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

Université A. Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Intelligence Artificielle

Thème

Système d'authentification biométrique multimodal à base du visage et de la signature

Présenté par : Slimani Nassima et Taguelmimt Lilia

Soutenu le 27 septembre 2022 devant le jury composé de :

Présidente	**Dr N. BOUADEM**	**Maître de conf. B**	**U. A/Mira Béjaia.**
Encadrant	**Dr A. ACHROUFENE**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Examinatrice	**Dr S. ZEBBOUDJ**	**Maître de conf. B**	**U. A/Mira Béjaia.**

Béjaïa, septembre 2022.

Remerciments

Notre gratitude va d'abord vers Allah, le tout miséricordieux qui nous a accordé la patience et le courage, nous permettant de finaliser notre mémoire.

Nous remercions notre jury pour la lecture et l'évaluation sincère et constructive de ce modeste travail.

Nous remercions particulièrement notre encadreur, monsieur Achroufene qui n'a pas ménagé ses efforts pour nous guider, en nous accordant son temps, ses conseils avisés et ses critiques constructives qui nous ont constamment poussées à nous améliorer à chaque étape.

Nous exprimons notre profonde gratitude à nos professeurs d'université auprès de qui nous avons acquis des connaissances inestimables.

Un merci à nos amies, Lydia, Mina et Sofia, notre source de courage et joie quotidienne et dont le soutien ne failli jamais.

À nos familles et nos proches respectifs qui nous ont soutenu et épaulé depuis toutes petites jusqu'à ce jour. Nous les remercions pour leur patience, leurs encouragements constants et inconditionnels.

Enfin, nous remercions toutes les personnes ayant joué un rôle, aussi grand ou petit soit-il, dans la réalisation de cet écrit.

Table des matières

Table des figures

Liste des abréviations

ACC	Accuracy
ACP	Analyse en Composantes Principales
AUMI	Aspect United Moment Invarient
BBA	Basic Belief Assignment
BLSTM-NN	Bidirectional Long Short-Term Memory Neural Network
BSA	Backtracking Search optimization Algorithm
CE	Cross Entropy
CLAHE	Contrast Limited Adaptive Histogram Equalizations
CMC	Cumulative Match Characteristic
CNN	Convolutional Neural Network
CS	Compressing Sensing
DET	Detection Error Tradeoff
DST	Dempster Shafer Theory
DTW	Dynamic Time Warping
ECG	ElectroCardioGram
EEG	ElectroEncephaloGram
EER	Equal Error Rate
f-MLP	Fuzzy-Multi-Layer Perceptron
FAR	False Acceptation Rate
FCM	Fuzzy C-Medoid
FN	False Negative
FP	False Positive
FRR	False Rejection Rate
GIF	Graphics Interchange Format
GPU	Graphics Processing Unit
HBF	HyBrid Fusion
IA	Intelligence Artificielle
KDCV	Kernel Discriminative Common Vector

KNN	K-Nearest Neighbors
LBP	Localy Binary Pattern
LDP	Local Directional Patern
LPQ	Local Phase Quantization
NN	Nearest Neighbors
ORL	Olivetti Research Laboratories
PCA	Principal Component Analysis
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PTZ	Pan Tilt Zoom
ROC	Receiver Operating Characteristic Curve
RR	Recognition Rate
SS	Sub-Sampling
SVM	Support Vector Machines
TN	True Negative
TP	True Positive
TPR	True Positive Rate
WHBF	Weighted Hybrid Fusion

Introduction générale

Aussi bien pour les restrictions d'accès à des systèmes physiques ou logiques, que pour la reconnaissance d'individus, l'authentification et l'identification sont des outils de plus en plus indispensables dans beaucoup de cas d'applications tels que la restriction d'accès à des comptes bancaires, la reconnaissance des personnes via caméra de surveillance, ou encore, la protection des locaux privés des entreprises.

Diverses méthodes sont utilisées à cet effet telles que la mise en place de systèmes d'authentification par mot de passe, l'utilisation des clés, des cartes magnétiques ou bien des codes PIN. Ces solutions utiles présentent néanmoins des risques de sécurité tels que leur fragilité aux éventuels vols, pertes, oublies, ou autre. L'usage des traits biométriques à l'instar de ces moyens classiques est, de ce fait, étudié en tant que méthode de reconnaissance des personnes.

La biométrie est un concept se basant sur le principe d'unicité des individus selon plusieurs critères physiques (iris, empreintes, réseaux veineux, etc.) et comportementaux (voix, signatures, démarche, etc.). Elle constitue une mesure fiable permettant l'authentification ou l'identification des individus en leur accordant une forme d'identification unique et universelle. Les systèmes conçus à cet effet prennent en entrée des données biométriques, nommées modalités, à des fins d'authentification ou d'identification.

Dans la pratique, les systèmes biométriques basés sur une seule modalité sont restrictifs en termes de performances. En effet, les traits biométriques tels que le visage, la voix ou encore les empreintes, peuvent présenter chacune, des limitations liées à divers facteurs tels que le mode d'acquisition, les différences entre les échantillons d'un seul individu, les effets du temps sur les traits biométriques, etc [50].

Une solution à ces limitations est les systèmes biométriques multimodaux qui exploitent plus d'une modalité appartenant à la même personne [114]. C'est dans cette direction que s'insère le présent travail qui a pour but la mise en œuvre d'un système d'authentification biométrique multimodal fusionnant les modalités visages et signatures en utilisant la théorie de Dempster-Shafer [161].

Pour cela, ce document est composé de quatre chapitres. Le premier a pour but d'introduire des généralités et quelques définitions sur la biométrie et les systèmes d'authentification biométriques. Le deuxième chapitre est un état de l'art des travaux récents portant sur l'authentification basée sur la multimodalité biométrique. Le troisième chapitre, quant à lui, vise à expliquer

le processus d'authentification biométrique multimodal du système proposé. Le dernier chapitre présente les détails d'implémentation ainsi que les résultats obtenus des différents tests effectués.

Chapitre 1

Généralités sur la biométrie

1.1 Introduction

Les avancées technologiques de nos jours arrivent à différencier entre les individus en associant à chaque personne une sorte d'identification unique difficilement réplicable. Ces informations, dites biométriques, peuvent être physiologiques ou comportementales, et présentent une utilité particulière pour toute sorte de domaines comme la médecine. En effet, étant donné que les informations biométriques, aussi appelées modalités, permettent la distinction exacte entre les individus, elles sont aussi utilisées dans des systèmes, dit systèmes biométriques, permettant l'acquisition et le traitement de ces informations. Le point de départ de ce travail est donc un chapitre définissant toutes ces notions importantes autour de la biométrie, ainsi que des détails sur les systèmes biométriques utilisant une ou plusieurs modalités.

1.2 Définition de la biométrie

La biométrie signifie au sens littéral "mesure du corps humain", ce terme est aujourd'hui utilisé pour définir la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu et permet de manière fiable, et rapide, son authentification et son identification [26], [34].

On peut classer les mesures biométriques en deux catégories [75] : les mesures physiologiques et les mesures comportementales. Les mesures physiologiques peuvent être morphologiques ou biologiques [34], [86] :

- Biologiques : l'ADN, le sang, la salive, ou l'urine, etc ;
- Morphologiques : les empreintes digitales, la forme de la main, du doigt, le réseau veineux, l'œil (iris et rétine), ou encore, la forme du visage, etc.

En ce qui concerne les mesures comportementales, on trouve souvent parmi celles-ci [85], la reconnaissance vocale, la dynamique des signatures (vitesse de déplacement du stylo, accélération, pression exercée, inclinaison), la dynamique de frappe au clavier d'un ordinateur, la façon d'utiliser des objets, la démarche, le bruit des pas, la gestuelle, etc.

Toutes techniques biométriques doivent impérativement avoir certaines spécificités [157] :

- Universelles, car elles existent chez tous les individus ;
- Uniques, permettant ainsi de différencier un individu par rapport à un autre ;
- Permanentes, autorisant l'évolution dans le temps ;
- Enregistrables, car collecter les caractéristiques d'un individu ne peut se faire sans son accord ;
- Mesurables, autorisant une comparaison future.

Toutefois, dans le cas pratique, on ne peut trouver toutes ces spécificités dans une même modalité [170] et on remarque aussi une différence au niveau de la fiabilité des différentes techniques, selon leur catégorie. Étant donné que les mesures physiologiques sont plus stables et invariables que les mesures comportementales, celles-ci sont donc plus fiables [50].

1.3 Intérêt de la biométrie

De nos jours, la technologie biométrique est populaire non seulement dans le domaine de la sécurité publique (ex : bases de données criminelles, systèmes de surveillance par reconnaissance faciale), mais est également utilisée dans la vie de tous les jours (ex : smartphones avec identification tactile/reconnaissance faciale). De même que pour le domaine de la sécurité, l'utilisation des informations biométriques comme moyen de contrôle d'accès préféré aux mots de passe, clés, cartes magnétiques, et autres moyens en général est dû à plusieurs facteurs que les utilisateurs dans le secteur privé rapportent eux-mêmes et dont nous pouvons résumer quelques-uns [169] :

- La rapidité : étant un moyen reposant généralement sur des processus simples presque instantanés, un système biométrique est bien plus rapide, ce qui représente un avantage pratique ;

- L'efficacité et la confiance : les mesures biométriques sont généralement exactes et difficilement falsifiables et sont donc une solution de sécurité très efficace, peu fragile au vol, comme le sont les clés, les codes PIN (Personal Identification Number) ou les cartes magnétiques par exemple ;

- Le confort : le contrôle d'accès basé sur la biométrie est bien plus facile pour l'utilisateur, qui n'aura pas à apprendre un long mot de passe, ou à transporter sur lui la clé d'accès, ce qui élimine les risques d'oublie qu'il peut rencontrer en général dans les autres cas.

Autre que le domaine de la sécurité, la biométrie est utilisée dans divers autres secteurs tels que le secteur de la médecine, l'administration (carte d'identité et passeport biométriques), ou encore, dans les transactions financières dans les banques [179].

1.4 Définition d'un système biométrique

Les systèmes biométriques représentent les moyens les plus sécurisés pour l'identification et le contrôle d'accès [27], ce qui explique la croissance continue de l'industrie biométrique (voir la figure 1.1). Ils permettent de reconnaître des formes en traitant les données biométriques fournies en entrées, et les compares aux modèles de la base de données afin de réaliser des objectifs opérationnels tels que : la recherche des individus connus, la recherche des individus inconnus, vérification d'identité proclamée, etc. Ces buts sont aussi variés que les technologies existantes[178]

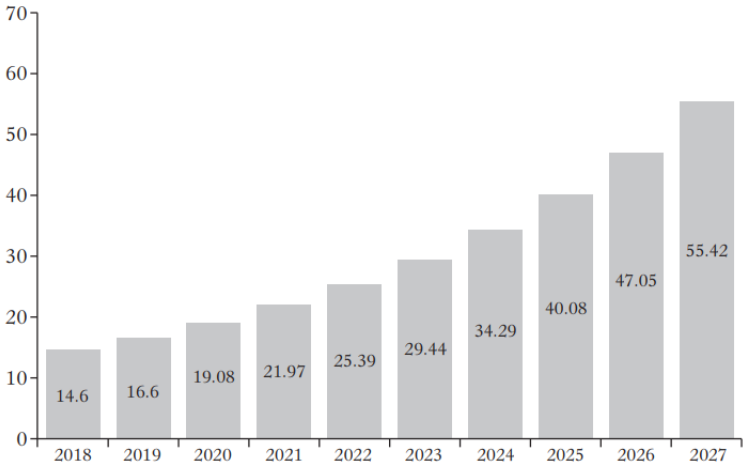


FIGURE 1.1 – Chiffre d'affaires du marché mondial des technologies biométriques de 2018 à 2027 (en milliards de Dollars américains) [169]

1.5 Architecture d'un système biométrique et principe de fonctionnement

Dans un grand nombre d'études, l'architecture des systèmes biométriques est présentée comme un ensemble de plusieurs composants (voir la figure 1.2), aussi appelés modules, dont nous pouvons lister cinq [122] :

- Module d'acquisition des données : c'est le moyen qui permet de capturer les données liées à une modalité ou un caractère biométrique. Ces capteurs peuvent être avec contact (un lecteur d'empreinte), ou sans contact (une caméra dans le cas de l'iris ou du visage) ;

- Module de traitement de signal : effectue un prétraitement des données brutes, puis les caractéristiques les plus pertinentes sont extraites, afin de former une nouvelle représentation des données, qui doit être unique pour chaque personne ;

- Module de stockage : contient les modèles biométriques des utilisateurs enrôlés dans le système. Le système de stockage peut être un simple fichier dans une carte à puce, ou bien une grande base de données gérée par un système de gestion de base de données ;

- Module de mise en correspondance (Matching) : permet de voir la similarité ou divergence de deux vecteurs biométriques en comparant les données des caractéristiques extraites, avec des modèles préalablement enregistrés dans la base de données ;

- Module de décision : une décision est prise selon les exigences de l'application du système, et suivant le résultat de comparaison qui est un score compris entre 0 ou 1 (plus la valeur est élevée, plus la correspondance est parfaite), afin de vérifier ou déterminer l'identité d'un utilisateur.

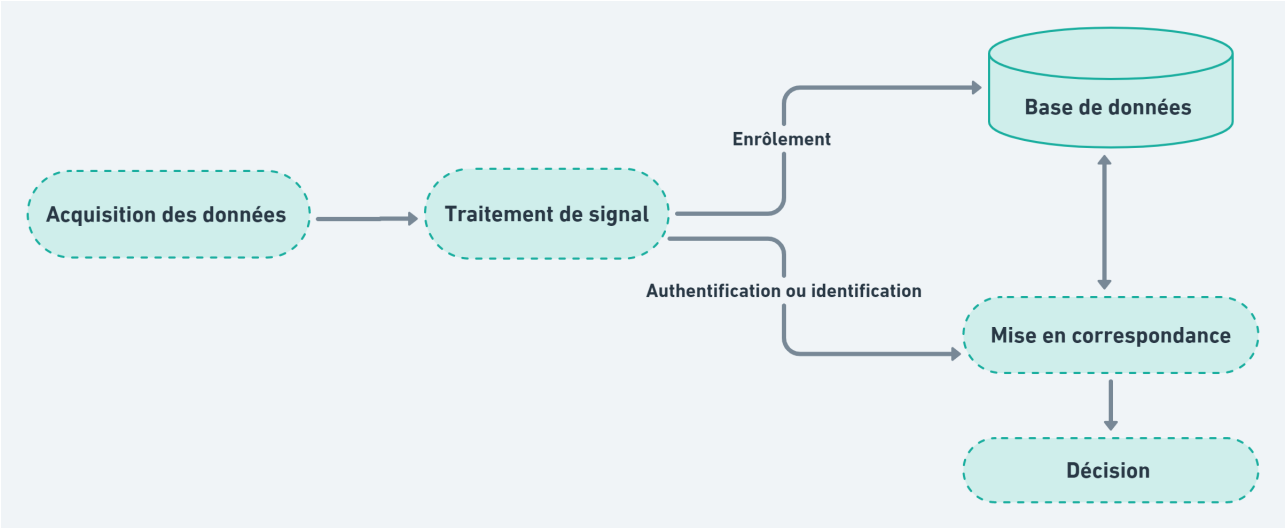


FIGURE 1.2 – Architecture globale des systèmes biométriques [179]

Le mode de fonctionnement des systèmes biométriques repose donc, sur la combinaison de ces modules, afin de réaliser les principaux processus suivants [82] :

- L'enrôlement : le système biométrique doit tout d'abord ajouter l'utilisateur à la base afin de pouvoir le reconnaître plus tard. Pour cela, le système récupère les caractéristiques biométriques à l'aide d'un capteur biométrique dans le but d'obtenir une représentation numérique de celle-ci. Une fois ces données numériques réduites à l'aide d'un algorithme d'extraction, le modèle biométrique est stocké dans une base de données ;

- La vérification : c'est la phase pendant laquelle le système doit pouvoir savoir si l'utilisateur est bien celui que l'on croit être. En comparant les informations nouvellement saisies au modèle biométrique présent déjà dans la base, le système effectue une comparaison 1 : 1 dont la réponse est dans ce cas binaire pouvant avoir un certain poids. La représentation formelle peut alors être sous forme de la fonction suivante :

$$f(C_{U'}, M_U) = \begin{cases} 1 & \text{si } S(C_{U'}, M_U) \geq \tau \\ 0 & \text{sinon} \end{cases} \tag{1.1}$$

où :
— $C_{U'}$: Vecteur d'entré représentant les caractéristiques biométriques d'un nouvel utilisateur U' ;
— M_U : Le modèle biométrique de l'utilisateur U stocké dans la base de données ;
— La fonction f : Fonction du système qui retourne un résultat booléen ;
— La fonction S : Fonction similarité définissant le taux de correspondance ;
— Le seuil τ : La valeur à partir de laquelle les deux vecteurs biométriques sont considérés comme identiques.

- L'identification : le système biométrique effectue une identification en essayant de déterminer l'identité d'une personne à partir d'une base de données. Le résultat retourné sera alors soit négatif signifiant la personne n'est pas dans la base, soit positif et donnera donc le profil le plus correspondant, ou bien une liste de plusieurs. En représentation formelle, cela correspondra à la fonction ci-dessous :

$$f(C_{U'}) = \begin{cases} I_k & \text{si} \quad max_{1 \leq k \leq N} \ \{S(C_{U'}, M_k)\} \geq \tau \\ I_0 & \text{sinon} \end{cases} \tag{1.2}$$

où :
— $C_{U'}$: Vecteur d'entré représentant les caractéristiques biométriques d'un nouvel utilisateur U' ;
— I_0 : L'identité inconnue ;
— I_k : L'identité recherchée appartenant à l'ensemble des personnes déjà enregistrées, de nombre allant de 1 à N ;
— Le seuil τ : La valeur à partir de laquelle les deux vecteurs biométriques sont considérés comme identiques ;
— M_k : Le modèle biométrique correspondant à I_k ;
— S : Fonction similarité, définissant le taux de correspondance.

La structure des systèmes biométriques est donc, de façon générique, un regroupement de plusieurs modules avec des rôles spécifiques dont le mode de fonctionnement est expliqué dans le schéma représentatif réalisé (voir la figure 1.3). Le système peut alors se charger de l'enrôlement de nouveaux utilisateurs dans la base de données, d'identifier les individus en faisant une comparaison de un à plusieurs, ou encore, de vérifier que la personne prétendue est bien celle que l'on croit être, c'est-à-dire, l'authentification. Les modules du système en question peuvent intervenir pour tous ces processus à des étapes différentes, dépendamment de l'opération effectuée.

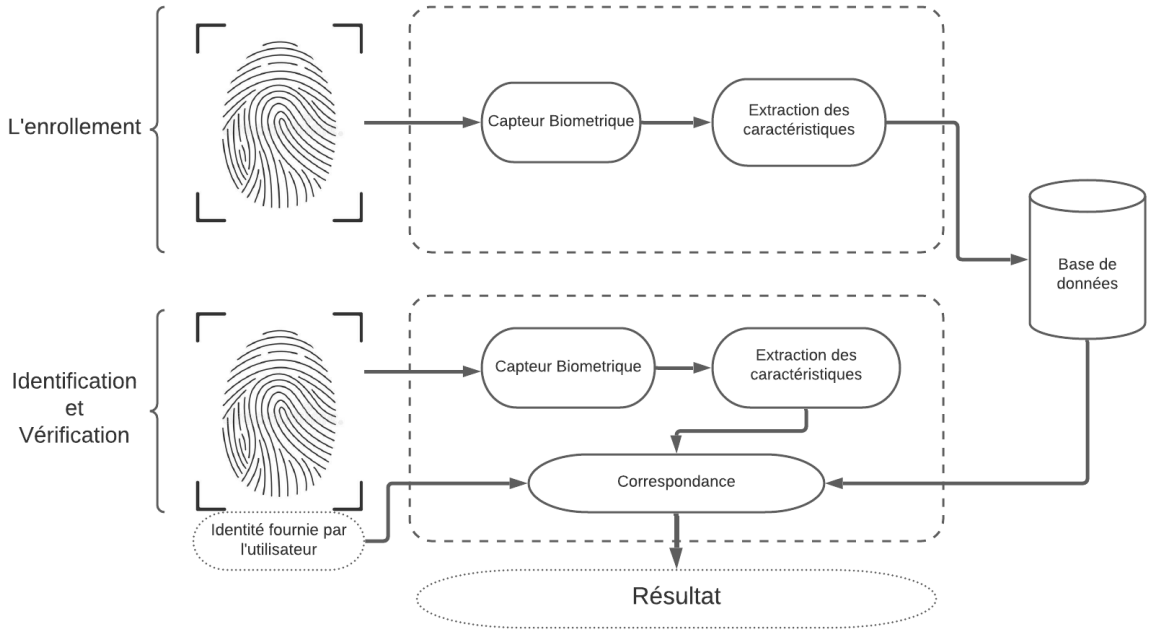


FIGURE 1.3 – Représentation simplifiée du mode de fonctionnement des systèmes biométriques

1.6 Mesures de performances d'un système biométrique

Il existe deux types d'utilisateurs qui peuvent solliciter un système biométrique, la première catégorie est les clients, ceux qui ont l'autorisation d'utiliser le système et la deuxième catégorie est les imposteurs, ceux qui n'ont pas cette autorisation, mais essaie quand même d'y accéder. Pour cela, l'évaluation des performances d'un système biométrique est indispensable et très importante [86]. Plusieurs critères sont essentiels dans l'évaluation des performances des systèmes, voici la définition de certains d'entre eux [85] :

- Taux de faux rejet ("False Rejection Rate" ou FRR) : ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système ;

$$FRR = \frac{nombre\ de\ faux\ rejets}{nombre\ total\ des\ requetes\ client} \tag{1.3}$$

- Taux de fausse acceptation ("False Acceptation Rate" ou FAR) : ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système ;

$$FAR = \frac{nombre\ de\ fausses\ acceptations}{nombre\ total\ des\ requetes\ imposteurs} \tag{1.4}$$

- Taux d'égale erreur ("Equal Error Rate" ou EER) : ce critère est très courant, ça correspond au point ou $FRR = FAR$, c'est-à-dire que ça représente généralement le meilleur compromis entre faux rejets et fausses acceptations.

$$EER = \frac{nombre\ de\ fausses\ acceptations\ +\ nombre\ de\ faux\ rejets}{nombre\ total\ d'acces} \tag{1.5}$$

La figure (1.4) illustre le FRR et le FAR à partir de distributions des scores authentiques (clients) et imposteurs.

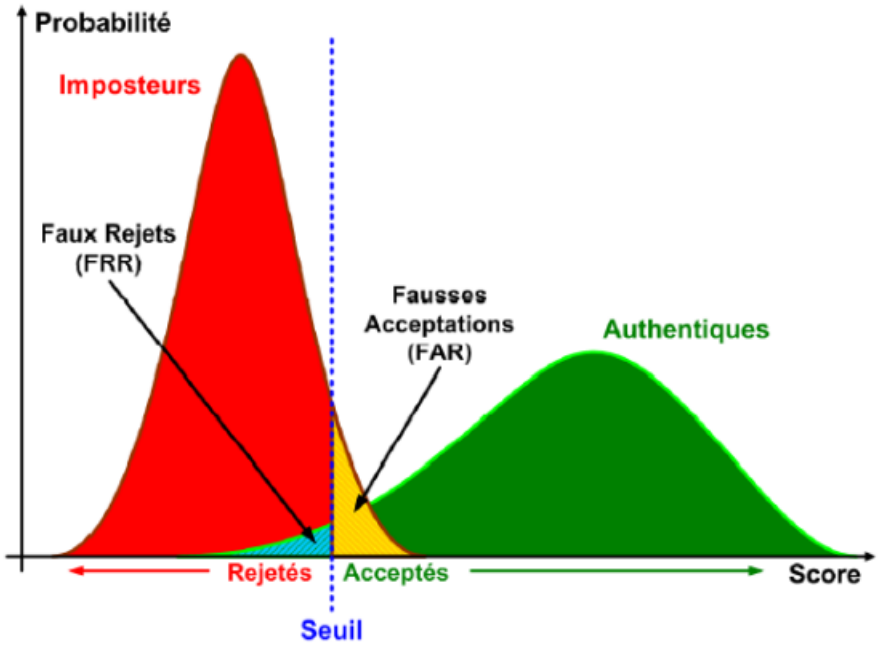


FIGURE 1.4 – Illustration du FRR et du FAR [50].

Un système biométrique est considéré performant, quand les taux des faux rejets et des fausses acceptations sont faibles, mais la relation entre FRR et FAR est de la façon suivante : un taux de FAR faible implique un taux de FRR élevé et inversement. Ces deux éléments dépendent du réglage d'un seuil qui est le résultat d'un compromis selon le choix de l'application.

Pour les applications nécessitant une grande sécurité, le choix du seuil tend vers un taux de fausses acceptations (positifs) faible, c'est-à-dire limiter au maximum les possibilités d'intrusions. Dans le cas des applications qui ne nécessitent pas de sécurité élevée, mais plutôt de commodité, c'est-à-dire le besoin de confort et utilisation aisée du système, dans ce cas, on cherche à minimiser le rejet par erreurs des personnes, ce qui veut dire que le choix du seuil tend vers un taux de faux rejet (négatifs) faible [66].

La figure (1.5) illustre la relation entre le FRR et le FAR, ainsi que le choix du seuillage.

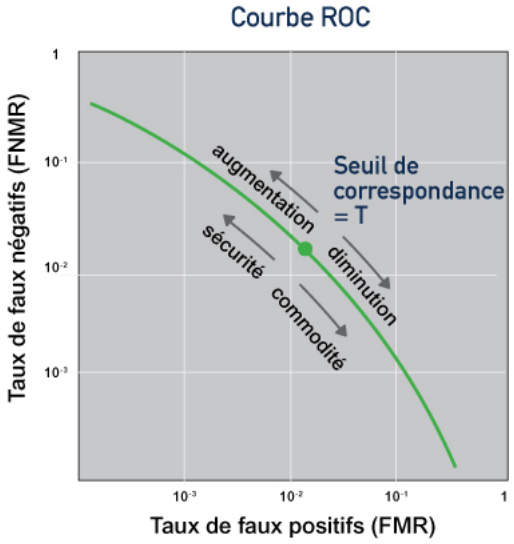


FIGURE 1.5 – Courbe ROC pour un système de recherche de correspondance biométrique et un ensemble de données [36].

La courbe "ROC"(Receiver Operating Characteristic) est celle qui permet de montrer la relation entre les critères cités précédemment. Le taux d'égale erreur peut être facilement identifiable puisqu'il s'agit de l'intersection de cette courbe avec la droite d'équation $y = x$ [68]. Il est très couramment utilisé dans le mode de fonctionnement "authentification". Pour le mode "identification", c'est la courbe "CMC" (Cumulative Match Characteristic) qui est souvent utilisée. Cette courbe donne le pourcentage de personnes reconnues en fonction du rang, plus le choix d'image de reconnaissance est proche plus la valeur du rang est petite donc le système est plus fiable [68].

Un autre critère de performance souvent utilisé est la précision (accuracy) [19]. Il représente le nombre de fois où de bonnes prédictions sont fournies. Deux formules de calcul existent pour ce critère :

$$precision = \frac{nombre\ de\ predictions\ correctes}{nombre\ total\ de\ predictions} \tag{1.6}$$

ou bien (classification binaire) :

$$precision = \frac{TP\ +\ TN}{TP\ +\ TN\ +\ FP\ +\ FN} \tag{1.7}$$

où :

- TP : nombre de vraies acceptations ;
- TN : nombre de vrais rejets ;
- FP : nombre de fausses acceptations ;
- FN : nombre de faux rejets.

1.7 Modalités biométriques

Nous pouvons définir une modalité biométrique comme étant la caractéristique de l'individu que le système biométrique capte, récupère, et analyse à des fins d'authentification ou d'identification, en suivant un certain nombre d'étapes dépendamment du type de système.

Il existe en effet différentes sortes de systèmes biométriques, relativement au nombre de caractéristiques prises en charge ainsi que le type de modalité utilisée. Dans la section qui suit, nous mettons en avant les types de modalités les plus couramment utilisées de façon individuelle, puis présentons le mode de fonctionnement des systèmes multimodaux.

1.7.1 Unimodalité

Les systèmes biométriques n'utilisant qu'une seule source d'information pour effectuer le processus d'authentification ou d'identification, sont des systèmes biométriques unimodaux qui se spécialisent dans le traitement d'un seul trait biométrique, soit physiologique ou comportementale. Nous détaillons d'ailleurs quelques modalités qui y sont incluses dans ce qui suit.

A. **Modalités physiologiques**

Les modalités physiologiques regroupent l'ensemble des traits biométriques, relatifs à la physiologie de l'individu. Il en existe un très grand nombre utilisé à des fins de reconnaissance biométrique ou autre, telles que la vérification de la parenté. Nous en citons notamment quelques-unes des plus utilisées.

La biométrie veineuse : La biométrie veineuse des doigts ou bien de la main repose sur le principe de détection des points d'intersection des veines, grâce à une lumière infrarouge à fréquence inoffensive émise par le capteur (voir la figure 1.6). Sous l'effet de cette lumière, le sang circulant dans les veines se distingue, permettant donc de dresser une sorte de carte du réseau veineux des doigts ou de la paume de la main impossible à reproduire vus la complexité des réseaux veineux et leurs différences d'un individu à un autre, ce qui constitue une identification biométrique efficace, (voir la figure 1.7). Ces dispositifs peuvent se présenter sous plusieurs formes, mais ressemble généralement à l'exemple montré dans la figure (1.8).

