الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic OF Algeria
وزارة التعليم العالي و البحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جامعة الشهيد الشيخ العربي التبسي-تبسة
Echahid Cheikh Larbi Tebessi University-Tebessa
كلية العلوم و التكنولوجيا

DEPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE

DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME DE MASTER EN

RESEAUX ET TELECOMMUNICATION

THEME

Conception et évaluation d'an système d'authentification biométrique basé sur l'empreint palmaire

Présenté par le binôme :

- Haithem Laadjal

Devant le jury :

- Dr. Bentahar tarek **Président**
- Saigaa mohammed **Encadreur**
- Dr.houam loutfi **Examinateur**

2022/2023


بسم الله الرحمن الرحيم

Remerciements

Au terme de ce travail, on tient à exprimer notre profonde gratitude et nos sincères remerciements à Monsieur Saigaa mohammed directeur et encadrant de mémoire pour les efforts qu'il a déployés et les conseils qu'il nous a prodigués, sa patience, son soutien et sa confiance et surtout sa compréhension qui nous ont permis d'avancer et de bien mener ce travail le l

long de ces mois.

On tient à remercier aussi les membres de jury :

Monsieur : Mr. BENTAHAR Tarek.

Monsieur : Mr.houam loutfi

Qui ont accepté d'évoluer notre travail.

Nous remercions tous ceux qui nous ont aidés de près ou de loin afin de pouvoir réaliser et accomplir ce travail

Dédicace

Je dédie cet humble travail à : mon père. Aucun hommage ne peut égaler l'amour qu'ils continuent de montrer. Que Dieu leur accorde bonne santé et longue vie.

Aux personnes qui m'ont soutenu tout au long de ce projet :

Mes frères, sœurs, famille et amis.

Bien sûr, mes superviseurs sont M.

Et tous ceux qui y ont contribué directement ou indirectement

Ce projet peut dire merci

Résume

La biométrie concerne la reconnaissance automatique des individus en fonction de leurs traits physiologiques ou comportementaux. Les systèmes biométriques unimodaux reposent sur une source unique de données biométriques pour l'identification des personnes, bien qu'ils ne garantissent pas une précision sans faille. De nombreux défis rencontrés dans les systèmes unimodaux peuvent être surmontés en mettant en œuvre des systèmes biométriques multimodaux, qui intègrent plusieurs modalités ou caractéristiques biométriques d'une même personne. Cet article commence par introduire le concept de biométrie, suivi par l'élucidation de la structure des systèmes biométriques et des mesures utilisées pour évaluer leurs performances. En outre, il examine les modalités biométriques les plus répandues et diverses approches pour les amalgamer afin de construire des systèmes multimodaux. Enfin, il présente les résultats expérimentaux relatifs aux systèmes utilisant la biométrie à deux mains, en particulier l'empreinte palmaire et la veine palmaire.

Keywords: authentication, biometrics, palm print, Local binary pattern

Abstract

Biometrics pertains to the automatic recognition of individuals based on their physiological or behavioral traits. Unimodal biometric systems rely on a solitary source of biometric data for person identification, although they do not ensure flawless accuracy. Many challenges encountered in unimodal systems can be overcome by implementing multimodal biometric systems, which integrate several biometric modalities or characteristics of the same person. This piece commences by introducing the concept of biometrics, followed by elucidating the structure of biometric systems and the metrics employed to evaluate their performance. Furthermore, it examines the most prevalent biometric modalities and diverse approaches to amalgamating them in order to construct multimodal systems. Finally, it presents experimental findings pertaining to systems utilizing two hand biometrics, specifically palmprint and palm vein.

Mots-clés : authentification, biométrie, empreinte palmaire, modèle binaire local

ملخص

تتعلق القياسات الحيوية بالاعتراف التلقائي للأفراد بناءً على سماتهم الفسيولوجية أو السلوكية. تعتمد أنظمة القياسات الحيوية أحادية الوسائط على مصدر فردي لبيانات القياسات الحيوية لتحديد هوية الشخص ، على الرغم من أنها لا تضمن دقة لا تشوبها شائبة. يمكن التغلب على العديد من التحديات التي تواجه الأنظمة أحادية الوسائط من خلال تنفيذ أنظمة القياسات الحيوية متعددة الوسائط ، والتي تدمج العديد من طرائق أو خصائص القياسات الحيوية للشخص نفسه. تبدأ هذه القطعة بتقديم مفهوم القياسات الحيوية ، متبوعًا بتوضيح هيكل أنظمة القياسات الحيوية والمقاييس المستخدمة لتقييم أدائها. علاوة على ذلك ، فإنه يدرس طرائق القياسات الحيوية الأكثر انتشارًا والنهج المتنوعة لدمجها من أجل بناء أنظمة متعددة الوسائط. أخيرًا ، يقدم نتائج تجريبية تتعلق بالأنظمة التي تستخدم قياسات بيولوجية لليد ، على وجه التحديد بصمة الكف وعرق النخيل

الكلمات المفتاحية: المصادقة ، القياسات الحيوية ، بصمة الكف ، النمط الثنائي المحلي.

Table des matières

Listes des figures

Listes des tableaux

Glossaire

A

ADN : Acide Désoxyribonucléique

C

CMC : Cumulative match characteristic

D

DET : Detection error Tradoff

E

EER : Error equal

F

FAR : False acceptance rate

FMR : False match rate

FNMR : False non match rate

FTA : failure to acquire

FTE : Failure to enroll

FRR : False reject rate

M

MAD : Median absolute deviation

MAX : Maximum scores

MIN : Minimum scores

MUL : Multiplication scores

N

NIR : near-infrared

P

PLDA : Probability of linear discriminant analysis

PLV : Palm-Vein

R

ROC : Receiver operating characteristic

S

SUM : Sum scores

W

WHT : Sum-weighting scores

INTRODUCTION GÉNÉRAL

Introduction général

L'authentification biométrique est devenue une nécessité dans notre société moderne où la sécurité et l'identification précise des individus sont essentielles. Les méthodes traditionnelles d'authentification, telles que les mots de passe et les cartes d'identité, sont sujettes à des problèmes de sécurité tels que le vol ou la falsification. L'authentification biométrique utilise des caractéristiques physiques uniques, telles que les empreintes digitales, l'iris, la voix ou la reconnaissance faciale, pour identifier de manière fiable et précise les indiv{'authentification}idus. Cette approche offre des avantages tels que la praticité, la précision et la résistance à la fraude, faisant de l'authentification biométrique une nécessité pour garantir la sécurité et la confidentialité des données dans divers domaines, allant des services bancaires aux contrôles d'accès physiques.Les systèmes d'authentification biométrique unimodaux, qui se basent sur une seule caractéristique biométrique, présentent certaines limitations. L'une des principales limitations est la possibilité d'usurpation ou de contournement du système en utilisant des méthodes de contrefaçon ou de copie de la caractéristique biométrique. Par exemple, une empreinte digitale peut être reproduite à partir d'une empreinte laissée sur une surface, ou une image du visage peut être utilisée pour tromper un système de reconnaissance faciale.

C'est là que l'authentification biométrique multimodale entre en jeu. Les systèmes d'authentification multimodale combinent plusieurs caractéristiques biométriques, telles que l'empreinte digitale, la reconnaissance faciale et la voix, pour renforcer la sécurité et la précision de l'identification. En utilisant plusieurs modalités, les limitations inhérentes à chaque modalité individuelle peuvent être atténuées.

Les avantages de l'authentification biométrique multimodale sont multiples. Tout d'abord, elle améliore la fiabilité de l'identification en utilisant plusieurs sources de données pour vérifier l'identité d'un individu. Les caractéristiques biométriques peuvent être corrobées, réduisant ainsi les risques de fausses identifications. De plus, l'utilisation de plusieurs modalités permet de renforcer la résistance aux tentatives de contournement et de fraude.

En outre, l'authentification biométrique multimodale offre une plus grande flexibilité en termes d'adaptabilité aux différents environnements et conditions. Par exemple, dans des situations où l'éclairage ambiant peut affecter la reconnaissance faciale, l'utilisation simultanée d'autres modalités, telles que la reconnaissance vocale, peut compenser ces variations.

En résumé, l'authentification biométrique multimodale surmonte les limitations des systèmes unimodaux en combinant plusieurs caractéristiques biométriques. Elle améliore la fiabilité, renforce la sécurité et offre une expérience utilisateur plus fluide. L'adoption de cette approche permet de répondre aux exigences croissantes en matière de sécurité et de précision dans divers domaines d'application.

L'objectif de ce projet de fin d'études est de concevoir et d'évaluer un système d'authentification biométrique basé sur l'empreinte palmaire en utilisant l'algorithme Local Binary Pattern (LBP) multi-échelle avec la distance euclidienne. Ce système sera développé en exploitant deux bases d'images distinctes : une première base d'images au niveau de gris et une deuxième base d'images dans le spectre NIR (Near InfraRed).

Le système d'authentification biométrique que nous développons exploite l'empreinte palmaire, une caractéristique unique présente sur la paume de la main. En utilisant des images de l'empreinte palmaire et l'algorithme LBP pour extraire les variations locales de l'image, notre système facilite l'identification et l'authentification des individus. Cependant, afin de garantir la fiabilité et l'efficacité du système, nous adoptons une approche multimodale en utilisant deux bases d'images distinctes : une en niveau de gris et l'autre dans le spectre NIR. Cette approche permet de tester la robustesse et la performance du système dans des conditions d'éclairage et de qualité d'image variées, assurant ainsi une identification précise et fiable.

En resmué, ce projet de fin d'études se concentrera sur la conception et l'évaluation d'un système d'authentification biométrique basé sur l'empreinte palmaire. En utilisant l'algorithme LBP multi-échelle avec la distance euclidienne et en exploitant deux bases d'images distinctes, nous chercherons à développer un système fiable et efficace pour l'identification et l'authentification des individus. Les résultats de cette étude contribueront à l'avancement des technologies biométriques et à l'amélioration de la sécurité dans différents domaines d'application.

Ce mémoire est organisé en trois chapitres :

Le premier chapitre de ce mémoire commence par une revue de l'état de l'art de la biométrie, en mettant en évidence les différentes technologies biométriques utilisées dans le domaine de la reconnaissance. Une discussion détaillée des technologies existantes est présentée, mettant en évidence leurs avantages. Étant donné que ces technologies sont le sujet de nombreuses recherches, nous abordons les principaux points forts et faiblesses associés à chacune d'entre elles.

Dans le deuxième chapitre, nous abordons l'introduction du système multi-modal, en présentant les différentes catégories de modalités et leurs architectures respectives. Ensuite, nous expliquons en détail les niveaux de fusion des données. Nous examinons également diverses méthodes de fusion de scores, soulignant l'importance de la normalisation des scores pour les mettre tous dans la même plage de valeurs.

Le troisième chapitre met en avant notre contribution et les résultats expérimentaux du système que nous proposons. Nous présentons en détail les analyses et les discussions pertinentes, en nous appuyant sur l'utilisation de deux bases de données, chacune comprenant 100 personnes. Cette section permet de mettre en évidence notre travail et de fournir une évaluation complète de notre système, basée sur des expérimentations concrètes.

Enfin, ce mémoire présente une conclusion générale des résultats et des conclusions obtenues dans le cadre de cette étude. Nous soulignons également les perspectives futures envisagées pour poursuivre les recherches dans ce domaine. La conclusion générale offre une réflexion globale sur l'ensemble du travail réalisé et met en évidence les directions potentielles pour de futurs développements et approfondissements.

Chapitre I :

Initiation à la biométrique

Introduction

La biométrie est une technologie qui permet l'identification ou la vérification de l'identité d'un individu en utilisant des caractéristiques biologiques ou comportementales uniques telles que les empreintes digitales, les iris, les traits du visage, la voix, ou encore la signature. Cette technologie a connu une croissance rapide au cours des dernières années et a été largement adoptée dans de nombreux domaines tels que la sécurité, la surveillance, les transactions financières, la santé et les soins personnels. Dans ce chapitre, nous explorerons les différents types de biométrie, les différents types de systèmes biométriques ainsi que les avantages et les limites de cette technologie en matière de sécurité et de confidentialité.

I.1. La biométrique

I.2.1. Définition

La biométrie peut être définie comme l'utilisation de caractéristiques biologiques uniques pour l'identification et la vérification des individus. Ces caractéristiques peuvent inclure des éléments tels que les empreintes digitales, la reconnaissance faciale, les traits de la rétine, la géométrie de la main ou de la paume, la voix, ou même les modèles de frappe au clavier.

La biométrie se base sur le fait que chaque individu possède des caractéristiques physiques ou comportementales distinctives qui le distinguent des autres. Ces caractéristiques sont capturées à l'aide de dispositifs de capture spécifiques, tels que des scanners d'empreintes digitales, des caméras de reconnaissance faciale ou des systèmes de reconnaissance vocale.

L'utilisation de la biométrie permet d'identifier de manière fiable et précise les individus, car les caractéristiques biométriques sont difficiles à falsifier ou à reproduire. Elle offre des avantages tels qu'une sécurité renforcée, une facilité d'utilisation et une réduction des fraudes. [1]

I.2.2. Les caractéristiques biométriques

Les caractéristiques biométriques sont des attributs uniques et mesurables qui sont utilisés dans le domaine de la biométrie pour identifier de manière fiable et authentifier les individus. Ces

caractéristiques présentent plusieurs propriétés clés : collectabilité, unicité, permanence, universalité, acceptabilité et non répudiation. [2]

La collectabilité fait référence à la facilité avec laquelle les caractéristiques biométriques peuvent être mesurées et collectées chez un individu. Il est essentiel que ces caractéristiques puissent être obtenues de manière non intrusive et sans causer d'inconfort ou de douleur à la personne. [2]

L'unicité signifie que chaque individu possède des caractéristiques biométriques qui lui sont propres et distinctes des autres. Par exemple, les empreintes digitales sont réputées être uniques pour chaque personne, ce qui les rend idéales pour l'identification biométrique. [2]

La permanence fait référence à la stabilité des caractéristiques biométriques dans le temps. Bien que certaines caractéristiques puissent changer légèrement avec l'âge ou les blessures, elles sont généralement considérées comme relativement constantes sur une longue période. [2]

L'universalité signifie que les caractéristiques biométriques sont présentes chez tous les individus. Cependant, certaines caractéristiques peuvent être plus répandues que d'autres. Par exemple, la reconnaissance faciale peut être moins fiable chez les personnes présentant des anomalies faciales ou des maladies affectant les traits du visage. [2]

L'acceptabilité fait référence à la volonté des individus de fournir leurs caractéristiques biométriques. Il est important que les méthodes biométriques soient socialement acceptées et que les individus se sentent à l'aise de partager leurs informations biométriques pour des raisons de sécurité et d'identification. [2]

La non répudiation est une propriété importante des caractéristiques biométriques, ce qui signifie qu'une fois qu'une caractéristique biométrique est utilisée pour l'identification ou l'authentification, il est difficile pour l'individu de nier son association avec cette caractéristique. [2]

I.2. Les modalités biométriques

Les modalités biométriques font référence aux différentes caractéristiques physiques ou comportementales utilisées dans le domaine de la biométrie pour l'identification et l'authentification des individus. Il existe plusieurs types de modalités biométriques, chacune étant associée à des caractéristiques spécifiques.

