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

Biométrie multimodale basée sur l'iris et le visage

Ce projet est réalisé par :

- BAHLOUL Rami
- GOUHMAZ Mohammed
- YOUCEFI Mohamed
- SOUM Mohamedislam
- HADJOUDJ Charafeddine

Encadré par :

— Dr. BENZENATI RAHIMA

Remerciements

Nous souhaitons adresser nos plus sincères et profonds remerciements à Madame Dr Benzenati, enseignante de biométrie, pour son accompagnement précieux, la richesse de son enseignement et sa grande disponibilité tout au long de ce module.

Grâce à sa pédagogie claire, son exigence intellectuelle et sa bienveillance, elle a su éveiller en nous un réel intérêt pour la biométrie et nous a permis de mieux appréhender les concepts complexes abordés au cours de cette formation.

C'est en grande partie grâce à la qualité de son encadrement que nous avons pu mener à bien ce travail avec rigueur et motivation.

Qu'elle trouve ici l'expression de notre reconnaissance collective et de notre profond respect

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Dans un monde de plus en plus connecté, la protection des données sensibles et l'authentification fiable des individus sont devenues des enjeux cruciaux. Les méthodes traditionnelles d'identification, telles que les mots de passe ou les cartes d'accès, présentent des vulnérabilités notables, notamment en termes de perte, de vol ou de falsification. Face à ces défis, la biométrie s'impose comme une solution prometteuse, en s'appuyant sur des caractéristiques physiologiques ou comportementales uniques à chaque individu pour garantir une identification précise et sécurisée. Parmi les différentes approches biométriques, la biométrie multimodale se distingue par sa capacité à combiner plusieurs modalités, telles que l'iris et le visage, afin d'améliorer la fiabilité et la robustesse des systèmes d'authentification. Cette fusion permet de pallier les limitations inhérentes aux systèmes monomodaux, tels que la sensibilité aux conditions environnementales ou les variations physiologiques.

Ce travail se propose d'explorer en profondeur les fondements de la biométrie multimodale, en mettant l'accent sur la combinaison des modalités de l'iris et du visage. Nous analyserons les principes techniques sous-jacents à chacune de ces modalités, leurs avantages respectifs, ainsi que les défis associés à leur mise en œuvre. Par la suite, nous aborderons les méthodes de fusion multimodale, en examinant les approches existantes et en évaluant leur efficacité dans des contextes applicatifs variés. Enfin, une attention particulière sera portée aux aspects de cybersécurité, en iden-

tifiant les vulnérabilités potentielles des systèmes biométriques et en proposant des contre-mesures adaptées pour renforcer leur sécurité.

À travers cette étude, nous visons à fournir une compréhension approfondie des enjeux et des perspectives liés à l'intégration de la biométrie multimodale dans les systèmes de sécurité modernes, tout en mettant en lumière les avancées technologiques et les défis à relever pour assurer une authentification fiable et sécurisée des individus.

Chapitre 1

Fondements de la biométrie multimodale

1.1 Définition de la biométrie multimodale

L'identification par la biométrie multimodale consiste à combiner plusieurs systèmes biométriques, elle permet de réduire certaines limitations des systèmes basés sur une seule modalité tout en améliorant de manière significative leurs performances. Dans cet article, des systèmes d'identification multimodaux sont implémentés en combinant les informations issues de deux sources biométriques à savoir le visage et la démarche aux niveaux des caractéristiques et des scores. Une étape de modélisation (définit les modèles constitutifs de la base de données) basée sur un algorithme hybride qui englobe les règles sociales dérivées de l'intelligence en essaim (Optimisation à Essaim de Particules) et les concepts de la sélection et l'évolution naturelle (Algorithme Génétique) est testée, de bonnes performances ont été obtenues.

1.2 Contexte d'application en cybersécurité

L'un des principaux enjeux de la biométrie demeure la sécurité. En utilisant des méthodes d'identification avancées, il devient plus

difficile pour les fraudeurs de s'introduire dans des systèmes critiques. La biométrie protège non seulement les accès, mais sécurise également des données sensibles. Malgré ses nombreux avantages, la biométrie soulève des questions cruciales concernant la vie privée. La collecte et le stockage des données biométriques peuvent mener à des abus. L'utilisation non régulée de ces données pose un véritable problème de contrôle à l'individu.

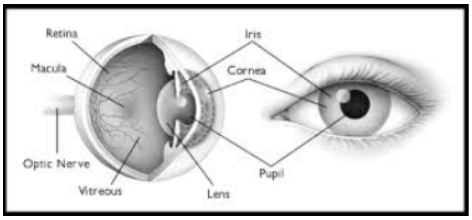
1.3 Applications dans notre quotidien

Dans le secteur financier, la biométrie garantit des transactions plus sûres. Les banques adoptent la reconnaissance faciale et les empreintes digitales pour valider l'identité des clients. Cette méthode réduit le risque de fraude et renforce la confiance des utilisateurs. Dans les établissements de santé, la biométrie simplifie l'identification des patients. Elle permet d'accéder rapidement à des dossiers médicaux tout en assurant la confidentialité des informations. Les données biométriques évitent les erreurs d'identité qui peuvent être catastrophiques. À l'aéroport, l'authentification biométrique est devenue la norme. Les systèmes de reconnaissance faciale permettent des passages plus rapides aux contrôles de sécurité. Ce processus améliore l'efficacité tout en renforçant la sécurité à l'échelle mondiale. Les appareils modernes exploitent la biométrie pour déverrouiller les écrans ou authentifier des achats en ligne. La simplicité d'utilisation et la rapidité d'accès séduisent de nombreux utilisateurs, représentant une révolution dans notre interaction avec la technologie.

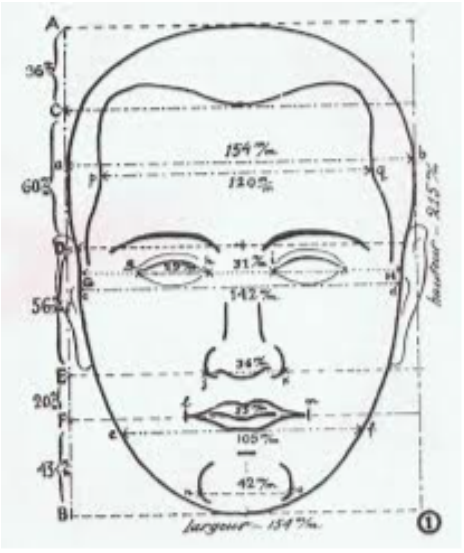
Comprendre la biométrie et ses implications nous permet d'apprécier toutes ses applications au quotidien. Bien qu'elle améliore significativement notre sécurité, il est essentiel de rester vigilant face aux enjeux qu'elle véhicule pour notre vie privée.