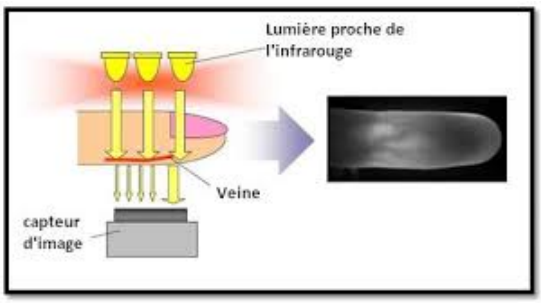


FIGURE 1.6 – Mode de fonctionnement du capteur infrarouge [12].

FIGURE 1.7 – Réseau veineux de la main sous un capteur infrarouge [13].

FIGURE 1.8 – Exemple de dispositif pour la détection biométrique veineuse [13].

La biométrie veineuse est une solution efficace qui toutefois, possède des limites liées à la sensibilité de ces systèmes à la lumière du soleil ainsi qu'aux problèmes de diminution de la circulation sanguine pouvant être occasionnés par le froid, rendant alors la détection difficile [34].

Les empreintes digitales : Une des modalités les plus utilisées aujourd'hui pour sa facilité d'utilisation et sa fiabilité, est l'empreinte digitale, qui repose sur la représentation des caractéristiques durables et non-variable [93]. Que ce soit de façon globale, en prenant l'intégralité des empreintes en compte, ou bien locale, se situant sur des zones spécifiques des images. Il existe en général trois catégories d'empreintes [2], selon la forme du motif qu'elles forment, (voir la figure 1.9).

FIGURE 1.9 – Trois types d'empreintes digitales [2]

La distinction entre les empreintes repose sur la distinction de leurs formes mais aussi l'identification des minuties. Ces dernières sont des points d'irrégularités qui se situent sur les changements des stries, pouvant prendre plusieurs formes, (voir la figure 1.10).

FIGURE 1.10 – Différentes formes de minuties des empreintes digitales [3].

Parmi les limitations de cette modalité est le fait que la qualité de l'image puisse influencer grandement les résultats. En effet, à cause des problèmes d'acquisition des empreintes, un simple bruit sur l'image peut créer une bifurcation et le manque de clarté d'une image peu rendre difficile la distinction de caractéristiques importantes que ce soit en effaçant des minuties ou en ajoutant de fausses.

Un autre défit de la biométrie des empreintes, est la modélisation des distorsions élastiques, ainsi que la variabilité intra-classe de façon efficace et sans perte d'information.

L'iris : De forme circulaire, l'anatomie de l'iris est une structure complexe composée de plusieurs éléments, (voir la figure 1.11). Étant une zone facilement accessible qui contient plusieurs informations uniques sur l'individu, elle représente un grand intérêt

pour la reconnaissance biométrique. En effet, l'iris présente des signes distinctifs permettant de différencier de vrais jumeaux, et même les deux yeux d'une même personne [50].

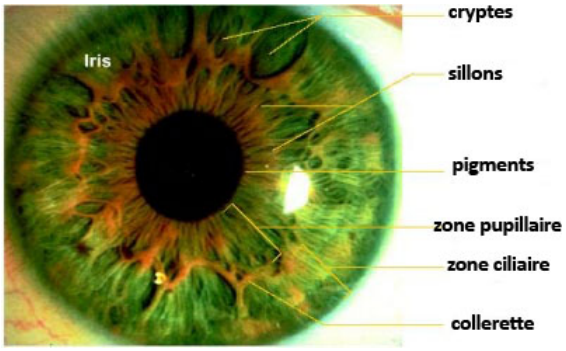


FIGURE 1.11 – Structure de l'iris [4].

L'iris, en tant que modalité de système biométrique, permet donc la reconnaissance d'une personne grâce à l'acquisition d'une image de l'iris de l'individu, à l'aide d'une caméra qui fait un balayage de l'œil à une distance courte du dispositif. À la suite de l'acquisition, l'image est traitée de façon à extraire les signes distinctifs de la personne ecomparée à une base de données afin de trouver une quelconque correspondance. Les étapes basiques d'un système biométrique traitant les images d'iris ont d'ailleurs été illustrées dans un schéma, (voir la figure 1.12). Celui-ci inclus les étapes d'acquisition, segmentation, normalisation, extraction des caractéristiques et mise en correspondance.

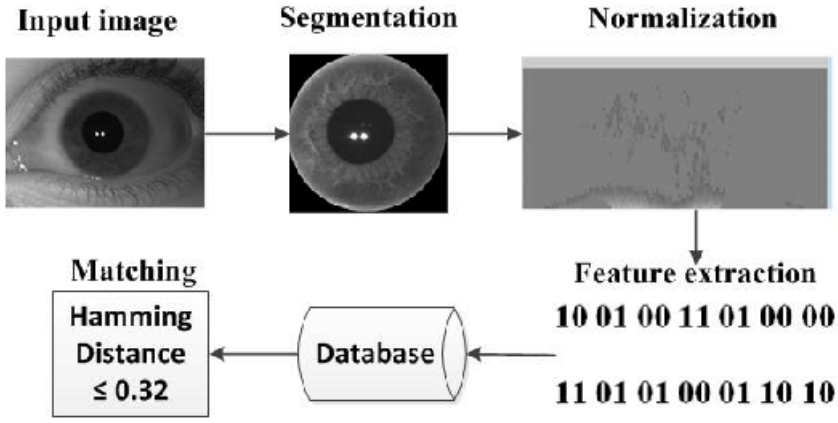


FIGURE 1.12 – Étapes basiques de la reconnaissance par l'iris [14]

Du point de vue de la sécurité, la reconnaissance par l'iris est une méthode puissante, mais qui toutefois présente certaines failles. En effet, un système biométrique reposant entièrement sur celle-ci, peu être trompé à l'aide d'une image de l'iris d'une personne présente déjà dans la base [4].

Le visage : Le système utilisant cette modalité effectue la reconnaissance en créant un modèle 2D ou bien 3D à partir de plusieurs photos de la même personne ayant été acquises par une caméra ou sur une vidéo. Le modèle du visage réalisé est alors analysé en prenant en considération certains détails distinctifs de l'individu tels que l'orientation du nez, la forme des lèvres, la taille des yeux, etc. Un exemple de cela est le modèle de la figure (1.13) qui modélise le visage en plusieurs points, avec des distances spécifiques correspondant à la position des caractéristiques de celui-ci. Grâce à l'étude de ces distances, le système peut associer à chaque individu un modèle de visage.

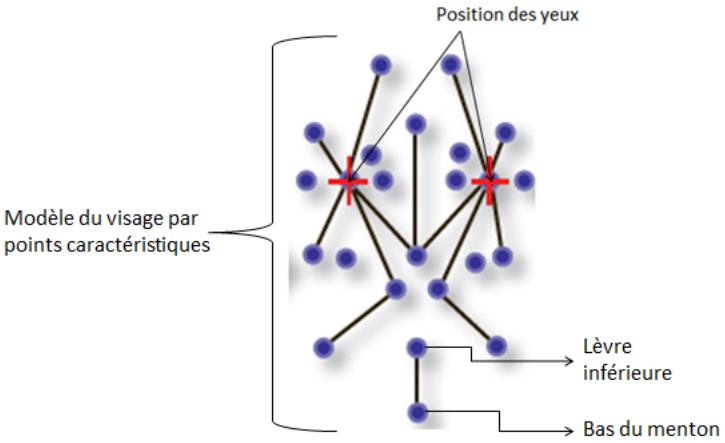


FIGURE 1.13 – Fonctionnement de la reconnaissance faciale en biométrie [11]

Bien que l'apparence du visage soit sensible au changement dans le temps, certaines caractéristiques demeurent les mêmes telles que la distance entre les deux points des yeux. Toutefois, cela peut ne pas être toujours suffisant pour distinguer entre deux personnes différentes [98].

La reconnaissance faciale est une sorte de reconnaissance de forme appliquée sur des images d'un visage, mais cette méthode est aussi utilisée pour la reconnaissance de la forme des mains ou des oreilles à des fins de reconnaissance biométrique.

B. Modalités comportementales

Les modalités comportementales sont les comportements par lesquels un individu est identifiable lorsque celui-ci effectue une action précise. Un exemple de cela, serait le comportement de la personne lorsqu'elle est en train de marcher, c'est-à-dire la vitesse, la longueur des pas, etc. Il existe différentes modalités comportementales dont nous en détaillons quelques-unes dans la section qui suit.

La voix : En se basant sur les fréquences et les variations des caractéristiques distinctives de la voix telles que les pauses silencieuses, le bégaiement, l'essoufflement, ou autre, les systèmes utilisant la modalité vocale peuvent réussir à identifier un locuteur grâce à son enregistrement vocal comparé à ceux présents dans une base, (voir la figure

1.14). Le mode de fonctionnement de ces systèmes biométriques, repose sur la distinction de la voix et non de ce qui se dit. Elle est une bonne méthode pour la distinction entre les personnes dans une même pièce.

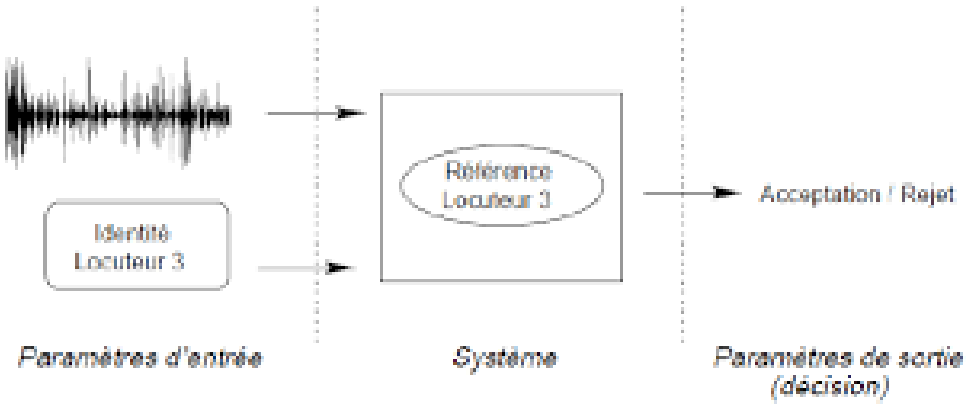


FIGURE 1.14 – Étapes basiques de la reconnaissance vocale [97]

Malgré son intérêt dans la biométrie, la sensibilité au bruit environnemental et l'imitation rendue possible par divers logiciels de synthèse vocale rendent l'utilisation de ces systèmes de façon unique peu pertinente dans le cadre d'une reconnaissance biométrique.

La signature dynamique : Les signatures manuscrites sont souvent utilisées pour des authentifications manuscrites sur des papiers administratifs importants. Elles sont une forme de gestes d'écriture de nom unique à son utilisateur. Le système garde une trace de la signature de l'intéressé auquel seront associées différentes caractéristiques indicatives de la personne (voir la figure 1.15), telles que la vitesse lors de la signature, l'accélération, la pression sur le dispositif, etc [10]. Toutes ses futures signatures seront comparées et reconnues à l'aide de ces paramètres, de sortes à constituer une matrice permettant de décider si oui ou non, la signature est celle de la personne prétendue (voir la figure 1.16). Il n'est pas rare de trouver la signature manuscrite en tant que modalité biométrique présente sur les papiers d'identifications.

FIGURE 1.15 – Exemple de reconnaissance biométrique sur deux signatures [10]

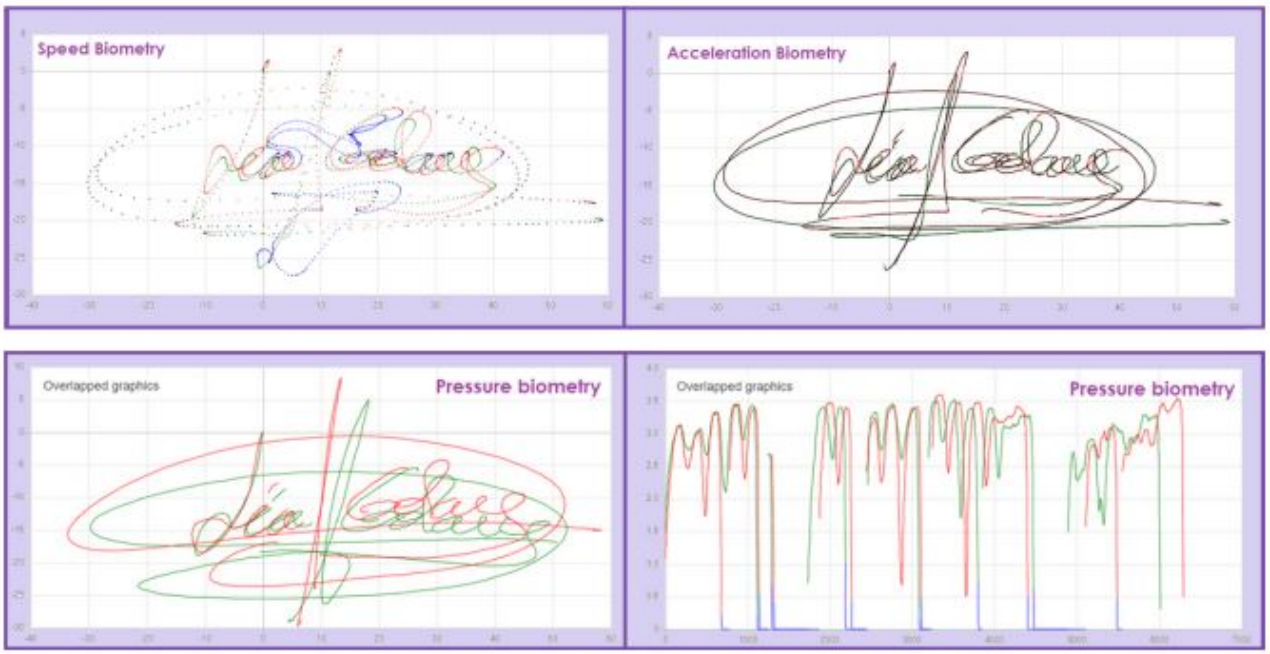


FIGURE 1.16 – Exemples des caractéristiques soulevées dans une signature[10]

Cette modalité est très répandue, mais ne constitue pas un moyen rapide de la reconnaissance biométrique.

La démarche : Plusieurs travaux s'intéressent à la démarche comme moyen d'identification, notamment pour son utilité lors du besoin d'identification d'individus sur des enregistrements de caméras de surveillance. La démarche est étudiée de sorte à en extraire des caractéristiques distinctives, telles que l'inclinaison du dos, la vitesse moyenne, etc. Un exemple de cela, est le système utilisé en Chine, (voir la figure 1.17).

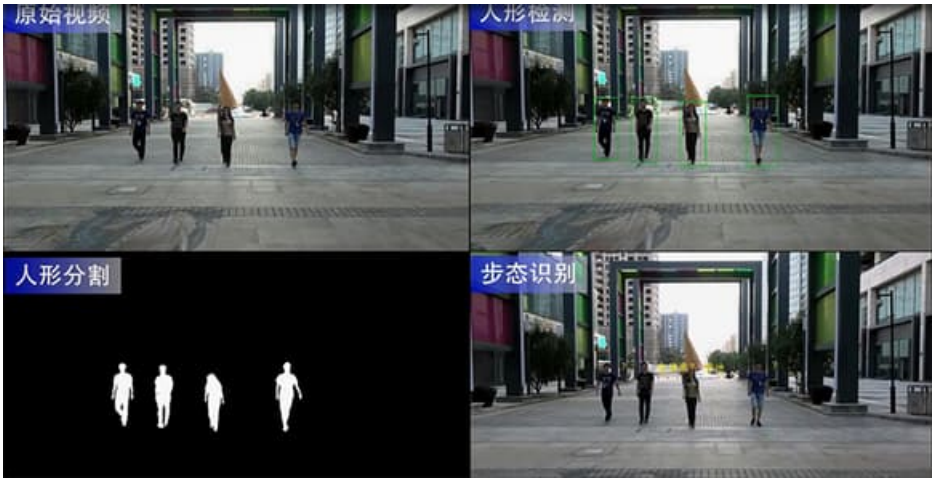


FIGURE 1.17 – Exemple d'analyse de la démarche [9]

La posture est une modalité qui peut être incluse dans la démarche car de la même façon, elle s'intéresse à la silhouette de la personne à un moment donné.

La dynamique de frappe au clavier : Cette modalité vise à l'identification de la personne grâce à sa façon de taper sur un clavier. Le mode de fonctionnement des systèmes basés sur cette technique s'appuie sur l'étape de l'enrôlement qui consiste à établir un modèle du comportement de l'utilisateur tapant sur le clavier. Plusieurs caractéristiques sont alors prises en compte telles que la vitesse de frappe, la pression sur les touches, le temps nécessaire au relâchement de chaque touche, etc. L'étape de vérification dans ce système consistera alors à capturer le comportement courant de l'utilisateur et de le comparer au modèle de son comportement usuel. Grâce à un certain seuil, le système peut classifier le comportement comme étant normale, ou bien anormale, selon les données collectées.
En se basant sur ce principe, des chercheurs ont d'ailleurs pu mettre en œuvre un clavier permettant de produire des impulsions électriques à chaque touche pressée de sorte à créer un profil de l'utilisateur auquel seront comparés les autres comportements (voir la figure 1.18).

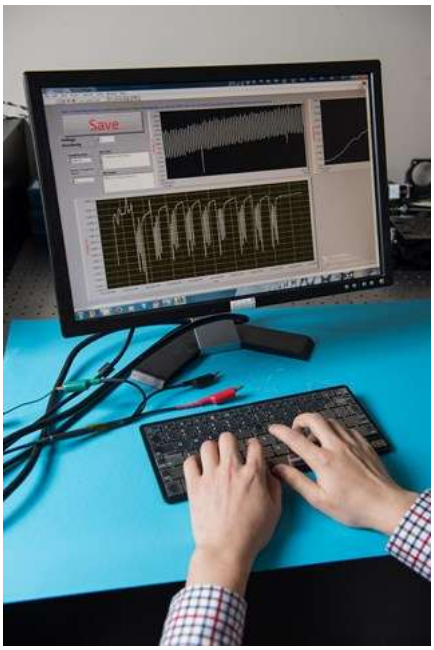


FIGURE 1.18 – Exemple de clavier biométrique [15]

Cette modalité est utile pour protéger les systèmes informatiques mais présente toutefois des problèmes de faux négatifs pouvant apparaître lors de changements abrupts de comportement sur le clavier, tel qu'une diminution soudaine de vitesse d'écriture occasionnée par l'utilisation d'une seule main par exemple.

Il existe bon nombre d'autres modalités, notamment les signaux ECG, l'ADN, l'empreinte palmaire, la géométrie de la main, et autre [170], qui peuvent présenter un intérêt particulier, dépendamment du but et le domaine d'application pour lesquels le système biométrique est conçu.

C. Limites des systèmes biométriques unimodaux

Les modalités utilisées dans les systèmes biométriques sont diverses, mais aucune n'est parfaite, car l'utilisation de chacune fait face à des limitations pouvant engendrer des problèmes lors de l'utilisation de ces systèmes. D'un point de vue plus général, nous pouvons résumer certaines de ces limites en ces quelques points [50] :

- Le bruit sur la donnée capturée : une donnée censée être valide peut être plus compatible à cause de bruits originaires d'un capteur endommagé ou même juste mal entretenu comme le cas d'accumulation de poussière sur un capteur d'empreinte, le dommage ou le bruit peut aussi venir de la source des données : cicatrisation de la main ou d'empreinte, changement de couleur des cheveux, barbe plus longue, etc ;

- Les variations intra-classe : à cause des conditions différentes ou comportements incorrects d'un individu pendant la phase d'authentification, les données résultantes

peuvent être très variées par rapport aux données enregistrées dans la base de données ;

- Unicité : tandis qu'on s'attend à recevoir certains traits biométriques de manière unique pour chaque individu, on s'aperçoit que ce n'est pas toujours le cas, ceci implique comme résultat une fausse acceptation ;

- Non-universalités : certains traits biométriques qui en général sont universels, peuvent ne pas être utiles et présentent un défi dans le cas de quelques catégories d'utilisateurs telles que les personnes handicapées ou malades ;

- Les attaques : c'est toute tentative de falsification d'un trait biométrique afin de tromper le système et d'avoir accès de manière illégitime. Ces attaques peuvent cibler les caractéristiques comportementales (imitation d'une voix), tout comme les caractéristiques physiologiques (construction d'empreintes artificielles).

1.7.2 Multimodalité

La multimodalité est l'utilisation de plusieurs modalités biométriques. Cette démarche permet d'améliorer la robustesse du système, et les résultats par rapport aux taux de faux positifs et faux négatifs. Un exemple simple de l'utilité de la multimodalité, est lors du refus d'une personne censée être authentifiée à cause d'un changement dans un trait biométrique tel qu'une cicatrice sur le doigt, ou bien une barbe sur le visage. Un système reposant sur d'autres modalités pourra facilement reconnaître la personne en prenant en compte un autre trait biométrique.

A. **Types de multimodalité**

Le fonctionnement d'un système multimodal repose sur le principe de tirer profit de plusieurs sources d'informations en les combinant dans le but de surmonter les limites d'utilisation d'une seule modalité. En général, on trouve 5 types de fusion de modalités [100] :

- Systèmes multi-capteurs : acquisition du même trait biométrique par différents capteurs (capture des traits du visage avec une caméra digitale et webcam) ;

- Systèmes multi-échantillons : effectuer plusieurs captures d'une même modalité, et associer ces échantillons du même trait biométrique. (Exemple : capture de la vue frontale du visage ainsi du profil gauche et droite) ;

- Systèmes multi-instances : considérer la variation interpersonnelle par acquisition du même caractère biométrique sur plusieurs intervalles temporaux en faisant usage du même capteur. (Exemple : plusieurs captures du visage et un changement d'expression sur chaque instance) ;

- Systèmes multi-algorithmes : combinaison de plusieurs algorithmes dans le traitement d'image ;

- Systèmes multi-biométries : combinaison de plusieurs et différentes modalités ou traits biométriques (système biométrique basé sur l'iris et l'empreinte).

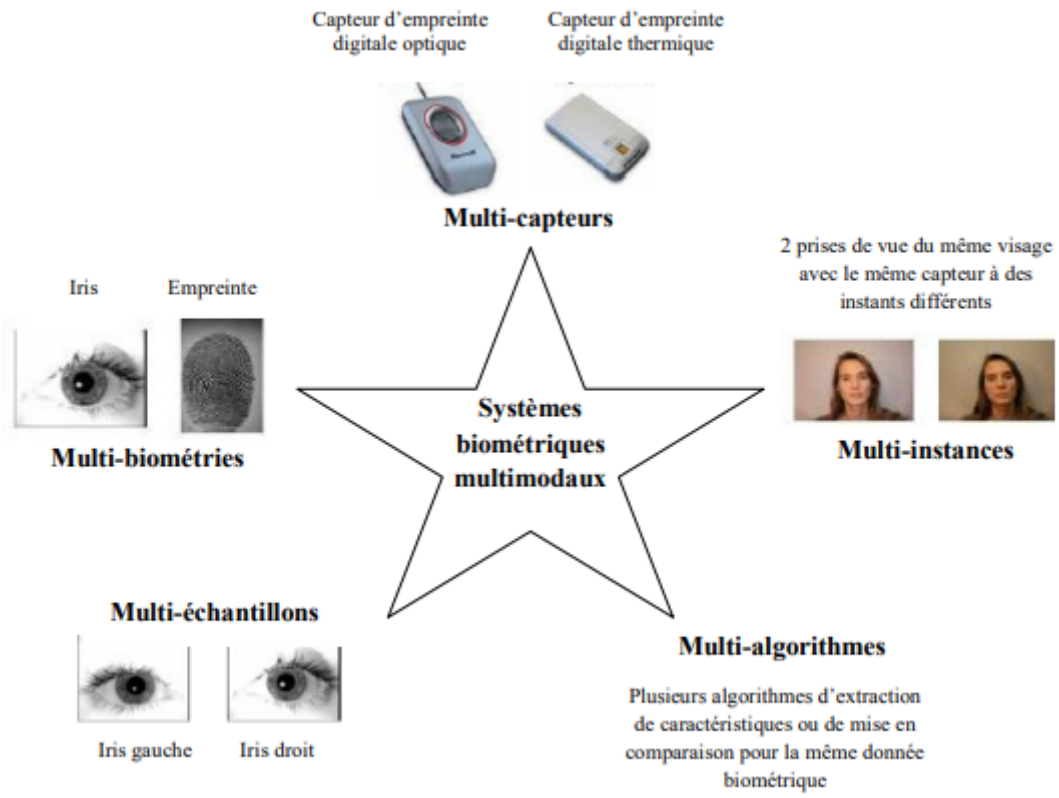


FIGURE 1.19 – Différents systèmes multimodaux [50].

B. Fusion multimodale

Le processus d'intégration d'informations provenant de diverses modalités et la combinaison de ces dernières est le concept connu sous le nom de fusion multimodale [81]. La fusion biométrique peut intervenir dans quatre niveaux [50] :

- Fusion au niveau des capteurs : c'est une combinaison des données brutes (Raw Data) au niveau des capteurs, cette fusion peut se faire soit dans le cas d'acquisition de plusieurs instances d'une même caractéristique biométrique provenant de plusieurs capteurs compatibles, ou d'un seul capteur car cette fusion nécessite une homogénéité des données.

- Fusion au niveau des caractéristiques : la fusion au niveau des caractéristiques consiste à combiner différents vecteurs des caractéristiques dans un seul vecteur commun. Les données des vecteurs des caractéristiques sont obtenus par les sources suivantes :

la même donnée biométrique en utilisant plusieurs capteurs, multiples instances, ou plusieurs traits biométriques. Si les données d'entrée sont homogènes le vecteur résultant est calculé comme une somme pondérée des vecteurs des caractéristiques individuelles. Si ces données sont hétérogènes, on effectue une concaténation des différents vecteurs pour avoir le vecteur commun.

- Fusion au niveau des scores : dans les systèmes biométriques multimodaux, la fusion au niveau des scores est la plus utilisée, car elle permet d'avoir des informations riches, et de faire une implémentation facile. De plus, on note parmi ses avantages la facilité d'accès aux scores générés par les différents sous-systèmes. Les modules de comparaison de ces derniers génèrent des scores qui, combinés, produisent un score total, plus précisément un vecteur de dimension égale aux nombres de sous-systèmes qui sera remis ensuite au module de décision. Un score est une valeur numérique qui désigne le degré de similarité entre deux individus. Cette approche est souvent considérée dans la littérature comme un problème de " Multiple Classifier Systems " [64].

- Fusion au niveau des décisions : cette fusion est effectuée quand chaque sous-système remet une décision selon ses données d'entrées. Une décision est généralement sous forme de OUI, ou NON, qu'on peut représenter par 1 ou 0. [64]. Pour arriver à la décision finale, il existe plusieurs manières telles que les règles « OU et ET », le vote par majorité, etc.

- Fusion au niveau des rangs : c'est une fusion qui s'effectue lorsque chaque classificateur d'un système biométrique multimodal associe un rang à chaque identité inscrite. Plus le rang est élevé, plus la correspondance est forte. Ces rangs, une fois attribués, sont consolidés entre eux afin de former un nouveau rang associé à une identité donnée dans le but d'aide à la décision finale [130].

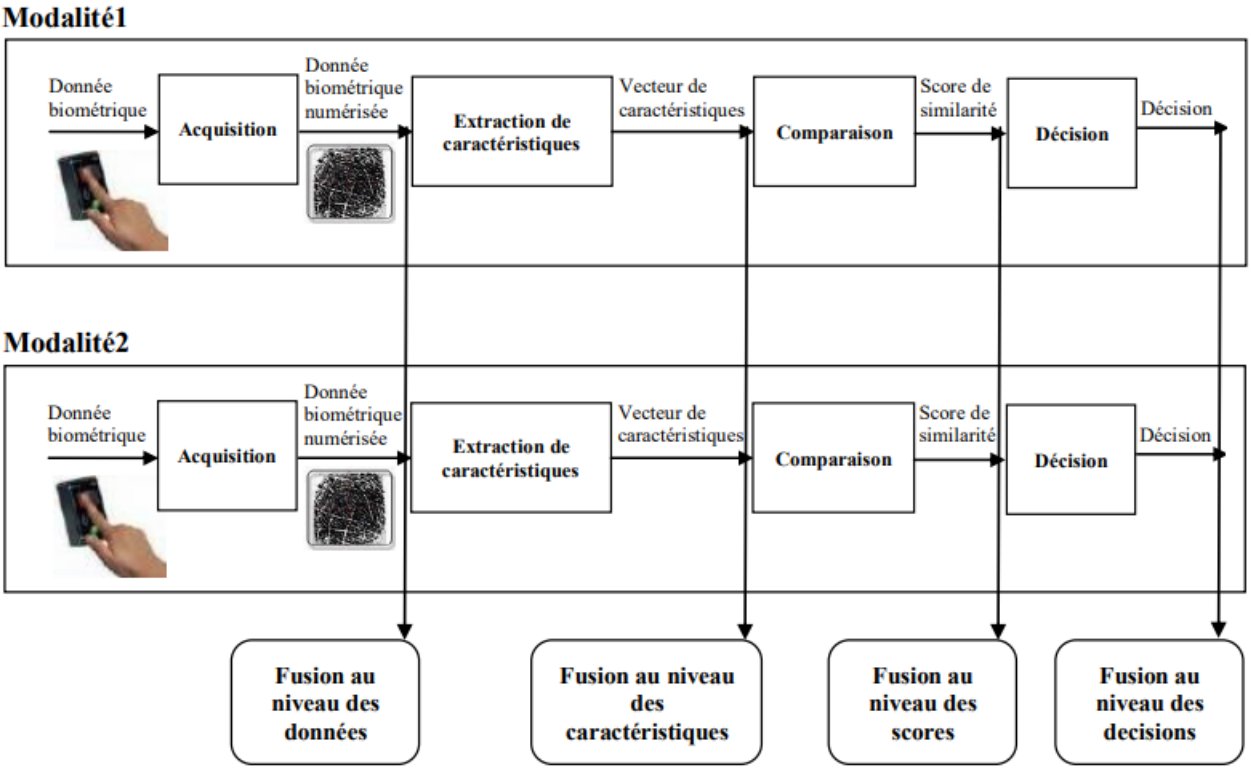


FIGURE 1.20 – Différents niveaux de fusion [50].