Chaque modalité biométrique a ses propres avantages et limitations en termes de précision, de convivialité, de coût et de sécurité. L'utilisation de plusieurs modalités biométriques combinées peut renforcer la fiabilité et la précision du système biométrique. [3]

I.3.1. Les modalités biométriques physiques

Les modalités biométriques physiques sont des caractéristiques anatomiques distinctives utilisées pour l'identification et l'authentification des individus dans le domaine de la biométrie. Ces modalités sont basées sur des attributs physiques uniques et spécifiques à chaque individu.

Les modalités biométriques physiques comprennent différentes caractéristiques telles que les empreintes digitales, les traits du visage, les iris, la rétine, la géométrie de la main, la forme de l'oreille et la vascularisation de la main ou du doigt. Chacune de ces modalités a des propriétés distinctes qui les rendent appropriées pour l'identification biométrique.

Néanmoins, l'utilisation des modalités biométriques physiques présente également quelques inconvénients. Tout d'abord, leur mise en œuvre et leur maintenance peuvent être coûteuses. Deuxièmement, elles peuvent être lentes et nécessiter une procédure fastidieuse lors de leur utilisation. Troisièmement, elles peuvent être plus délicates à utiliser dans des environnements spécifiques, tels que des conditions de faible luminosité ou des environnements bruyants. [3]

L'empreinte palmaire

Les empreintes de la paume (palm prints) sont des empreintes spécifiques qui se trouvent sur la surface de la paume de la main d'une personne, et elles sont uniques à chaque individu. Ces particularités sont exploitées pour identifier et vérifier l'identité d'une personne. [3]

Figure I. 1L'empreinte palmaire

Avantages des empreintes de paume :

- Universalité et stabilité tout au long de la vie.
- Faible probabilité de correspondance accidentelle (faux positifs).
- Résistance à l'altération et aux blessures.
- Grande surface d'acquisition pour capturer plus de détails.

Inconvénients des empreintes de paume :

- Nécessite des dispositifs de capture spécifiques.

- Sensibilité à la pression lors de la capture.
- Coût potentiellement plus élevé que d'autres technologies biométriques.

La reconnaissance faciale

La reconnaissance faciale est une méthode biométrique qui exploite les caractéristiques distinctives du visage pour identifier une personne. Elle opère en comparant les traits faciaux d'une personne présents dans une image ou une vidéo en temps réel avec une base de données de visages connus. La reconnaissance faciale est couramment utilisée dans des applications de sécurité telles que le contrôle d'accès et la détection de fraudes. [3]

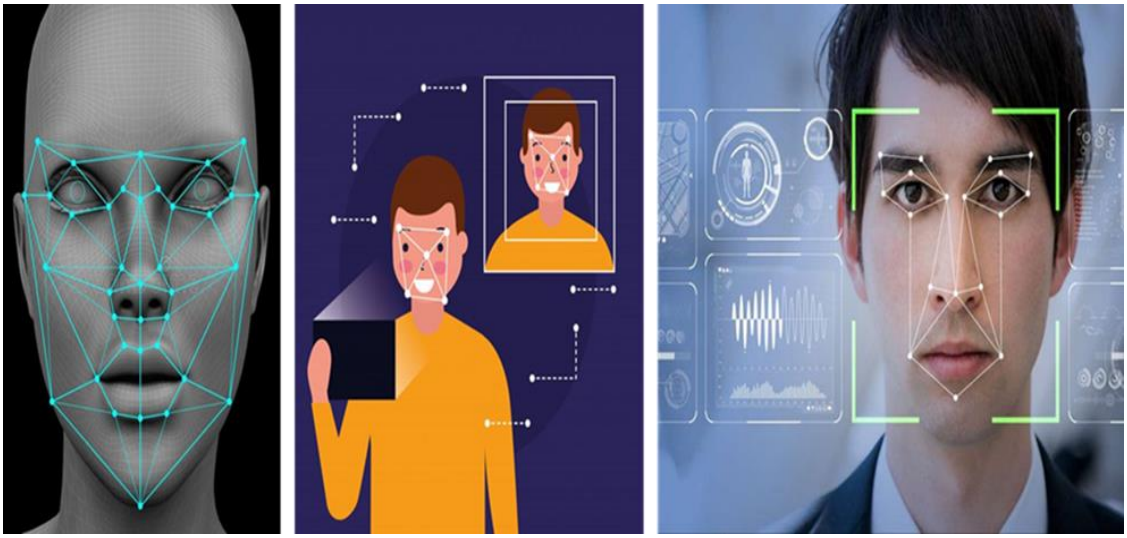


Figure I. 2. L'empreinte faciale

Avantages de la reconnaissance faciale

- La reconnaissance faciale est non intrusive et ne nécessite pas que la personne fournisse des informations personnelles.
- La reconnaissance faciale est très fiable, même lorsque la personne porte un déguisement ou a changé d'apparence.
- La reconnaissance faciale peut être utilisée pour identifier des personnes à distance.

Inconvénients de la reconnaissance faciale

- La reconnaissance faciale peut être trompée par des masques ou d'autres déguisements.
- La reconnaissance des visages peut être affectée par les conditions d'éclairage.
- La reconnaissance faciale peut être lente et difficile à utiliser.

La reconnaissance des empreintes digitales

La reconnaissance des empreintes digitales est une méthode biométrique qui exploite les motifs distinctifs présents sur les crêtes des doigts d'une personne pour son identification. Elle consiste à

numériser l'empreinte digitale d'un individu et à la comparer à une base de données d'empreintes digitales préalablement enregistrées. La reconnaissance des empreintes digitales est fréquemment employée dans des applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude. [4]

Figure I. 3. L'empreinte digitale

Avantages de la reconnaissance des empreintes digitales

- La reconnaissance des empreintes digitales est très fiable et difficile à falsifier.
- La reconnaissance des empreintes digitales est non intrusive et ne nécessite pas que l'individu fournisse des informations personnelles.
- La reconnaissance des empreintes digitales peut être utilisée pour identifier des personnes à distance.

Inconvénients de la reconnaissance des empreintes digitales

- La reconnaissance des empreintes digitales peut être affectée par des coupures, des cicatrices ou d'autres lésions des doigts.
- La reconnaissance des empreintes digitales peut être lente et difficile à utiliser.

La reconnaissance de l'iris

La reconnaissance de l'iris est une méthode biométrique qui exploite les caractéristiques uniques présentes dans l'iris de l'œil d'un individu pour son identification. Elle implique la capture de l'image de l'iris et sa comparaison avec une base de données d'iris préalablement enregistrés. La reconnaissance de l'iris est largement utilisée dans des applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude. [4]

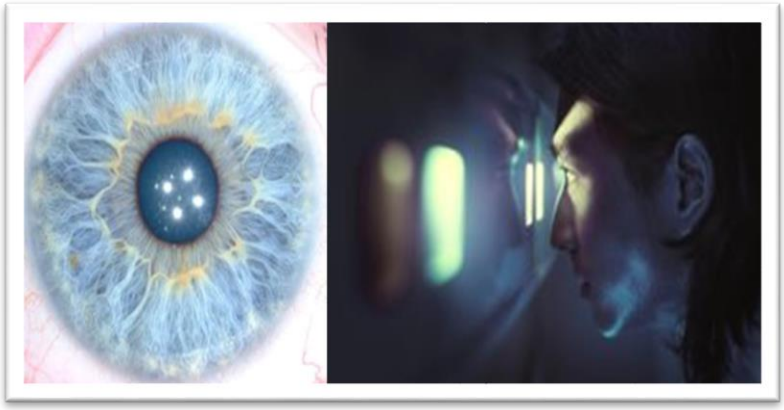


Figure I. 4. L'empreinte d'iris

Avantages de la reconnaissance de l'iris

- La reconnaissance de l'iris est très fiable et difficile à falsifier.
- a reconnaissance de l'iris est non intrusive et ne nécessite pas que l'individu fournisse des informations personnelles.
- La reconnaissance de l'iris peut être utilisée pour identifier des personnes à distance.

Inconvénients de la reconnaissance des empreintes digitales

- La reconnaissance de l'iris peut être affectée par les conditions d'éclairage.
- La reconnaissance de l'iris peut être lente et difficile à utiliser.

L'empreinte de doigt

L'empreinte de doigt est un motif unique formé par les caractéristiques papillaires présentes sur la surface des doigts, utilisé pour l'identification et la vérification biométriques dans divers domaines tels que la sécurité, la criminalistique et les technologies de reconnaissance, exploitant les singularités dermatoglyphiques pour garantir une identification précise et fiable des individus. [5]

Figure I. 5. L'empreinte de doigt

Les avantages l'empreinte de doigt

- Les empreintes digitales peuvent être facilement collectées à l'aide de scanners d'empreintes digitales, ce qui rend le processus d'identification rapide et pratique.
- Les empreintes digitales restent généralement inchangées tout au long de la vie d'une personne, ce qui garantit la permanence de cette modalité biométrique.
- Les empreintes digitales sont largement acceptées et utilisées dans de nombreux domaines, tels que les applications de sécurité, les contrôles d'accès, les services bancaires et les enquêtes criminelles.

Les inconvénients l'empreinte de doigt

- Bien que les empreintes digitales soient uniques, il existe des techniques sophistiquées permettant de reproduire artificiellement des empreintes digitales. Cela peut entraîner des problèmes de sécurité et nécessite des mesures de protection supplémentaires.
- La mise en place de systèmes de reconnaissance d'empreintes digitales, tels que des scanners et des logiciels spécialisés, peut être coûteuse, en particulier pour les organisations nécessitant une infrastructure étendue.

La reconnaissance géométrique de la main

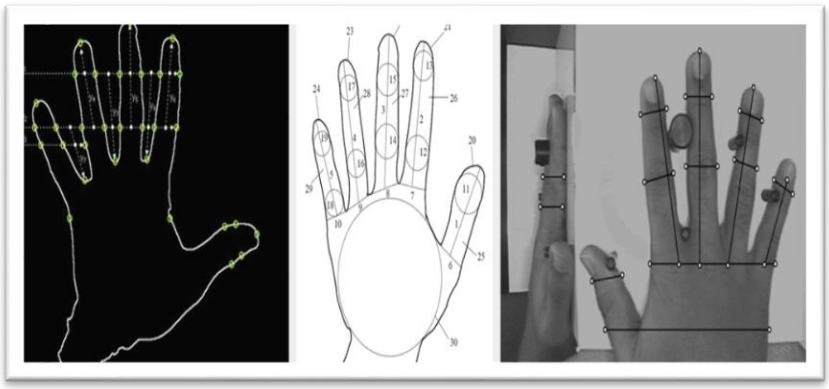


Figure I. 6. L'empreinte de la déommétrie de la main

La reconnaissance géométrique de la main est une technologie biométrique qui utilise la taille, la forme et d'autres caractéristiques uniques de la main d'une personne pour l'identifier. Elle fonctionne en scannant la main d'une personne et en la comparant à une base de données de mains connues. La reconnaissance de la géométrie de la main est souvent utilisée dans des applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude. [4]

Avantages de la reconnaissance géométrique de la main

- La reconnaissance géométrique de la main est très fiable et difficile à falsifier.

- La reconnaissance géométrique de la main est non intrusive et ne nécessite pas que l'individu fournisse des informations personnelles.
- La reconnaissance de la géométrie de la main peut être utilisée pour identifier des personnes à distance.

Inconvénients de la reconnaissance géométrique de la main

- La reconnaissance de la géométrie de la main peut être affectée par des blessures ou des déformations de la main.
- La reconnaissance de la géométrie de la main peut être lente et difficile à utiliser.

Le balayage rétinien

Le balayage rétinien est une technologie biométrique qui utilise les motifs uniques des vaisseaux sanguins de la rétine d'une personne pour l'identifier. Elle fonctionne en scannant la rétine d'une personne et en la comparant à une base de données de rétines connues. Le balayage rétinien est souvent utilisé dans des applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude. [4]

Figure I. 7. L'empreinte de retinien

Avantages du scanner rétinien

- Le balayage rétinien est très fiable et difficile à falsifier.
- Le balayage rétinien est non intrusif et n'exige pas que l'individu fournisse des informations personnelles.
- Le balayage rétinien peut être utilisé pour identifier des personnes à distance.

Inconvénients du scanner rétinien

- Le balayage rétinien peut être affecté par une lumière vive.
- Le balayage rétinien peut être lent et lourd à utiliser.

Dans l'ensemble, les modalités biométriques constituent un outil précieux pour l'identification. Elles sont fiables, sûres et non intrusives. Cependant, elles peuvent être coûteuses et lentes à utiliser.

I.3.2. La modalité biométrique comportementale

La modalité biométrique comportementale est un type d'identification biométrique qui utilise les modèles uniques de comportement pour identifier un individu. Il peut s'agir de caractéristiques telles que la façon dont une personne marche, la façon dont elle tape ou la façon dont elle parle. La biométrie comportementale est souvent utilisée dans les applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude. [6]

La dynamique de la frappe

Figure I. 8. La dynamique de la frappe

La dynamique de la frappe, également connue sous le nom de reconnaissance de la frappe au clavier ou de frappe au clavier dynamique, est une technique biométrique comportementale qui consiste à mesurer et analyser les caractéristiques individuelles de la manière dont une personne tape sur un clavier. Cette méthode utilise les modèles de pression, de timing et de style de frappe d'un individu pour identifier et authentifier l'utilisateur. [6]

La dynamique de la frappe se base sur le fait que chaque individu a une manière unique et distincte de taper sur un clavier. Les caractéristiques prises en compte peuvent inclure la pression exercée sur les touches, les intervalles de temps entre les pressions successives, la durée de pression de chaque touche, la vitesse de frappe et les modèles de digitation. Ces caractéristiques peuvent être mesurées à l'aide de capteurs spéciaux ou de logiciels installés sur le clavier. [6]

Avantages de la dynamique de la frappe

- La dynamique de la frappe est non intrusive et ne nécessite pas que l'individu fournisse des informations personnelles.
- La dynamique de la frappe peut être utilisée pour identifier des individus à distance.
- La dynamique de la frappe peut être utilisée pour authentifier des personnes en temps réel.