1.4 Combinaison iris + visage

Construire un système automatisé pour reconnaître des individus à partir d'images faciales de l'iris et d'autres modalités revient à construire un système biométrique multimodal. Un tel système combine plusieurs systèmes biométriques monomodaux en fusionnant les informations fournies par ces derniers. Cette fusion se fait par diverses méthodes, à plusieurs niveaux du système. Le système de reconnaissance d'iris étudié passe par les étapes de segmentation, de normalisation, d'extraction de caractéristiques et de correspondance dont l'extraction du vecteur de caractéristiques est obtenue par la méthode LBP. La reconnaissance faciale est aussi composée des modules de prétraitement, de l'extraction de caractéristiques et de comparaison. Les scores de l'iris et de visage obtenus sont fusionnés puis normalisés pour pouvoir prendre une décision sur l'identification des personnes.



(a) Iris



(b) Visage

FIGURE 1.1 – Système biométrique multimodal iris-visage

Chapitre 2

Partie Iris : Fondements Techniques

L'œil est l'un des cinq organes de sens du corps humain, c'est l'organe de la vue. La vision est donc la perception de l'organe de la vue qui en est l'œil. Ce dernier est l'organe récepteur de la lumière. Sa fonction est de transformer l'information lumineuse en influx nerveux transmis au cerveau. Pour voir un objet, il faut que de la lumière issue de cet objet pénètre dans l'œil que celui-ci la transforme en influx nerveux transmis au cerveau et que celui-ci interprète à son tour les informations reçues.

2.1 Structure de l'iris

2.1.1 Anatomie macroscopique

Situé dans un plan frontal, coronal, identique à celui du cristallin, l'iris, perforé en son centre par un orifice circulaire, la pupille, sépare les deux chambres antérieure et postérieure du segment antérieur de l'œil, remplies par l'humeur aqueuse. Il bombe légèrement en avant, la pupille étant dans un plan légèrement plus antérieur que l'insertion périphérique de l'iris. On lui décrit deux faces, antérieure et postérieure, et deux bords : un bord interne, formant le bord pupillaire, et un bord externe, périphérique, inséré

sur le corps ciliaire. Le diamètre de l'iris est de 12 à 13 mm. Son épaisseur varie, fine (0,1 mm) au bord périphérique, elle augmente à la collerette, atteignant 0,6 mm, puis re-diminue en allant vers la pupille. Pour Kobayashi, l'épaisseur moyenne de la partie la plus épaisse de l'iris va de 249 à 579 μm (moyenne : 434,6). Chez l'enfant prématuré, elle varie de 188 à 306 μm (moyenne 247).

2.1.2 Face antérieur de l'iris

Bien visible, en particulier en biomicroscopie, elle présente un relief très irrégulier avec deux zones, une interne pupillaire et une externe périphérique ou ciliaire, séparées par la collerette irienne.

Collerette irienne

Elle est située à l'union du tiers interne et des deux tiers externes de la face antérieure et apparaît comme une ligne irrégulière, saillante. Elle correspond à la limite de résorption de la membrane pupillaire, avec souvent présence de reliquats de cette membrane. Plus ou moins marquée, elle est en général bien visible avec souvent des dépôts pigmentés.

Zone interne ou pupillaire

Étendue entre le bord pupillaire et la collerette, elle mesure 2 mm de large. Elle présente trois zones en allant de la pupille vers la collerette :

- le bord pupillaire, anneau festonné, pigmenté, formé par le débordement en avant du feuillet postérieur pigmenté de l'iris d'origine neuroblastique. Il est en général plus large en haut qu'en bas. Sa pigmentation diminue avec l'âge.
- la zone du sphincter, bande circulaire, plus marquée sur les iris clairs.

- la zone des cryptes de Fuchs ou stomates : ce sont des déhiscences plus ou moins profondes, à concavité dirigée vers la pupille, dont le fond apparaît réticulé et dont les bords sont formés par des arcs charnus. Chez le nouveau-né, collerette et cryptes ne sont pas visibles.

Zone externe ou ciliaire

Plus large, 3 à 4 mm, elle comporte également trois zones :

- une zone interne, plane, qui fait suite à la collerette.
- une zone moyenne, formée de plis circulaires à disposition concentrique séparés par des sillons qui augmentent lors de la mydriase, les sillons de contraction. Le pli le plus périphérique forme la ligne des crêtes de Busacca (ourlet marginal de Fuchs). Il constitue par définition la limite de la paroi postérieure de l'angle iridocornéen.
- une zone externe comportant des anfractuosités ou cryptes ciliaires peu profondes.

Coloration

La coloration de l'iris est celle de sa face antérieure. Elle dépend de l'épaisseur de la couche pigmentée postérieure et de l'intensité de la pigmentation du stroma : plus le stroma est riche en pigment et plus l'iris est foncé. On peut opposer ainsi des iris clairs (bleus ou verts), ayant un épithélium pigmenté mince et peu de cellules pigmentées dans le stroma, et des iris foncés (marrons), ayant une pigmentation stromale abondante. La couleur de l'iris varie avec l'âge : maximale vers 15 ans, la pigmentation diminue ensuite progressivement.

2.1.3 Face postérieure de l'iris

Uniformément noire, elle présente trois types de plis :

- les plis de contraction de Schwalbe, lignes radiaires minces situées au pourtour de la pupille.
- les plis structuraux de Schwalbe, lignes radiaires tendues de la pupille à la périphérie irienne, correspondant à des vaisseaux.
- les plis circulaires, concentriques à la pupille, liés à des différences d'épaisseur de l'épithélium pigmenté.

2.2 Acquisition de l'iris

L'acquisition d'une image d'iris est considérée comme l'une des plus difficiles en biométrie. Premièrement, l'iris est sombre, il faut donc l'éclairer mais en même temps l'iris est sensible à la lumière et de fortes illuminations peuvent engendrer des malaises chez l'utilisateur. Deuxièmement, l'iris est un objet de petite taille (environ 1cm de diamètre) il est alors impératif d'utiliser des focales très puissantes ou de rapprocher l'iris de l'objectif mais non sans risque, car dans ce dernier cas, on rapprocherait l'iris de la source d'illumination ce qui pourrait nuire aux personnes. Enfin l'iris est une surface qui réfléchit la lumière dans toutes les directions et est située derrière la cornée un miroir hautement réfléchissant. Ces deux dernières caractéristiques font que si aucune technique particulière n'est employée l'iris photographié sera couvert par des reflets de toutes les sources lumineuses présentes dans l'environnement d'acquisition comme illustré dans la. Il est bien clair que l'image ci-dessus ne montre pas la richesse de texture que nous sommes en mesure d'espérer. Une deuxième option, adoptée par tous les industriels de la reconnaissance de l'iris qui correspond à la norme ISO, est l'utilisation d'une ou plusieurs sources infrarouge comme illuminateur puissant. L'infrarouge possède deux

avantages majeurs sur la lumière visible. Premièrement, la lumière est invisible, l'utilisateur ne sera pas aussi gêné qu'en lumière visible par une puissante illumination. Le deuxième avantage est que le proche infrarouge possède un pouvoir de pénétration de la cornée qui est largement plus grand que celui de la lumière visible et il est ainsi possible de récupérer une richesse de texture supérieure à celle obtenue en lumière visible surtout pour les iris sombres.