1.8 Conclusion

Dans ce chapitre, nous avons défini les notions les plus importantes de la biométrie, nécessaires à la suite du projet. Une vue globale sur les différentes modalités et les techniques utilisées pour la fusion a été détaillée, nous permettant ainsi d'entamer un état de l'art sur les travaux récemment réalisés dans le deuxième chapitre de ce travail.

Chapitre 2

État de l’art sur les systèmes biométriques multimodaux

2.1 Introduction

Divers systèmes biométriques unimodaux ont été proposés dans la littérature. Toutefois, les problèmes de performances de ces systèmes engendrés par les imitations propres à chaque modalité ont poussé les chercheurs à l'exploration de la multimodalité pour les systèmes biométriques. Nombreux sont les travaux qui incorporent la multimodalité en tant que moyen pour augmenter la précision de leurs systèmes biométriques, et ce, en proposant des approches qui combinent les informations de plusieurs sources différentes. Dans ce chapitre, nous allons nous intéresser à ces travaux dont les plus récents. Nous aborderons tout d'abord brièvement, divers documents lus à ce sujet. Puis, une synthèse des travaux sera mise en avant selon une classification en niveaux de fusion.

2.2 Travaux connexes

Afin de se situer dans la littérature autour des systèmes biométriques multimodaux, cette section a pour but de résumer les points les plus importants du domaine en question, tout en citant, de façon générale, quelques documents lus à ce sujet.

Divers travaux aujourd'hui s'intéressent à la multimodalité biométrique dans le cadre de la reconnaissance biométrique des personnes. Dans un souci de sécurité et d'amélioration, diverses propositions ont vu le jour. Certaines d'entre elles se basent sur la multimodalité des capteurs, des échantillons, des instances, des algorithmes, ou des traits biométriques, expliqués dans le chapitre 1 section (1.7.2) :

- Les systèmes multicapteurs traitent des informations du même trait biométrique obtenu par plusieurs capteurs. Un grand nombre de travaux reprennent notamment ce concept dans leurs systèmes multimodaux de sorte à pouvoir augmenter L'efficacité de ceux-ci, sans encombrer l'utilisateur avec plusieurs procédures [117].

- Les systèmes multi-échantillons quant à eux, ont pour but de reconnaître un individu grâce à plusieurs informations différentes dites, échantillons, du même trait biométrique étudié. Ils sont mis en avant dans divers articles de recherche [61], [106].

- En étudiant le même caractère biométrique sur des instants dans le temps différents, le système multimodal multi-instance est un autre type particulièrement utilisé dans l'audio visuel, à des fins de reconnaissance [91], [57].

- Les systèmes multi-algorithmes, décrivent la combinaison de plusieurs algorithmes dans le traitement d'images dans le but de la reconnaissance biométrique. Il existe d'ailleurs divers travaux qui le font dont [84].

- Le dernier type de multimodalité énuméré est l'un des plus répondus. C'est la combinaison de plusieurs traits biométriques soit de type physiologique ou comportemental, afin de réaliser une complémentarité de sorte à couvrir les limitations de chaque modalité utilisée seule. La majorité des travaux utilisent la multibiométrie entre deux modalités

[108], [57], [124], [91], [149], [120], tandis que certains vont jusqu'à utiliser trois [152], [84], [54], [95], voir quatre [165], ou plus.

L'ensemble des systèmes biométriques multimodaux, notamment ceux déjà cités précédemment dans cette section, s'appuient sur un ou plusieurs processus de fusion des informations, afin de pouvoir les combiner et ainsi obtenir une décision finale. Comme la fusion peut être effectuée à plusieurs niveaux, les chercheurs optent soit pour la fusion au niveau des caractéristiques, [152], [158], [124], [74], des scores [102], [108], [61], [149], [106], des rangs [53], [95], des capteurs [117], ou des décisions [84], [120], [163]. Il n'est toutefois pas rare de voir une utilisation de plusieurs types de fusions. Ces propositions dites, hybrides, combinent généralement deux niveaux de fusion, parfois plus comme le montrent les travaux [147], [57], [54]. Nombreux sont les documents qui font la liste des types de fusion en expliquant leurs modes de fonctionnement dont des revues [54], [114].

Selon l'architecture adoptée, les systèmes multimodaux font usage de divers algorithmes, notamment des techniques de l'intelligence artificielle, dont le Deep Learning [53], [84], [54], [61], le Machine Learning tel que SVM [102], KNN [152], [158], ou encore d'autres méthodes, comme la logique floue [165], [163], etc.

De plus, des bases de données contenant un grand nombre d'échantillons de traits biométriques sont utilisées, telles que CASIA-IrisV3 pour l'iris [53], CASIA pour l'empreinte palmaire [147], ou encore, WPUT pour l'oreille [147], et ce, afin d'évaluer les systèmes multimodaux et les comparer aux autres. Les chercheurs s'appuient aussi pour cela, sur plusieurs mesures de performances, dont la précision, le taux d'erreur, des courbes de performances tel que DET et ROC, etc. Ces mesures de performances sont souvent citées de façon détaillée dans de nombreuses thèses [102].

Le but d'évaluation de chaque système proposé, est bien entendu d'en étudier l'efficacité vis-à-vis des autres systèmes, le but étant de réussir à mettre en œuvre un système surpassant les autres dans le cadre des mesures de performances déjà citées. Divers documents réalisés, se spécialisent dans l'évaluation des solutions proposées dans ce domaine, dont les comparatifs qui implémentent et testent de multiples approches réalisées [91], [165]. D'autres travaux, font juste un état de l'art, ou bien une taxonomie sur ce qui a été fait, dans un but d'aide à la recherche [147], [162], [114].

2.3 Synthèse de documents

Comme nous pouvons le constater à l'issue de la section précédente, les systèmes biométriques multimodaux proposés, et les travaux réalisés là-dessus dans la littérature, sont très variés et nombreux. De ce fait, notre état de l'art se concentrera dans une première partie sur la synthèse de quelques travaux récents. Puis, un comparatif des travaux synthétisés sera mis en avant dans la seconde partie.

En optant pour une classification en niveau de fusion [48], nous réalisons une taxonomie permettant d'avoir une vue plus claire des documents collectés. Dans cette section, ces derniers seront analysés de façon à en extraire les points les plus importants à l'issus desquels nous pourrons les comparer ensuite.

2.3.1 Fusion au niveau des capteurs (Sensor Level)

La fusion au niveau des capteurs est une fusion très tôt des données, ce qui implique beaucoup d'informations par rapport aux autres types de fusions. C'est un domaine de recherche émergeant donc les travaux faits sur cette fusion sont peu nombreux [176], [174].

Le travail de Khemmar et al [116]

Le travail de Khemmar et al propose une plateforme d'authentification biométrique pour les applications de contrôle d'accès basées sur la reconnaissance du visage. Cette recherche fait partie d'un projet destiné aux personnes handicapées, ayant comme but le développement d'un fauteuil roulant intelligent. La plateforme s'agit d'un système de vision multicapteurs qui fusionne un capteur catadioptrique et une caméra pan tilt zoom (PTZ), le processus de reconnaissance est basé sur l'algorithme d'Eigenfaces[171].

Les auteurs de ce travail ont utilisé leur propre base de données hétérogène, combinée avec la base de données ORL (Olivetti Research Laboratories) [44]. Des tests comparatifs ont été faits pour l'évaluation de ce système. Selon l'histogramme des résultats obtenus, on peut constater que la combinaison d'algorithmes CS (Compressing Sensing) [118] et SS (Sub-Sampling) [94] donne les meilleurs résultats, étant donné que sur dix itérations, neufs ont donné un taux de reconnaissance supérieur à 0.9, et que dans toutes les itérations le taux de reconnaissance de cette combinaison est meilleure que ceux des deux autres combinaisons d'algorithmes (CS + LBP [51] et LBP + NN [160]).

Le travail de Boussad et Boucetta [55]

Boucetta et Boussad ont présenté un nouveau système d'identification biométrique multimodal qui combine les modalités de l'iris, visage et empreinte palmaire. Les trois modalités sont traitées comme des canaux RVB [39] d'une image, et utilisées en entrées de l'algorithme de réseau de neurones convolutifs(CNN) [40]. Inceptionv3 [44][167], GoogleNet [41][166], ResNet18 [42][99] et SqueezeNet [43][104] sont les quatre modèles pré-entraînés employés dans l'approche de ce travail.

Cette approche est divisée en deux stratégies : l'extraction de caractéristiques et fine-tuning. Cette dernière n'utilise que le modèle SqueezeNet. D'après les résultats des tests comparatifs, de bonnes valeurs de précision sont atteintes. On remarque que pour la première stratégie le meilleur résultat est de 99.42% et pour la deuxième stratégie la précision moyenne est de 99.67%.

2.3.2 Fusion au niveau des caractéristiques (Feature Level)

La fusion au niveau des caractéristiques est l'un des types de fusion les plus utilisés récemment. Divers systèmes multimodaux en font usage dont ces quelques travaux :

Le travail de Huang [103]

L'article de recherche de Quan Huang met en avant un système biométrique multimodal qui incorpore un nouvel algorithme pour la fusion basé sur le Deep Learning. Le but étant de réduire l'influence du comportement, des caractéristiques personnelles et de l'environnement de l'utilisateur, lors de l'étape d'acquisition des informations qui peu rendre ces dernières peu fiables.

Afin de réaliser cet objectif, le système multimodal commence par un prétraitement des données de chaque modalité. Cela consiste à éliminer les informations inutiles sur les images, en procédant en deux étapes. La première, qui est la transformation de données en effectuant une normalisation, et la seconde la segmentation des images de chaque modalité en régions. Ensuite, les caractéristiques biométriques sont analysées, extraites, puis fusionnées à l'aide d'un algorithme de Deep Learning renforcé basé sur les réseaux de neurones convolutifs.

Les deux datasets, CASIA-Iris-Interval-v4 [138] contenant des images binoculaires d'iris de 100 personnes et NFBS [78] incluant 125 ensembles d'images de cerveaux, ont été utilisés pour tester la méthode proposée. Les résultats indiquent que l'algorithme proposé consomme moins de temps de traitement relativement aux autres propositions auxquelles il a été comparé, tout en ayant une précision assez haute de 97% répondant ainsi, au problème de fusion de modalités posé.

Le travail de Sarangi et al [158]

Les auteurs Partha Pratim Sarangi et al proposent un système biométrique multimodal basé sur l'oreil et le profile facial, en utilisant une méthode de fusion des caractéristiques améliorée.

Tout d'abord, pour l'extraction efficace des caractéristiques des deux modalités biométriques, elles ont été représentées de façon individuelle en utilisant à différentes échelles, deux descripteurs de caractéristiques : l'un qui est LPQ (Local Phase Quantization) et l'autre LDP (Local Directional Patern). Une fois ces derniers combinés en des vecteurs de caractéristiques, une réduction de dimensions et une normalisation ont été appliquées. Les vecteurs résultants sont ensuite combinés en un ensemble de caractéristiques. Enfin, l'approche KDCV (Kernel Discriminative Common Vector) a été utilisée afin de réduire encore plus l'ensemble des caractéristiques obtenues durant la fusion, et ainsi, obtenir des caractéristiques plus discriminantes et non-linéaires nécessitant moins d'échantillons d'apprentissage pour la classification KNN. Les étapes de cette approche ont été détaillées dans un schéma explicatif, (voir la figure 2.1).

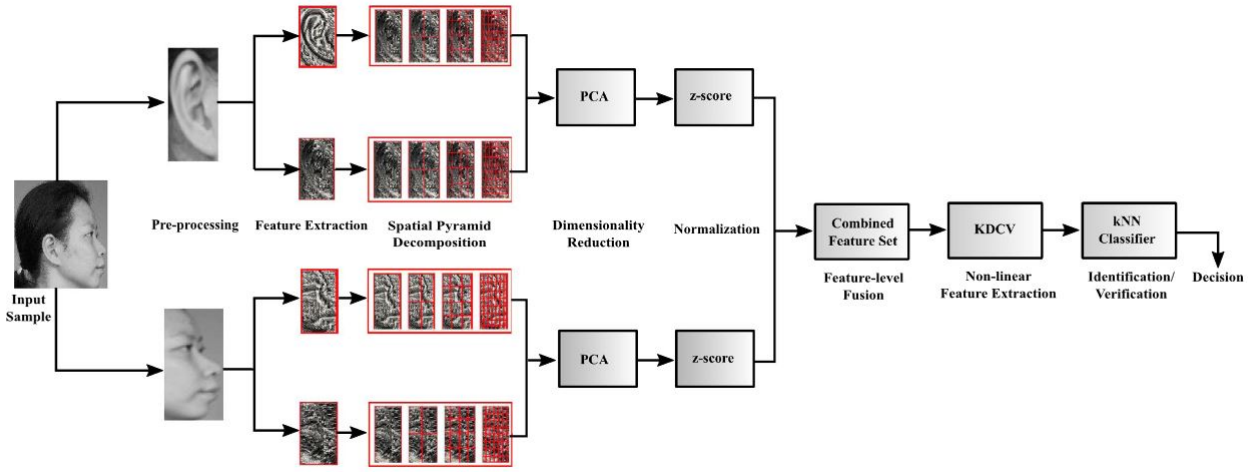


FIGURE 2.1 – Architecture du système proposé par Sarangi et al [158]

Les performances de chaque modalité sont mesurées séparément et leurs résultats sont comparés avec la méthode multimodale proposée. De plus, une analyse comparative avec les méthodes de l'état de l'art qu'ils ont mis en avant au début du travail a été faite pour vérifier l'efficacité du schéma proposé. Pour cela, les deux bases de données UND-E [1], et UND-J2 [1] ont été utilisées. Les résultats démontrent un taux d'identification maximum de 99.42% pour la base de données UND-E et 98.53% pour la base de données UND-J2.

Le travail de Bayan et al [140]

Dans cette étude, les auteurs Bayan Omar Mohammed et al mettent en avant un nouveau système biométrique multimodal basé sur la fusion au niveau des caractéristiques. En optant pour deux modalités qui sont le visage et les empreintes digitales, ils tentent d'améliorer l'identification des personnes à travers l'utilisation d'échantillons de leurs empreintes et leurs visages.

Selon l'architecture proposée, le système commence d'abord par l'extraction des caractéristiques après acquisition et prétraitement, et ce, en faisant usage de la technique "AUMI (Aspect United Moment Invarient) [28]". Ensuite, vient la fusion des caractéristiques qui est mise en œuvre grâce à l'algorithme proposé nommé Dis-Eigen algorithm. Le mode de fonctionnement de celui-ci, repose sur le principe de la fusion des vecteurs de caractéristiques et leur transformation, afin de fournir une meilleure représentation des caractéristiques à partir des multiples modalités. Enfin, après la fusion, vient la recherche d'une correspondance dans les bases de données donnant lieu à une décision finale. La figure (2.2) représente l'architecture du système en question.

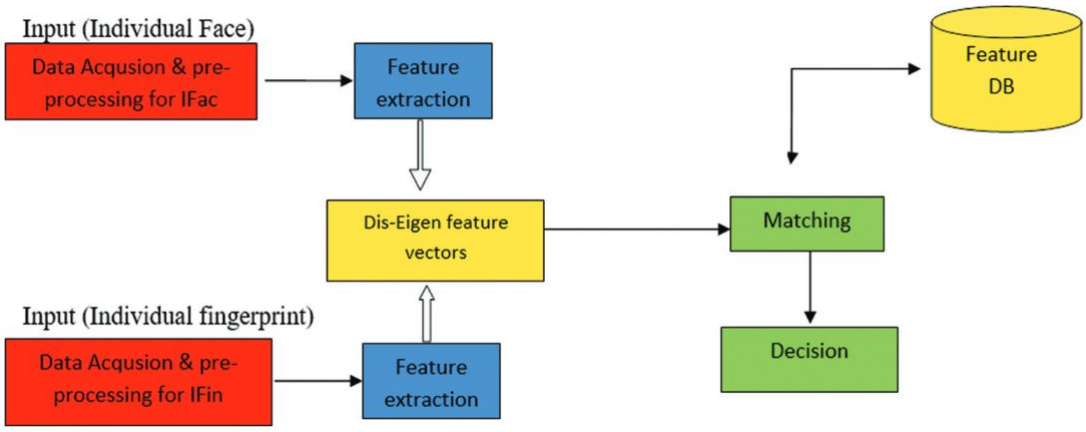


FIGURE 2.2 – Architecture du système proposé par Bayan et al [140]

Pour tester l'approche proposée, des échantillons des visages et des empreintes de 20 individus ont été utilisés, donnant divers résultats selon différents paramètres d'implémentation. En moyenne, la précision de l'approche proposée est de 97,18 %, bien plus que dans le cas de chaque modalité utilisée seule.

Le travail de Leghari et al [124]

Le travail de Mehwish Leghari et al, propose un système biométrique multimodal combinant les empreintes et les signatures en ligne, dans le but de remédier aux limitations de l'unimodalité en utilisant du Deep Learning, et deux utilisations différentes de la fusion au niveau des caractéristiques.

En prenant en entrée les informations de chaque modalité de façon individuelle, le système multimodal fait un traitement en multicouche séparément, puis effectue la fusion des caractéristiques produites, soit avant la connexion des couches, ou bien après la connexion. La décision est ensuite prise après l'étape de Matching.

Afin de tester le système, un dataset regroupant des images d'empreintes digitales, et un autre contenant les caractéristiques des signatures, tous deux collectés par des étudiants volontaires, ont été utilisés. Les résultats ont été ensuite comparés à ceux des autres travaux étudiés dans l'état de l'art mis en avant dans le document. Ce système achève une performance prometteuse avec une précision de 99.1 % pour la fusion avant la connexion, et 98,35 % pour la fusion après connexion des couches, ce qui présente un intérêt particulier pour l'augmentation de la sécurité dans les processus d'authentification en ligne.

Le travail de Ryszard S. Choras [110]

L'auteur Ryszard S. Choras propose une approche dans son travail qui combine trois modalités biométriques : les veines dorsales de la main, l'empreinte palmaire et l'œil de l'individu.

Après un bref état de l'art, le document met en avant le système proposé. Celui-ci commence par l'acquisition des images de chaque modalité et leur prétraitement. Ensuite, les caractéristiques extraites, après le prétraitement, sont fusionnées puis normalisées, afin d'effectuer une classification, qui permettra une décision finale. Le mode de fonctionnement de ce système est d'ailleurs résumé, dans un schéma explicatif, (voir la figure 2.3).

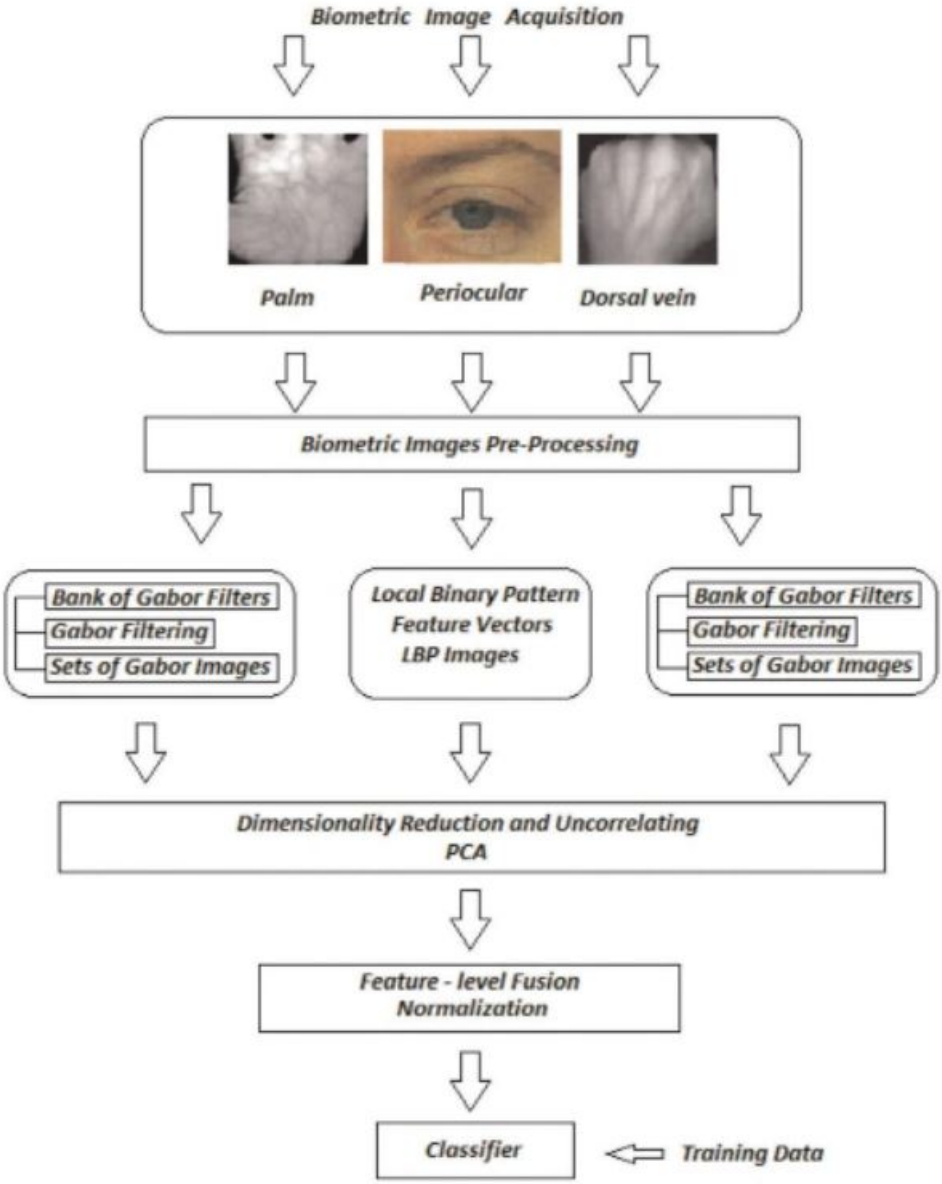


FIGURE 2.3 – Architecture du système proposé par Ryszard S. Choras [110]

Les résultats des tests sur ce système démontrent que l'utilisation des trois modalités achève globalement une plus grande performance que lors de l'utilisation des traits biométrique en mode unimodal, ou bimodal, avec un taux de reconnaissance (Recognition rate) maximum de 95,3 %.

2.3.3 Fusion au niveau des rangs (Rank Level)

La fusion au niveau des rangs, un peu moins utilisée que les autres types de fusion, est mise en œuvre après le processus de Matching en se basant sur les rangs attribués à chaque ensemble de données d'utilisateur [150]. ce type de fusion possède un inconvénient majeur. En effet, dans un système biométrique multimodal se basant sur la fusion au niveau des rangs, il est probable d'obtenir plus d'identités en sortie du module de Matching que le nombre d'identités en entrées [130].

Le travail de Al-waisy et al [53]

Le travail de Alaa S. Al-Waisy et al met en avant un système biométrique multimodal à temps réel, qui fait la fusion entre les informations obtenues à partir des deux yeux d'une personne, au niveau des rangs.

Le système proposé et illustré dans la figure (2.4) fait en premier lieu une localisation des iris, en faisant une localisation de la pupille. Après acquisition, les images d'iris sont normalisées de sorte à réduire les irrégularités dimensionnelles entre les échantillons. Puis, une extraction des caractéristiques et une classification des images normalisées est effectuée en utilisant une approche du Deep Learning, combinant un CNN et un Softmax classifier [153] qui donne lieu, après l'apprentissage et tests de l'algorithme, à une décision finale.

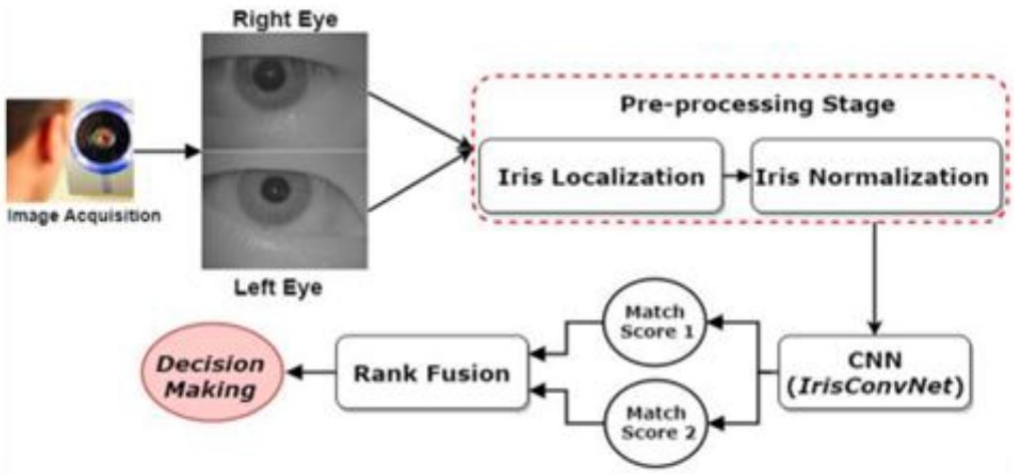


FIGURE 2.4 – Architecture du système proposé par Al-waisy et al [53]

Afin de tester le système biométrique multimodal mis en œuvre, les bases de données SDUMLA-HMT [173], CASIA-iris-V3 [89], IITD [121], ont été utilisées avec plusieurs méthodes de fusion au niveau des rangs. Les résultats démontrent globalement de très bonnes performances, avec un taux d'identification (Identification rate) de 99.1 % sur toutes les bases de données utilisées.

Le travail de Tahmasebi et Pourghassem [168]

Les auteurs Ava Tahmasebi, et Hossein Pourghassem, proposent dans cette étude un système biométrique multimodal qui fait la fusion au niveau des rangs entre les informations obtenues à partir des trois modalités : l'oreille, l'empreinte palmaire, ainsi que la signature dynamique (voir la figure 2.5). Le but étant, de remédier aux limitations des systèmes biométriques unimodaux.

En utilisant le filtre Gabor [77], le système se charge tout d'abord d'extraire localement les caractéristiques de texture de chaque modalité durant la phase de traitement après acquisition. Plus précisaient, le filtre Gabor proposé fait la représentation des caractéristiques des modalités étudiées, et en réduit les dimensions afin de faciliter l'étape de vérification. Ensuite, un algorithme basé sur la vérification des distances intra-classe est utilisé, pour la phase de vérification, dans le but de séparer les caractéristiques authentiques, des fausses. Enfin, la fusion au niveau des rangs est mise en œuvre en utilisant l'algorithme proposé. Celui-ci se base sur la théorie des jeux, pour de meilleurs résultats après fusion.

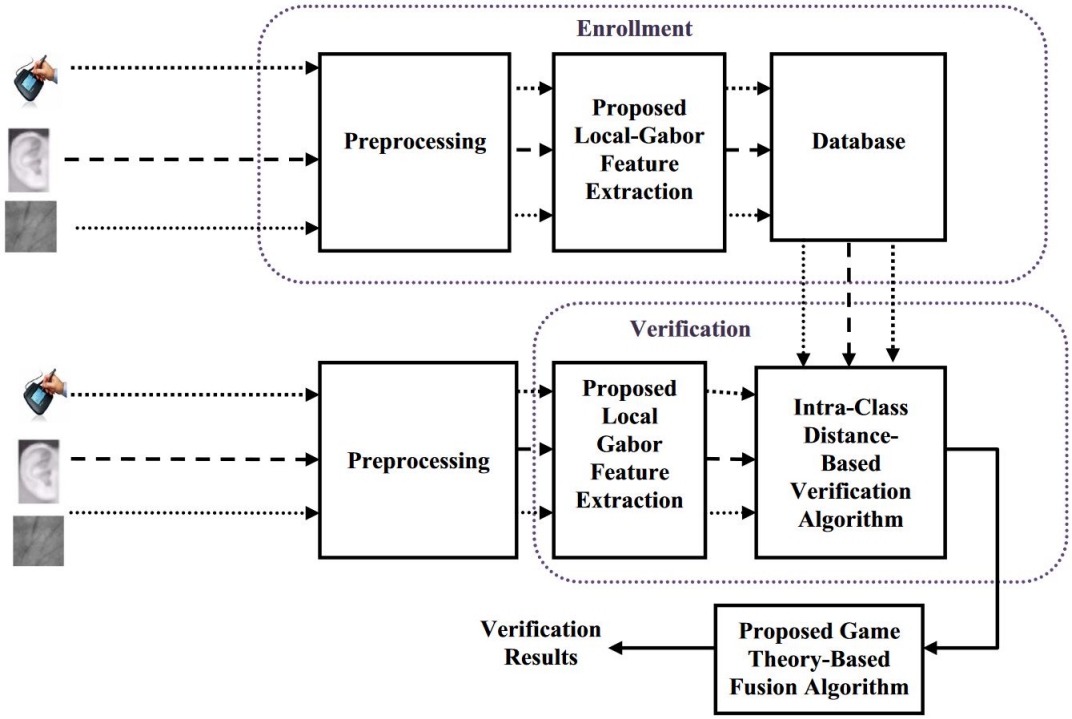


FIGURE 2.5 – Architecture du système proposé par Tahmasebi et Pourghassem [168]

Pour l'évaluation du système multimodal proposé, les chercheurs ont opté pour les trois bases de données SVC2004[181], PolyU [123], et UND[1]. Les résultats démontrent une précision de 99,63 %. Confirmant ainsi l'efficacité de l'approche proposée.