Inconvénients de la dynamique de la frappe

- La dynamique de la frappe peut être affectée par des facteurs tels que la fatigue, le stress et l'utilisation de claviers différents.
- La dynamique de la frappe peut être trompée par des personnes qui connaissent les habitudes de frappe de l'utilisateur.

La reconnaissance vocale

La reconnaissance vocale est une modalité biométrique comportementale qui mesure la façon dont une personne parle. Elle peut inclure des caractéristiques telles que la hauteur, le ton et le rythme de la voix d'une personne. La reconnaissance vocale peut être utilisée pour identifier des personnes avec un degré élevé de précision. [6]

Figure I. 9. La reconnaissance vocale

Avantages

- La reconnaissance vocale est non intrusive et ne nécessite pas que l'individu fournisse des informations personnelles.
- La reconnaissance vocale peut être utilisée pour identifier des personnes à distance.
- La reconnaissance vocale peut être utilisée pour authentifier des personnes en temps réel.

Inconvénients

- La reconnaissance vocale peut être affectée par des facteurs tels que la fatigue, le stress et l'utilisation de différents microphones.
- La reconnaissance vocale peut être trompée par des personnes qui sont familières avec les modèles vocaux de l'utilisateur.

L'analyse de la démarche

L'analyse de la démarche est une modalité biométrique comportementale qui mesure la façon dont une personne marche. Elle peut inclure des caractéristiques telles que la vitesse, la longueur de la foulée et la cadence de la marche d'une personne. L'analyse de la démarche peut être utilisée pour identifier des individus avec un haut degré de précision. [6]

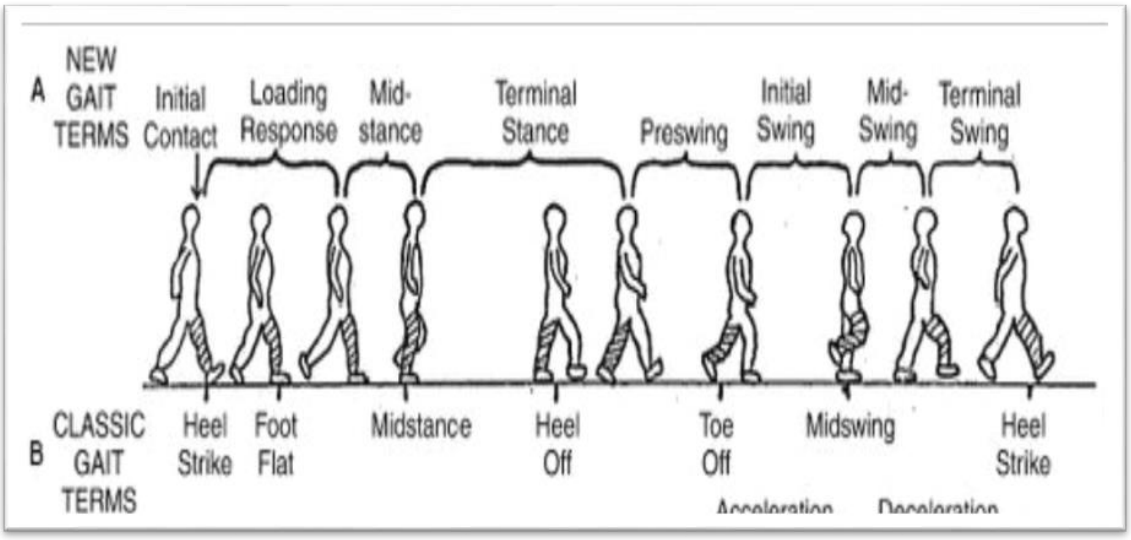


Figure I. 10. L'analyse de la démarche

Avantages du suivi des mouvements oculaires

- Le suivi des mouvements oculaires est non intrusif et ne nécessite pas que l'individu fournisse des informations personnelles.
- Le suivi des mouvements oculaires peut être utilisé pour identifier des personnes à distance.
- Le suivi des mouvements oculaires peut être utilisé pour authentifier des personnes en temps réel.

Inconvénients du suivi des mouvements oculaires

- Le suivi des mouvements oculaires peut être affecté par des facteurs tels que la fatigue, le stress et l'utilisation de conditions d'éclairage différentes.
- Le suivi des mouvements oculaires peut être trompé par des personnes qui connaissent bien les mouvements oculaires de l'utilisateur.

I.3.3. La modalité biométrique biologie

Ce type de biométrie est basé sur l'analyse des caractéristiques biologiques uniques de chaque individu, telles que l'odeur, l'ADN et les signaux physiologiques. L'idée fondamentale est que ces données biologiques peuvent servir de signature personnelle. Cependant, cette modalité n'est pas souvent utilisée pour le contrôle d'accès logique ou physique, et nous ne fournirons pas de détails supplémentaires à ce sujet. [4]

ADN

L'ADN, ou acide désoxyribonucléique, est une molécule présente dans toutes les cellules vivantes. En tant que modalité biométrique dans le domaine de la biologie, l'ADN est utilisé pour l'identification et l'authentification des individus en se basant sur leur code génétique unique. [4]

Chaque personne a un ADN spécifique qui lui est propre, à l'exception des jumeaux monozygotes. L'ADN est constitué de séquences de nucléotides (A, T, C, G) qui forment des gènes et des régions non codantes. Les variations dans ces séquences et leur arrangement spécifique déterminent les différences génétiques entre les individus. [4]

Avantages de l'utilisation de l'ADN comme modalité biométrique en biologie :

Unicité : L'ADN est unique pour chaque individu (sauf dans le cas des jumeaux monozygotes), ce qui permet une identification précise et fiable. [4]

Stabilité à long terme : L'ADN est relativement stable et peut être préservé pendant de longues périodes, ce qui facilite les comparaisons dans le temps. [4]

Figure I. 11. L'ADN

Avantages de [4]**:**

- Collecte non intrusive : L'échantillonnage de l'ADN peut être effectué à partir de diverses sources non invasives, telles que des cellules buccales, des cheveux ou des tissus, sans causer de dommages significatifs à l'individu.
- Capacité de résolution : L'ADN peut être utilisé pour résoudre des affaires criminelles, aider à l'identification de restes humains non identifiés et faciliter la recherche généalogique.
- Inconvénients et considérations liées à l'utilisation de l'ADN comme modalité biométrique :
- Confidentialité et protection des données : L'ADN contient des informations génétiques personnelles et sensibles, ce qui soulève des préoccupations en matière de confidentialité et de protection des données. Des mesures strictes doivent être prises pour garantir la sécurité des informations génétiques.

Les inconvénients [4] **:**

- Coût et complexité : L'analyse de l'ADN nécessite des équipements spécialisés et des compétences techniques avancées, ce qui peut rendre la mise en place et l'exploitation de ces systèmes coûteux.
- Limitations de la base de données : La création et la maintenance d'une base de données d'ADN pour la comparaison peuvent être complexes et nécessitent une gestion appropriée pour éviter les erreurs et les faux positifs.
- Sensibilité aux contaminants et à la dégradation : L'ADN peut être facilement contaminé ou dégradé, ce qui peut affecter la qualité des échantillons et conduire à des résultats incohérents ou incorrects.

I.3. Système biométrique :

I.4.1. Définition :

Un système biométrique est un système de reconnaissance et d'authentification des individus qui utilise des caractéristiques physiques, comportementales ou biologiques uniques et mesurables, appelées "données biométriques". Ces caractéristiques peuvent inclure des empreintes digitales, des images faciales, des iris, des rétines, des voix, des signatures et même des comportements tels que la façon de taper sur un clavier ou de marcher. [5]

Le système biométrique collecte et stocke les données biométriques d'un individu dans une base de données sécurisée, et les compare à chaque fois que l'individu tente d'accéder au système ou de s'identifier. Les systèmes biométriques sont de plus en plus utilisés dans des applications telles que le contrôle d'accès physique, la sécurité des données, les transactions bancaires, les passeports biométriques et les systèmes de vote en ligne. [5]

L'avantage des systèmes biométriques est que les données biométriques sont uniques pour chaque individu et ne peuvent être facilement imitées ou volées. Cependant, les systèmes biométriques présentent également des risques de sécurité, car les données biométriques sont des données personnelles sensibles qui doivent être stockées et protégées de manière adéquate. Les attaques et les vulnérabilités sur les systèmes biométriques peuvent compromettre la vie privée et la sécurité des individus, il est donc important de mettre en place des mesures de sécurité robustes pour protéger les données biométriques. [5]

I.4.2. Structure d’un système biométrique

La structure d'un système biométrique comprend plusieurs composants interconnectés, chacun jouant un rôle important dans le processus de reconnaissance et d'authentification des individus. Voici les principaux composants d'un système biométrique : [5]

Acquisition des données biométriques : Ce composant est responsable de la capture des données biométriques d'un individu à partir d'un périphérique de capture, tel qu'une caméra, un scanner ou un microphone. Les données biométriques acquises sont ensuite converties en format numérique et stockées dans une base de données.

Prétraitement

Les données biométriques brutes peuvent contenir des variations et des imperfections qui peuvent affecter les performances du système de reconnaissance. Le composant de prétraitement est responsable de nettoyer et de normaliser les données biométriques en utilisant des techniques de filtrage, de normalisation et d'optimisation pour améliorer la qualité des données. [5]

Extraction de caractéristiques

Ce composant est responsable de l'extraction des caractéristiques les plus pertinentes et distinctives des données biométriques, qui peuvent être utilisées pour identifier et authentifier les individus. Des techniques avancées telles que la reconnaissance de motifs et l'apprentissage automatique sont souvent utilisées pour extraire ces caractéristiques. [5]

Stockage de la base de données

Les données biométriques acquises et les caractéristiques extraites sont stockées dans une base de données sécurisée pour une utilisation ultérieure lors du processus d'authentification. [5]

Comparaison et décision

Ce composant est responsable de comparer les données biométriques de l'utilisateur actuel avec celles stockées dans la base de données et de prendre une décision d'authentification en fonction de la similitude des données. Des algorithmes sophistiqués tels que les réseaux de neurones et les machines à vecteurs de support sont souvent utilisés pour cette étape. [5]

En résumé, la structure d'un système biométrique est complexe et comprend plusieurs composants interconnectés qui travaillent ensemble pour fournir une reconnaissance et une authentification précises et sécurisées des individus.

I.4.3. Fonctionnement d’un système biométrique

Le fonctionnement d'un système biométrique peut être divisé en trois grandes étapes : l'enrôlement, la vérification et l'identification. Voici une description détaillée de chacune de ces étapes :

Enrôlement

Cette étape consiste à collecter les données biométriques d'un individu et à les stocker dans une base de données. Les données peuvent inclure des images faciales, des empreintes digitales, des modèles d'iris, des schémas de veines de la paume, etc. Les données peuvent également être prétraitées pour réduire les variations dues aux conditions d'acquisition. [5]

Vérification

Lors de la vérification, le système biométrique compare les caractéristiques biométriques d'un individu à celles stockées dans la base de données d'enrôlement pour confirmer son identité. Le processus de vérification est utilisé pour authentifier un individu qui prétend être la personne qu'il prétend être. Si la vérification réussit, l'individu est autorisé à accéder au système ou à une zone sécurisée. [5]

Identification

Contrairement à la vérification, l'identification ne nécessite pas que l'individu soit préalablement enregistré dans la base de données. Le système biométrique compare les caractéristiques biométriques de l'individu à toutes les données stockées dans la base de données pour identifier la personne. Le processus d'identification peut être utilisé pour identifier un individu inconnu ou pour rechercher une personne spécifique dans une base de données volumineuse. Si l'identification réussit, le système fournira l'identité de la personne correspondante. [5]

Dans l'ensemble, le fonctionnement d'un système biométrique est complexe et nécessite une combinaison de techniques d'acquisition de données, de traitement de données et d'algorithmes de reconnaissance pour produire des résultats précis et fiables. [5]

I.4. Performance des systèmes biométriques

La mesure de la performance d'un système biométrique dans un contexte d'utilisation donné évalue son efficacité et sa fiabilité. Cette section commence par la définition des différentes mesures de taux d'erreur utilisées pour quantifier la performance d'un tel système. Ensuite, les principales bases de données collectées, les compétitions de comparaison de systèmes biométriques ainsi que les plateformes d'évaluation existantes sont présentées. [1]

I.5.1. Les mesures des taux d’erreur

Taux d’erreur fondamentale

Taux d'échec à l’enrôlement (FTE) : Le pourcentage d'utilisateurs qui ne parviennent pas à s'inscrire avec succès dans le système. [1]

Taux d'échec à l'acquisition (FTA) : Le pourcentage de tentatives de capture de données biométriques qui n'aboutissent pas. [1]

Taux de non-correspondance (FNMR) : Le pourcentage de tentatives authentiques qui sont rejetées à tort par le système. [1]

Taux de fausse correspondance (FMR) : Il s'agit de la mesure de la proportion d'appariements incorrects, effectuée par l'algorithme de comparaison, entre les données biométriques acquises et le modèle correspondant à un individu différent. [1]

Taux d'erreur de systèmes d'authentification

Taux de fausse acceptation (FAR) : Le pourcentage d'utilisateurs non autorisés qui sont faussement acceptés par le système. Un faible FAR indique que le système est efficace pour empêcher les accès non autorisés. [1]

Taux de faux rejets (FRR) : Le pourcentage d'utilisateurs autorisés qui sont rejetés à tort par le système. Une FRR faible indique que le système accepte bien les utilisateurs autorisés. [1]

Taux d'erreur égal (EER) : Le point où le FAR et le FRR sont égaux. L'EER est une mesure unique qui peut être utilisée pour comparer les performances de différents systèmes biométriques. [1]

I.5.2. Les courbes de performance

Courbe DET : La courbe DET (Detection Error Tradeoff) est une représentation graphique du taux de fausses acceptations (FAR) et du taux de faux rejets (FRR) d'un système biométrique. La courbe DET est un outil utile pour comparer les performances des systèmes biométriques. [1]