2.3 Techniques de reconnaissance par iris

L'extraction des caractéristiques doit être capable de capturer et d'encoder cette particularité aléatoire présente dans la texture de l'iris. Les méthodes de traitement algorithmique reposent donc sur une analyse du relief et de strie de l'iris.

- **Techniques basées sur la texture**
  Elles font usage de filtres pour le traitement des images et l'extraction de quelques propriétés des images filtrées afin de quantifier les images d'iris données.
- **Techniques basées sur les caractéristiques**
  Elles font usage des caractéristiques locales présentes dans l'image (blocs ou taches) et enregistrent leurs localisations et caractéristiques (propriétés) pour distinguer les différentes images.
- **Techniques basées sur l'apparence**
  Elles font usage d'approches statistiques classiques telles que l'analyse en composantes principales (ACP) ou l'analyse en composantes indépendantes (ACI) pour représenter les images d'iris.

2.4 Segmentation de la pupille et de l'iris

La segmentation est une technique nécessaire pour isoler et exclure les informations inutiles, ainsi que la localisation de la région circulaire. L'image peut être considérée comme une scène composée de différentes régions, objets, etc. Ainsi, la segmentation permet de montrer les contours des objets dans une image. Dans le cas de la reconnaissance de l'iris, elle consiste à trouver la frontière intérieure entre la pupille et l'Iris et la frontière extérieure entre l'Iris et la sclérotique. Elle est entourée par des frontières extérieures (iris-blanc de l'œil) et des frontières intérieures (iris-pupille). Ces limites, bien que pas toujours parfaitement circulaire, les deux frontières, intérieure et extérieure, d'un Iris typique peuvent être prises approximativement par des cercles. Toutefois, les deux cercles ne sont généralement pas centralisés.

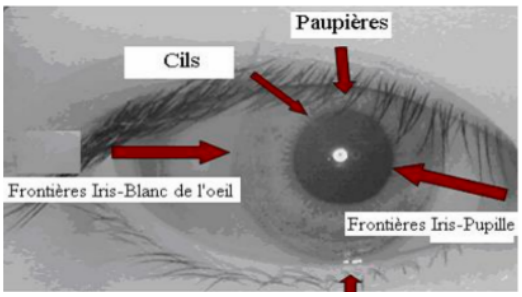


FIGURE 2.1 – Segmentation de la pupille et de l'iris

2.5 Détection d'iris de la pupille

Il existe plusieurs méthodes dans la littérature pour aboutir à l'extraction de l'iris, nous allons présenter La méthode par La transformée de Hough dans ce qui suit.

2.5.1 La méthode par La transformée de Hough

La transformée de Hough est une technique qui peut être utilisée afin d'isoler des objets de formes géométriques simples dans l'image. En général, on se limite aux lignes, cercles ou ellipses présents dans l'image. L'un des grands avantages de la transformation de Hough est qu'elle est tolérante aux occlusions dans les objets recherchés et demeure relativement affectée par les bruits. Cette technique nous permet de reconnaître les lignes (droite), les cercles ou n'importe quelle forme présente dans une image. Les objets à détecter dans l'image de l'œil (iris, pupille, paupières) sont circulaires ou ellipsoïdaux et donc se prêtent bien à une détection par la transformée de Hough.

Les étapes de la transformée de Hough sont les suivantes :

— Une image de contours est générée par une quelconque méthode de génération de contours.

— Un processus de vote est mis en place sur l'image de contours obtenue. Chaque point de contour vote pour les cercles dont il appartient et le cercle qui obtient le plus de vote est le cercle recherché. Dans ce cas, nous comptabilisons pour chaque cercle dans la zone recherchée ; le cercle qui possède le plus de points de contours est le cercle recherché.

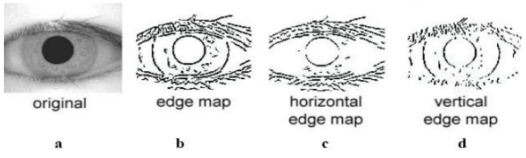


FIGURE 2.2 – Détection circulaire par transformée de Hough

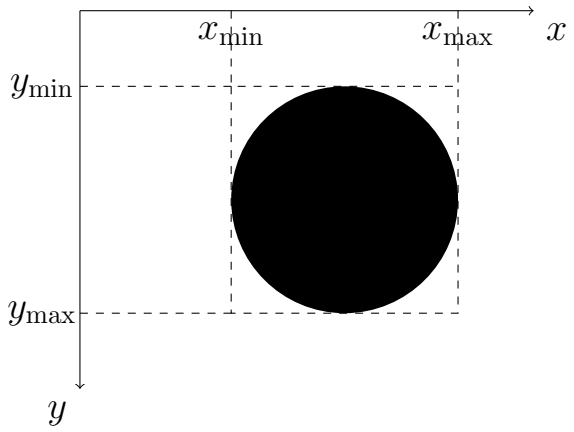
Détermination du rayon et du centre de la pupille et de l'iris

Pour déterminer le centre de la pupille on procède comme suit :

— Binarisation de l'image

— Seuillage

— Détermination du rayon et du centre de la pupille Cp(Xp,Yp)



Le rayon et le centre de la pupille sont donnés par les formules suivantes :

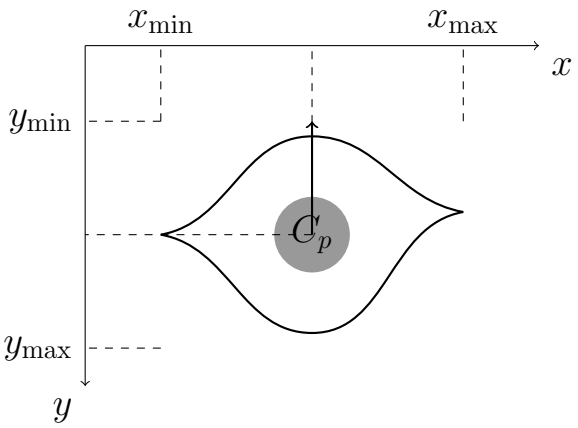
$$R_p = \frac{(x_{\max} - x_{\min})}{2}$$

$$x_p = R_p + x_{\min}$$

$$y_p = R_p + y_{\min}$$

Détermination du Rayon de l'iris

Après avoir déterminé Cp(Xp,Yp) on peut extraire le rayon de l'iris Ri : à partir du centre de la pupille et en partant du ce point (Cp) que nous avons trouvé, nous avançons jusqu'à trouver un deuxième contour. Nous notons alors le point (Xi) où nous sommes arrivés : il appartient au bord de l'iris.