Le travail d'Ahmad et al [49]

L'Article de Shadab Ahmad et al propose un système multimodal dans le but de remédier aux risques de sécurité que représentent les limitations de l'unimodalité.

Afin d'atteindre cet objectif, cette étude se base sur la fusion de plusieurs traits biométriques au niveau des rangs. En formulant ce niveau de fusion comme un problème d'optimisation, les auteurs tentent de minimiser les distances entre une liste de rangs agrégée et chaque liste de rangs d'entrées, et ce, en proposant une solution se basant sur la méthode Monte Carlo d'entropie croisée (CE) de distances.

Pour tester leur proposition, les auteurs utilisent le dataset BSSR1 [139], incluant quatre modalités, dont deux pour le visage, et 2 autres, pour les empreintes digitales. Leur méthode est comparée à plusieurs autres techniques de fusion mentionnées dans l'état de l'art qu'ils mettent en avant dans leur document.

Les résultats démontrent des bonnes performances, dont 99.42 % de précision, ce qui répond avec succès à la problématique posée au départ.

Le travail de Gunasekaran et al [95]

L'article de K. Gunasekarana, met en avant un système multimodal utilisant trois traits biométriques : le visage, l'empreinte digitale, et l'iris.

Le mode de fonctionnement du système multimodal proposé repose sur un processus en plusieurs étapes. Tout d'abord, les informations acquises sont prétraitées de sorte à réduire les dimensionnalités. Puis, vient l'étape d'extraction des caractéristiques qui consiste en partie à la mise en œuvre d'histogramme pour chaque modalité. Les images seront ensuite fusionnées, en utilisant la fusion pondérée au niveau des rangs, où les poids assignés représentent le niveau de pertinence de chaque modalité. Enfin, le processus de matching est effectué à l'aide du Deep Learning. La figure (2.6), est une représentation globale de l'architecture du système.

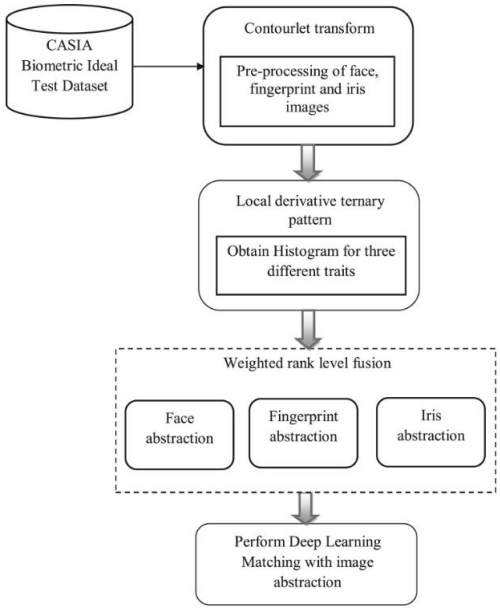


FIGURE 2.6 – Architecture du système proposé par Gunasekaran et al [95]

Pour tester le système, le dataset CASIA Biometric Ideal [138] est utilisé. Les résultats démontrent un taux de reconnaissance (recognition rate) maximum de 96 %, avec un taux de traitement de 49.2 ms, pour les échantillons biométriques de 500 personnes.

Le travail de Monwar and Gavrilova [130]

L'étude un peu moins récente de Md Maruf Monwar et Marina L Gavrilova met en avant un système multimodal combinant trois modalités : le visage, l'oreil, et la signature, en utilisant une méthode de fusion au niveau des rangs améliorée. Le but étant de réduire le taux d'erreur des méthodes de fusion au niveau des rangs classiques au maximum.

Le mode de fonctionnement du système en question consiste à l'acquisition initiale des images de chaque modalité dans une étape d'enrôlement. Ensuite, les caractéristiques sont extraites afin d'effectuer une mise en correspondance pour chaque modalité de façon individuelle. Puis, la fusion au niveau des rangs est effectuée pour une décision finale. Le système proposé est schématisé dans la figure (2.7).

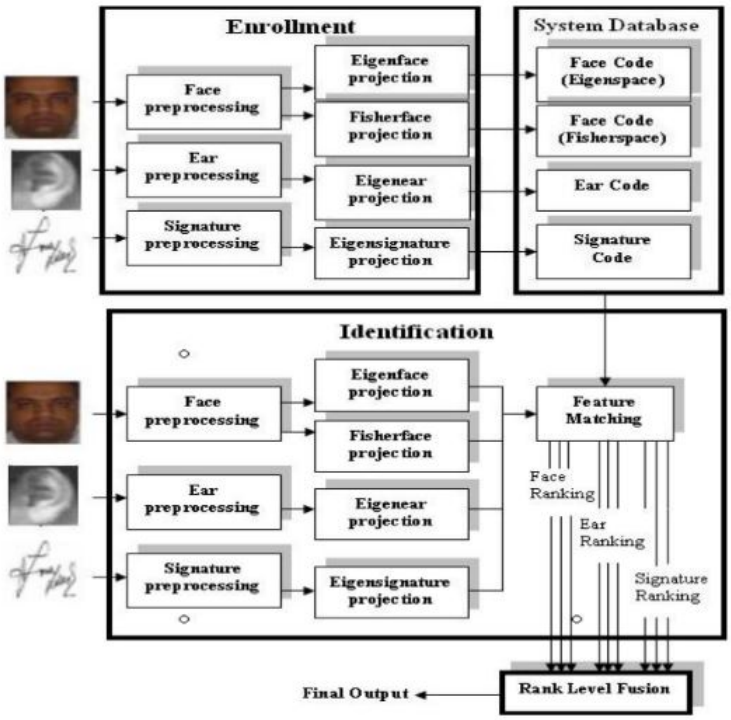


FIGURE 2.7 – Architecture du système proposé par Monwar and Gavrilova [130]

En comparant le système à une version unimodale de celui-ci, les résultats démontrent que l'utilisation des trois traits biométriques, achève une plus grande précision que leur utilisation en mode unimodal.

2.3.4 Fusion au niveau des scores (Score Level)

La fusion au niveau des scores est le choix le plus couramment mis en œuvre, et ceci est grâce à la facilité d'accès et traitement des scores de comparaison, un nouveau et unique score est produit comme résultat de cette fusion pour passer à l'étape de décision [154].

Le travail de Rajasekar et al [149]

Dans un travail destiné pour les villes intelligentes, une approche améliorée de biométrie multimodale a été proposée. Les auteurs de ce travail utilisent un algorithme génétique flou optimisé, ce qui donne une amélioration au niveau des performances avec un haut taux de précision de 99.88% et un taux d'EER faible de 0.18%. Dans cette approche, les modalités utilisées sont l'iris et l'empreinte. Après un processus de prétraitement, les caractéristiques extraites de chaque modalité sont comparées aux modèles obtenus à partir des bases de données CASIA V3[89] pour l'iris et FVC2006[31] pour l'empreinte. Ensuite, vient l'étape de fusion des deux scores, et enfin, on obtient une décision.

Le travail de Attia et al [47]

Un système biométrique multimodal basé sur la main a été proposé par Attia et al. L'empreinte palmaire, et les empreintes d'articulations des doigts sont les modalités choisies dans cette recherche. La base de donnée PolyU [123] a été utilisée dans l'évaluation des performances du système. Plusieurs expérimentations ont été faites sur chaque modalité individuelle, et sur la fusion de ces modalités. Ce système utilise PCAN [73] et pour l'extraction de caractéristiques, SVM multiclasse dans le calcul des scores individuels, ainsi que différentes règles dans la fusion de ces scores (min, sum, max et multiplication), et a été capable d'atteindre 0.0% de EER sur la base de données utilisé.

Le travail d'Aizi et Ouslim [111]

Aizi et Ouslim ont présenté une nouvelle méthode biométrique multimodale en utilisant deux modalités : iris, et empreinte. Une fusion au niveau du score est faite sur les zones d'intérêts, qui sont résultats de l'application de l'algorithme K-means. Deux approches de fusion ont été réalisées, une approche basée sur la logique floue [71] et une autre basée sur les arbres de décisions combinées, avec une somme pondérée qui est d'après les résultats de l'étude des auteurs, légèrement plus performante que la première approche avec une valeur de taux de reconnaissance de 95.00% .

Le travail de Iula et Micucci [60]

Dans le travail de Iula et Micucci, l'utilisation de la biométrie multimodale avec la technologie de l'ultrason est mise en œuvre. Le système biométrique multimodal combine la géométrie 3D de la main, et les caractéristiques de la paume en 3D. La performance de ce système est évaluée selon des expérimentations sur l'identification et la vérification. Une comparaison entre les systèmes unimodaux, des deux modalités, et le système de la fusion de ces modalités, a montré que ce dernier permet d'augmenter la performance tel que l'EER obtenu est de 0.08%, et le taux d'identification est de 100%, ces résultats sont relatifs à la base de données propre à cette étude.

Le travail de Walia et al [177]

Dans ce travaille une méthode de fusion de score optimal a été proposée, en fusionnant trois modalités qui sont : l'iris ; empreinte du doigt et veines du doigt. Cette méthode est basée sur deux algorithmes, l'algorithme BSA (Backtracking Search Optimization Algorithm) et PCR-6[164]. En moyenne, les resultats obtenus de l'évaluation des performances, sont 98.43% de précision et 1.57% de EER.

2.3.5 Fusion au niveau des décisions (Decision Level)

Une des formes de fusion de données est la fusion au niveau des décisions qui est la fusion la plus tardive des informations. Elle vise à retourner une décision en prenant comme bases plusieurs autres en entrées.

Le travail de Cherrat et al [83]

Cherrat, Alaoui et Bouzahir ont présenté dans leurs travail la fusion de trois modalités au niveau de décision, qui s'agissent de : l'empreinte digitale ; veines digitales et visage. Leur système multimodal est basé sur une architecture en cascade. Trois modes de fonctionnement ont été élaborés. Le premier, consiste à ce qu'un individu soit reconnue dès qu'une seule modalité est validée. Dans le deuxième mode bimodal, la règle ET est utilisée, où on doit avoir au moins deux modalités validées. Dans le dernier mode, le mode multimodal avec la règle ET, un individu ne peut être reconnu que si les trois modalités sont validées. Les résultats issus des bases de données suivantes : "Fingerprint Verification Competition 2004 dataset "[21], "the VERA Fingervein Database"[23] et "The AR face database"[18], ont démontré une amélioration de précision de 99.43%, ce résultat est obtenu à partir du premier mode.

Le travail de Kumar et al [145]

Un nouveau framework de la biométrie multimodale pour vérification et identification a été proposé dans le travail de Kumar et al. C'est une combinaison au niveau de décision de la signature dynamique et électroencéphalogramme (EEG). Chaque sous-système de chaque modalité individuelle utilise BLSTM-NN (bidirectional long short-term memory neural network) [143] comme classificateur. La technique de fusion Borda Count a donné les meilleurs résultats, que ce soit dans le cas d'identification, tel qu'une précision de 98.78% est atteinte, qui est supérieur aux valeurs de précisions 96.36% et 97.57% issue de système de la signature dynamique et système de signal EEG respectivement, ou dans le cas de vérification, qui est basé sur la détection d'imposteur, dont de bons résultats sont obtenus pour FAR de 3.75% TPR de 100%, tous ces résultats sont basés sur les données expérimentales collectées issues de la recherche du travail en question.

Le travail de Sharma et al [146]

Dans le travail de Sharma et Al, un système biométrique multimodal basé sur l'empreinte et le visage a été proposé. Deux bases de données sont utilisées : FVC2002 [20] et Face94 (university of Essex, UK) [63], la première base de données permet l'évaluation du système de reconnaissance d'empreinte en utilisant un algorithme basé sur les minuties, tandis que la dernière base de données est utilisée pour évaluation du système de reconnaissance de visage qui utilise l'algorithme de PCA [62]. Les valeurs de FAR et de FRR ont été calculées pour chaque système individuellement, et dans le cas de combinaison des décisions de ces systèmes. Les résultats d'observation permettent de constater que la méthode proposée dans cette recherche qui utilise la logique floue en tant que technique de fusion, améliore considérablement le taux de précision de 99.5%.

Le travail de Hameed et al [87]

Hameed et al ont mené une étude d'un système biométrique multiéchantillon, qui combine selon la logique floue trois empreintes différentes. Ce système est composé d'un sous-système de reconnaissance d'empreinte, et un sous-système de décision. EER est la mesure d'évaluation de performance considérée. La fusion au niveau de décision avec logique flou améliore la performance du système de 10% et 12% par rapport à la fusion par vote de majorité et réponse de trois sur trois respectivement.

2.3.6 Méthodes de fusion hybrides

Dans cette section, nous regroupons des synthèses des travaux utilisant plus d'un niveau de fusion. Plusieurs chercheurs optent pour l'implémentation de plusieurs types de fusion dépendamment de l'approche proposée. Tandis que certains travaux mettent en œuvre un système effectuant de la fusion à deux niveaux différents pour accroître son efficacité [109], d'autres implémentent le même système avec plusieurs types de fusion, dans un but de comparaison des performances [96].

Le travail de Punyani et al [147]

L'article de Prachi Punyani et al propose un système multimodal combinant les informations obtenues des empreintes palmaires et des oreilles des personnes, en se basant sur deux techniques de fusion, au niveau des scores et décisions.

De façon globale, le système proposé commence d'abord par faire l'acquisition des images, et leur conversion vers des images de même taille. Puis, une extraction des caractéristiques de chaque modalité est effectuée, afin de les mettre en correspondance durant l'étape de matching, après une normalisation. À l'issue du traitement de chaque modalité, deux décisions en résultent. Celles-ci sont ensuite fusionnées pour une décision finale. Ces étapes, sont notamment représentées sur le schéma explicatif de la figure (2.8).

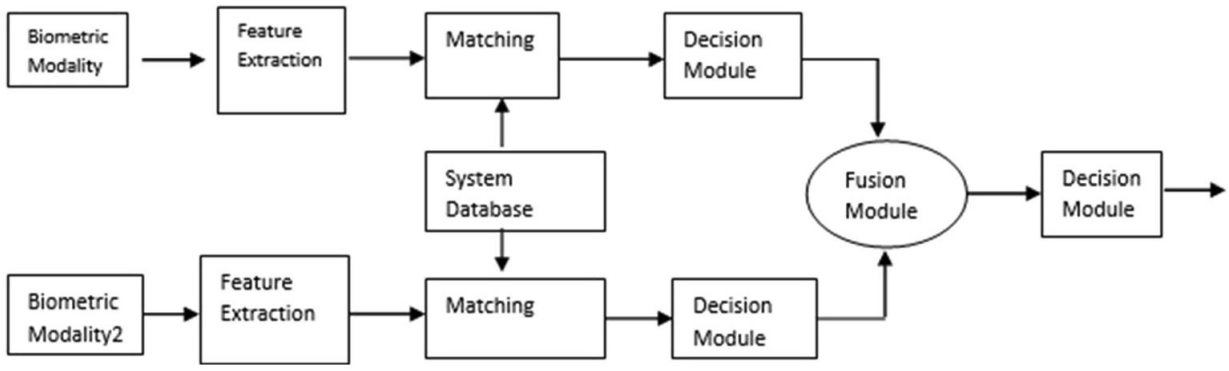


FIGURE 2.8 – Architecture du système proposé par Punyani et al [147].

Pour les tests effectués, les bases de données CASIA pour les empreintes palmaires [134], et WPUT [92] pour les oreilles, sont utilisées. Les résultats démontrent une précision de 94.7 %, pour la méthode proposée.

Le travail d'Anil et Ravikumar [57]

Le travail d'Anil et Ravikumar, propose un système biométrique multimodal, combinant les informations obtenues à partir du visage, et de la voix d'une personne sur une vidéo, en utilisant la fusion au niveau des décisions et des caractéristiques. Le but de l'étude étant de faire la comparaison entre huit algorithmes, pour l'identification.

Pour les tests, les modalités sont d'abord testées chacune individuellement, puis en combinaison avec différents types de fusion et algorithmes. Le test effectué, combinant le visage et la voix, à l'aide de la fusion au niveau des décisions et des caractéristiques avec les algorithmes classifieurs f-MLP (fuzzy-multi-layer perceptron) & FCM (fuzzy c-medoid), achève une plus grande performance, selon les résultats, dont une précision de 98,47 %.

Le travail de Hammad et al [96]

L'article de Mohamed Hammad et al met en avant deux systèmes biométriques multimodaux, combinant deux modalités qui sont les signaux ECG, et les empreintes digitales, en utilisant du Deep Learning. L'un se basant sur la fusion au niveau des caractéristiques, et l'autre se basant sur la fusion au niveau des décisions.

Le document présente en premier le système se basant sur la fusion au niveau des décisions. Celui-ci effectue d'abord, une authentification à l'aide de l'ECG, afin de s'assurer que c'est bien une personne. Puis, l'authentification à l'aide d'empreinte est utilisée, afin d'authentifier l'utilisateur. Les décisions prises par la suite du traitement de chaque modalité sont fusionnées dans le cas d'un rejet de l'empreinte, de sorte à bien authentifier la personne. Le second système proposé, traite les informations de chaque modalité de façon parallèle, contrairement au premier. Après une extraction des caractéristiques, à l'aide du Deep Learning, le système effectue une fusion de celles-ci. Afin d'obtenir la décision finale en faisant une classification à l'aide Machine Learning.

Les tests sont faits à l'aide de deux bases de données pour chaque modalité : PTB database [69] et CYBHi database [79], pour les signaux ECG, LivDet2015 [101] et FVC 2004 database [136], pour les empreintes digitales. Les résultats de l'étude démontrent une précision moyenne (average accuracy) de 99,12 %, pour le système séquentiel, et 98,94 %, pour le système parallèle. Cela confirme que le système séquentiel est bien plus performant.

Le travail de Kabir et al [109]

L'étude de Waziha Kabir et al propose un système biométrique multimodal alliant les informations de trois traits biométriques en utilisant une technique de fusion hybride. Le but de l'étude est de proposer et tester plusieurs algorithmes mis en œuvre intervenant dans le système, notamment l'algorithme de la fusion hybride.

L'étude commence d'abord par l'explication des trois algorithmes proposés implémentés pour le système multimodal. Le premier est celui de la fusion hybride "Hybrid Fusion" (HBF) qui combine la fusion au niveau des caractéristiques, avec la fusion au niveau des scores. Le mode de fonctionnement de ce dernier se base sur une extraction des caractéristiques de chaque modalité pour la fusion au niveau des caractéristiques. Le résultat est ensuite codé, et mis en correspondance, pour une autre fusion au niveau des scores. Cet algorithme est d'ailleurs représenté par le schéma de la figure (2.9). Étant donné que la fusion des informations de matching produit des résultats non uniformes, tels que des taux d'erreur différents, la deuxième technique de fusion "Mean-Extrema Based Confidence Weighting" est proposée afin d'attribuer des poids aux scores, et ainsi donner plus de poids aux Matchers ayant le résultat correct. Enfin, le troisième algorithme "Weighted Hybrid Fusion" (WHBF) proposée intervient au niveau du module de décision.

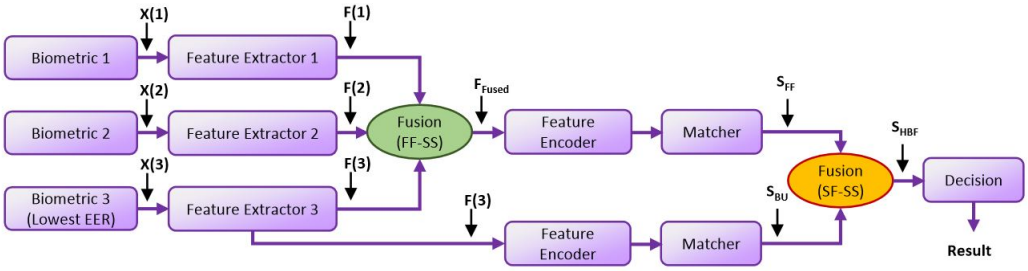


FIGURE 2.9 – Architecture du système proposé par Punyani et al [147]

Les résultats expérimentaux sont mis en avant à la suite de l'implémentation et tests avec les datasets : AMI-subset-1 [88], FVC2002DB1-A [135], Palmprint-IITD Right [119] pour les oreilles, les empreintes digitales, et palmaires. On note des résultats prometteurs dont 5.09 % d'EER pour la technique WHBF et 5.39 % d'EER pour l'algorithme HBF.

Le travail d'Alay et Al-baity [54]

Le travail de Nada Alay et Heyam H. Al-Baity, propose un système biométrique multimodal alliant trois modalités : l'iris, le visage et les veines des doigts. Le but étant de remédier aux limitations de l'unimodalité, en mettant en œuvre système multimodal basé sur du Deep Learning.

La méthode proposée prend en entrée les images de chaque modalité. Après un prétraitement pour plusieurs opérations, telle que la redimension, les images de chaque trait biométrique sont soumises à un CNN, un pour chaque type de modalité. Cette étape permet d'extraire les caractéristiques des images, ainsi que la mise en correspondance. Enfin, les données sont fusionnées, de sorte à produire une décision finale.

Afin de tester le système, les datasets SDUMLA-HMT [173], IT Delhi [121], et FERET [137], ont été utilisés, de même qu'une implémentation en deux niveaux de fusion différents, à des fins de comparaison. De façon générale, les résultats mettent en avant une précision de 100 % pour la fusion au niveau des scores, et 99,39 % pour la fusion au niveau des caractéristiques relativement aux bases de données utilisées, concluant ainsi, que la fusion au niveau des scores est meilleure pour ce système. L'approche proposée a été aussi comparée à divers travaux semblables, abordés dans l'état de l'art mis en avant dans le document.

2.4 Comparatif des travaux

Tandis que les chercheurs proposent constamment de nouvelles approches pour les systèmes biométriques multimodaux, d'autres se chargent de faire des revues ou des comparatifs, où ces approches récemment proposées sont généralement collectées et classées sous forme de taxonomie et comparées entre elles, selon des mesures de performances communes, dans le but d'aide à la recherche.

Un exemple de cela, est la revue de Shaheed et al [162], qui fait un état de l'art sur les méthodes utilisées dans les systèmes de reconnaissance biométrique, basées sur les traits physiologiques, en les classant selon le type de modalités utilisées, ou encore, la revue de Kaur et al [114], classant les travaux par type de fusion utilisée, afin de les comparer dans un tableau.

De la même façon, nous mettons en œuvre dans cette section un tableau comparatif des travaux synthétisés, afin d'avoir une vision plus claire et pouvoir comparer les approches, et les points distinctifs de celles-ci, selon des mesures de performance fixes (voir le tableau 2.1).

Auteurs	Année	Base de données	Modalités	Type de fusion	Résultats (ACC, average ACC, RR, EER)
Monwar et Gavrilova [130]	2009	ORL Database, University of Rajshahi signature database, USTB China dataset.	Visage, oreilles, signatures	Rangs	ACC= 99,02 %
Tahmasebi et Pourghassem [168]	2017	SVC2004, PolyU, UND.	Signatures, oreilles, empreintes palmaires.	Rangs	ACC= 99.63%
Sharma et Al [146]	2017	FVC2002, Face94(university of Essex, UK).	empreintes, visage.	Decisions	ACC= 99.5%
Al-waisy et al [53]	2017	SDUMLA-HMT, CASIA-IrisV3 Interval, IITD iris.	Iris gauche et iris droit.	Rangs	CASIA ACC= 99.07% SDUMLA-HMT ACC= 96.99%
Khemmar et al [116]	2017	ORL database., homemade database	visage	capteurs	RR=0.9
Kabir et al [109]	2018	AMI-subset-1, FVC2002DB1-A, Palmprint-IITD.	Oreilles, empreintes digitales, empreintes palmaires.	Décisions et caractéristiques	ACC : 94,91 % et 94,61 %
Hammad et al [96]	2018	PTB, CYBHi, LivDet2015, FVC 2004.	ECG, Empreintes digitales.	Caractéristiques et décisions	average ACC= 99,12 %
Hameed et al [87]	2019	Données collectées	Empreintes	Decisions	EER=13.61
Walia et al [177]	2019	Données collectées	iris, empreintes digitales, veines des doigts	Scores	ACC=98.43%, EER=1.57%
Gunasekaran et al [95]	2019	CASIA Biometric Ideal.	Visage, empreintes digitales, iris	Rangs	RR= 82%
Alay et Albaity [54]	2020	SDUMLA-HMT.	Iris, visage, veines des doigts	Caractéristiques et scores	ACC= 99.39%

Auteurs	Année	Base de données	Modalités	Type de fusion	Résultat (ACC, average ACC, RR, EER)
Cherrat et Al [83]	2020	Fingerprint Verification Competition 2004 dataset , the VERA Fingervein Database, The AR face database.	Empreintes digitales, veine digitale, visage	Decisions	ACC= 99.43%
Ahmad et al [49]	2020	NIST BSSR1, OU-ISIR BSS4.	Empreintes digitales, démarche, et visage.	Rangs	NIST BSSR1 ACC= 99.42 % ,OU-ISIR BSS4 ACC= 91.63 %
Ryszard S. Choras [110]	2020	200 images collectées de 20 individus.	Veines palmaires, veines dorsales de la main et le contour des yeux.	Caractéristiques	RR = 95.3 %
Kumar et al [145]	2020	200 images collectées de 20 individus	Signatures dynamiques, électroencéphalogramme (EEG).	Decisions	ACC = 98.78%
Leghari et al [124]	2021	4200 Empreintes, et 4200 signatures collectées.	Empreintes digitales et signatures en ligne.	Caractéristiques	ACC= 99.10%
Boucetta et al [55]	2021	données collectées	Iris, visage, empreintes palmaires	Capteurs	ACC=99.67%
Sarangi et al [158]	2021	UND-J2 database, UND-E database.	Profil facial, oreilles.	Caractéristiques	UND-J2 ACC= 98.97 % , UND-E ACC= 97.92 %
Huang [103]	2022	Casia-iris-interval-v4, NFBS.	Iris et IRM du cerveau	Caractéristiques	Average ACC= 97%
Bayan et al [140]	2022	Images de visages et empreintes de 20 individus.	Visage, empreintes digitales	Caractéristiques	Average ACC= 90,23%
Punyani et al [147]	2022	WPUT, CASIA.	Oreilles, et empreintes palmaires	Scores et décisions	ACC= 98.4%

Anil and Ravikumar [57]	2022	Images et voix extraites de vidéos.	Visage, et voix	Décisions et caractéristiques	ACC= 98,47 %
Rajasekar et Al [149]	2022	CASIA V3 iris dataset, FVC2006 fingerprint dataset.	Iris et empreintes digitales.	Scores	ACC= 99.88%
Atia et Al [47]	2022	PolyU	Empreintes palmaires, empreintes d'articulations des doigts	Scores	EER= 0.0%
Aizi et Al [111]	2022	données collectées,	Iris, empreintes.	Scores	RR=95.00%
Iula et Al [60]	2022	données collectées	main, paume	Scores	EER=0.08%

TABLE 2.1 – Tableau comparatif des travaux

2.5 Conclusion

Dans ce chapitre, nous avons synthétisé et comparé quelques travaux dans le cadre d'un état de l'art sur la multimodalité biométrique. La comparaison de ces documents nous permet d'observer les différents cas d'application des modalités et des types de fusion existants dans le but de proposer un système biométrique multimodal qui vient améliorer l'une des approches existantes.

Chapitre 3

Système d'authentification biométrique multimodal proposé

3.1 Introduction

Comme vue dans les chapitres un et deux, la multimodalité a été adoptée comme solution dans les systèmes biométriques, afin de pallier les limitations de l'unimodalité. L'existence de multiples traits biométriques, de méthodes pour la fusion et la prise de décision, rend le domaine de la multimodalité biométrique très vaste. Plusieurs propositions différentes de systèmes, notamment celles présentées précédemment dans la synthèse de documents, ont vu le jour, selon divers buts d'études. Ce chapitre mettra donc en avant une proposition de système biométrique multimodal. Il abordera tout d'abord la problématique étudiée, puis mettra en avant la solution proposée en justifiant les modalités utilisées. Enfin, il présentera de manière détaillée les différentes phases du système multimodal proposé.

3.2 Problématique

La croissance du nombre d'utilisateurs sur internet augmente très rapidement (voir la figure 3.1), plus particulièrement après la pandémie du covid 19, et avec eux augmente le nombre de transactions en ligne, de connexions à des comptes privés, et de données confidentielles à sécuriser [30]. Bien que les mots de passe soient largement utilisés pour la sécurité sur internet [32], ils présentent plusieurs désavantages, tels que leur fragilité aux vols, le risque d'oubli, etc., qui sont un risque de sécurité évident.

