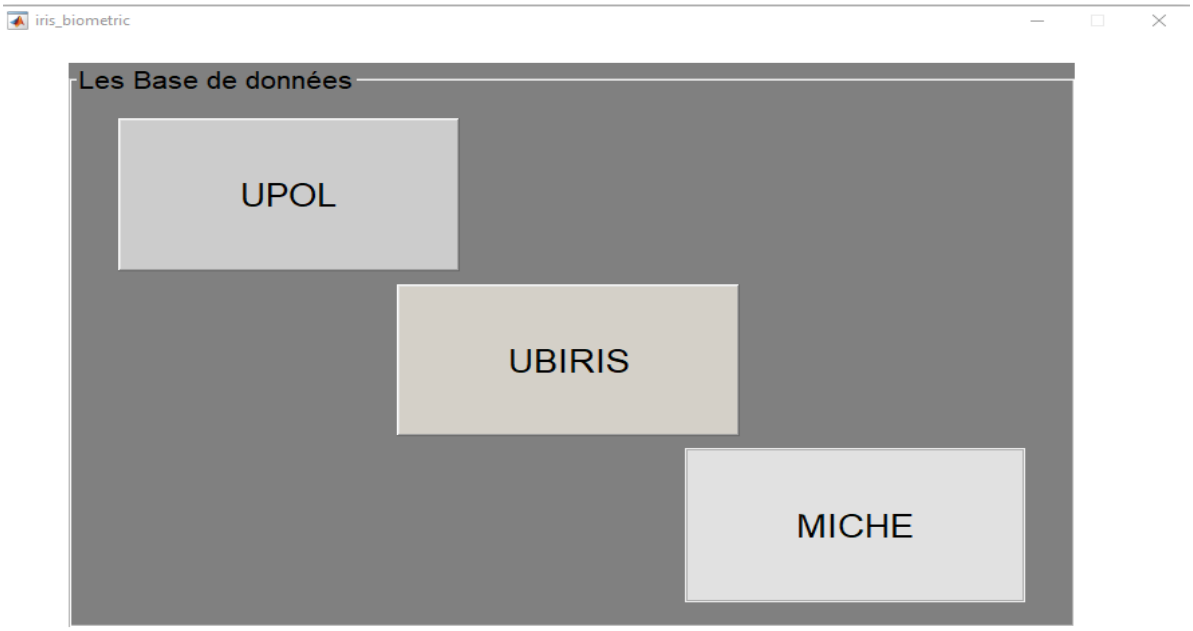
Chapitre IV : Interface (A, I) graphique d’application

Annexes

Annexe 01 :