Donc le rayon de l'iris est donné par l'équation suivante :

Ri = (Cp - Xi)

À partir de ces équations, on peut facilement isoler la région de l'iris.

2.6 Démarche adoptée

Après avoir parcouru les principales méthodes, nous présentons dans ce qui suit le schéma général intervenant dans l'identification de l'iris.

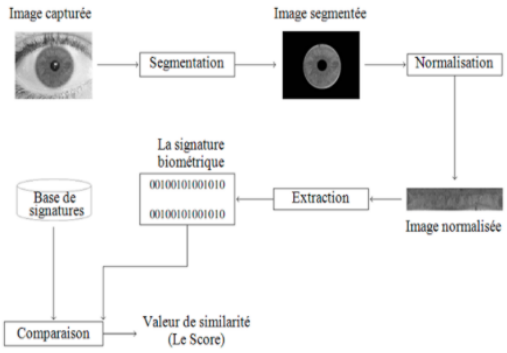


FIGURE 2.3 – Démarche adoptée

- **Image capturée**
  On commence par prendre une photo de l'œil (généralement avec une caméra infrarouge pour bien voir les détails de l'iris, sans être gêné par la lumière ambiante ou la couleur des yeux).
- **Segmentation**
  L'image capturée contient beaucoup d'informations inutiles (paupières, cils, fond). L'étape de segmentation permet de repérer et isoler uniquement la zone de l'iris, en traçant les contours de la pupille (au centre) et du bord extérieur de l'iris.
- **Image segmentée**
  À ce stade, on a une image propre du seul iris, sans le reste de l'œil. Cette image est prête à être traitée.
- **Normalisation**
  Comme chaque iris peut être de taille différente (à cause de la distance, du zoom, ou de la dilatation de la pupille), on transforme l'image pour qu'elle ait toujours la même taille et la même forme. On "déplie" en quelque sorte l'iris en un rectangle régulier, ce qui facilite la comparaison plus tard.
- **Extraction**
  On analyse l'image normalisée pour extraire une signature numérique unique de l'iris. C'est une suite de 0 et de 1 qui représente les motifs et textures présents dans l'iris. Cette signature est comme une empreinte digitale, mais pour les yeux.
- **Base de signatures**
  Les signatures extraites peuvent être enregistrées dans une base de données. Lorsqu'on veut reconnaître une personne, on compare sa signature avec celles déjà enregistrées.

- **Comparaison**
  La signature de l'iris capturé est comparée à celles de la base de données pour chercher une correspondance.
- **Valeur de similarité (Score)**
  La comparaison donne un score de similarité, qui indique à quel point les deux signatures (celle de la personne actuelle et celle enregistrée) se ressemblent. Si le score est suffisamment élevé, l'identité est reconnue.

2.7 Les difficultés de la reconnaissance par l'iris

La biométrie de l'iris présente plusieurs difficultés et défis que nous devons surmonter pour définir un système de reconnaissance fiable basé sur cette modalité. L'iris est comme nous l'avons indiqué, un organe interne du corps qui doit sa visibilité depuis l'extérieur à la cornée, censée jouer le rôle d'un miroir hautement réfléchissant. Ce miroir implique quelque soit le mode d'acquisition de l'iris, des réflexions sur la pupille et/ou sur l'iris qui peuvent compliquer la reconnaissance. La texture de l'iris peut être couverte par ce qu'on appelle des bruits occultants. Ces bruits peuvent être dûs à la présence des paupières selon l'ouverture de l'œil et selon les populations peuvent aussi résulter de la présence des cils. La texture de l'iris peut aussi souffrir des réflexions dues au port des lunettes ou des lentilles. Un phénomène peut être rencontré avec l'iris en présence concerne les mouvements brusques d'œil (ouverture/fermeture des paupières) avec ceux de la contraction ou dilatation de la pupille selon la quantité de lumière dans l'environnement d'acquisition.

Chapitre 3

Partie Visage : Fondements Techniques

3.1 Définition

Le visage est un modus non invasif de biometrique servant à identifier ou authentifier une individu par les traits du visage qui sont uniques : forme des yeux, distance des yeux, forme du nez, mâchoire, etc.

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

3.2 Types

3.2.1 Méthodes Globales

Les méthodes globales considèrent le visage comme un tout. Elles ne se préoccupent pas des détails comme les yeux, le nez ou la bouche individuellement, mais plutôt de l'aspect général de l'image faciale. Ces techniques transforment le visage en un vecteur ou une matrice de données, puis utilisent des méthodes statistiques et mathématiques pour le comparer à d'autres visages enregistrés. L'exemple le plus connu est l'Analyse en Composantes Principales (PCA), aussi appelée méthode des eigenfaces, qui réduit la dimension des images tout en conservant les informations essentielles. Cela permet une reconnaissance rapide et efficace dans des environnements contrôlés. Cependant, ces méthodes montrent leurs limites dès qu'il y a des variations d'éclairage, de pose, ou d'expression faciale. Par exemple, un visage tourné de 30 degrés ou partiellement ombré sera mal reconnu, car le modèle n'est pas capable d'analyser les régions localisées du visage de manière indépendante. Elles sont tout de même très populaires dans des systèmes simples, comme les applications de base de reconnaissance sur des photos frontales, bien éclairées, prises dans de bonnes conditions.

3.2.2 Méthodes Locales (ou Analytiques)

Les méthodes locales, contrairement aux méthodes globales, se focalisent sur des parties spécifiques du visage telles que les yeux, le nez, la bouche.. etc. Elles extraient des caractéristiques locales autour de ces zones, ce qui permet d'avoir une description plus robuste.

Cette catégorie se focalise sur l'idée que quelques zones du visage sont plus discriminantes que d'autres, et que basant sur ces zones permet d'améliorer la précision, surtout en cas d'occlusions

(lunettes, barbe, casquette).

Parmi les techniques locales, on trouve :

— LBP (Local Binary Patterns) qui encode les textures locales du visage.

— HMM (Hidden Markov Models) qui modélisent les séquences de traits du visage.

— EBGM (Elastic Bunch Graph Matching) qui est une méthode sophistiquée qui utilise des graphes élastiques pour bien modéliser la structure du visage.

Ces méthodes sont plus résistantes aux perturbations, mais elles sont aussi plus complexes à mettre en œuvre, car elles nécessitent une détection très précise des points clés du visage, ce qui n'est pas toujours évident, surtout dans des images de mauvaise qualité.

3.2.3 Méthodes Hybrides

Face aux limites des approches globales et locales, les chercheurs ont proposé des méthodes hybrides qui cherchent à tirer parti des avantages des deux mondes. Ces approches combinent souvent :

- des techniques globales pour une représentation générale du visage,
- des techniques locales pour renforcer les détails importants,
- et des algorithmes d'apprentissage automatique ou profond pour améliorer encore la précision.