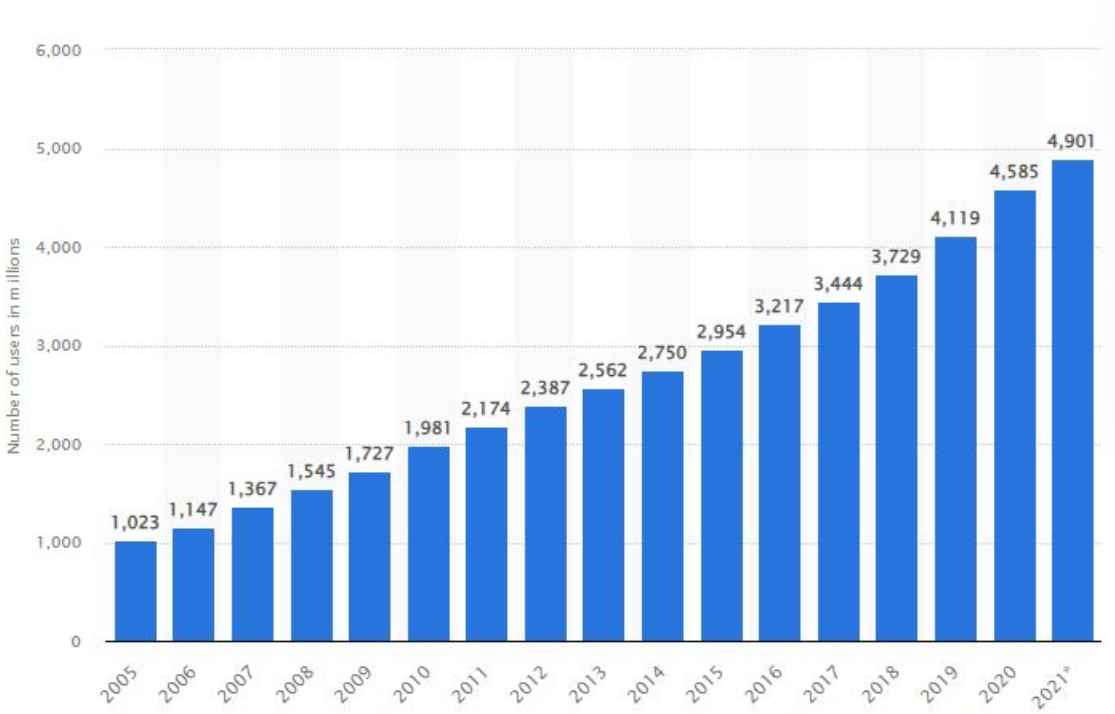


FIGURE 3.1 – Progression du nombre d'internautes dans le monde de 2005 à 2021[30]

L'utilisation de la biométrie pour l'authentification en ligne est une alternative intéressante qui commence déjà à être adoptée [159].

Toutefois, les systèmes biométriques au service de l'authentification en ligne limitent le nombre de modalités utilisables et soulèvent d'autres défis quant à l'efficacité de ces systèmes. En effet, la mise en place des systèmes biométriques sur des plateformes en ligne permet moins de contrôle sur l'environnement d'acquisition des modalités, ainsi que le temps et la vitesse du processus d'authentification. De plus, d'autres défis comme la disposition des utilisateurs à offrir leurs informations biométriques et leur difficulté d'accès au système suite aux inconvénients liées à l'acquisition des modalités telles que la disponibilité des dispositifs adéquats [8].

3.3 Solution proposée

Dans ce travail, nous proposons de développer un système d'authentification biométrique multimodal non coûteux et facile d'utilisation en utilisons des modalités adaptées. Cependant, la proposition d'un système biométrique multimodal soulève certaines questions sur le choix des modalités à combiner, les différents traitements à appliquer pour mieux exploiter ces dernières, ainsi que la technique de fusion à adopter afin d'améliorer les performances du système. Dans ce qui suit, nous justifions le choix des modalités et des techniques de fusion d'information à utiliser tout en expliquant les étapes de la solution proposée.

3.3.1 Choix des modalités

Étant donné que notre système utilise plusieurs modalités, le choix de celles-ci est une étape primordiale. Il est impossible de dire qu'une modalité est meilleure qu'une autre de façon universelle. Toutefois, certains traits biométriques sont clairement plus appropriés que d'autres pour certains cas d'application [178].

Comme nous souhaitons opter pour des modalités facilement accessibles via des dispositifs présents chez la plupart des utilisateurs tels que les ordinateurs classiques et les smartphones, nous avons choisi deux modalités de nature différentes qui sont la signature et le visage. Celles-ci ont été choisies, selon divers facteurs dont le degré d'intrusivité, le coût, etc. [148]. Comme indiqué sur la figure (3.2), le visage est une modalité moyennement intrusive et sans effort pour l'utilisateur, tandis que la signature est non intrusive. La combinaison des deux aura donc pour but d'augmenter l'efficacité globale du système, sans pour autant encombrer l'utilisateur avec de longues procédures.

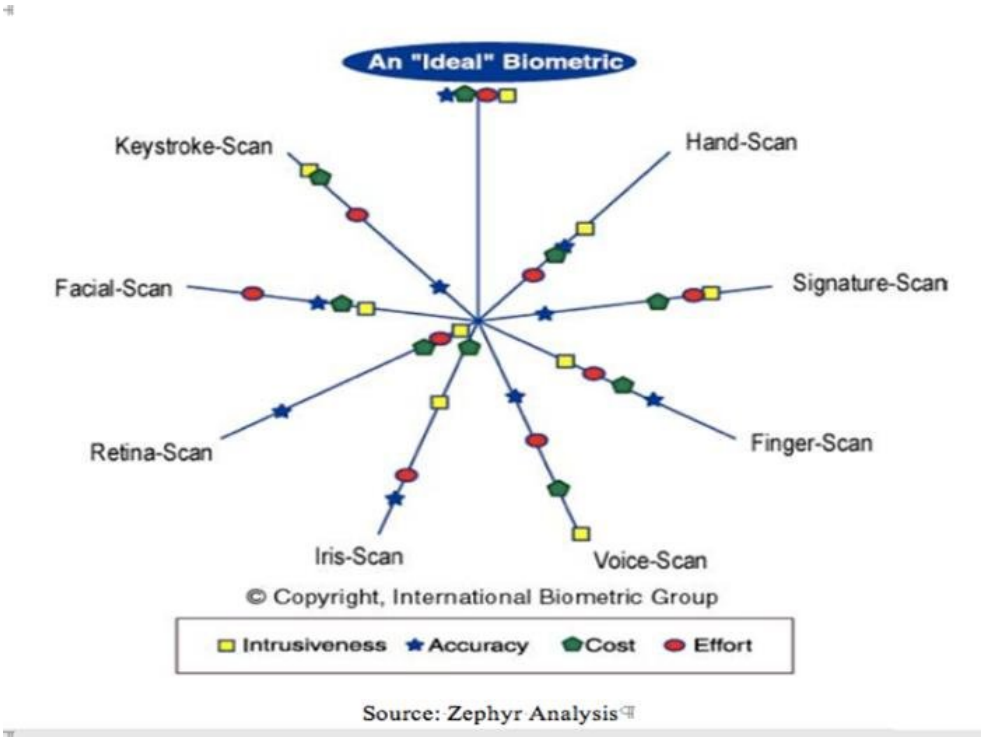


FIGURE 3.2 – Schéma comparatif entre plusieurs modalités selon différents critères [148]

3.3.2 Choix de type de fusion

La fusion est effectuée au niveau des scores, car cela offre un meilleur compromis en termes d'informations et de simplicité de fusion [132]. Elle se divise en plusieurs étapes : la modélisation, la combinaison et la décision, et se base sur la théorie de Dempster-Shafer (DST). Cette théorie est intéressante pour la fusion, puisqu'elle offre des mécanismes pour chacune des étapes du processus de fusion et permet de représenter les imperfections des informations et les fiabilités des sources d'informations. De plus, dans les travaux se basant sur DST [133], [129], il n'y a pas de document abordant la fusion des signatures en ligne et le visage. Les fondements de la théorie de Dempster-Shafer seront présentés dans la section (3.3.4).

3.3.3 Explication du système proposé

Dans ce travail, nous proposons un système biométrique multimodal basé sur deux modalités : le visage et la signature en ligne. Chacune sera traitée dans un sous-système qui fournit des scores de similarités utiles pour l'étape de fusion (voir la figure 3.3).

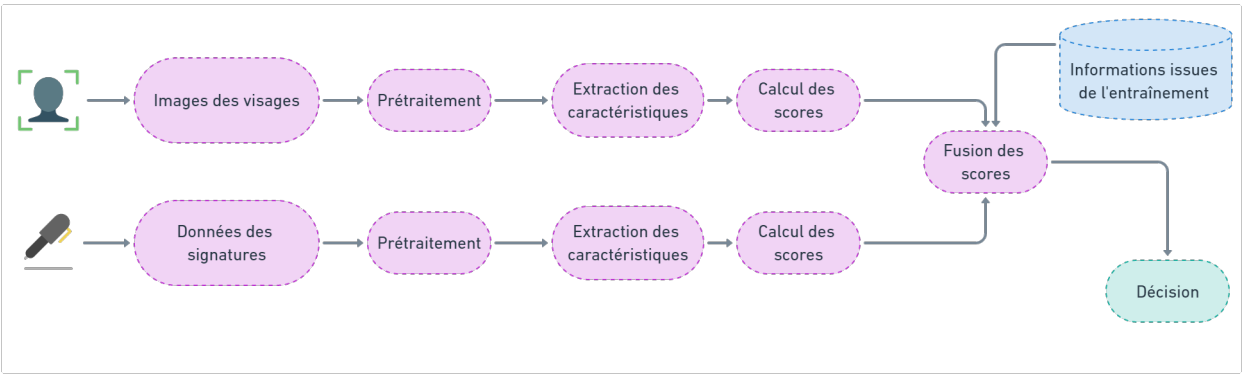


FIGURE 3.3 – Étapes du système biométrique multimodal proposé

Le premier sous-système, le système traitant la modalité du visage, prend en tant que données d'entrées des images brutes, qui passent par des prétraitements dans le but de leur préparation à la phase d'extraction de caractéristiques. Cette phase fournie les informations les plus utiles et importants. En se basant sur une mesure de distance, une comparaison est faite avec la base de référence, ce dont résulte des scores de dissimilarité. Ceux-ci seront ensuite normalisés vers une échelle de $[0, 1]$ à l'aide de la normalisation min-max, pour permettre de les transformer en scores de similarités, nécessaire en tant que données d'entrées pour l'approche choisie comme moyen de fusion.

Le deuxième sous-système abordant les signatures utilise les caractéristiques des signatures afin de comparer entre celles-ci. La mise en correspondance, c'est-à-dire la comparaison, est effectuée à l'aide de l'algorithme Dynamic Time Warping (DTW) expliqué dans la section (3.3.4). Les distances résultantes sont alors transformées en scores de similarité.

3.4 Phase d'acquisition

Comme vue précédemment dans l'architecture des systèmes multimodaux, le module d'acquisition englobe le processus d'obtention des traits biométriques sous forme de données brutes. Pour le processus d'acquisition d'images des visages, les dispositifs utilisés sont des capteurs sans contact (caméra, appareil photo, etc.). Toutefois, dans notre travail, ce processus n'est pas concrètement mis en œuvre, car nous avons utilisé des données déjà disponibles. De même dans le cas des signatures. Néanmoins, nous détaillons quelques concepts fondamentaux concernant les types et les moyens d'acquisition des signatures.

Les signatures manuscrites peuvent être collectées de deux manières différentes (voir la figure 3.4). La première est hors ligne, c'est-à-dire que les données d'entrées au système sont des images statiques de signatures sur papier. La deuxième est en ligne, c'est-à-dire que les informations temporelles et spatiales sont collectées durant l'action de la signature telles que les coordonnées, la durée, la pression, l'inclinaison, etc [125]. Dépendamment du type d'acquisition, les signatures peuvent exiger des traitements différents bien qu'ils soient similaires [144].

Pour que les caractéristiques des signatures en ligne soient collectées de façon dynamique, l'utilisation des dispositifs spéciaux est requise. Autre que les appareils spécialement conçus à cet effet [180], il existe d'autres moyens d'acquisition tels que les PC tablettes [56], Les caméras (qui tracent la trajectoire des signatures dans une séquence vidéo) [131], ou encore, d'autres appareils personnels, PDA (personal digital assistant) tels que les smartphones ou les tablettes [128].

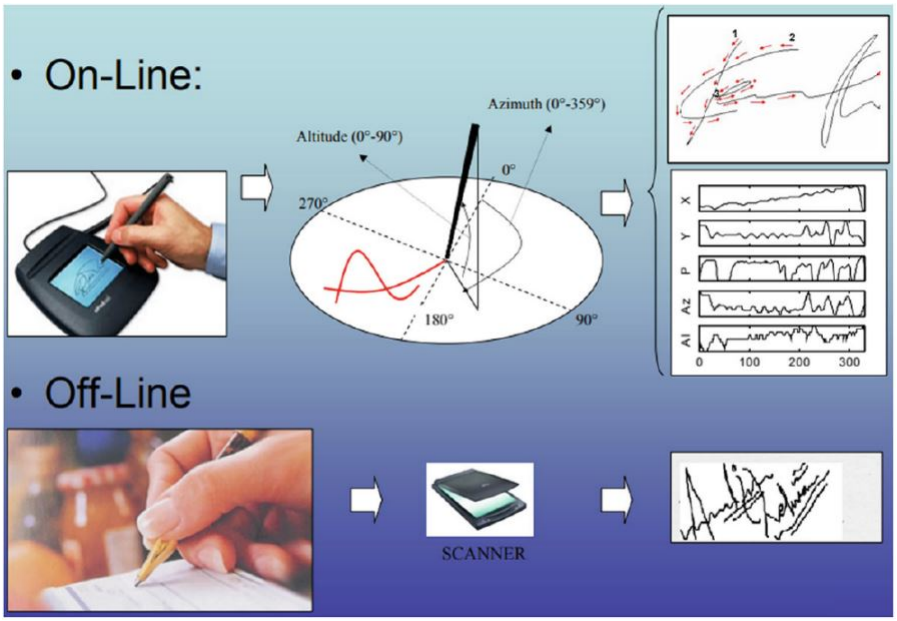


FIGURE 3.4 – Différences entre les signatures en ligne et hors ligne [155]

3.5 Phase de prétraitement

Le prétraitement joue un rôle de préparation des données pour l'extraction des caractéristiques. Les méthodes de celui-ci dépendent du type de données brutes à traiter.

3.5.1 Prétraitement des données de visages

Les images des visages en tant que données brutes augmentent la difficulté du processus de reconnaissance, car celles-ci peuvent inclure une quantité significative de bruits, une variation importante en termes de luminosité, des problèmes associés au type d'images acquises (photo, vidéo, 3D, infrarouge, etc.) ou bien des défis non techniques tels que les changements d'expression d'un individu [70].

Un prétraitement est nécessaire afin d'uniformiser les données acquises comme le montrent les exemples de la figure (3.5). Ainsi, pour pallier les problèmes cités ci-dessus, on peut trouver utile la transformation en niveaux de gris pour les images en couleur [113], l'application des filtres pour l'élimination des bruits [141], l'égalisation d'histogramme pour remédier aux variations de luminosité [58], l'alignement et le recadrement d'image [126].

Dans notre cas, les prétraitements auxquels se restreint notre étude sont : égalisation d'histogramme et recadrement d'image :

- Recadrement d'image : comme la partie de l'image qui nous intéresse est juste le visage, nous souhaitons éliminer au maximum les région de l'arrière-plan et rogner l'image de sorte à garder que les régions d'intérêts. Pour cela, nous utiliserons afin de détecter la zone du visage un classificateur pré-entraîné Haar-cascade d'OpenCV. Ce dernier est un classificateur utilisé pour détecter l'objet pour lequel il a été formé qui est dans ce cas-là le visage [38]. Ensuite, on applique le rognage d'image.

- Égalisation d'histogramme : elle consiste à l'étirement de l'histogramme de l'image de sorte à obtenir un histogramme relativement plat qui s'étend sur toute la plage d'intensités des valeurs, et cela permet d'ajuster le contraste de l'image.

FIGURE 3.5 – Exemples d'images faciales prétraitées [70]

3.5.2 Prétraitement des données de signatures

Il existe diverses techniques de prétraitement dépendamment du type de signature. De multiples documents classifient les techniques de prétraitement les plus utilisées dans la littérature. Nous citons parmi celles-ci les classes suivantes [155] :

- Filtrage : le filtrage consiste à l'élimination des bruits et l'amélioration de la qualité de l'image de la signature avant l'extraction de caractéristiques. Cela inclut l'usage de filtres tels que le filtre médian, gaussien, etc.

- Rééchantillonnage : en augmentant, ou en diminuant le nombre d'échantillons, les résultats peuvent être améliorés.

- Normalisation : les données brutes acquises peuvent avoir des échelles et des unités différentes selon le type d'appareil d'acquisition. Il y a plusieurs techniques de normalisation dont la translation de la position du centroïde de la signature vers l'origine définie par l'équation (3.1), la standardisation mise en avant par l'équation (3.2), et la normalisation min-max définie par l'équation (3.3), etc.

Ce travail repose sur le traitement des signatures en ligne. De ce fait, les données sont de type numérique et n'exigent pas nécessairement un prétraitement. En effet, un prétraitement tel qu'une normalisation peut être cause de perte d'informations et une altération significative des résultats [144]. Pour cela, plusieurs tests avec et sans prétraitement sont pratiqués afin d'en étudier l'effet sur les résultats. Les techniques utilisées dans les cas de prétraitement sont :

- Translation des centroïdes des coordonnées des signatures vers l'origine du système des coordonnées :

$$x_i^N = x_i - \bar{x} \quad \text{avec} \quad \bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad , \quad y_i^N = y_i - \bar{y} \quad \text{avec} \quad \bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i \tag{3.1}$$

  où :
  — x : la coordonnée x ;
  — y : la coordonnée y ;
  — N : le numéro de l'échantillon (signature) ;
  — i : le numéro de la ligne dans un échantillon ;
  — n : le nombre total de lignes dans un échantillon ;
  — $\bar{x}$: la moyenne de toutes les coordonnées x de la signature N ;
  — $\bar{y}$: la moyenne de toutes les coordonnées y de la signature N.

- Standardisation en divisant l'équation (3.1) par l'écart type :

$$x_i^N = \frac{x_i - \bar{x}}{\sigma_x} \quad , \quad y_i^N = \frac{y_i - \bar{y}}{\sigma_y} \tag{3.2}$$

  où :
  — x : la coordonnée x ;
  — y : la coordonnée y ;
  — N : le numéro de l'échantillon (signature) ;
  — i : le numéro de la ligne dans un échantillon ;
  — σ : l'écart type.

- Normalisation min-max afin de ramener l'échelle des coordonnées x et y entre 0 et 1000. La valeur maximale de l'échelle a été choisie de sorte à avoir une uniformité des échelles tout en ayant une quantité d'informations suffisante pour la distinction entre les échantillons [59] :

$$x_n = \frac{x - min(x)}{max(x) - min(x)} \times 1000 \quad , \quad y_n = \frac{y - min(y)}{max(y) - min(y)} \times 1000 \tag{3.3}$$

  où :
  — x : la coordonnée x ;
  — y : la coordonnée y ;
  — n : le numéro de la ligne dans un échantillon ;
  — $min(x)$: la valeur minimum des coordonnées x ;
  — $max(x)$: la valeur maximum des coordonnées x ;
  — $max(y)$: la valeur maximum des coordonnées y ;
  — $min(y)$: la valeur minimum des coordonnées y.

Dans le cas de notre système, les prétraitements des signatures sont testés sur les caractéristiques de coordonnées x et coordonnées y. Le reste des caractéristiques, moins sensibles aux bruits [59], n'est pas préretraités de sorte à conserver les informations cruciales que peuvent apporter les valeurs originales.

3.6 Phase d'extraction des caractéristiques

Cette étape permet de rendre les données moins volumineuses. Cela, en faisant une numérisation de ces dernières et en gardant que les informations les plus intéressantes, ce qui facilite le traitement des données dans les prochaines étapes. Étant donné que dans notre travail, on utilise plusieurs modalités, plus précisément le visage et la signature, on aura deux phases d'extraction de caractéristiques, une pour chaque modalité.

3.6.1 Extraction des caractéristiques des visages

L'analyse de composantes principales (ACP) aussi appelé en anglais Principal Component Analysis (PCA) [62] est un algorithme qui permet de réduire la dimensionnalité, il est largement utilisé dans la reconnaissance des formes, et est peu sensible aux bruits. Turk et Pentland sont les premiers ayant mis en évidence l'efficacité de cet algorithme dans le domaine de reconnaissance faciale [172]. L'ensemble des vecteurs propres (eigenvectors) et valeurs propres (eigenvalues) permet de représenter un nouveau plan, la visualisation des vecteurs propres introduit le concept d'eigenfaces illustré dans la figure (3.6). C'est l'ensemble d'images de visages fantômes qui contiennent toutes les variations issues des images d'entrainement. Une projection de ces dernières sur le plan résultant, implique une nouvelle représentation sous forme d'une combinaison linéaire [72].

Tout ce processus constitue l'extraction des caractéristiques qui sera aussi appliqué sur les échantillons d'images tests en faisant une projection de celles-ci sur le nouveau plan. Dans ce qui suit, nous représentons les éléments utiles et étapes nécessaires dans les calculs de l'approche donnée [62] :

- Calcul d'image moyenne

$$\Psi = \frac{1}{n}\sum_{=1}^{n} x_i \tag{3.4}$$

où :
— n : nombre de vecteurs ;
— x : vecteur d'une image ;
— Ψ : vecteur de l'image moyenne.

- Soustraction d'image moyenne pour chaque vecteur (centralisation) :

$$a_i = x_i - \Psi \tag{3.5}$$

— x : vecteur d'une image ;
— Ψ : vecteur de l'image moyenne ;

— a : vecteur après centralisation.

- Calcul de la matrice de covariance :

$$C = A^t A, \text{ avec } A = \{a_1, a_2, a_3, ..., a_n\} \tag{3.6}$$

— A : matrice de vecteur a_i ;
— A^t : matrice transposée de A ;
— C : matrice de covariance.

- Calcul des vecteurs propres et valeurs propres

$$Cv_i = \lambda_i v_i \tag{3.7}$$

— λ_i : vecteur propre ;
— v_i : valeur propre.

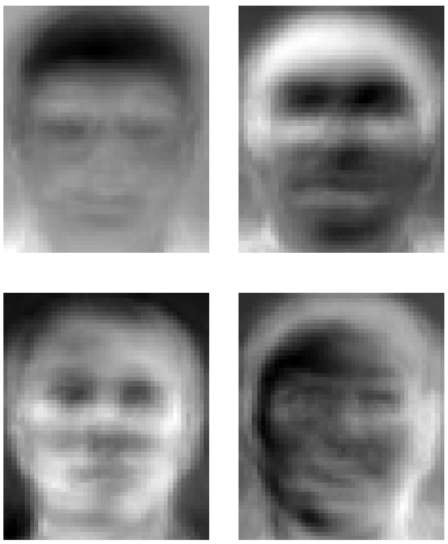


FIGURE 3.6 – Images d'eigenfaces obtenues par AT&T Laboratories Cambridge [33]

3.6.2 Extraction des caractéristiques des signatures

L'extraction des caractéristiques des signatures et le choix de ces dernières ont une influence sur les résultats du système d'authentification. Il existe de multiples caractéristiques utilisées dans divers travaux, et dont les plus communes sont listées dans le tableau (3.1) [90] :

#	Description
1	Coordonnées x(t)
2	Coordonnées y(t)
3	Pression p(t)
4	Horodatage (Time stamp)
5	Position absolut, $r(t) = \sqrt{x^2(t) + y^2(t)}$
6	Vélocité dans x, $v_x(t)$
7	Vélocité dans y, $v_y(t)$
8	Vélocité absolut $v(t) = \sqrt{v_x^2(t) + v_y^2(t)}$
9	Accélération dans x, $a_x(t)$
10	Accélération dans y, $a_y(t)$
11	Accélération absolut $a(t) = \sqrt{a_x^2(t) + a_y^2(t)}$

TABLE 3.1 – Liste des caractéristiques communes des signatures [90]

Dans notre cas, nous faisons usage de caractéristiques accessibles via les PDA, c'est-à-dire :

- Coordonnées x (X-coordinate) : les positions des points de la signature selon l'axe x ;
- Coordonnées y (Y-coordinate) : les positions des points de la signature selon l'axe y ;
- Horodatage (Time stamp) : le temps où la signature a été enregistrée dans le système ;
- L'état du bouton (Button status) : 0 pour stylo levé et 1 dans le cas contraire.

3.7 Phase de mise en correspondance (Matching)

Après l'extraction des caractéristiques, vient l'étape de mise en correspondance qui correspond à la phase où la comparaison 1 à 1 entre les échantillons est mise en œuvre. Étant donné que notre système multimodal fait usage de deux modalités, les comparaisons sont donc effectuées dans deux sous-systèmes. Initialement, les scores sont obtenus à partir des mesures de distances qui seront ensuite transformées en scores de similarité variant sur une échelle commune de $[0, 1]$ permettant leur fusion.

3.7.1 Comparaison

Dans cette phase, la vérification d'identité sera effectuée. Étant donné que le système de fusion est composé de deux sous-systèmes, deux vérifications sont donc mises en œuvre, une pour chaque sous-système.

Comparaison des visages

Dans le cas des visages, la comparaison entre une image donnée avec la base de référence se produit par des mesures de distances, dont on peut citer [24] :

- Distance euclidienne : c'est la distance la plus couramment utilisée, son calcul est basé sur les coordonnées cartésiennes des points en utilisant le théorème de Pythagore.

$$D(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{3.8}$$

- Distance manhattan : Cette distance est souvent mieux adaptée dans le cas ou les valeurs sont discrètes ou binaires, car son calcul fait référence à la distance entre deux vecteurs s'ils ne pouvaient se déplacer qu'à angle droit.

$$D(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{3.9}$$

Dans notre étude, des tests comparatifs basés sur ces deux distances seront effectués afin de choisir la mesure de distance qui permet d'atteindre les performances les plus hautes. Les résultats expérimentaux basés sur ces deux métriques de distances seront mis en évidence dans le chapitre 4.

Comparaison des signatures

Dans le cas des signatures, diverses méthodes, afin de les comparer entre elles, sont utilisées dans la littérature dont l'une des plus populaires est l'algorithme Dynamic Time Warping (DTW) [144]. L'algorithme DTW permet de calculer la distance entre deux tableaux de longueurs différentes [182]. Son mode de fonctionnement repose sur le principe de construction d'une matrice des distances entre deux séries de points afin de créer des correspondances un à plusieurs et plusieurs à un et de retourner la distance totale minimum qui permet d'aligner les deux séries de points. L'exemple de la figure (3.7), illustre le déroulement de l'algorithme sur deux exemples de séries de points de longueurs différentes, avec des courbes similaires. La dernière case indiquée de la matrice correspond à la distance globale (aussi appelée coût minimum) entre les deux séries.

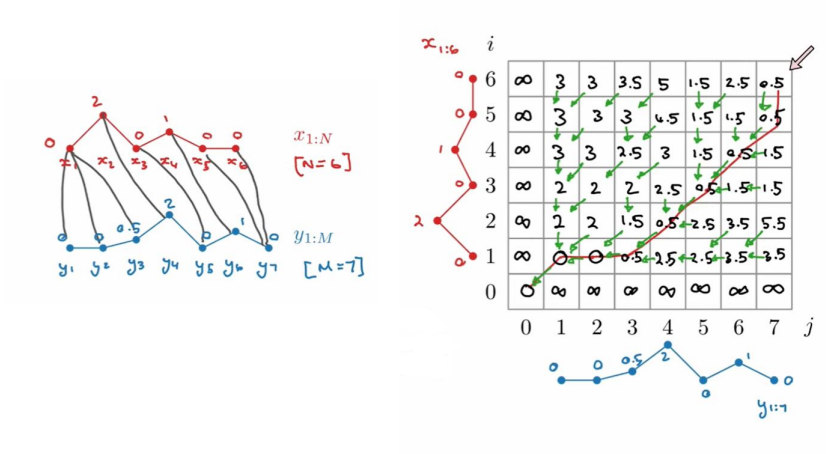


FIGURE 3.7 – Déroulement de l'algorithme DTW [112]

L'usage de DTW pour les signatures au lieu de la distance euclidienne classique permet de remédier au problème des longueurs différentes qui peut survenir dans le cas des données des signatures (voir la figure 3.8) [182].

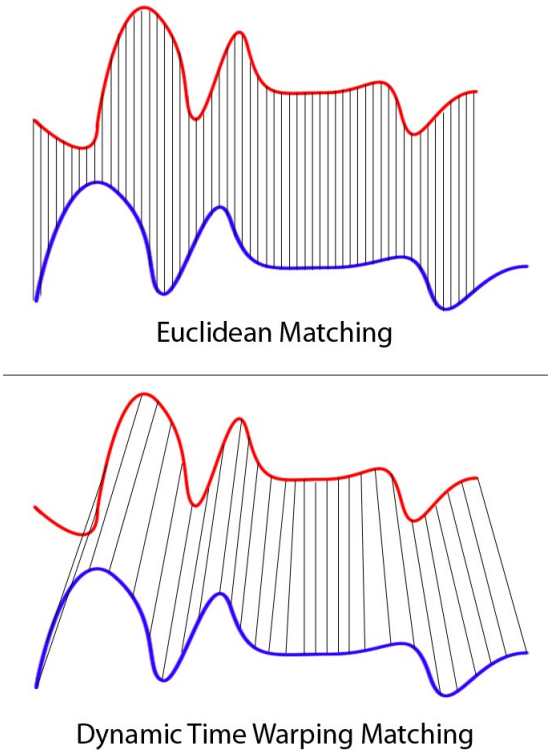


FIGURE 3.8 – Différence entre la distance euclidienne et DTW [112]

3.7.2 Attribution des scores

Après le calcul des distances, les deux sous-systèmes procèdent au même traitement qui permet de transformer ces dernières en scores de similarité.
Tout d'abord, une normalisation est appliquée aux distances pour passer à la transformation en scores de dissimilarité, il existe plusieurs normalisations telles que z-score, décimal et min-max [142]. Cette dernière normalisation, mise en avant dans l'équation (3.10), a été prise comme choix idéal pour les deux sous-systèmes, afin d'avoir une échelle commune de $[0, 1]$ pour les valeurs des deux sources.

$$z_i = \frac{v_i - min}{max - min} \tag{3.10}$$

— v_i : la ième valeur du vecteur de distances ;
— z_i : la ième valeur après normalisation ;
— min : valeur minimum du vecteur de distances ;
— max : valeur maximum du vecteur de distances.