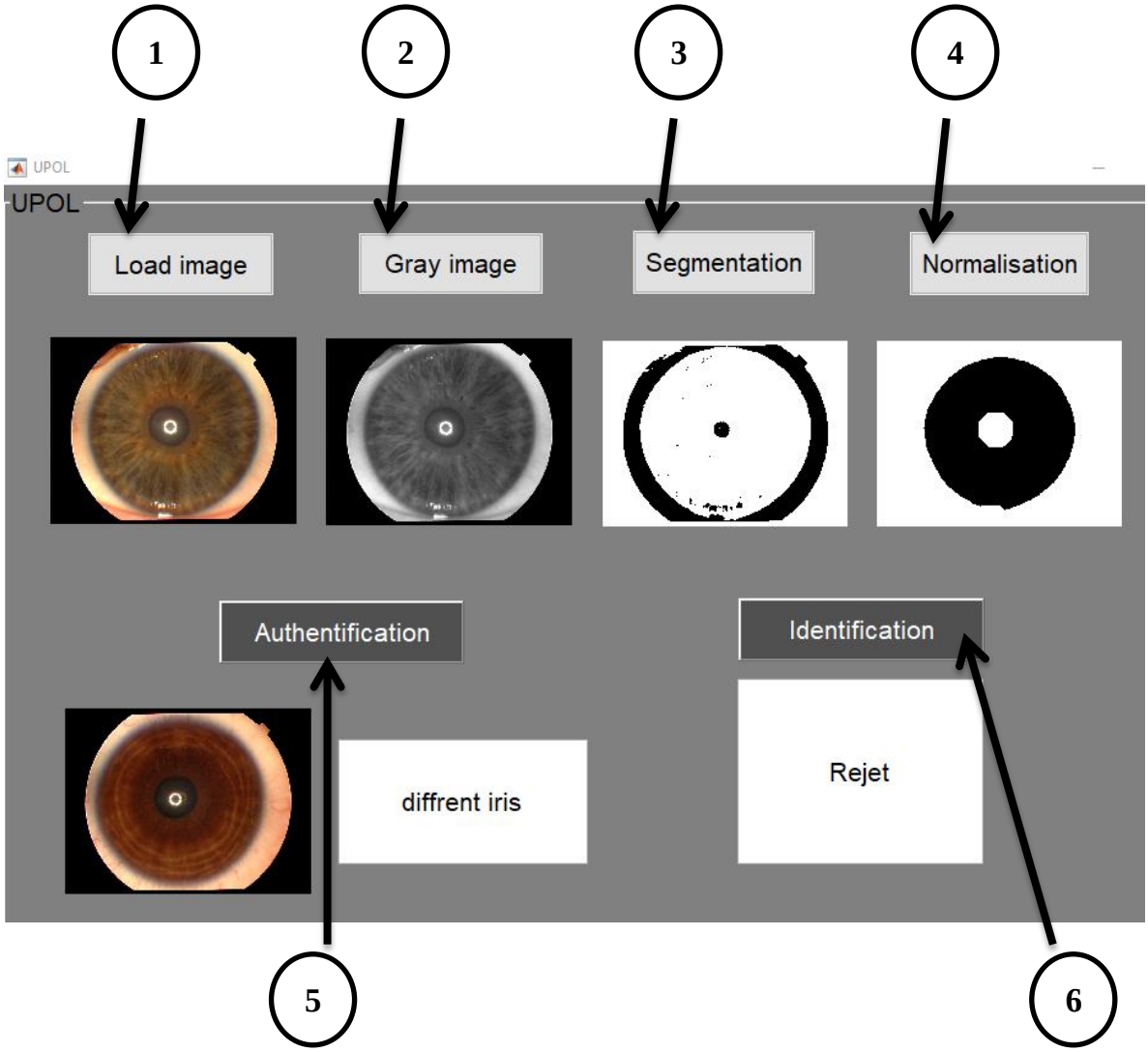
➔ **On appuie sur « Entrée » pour atteindre les trois bases de données.**

Annexe 02 :



Les trois bases de données

Annexe 03 :



L'authentification et l'identification d'iris de la base de données UPOL

1/ L'acquisition d'image (charger l'image d'iris).

2/ Conversion de l'image d'iris en niveau de gris.

3/ Segmentation d'iris en utilisant le seuillage automatique.

4/ Détection et réglage d'iris et la pupille en utilisant des opérations morphologiques.

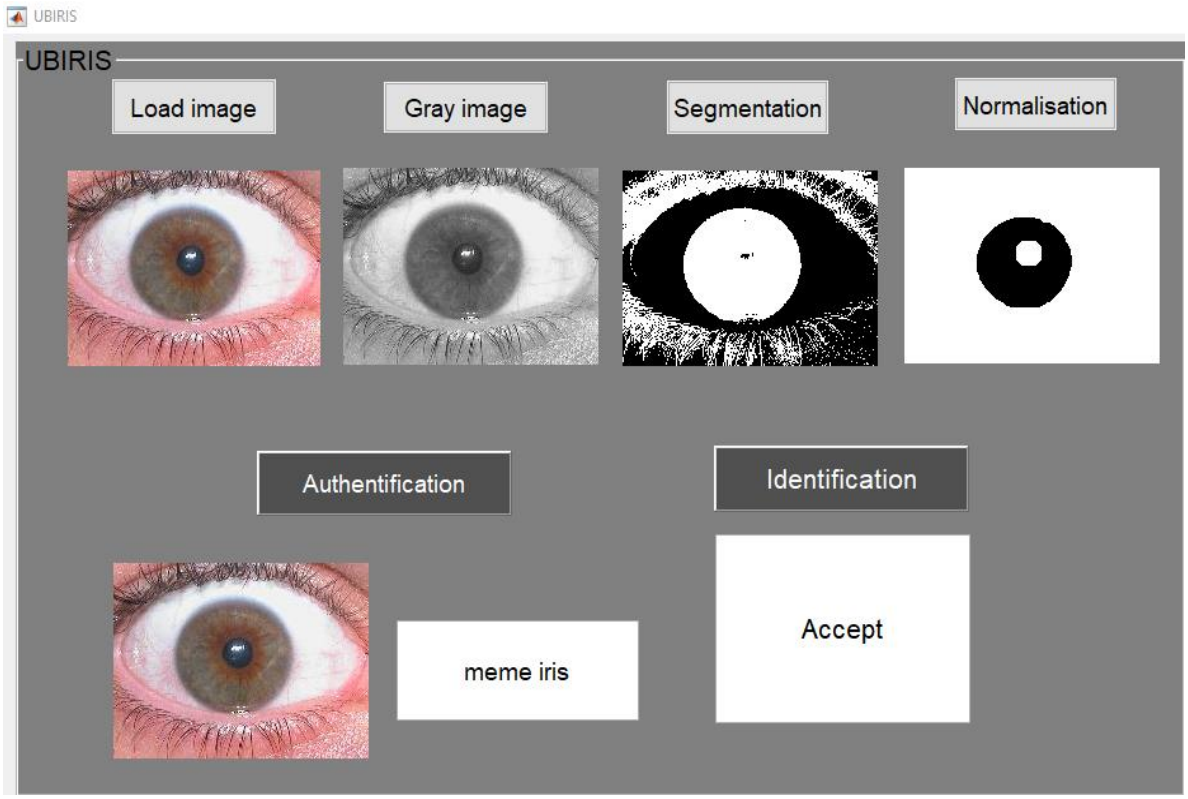
5/ La comparaison entre l'image acquise et autre image (la vérification).