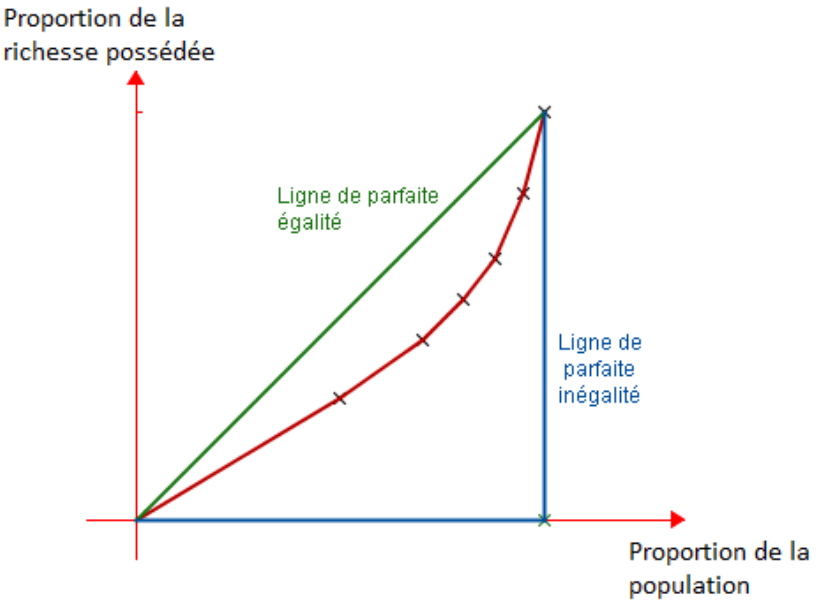


Figure I. 12. Courbe DET

Courbe ROC : La courbe ROC (Receiver Operating Characteristic) est une représentation graphique du taux de vrais positifs (TPR) et du taux de faux positifs (FPR) d'un système biométrique. La courbe ROC est un outil utile pour comparer les performances de différents systèmes biométriques. [1]

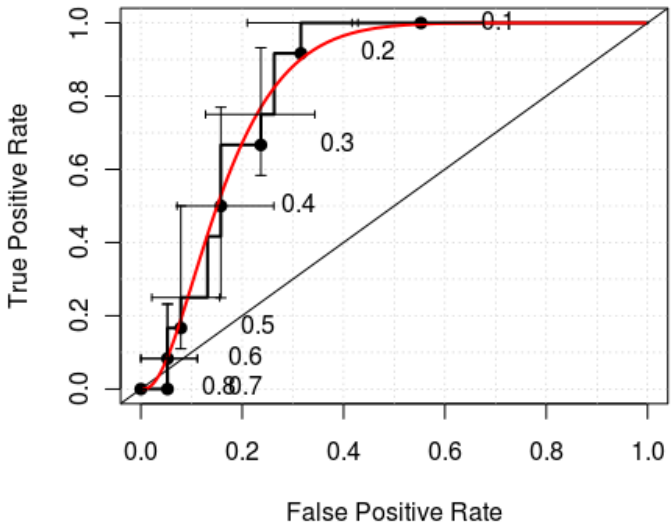


Figure I. 13. Courbe ROC

Courbe CMC : La courbe CMC (Cumulative Match Characteristic) est une représentation graphique des scores ordonnés de toutes les correspondances possibles entre une sonde et une galerie. La courbe CMC est un outil utile pour évaluer les performances d'un système biométrique à différents niveaux de précision. [1]

Courbe de distribution des scores des clients et des imposteurs : La courbe de distribution des scores des clients et des imposteurs est une représentation graphique de la distribution des scores pour les correspondances authentiques (clients) et les correspondances imposteurs. La courbe peut être utilisée pour évaluer les performances d'un système biométrique à différents niveaux de confiance. [1]

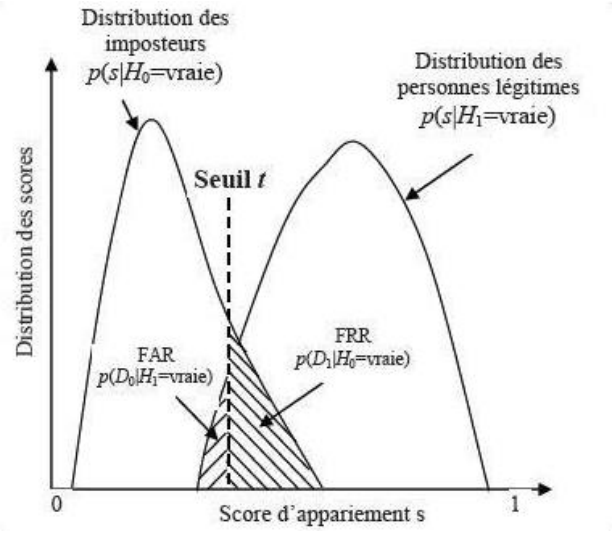


Figure I. 14. Courbe de distribution des scores des clients et des imposteurs

Courbe de taux d'erreur : La courbe du taux d'erreur est une représentation graphique du taux d'erreur d'un système biométrique en fonction du seuil de décision. La courbe peut être utilisée pour évaluer les performances d'un système biométrique à différents niveaux de sécurité. [1]

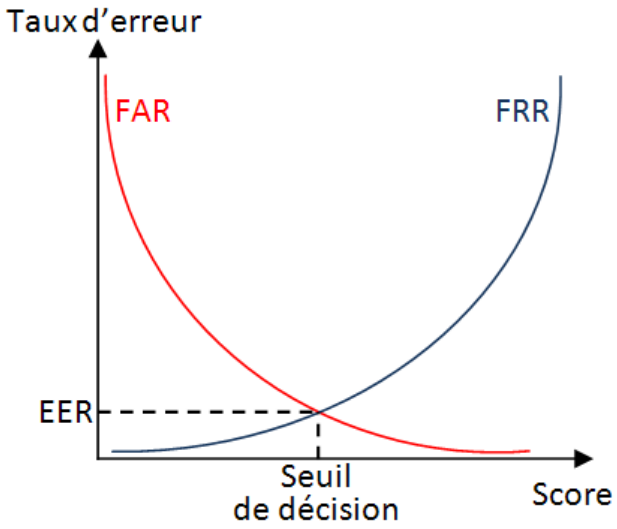


Figure I. 15. Courbe de taux d'erreur

I.5. L'application de la biométrie

L'utilisation de la biométrie est devenue de plus en plus répandue dans de nombreux domaines, notamment la sécurité, la surveillance, la gestion des identités et des accès, la santé, la banque et les transactions financières, ainsi que la gestion des frontières et des voyageurs. Les systèmes biométriques peuvent offrir des avantages significatifs par rapport aux méthodes traditionnelles d'identification et d'authentification, tels que les mots de passe, les cartes d'identité et les clés. [6]

I.6.1. La sécurité

Dans le domaine de la sécurité, les systèmes de reconnaissance faciale, les empreintes digitales et les scanners de rétine sont couramment utilisés pour contrôler l'accès aux bâtiments, aux ordinateurs et aux données sensibles. Ces systèmes peuvent également être utilisés dans les aéroports, les gares et les ports pour identifier les personnes à risque et empêcher l'entrée de personnes non autorisées. [6]

I.6.2. La surveillance

Dans le domaine de la surveillance, les systèmes biométriques peuvent être utilisés pour identifier les suspects lors d'enquêtes criminelles et pour prévenir les fraudes et les vols. Les systèmes de reconnaissance faciale peuvent être utilisés pour surveiller les zones publiques, telles que les centres commerciaux et les gares, afin d'identifier les personnes recherchées ou de détecter les comportements suspects. [6]

I.6.3. La gestion des identités et des accès

Dans la gestion des identités et des accès, les systèmes biométriques peuvent être utilisés pour renforcer la sécurité des données sensibles et de l'infrastructure des entreprises. Les empreintes digitales, les scans de rétine et les reconnaissances vocales peuvent être utilisés pour s'assurer que seules les personnes autorisées ont accès aux informations confidentielles. [6]

I.6.4. La santé

Les systèmes biométriques peuvent être utilisés pour garantir que les patients reçoivent les soins appropriés et que leurs dossiers médicaux sont correctement identifiés. Les scans de rétine et les empreintes digitales peuvent être utilisés pour garantir que les soins sont administrés à la bonne personne. [6]

I.6.5. Les banques et Les transactions financières

Les systèmes biométriques peuvent être utilisés pour renforcer la sécurité des transactions. Les systèmes de reconnaissance vocale, de reconnaissance faciale et de scan de rétine peuvent être utilisés pour authentifier les utilisateurs et empêcher les fraudes financières. [6]

I.6.6. La gestion des frontières et des voyageurs

Dans la gestion des frontières et des voyageurs, les systèmes biométriques peuvent être utilisés pour faciliter les contrôles d'identité et accélérer les procédures de passage en douane. Les systèmes de reconnaissance faciale et de scan de rétine peuvent être utilisés pour vérifier l'identité des voyageurs et pour empêcher les personnes recherchées de traverser les frontières.

Dans l'ensemble, l'utilisation de la biométrie offre une alternative efficace aux méthodes traditionnelles d'identification et d'authentification, offrant une sécurité accrue et une meilleure protection de la vie privée. Cependant, il est important de considérer les préoccupations liées à la collecte et à l'utilisation de données biométriques sensibles, ainsi que les limites techniques et légales de ces systèmes. [6]

I.6. Conclusion

La biométrie est la science qui permet d'identifier les individus sur la base de leurs caractéristiques physiques ou comportementales uniques. Les systèmes biométriques sont utilisés dans diverses applications, notamment le contrôle d'accès, le suivi des horaires et des présences et la détection des fraudes.

Les traits biométriques les plus courants sont les empreintes digitales, la reconnaissance faciale et la reconnaissance de l'iris. Les empreintes digitales sont les caractéristiques biométriques les plus utilisées, car elles sont relativement faciles à capturer et peuvent être utilisées pour identifier des individus même

s'ils portent des gants ou ont les mains sales. La reconnaissance faciale devient de plus en plus populaire, car il s'agit d'un moyen non intrusif d'identifier les individus. La reconnaissance de l'iris est la caractéristique biométrique la plus précise, mais c'est aussi la plus coûteuse à mettre en œuvre.

Chapitre II :

Biométrie multimodal et stratégies et techniques de fusion

Introduction

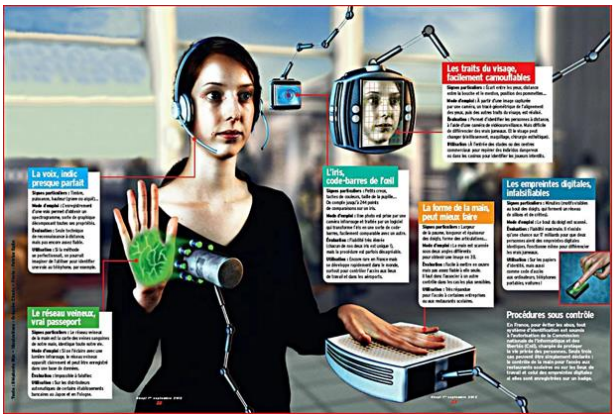
Le système biométrique optimal et robuste doit posséder les caractéristiques universelles, acceptables, uniques, colléctables et sécurisées. Cependant, aucune modalité ne peut réunir toutes ces propriétés. La solution consiste donc à utiliser plusieurs caractéristiques biométriques dans un système unique afin d'améliorer ses performances.

Dans ce chapitre, nous aborderons la multi-biométrie et ses différentes catégories, puis nous présenterons les stratégies de fusion ainsi que les niveaux d'informations. Enfin, nous expliquerons le principe de fusion de scores, ses approches et la normalisation des scores.

II.1. Biométrie multimodale

La reconnaissance des individus repose sur l'utilisation de modalités biométriques physiques ou comportementales. Cependant, chaque modalité prise isolément ne peut pas toujours être utilisée de manière fiable pour effectuer une reconnaissance précise. C'est pourquoi la consolidation d'informations provenant de différentes modalités peut être utilisée pour améliorer la précision de la reconnaissance de l'identité.

Lorsqu'il s'agit de reconnaître les individus, il existe plusieurs modalités biométriques disponibles, telles que les empreintes digitales, les traits du visage, la rétine, l'iris, la voix, la démarche, etc. Chacune de ces modalités présente ses propres avantages et limitations. Par exemple, les empreintes digitales peuvent être altérées ou difficiles à capturer dans certaines conditions, tandis que la reconnaissance faciale peut être affectée par des changements d'apparence tels que les barbes ou les lunettes.



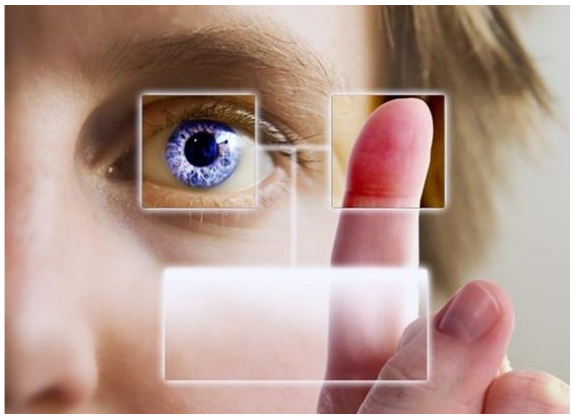


Figure II. 1Biométrie multimodale

La combinaison de plusieurs modalités biométriques dans un système multimodal vise à surmonter ces limitations. En intégrant des informations provenant de différentes sources, telles que les empreintes digitales, les empreintes palmaires, les traits du visage et la voix, il est possible d'obtenir une représentation plus complète et plus discriminante de l'identité d'une personne.

L'avantage de l'approche multimodale est qu'elle permet d'exploiter les forces de chaque modalité tout en atténuant leurs faiblesses. Par exemple, si une modalité échoue à identifier une personne en raison d'une altération ou d'une défaillance, les autres modalités peuvent compenser cette lacune et fournir des informations supplémentaires pour une reconnaissance plus précise.

En augmentant la quantité et la diversité des informations discriminantes disponibles pour chaque individu, les systèmes biométriques multimodaux visent à améliorer les performances de reconnaissance, que ce soit pour la vérification (vérifier si une personne est celle qu'elle prétend être) ou pour l'identification (déterminer l'identité d'une personne parmi un groupe).

Cependant, l'utilisation de multiples modalités biométriques soulève également des défis techniques tels que l'alignement et la fusion des données, la gestion de la dimensionnalité, la confidentialité des données et la robustesse contre les attaques frauduleuses.