Par exemple, une méthode hybride peut utiliser PCA pour réduire les dimensions de l'image, puis appliquer un classificateur SVM ou un réseau de neurones pour la reconnaissance. D'autres intègrent des modèles 3D du visage pour mieux gérer les changements de pose et d'angle.

C'est cette catégorie qui a permis les plus grandes avancées en reconnaissance faciale, notamment avec l'arrivée du deep learning : les réseaux de neurones convolutifs (CNN) comme FaceNet, DeepFace ou ArcFace sont capables d'extraire automatiquement à la fois des informations globales et locales, en s'adaptant à des milliards de visages dans des conditions très variées.

Ces systèmes sont ceux utilisés aujourd'hui dans :

— le déverrouillage facial des smartphones,

— la surveillance automatisée,

— les contrôles d'identité dans les aéroports, etc.

3.2.4 Étapes

La reconnaissance faciale comporte plusieurs étapes principales :

1. **Détection faciale :** Détecter et déterminer la présence d'un ou plusieurs visages dans une image ou une vidéo (par exemple, à l'aide du classificateur Haar d'OpenCV).
2. **Prétraitement :** Alignement, redimensionnement et normalisation du visage (conversion en niveaux de gris, égalisation d'histogramme, etc.).
3. **Extraction de caractéristiques :** Transformation d'un visage en vecteurs de caractéristiques à l'aide de descripteurs tels que LBPH, HOG ou des plongements profonds (faceNet, DeepFace).
4. **Comparaison/Classification :** Comparaison à une base de données (reconnaissance) ou vérification (authentification), généralement à l'aide d'un classificateur (SVM, KNN, etc.).
5. **Décision :** Accepter ou rejeter en fonction d'un seuil de similarité ou de confiance.

3.2.5 Avantages

Non-intrusif : Ne nécessite pas de contact physique

La reconnaissance faciale fonctionne à distance, contrairement à d'autres méthodes biométriques (empreintes digitales, iris) qui nécessitent une interaction physique.

— Déverrouillage d'un smartphone (ex : Face ID d'Apple) sans toucher l'appareil.

— Contrôle d'accès dans les aéroports (ex : PARAFES en France).

Avantage clé : "Réduit les risques sanitaires (pas de surfaces touchées) et améliore l'expérience utilisateur."

Rapide et automatisable : Compatible avec vidéos en temps réel

Les algorithmes modernes (ex : Dlib, FaceNet) traitent >30 images/seconde, permettant une analyse en flux continu.

Performance des méthodes		
Méthode	Vitesse (FPS)	Hardware requis
LBPH (OpenCV)	10–15	CPU standard
DNN (FaceNet)	20–30	GPU NVIDIA

TABLE 3.1 – Comparaison des performances

Cas d'usage :

— Surveillance urbaine (ex : caméras de rue à Paris).

— Authentification en temps réel pour les paiements (ex : Alipay en Chine).

Facile à intégrer : Compatible avec des caméras standards

Fonctionne avec des caméras RGB bas coût (ex : webcam à 10€), sans besoin d'infrarouge ou de capteurs spécialisés.

Modalité	Coût capteur	Résolution requise
Visage	10–100€	720p (HD)
Iris	500–2000€	NIR + 5MP

TABLE 3.2 – Comparaison des coûts et exigences

Polyvalent : Applications multiples

Possible utilisation pour l'authentification, la surveillance, le contrôle d'accès, etc.

Domaines d'application

Secteur	Exemple concret
Sécurité	Reconnaissance de suspects (Interpol)
Retail	Publicité ciblée (ex : caméras en magasin analysant l'âge/sexe)
Banque	Paiement biométrique (ex : Société Générale)
Santé	Suivi des patients (détection de fatigue)

TABLE 3.3 – Applications par secteur

3.2.6 Risques et limites

1. **Variabilité des conditions :** Lumière, angle, expressions faciales, vieillissement peuvent détériorer les performances.
2. **Faux positifs/négatifs :** Moins précis que l'iris ou les empreintes.
3. **Vie privée :** Soulève des questions éthiques et juridiques (RGPD).
4. **Usurpation d'identité :** Risque d'attaques par "spoofing" (photo/vidéo 2D ou masques 3D).

Chapitre 4

Fusion Multimodale

4.1 Définition

Les systèmes biométriques unimodaux, basés sur une seule modalité comme l'iris ou le visage, présentent des limites en termes de fiabilité, de bruit, et de vulnérabilité aux attaques. Pour pallier ces problèmes, les systèmes biométriques multimodaux utilisent plusieurs caractéristiques biométriques d'un même individu. Ce chapitre porte sur un système de reconnaissance multimodal combinant les images du visage et de l'iris. Les deux modalités subissent des étapes spécifiques d'extraction de caractéristiques (avec LBP pour l'iris), et leurs scores de correspondance sont fusionnés puis normalisés pour prendre une décision d'identification.

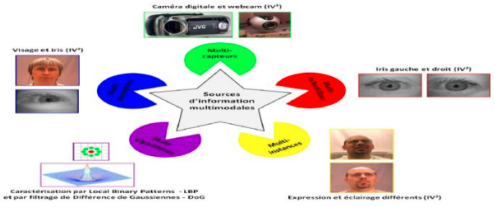


FIGURE 4.1 – Reconnaissance multimodale : fusion iris et visage

La fusion multimodale consiste à combiner plusieurs traits biométriques (ex : iris + visage) pour améliorer :

- **La précision :** Réduction des faux positifs/négatifs.
- **La sécurité :** Contourne les limites d'une modalité seule.
- **La robustesse :** Fonctionne même si une modalité échoue (ex : mauvaise luminosité pour le visage).

4.2 Principe de fonctionnement

Le processus de fusion biométrique multimodale repose sur un ensemble de procédures techniques rigoureuses. La première étape, l'acquisition des données, nécessite une capture simultanée des deux modalités.

Pour le visage, une caméra RGB standard avec une résolution minimale de 720p est utilisée, fonctionnant de préférence dans des conditions d'éclairage entre 300 et 500 lux. L'angle de capture doit être frontal, avec une tolérance de $\pm 15°$, en prenant soin de capturer la tête entière et les épaules dans le cadre.

Pour l'iris, une caméra NIR dans la gamme de longueurs d'onde 700-900nm est cruciale, positionnée entre 30-50 cm du sujet pour obtenir un angle d'au moins 200 pixels par iris sans perdre le contrôle des réflexions spéculaires, qui peuvent entraîner une déformation de la qualité de l'image.