➔ Diffèrent iris: La deuxième image qu'on a inséré n'est pas la même que l'image acquise.

6/ La recherche d'existence de l'iris dans la base de données qu'on a créé.

➔ Rejet: La personne n'existe pas dans la base de données UPOL.

Annexe 04 :

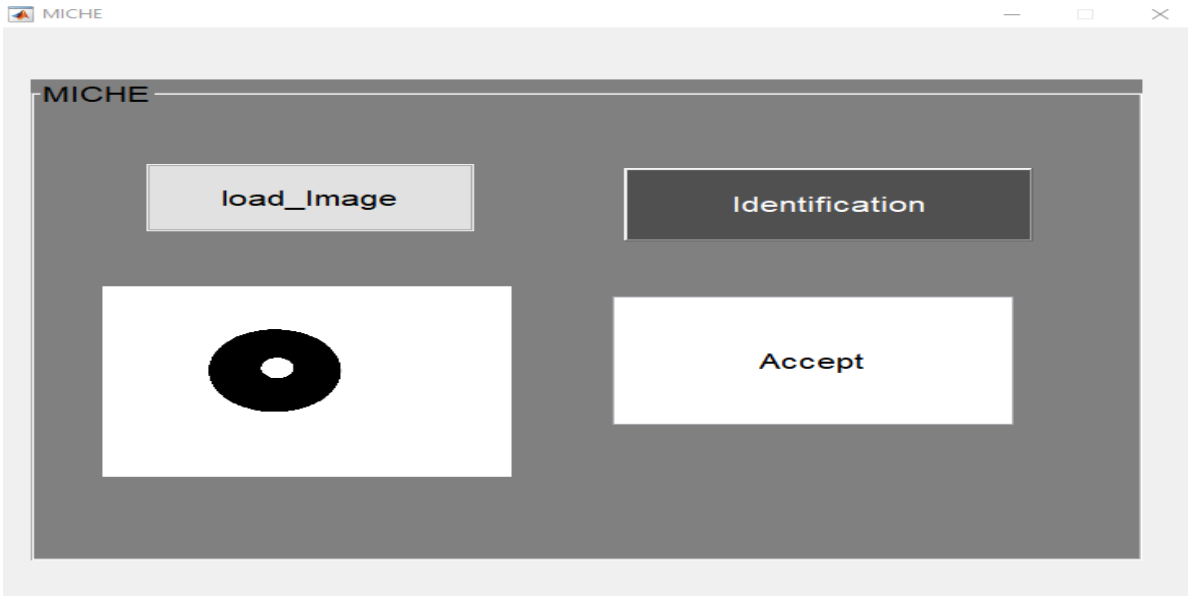


L'authentification et l'identification d'iris de la base de données UBIRIS v1

➔ **Diffèrent iris: La deuxième image qu'on a inséré est la même que l'image acquise.**