En résumé, la consolidation d'informations provenant de différentes modalités biométriques dans un système biométrique multimodal permet d'améliorer la précision et la fiabilité de la reconnaissance des individus. Cette approche offre de nombreux avantages et constitue une voie prometteuse pour surmonter les limitations des systèmes biométriques unimodaux.[5]

II.2. Nécessites de la biométrie multimodale

La biométrie multimodale présente plusieurs nécessités :

Amélioration des performances

L'utilisation de plusieurs modalités biométriques permet d'obtenir des performances plus élevées en termes de précision et de fiabilité de l'identification ou de la vérification biométrique. En combinant différentes caractéristiques biométriques.[7]

Robustesse aux limitations unimodales

Les systèmes biométriques unimodaux peuvent être affectés par des limitations telles que des taux de faux positifs ou négatifs élevés, des problèmes de captation des données ou des variations intra-classes. [7]

Réduction du risque d'impossibilité d'enregistrement

Certaines personnes peuvent ne pas être en mesure de fournir certaines modalités biométriques en raison de problèmes physiques ou médicaux. En utilisant plusieurs modalités, il est plus probable de trouver une combinaison d'informations biométriques disponibles pour chaque individu, réduisant ainsi le risque d'impossibilité d'enregistrement.[8]

Renforcement de la sécurité

L'utilisation de plusieurs modalités biométriques augmente la robustesse du système face aux tentatives de fraude ou d'usurpation d'identité. Les fraudeurs doivent non seulement contourner une modalité biométrique, mais aussi plusieurs modalités, ce qui rend la tâche plus difficile.[8]

II.2.1. Limitations des systèmes uni-modaux

Les systèmes biométriques unimodales sont affectés par plusieurs facteurs qui dégradent leurs performances par nombreuses techniques de reconnaissance tels que :

II.2.1.1. Le bruit

L'utilisation d'un capteur défaillant ou mal entretenu, par exemple l'accumulation de poussière sur le capteur d'empreinte digitale, peut sérieusement compromettre la précision du système. [9]

II.2.1.2. Non-universalité

Certaines personnes peuvent avoir des empreintes non enregistrables en raison d'un accident ou d'un travail manuel prolongé. [5]

II.2.1.3. Manque d'individualité

Il est possible d'observer une similarité des caractéristiques extraites de deux personnes différentes en raison de facteurs génétiques tels que les jumeaux, les membres de la même famille ou même les membres de la même population. Cela peut avoir un impact significatif sur les performances du système biométrique en augmentant le taux de fausses acceptations. [9]

II.2.1.4. Manque de représentation invariante

Les variations à l'intérieur d'une même modalité biométrique peuvent se manifester, par exemple, par deux signatures différentes correspondant à la même personne. [9]

II.2.1.5. Sensibilité aux attaques

Les méthodes biométriques aident à réduire les problèmes de fraude et de vol, il est important de noter qu'ils ne les éliminent pas complètement. Des études ont démontré qu'il est possible de voler une empreinte digitale et de la reproduire en utilisant des techniques telles que l'utilisation de silicone. De même, les modalités biométriques telles que la signature et la voix sont relativement faciles à falsifier. Par conséquent, malgré les avantages des méthodes biométriques, il reste important d'être conscient des limitations et de prendre des mesures supplémentaires pour renforcer la sécurité et la fiabilité des systèmes biométriques. [9]

II.2.2. Avantage des systèmes multimodaux

Les systèmes multimodaux offrent plusieurs avantages lorsqu'il s'agit de traiter et de présenter des informations provenant de différentes sources. Voici quelques-uns de ces avantages :

II.2.2.1. Amélioration de la compréhension

Les systèmes multimodaux, en intégrant plusieurs modes d'interaction tels que la voix, le texte et les images, permettent une meilleure compréhension des informations.[10]

II.2.2.2. Adaptation à l'utilisateur

Les systèmes multimodaux peuvent s'adapter aux préférences et capacités des utilisateurs, offrant une communication personnalisée et adaptée à leurs besoins individuels.[11]

II.2.2.3. Interaction naturelle

Les interfaces multimodales permettent une interaction plus naturelle avec les systèmes informatiques en utilisant différents modes d'interaction.[12]

II.2.2.4. Compensation des limitations des modes individuels

Les systèmes multimodaux peuvent compenser les faiblesses d'un mode d'interaction en tirant parti des forces des autres modes, améliorant ainsi l'efficacité et la précision globales [13]

II.3. Fusion des données

La fusion des données est une technique utilisée pour traiter des informations provenant de multiples sources. Elle consiste à combiner des données issues de plusieurs sources afin d'obtenir une décision meilleure que celle obtenue à partir de chacune des sources considérées individuellement. À l'origine, la fusion des données a été développée dans un contexte militaire pour des objectifs tels que la localisation des cibles ennemies et la fusion d'images radar. Les systèmes utilisés font appel à diverses techniques issues de domaines variés tels que le traitement du signal, l'intelligence artificielle, la reconnaissance des formes, la classification, etc.[5]

De manière générale, la fusion des données est une opération d'intégration de plusieurs données en vue d'extraire une nouvelle information plus représentative de l'ensemble des données. Actuellement, la fusion des données joue un rôle de plus en plus important dans de nombreux domaines. Elle permet d'aider efficacement les scientifiques à extraire des informations de plus en plus pertinentes et précises. Initialement axée sur l'amélioration de la qualité des réponses aux problèmes militaires, la fusion des données s'étend désormais à de nombreux domaines tels que la télédétection, la prévision météorologique, la biométrie multimodale, les applications médicales et la robotique.[14]

Dans ces domaines, la fusion des données permet de combiner différentes sources d'informations, telles que des données géospatiales, des données météorologiques, des données biométriques provenant de modalités multiples, des données médicales variées, ou encore des données sensorielles pour les robots. En intégrant ces différentes sources de données, la fusion permet de générer une information plus complète, plus précise et plus robuste, fournissant ainsi des avantages significatifs dans la prise de décision, la détection de modèles, la prévision et d'autres applications.[15]

II.4. Stratégies de fusion

Stratégies de fusion au sens large se réfère à cinq scenarios différents (Figure 2.2) qui sont :

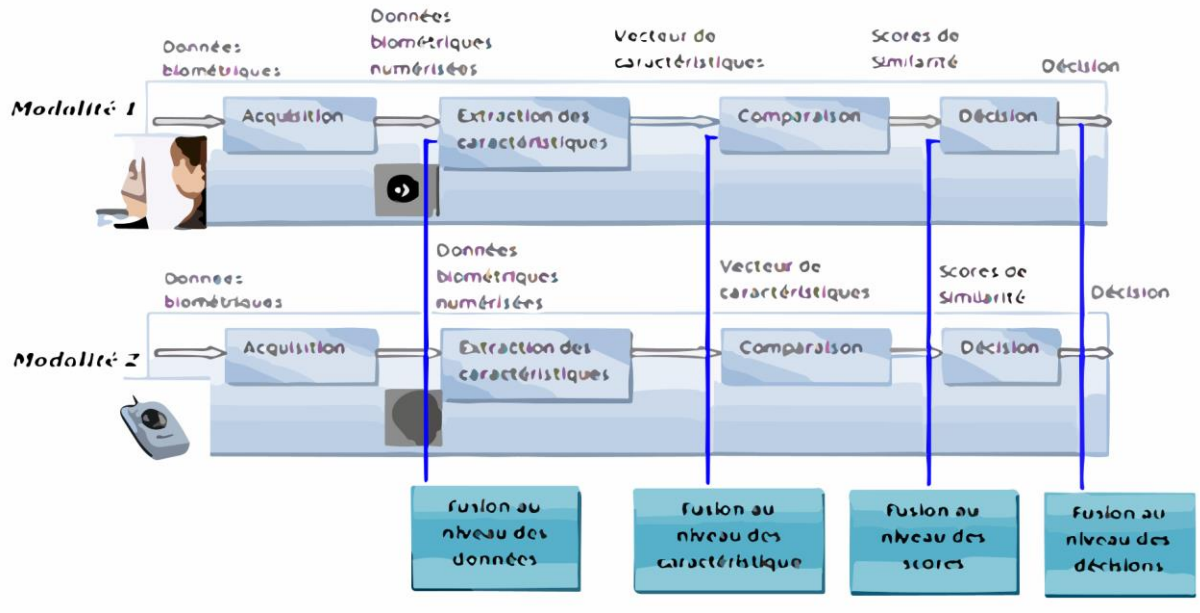


Figure II. 2Différents niveaux de fusion biométrique

II.4.1. Systèmes multi-capteurs

Dans ce système, nous utilisons plusieurs capteurs pour acquérir différentes modalités d'un même trait biométrique, permettant ainsi d'extraire plusieurs informations. Par exemple, nous capturons la texture 2D, la surface 3D et l'image infrarouge du visage de l'individu à l'aide de différents types de capteurs. [16]

II.4.2. Systèmes multi-instances

Dans ce cas, on utilise un seul capteur pour extraire différentes instances du même caractère biométrique, permettant d'obtenir plusieurs variations de ce trait et d'enrichir le modèle biométrique de l'individu. Par exemple, on acquiert plusieurs images du visage en variant la pose, l'expression et l'illumination. [16]

II.4.3. Systèmes multi-algorithmes

Les systèmes multi-algorithmes sont conçus pour utiliser plusieurs algorithmes afin d'extraire des caractéristiques et de calculer la similarité dans le cadre d'une même modalité biométrique. Par exemple, lorsque l'on traite une image d'empreinte palmaire, il est possible de combiner des algorithmes d'analyse de texture et de minuties afin d'extraire différents types de caractéristiques. Cette approche permet d'améliorer les performances globales du système.

L'idée derrière les systèmes multi-algorithmes est d'exploiter les forces spécifiques de chaque algorithme pour obtenir des informations complémentaires sur la modalité biométrique. En utilisant plusieurs algorithmes, le système peut tirer parti de leurs capacités individuelles et combiner les résultats pour obtenir une analyse plus précise et fiable.[16]

Par exemple, les algorithmes d'analyse de texture se concentrent sur les motifs et les structures présents dans l'image, tandis que les algorithmes de minuties se concentrent sur les caractéristiques spécifiques des empreintes digitales, telles que les points de bifurcation et les points finaux. En combinant ces deux approches, le système peut extraire un ensemble plus diversifié de caractéristiques, ce qui peut conduire à une meilleure performance en termes d'identification ou de vérification biométrique.[16]

L'avantage des systèmes multi-algorithmes réside dans leur capacité à améliorer la robustesse et la fiabilité des systèmes biométriques. En exploitant la complémentarité des algorithmes, ces systèmes sont mieux équipés pour faire face à des conditions variables telles que les variations de qualité d'image, les altérations ou les tentatives de contournement frauduleuses.[16]

En conclusion, les systèmes multi-algorithmes offrent une approche prometteuse pour améliorer les performances des systèmes biométriques en combinant plusieurs algorithmes d'extraction de caractéristiques et de calcul de similarité. Cette approche permet d'obtenir des informations plus riches et de renforcer la fiabilité des systèmes biométriques dans des situations diverses et complexes.[16]

II.4.4. Systèmes multi-échantillons

Les systèmes multi-échantillons sont conçus pour utiliser un seul capteur afin d'acquérir plusieurs échantillons d'une même caractéristique biométrique. Cette approche vise à prendre en compte les variations pouvant se produire au sein de cette caractéristique ou à obtenir une représentation plus complète de celle-ci.

L'utilisation d'un seul capteur pour capturer plusieurs échantillons permet au système de mieux saisir les différentes nuances et variations présentes dans le trait biométrique. Par exemple, lors de la capture d'empreintes digitales, le système peut acquérir plusieurs images d'une même empreinte digitale sous différents angles ou conditions d'éclairage. Cela permet de tenir compte des variations naturelles qui peuvent se produire, telles que les plis de la peau, les cicatrices ou les changements de pression lors de la capture.[16]

L'avantage des systèmes multi-échantillons réside dans leur capacité à améliorer la précision et la fiabilité des systèmes biométriques en utilisant des informations provenant de plusieurs échantillons. En utilisant une représentation plus complète de la caractéristique biométrique, le système peut réduire les erreurs de correspondance et améliorer les performances d'identification ou de vérification biométrique.

En conclusion, les systèmes multi-échantillons sont une approche efficace pour prendre en compte les variations et obtenir une représentation plus complète des caractéristiques biométriques. En utilisant un seul capteur pour acquérir plusieurs échantillons, ces systèmes renforcent la précision et la fiabilité des systèmes biométriques dans des conditions variables, contribuant ainsi à des performances plus robustes et précises.[16]

II.4.5. Systèmes multi-biométries

Les systèmes multi-biométries sont des systèmes qui combinent différentes modalités biométriques pour établir l'identité d'une personne. Dans le cadre de ces systèmes, plusieurs caractéristiques biométriques sont utilisées ensemble.

Cependant, le nombre de caractéristiques biométriques utilisées dans une application spécifique est souvent limité pour des raisons pratiques. Ces limitations sont liées à des considérations telles que le coût de déploiement, le temps nécessaire pour l'enrôlement des individus, le temps de réponse du système et le taux d'erreur attendu.

L'objectif de l'utilisation de plusieurs biométries est de renforcer la fiabilité et la précision de l'identification biométrique en combinant les avantages de différentes modalités. Par exemple, un système multi-biométrie pourrait combiner l'empreinte digitale, la reconnaissance faciale et la reconnaissance de l'iris pour obtenir une identification plus précise et fiable.

Cependant, pour des raisons de praticité, il est important de trouver un équilibre entre le nombre de caractéristiques biométriques utilisées et les contraintes opérationnelles. Cela permet de garantir des performances satisfaisantes tout en prenant en compte les limitations en termes de coût, de temps et de taux d'erreur.

En conclusion, les systèmes multi-biométries combinent différentes modalités biométriques pour améliorer l'identification et la vérification des individus. Toutefois, le nombre de caractéristiques biométriques utilisées est généralement limité pour des raisons pratiques, afin de garantir des performances optimales tout en respectant les contraintes opérationnelles. [16]

II.5. Niveaux de fusion

Dans un système biométrique multimodal, la fusion peut utiliser les informations disponibles dans n'importe quel module du système. La combinaison de plusieurs systèmes biométriques peut être réalisée à quatre niveaux différents [17]. La fusion des informations biométriques peut être classifiée en fusion pré-classification et fusion post-classification.