Les images recueillies subissent ensuite une phase incontournable de prétraitement. Pour le visage, cette étape comprend une détection automatique via des classificateurs en cascade de Haar ou des réseaux de neurones profonds, suivie d'un alignement précis basé sur 68 points d'intérêt grâce à la bibliothèque Dlib. Une normalisation de l'éclairage par égalisation d'histogramme est appliquée avant un redimensionnement standard à 300x300 pixels.

Le traitement de l'iris comprend la détermination exacte des frontières pupille/iris par l'algorithme intégro-différentiel de Daug-

man, l'élimination des zones masquées par les cils ou les paupières, une transformation en coordonnées polaires pour obtenir une représentation linéaire de la texture de l'iris, et une phase finale d'amélioration de contraste par filtres de Gabor.

L'extraction des caractéristiques est un point-clé de la chaîne de traitement. Pour le visage, les approches modernes s'appuient sur des réseaux neuronaux profonds comme FaceNet, capables de produire des vecteurs de dimensions 128-512, tandis que les méthodes classiques utilisent des descripteurs comme les motifs binaires locaux (LBPH), les histogrammes de gradients orientés (HOG) ou les points d'intérêt SIFT/SURF. L'iris est codé par un algorithme sophistiqué à ondelettes selon la méthode de Daugman, qui donne un modèle irien de 2048 bits, ou plus récemment par des méthodes fondées sur des réseaux neuronaux convolutifs tels que DeepIris.

4.3 Avantages de la Fusion Multimodale

La combinaison des modalités visage et iris apporte des améliorations substantielles dans les systèmes biométriques. Du point de vue de la précision, cette stratégie permet une réduction spectaculaire des taux d'erreur, diminuant les faux positifs et les faux négatifs d'un ordre de dix par rapport aux solutions unimodales, comme le montrent les évaluations du NIST. Cette performance est justifiée par la complémentarité des modalités : la stabilité de l'iris dans la lumière infrarouge compense la sensibilité du visage aux variations lumineuses, et la facilité d'acquisition faciale compense la complexité de capture de l'iris.

La sécurité bénéficie également d'un renforcement significatif. Les tentatives de spoofing par masque facial ou photo échouent en raison de la nécessité de produire conjointement un iris valide, et inversement, les lentilles de contact artificielles sont détectées par leur contradiction avec les caractéristiques faciales. Des banques comme HSBC utilisent déjà cette synergie pour protéger leurs

transactions de luxe.

Un autre avantage principal réside dans la robustesse opérationnelle. Le système maintient ses capacités même dans des conditions altérées : un visage partiellement masqué à cause de lunettes ou d'un masque est compensé via l'iris, et inversement, une capture difficile de l'iris due aux reflets est compensée par les informations faciales. Cette redondance intelligente garantit un niveau élevé de disponibilité pour le système.

Enfin, l'expérience utilisateur est optimale. L'absence de contact physique, caractéristique des deux modalités, élimine les réticences sanitaires tout en maintenant des délais de réponse inférieurs à deux secondes sur les équipements modernes, comme le proposent les systèmes de déverrouillage des smartphones haut de gamme actuels.

4.4 Risques et Limites

4.4.1 Complexité Technique

- **Intégration difficile :**
  - — Synchronisation des capteurs (temps réel).
  - — Calibrage des algorithmes (poids de fusion optimaux).
- **Coût accru :**

Composant	Coût (€)
Caméra RGB	50–200
Caméra NIR (iris)	500–2000
Logiciel de fusion	10k–50k

TABLE 4.1 – Coûts des composants

4.4.2 Vie Privée et Réglementation

— **RGPD :** Stockage de multiples données biométriques nécessite :
  — Consentement explicite.
  — Chiffrement des templates (ex : AES-256).
— **Biais algorithmiques :**
  — Les performances peuvent varier selon l'ethnicité (ex : erreurs +15% pour les visages noirs, étude MIT).

4.4.3 Vulnérabilités Résiduelles

- **Attaques sophistiquées :**
  — Deepfakes + lentilles iris synthétiques.
  — Détournement des canaux de fusion (MITM).
- **Solution :** Ajouter de la détection de vivacité (ex : micro-mouvements pupillaires).

4.5 Méthodes de Fusion

La fusion multimodale peut se produire à différents niveaux de la chaîne de traitement, chacun ayant des caractéristiques techniques uniques.

Au niveau du capteur, la méthode la plus précoce consiste à fusionner directement les images brutes des différentes modalités avant tout traitement. Ainsi, par exemple, on peut superposer une image faciale RGB avec une image d'iris en proche infrarouge pour générer une représentation composite. L'opération se réalise habituellement par l'intermédiaire de fonctions de pondération d'image telles que `cv2.addWeighted()` d'OpenCV, où chaque source est assignée un coefficient spécifique. Le plus grand intérêt réside dans l'élimination précoce du bruit par combinaison des informations

complémentaires, mais cette technique n'a pas de grande flexibilité pour des modalités très hétérogènes.

La fusion au niveau des caractéristiques est effectuée après avoir extrait les traits uniques de chaque modalité. Elle se fait par concaténation des vecteurs de caractéristiques - par exemple, un vecteur facial 128D obtenu à l'aide de FaceNet et un vecteur iridien 2048 bits obtenu à l'aide de l'algorithme de Daugman - afin de créer un espace de représentation commun de dimension élevée (2176D dans cet exemple). Pour compenser la malédiction de la dimensionnalité, des techniques de réduction de dimension telles que l'Analyse en Composantes Principales (PCA) ou l'Analyse Discriminante Linéaire (LDA) sont ensuite utilisées. Bien que plus complexe à mettre en œuvre, cette stratégie offre une précision plus élevée grâce à la préservation des informations discriminantes de chaque modalité.

Au niveau de la décision, la fusion est effectuée sur les scores de similarité finaux. Les plus courantes sont la moyenne pondérée (par exemple avec les pondérations 0,6 pour l'iris et 0,4 pour le visage) ou des régimes de vote majoritaire. Cette solution, facilement implémentable avec `numpy.average()` en Python, offre beaucoup de flexibilité et permet l'introduction facile de modalités additionnelles. Elle nécessite en revanche un étalonnage fin des poids et seuils de décision pour obtenir des performances optimales.

4.6 Bilan Final

4.6.1 Avantages et Limites de l'Approche Multimodale (Iris + Visage)

La biométrie multimodale combinant iris et visage représente une avancée significative dans les systèmes d'authentification modernes. Son principal atout réside dans l'amélioration spectacu-

laire de la précision, avec une réduction d'un facteur 10 des taux d'erreur par rapport aux solutions unimodales. Les systèmes aéroportuaires comme PARAFES démontrent cette efficacité en atteignant des niveaux de précision avoisinant les 99,9%. La sécurité bénéficie également d'un renforcement considérable grâce à la complémentarité des formes : les tentatives de spoofing par photo ou masque facial échouent face à l'obligation de présentation simultanée d'un iris valide, et les lentilles de contact synthétiques sont détectées par leur incohérence avec le visage.