➔ **Accept: La personne existe dans la base de données UBIRIS v1.**

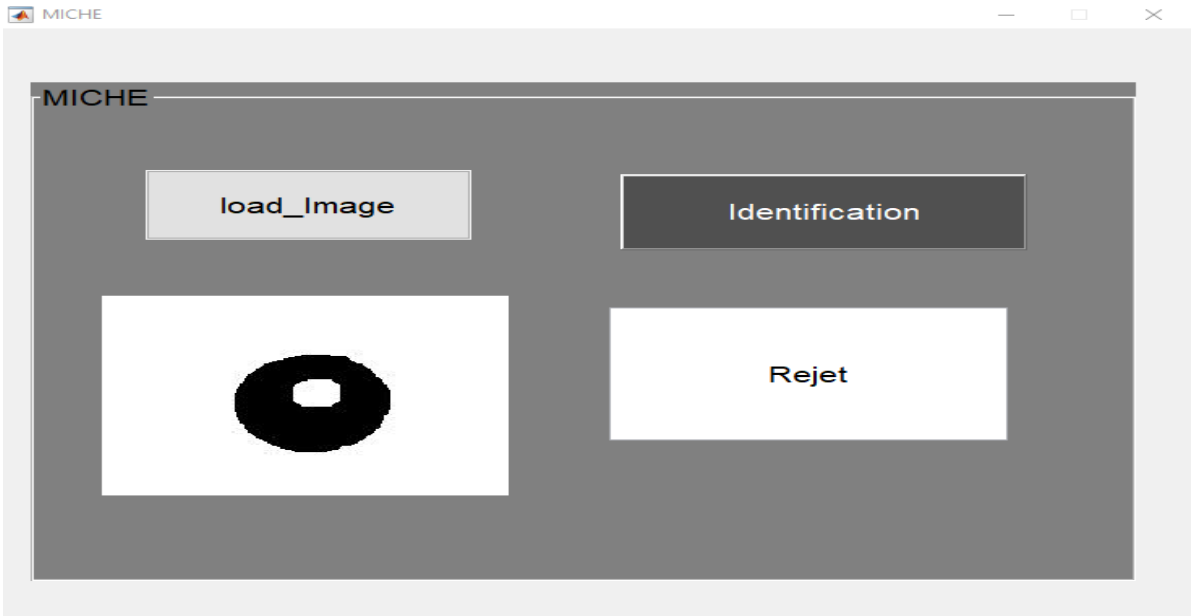
Annexe 05 :



L'identification d'iris de la base de données MICHE

➔ **Accept: La personne existe dans la base de données MICHE.**

Annexe 06:



➔ **Rejet: La personne n'existe pas dans la base de données MICHE.**

Conclusion générale et perspectives

L'objectif de notre travail était la réalisation d'un système biométrique automatique basée sur l'iris. Pour atteindre notre objectif, nous avons donné une vision générale sur la biométrie et l'iris en particulier ainsi que les méthodes et les étapes qu'on a utilisées dans notre mémoire.

Nous avons présenté le résultat de la première étape d'un projet portant sur l'élaboration d'une méthode biométrique basée sur l'iris. Cette étape inclut le traitement et la segmentation d'iris. Pour la segmentation d'iris, nous avons utilisé la segmentation par seuillage automatique, après nous avons appliqué une série des opérations morphologiques tel que la dilatation, l'érosion et la fermeture…etc. Enfin, nous avons utilisé la distance de Hamming pour atteint l'étape de l'authentification et l'identification avec la comparaison entre les iris.

Les résultats expérimentaux obtenus dans notre travail prouvent la performance de notre système biométrique par l'iris. La validation de notre système est faite sur les bases de données UBIRIS, UPOL et MICH, et nous avons remarqué la fiabilité et l'efficacité de notre système global par le degré de correspondance (distance de Hamming).

Les perspectives :

A partir des résultats obtenus nous pouvons :

- Essayer d'autres méthodes de segmentation pour la détection des éléments principaux de l'iris.
- Développer le programme proposé dans ce mémoire dans le but de résoudre le problème de L'absence d'un système d'acquisition des images : Faute de la disponibilité d'un système d'acquisition, les seules données utilisées par le système proviennent des bases. Cela rend les opérations d'identification et de vérification de simples simulations.
- Développer des nouvelles techniques pour augmenter la sensibilité et la spécificité de l'iris.
- fournir des mises à jour pour chaque nouvelle version.