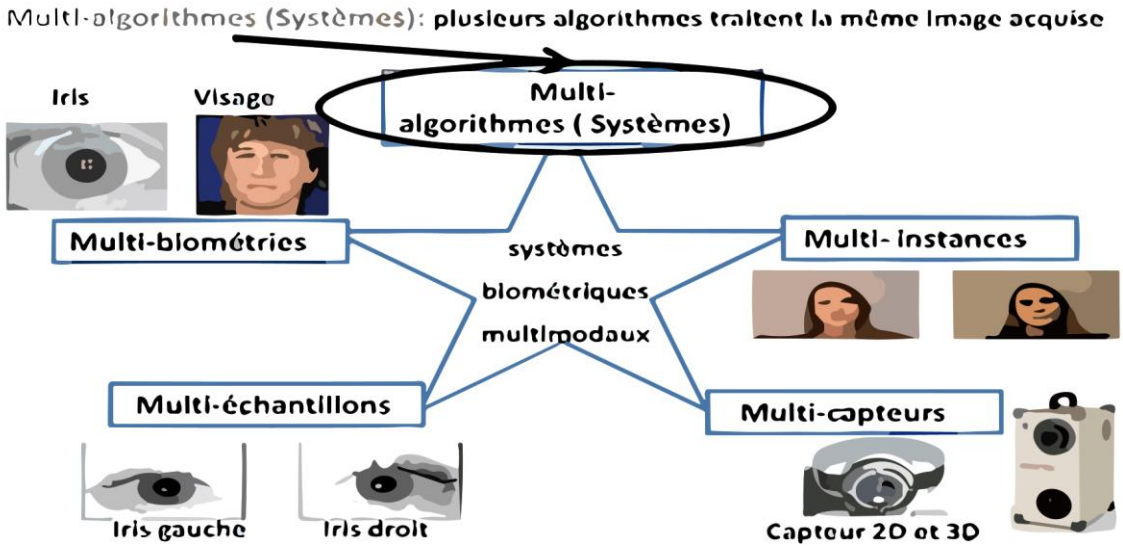


Figure II. 3Système biométrique multimodaux

II.5.1. Fusion Pré-classification

La fusion pré-classification consiste à fusionner les informations provenant de différentes données biométriques, que ce soit au niveau du capteur ou au niveau des caractéristiques extraites par le module d'extraction.

Niveau capteur

Dans ce niveau implique la fusion des données biométriques provenant de capteurs différents. La fusion de ces données est possible lorsque les captures sont des instances du même trait biométrique obtenues à partir de capteurs compatibles entre eux. Par exemple, au niveau de fusion des capteurs, il est possible de détecter un signal vocal simultanément à l'aide de deux microphones différents. [17]

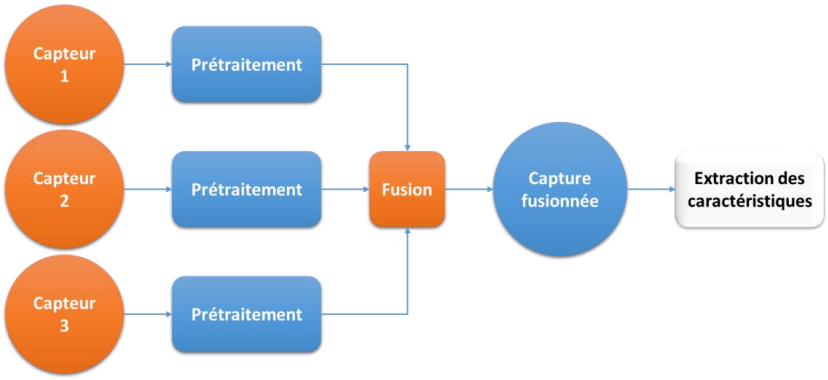


Figure II. 4Schéma bloc : fusion au niveau du capteur

Niveau des caractéristiques

La fusion au niveau caractéristiques, appelée fusion de caractéristiques, consiste à combiner différents vecteurs de caractéristiques obtenus à partir de phases de traitement et d'analyse différentes.

Lorsque les vecteurs de caractéristiques sont homogènes (par exemple, plusieurs images d'empreinte palmaires d'un utilisateur), un seul vecteur de caractéristiques peut être calculé en effectuant une somme pondérée des vecteurs individuels. Lorsque les vecteurs de caractéristiques sont hétérogènes (par exemple, des vecteurs de caractéristiques de différentes modalités biométriques telles que le visage et la géométrie de la main), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.[18]

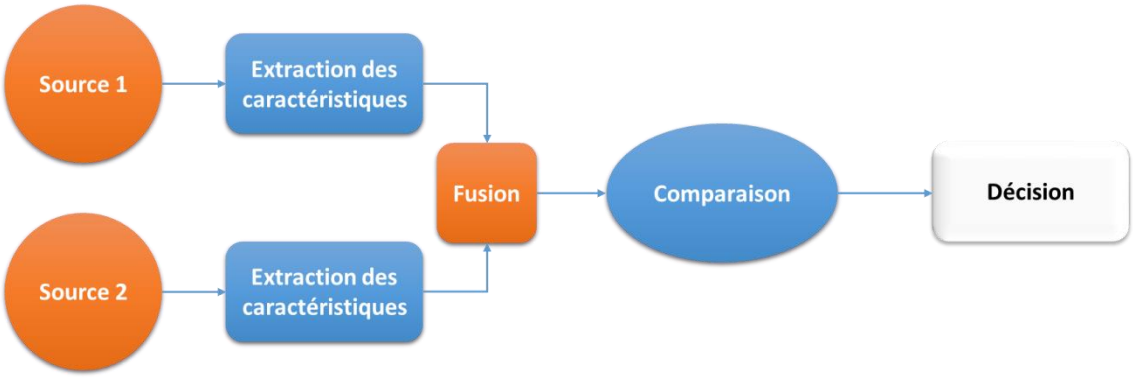


Figure II. 5fusion au niveau du l'extraction des caractéristiques

II.5.2. Post-classification

La fusion post-classification est un domaine de recherche très étudié par les chercheurs. Cette fusion peut être réalisée au niveau des scores provenant des modules de comparaison ou au niveau des décisions.

Fusion au niveau scores

Les scores individuels sont combinés de manière à former un score unique qui est ensuite utilisé pour prendre la décision finale. La fusion au niveau des scores est le type de fusion le plus couramment utilisé [19], car elle peut être appliquée à tous les types de systèmes grâce à des méthodes simples et efficaces.

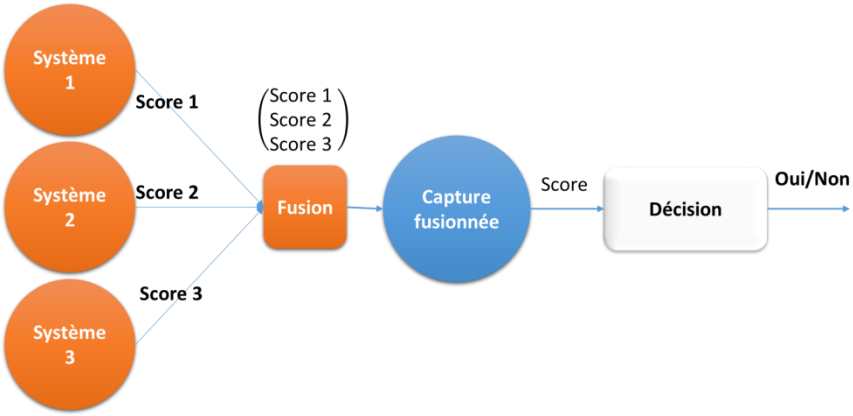


Figure II. 6 Schéma de fusion au niveau de scores

1. *Somme des scores (SUM)*

Cette méthode consiste à combiner les scores en les additionnant. Chaque score individuel est représenté par "di", et le score final fusionné est calculé en faisant la somme de tous les scores individuels :

$$D_f = \sum D_i$$

2. *Somme pondérée des scores (WHT)*

Cette règle est la somme des scores en pondérant chaque score individuel en fonction de son taux d'erreur associé ou de sa performance individuelle. Chaque score est multiplié par un poids (wi) qui est calculé en inversant le rapport entre l'erreur de chaque système (εi) et la somme des inverses des erreurs de tous les systèmes (PΣ1/εj). Ainsi, le score final fusionné (Df) est calculé en faisant la somme pondérée des scores individuels :

$$D_f = \sum D_i$$

3. *Minimum des scores (MIN)*

Dans cette méthode, le score final fusionné est déterminé en choisissant le meilleur (minimum) score parmi les différents systèmes. Le score final (D_f) est égal au minimum des scores individuels :

$$D_f = \min(D_i)$$

4. *Maximum des scores (MAX)*

Cette méthode attribue le score maximum comme score final fusionné. Le score final (D_f) est égal au maximum des scores individuels :

$$D_f = \max(D_i)$$

5. Produit des scores (MUL)

Cette méthode combine les scores en les multipliant entre eux. Chaque score individuel est représenté par "di", et le score final fusionné est calculé en faisant le produit de tous les scores individuels :

$$D_f = \prod D_i$$

Niveau de décision

Chaque modalité est tout d'abord identifiée de manière indépendante, puis la décision finale est prise en fusionnant les décisions des différents processus biométriques. Les résultats des différents classificateurs sont consolidés en utilisant des techniques telles que la majorité des votes. La fusion au niveau des décisions est considérée comme rigide en raison de la disponibilité limitée des informations.[17]

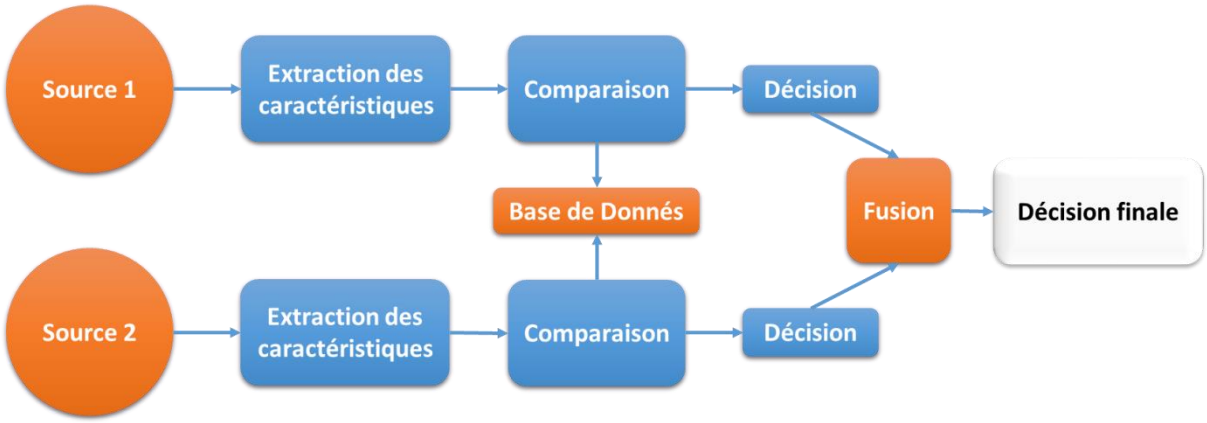


Figure II. 7Schéma de fusion au niveau de la décision

2.2.Normalisation des scores

L'objectif des méthodes de normalisation des scores est de rendre homogènes, de manière individuelle, les scores générés par les différents systèmes avant de les combiner. Certains systèmes produisent des scores de similarité, où un score élevé indique une forte ressemblance entre la référence et le test, ce qui signifie que l'utilisateur est un client. D'autres systèmes produisent des distances, où une faible distance indique une proximité entre la référence et le test, ce qui implique également que l'utilisateur est un client. [5]

2.2.1. Normalisation par la méthode Z –Score (normalisation standard)

Cette méthode transforme les scores en scores z en les centrant sur la moyenne et en les divisant par l'écart type. Cela permet de mettre les scores sur une échelle commune et de rendre leur distribution normale. Ainsi, les scores z peuvent être comparés et fusionnés plus facilement. [5]

$$z = \frac{(x - \mu)}{\sigma}$$

Où z est le score normalisé, x est le score brut, μ est la moyenne des scores et σ est l'écart type des scores. [5]

2.2.2. Normalisation par la méthode Min-Max :

Cette méthode redimensionne les scores sur une échelle commune en utilisant la plage des valeurs minimale et maximale. Les scores sont linéairement transformés pour correspondre à l'intervalle spécifié (par exemple, de 0 à 1). Cela permet de normaliser les scores de différentes modalités dans la même plage et de faciliter leur comparaison. [5]

$$z = \frac{x - min}{\max - min}$$

Où z est le score normalisé, x est le score brut, min est le score minimum et max est le score maximum. [5]

2.2.3. Normalisation Analyse discriminante linéaire probabiliste(PLDA) :

Cette méthode est basée sur l'analyse discriminante linéaire probabiliste. Elle modélise les scores de chaque modalité à l'aide de distributions probabilistes et normalise les scores en fonction de ces modèles. Cela permet de rendre les scores comparables et d'effectuer une fusion plus précise. [5]

$$z = W * (x - \mu)$$

Où z est le score normalisé, x est le score brut, μ est le vecteur moyen des scores, et W est la matrice de projection apprise à partir des modèles probabilistes. [5]

2.2.4. Normalisation par la médiane et l'écart absolu médian (MAD) :

La méthode est robuste, mais les estimateurs basés sur la médiane et l'écart absolu médian (MAD) sont moins efficaces que ceux basés sur la moyenne et l'écart-type. En d'autres termes, lorsque la distribution des scores n'est pas gaussienne, la médiane et le MAD sont de mauvais estimateurs des

paramètres de position et d'échelle. Par conséquent, cette technique de normalisation ne préserve pas la distribution d'entrée et ne transforme pas les scores dans un intervalle commun. [5]

$$x_{normalisé} = \frac{c - mediane}{MAD}$$

II.6. Conclusion

En conclusion, le système biométrique multimodal et la fusion des données constituent une approche prometteuse pour améliorer la précision et la fiabilité de l'identification biométrique. En utilisant plusieurs modalités biométriques et en fusionnant les données de manière appropriée, le système peut surmonter les limitations individuelles des modalités et fournir des performances plus élevées en termes de reconnaissance et d'identification des individus. Cependant, des défis techniques et des considérations de sécurité doivent être pris en compte lors de la conception et de la mise en œuvre de tels systèmes.

Chapitre III :

Résultats expérimentaux

Introduction

Dans ce chapitre, nous allons présenter une technique d'extraction de caractéristiques basée sur MS-LBP (Multiscale Local Binary Pattern) pour faire la conception et évaluation d'un système d'authentification biométrique basé sur l'empreinte palmaire. La base de données d'empreintes palmaires de PolyU multispectrales a été utilisée pour évaluer les performances du système. Dans ce chapitre, nous présenterons les résultats expérimentaux de notre système de biométrie d'authentification basé sur LBP (Local Binary Patterns) multiscale. Les expériences que nous avons menées visaient à évaluer les performances de notre système en utilisant à la fois des approches uni-modales et multimodales.