La résistance fonctionnelle est un autre avantage majeur. Le système conserve ses performances dans des environnements variés : lorsque le visage d'un individu est partiellement caché derrière des lunettes ou un masque, l'iris prend le relais pour assurer la sécurisation de l'authentification, et inversement, des problèmes de capture d'iris dus à des reflets sont compensés par les informations faciales. Cette polyvalence promet des applications allant des contrôles d'enregistrement dans les aéroports aux systèmes bancaires sécurisés, en passant par le déverrouillage des smartphones de nouvelle génération.

Cependant, la technologie présente des défis importants. Les exigences techniques nécessitent une coordination précise des capteurs en temps réel et un ajustement fin des poids de fusion entre les modalités. Les coûts restent relativement élevés en matériel, notamment avec les caméras spécialisées en proche infrarouge nécessaires pour l'iris. Sur le plan éthique, le stockage de plusieurs données biométriques sensibles soulève des questions essentielles en matière de respect de la vie privée et de risques potentiels de surveillance de masse, encadrées par des réglementations strictes comme le RGPD en Europe.

4.6.2 Applications Industrielles et Projets de Recherche Futurs

L'industrie s'intéresse de plus en plus à ces technologies. Les fabricants de smartphones emploient progressivement des solutions qui intègrent la reconnaissance faciale et de l'iris, comme dans le système d'authentification du Samsung Galaxy. Les initiatives de villes intelligentes à Dubaï ou en Chine mettent en œuvre des réseaux de caméras multimodales pour la surveillance en temps réel, et le secteur bancaire utilise de telles solutions pour vérifier les transactions sans contact.

La recherche future s'oriente vers plusieurs directions prometteuses. Les algorithmes de fusion adaptative, capables de réajuster dynamiquement les pondérations de chaque modalité en fonction des caractéristiques environnementales, contribueraient significativement à l'amélioration des performances. Les techniques anti-spoofing croisées, combinant par exemple l'analyse des micromouvements pupillaires et la reconnaissance d'expressions faciales naturelles, renforceront la sécurité contre les attaques évoluées. Le concept de biométrie continue, permettant une authentification passive et transparente par des caméras omniprésentes, est une perspective intéressante mais soulève également de sérieuses questions éthiques.

Ces avancées techniques doivent s'accompagner d'un cadre réglementaire rigoureux. L'Union européenne, par exemple, débat de l'interdiction de la reconnaissance faciale dans les lieux publics, ce qui reflète l'équilibre délicat à trouver entre développement technologique et préservation des droits individuels. La biométrie multimodale du futur reposera donc sur le maintien d'une excellence technique associée à une approche éthique et équitable.

Chapitre 5

Cybersécurité Appliquée à la Biométrie

5.1 Introduction

Alors que le numérique continue de s'imposer, la biométrie se révèle être un pilier essentiel de la cybersécurité. L'authentification biométrique offre un moyen sûr et pratique pour vérifier l'identité d'un individu, minimisant ainsi les risques associés aux méthodes d'authentification conventionnelles.

5.2 Le rôle de la biométrie dans la cybersécurité

Les technologies biométriques ont connu un succès croissant dans le domaine de la cybersécurité, car elles représentent un niveau de sécurité et de commodité supérieur à celui des systèmes d'authentification traditionnels. En exploitant des attributs physiologiques ou comportementaux uniques, les entreprises peuvent vérifier l'identité d'un individu, permettant ou non l'accès à des installations physiques ou virtuelles. L'authentification biométrique présente plusieurs avantages :

5.2.1 Sécurité renforcée

Les identifiants biométriques possèdent un caractère unique et sont difficiles à contrefaire, rendant improbable l'accès de personnes non autorisées à des informations sensibles. Même si un gabarit biométrique est volé, il ne peut pas être utilisé efficacement car sa mise en œuvre nécessite la présence physique de la personne (le titulaire de l'empreinte).

5.2.2 Commodité pour l'utilisateur

Contrairement aux mots de passe et aux codes PIN qui peuvent être oubliés ou perdus, l'authentification biométrique repose sur des caractéristiques que l'on possède naturellement. Plus besoin de les mémoriser, et l'accès est rapide et fluide.

5.2.3 Prévention de la fraude

La biométrie constitue un moyen de sécurité efficace contre les risques d'usurpation d'identité. En vérifiant les caractéristiques intrinsèques d'un individu, les organisations peuvent s'assurer de l'identité des personnes ayant accès à des informations sensibles, réduisant ainsi le risque d'activités frauduleuses.

5.3 Menaces pour la sécurité biométrique

La biométrie, bien qu'elle offre de nombreux avantages, reste vulnérable à diverses menaces qu'il est crucial de comprendre pour assurer l'efficacité des mesures de sécurité mises en place.

Les attaques par usurpation d'identité consistent à reproduire ou imiter les caractéristiques biométriques d'un individu, telles que les empreintes digitales, la voix ou même le visage en 3D, afin d'accéder illégalement à un système, posant ainsi un défi important aux systèmes biométriques classiques.

Les violations de données constituent une autre menace sérieuse, puisque les informations biométriques, tout comme les données personnelles, peuvent être compromises en cas d'atteinte à la base de données d'un organisme, ce qui peut entraîner des usurpations d'identité et des conséquences graves en matière de sécurité.

En outre, l'utilisation croissante de la biométrie soulève également des préoccupations légitimes en matière de protection de la vie privée, car de nombreuses personnes se montrent réticentes à fournir leurs données biométriques sensibles par crainte d'un usage abusif ou d'un accès non autorisé, ce qui oblige les organisations à faire preuve de transparence et à respecter les réglementations en vigueur pour instaurer un climat de confiance.

5.4 Étude de cas : Vulnérabilité dans les systèmes biométriques

En 2017, le Samsung Galaxy S8 a été salué comme un smartphone de pointe, vantant des fonctionnalités biométriques avancées telles que la reconnaissance faciale et l'authentification par scanner d'iris. Cependant, ces technologies ont rapidement montré leurs limites en matière de sécurité.

5.4.1 Reconnaissance faciale

Peu après sa sortie, des experts en sécurité ont démontré que la reconnaissance faciale du Galaxy S8 pouvait être facilement contournée. Par exemple, un test a montré que le téléphone pouvait être déverrouillé en présentant simplement une photo de l'utilisateur devant l'appareil. Cette vulnérabilité a été mise en évidence par des vidéos partagées en ligne, notamment par l'expert Marciano Tech lors de l'événement de lancement du S8 à New York. Samsung a réagi en précisant que la reconnaissance faciale était une fonctionnalité de commodité et non une mesure de sécu-

rité robuste. L'entreprise a recommandé d'utiliser des méthodes plus sécurisées, telles que le scanner d'iris ou l'empreinte digitale, pour des applications sensibles comme Samsung Pay.