Finalement, nous espérons que l'ALGERIE utilisera la technologie de la biométrie d'iris dans les sociétés et les aéroports...etc, pour augmenter la sécurité en son sein.

Bibliographie

Chapitre I :

[1] : Thales, leader de la cybersécurité et de la protection des données, organise le 31 mai 2022 à l'attention des médias, une nouvelle édition de son évènement Thales Media Day dédié à la cybersécurité

[2] : Christel -Loïc TISSE. ''Contribution à la vérification biométrique de personnes par reconnaissance de l'iris ". Thèse de doctorat de l'université de Montpellier II, Octobre 2003.

[3] : https://www.biometrie-online.net/biometrie/histoire (consulter le 13/01/2022)

[4] : https://fr.wikipedia.org/wiki/Biom%C3%A9trie

[5] : Règlement (UE) 2016/679 du 27-4-2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE du 24-10-1995 (règlement général sur la protection des données), art. 4 § 14.

[6] : « Reconnaissance faciale » [archive], 28 juillet 2015

[7] : CABAL (C.) - Méthodes scientifiques d'identification des personnes à partir de données biométriques et techniques de mise en œuvre -. Rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques (2002).

[8] : https://www.vulgaris-medical.com/encyclopedie-medicale/biometrie

[9] : https://www.biometrie-online.net/technologies/signature-dynanique

[10] :http://www.linternaute.com/science/biologie/dossiers/06/0607biometrie/autres.shtml

[11] : Robert Moskovitch, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, Bernhard Lohlein, Ulrich Heister, Sebastian Moller, Lior Rokach, Yuval Elovici (2009). «Identity theft, computers and behavioral biometrics [archive] » dans Proceedings of the IEE international Conference on Intelligence and Security Informatics: 155-160 p

[12] : Goode, M. R., Cheong, S. Y., Li, N., Ray, W. C., & Bartlett, C. W. (2014). Collecte et d'extraction de l'ADN de la salive pour le séquençage de prochaine génération [archive]

[13] : C. Fredouille, J. Mariethoz, C. Jaboulet, J. Hennebert, J.-F. Bonastre, C. Mokbel, F. Bimbot, « Behavior of a Bayesian Adaptation Method for Incremental Enrollment in Speaker Verification », International Conference on Acoustics, Speech, and Signal Processing, p. 1197-1200, Istanbul, Turquie, 5-9 Juin 2000.

[14] : L. Heck, N. Mirghafori, « On-Line Unsupervised Adaptation in Speaker Verification », International Conference on Spoken Language Processing, Vol. 2, p. 454-457, Pékin, Chine, 16-20 Octobre 2000.

[15] : H Benaliouche · Cité 56 fois — MULTIMODAL BIOMETRIC SYSTEM

https://www.hindawi.com/journals/tswj/2014/829369/

[16] : L. Hong, A. Jain, S. Pankanti, « Can Multibiometrics Improve Performance? », Proceedings AutoID'99, Summit, NJ, p.59-64, Oct 1999.

[17] : https://www.biometrie-online.net/biometrie/f-a-q

[18] : J. Egan, « Signal Detection Theory and ROC Analysis », Academic Press,
New-York, 1975

[19] : Nicolas Morizet. Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris. Domain_other. Télécom ParisTech, 2009. English. ffpastel-00005811

[20] : https://www.redsen-consulting.com/transformation-digitale/le-paiement biométrique-l 'avenir-du-paiement-en-magasin/

[21] : https://www.solutionsinformatiques.dz/?Applications-de-la-Biometrie-en-Algerie#

[22] : N. Morizet, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l"Iris", Ecole Nationale Supérieure des Télécommunications, 2009.

Chapitre II:

[1] : Anatomie, fonctionnement et physiologie de l'œil - Futura ...

https://www.futura-sciences.com › Santé › Dossiers, 25 janv. 2019, consulter le 12/03/2022

[2] : https://www.larousse.fr/dictionnaires/francais/iris/44237

[3] : https://www.guide-vue.fr/glossaire/iris

[4] : https://www.biometrie-online.net/biometrie/f-a-q

[5] : Iris (anatomie) - Wikipédia

https://fr.wikipedia.org/wiki/Iris_(anatomie)

[6]: Thukral, A., & Kumar, M. (2022, January). IRIS Spoofing through Print Attack Using SVM Classification with Gabor and HOG Features. In *2022 International Conference for Advancement in Technology (ICONAT)* (pp. 1-6). IEEE.