III.1. LBP MULTI-ÉCHELLE HIÉRARCHIQUE

LBP est un opérateur de texture en niveaux de gris qui caractérise la structure spatiale locale de la texture de l'image. Étant donné un pixel central dans l'image, un code de motif est calculé en le comparant à ses voisins :

$$LBP_{P,R} = \sum_{p=0}^{p-1} s(g_p - g_c)2^P$$

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

où g_c est la valeur de niveau gris du pixel central, g_p est la valeur de ses voisins, P est le nombre total de voisins impliqués et R est le rayon du voisinage. Supposons que la coordonnée de g*c* soit (0, 0), alors les coordonnées de g_p sont (R*cos(2πp/P),R*sin(2πp/P)). La figure 1 donne

des exemples d'ensembles voisins à symétrie circulaire pour différentes configurations de (P,R). Les valeurs de gris des voisins qui ne sont pas au centre des grilles peuvent être estimées par interpolation.

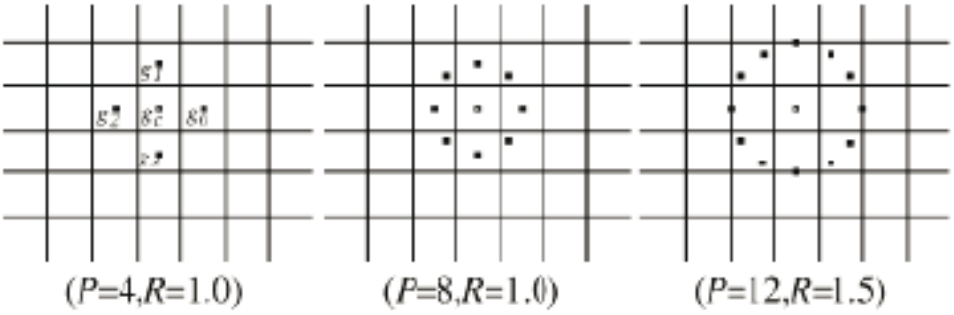


Figure III. 1Ensembles voisins à symétrie circulaire pour différents (P, R).

Dans l'approche du LBP multi-échelles (MLBP), une image est analysée en utilisant des fragments de P-voisins. Chaque fragment est considéré comme un cercle de rayon R, qui englobe les pixels voisins de chaque pixel de l'image. Chaque pixel $(g_i|P_{i=0})$ dans le voisinage de P pixels est converti en une valeur binaire, soit 0 soit 1, en fonction de la valeur de son centre (g_c) utilisée comme seuil. En conséquence, les P voisins sont représentés sous forme d'un mot de code binaire. Pour représenter le descripteur LBP, le mot de code binaire obtenu pour chaque pixel est décodé en utilisant l'ensemble des puissances de la base 2 :

$$LBP_{P,R}(x,y) = \sum_{i=0}^{P} s(g_p - g_c) \times 2^i, x, y = 1, \cdots H, W$$

La valeur LBP du pixel à x, y est représentée par $LBP_{P,R}(x,y)$, où $s(\alpha)$ est égale à α si $\alpha \geq 0$, sinon elle est égale à 0. Pour chaque fragment, les coordonnées de g_c sont (0,0), et les coordonnées de chaque g_p sont calculées en utilisant les formules $(R \cdot \cos\left(\frac{2\pi p}{P}\right), R \cdot \sin\left(\frac{2\pi p}{P}\right))$. La dernière étape de la méthode d'extraction de caractéristiques basée sur LBP consiste à créer un vecteur de caractéristiques sous forme d'un histogramme (H).

$$H(k) = \sum_{i=1}^{H} \sum_{j=1}^{W} F_{HIST}(LBP_{P,R}(i,j), k), k \in [0, K]$$

où FHIST$F_{HIST}(\alpha, \beta) = 1\ si\ \alpha = \beta$ et 0 sinon et K désigne la valeur maximale du modèle LBP.

Lors de la rotation de l'image, tous les pixels P se déplacent également le long du périmètre du cercle formé par le rayon R. Cette rotation provoque un décalage circulaire du nombre binaire

résultant, résultant en un nombre décimal $LBP_{P,R}$ différent. Pour cela, un opérateur invariant en rotation est appliqué pour surmonter cet effet.

$$LBP_{P,R}^{ri}(x,y) = min\{F_{ROT}(LBP_{P,R}(x,y),\ell)\}$$

tant que $\ell \in [0 \cdots P-1]$,L'opérateur circulaire de décalage à droite, représenté par $F'_{HIST}(\beta, l)$, effectue un décalage de β positions vers la droite au niveau du bit ℓ. Cependant, les opérateurs $LBP_{P,R}$ et $LBP_{P,R}^{ri}$ ne permettent pas toujours une bonne discrimination en raison de l'apparition de fréquences spécifiques dans les motifs individuels. Pour améliorer leur capacité de discrimination, un nouvel opérateur a été proposé, qui capture les propriétés fondamentales du motif. En pratique, les motifs fondamentaux sont déterminés en fonction du nombre de transitions spatiales ($0 \rightarrow 1\ or/and\ 1 \rightarrow 0$) présentes dans le motif. Cette méthode est définie par...

$$U(LBP_{P,R}) = |s(g_{p-1} - g_c) - s(g_0 - g_c)| + |s(g_p - g_c) - s(g_{p-1} - g_c)|$$

En utilisant l'équation 3, les modèles fondamentaux de la texture locale de l'image, notés $LBP_{P,R}^{u2}$, peuvent être définis comme des modèles présentant une transition ou des discontinuités limitées

(U ≤ 2) dans une représentation binaire circulaire. En général, le descripteur LBP est calculé à plusieurs échelles (LBP multi-échelles) en utilisant différents paramètres de R et P. Ensuite, les histogrammes obtenus sont concaténés en un seul histogramme, qui représente la caractéristique de l'image.

$$H'_{IMG} = \bigotimes_{i=0}^{k} H'_i, H'_i = H'^{(P,R)}$$

La fonction de concaténation, représentée par ⊗, est utilisée pour combiner différentes parties. L'histogramme de l'image entière est représenté par H'_{IMG}. Le nombre d'échelles, c'est-à-dire le nombre de couples (P, R), est noté k. Chaque histogramme individuel obtenu avec les paramètres P_i et R_i est représenté par $H'(P_i,R_i)$. [20]

III.2. Résultats expérimentaux

III.2.1. Base de données d'empreintes palmaires

La base de données d'images d'empreintes palmaires multispectrales PolyU comprend 6000 images obtenues à partir de 500 paumes différentes pour chaque bande à l'aide d'un dispositif de capture d'images d'empreintes palmaires conçu par des chercheurs de l'Université polytechnique de Hong Kong décrit dans. La base de données multispectrale contient des images d'empreintes palmaires multispectrales recadrées de quatre bandes différentes (rouge, vert, bleu et NIR) illustrées à la figure 3.1. Les images ont été collectées en deux sessions distinctes à un intervalle de temps d'environ deux mois. Dans chaque session, la personne fournit 6 images par paume, il y a donc 12 images pour chaque personne. Par conséquent, 48 images du spectre de toute l'illumination de 2 paumes ont été recueillies auprès de chaque personne. L'intervalle de temps moyen entre la première et la deuxième session était d'environ neuf jours. De plus, toutes les images de la paume sont en basse résolution \ 150 dpi stockées sous forme d'images en niveaux de gris 8 bits par bande avec des dimensions de 128 128.[22]

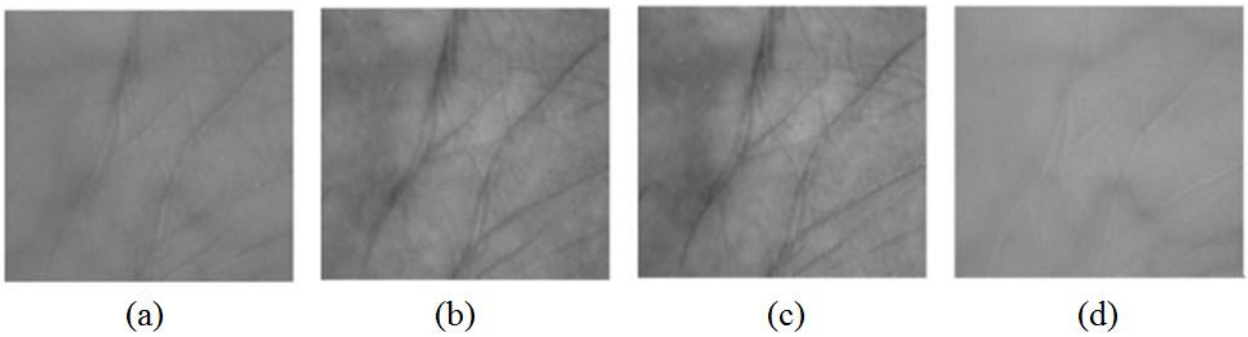


Figure III. 2 Échantillons de ROI d'empreintes palmaires de la base de données multispectrale PolyU. a Rouge, b Vert, c Bleu et d NIR

III.2.2. Partie 1 : sélection de paramètre

Il s'emble difficile d'avoir un résultat exact pour un système de reconnaissance de personnes. Cela est principalement dû au choix des caractéristiques qui doivent représenter avec précision l'identité des personnes. Il est donc impératif d'évaluer les performances du système d'identification pour sélectionner les paramètres appropriés offrant les meilleurs résultats. Mathématiquement, il n'y a pas de formule magique pour déterminer directement les paramètres essentiels offrant les meilleures performances du système. En général, dans ces cas, les tests expérimentaux sont réalisés en faisant varier les différents paramètres ($[\boldsymbol{R_s}, \boldsymbol{P_s}]$) dans des ensembles prédéfinis puis en sélectionnant la combinaison qui optimise une fonction objectif.

Il faut noter que nos tests sont effectués sur un système d'identification biométrique basé sur l'empreinte de la paume, qui fonctionne en mode ensemble-ouvert.

De nombreuses expériences ont été réalisées en utilisant MLBP sur l'image de test. Dans cette expérience, nous limitons les tests pour choisir le rayon de voisinage (R) et le nombre de voisins (P).

Dans un premier temps en faisant varier le rayon de voisinage (R) le nombre de voisins (P) de l'ensemble (P,R) = (2,2), (2,4), (2,6), (4,2), (4,4), (4,6), (6,2), (6,4) et (6,6) (Niveau 1) différents vecteurs caractéristiques peuvent être obtenus. Ces test sont réalisé pour l'empreinte palmaire (PLM) et l'empreinte palmaire veineuse (PLV). Pour évaluer les descripteurs précédemment fournis, les performances du système) ont été résumées dans le tableau 1 et 2. Les réglages des paramètres pour chaque descripteur H-MLBP (R et P) se réfèrent au rayon et le nombre de voisins du LBP, respectivement. Il ressort clairement de tableau 1 et figure 3.2 que la combinaison [Rs, Ps] = [6, 6] peuvent effectivement améliorer les performances du système dans le niveau1 pour la modalité PLM avec *EER* = 055 % à T_0 = 0.28, pour PLV plusieurs combinaison donne des résultats parfaite [Rs, Ps] = [2, 2], [2, 6]. Le tableau 3 donne les meilleurs paramètres dans le 2ème niveau [Rs, Ps] = [(6,6), (6,6)] avec EER = 0.45 % à T_0 = 0.28.

$[R_s, P_s]$	[2,2]	[2,4]	[2,6]	[4,2]	[4,4]	[4,6]	[6,2]	[6,4]	[6,6]
EER%	1.601	0.77	0.94	1.11	0.77	0.60	1	1.1	**0.55**
T_0	0.1	0.18	0.22	0.128	0.25	0.25	0.17	0.309	**0.28**

Tableau III. 1 PERFORMANCES DU SYSTÈME H-MLBP (Niveau 1 pour PLM)

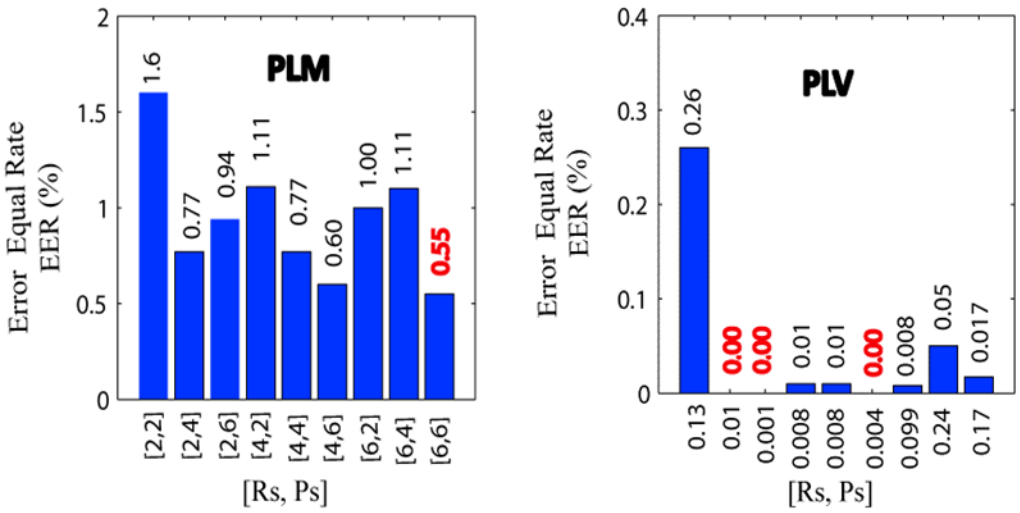


Figure III. 3 Résultats expérimentaux des sélections de paramètres (choix empirique du meilleur type de nombre de coefficients (P et R) se réfèrent au rayon et le nombre de voisins du LBP (Niveau1).