5.4.2 Scanner d'iris

Le scanner d'iris du Galaxy S8, présenté comme une alternative plus sécurisée, a également été compromis. Le Chaos Computer Club (CCC), un groupe de hackers allemands, a démontré qu'il était possible de contourner ce système en utilisant une photo de l'œil de l'utilisateur, une imprimante et une lentille de contact pour simuler la courbure de l'œil. Cette démonstration a révélé que même des systèmes biométriques avancés pouvaient être vulnérables à des attaques relativement simples, mettant en lumière les défis liés à la sécurité des données biométriques.

5.4.3 Conséquences et leçons tirées

Ces failles de sécurité ont eu un impact significatif sur la perception des technologies biométriques. Elles ont mis en évidence la nécessité d'intégrer des mesures de sécurité plus robustes, telles que la détection de la vivacité et l'analyse en 3D, pour prévenir les tentatives de contournement. En réponse à ces vulnérabilités, les fabricants de smartphones ont renforcé leurs systèmes biométriques, intégrant des technologies plus avancées pour garantir la sécurité des utilisateurs.

En conclusion, bien que le Galaxy S8 ait introduit des fonctionnalités biométriques innovantes, ses vulnérabilités ont servi de catalyseur pour l'amélioration des standards de sécurité dans l'industrie des smartphones. Cet épisode souligne l'importance de ne pas se fier uniquement aux technologies biométriques pour la sécurité, mais de les combiner avec d'autres méthodes de protection pour assurer une défense efficace.

5.5 Solutions aux défis de la sécurité biométrique

Pour mieux protéger la biométrie face aux menaces qui pèsent sur elle, plusieurs solutions ont été mises en place pour renforcer la sécurité tout en rassurant les utilisateurs.

La détection du caractère vivant permet de s'assurer que la personne en train de s'authentifier est bien réelle et présente, ce qui évite qu'un simple masque ou une copie d'empreinte ne suffise à tromper le système, une façon de s'assurer qu'on interagit bien avec un être humain.

À cela s'ajoute l'authentification multifactorielle qui combine différents types de vérification – ce que l'on sait comme un mot de passe, ce que l'on possède comme un badge ou un téléphone, et ce que l'on est, à travers les traits biométriques – afin de rendre l'accès encore plus sûr.

En parallèle, une surveillance continue du système permet de repérer rapidement des comportements inhabituels, comme un accès à des heures étranges ou depuis des endroits suspects, pour pouvoir réagir avant qu'un problème ne survienne.

Et bien sûr, tout cela ne serait pas complet sans un bon chiffrement et un stockage sécurisé des données biométriques, pour éviter qu'en cas de fuite, ces informations sensibles ne puissent être utilisées contre les utilisateurs, car même si quelqu'un y accède, elles resteraient protégées et inutilisables sans les bonnes clés.

5.6 Conclusion

Toutefois, les systèmes biométriques ne sont pas infaillibles, et des mesures proactives doivent être prises pour faire face aux menaces potentielles, telles que les attaques par usurpation d'identité et les violations de données. En s'appuyant sur des solutions telles que la détection de la présence, l'authentification multifactorielle, la surveillance continue et le stockage sécurisé, les organisations peuvent améliorer leur posture de cybersécurité et protéger efficacement leurs données sensibles.

Chapitre 6

Conclusion générale

La biométrie est devenue essentielle dans notre vie quotidienne. Cette technologie utilise nos caractéristiques physiques pour nous identifier et nous authentifier. Pensez aux empreintes digitales, à la reconnaissance faciale ou même à l'analyse de l'iris. Elle assure notre sécurité dans un monde de plus en plus connecté. Cependant, derrière cette avancée se cachent des défis. La protection des données personnelles reste cruciale. Les utilisateurs doivent être conscients des risques dès qu'ils partagent leurs informations biométriques. Une fuite d'informations peut entraîner des conséquences désastreuses pour la vie privée d'un individu. Les entreprises doivent donc être vigilantes et responsables dans la gestion des données biométriques. Dans le secteur des services financiers, la biométrie offre des solutions pratiques pour renforcer la sécurité. Les transactions peuvent être validées instantanément grâce à des techniques biométriques, ce qui facilite l'expérience utilisateur. De même, dans le domaine de la santé, les systèmes biométriques protègent les dossiers médicaux sensibles, garantissant ainsi la confidentialité des patients. Les applications de la biométrie touchent également les voyages et les contrôles d'identité. Les aéroports utilisent des systèmes de reconnaissance faciale pour accélérer le passage des voyageurs. Cela réduit les files d'attente tout en améliorant la sécurité. C'est une véritable révolution dans

la gestion des flux de personnes. En somme, la biométrie, bien que prometteuse, nécessite une approche équilibrée. La technologie doit évoluer tout en préservant la confidentialité et la sécurité des individus. Nos données personnelles méritent le respect et la protection qu'elles nécessitent. Le bon équilibre entre innovation et éthique sera la clé pour l'avenir de la biométrie.

Bibliographie

[1] HFSecurity, *Qu'est-ce que la biométrie multimodale*, 2021. Disponible en ligne : https://hfsecurity.cn/fr/quest-ce-que-la-biometrie-multimodale/

[2] Université de Guelma, *Un système biométrique multimodal basé sur la fusion visage-iris*, mémoire de Master, 2020. Disponible en ligne : https://dspace.univ-guelma.dz/xmlui/handle/123456789/14246

[3] Libor Masek, *Code MATLAB pour la reconnaissance de l'iris*, 2003. Disponible en ligne : https://www.peterkovesi.com/studentprojects/libor/index.html

[4] Qingbao, *Iris Recognition Algorithms - GitHub*, 2020. Disponible en ligne : https://github.com/Qingbao/iris

[5] Adrian Rosebrock, *Reconnaissance faciale avec LBPH et OpenCV*, 2021. Disponible en ligne : https://pyimagesearch.com/2021/05/03/face-recognition-with-local-binary-patterns-lbps-and-opencv/

[6] Akarsh Zingade, *Détection et reconnaissance faciale avec OpenCV et Dlib - GitHub*, 2019. Disponible en ligne : https://github.com/akarshzingade/face_detection_recognition_dlib_opencv

[7] Pooja Sharma et Jyoti Rana, *Vue d'ensemble des techniques de fusion dans la biométrie multimodale*, IJERT, 2013. Disponible en ligne : https://www.ijert.org/research/

overview-of-fusion-techniques-in-multimodal-biometrics-IJERTCONV2
pdf

[8] R.H. Tapia et al., *Comparaison des niveaux et des approches de fusion pour la biométrie multimodale*, 2021. Disponible en ligne : https://www.researchgate.net/publication/353752911_Comparison_of_levels_and_fusion_approaches_for_multimodal_biometrics