[7]: Labati, R. D., Genovese, A., Piuri, V., Scotti, F., & Vishwakarma, S. (2021). I-SOCIAL-DB: A labeled database of images collected from websites and social media for iris recognition. *Image and Vision Computing*, *105*, 104058

[8]: Phillips, S., & Karakaya, M. (2022, March). Effects of Distance and Gaze Angle on CNN-based Standoff Iris Recognition. In *SoutheastCon 2022* (pp. 765-772). IEEE.

[9]: Zambrano, J. E., Benalcazar, D. P., Perez, C. A., & Bowyer, K. W. (2022). Iris Recognition Using Low-Level CNN Layers Without Training and Single Matching. *IEEE Access*, *10*, 41276-41286.

[10]: http://Biometrie.online.fr

[11]:http://documents.irevues.inist.fr/bitstream/handle/2042/2444/03%22Torres+couleur.pdf?sequence=1

[12]:L. Masek, “Recognition of Human Iris Patterns for Biometric Identification”, thèse de Mster présentée à l’Université de Western Australia, Australie, 2003

[13] : N. Morizet, “Reconnaissance Biométrique par Fusion Multimodale du Visage et de l’Iris”, thèse de Doctorat présentée à l’Ecole Nationale Supérieure des
Télécommunications, France, 2009

[14]: Paulín-Martínez, F., Lara-Guevara, A, Romero-Gonzalez, R.and Jiménez-Hernandèz, H. (2019) Implementation of the Hough Transform for Iris Detection and Segmentation.

[15]: [Canny 1986] (en) J. Canny, « A Computational Approach To Edge Detection », IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 8, 1986, p. 679-698.
[16] W.W. Boles, B. Boashash, « A human identification technique using images of the iris and wavelet transform », IEEE Transactions on signal processing, Vol. 46, N° 4, Avril 1998.
17]: Jain, Anil K., and Farshid Farrokhnia. "Unsupervised Texture Segmentation Using Gabor Filters." PATTERN RECOGNITION 24, no. 12 (January 1991): 1167–86. https://doi.org/10.1016/0031-3203(91)90143-S.

[18]: J. Daugman. ‘‘How Iris Recognition Works’’, IEEE transactions on circuits and systems for video technology,vol.14, no.1, January 2004.
[19]: Mémoire de Mastère Protocoles, Réseaux, Images et Systèmes Multimédia, Réalisé Par Mohamed Nadhir KHEMAKHEM
[20]; Thèse présentée au Département d'Informatique réalisée par Hugo Pedro Martins.
[21] : Ferroui Amel, analyse des images couleur du fond d’oeil pour l’aide au diagnostic en ophtalmologie: application a la detection des pathologies retiniennes, Electronique Biomédicale, université de Tlemcen, facult é de technologie, (mai 2014)

Chapitre III:

[1] Data bases CASIA : Anil K Jain & R.C.Dubes…(2009), Encyclopidea of Biometrics, page 770https://books.google.dz/books?id=0bQbOYVULQcC&pg=PA770&dq=casia+v1.

[2] Data bases UPOL : Ainhoa Berciano Daniel Diaz-Pernil, Walter Kropatsch(2011), http://pesona.mmu.edu.my/~ccteo/Upol

[3] Data bases UBIRIS : http://phoenix.inf.upol.cz/iris/Ubiris

[4] Data bases : http://iris.di.ubi.pt/index_arquivos/Page374.html

[5] Data bases : Michele Nappi, Hugo Proença, Mobile Iris CHallenge Evaluation part I (MICHE I)https://www.sciencedirect.com/journal/pattern-recognition-letters/vol/57/suppl/C

[6] Base dedonne MICHE: http://biplab.unisa.it/MICHE/database/MICHE_BIPLAB_DATABASE/

[7] : Kamel Ghalem, mai (2014), Reconnaissance des personnes à partir des images de l’iris, Ecole superieur en genie electrique et energitique d’oran,

https://www.researchgate.net/publication/306057926_Reconnaissance_des_personnes_a_partir_des_images_de_l'iris

[8] : https://www.webteb.com/articles/