Afin de passer des scores de dissimilarité vers des scores de similarité, c'est-à-dire plus la valeur est proche de 1 plus la correspondance est forte, une simple soustraction a été utilisée :

$$S_i = 1 - D_i \tag{3.11}$$

— S_i : score de la ième valeur ;
— D_i : distance de la ième valeur.

3.8 Fusion d'informations

Les scores obtenus de chaque sous système sont des informations numériques acquises à partir de deux sources différentes. La fusion de ces valeurs vise à la gestion de ces données multi-sources, dans le but d'une prise de décision finale qui sera retournée par le système d'authentification. Comme mentionné précédemment, nous avons choisi la théorie Dempster-Shafer pour fusionner les scores obtenus. Toutefois, avant d'appliquer cette théorie, nous rappelons brièvement ses fondements.

3.8.1 Définitions préliminaires

La théorie de l'évidence, aussi appelée théorie des fonctions de croyance, ou encore théorie de Dempster Shafer, est une théorie mathématique mise en avant par Dempster en 1967, et améliorée par Shafer en 1976. Elle définit une représentation de l'information différente de l'approche probabiliste, en permettant l'assignation de probabilités appelées masses à des ensembles non-singletons, ainsi que la gestion des informations provenant de sources différentes. Il existe trois fonctions importantes dans la théorie de Dempster-Shafer : fonction d'assignation des masses (*m*), fonction de croyance (Bel), fonction de plausibilité (Pls) [161]. Celles-ci ainsi que d'autres notions de la théorie de l'évidence sont définies dans la liste suivante :

- Cadre de discernement : est l'ensemble des hypothèses d'un problème donné noté $\theta = \{\theta 1, \theta 2, ..., \theta k\}$ [133] ;

- Ensemble puissance : est l'ensemble des sous-ensembles possibles à partir du cadre de discernement noté 2^θ. Il inclut aussi l'ensemble θ et l'ensemble vide [133] ;

- Fonction d'assignation des masses : aussi appelée Basic Belief Assignment (BBA), est une fonction permettant d'associer à chaque élément A de l'ensemble de puissance 2^θ un degré de croyance (masse) dans l'ensemble $[0, 1]$ [133] ;

- Fonction de croyance (Belief Function) : est la somme des masses des hypothèses B incluses dans l'hypothèse A. Elle est définie par la formule suivante [183] :

$$\text{Bel}(A) = \sum_{B \subseteq A} m(B) \tag{3.12}$$

- Fonction de plausibilité (Plausibility function) : est la somme des masses des hypothèses incluant l'hypothèse A. Elle est définie par la formule suivante [183] :

$$\text{Pls}(A) = \sum_{A \cap B \neq \varnothing} m(B) = 1 - \text{Bel}(\bar{A}) \tag{3.13}$$

- Fonction de communalité (Commonality function) : représente l'intégralité de la croyance accordée aux sur-ensembles de A. Elle est décrite par la formule suivante [46] :

$$q(A) = \sum_{A \subseteq B} m(B) \quad \forall A \subseteq \Omega \tag{3.14}$$

- Règles de combinaison (Combination Rules) : la théorie de Dempster Shafer permet la fusion des masses de plusieurs sources dans le but de palier les imperfections des informations apportées par chacune d'elles. Il existe plusieurs règles dont la règle de Dempster, la règle de Smets, la règle de Yager, la règle de Dubois et Prade, ou autre [161].

3.8.2 Étapes de fusion

Le système multimodal proposé repose sur une architecture ayant deux systèmes, l'un pour les visages, et l'autre pour les signatures qui produisent tous deux des scores de similarité. Ces scores, une fois transformé en masses, seront fusionnés grâce à une règle de combinaison afin de produire une masse globale sur laquelle se basera la prise de décision (voir la figure 3.9).

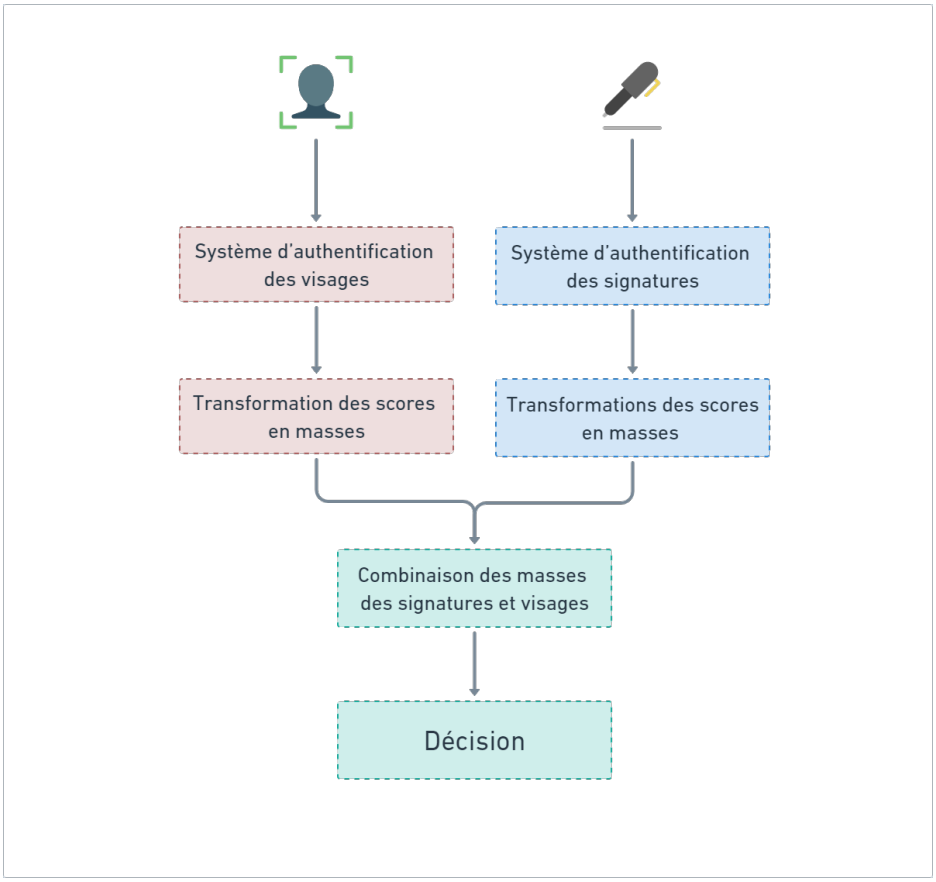


FIGURE 3.9 – Schéma de la fusion au niveau des scores appliquée

Dans le cas de cette fusion, nous détaillons les trois étapes : la modélisation, la combinaison des informations à fusionner, et la dernière qui est la prise de décisions.

Modélisation

Cette étape consiste à poser les formalismes se basant sur la théorie de Dempster Shafer afin de représenter le problème étudié. Dans notre cas, nous étudions l'authentification, c'est-à-dire, est-ce que l'utilisateur cherchant à s'authentifier est bien celui qu'il prétend être (genuine), ou pas (imposteur). Ces deux hypothèses sont donc notre cadre de discernement, formellement représenté par :

$$\theta = \{gen, imp\} \tag{3.15}$$

L'ensemble puissance est alors :

$$2^{\theta} = \{\varnothing, gen, imp, \theta\} \tag{3.16}$$

Toutes les issues possibles sont dans le cadre de discernement (monde fermé). La masse associée à l'ensemble vide est donc nulle.

La combinaison des informations équivaut à une combinaison entre les fonctions de masses différentes. En considérant le système des signatures et le système des visages comme deux sources d'information différentes, nous pouvons les représenter par deux fonctions de masses $m1$ et $m2$.

L'assignation de masses s'effectue à l'aide d'une fonction de transformation. Les scores seront alors transformés en degrés de croyances, en faisant usage d'une fonction de transformation reposant sur le score minimum des échantillons vrais et maximum des échantillons imposteurs de l'ensemble d'entraînement [129].

$$\begin{cases} \text{if}(S_{ik} > Max_{imp}) : \begin{cases} m_{ik}(gen) = S_{ik} \\ m_{ik}(\theta) = 1 - S_{ik} \end{cases} \\ \\ \text{if}(S_{ik} < Min_{gen}) : \begin{cases} m_{ik}(imp) = 1 - S_{ik} \\ m_{ik}(\theta) = S_{ik} \end{cases} \\ \\ \text{if}(S_{ik} \in [Min_{gen}, Max_{imp}]) : \begin{cases} \text{if}(S_{ik} > t_i) : \begin{cases} m_{ik}(gen) = 1 - S_{ik} \\ m_{ik}(\theta) = S_{ik} \end{cases} \\ \\ \text{if}(S_{ik} < t_i) : \begin{cases} m_{ik}(imp) = S_{ik} \\ m_{ik}(\theta) = 1 - S_{ik} \end{cases} \end{cases} \end{cases} \tag{3.17}$$

où :

— S_{ik} : score k de la source i ;
— $m_{ik}(gen)$: masse k de la source i pour le singleton (gen) ;
— $m_{ik}(imp)$: masse k de la source i pour le singleton (imp) ;
— $m_{ik}(\theta)$: masse k de la source i pour l'ensemble θ ;
— Max_{imp} : valeur maximum des scores imposteurs ;
— Min_{gen} : valeur minimum des scores vrais (genuine) ;
— t_i : seuil de la source i. Chaque sous-système possède un seuil définit.

Combinaison

Étant donné que les hypothèses du problème évoluent dans un monde fermé, les masses des visages et les masses des signatures obtenues seront fusionnées à l'aide de la combinaison conjonctive de Dempster mise en avant dans l'équation (3.18) [127] adaptée à notre cas.

$$m(A) = (m_1 \oplus m_2)(A) = \sum_{B \cap C = A} m_1(B) m_2(C) \tag{3.18}$$

où :

— A, B et C : trois hypothèses de l'ensemble puissance ;
— m_1 et m_2 : fonctions de masses.

Phase de décision

La dernière étape est la prise de décisions. Elle consiste à décider si oui ou non l'utilisateur est le vrai utilisateur, ou bien quelqu'un d'autre, ce qui équivaut à confirmer l'une des deux hypothèses de départ, ou bien à retourner une réponse neutre. Il existe diverses méthodes de prise de décisions allant dans ce sens [127]. Une fois les masses globales obtenues, il est facile de calculer les fonctions de croyance et de plausibilité permettant d'adopter un critère de décision. Dans le système proposé, nous explorons les critères suivants [127] :

A. **Maximum de plausibilité :**

Ce critère choisit l'hypothèse donnant le maximum de plausibilité (voir l'équation 3.19). C'est un critère optimiste, car il donne le maximum de chance à chacune des hypothèses.

$$\forall H_i \in \theta, Pls(H_k) = maxPls(H_i) \tag{3.19}$$

B. **Maximum de crédibilité (croyance) :**

Ce critère opte pour l'hypothèse donnant le maximum de crédibilité. Il repose sur la formule suivante :

$$\forall H_i \in \theta, Bel(H_k) = maxBel(H_i) \tag{3.20}$$

C. **Maximum de communalité :**

C'est un critère qui opte pour le maximum de communalité. Il se caractérise par la formule suivante :

$$\forall H_i \in \theta, Q(H_k) = maxQ(H_i) \tag{3.21}$$

3.9 Conclusion

Dans ce troisième chapitre, nous avons mis en avant les détails théoriques du système d'authentification proposé. les différentes étapes de celui-ci ont été expliqués et diverses notions intervenant dans l'approche de fusion adoptée ont été définies.

Chapitre 4

Implémentation et validation du système d'authentification proposé

4.1 Introduction

Ce chapitre est consacré à l'implémentation et la validation du système d'authentification biométrique multimodal proposé. Il commence par un aperçu de l'environnement matériel et logiciel utilisé dans l'implémentation du système proposé, puis une description des bases de données utilisées. Il met ensuite en avant l'apport de l'utilisation de la multimodalité basée sur DST par rapport aux systèmes unimodaux utilisant soit les signatures en ligne, soit les visages. Enfin, les résultats obtenus sur ces bases sont présentés selon les mesures de performances choisies.

4.2 Environnement de développement

Dans le but de programmer notre système, nous avons fait usage de plusieurs outils d'implémentation dont le langage python utilisé sur la plateforme Google Colab. Les spécificités matérielles de celle-ci sont abordées dans cette section, de même qu'une définition portant sur le langage python.

Langage Python

Python est un langage de programmation interprété, interactif et orienté objet créé par Guido Van Rossum. Il compte plusieurs modules, et permet la manipulation des types de données de façon dynamique. Autre que l'orienté objet, ce langage de programmation permet l'exécution de code procédural ou fonctionnel. Python est portable sur de multiples systèmes d'exploitation, cela inclut Linux, Windows, et MacOS [28].

Plusieurs modules de Python ont été utilisés dans le cadre de l'implémentation du système proposé. Nous en citons les plus importants :

- fastdtw : est une implémentation python de FastDTW [156], un algorithme approximatif du Dynamic Time Warping avec une complexité moins importante de $\mathcal{O}(N)$. Ce module a été utilisé afin de comparer les signatures et de retourner les distances [6] ;

- pyds : est une librairie python dédiée au calcul dans le cadre de la théorie de Dempster Shafer. Elle offre plusieurs méthodes pour le calcul des fonctions de croyances, la combinaison d'informations, etc [7].

Google Colab

Google Colab est une plateforme permettant la création d'environnements interactifs appelés Notebooks Colab qui sont des notebooks Jupiter hébergés par Colab. Elle permet l'écriture et l'exécution de code en langage Python et la collaboration entre plusieurs personnes dans le même environnement.

D'autres options utiles sont aussi disponibles telles que l'importation de données pour l'entraînement de modèles IA, l'accès gratuits au GPU, ou encore l'organisation du notebook en

plusieurs sections de codes exécutables, etc [16]. Les spécificités matérielles de Google Colab sont présentées dans la figure (4.1). Dans notre cas, nous utilisons un processeur CPU.

Parameter	Specification
GPU Model Name	Nvidia K80
GPU Memory	12 GB
GPU Memory Clock	0.82 GHz
GPU Performance	4.1 TFLOPS
CPU Model Name	Intel(R) Xeon(R)
CPU Frequency	2.30 GHz
Number of CPU Cores	2
Available RAM	12 GB
Disk Space	25 GB

FIGURE 4.1 – Spécifications matérielles de Google Colab [115]

Le système proposé a été implémenté sur un notebook organisé en 3 sections. La première pour le système des visages, la deuxième pour le système des signatures et la dernière pour la partie fusion.

4.3 Bases de données

Dans ce document, deux bases de données ont été utilisées, une pour chaque modalité : SVC2004 [5], et Yale Face Database [25]. L'échantillonnage du nombre de sujets de ces deux bases est identique, de sorte à simuler un nombre de personnes spécifiques avec chacune des images, des visages et des signatures associées. En effet, ceci a une importance dans l'étape de fusion qui exige le même nombre de scores donnés par les deux sous-systèmes. Pour cela, 15 personnes, dont 8 sont supposées être des vrais utilisateurs et 7 des imposteurs, sont prises dans les deux systèmes. Dans ce qui suit, une présentation des bases de données, ainsi que des détails concernant l'échantillonnage dans les deux cas sont mis en avant.

4.3.1 Base de données des visages

La base de données Yale Face Database de taille 6,4 Mo contient 165 images en niveaux de gris au format GIF de 15 individus. Il y a 11 images par sujet, selon différentes expressions faciales ou configuration. Dans notre étude, 135 images en été utilisées dans l'entraînement et les 30 images restantes dans le test, la séparation de ces données a été faite de sorte que 8 des sujets représentent les clients authentiques du système tandis que les 7 restants correspondent aux imposteurs. Le nombre d'échantillons a été devisé de la façon suivante :

- Dans l'ensemble d'entraînement : il y a 9 images par sujet ;
- Dans l'ensemble test : il y a 2 images par sujet.

4.3.2 Base de données des signatures

La base de données SVC2004 possède trois ensembles de données : Sample Data, Task1, et Task2. Étant donné que nous nous basons sur la signature en ligne, l'utilisation de Task1 est adaptée dans notre cas, car les informations qui y sont incluses peuvent être collectées par des PDA [181].

Task1 est un ensemble de données incluant 40 utilisateurs, chacun avec 20 vraies signatures et 20 imitations. L'ensemble d'entraînement du sous-système de signature est constitué de 270 signatures, dont 144 sont des signatures vraies et 126 sont des imitations. Pour l'ensemble test, 30 signatures ont été prises, dont 16 sont des vraies signatures et 14 sont des imitations.

Chaque fichier .TXT correspond à une signature respectivement labellisée par le numéro d'utilisateur et le numéro de la signature (voir la figure 4.2). Le premier numéro dans le fichier de chaque signature représente le nombre de lignes qui peut différer d'une signature à une autre, tandis que chaque colonne correspond respectivement aux caractéristiques : x-coordinate, y-coordinate, time stamp, et button status.

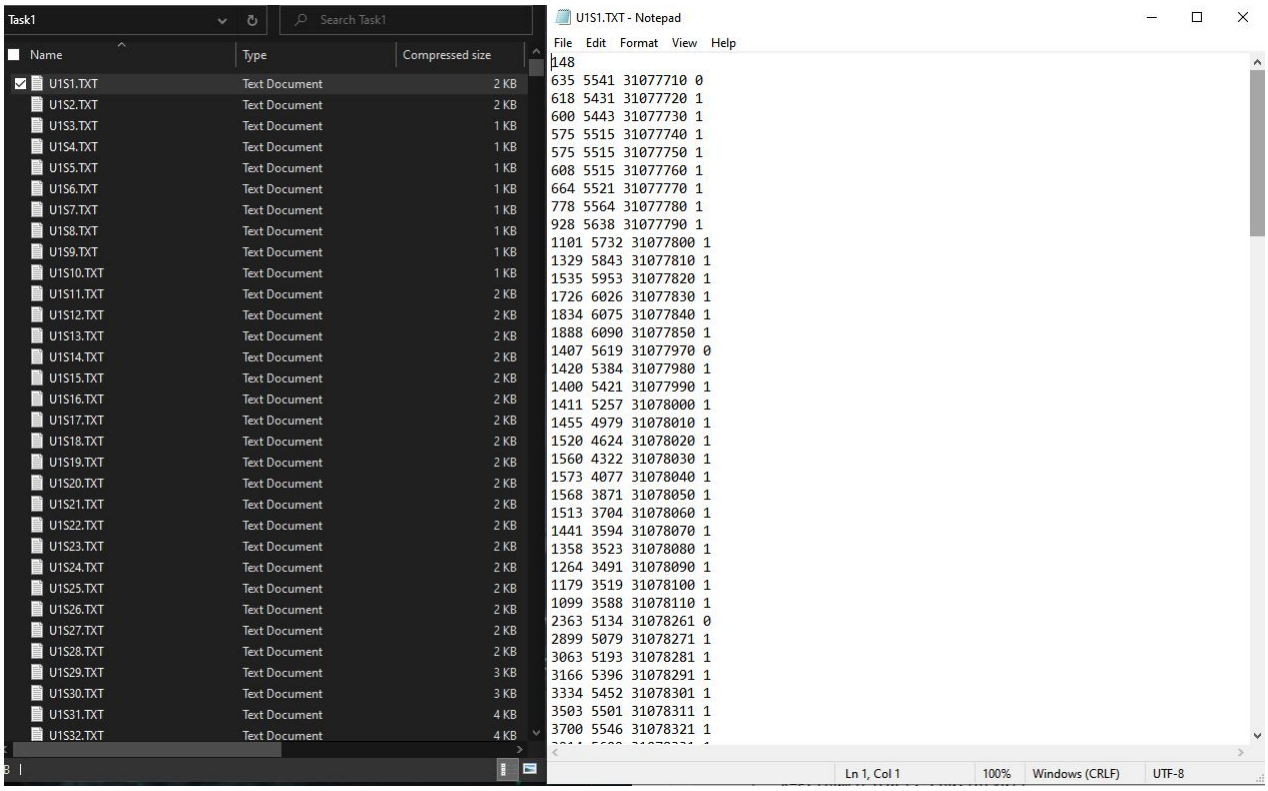


FIGURE 4.2 – Les données Task1 de SVC 2004

4.4 Résultats et discussion

Plusieurs tests ont été pratiqués dans un souci de choix des méthodes adéquates dans chaque phase du système proposé. Cette section aborde donc les résultats des divers tests mis en œuvre sur chaque sous système séparément, ainsi que d'autres tests globaux du système de fusion.

Les métriques d'évaluation utilisées sont le FAR, FRR, EER, et la précision, expliqués dans la section (1.6) du chapitre 1. Toutefois, il est intéressant de préciser l'ordre de priorité de ces dernières. La précision et le EER qui possèdent une relation de corrélation négative, présentent les premiers critères à prendre en considération. Ceci étant dû au fait que le EER est basé sur les deux autres critères, le FAR et FRR.

Une bonne performance selon le EER, FAR et FRR est obtenue lorsque le résultat est proche de 0, tandis que pour la précision, c'est le contraire, c'est-à-dire quand la valeur du résultat tend vers 1. En considérant que le facteur de sécurité est plus privilégié dans les systèmes d'authentification, l'ordre de priorité du FAR est donc supérieur au FRR.

4.4.1 Résultats des tests sur le sous-système des visages

Trois tests ont été effectués sur ce sous-système : un test lié à la luminosité des images, un test sur un paramètre de l'algorithme PCA et un test au sujet des mesures des distances : la distance euclidienne et Manhattan. Ces tests permettent la combinaison des meilleures configurations selon les critères d'évaluation de performances choisies, ce qui implique un sous-système de visage de haute performance, prêt pour l'étape de fusion.

Test sur la luminosité

Au sujet du test sur la luminosité, les deux prétraitements utilisés sont : égalisation d'histogramme (voir la figure 4.3) et une version améliorée de cet algorithme égalisation d'histogramme CLAHE (Contrast Limited Adaptive Histogram Equalization) (voir la figure 4.4)[22].

FIGURE 4.3 – Exemple de l'application d'égalisation d'histogramme

La figure (4.3) présente deux exemples de l'effet d'application de l'égalisation d'histogramme classique sur le premier individu. On peut remarquer que la luminosité est ajustée, telle que les images sont devenues moins sombres.

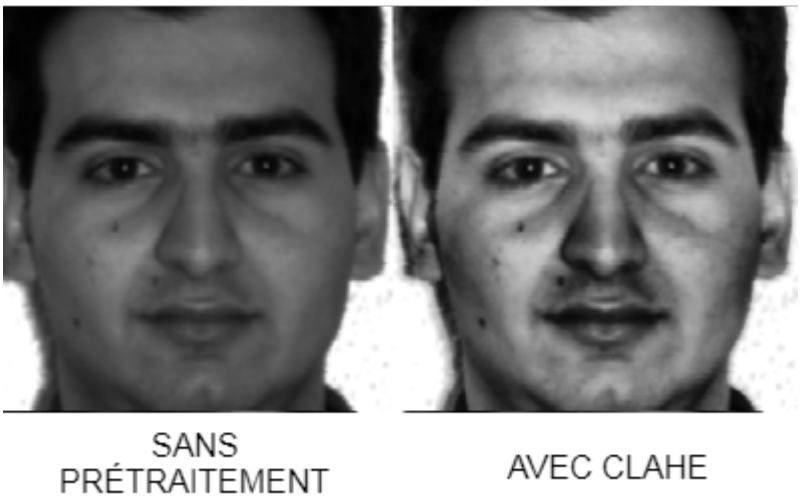


FIGURE 4.4 – Exemple de l'application d'égalisation d'histogramme CLAHE

La figure (4.4) présente deux exemples de l'effet d'application de l'égalisation d'histogramme CLAHE sur le premier individu. On peut remarquer un effet semblable à l'égalisation d'histogramme classique à une différence près. En effet, le problème de contraste élevé est moins présent dans ce cas-là.

Test sur l'algorithme PCA

Au sujet du test sur le paramètre de l'algorithme PCA, c'est un test sur le choix idéal de la valeur du nombre N qui correspond au nombre d'eigenfaces. Ces derniers permettent de déterminer la nouvelle représentation des images suite à la phase d'extraction de caractéristiques.

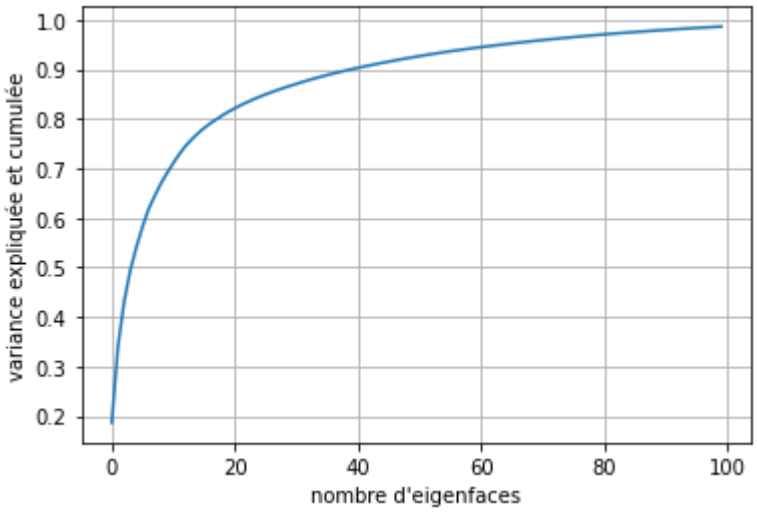


FIGURE 4.5 – Schéma représentatif des taux de variance selon le nombre d'eigenfaces

Le schéma de la figure (4.5) montre la relation entre le nombre N et la variance de l'ensemble des images. Ce dernier nous montre, selon les variances cumulées, que les informations et les changements les plus significatifs se situent dans l'intervalle $[5, 40]$. Ceci est dû au fait qu'une variance cumulée de 1.0 implique une représentation des images selon la totalité d'informations contenues à l'origine, incluant les moins utiles. Une variance cumulée près de 0.9 est donc une représentation assez suffisante des informations les plus intéressantes, ce qui explique la sélection de $N = 40$ comme borne maximale.

Test sur les métriques de distance

Au niveau de la phase de comparaison, s'effectue le test de la métrique de distance adéquate, euclidienne ou Manhattan. Ceci permet de voir l'influence sur les scores ainsi que la performance du sous-système.

Bien que tous les tests appliqués au sous-système interviennent dans des phases différentes, ceux-ci sont exécutés de manière synchronisée. Les résultats de l'ensemble des tests sont mis en évidence dans les tableaux (4.1) (4.2) (4.3) (4.4) (4.5) (4.6). Pour chaque distance, trois tableaux sont mis en avant, représentant respectivement les cas de : le non-prétraitement sur la luminosité, l'application de l'égalisation d'histogramme et l'application de l'égalisation d'histogramme CLAHE. Chaque tableau présente les performances du sous-système selon différentes valeurs de N, qui varient sur une échelle de 5 jusqu'à 40.

Distance euclidienne : Les tableaux (4.1) (4.2) (4.3) représentent les résultats relatifs à la distance euclidienne.

N	FRR	FAR	EER	Précision
5	0.1875	0.2857	0.2366	0.7667
10	0.1875	0.2143	0.2009	0.8000
15	0.1875	0.1429	0.1652	0.8334
20	0.1875	0.1429	0.1652	0.8334
25	0.1875	0.1429	0.1652	0.8334
30	0.1875	0.1429	0.1652	0.8334
35	0.1875	0.1429	0.1652	0.8334
40	0.1875	0.2143	0.2009	0.8000

TABLE 4.1 – Résultats des tests sans prétraitement sur la luminosité relatifs à la distance euclidienne

À partir du tableau (4.1), on note qu'un EER de 0.1652 et une précision de 0.8334 sont le meilleur résultat obtenu, dans le cas de non-prétraitement sur la luminosité. On atteint ce résultat à partir de $N = 15$, à l'exception du cas $N = 40$, où les performances ont diminué.

N	FRR	FAR	EER	Précision
5	0.1250	0.2857	0.2053	0.8000
10	0.1250	0.2143	0.1696	0.8334
15	0.1250	0.2143	0.1696	0.8334
20	0.1250	0.2143	0.1696	0.8334
25	0.1250	0.2143	0.1696	0.8334
30	0.1250	0.2143	0.1696	0.8334
35	0.1250	0.2143	0.1696	0.8334
40	0.1250	0.2143	0.1696	0.8334

TABLE 4.2 – Résultats des tests avec égalisation d'histogramme relatifs à la distance euclidienne

À partir du tableau (4.2), on note qu'un EER de 0.1696 et une précision de 0.8334 sont le meilleur résultat obtenu, dans le cas d'application de l'égalisation d'histogramme comme prétraitement sur la luminosité. On atteint ce résultat à partir de $N = 10$.