$[R_s, P_s]$	[2,2]	[2,4]	[2,6]	[4,2]	[4,4]	[4,6]	[6,2]	[6,4]	[6,6]
EER	0.26	**0**	**0**	0,01	0.01	**0**	0,008	0,05	0,017
T_0	0,13	**0.01**	**0.001**	0.088	0,088	**0,004**	0,099	0,24	0,17

Tableau III. 2PERFORMANCES DU SYSTÈME H-MLBP (Niveau 1 pour PLV)

$[R_s]$	[6,2]	[6,2]	[6,2]	[6,4]	[6,4]	[6,4]	[6,6]	[6,6]	[6,6]
$[P_s]$	[6,2]	[6,4]	[6,6]	[6,2]	[6,4]	[6,6]	[6,2]	[6,1]	[6,6]
EER%	0,66	0,77	0,88	1	0,66	1	0,66	0,77	**0,45**
T_0	0,3	0,31	0,32	0,17	0,31	0,17	0,3	0,32	**0.28**

Tableau III. 3PERFORMANCES DU SYSTÈME H-MLBP (Niveau 2 pour PLM)

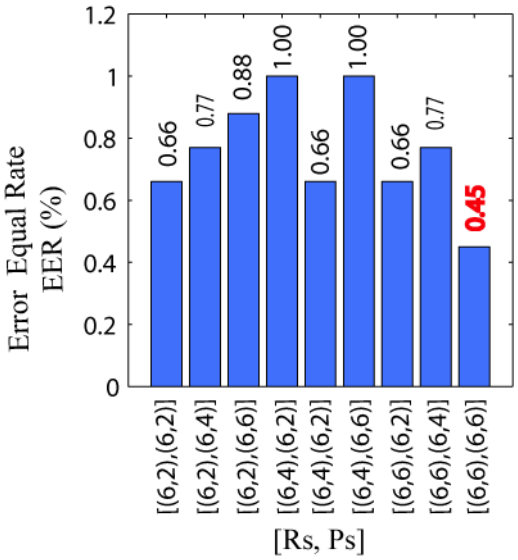


Figure III. 4 Résultats expérimentaux des sélections de paramètres (choix empirique du meilleur type de nombre de coefficients (P et R) se réfèrent au rayon et le nombre de voisins du LBP (Niveau2).

III.2.3. Partie 02 : Système uni-modal

En fonction du niveau de sécurité des applications et des performances du dispositif utilisé pour mettre en œuvre le système d'identification biométrique, on peut choisir la configuration appropriée, qui permet d'atteindre l'objectif souhaité. Ainsi, pour construire un système unimodal efficace, basé sur une seule modalité, nous devons sélectionner soigneusement les paramètres appropriés qui donnent les meilleures performances.

Dans ce système d'authentification, Nous avons effectué une étude sur deux types d'images pour représenter les empreintes palmaires : des images en niveau de gris (NG : PLM) et des images infrarouges (NIR : PLV).

Base de donné	T_0	EER
PLM	0.25	0.55
PLV	0.067	0

Tableau III. 4PERFORMANCES DU SYSTÈME UNIMODAL

En observant ce tableau, On note que la base d'images NIR présente une performance supérieure par rapport la base d'images en niveau de gris. Dans ce scénario, le système fonctionne avec une erreur minimale, atteignant un EER de 0%.

La figure 3.5 montre les courbes caractéristiques (Receiver Operating Characteristic (ROC)) du système, en utilisant quatre bandes des empreintes palmaires. Il est clair, d'après cette figure, que la bande NIR offre le meilleure EER (EER = 0%) avec un seuil To= 0.067, en comparaison avec les autres.

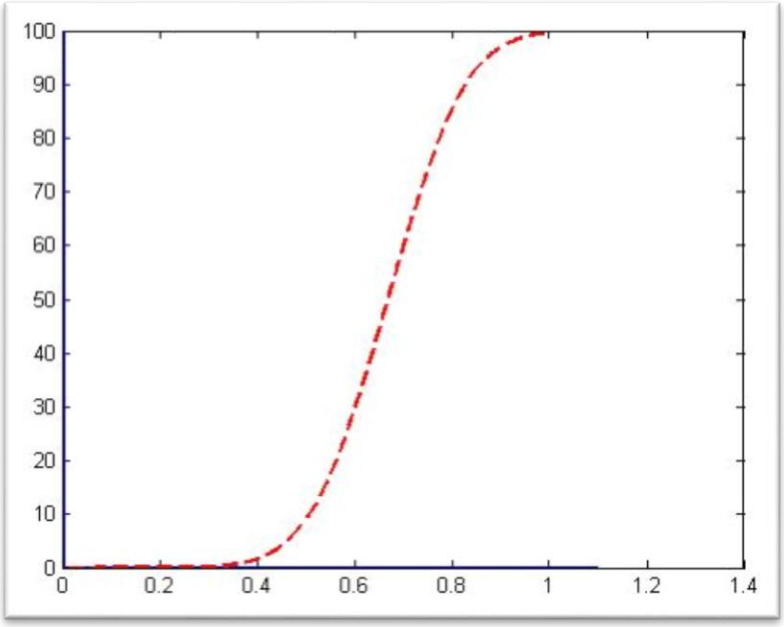


Figure III. 5 Performance d'un système uni-modal PLM

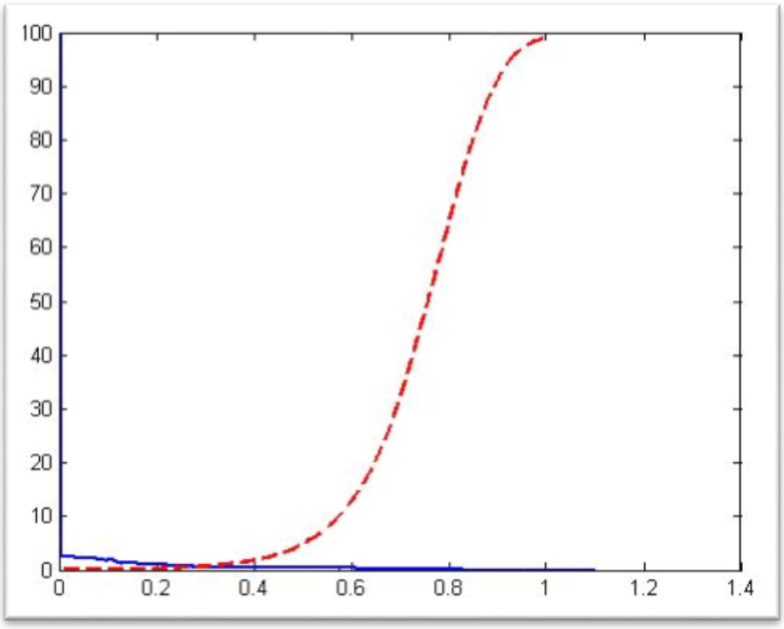


Figure III. 6 Performance d'un système uni-modal PLV

III.2.4. Partie 3 : Système multi modale

Afin d'améliorer nos résultats, nous allons combiner les scores provenant de différentes bases d'images pour créer un système multimodal. Le schéma de principe du système proposé est illustré dans le tableau 5. Cette approche de fusion vise à renforcer la performance globale du système.

Nous allons appliquer une fusion biométrique en combinant les deux bandes NIR et NG de l'empreinte palmaire dans toutes les orientations. Dans notre méthodologie, nous avons fusionné deux représentations différentes de l'empreinte palmaire au niveau des scores en utilisant des règles telles que la somme, la moyenne, le maximum, le minimum, la somme pondérée et la multiplication. Cette approche de fusion permet d'exploiter pleinement les informations des deux modalités pour améliorer la performance du système.

Tableau III. 5 PERFORMANCES DU SYSTÈME MULTIMODAL

	T_0	EER
SUM	0.09	0.008
MUL	0.0009	0.02
MIN	0.0009	0.02
MAX	0.3	0.2

WHT	0.09	0.008

Dans ce tableau, nous remarquons que la fusion donnés un bon résultat avec la règle SuM. Dans ce cas, le système fonctionne avec une erreur minimale égale à EER= 0.008% en même temps que le seuil To = 0.09.

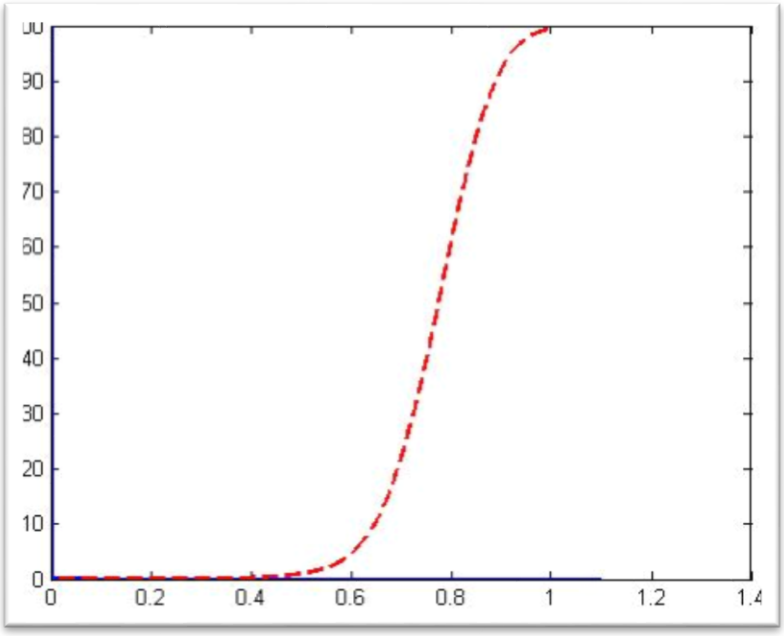


Figure III. 7 PERFORMANCES DU SYSTÈME MULTIMODAL

III.3. Conclusion

Nous avons implanter dans ce travail, une méthode d'extraction de caractéristiques, dont le rôle est d'analyser la texture de l'image, est proposée pour extraire uniquement la caractéristique d'image discriminante afin qu'elle soit utilisée pour la tâche de reconnaissance. En effet, cette méthode MS-LBP peut donner des vecteurs de traits distinctifs qui peut résoudre le problème de variation de l'angle.

CONCLUSION GENERAL

CONCLUSION GENERAL

Le travail exposé dans cette mémoire s'inscrit dans le champ de l'identification automatisée des personnes en se basant sur leurs caractéristiques biométriques. Nous avons employé deux caractéristiques biométriques, spécifiquement l'empreinte de la paume et le réseau veineux, pour concevoir nos systèmes biométriques, qu'ils soient uni modaux ou multimodaux. Après avoir introduit les concepts généraux de la biométrie, nous avons étudié l'état de l'art des technologies biométriques. Nous avons également exposé la structure globale d'un système d'identification biométrique.

Par conséquent, l'objectif principal était de concevoir un système biométrique résistant garantissant une identification fiable des individus. L'utilisation simultanée de différentes modalités biométriques permet d'améliorer les performances du système d'identification. Toutefois, la performance du système demeure sensible aux caractéristiques extraites des modalités biométriques. Un choix judicieux de la méthode d'extraction des caractéristiques permet de répondre à ce critère. C'est dans ce contexte que notre contribution a été proposée. Ainsi, nous avons formulé une représentation basée sur une méthode d'extraction des caractéristiques inédite. Les résultats expérimentaux démontrent que cette représentation offre un taux d'identification très satisfaisant (EER = 0,00% pour le réseau veineux), avec une base de données de taille moyenne. Cette performance est celle qui est requise dans les applications nécessitant une sécurité très élevée.

En tenant compte des conclusions tirées de notre travail réalisé dans le cadre de cette thèse, nous envisageons d'adopter d'autres méthodes pour l'extraction des caractéristiques des modalités biométriques dans nos futurs travaux. Par exemple, l'apprentissage profond (deep learning) pourrait être exploité afin d'obtenir un vecteur de caractéristiques très efficace.

BIBLIOGRAPHIE

[1] M. El-Abed, Évaluation de système biométrique, Université de Caen: HAL Id: tel-01007679, 2011.

[2] A. K. R. A. &. P. S. Jain, «An introduction to biometric recognition.,» *IEEE* , pp. 4-20, 2004.

[3] F. LAMARE, OCT en phase pour la reconnaissance biométrique OCT en phase pour la reconnaissance biométrique, Paris: École doctorale : Informatique, Télécommunications et Électronique de Paris, 2016.

[4] F. MASSICOTTE, A BIOMÉTRIE, SA FIABILITÉ ET SES IMPACTS SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE, MONTRÉAL: UNIVERSITÉ DU QUÉBEC À MONTRÉAL, 2007.

[5] A. MERAOUMIA, Modée de Markov caché appliqué à la multi-biométrie, Alger: UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOMEDIENNE, 2014.

[6] T. S. BENOUAER Aichouche, Système biométrique basé sur les motifs locaux binaires orientés (LBPθ), OUARGLA: UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[7] D. &. J. A. Zhang, Advances in Biometric Person Authentication, Springer, 2004.

[8] S. &. J. A. Li, Handbook of Face Recognition (2nd ed.)., Springer, 2011.

[9] A. M. A. K. B. Raju Halder, «Limitations and Challenges in Unimodal Biometric Systems: A Comprehensive Review,» *International Journal of Computer Applications,* vol. Volume 117, n° %1No. 8, 2015.

[10] B. D. e. al., ACM Transactions on Computer-Human Interaction, 2011.

[11] S. Oviatt, The Human-Computer Interaction Handbook, 2007.

[12] W. e. al, Proceedings of the IEEE, 1998.

[13] S. Oviatt, Communications of the ACM, 1999.

[14] J. T. M. a. M. A. A.-R. H. T. Nguyen, «Data Fusion: Definitions and Architectures,» *Proceedings of the IEEE*, vol. Vol. 88, n° %1 No. 7, 2000.

[15] D. L. H. L. N. C. a. R. A. J. James Llinas, «Multisensor Data Fusion: A Review of the State-of-the-Art,» *Proceedings of the IEEE,* vol. Vol. 85, n° %1No. 1, 1997.

[16] S.Benkhaira, «Systèmes multimodaux pour l'identification et l'authentification biométrique Mémoire de Magister,» Universite 20 aout 1955-Skikda, 2010 .

[17] H. Guesmi, Identification de personnes par fusion de differentesmodalites biometriques, Universite Europeenne De Bretagneen Habilitation Conjointe Avec L'universite De Sfax, 2014.

[18] H. F. Y. Y. Lin K.M., Second International Conference on Advances in Swarm Intelligence-ICSI, Heidelberg, Germany, 2011.

[19] K. N. a. A. K. J. S. Dass, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, 2005.

[20] M. e. a. Mebarkia, Hierarchical Multiscale Local Binary Pattern For Better Osteoporosis Detection, IEEE, 2021.

[21] «Multimodal Biometric Systems: A Comprehensive Survey,» *Arun Ross, Anil K. Jain, and Sharath Pankanti,* vol. Vol. 37, n° %1No. 2, 2004.

[22] The Hong Kong Polytechnic University, PolyU MSP Database, http://www.comp.polyu.edu.hk/sbiometrics/MultispectralPalmprint/MSP.htm.