N	FRR	FAR	EER	Précision
5	0.1875	0.2857	0.2366	0.7667
10	0.1875	0.1429	0.1652	0.8334
15	0.1875	0.1429	0.1652	0.8334
20	0.1875	0.1429	0.1652	0.8334
25	0.1875	0.1429	0.1652	0.8334
30	0.1875	0.1429	0.1652	0.8334
35	0.1875	0.1429	0.1652	0.8334
40	0.1250	0.2143	0.1696	0.8334

TABLE 4.3 – Résultats des tests avec égalisation d'histogramme CLAHE relatifs à la distance euclidienne

À partir du tableau (4.3), on note qu'un EER de 0.1652 et une précision de 0.8334 sont le meilleur résultat obtenu, dans le cas de l'application de l'égalisation d'histogramme CLAHE comme prétraitement sur la luminosité. On atteint ce résultat à partir de $N = 10$, à l'exception du cas où $N = 40$, où les performances ont diminué selon le EER.

Distance Manhattan : Les tableaux (4.4) (4.5) (4.6) représentent les résultats relatifs à la distance Manhattan.

N	FRR	FAR	EER	Précision
5	0.1875	0.2143	0.2009	0.8000
10	0.1875	0.1429	0.1652	0.8334
15	0.1875	0.1429	0.1652	0.8334
20	0.1875	0.1429	0.1652	0.8334
25	0.1250	0.1429	0.1339	0.8667
30	0.1250	0.1429	0.1339	0.8667
35	0.1250	0.1429	0.1339	0.8667
40	0.1875	0.1429	0.1652	0.8334

TABLE 4.4 – Résultats des tests sans prétraitement sur la luminosité relatifs à la distance Manhattan

À partir du tableau (4.4), on note qu'un EER de 0.1339 et une précision de 0.8667 sont le meilleur résultat obtenu, dans le cas de non-prétraitement sur la luminosité. On atteint ce résultat lorsque N appartient à l'intervalle $[25, 35]$.

N	FRR	FAR	EER	Précision
5	0.1250	0.2857	0.2054	0.8000
10	0.1250	0.2143	0.1696	0.8334
15	0.1250	0.1429	0.1339	0.8667
20	0.1250	0.0714	0.0982	0.9000
25	0.1250	0.0000	0.0625	0.9333
30	0.1250	0.0000	0.0625	0.9333
35	0.0625	0.1429	0.1027	0.9000
40	0.0625	0.2143	0.1384	0.8667

TABLE 4.5 – Résultats des tests avec égalisation d'histogramme relatifs à la distance Manhattan

À partir du tableau (4.5), on note qu'un EER de 0.0625 et une précision de 0.9333 sont le meilleur résultat obtenu, dans le cas de l'application de l'égalisation d'histogramme comme prétraitement sur la luminosité. On atteint ce résultat à deux reprises, lorsque $N = 25$ et $N = 30$.

N	FRR	FAR	EER	Précision
5	0.1250	0.2857	0.2053	0.8000
10	0.1250	0.1429	0.1340	0.8667
15	0.1250	0.0714	0.0982	0.9000
20	0.1250	0.1429	0.1340	0.8667
25	0.1250	0.0714	0.0982	0.9000
30	0.1250	0.1429	0.1340	0.8667
35	0.1875	0.0714	0.1295	0.8667
40	0.1250	0.1429	0.1340	0.8667

TABLE 4.6 – Résultats des tests avec égalisation d'histogramme CLAHE relatifs à la distance Manhattan

À partir du tableau (4.6), on note qu'un EER de 0.0982 et une précision de 0.9 sont le meilleur résultat obtenu, dans le cas de l'application de l'égalisation d'histogramme CLAHE comme prétraitement sur la luminosité. On atteint ce résultat à deux reprises, lorsque $N = 15$ et $N = 25$.

À partir des résultats obtenus avec les deux métriques, nous pouvons constater que dans le cas d'utilisation de la métrique de distance euclidienne, le meilleur résultat est un EER de 0.1652 et une précision de 0.8334. Le choix optimal de configuration est un traitement avec égalisation d'histogramme CLAHE, car il permet d'atteindre les résultats voulus avec une valeur de N minimale (N=10), qui implique un coût plus optimal de mémoire et du temps dans l'implémentation.

Dans le cas d'utilisation de la métrique de distance Manhattan, on constate que le meilleur résultat est un EER de 0.0652 et une précision de 0.9333. Le choix optimal de configuration est un traitement avec égalisation d'histogramme classique et $N = 25$ dans PCA.

Donc, on peut déduire que la performance la plus élevée que le sous-système du visage peut atteindre et celle obtenue dans le cas d'utilisation de la métrique de distance Manhattan, avec un prétraitement d'égalisation d'histogramme classique et le nombre d'eigenfaces $N = 25$ pour l'algorithme PCA.

4.4.2 Résultats des tests sur le sous-système des signatures

Plusieurs prétraitements ont été essayés sur les deux caractéristiques des signatures : $x - coordinate$, et $y - coordinate$. Le premier test s'est fait sans prétraitement, tandis que les autres y sont respectivement appliqués une standardisation, une centralisation et une normalisation des échelles. Ceci, selon deux calculs des scores, l'un basé sur la soustraction et l'autre sur l'exponentielle.

Les effets de ces prétraitements sur l'échelle des distances sont mis en avant dans les graphes des figures (4.6), (4.7), (4.8) et (4.9) et les résultats des performances du système unimodal des signatures sont renseignés dans le tableau (4.7). Ces derniers incluent le taux de fausses acceptations, le taux de faux rejets, le taux d'égale erreur, et la précision.

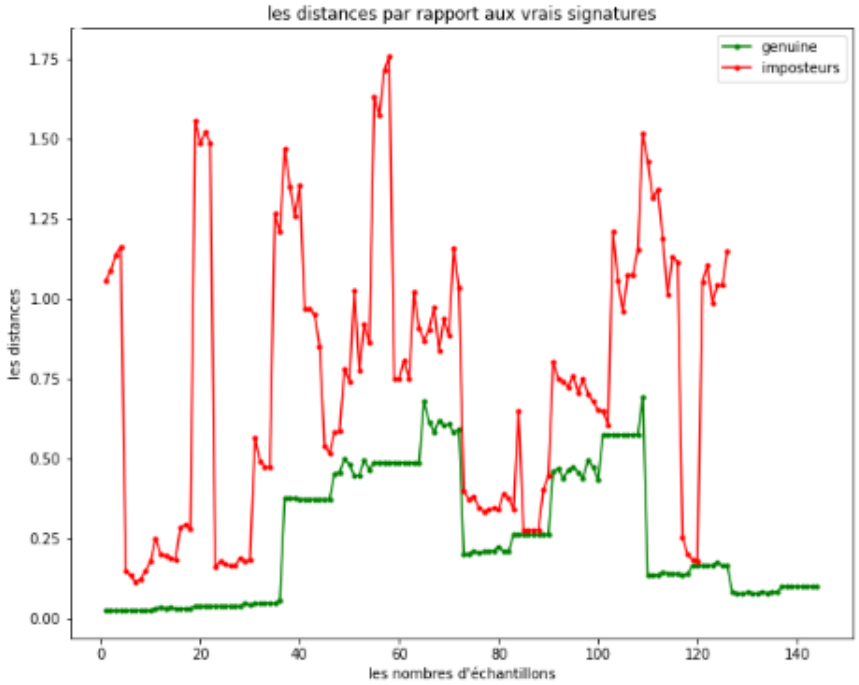


FIGURE 4.6 – Les distances dans le cas sans prétraitement

Dans le cas sans prétraitement montré dans la figure (4.6), les distances se situent sur une échelle assez grande qui se trouve réduite à la suite de la standardisation illustrée dans la figure (4.7).

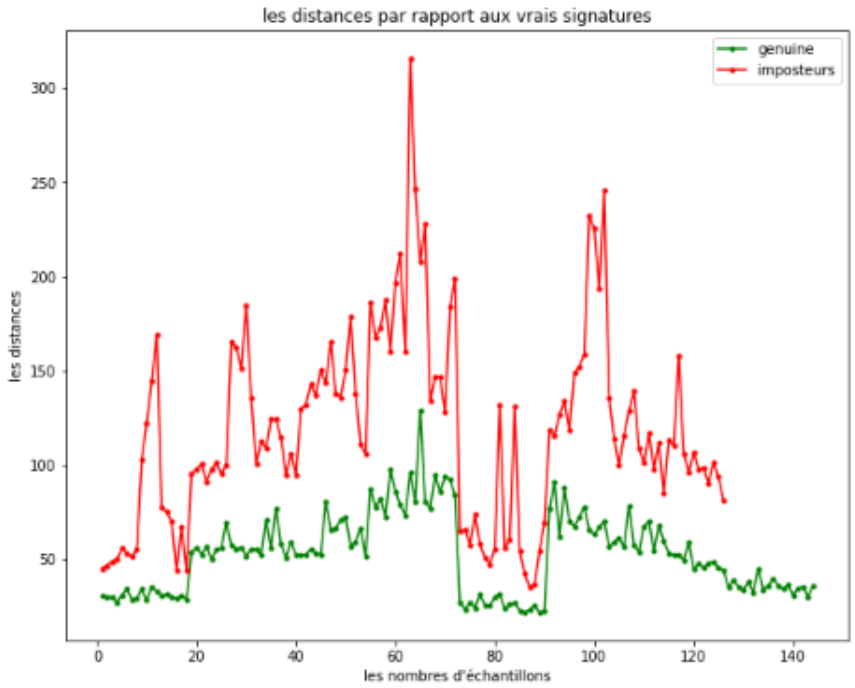


FIGURE 4.7 – Les distances dans le cas d'application d'une standardisation

La figure (4.8) met en avant les distances lorsqu'une centralisation des coordonnées x et y est appliquée. Elle cause un rapprochement entre les valeurs des échantillons vrais et imposteurs, ce qui peut nuire aux performances du système.

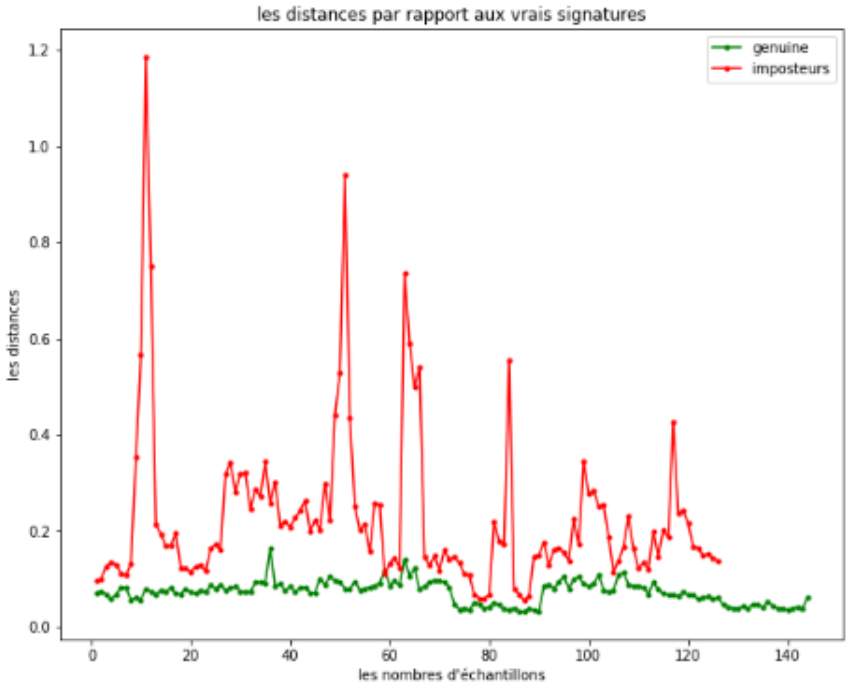


FIGURE 4.8 – Les distances dans le cas d'application d'une centralisation

La normalisation des échelles vers une échelle entre 0 et 1000, illustrés dans la figure (4.9), produit dans ce cas précis le même effet que la centralisation.

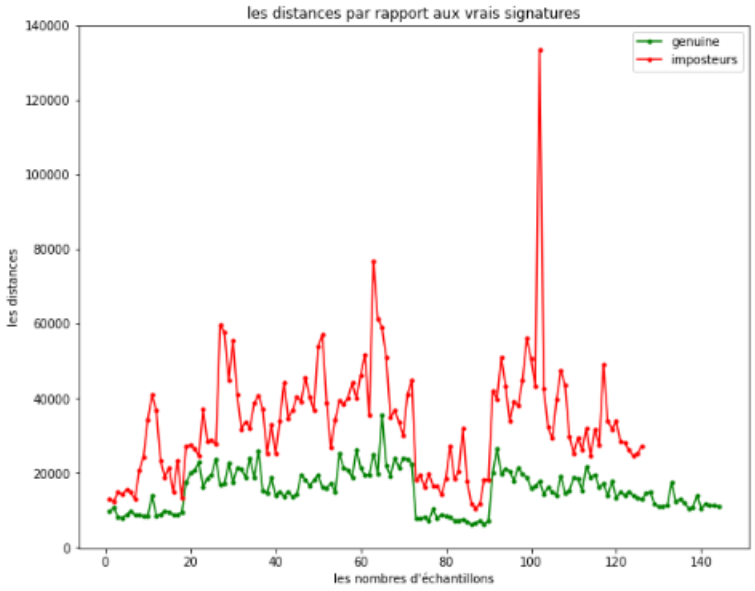


FIGURE 4.9 – Les distances dans le cas d'application d'une normalisation sur l'échelle $[0, 1000]$

Les résultats du tableau (4.7) renseignent les résultats des différents cas : sans prétraitement, standardisation, centralisation et normalisation.

Techniques de prétraitement	FAR	FRR	EER	Précision
Sans prétraitement	0.0000	0.3750	0.1875	0.8000
Standardisation	0.0000	0.3750	0.1850	0.8000
Centralisation	0.0000	0.7500	0.3750	0.6000
Normalisation	0.1400	0.3700	0.2500	0.7300

TABLE 4.7 – Résultats des tests de prétraitement sur le système des signatures

Le seuil choisi pour ce sous-système correspond au score permettant d'avoir un compromis entre le FAR et FRR, cela correspond à la valeur d'EER déduite de la figure (4.10).

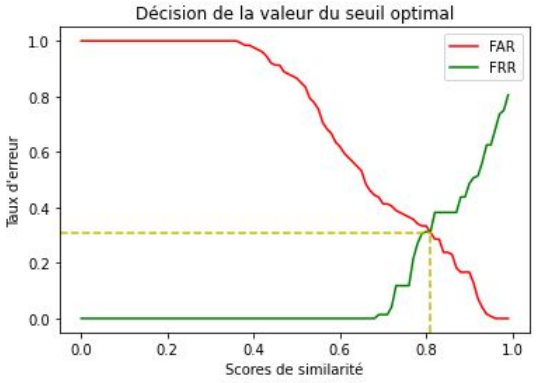
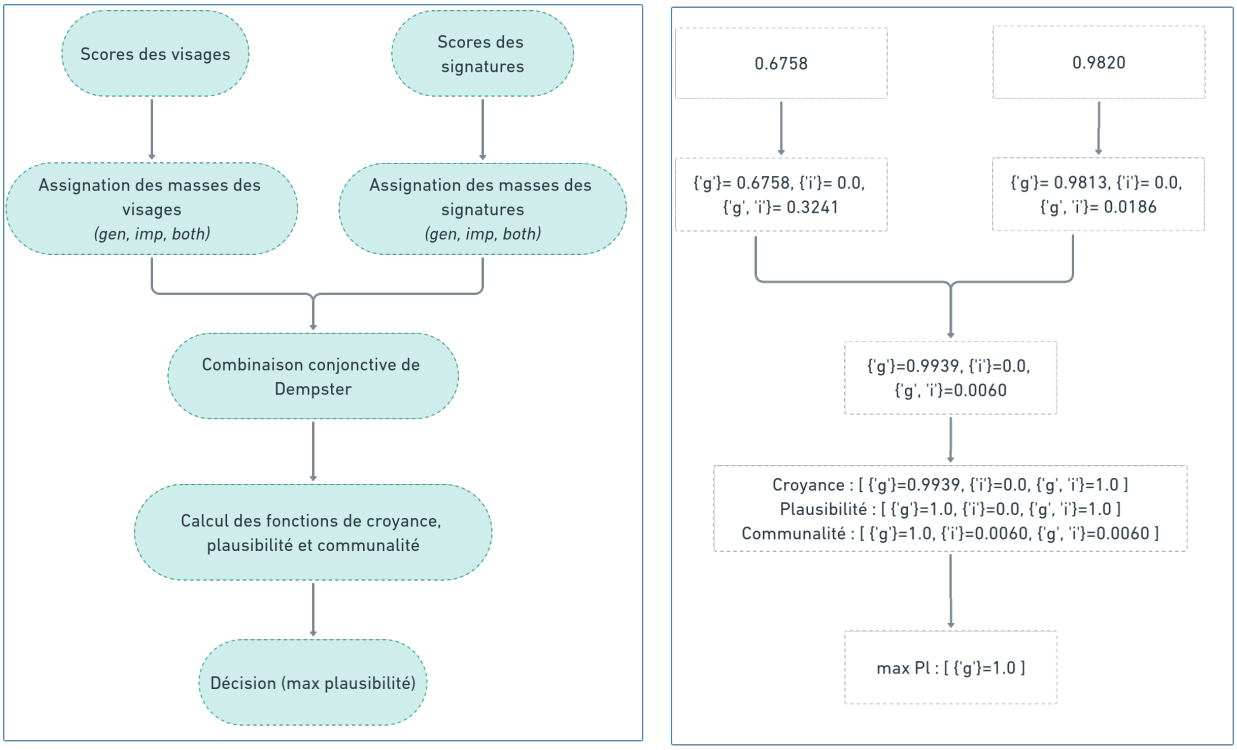


FIGURE 4.10 – Décision de la valeur du seuil optimal

En se basant sur ces résultats, nous en déduisons que le meilleur prétraitement pour le système des signatures dans notre cas précis correspond à une standardisation des coordonnées x et y. Toutefois, le cas sans prétraitement atteint les mêmes résultats que la standardisation. De ce fait, nous n'utilisons aucun prétraitement sur les données afin d'éviter des traitements inutiles.

4.4.3 Résultats des tests sur le système proposé

La fusion des scores résultants des deux systèmes unimodaux suit un ensemble d'étapes dans le cadre de la théorie de l'évidence illustrées dans l'organigramme de la figure (4.11). À titre explicatif, nous y donnons un exemple concret de la fusion des scores pour le sujet 3 censé être accepté.



Étapes de fusion basée sur DST

Exemple de la fusion pour le sujet n° 3

FIGURE 4.11 – Étapes de la fusion basée sur Dempster Shafer

Après la combinaison des masses de chacune des sources, des masses combinées des hypothèses gen, imp et $both$ (cas non classifié) en résulte.

La fonction de décision repose sur la comparaison d'un critère de décision. Plusieurs ont été essayés : maximum de croyance, maximum de plausibilité et maximum de communalité.

Après la décision, les trois résultats suivants ont été notés : authentifié, rejeté, et non classifié. Pour le calcul des performances, l'utilisation du taux d'égal erreur EER a été préféré à la précision. La précision correspond au nombre de vraies prédictions sur le total des requêtes clients. Étant donné que la classe $both$ (non classifié) n'est pas une prédiction correcte, mais est une meilleure prédiction que celle incorrecte, le calcul de précision est moins adapté dans notre cas, au risque d'une valeur négativement biaisée si l'on considère les non classifiés comme des fausses prédictions.

En plus du EER, les taux des sujets non classifiés sont renseignés dans le tableau (4.8). L'objectif étant d'avoir le moins de cas non classifiés possibles avec la valeur minimum de EER.

Critères de décision	EER	Taux des cas non classifiés
$maxPl$	0.031	20%
$maxBel$	0.0	$96,66\%$
$maxQ$	0.0625	0.0%

TABLE 4.8 – Résultats du système de fusion

Le choix du critère $maxQ$ permet de n'avoir aucun cas non classifié, toutefois, la valeur du EER est de $6,25\%$. Avec $maxBel$, la valeur de EER est nul, mais ce critère ne permet pas une prise de décision pour la plupart des sujets. Le critère de plausibilité permet d'atteindre un meilleur compromis entre le EER et le taux des cas non classifiés et est donc préférable en tant que critère de décision.

Le résultat du EER issus du calcul de plausibilité pour le système de fusion, est comparé avec les EER du système unimodal des signatures et celui des visages dans le tableau (4.9).

Critères de décision	EER
Système multimodal	0.0310
Système unimodal des signatures	0.1875
Système unimodal des visages	0.0625

TABLE 4.9 – Comparaison des EER des systèmes unimodaux et du système de multimodal

Les sous-systèmes de signatures et de visages possèdent respectivement des EER de $18,75\%$ et $6,25\%$. La fusion des deux systèmes permet d'atteindre un EER de $3,1\%$. Une valeur d'EER réduite indique un faible taux de fausses acceptations et de faux rejets. Cela implique un système d'authentification moins susceptible de commettre des erreurs telles que rejeter un utilisateur censé être authentifié ou bien accepter un imposteur.

4.5 Conclusion

Dans ce dernier chapitre, nous avons mis en avant les détails d'implémentation et de validation du système d'authentification biométrique multimodal proposé. Cela inclut des informations sur l'environnement ainsi que les outils d'implémentation en plus des résultats des différents tests pratiqués sur les systèmes multimodal et unimodaux. La comparaison des résultats de la fusion basée sur DST aux ceux des systèmes unimodaux a montré une amélioration des performances de l'authentification avec le système multimodal.

Conclusion générale

Cette étude a comme objectif la mise en œuvre d'un système d'authentification biométrique multimodal combinant les deux modalités visage et signature en ligne à l'aide de la théorie de Dempster-Shafer.

Tout d'abord, nous avons entamé ce travail en abordant des généralités sur la biométrie, les systèmes biométriques, la multimodalité, ainsi que les différentes techniques de fusion existantes. Nous avons vu que l'architecture globale d'un système biométrique est composée de plusieurs modules : module d'acquisition, de prétraitement, d'extraction des caractéristiques, de mise en correspondance, et module de décision. Nous avons également distingué deux types de systèmes : les systèmes unimodaux et les systèmes multimodaux.

Puisque les seconds systèmes sont plus performants que les premiers, nous avons établi un état de l'art critique sur le domaine de l'authentification biométrique multimodale. Nous avons constaté que les modalités visage et signature sont largement utilisées vu qu'elles sont accessibles par dispositifs banalisés. En outre, la théorie de Dempster-Shafer a également été employée pour combiner différentes modalités afin d'accroître les performances du système. Nous avons ainsi proposé un système d'authentification biométrique multimodal utilisant les deux modalités visage et signature en ligne basé la théorie de Dempster-Shafer.

Dans la mise en œuvre de notre système, plusieurs configurations ont été essayées dans les différentes phases du processus d'authentification, notamment, sur le prétraitement des données, les mesure de distances utilisées et les modes de prise de décision. Les résultats des tests expérimentaux sur des bases de données benchmarks ont prouvé que l'utilisation de la multimodalité à l'aide de DST améliore les performances d'authentification comparativement aux modalités visage et signature en ligne prisent séparément.

D'un point de vue critique, le nombre de sujets avec lequel le système a été testé est plutôt réduit. Une expérimentation avec d'autres bases de données est une bonne perspective afin d'améliorer les performances du système. D'autre part, le cas non classifié (l'ignorance) est non exploité dans l'état actuel de ce travail. Nous envisageons de remédier à ce problème d'ignorance par une autre modalité qui sera demandée par le système d'une manière interactive dans le but de confirmer l'identité de l'utilisateur.

Bibliographie

[1] University of north dakota libraries. https://libguides.und.edu/az.php, (Consulté le 03 septembre 2022).

[2] Biometrie - Empreintes digitales. https://www.biometrie-online.net/technologies/empreintes-digitales, (Consulté le 07 Janvier 2022).

[3] La biométrie : un nouveau moyen de sécuriser et rendre plus rapide nos paiements ? http://depgbcreteil.blogspot.com/2016/06/la-biometrie-un-nouveau-moyen-de.html, (Consulté le 07 Janvier 2022).

[4] Les systemes a reconnaissance d'iris invulnerables ? (partie 1). http://www.crime-expertise.org/les-systemes-a-reconnaissance-diris-invulnerables-partie-1-2/, (Consulté le 07 Janvier 2022).

[5] SVC 2004. https://cse.hkust.edu.hk/svc2004/download.html, (Consulté le 08 aout 2022).

[6] fastdtw. https://pypi.org/project/fastdtw/, (Consulté le 11 septembre 2022).

[7] Python library pyds. https://github.com/reineking/pyds, (Consulté le 11 septembre 2022).

[8] Choosing biometrics. https://www.ncsc.gov.uk/collection/biometrics/choosing-biometrics, (Consulté le 12 aout 2022).

[9] Chine : après la reconnaissance faciale, la reconnaissance de la démarche. https://www.bfmtv.com/tech/vie-numerique/chine-apres-la-reconnaissance-faciale-la-reconnaissance-de-la-demarche_AV-201811070060.html, (Consulté le 12 mars 2022).

[10] Expertise biometrique de signatures. https://criminalistique.fr/services/expertise-biometrique-signatures.html, (Consulté le 12 mars 2022).

[11] Fonctionnement de la reconnaissance faciale. https://sites.google.com/site/tpelabiometrie/home/biometrie-par-reconnaissance-faciale/fonctionnement-de-la-reconnaissance-faciale, (Consulté le 12 mars 2022).

[12] Lecteur biometrique veines du doigt zx-4000. http://www.zalix.fr/component/zalix/reseau-veineux/lecteur-biometrique-veines-du-doigt-zx-4000-fingervein-reseau-veineux-doigt,84.html, (Consulté le 12 mars 2022).

[13] Solution de paiement biométrique avec le réseau veineux de la main. https://technologie-innovation.fr/quixter-solution-de-paiement-biometrique-reseau-veineux, (Consulté le 12 mars 2022).

[14] Typical iris recognition system. https://www.researchgate.net/figure/Typical-iris-recognition-system_fig1_315472186, (Consulté le 12 mars 2022).

[15] Un clavier biométrique qui reconnaît son utilisateur. https://www.futura-sciences.com/tech/actualites/technologie-clavier-biometrique-reconnait-son-utilisateur-56927/, (Consulté le 12 mars 2022).

[16] What is colab ? https://colab.research.google.com/?utm_source=scs-index#scrollTo=5fCEDCU_qrC0, (Consulté le 12 septembre 2022).

[17] Les fonctions terminale. https://www.cmath.fr/0ter/fonctions/cours.php, (Consulté le 14 aout 2022).

[18] AR face database webpage. https://www2.ece.ohio-state.edu/~aleix/ARdatabase.html, (Consulté le 15 aout 2022).

[19] Classification : Accuracy. https://developers.google.com/machine-learning/crash-course/classification/accuracy, (Consulté le 15 aout 2022).

[20] FVC2002 - Second international fingerprint verification competition. http://bias.csr.unibo.it/fvc2002/databases.asp, (Consulté le 15 aout 2022).

[21] FVC2004 - Third international fingerprint verification competition. http://bias.csr.unibo.it/fvc2004/databases.asp, (Consulté le 15 aout 2022).

[22] OpenCV : Histogram equalization. https://docs.opencv.org/4.x/d5/daf/tutorial_py_histogram_equalization.html, (Consulté le 15 aout 2022).

[23] VERA FingerVein Database. https://www.idiap.ch:/en/dataset/vera-fingervein/index_html, (Consulté le 15 aout 2022).

[24] 9 distance measures in data science. https://towardsdatascience.com/9-distance-measures-in-data-science-918109d069fa, (Consulté le 17 aout 2022).

[25] Yale Face Database. http://vision.ucsd.edu/content/yale-face-database, (Consulté le 17 aout 2022).

[26] Biométrie. https://fr.wikipedia.org/w/index.php?title=Biom%C3%A9trie&oldid=190940702, (Consulté le 17 mars 2021).

[27] Systèmes biométriques. https://www.kimaldi.com/fr/produits/systemes_biometrique/, (Consulté le 19 mai 2022).

[28] General Python FAQ — Python 3.10.6 documentation. https://docs.python.org/3/faq/general.html#general-information, (Consulté le 20 aout 2022).

[29] Center for biometrics and security research. http://www.cbsr.ia.ac.cn/china/Iris%20Databases%20CH.asp, (Consulté le 22 aout 2022).

[30] Number of internet users worldwide 2021. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/, (Consulté le 24 mai 2022).

[31] FVC2006 - Fourth international fingerprint verification competition. http://bias.csr.unibo.it/fvc2006/, (Consulté le 25 aout 2022).

[32] The disadvantages and problems with passwords. https://www.iproov.com/blog/forgotten-passwords-increasing-websites-abandonment-rate, (Consulté le 25 mai 2022).

[33] Eigenface. https://en.wikipedia.org/wiki/Eigenface#/media/File:Eigenfaces.png, (Consulté le 25 mai 2022).

[34] La biométrie au service de l'identification et l'authentification. https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie, (Consulté le 26 décembre 2021).

[35] Le marché de la biométrie. https://www.biometrie-online.net/biometrie/le-marche, (Consulté le 26 décembre 2021).

[36] Test de fiabilité des systèmes biométriques. https://www.aware.com/quest-ce-que-la-biometrie/test-de-fiabilite-des-systemes-biometriques/, (Consulté le 26 décembre 2021).

[37] Filtre canny. http://www.optique-ingenieur.org/fr/cours/pdf/OPI_fr_M04_C05.pdf, (Consulté le 29 mai 2022).

[38] OpenCV : Face detection using Haar Cascades. https://docs.opencv.org/4.x/d2/d99/tutorial_js_face_detection.html, (Consulté le 29 mai 2022).

[39] Rouge, vert, bleu. https://fr.wikipedia.org/w/index.php?title=Rouge_vert_bleu&oldid=189591179, (Consulté le 29 mai 2022).

[40] What are convolutional neural networks ? https://www.ibm.com/cloud/learn/convolutional-neural-networks, (Consulté le 29 mai 2022).

[41] Convolutional neural network. https://www.mathworks.com/help/deeplearning/ref/googlenet.html;jsessionid=3ffd90d2935eb5dbf5308b36f6cb, (Consulté le 30 mai 2022).

[42] Convolutional neural network. https://www.mathworks.com/help/deeplearning/ref/resnet18.html#mw_591a2746-7267-4890-8390-87ae4dc7204c_sep_mw_6dc28e13-2f10-44a4-9632-9b8d43b376fe, (Consulté le 30 mai 2022).

[43] Convolutional neural network - Matlab. https://www.mathworks.com/help/deeplearning/ref/squeezenet.html, Consulté le 30 mai 2022).

[44] The database of faces. https://cam-orl.co.uk/facedatabase.html, (Consulté le 30 mai 2022).

[45] Filtre median. https://www.mathworks.com/help/deeplearnin, Consulté le 30 mai 2022).

[46] M FOULLOY Laurent Professeur à PolyTech. *Fonctions de croyance : de la théorie à la pratique*. PhD thesis, Université d'Artois, 2012.

[47] Sofiane Mazaa Abdelouahab Attia, Zahid Akhtar, and Youssef Chahir. Deep learning-driven palmprint and finger knuckle pattern-based multimodal person recognition system. 81(8) :10961–10980, 2022.

[48] Rohit Agarwal. A review on fusion in multimodal biometric spoofing attack by different materials. In *IOP Conference Series : Materials Science and Engineering*, volume 1116, page 012089. IOP Publishing, 2021.

[49] Shadab Ahmad, Rajarshi Pal, and Avatharam Ganivada. Rank level fusion of multimodal biometrics based on cross-entropy monte carlo method. In *International Symposium on Signal Processing and Intelligent Recognition Systems*, pages 64–74. Springer, 2019.

[50] Hadjar Ahmed. *Identification des individus par la biométrie multimodale*. Mémoire de magister, Université Des Sciences Et De La Technologie D'Oran Mohamed Boudiaf, Nouvembre 2014.

[51] Timo Ahonen, Abdenour Hadid, and Matti Pietikainen. Face description with local binary patterns : Application to face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 28(12) :2037–2041, 2006.

[52] Kamel Aizi and Mohamed Ouslim. Score level fusion in multi-biometric identification based on zones of interest. *Journal of King Saud University - Computer and Information Sciences*, 34(1) :1498–1509, 2022.

[53] Alaa S Al-Waisy, Rami Qahwaji, Stanley Ipson, Shumoos Al-Fahdawi, and Tarek AM Nagem. A multi-biometric iris recognition system based on a deep learning approach. *Pattern Analysis and Applications*, 21(3) :783–802, 2018.

[54] Nada Alay and Heyam H Al-Baity. Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors*, 20(19) :5523, 2020.

[55] Boucetta Aldjia and Boussaad Leila. Sensor level fusion for multi-modal biometric identification using deep learning. In *2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI)*, pages 1–5. IEEE, 2021.

[56] Fernando Alonso-Fernandez, Julian Fierrez-Aguilar, Francisco del Valle, and Javier Ortega-Garcia. On-line signature verification using tablet pc. In *ISPA 2005. Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, 2005.*, pages 245–250. IEEE, 2005.

[57] BV Anil and MS Ravikumar. Biometric recognition from face-voice using rough-neuro-fuzzy classifiers. In *High Performance Computing and Networking*, pages 489–501. Springer, 2022.

[58] Satish Anila and Nanjundappan Devarajan. Preprocessing technique for face recognition applications under varying illumination conditions. *Global Journal of Computer Science and Technology*, 2012.

[59] Abdul Quaiyum Ansari, Madasu Hanmandlu, Jaspreet Kour, and Abhineet Kumar Singh. Online signature verification using segment-level fuzzy modelling. *IET biometrics*, 3(3) :113–127, 2014.

[60] Monica Micucci Antonio Iula. Multimodal biometric recognition based on 3d ultrasound palmprint-hand geometry fusion. *IEEE Access*, 10 :7914–7925, 2022.

[61] Abdelouahab Attia, Sofiane Mazaa, Zahid Akhtar, and Youssef Chahir. Deep learning-driven palmprint and finger knuckle pattern-based multimodal person recognition system. *Multimedia Tools and Applications*, 81(8) :10961–10980, 2022.

[62] M Azriansyah, N Hartuti, Muhammad Fachrurrozi, Bayu Adhi Tama, et al. A study about principle component analysis and eigenface for facial extraction. In *Journal of Physics : Conference Series*, volume 1196, page 012010. IOP Publishing, 2019.

[63] Nawaf Hazim Barnouti. Face recognition using pca-bpnn with dct implemented on face94 and grimace databases. *International Journal of Computer Applications*, 142(6) :8–13, 2016.

[64] Mébarka Belahcen. *Authentification et Identification en Biométrie*. Thèse de doctorat, Université Mohamed Khider Biskra, 2013.

[65] Maïtine Bergounioux. Quelques méthodes de filtrage en traitement d'image. August 2010.

[66] Attallah bilal. *Conception d'un système de reconnaissance des empreintes digitales par apprentissage*. Mémoire de magister, Université Des Sciences Et De La Technologie D'Oran Mohammed Boudiaf, 2012.

[67] Boukerram. Cours N° 2 : Vision par ordinateur. https://elearning.univ-bejaia.dz/enrol/index.php?id=12942, (Consulté le 25 mai 2022).

[68] Boussad Faouzi Boussa Rahim Ryad. *Développement d'un système biométrique multimodal basé sur la fusion des scores de matching*. Mémoire de master, Université Mouloud Mammeri De Tizi Ouzou, 2019-2020.

[69] Ralf-Dieter Bousseljot. Ptb diagnostic ecg database. https://www.physionet.org/content/ptbdb/1.0.0/, (Consulté le 23 aout 2022).

[70] Guillermo Calvo, Bruno Baruque, and Emilio Corchado. Study of the pre-processing impact in a facial recognition system. In *International Conference on Hybrid Artificial Intelligence Systems*, pages 334–344. Springer, 2013.

[71] J. Campos, F.L. Lewis, L. Davis, and S. Ikenaga. Backstepping based fuzzy logic control of active vehicle suspension systems. In *Proceedings of the 2000 American Control Conference. ACC (IEEE Cat. No.00CH36334)*, volume 6, pages 4030–4035 vol.6, 2000.

[72] Dulal Chakraborty, Sanjit Kumar Saha, and Md Al-Amin Bhuiyan. Face recognition using eigenvector and principle component analysis. *International Journal of Computer Applications*, 50(10), 2012.

[73] Tsung-Han Chan, Kui Jia, Shenghua Gao, Jiwen Lu, Zinan Zeng, and Yi Ma. Pcanet : A simple deep learning baseline for image classification ? *IEEE transactions on image processing*, 24(12) :5017–5032, 2015.

[74] Arjun Benagatte Channegowda and Hebbakavadi Nanjundaiah Prakash. Image fusion by discrete wavelet transform for multimodal biometric recognition. *IAES International Journal of Artificial Intelligence*, 11(1) :229, 2022.

[75] Samer Chantaf. *Biométrie par signaux physiologiques*. PhD thesis, Université Paris-Est, 2011.

[76] Mouna Chebbah, Arnaud Martin, and Boutheina Ben Yaghlane. Estimation de la fiabilité des sources des bases de données évidentielles. *Revue des Nouvelles Technologies de l'Information*, (21) :191–208, 2011.

[77] Gong Cheng and Junwei Han. A survey on object detection in optical remote sensing images. *ISPRS Journal of Photogrammetry and Remote Sensing*, 117 :11–28, 2016.

[78] NFB Contributors. Nfbs skull-stripped sepository. http://preprocessed-connectomes-project.org/NFB_skullstripped/, (Consulté le 22 aout 2022).

[79] Hugo Plácido da Silva; André Lourenço; Ana Fred; Nuno Raposo; Marta Aires-de Sousa. Check your biosignals here initiative (cybhi) dataset for off-the-person electrocardiography (ecg) biometrics. https://zenodo.org/record/2381823#.YwTUoMLP1hE, (Consulté le 23 aout 2022).

[80] Naser Damer, Alexander Opel, and Alexander Nouak. Biometric source weighting in multi-biometric fusion : Towards a generalized and robust solution. In *2014 22nd European Signal Processing Conference (EUSIPCO)*, pages 1382–1386, 2014.

[81] Arianna D'Ulizia. Exploring multimodal input fusion strategies. In *Multimodal Human Computer Interaction and Pervasive Services*, pages 34–57. IGI Global, 2009.

[82] Mohamad El-Abed. *Évaluation de système biométrique*. Thèse de doctorat, Université de Caen Basse-Normandie, décembre 2011.

[83] Hassane Bouzahir El mehdi Cherrat, Rachid Alaoui. A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images. *Indonesian Journal of Electrical Engineering and Computer Science*, 17 :1562, 2020.

[84] Rachid Alaoui El mehdi Cherrat and Hassane Bouzahir. A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images. *Indonesian Journal of Electrical Engineering and Computer Science*, 18(1) :1562–1570, 2020.

[85] Khaled Mahdadi El-Moundher Hadjaidji. *Modélisation d'empreinte biométrique par un modèle flou de Sugeno optimisé*. Mémoire de master, Université Kasdi Merbah-Ouargla, Mai 2017.

[86] Bouttllaa Elhocine. *Système biométrique de vérification de signatures manuscrites en ligne*. Mémoire de magister, Ecole nationale Supérieure d'Informatique (E.S.I), March 2019.

[87] Ahmed A. Alani Emad Majeed Hameed, Noor Abbood. Fuzzy logic decision fusion in a fingerprints based nultimodal biometric system. *Journal of Engineering and Applied Sciences*, 14 :920–926, 2019.

[88] Luis Alvarez et Luis Mazorra. Esther Gonzalez. Ami ear database. `https://ctim.ulpgc.es/research_works/ami_ear_database/`, (Consulté le 23 aout 2022).

[89] Professor Tieniu Tan et Dr. Zhenan Sun. Casia-irisv4. `http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp`, (Consulté le 22 aout 2022).

[90] Mohsen Fayyaz, Mohammad Hajizadeh_Saffar, Mohammad Sabokrou, and Mahmood Fathy. Feature representation for online signature verification. *arXiv preprint arXiv :1505.08153*, 2015.

[91] Gianni Fenu and Mirko Marras. Demographic fairness in multimodal biometrics : A comparative analysis on audio-visual speaker recognition systems. *Procedia Computer Science*, 198 :249–254, 2022.

[92] Dariusz Frejlichowski and Natalia Tyszkiewicz. The west pomeranian university of technology ear database – a tool for testing biometric algorithms. In Aurélio Campilho and Mohamed Kamel, editors, *Image Analysis and Recognition*, pages 227–234, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[93] Nicolas Galy. *Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage*. PhD thesis, Institut National Polytechnique de Grenoble-INPG, 2005.

[94] Charles J Geyer. 5601 notes : The subsampling bootstrap. *Unpublished manuscript*, 2006.

[95] K Gunasekaran, J Raja, and R Pitchai. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. *Automatika : časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, 60(3) :253–265, 2019.

[96] Mohamed Hammad, Yashu Liu, and Kuanquan Wang. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ecg and fingerprint. *IEEE Access*, 7 :26527–26542, 2018.

[97] Boukada Yassine ; Bemmoussat Mohammed Hamza. *reconnaissance vocale*. Thèse de doctorat, Université Abou Bekr Belkaid De Tlemcen, 2017-2018.

[98] M Hassaballah and Saleh Aly. Face recognition : challenges, achievements and future directions. *IET Computer Vision*, 9(4) :614–626, 2015.

[99] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. Technical Report arXiv :1512.03385, arXiv, December 2015. arXiv :1512.03385 [cs] type : article.

[100] Nefissa Khiari Hili. *Biométrie multimodale basée sur l'iris et le visage*. Thèse de doctorat, Université Paris-Saclay ; Université de Tunis El Manar, mai 2016.

[101] Laura Holsopple. Livdet databases. `https://livdet.org/registration.php`, (Consulté le 23 aout 2022).

[102] Fatma Horo, Mohammed DEMRI, et al. *Sélection d'un modèle SVM pour la fusion des modalités biométriques*. PhD thesis, universite Ahmed Draia-ADRAR, 2019.

[103] Quan Huang. Multimodal biometrics fusion algorithm using deep reinforcement learning. *Mathematical Problems in Engineering*, 2022, 2022.

[104] Forrest N. Iandola, Song Han, Matthew W. Moskewicz, Khalid Ashraf, William J. Dally, and Kurt Keutzer. SqueezeNet : AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size. Technical Report arXiv :1602.07360, arXiv, November 2016. arXiv :1602.07360 [cs] type : article.

[105] Antonio Iula and Monica Micucci. Multimodal biometric recognition based on 3d ultrasound palmprint-hand geometry fusion. *IEEE Access*, 10 :7914–7925, 2022.

[106] Antonio Iula and Monica Micucci. Multimodal biometric recognition based on 3d ultrasound palmprint-hand geometry fusion. *IEEE Access*, 10 :7914–7925, 2022.

[107] Tansin Jahan, Md Shahriar Anwar, and SM Abdullah Al-Mamun. A study on preprocessing and feature extraction in offline handwritten signatures. *Global Journal of Computer Science and Technology*, 2015.

[108] Rami M Jomaa, Md Saiful Islam, Hassan Mathkour, and Saad Al-Ahmadi. A multilayer system to boost the robustness of fingerprint authentication against presentation attacks by fusion with heart-signal. *Journal of King Saud University-Computer and Information Sciences*, 2022.

[109] Waziha Kabir, M Omair Ahmad, and MNS Swamy. Weighted hybrid fusion for multimodal biometric recognition system. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–4. IEEE, 2018.

[110] Christos Kalloniatis and Carlos Travieso-Gonzalez. *Security and Privacy From a Legal, Ethical, and Technical Perspective*. BoD–Books on Demand, 2020.

[111] Mohamed Ouslim Kamel Aizi. Score level fusion in multi-biometric identification based on zones of interest. *Journal of King Saud University - Computer and Information Sciences*, 34(1) :1498–1509, 2022.

[112] Herman Kamper. Dynamic time warping : Algorithm. `https://www.youtube.com/watch?v=9GdbMc4CEhE`, (Consulté le 13 aout 2022).

[113] Christopher Kanan and Garrison W Cottrell. Color-to-grayscale : does the method matter in image recognition ? *PloS one*, 7(1) :e29740, 2012.

[114] G Kaur, S Bhushan, and D Singh. Fusion in multimodal biometric system : A review. *Indian Journal of Science and Technology*, 10(28) :1–10, 2017.

[115] Zhandos Kegenbekov and Ilya Jackson. Adaptive supply chain : Demand–supply synchronization using deep reinforcement learning. *Algorithms*, 14 :240, 08 2021.

[116] Redouane Khemmar, Fabien Bonardi, Jean-Yves Ertaud, and Xavier Savatier. Biometric authentication platform-based multisensor fusion. *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017.

[117] Wan Kim, Jong Min Song, and Kang Ryoung Park. Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (nir) camera sensor. *Sensors*, 18(7) :2296, 2018.

[118] Slavko Kovacevic, Vuko Djaletic, and Jelena Vukovic. Face recognition using compressive sensing. Technical Report arXiv :1902.05388, arXiv, February 2019. arXiv :1902.05388 [cs] type : article.

[119] Ajay Kumar. Iit delhi touchless palmprint database. `https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm`, (Consulté le 23 aout 2022).

[120] Pradeep Kumar, Rajkumar Saini, Barjinder Kaur, Partha Pratim Roy, and Erik Scheme. Fusion of neuro-signals and dynamic signatures for person authentication. *Sensors*, 19(21) :4641, 2019.

[121] The Biometrics Research Laboratory. Iit delhi iris database. https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm, (Consulté le 22 aout 2022).

[122] Nouar Larbi. *Identification Biométrique Par Fusion Multimodale*. Thèse de doctorat, Université Djillali Liabes De Sidi Bel Abbes, 2017-2018.

[123] lbali. Databases. = https ://www.lib.polyu.edu.hk/databases, September 2014.

[124] Mehwish Leghari, Shahzad Memon, Lachhman Das Dhomeja, Akhtar Hussain Jalbani, and Asghar Ali Chandio. Deep feature fusion of fingerprint and online signature for multimodal biometrics. *Computers*, 10(2) :21, 2021.

[125] HanSheng Lei and Venu Govindaraju SrinivaSPala. Er : An intuitive similarity measurefor on-line signature verification. *Mih Interndional Morkshop on FronrS in Handwring Recogrion (TKPHIRO4), October2004pp*, pages 191–195.

[126] Daniel PF Lopes and António JR Neves. A study on face identification for an outdoor identity verification system. In *European Congress on Computational Methods in Applied Sciences and Engineering*, pages 689–699. Springer, 2017.

[127] Arnaud Martin. La fusion d'informations. *Polycopié de cours ENSIETA-Réf*, 1484 :117, 2005.

[128] Marcos Martinez-Diaz, Julian Fierrez, Ram P Krish, and Javier Galbally. Mobile signature verification : Feature robustness and performance comparison. *IET Biometrics*, 3(4) :267–277, 2014.

[129] L. Mezai, F. Hachouf, and M. Bengherabi. Score fusion of face and voice using dempster-shafer theory for person authentication. In *2011 11th International Conference on Intelligent Systems Design and Applications*, pages 894–899, 2011.

[130] Md Maruf Monwar and Marina L Gavrilova. Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 39(4) :867–878, 2009.

[131] Daigo Muramatsu, Kumiko Yasuda, and Takashi Matsumoto. Biometric person authentication method using camera-based online signature acquisition. In *2009 10th International Conference on Document Analysis and Recognition*, pages 46–50. IEEE, 2009.

[132] Karthik Nandakumar, Yi Chen, Sarat C Dass, and Anil Jain. Likelihood ratio-based biometric score fusion. *IEEE transactions on pattern analysis and machine intelligence*, 30(2) :342–347, 2007.

[133] Kien Nguyen, Simon Denman, Sridha Sridharan, and Clinton Fookes. Score-level multibiometric fusion based on dempster–shafer theory incorporating uncertainty factors. *IEEE Transactions on Human-Machine Systems*, 45(1) :132–140, 2015.

[134] Institute of Automation chinese Academy of Sciences. Note on casia palmprint database. http://www.cbsr.ia.ac.cn/english/Palmprint%20Databases.asp, (Consulté le 23 aout 2022).

[135] BioLab University of Bologna. Fvc2002 databases. http://bias.csr.unibo.it/fvc2002/databases.asp, (Consulté le 23 aout 2022).

[136] Biometric System Lab University of Bologna. Fvc2004. http://bias.csr.unibo.it/fvc2004/download.asp, (Consulté le 23 aout 2022).

[137] Information Technology Laboratory of NIST. Face recognition technology (feret) database. https://www.nist.gov/programs-projects/face-recognition-technology-feret, (Consulté le 23 aout 2022).

[138] Chinese Academy of Sciences(CASIA). Casia biometric ideal. http://biometrics.idealtest.org/#/, (Consulté le 22 aout 2022).

[139] Information Technology Laboratory of the United States. Nist biometric scores set (bssr1). https://www.nist.gov/itl/iad/image-group/nist-biometric-scores-set-bssr1, (Consulté le 22 aout 2022).

[140] Bayan Omar, Hamsa D Majeed, Siti Zaiton Mohd Hashim, and Muzhir Al-Ani. New feature-level algorithm for a face-fingerprint integral multi-biometrics identification system. *UHD Journal of Science and Technology*, 6(1) :12–20, 2022.

[141] Pawan Patidar, Manoj Gupta, Sumit Srivastava, and Ashok Kumar Nagawat. Image denoising by various filters for different noise. *International journal of computer applications*, 9(4) :45–50, 2010.

[142] S Patro and Kishore Kumar Sahu. Normalization : A preprocessing stage. *arXiv preprint arXiv :1503.06462*, 2015.

[143] Yusuf Perwej. The bidirectional long-short-term memory neural network based word retrieval for arabic documents. *Transactions on Machine Learning and Artificial Intelligence*, 3(1) :16–27, 2015.

[144] Arkadiusz Pień and Marcin Adamski. Preprocessing techniques for online signature verification and identification. *Advances in Computer Science Research*, 2018.

[145] Rajkumar Saini Pradeep Kumar, Barjinder Kaur, Partha Pratim Roy, and Erik Scheme. Fusion of neuro-signals and dynamic signatures for person authentication. 19 :4641, 2019.

[146] Rajkumar Saini Pradeep Kumar, Barjinder Kaur, Partha Pratim Roy, and Erik Scheme. Multimodal biometric system fusion using fingerprint and face with fuzzy logic. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7 :482–489, 2019.

[147] Prachi Punyani, Rashmi Gupta, and Ashwani Kumar. A multimodal biometric system using match score and decision level fusion. *International Journal of Information Technology*, 14(2) :725–730, 2022.

[148] Siti Rahayu Selamat, Teh Teck Guan, and Robiah Yusof. Enhanced authentication for web-based security using keystroke dynamics. *International Journal of Network Security & Its Applications*, 12(4) :1–16, July 2020.

[149] Vani Rajasekar, Bratislav Predić, Muzafer Saracevic, Mohamed Elhoseny, Darjan Karabasevic, Dragisa Stanujkic, and Premalatha Jayapaul. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. *Scientific Reports*, 12(1) :1–11, 2022.

[150] G Ranganathan and A Rocha. *Inventive Communication and Computational Technologies*. PhD thesis, Springer, 2021.

[151] Nada Abdullah Rasheed. Proposed preprocessing algorithm for signatures recognition. In *Issue/special magazine College of Education Basic/University of Babylon, Fourth Scientific Conference of the Faculty of Education, basic/Babylon University*, volume 222. Citeseer, 2010.

[152] Meryem Regouid, Mohamed Touahria, Mohamed Benouis, and Nicholas Costen. Multimodal biometric system for ecg, ear and iris recognition based on local descriptors. *Multimedia Tools and Applications*, 78(16) :22509–22535, 2019.

[153] Adrian Rosebrock. Softmax classifiers explained. `https://pyimagesearch.com/2016/09/12/softmax-classifiers-explained//`, (Consulté le 22 aout 2022).

[154] Arun Ross and Karthik Nandakumar. Fusion, score-level. In Stan Z. Li and Anil Jain, editors, *Encyclopedia of Biometrics*, pages 611–616. Springer US, Boston, MA, 2009.

[155] Mohammad Majed Ahmad Saleem. Improved preprocessing and classification algorithms for online signature verification. 2021.

[156] Stan Salvador and Philip Chan. Toward accurate dynamic time warping in linear time and space. *Intelligent Data Analysis*, 11(5) :561–580, 2007.

[157] Akrouf Samir. *Une Approche Multimodale pour l'Identification du Locuteur*. Mémoire de doctorat, Université Ferhat Abbas-Setif, juillet 2011.

[158] Partha Pratim Sarangi, Deepak Ranjan Nayak, Madhumita Panda, and Banshidhar Majhi. A feature-level fusion based improved multimodal biometric recognition system using ear and profile face. *Journal of Ambient Intelligence and Humanized Computing*, 13(4) :1867–1898, 2022.

[159] Ben Schoon. Google's password autofill can now use biometric authentication on Android. `https://9to5google.com/2020/08/20/google-autofill-biometric-android-passwords/`, (Consulté le 12 aout 2022).

[160] Thomas Seidl. Nearest neighbor classification. In LING LIU and M. TAMER ÖZSU, editors, *Encyclopedia of Database Systems*, pages 1885–1890. Springer US, Boston, MA, 2009.

[161] Kari Sentz and Scott Ferson. Combination of evidence in dempster-shafer theory. 2002.

[162] Kashif Shaheed, Aihua Mao, Imran Qureshi, Munish Kumar, Qaisar Abbas, Inam Ullah, and Xingming Zhang. A systematic review on physiological-based biometric recognition systems : Current and future trends. *Archives of Computational Methods in Engineering*, 28(7) :4917–4960, 2021.

[163] Poonam Sharma and Kulvinder Singh. Multimodal biometric system fusion using fingerprint and face with fuzzy logic. *International Journal*, 7(5), 2017.

[164] Florentin Smarandache and Jean Dezert. Four versions of the proportional conflict redistribution rules of combination in information fusion. *Information Fusion*, 41(3) :386–395, 2004.

[165] Piotr Szczuko, Arkadiusz Harasimiuk, and Andrzej Czyżewski. Evaluation of decision fusion methods for multimodal biometrics in the banking application. *Sensors*, 22(6) :2356, 2022.

[166] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. Going deeper with convolutions. Technical Report arXiv :1409.4842, arXiv, 2014. arXiv :1409.4842 [cs] type : article.

[167] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jonathon Shlens, and Zbigniew Wojna. Rethinking the inception architecture for computer vision. Technical Report arXiv :1512.00567, arXiv, December 2015. arXiv :1512.00567 [cs] version : 3 type : article.

[168] Ava Tahmasebi and Hossein Pourghassem. Robust intra-class distance-based approach for multimodal biometric game theory-based rank-level fusion of ear, palmprint and signature. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 41(1) :51–64, 2017.

[169] Magdalena Tomaszewska-Michalak. Biometric technology 20 years after 9/11– opportunities and threats. *Studia Politologiczne*, 63, 2022.

[170] Hafs Toufik. *Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne*. Mémoire de doctorat, Université Badji Mokhtar Annaba, 2016.

[171] Matthew A Turk and Alex P Pentland. Face recognition using eigenfaces. In *Proceedings. 1991 IEEE computer society conference on computer vision and pattern recognition*, pages 586–587. IEEE Computer Society, 1991.

[172] M üge Çarıkçı and Figen Özen. A face recognition system based on eigenfaces method. *Procedia Technology*, 1 :118–123, 2012.

[173] Shandong University. Sdumla-hmt database. `https://time.sdu.edu.cn/kycg/gksjk.htm`, (Consulté le 22 aout 2022).

[174] K . Sandhyarani V. Sireesha. Overview of fusion techniques in multimodal biometrics. *International Journal of Engineering Research & Technology (IJERT)*, pages 25–31, 2014.

[175] Thierry Vaira. Traitement d'images matricielles en Python. page 28.

[176] HS Fadewar Waleed Dahea. Multimodal biometric system : A review. *International Journal of Research in Advanced Engineering and Technology*, 4(1) :25–31, January 2018.

[177] Gurjit Singh Walia, Tarandeep Singh, Kuldeep Singh, and Neelam Verma. Robust multimodal biometric system based on optimal score level fusion model. *Expert Systems with Applications*, 116 :364–376, 2019.

[178] James L Wayman, Anil K Jain, Davide Maltoni, and Dario Maio. *Biometric systems : Technology, design and performance evaluation*. Springer Science & Business Media, 2005.

[179] Qinghan Xiao. Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Computational Intelligence Magazine*, 2(2) :5–25, 2007.

[180] Mohammad E Yahyatabar and Jamal Ghasemi. Online signature verification using double-stage feature extraction modelled by dynamic feature stability experiment. *IET Biometrics*, 6(6) :393–401, 2017.

[181] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. Svc2004 : First international signature verification competition. In *International conference on biometric authentication*, pages 16–22. Springer, 2004.

[182] Jeremy Zhang. Dynamic Time Warping. explanation and code implementation. `https://towardsdatascience.com/dynamic-time-warping-3933f25fcdd?gi=279e33edef75`, (Consulté le 13 aout 2022).

[183] Zhenjiang Zhang, Tonghuan Liu, and Wenyu Zhang. Novel paradigm for constructing masses in dempster-shafer evidence theory for wireless sensor network's multisource data fusion. *Sensors*, 14(4) :7049–7065, 2014.

Résumé

L'authentification et l'identification d'individus dans des systèmes physiques ou logiques sont plus qu'indispensables dans beaucoup d'applications tels que l'accès à des comptes bancaires, la reconnaissance des personnes via caméra de surveillance, ou encore, la protection des locaux privés ou des entreprises. La biométrie est l'un des moyens utilisés pour l'authentification ou l'identification des individus en leur accordant une forme d'identification unique et universelle. C'est dans cette direction que s'insère le présent travail qui a mis en œuvre un système d'authentification biométrique multimodal fusionnant les modalités visage et signature en utilisant la théorie de Dempster-Shafer. Cette théorie a été employée pour combiner les deux modalités afin d'accroître les performances du système. Les résultats des tests expérimentaux sur des bases de données benchmarks ont prouvé que l'utilisation de la multimodalité à l'aide de la théorie de Dempster-Shafer améliore les performances d'authentification comparativement aux modalités visage et signature en ligne prisent séparément.

Mots clés : Authentification ; Biométrie ; Système Biométrique ; Multimodalité ; Fusion de Données ; Dempster-Shafer ; Visage ; Signatures.

Abstract

Authentication and identification of individuals in physical or logical systems are more than essential in many applications, such as access to bank accounts, recognition of people via surveillance cameras, or protection of private premises or companies. Biometrics is one of the means used to authenticate or identify individuals by granting them a unique and universal form of identification. In this direction, the present work is inserted, which has implemented a multimodal biometric authentication system merging the face and signature modalities using the Dempster-Shafer theory. This theory was used to combine the two modalities to increase the performance of the system. The results of experimental tests on benchmark databases proved that the use of multimodality using dempster-Shafer theory improves authentication performance compared to the face and online signature modalities separately.

Keywords : Authentification ; Biometrics ; biometric system ; Multimodality ; Data Fusion ; Dempster-Shafer ; Face ; Signatures.