

Mémoire de Master IA4IOT

Identification des personnes par les empreintes digitales

Encadrante :



Mme Kaid Slimane

Présenté par :



Aziz Nassim



Badlis Adel Nadir

Année universitaire : 2024/2025

Dédicaces

À nos parents, pour leur soutien indéfectible, leur amour inestimable et les sacrifices qu'ils ont consentis pour nous permettre d'avancer.

À nos familles respectives, pour leur patience, leurs encouragements et leur foi en nous.

À nos enseignants, pour la transmission de leur savoir, leur disponibilité et leur exigence, qui nous ont guidés tout au long de notre formation.

À nos camarades et amis, pour leur présence, leur entraide et les moments de partage qui ont enrichi notre parcours académique.

Remerciements

Nous souhaitons exprimer nos sincères remerciements à toutes les personnes qui ont contribué, de près ou de loin, à l'élaboration de ce mémoire.

Nos remerciements les plus chaleureux vont à Madame Kaid Slimane, notre encadrante, pour son accompagnement rigoureux, sa disponibilité et la qualité de ses conseils tout au long de ce travail.

Nous remercions également l'ensemble des enseignants du département MI de la Faculté des Sciences Exactes et de l'Informatique de l'Université Abdelhamid Ibn Badis de Mostaganem, pour l'enseignement de qualité qu'ils nous ont dispensé au fil des années.

Nous tenons aussi à remercier nos collègues et amis, pour leur soutien moral, leurs échanges enrichissants et leur bienveillance.

Enfin, nous exprimons notre reconnaissance à nos familles, véritables piliers de notre réussite, pour leur amour, leur patience et leur présence constante tout au long de notre parcours.

Sommaire

• Résumé	7
• Introduction générale	8
Chapitre 1 : Introduction à la Biométrie	
1.1 Introduction	11
1.2 Définition de la biométrie	11
1.3 Modalités biométriques.....	13
1.4 Méthodes biométriques.....	14
1.4.1 Analyse morphologique.....	14
1.4.2 Analyse comportementale.....	17
1.4.3 Analyse biologique	21
1.4.4 Modalité expérimentale	22
1.5 Fonctionnement d'un système biométrique	22
1.5.1 Authentification	23
1.5.2 Identification.....	23
1.6 Conclusion	26
Chapitre 2 : Reconnaissance par Empreintes Digitales	
2.1 Historique	28
2.2 Définition et structure	29
2.3 Empreinte digitale.....	31
2.3.1 Explication d'empreinte digitale.....	31
2.3.2 Propriétés d'empreinte digitale.....	32
2.4 Processus de reconnaissance.....	34
2.5 Technologies employées	34
2.5.1 Conversion en niveaux de gris.....	35
2.5.2 Seuillage (Binarisation).....	36
2.5.3 Squelettisation	36
2.6 Limites et solutions	37
2.7 Classification	38
2.8 Conclusion.....	39
Chapitre 3 : Mise en œuvre et résultats	
3.1 Introduction	41
3.2 Base de données SOCOFing.....	41
3.3 Répartition des données.....	42
3.4 Environnement	43
3.4.1 Outils de développement.....	43
3.5 Le système	44
3.5.1 Importation des bibliothèques	44
3.5.2 Prétraitement des images.....	44

3.5.3 Définition du modèle CNN (encodeur)	45
3.5.4 Chargement de l’empreinte	45
3.5.5 Chargement de la base de données	45
3.5.6 Lancement du test	46
3.6 Résultats obtenus	46
3.7 Conclusion	48
• Conclusion générale.....	49
• Bibliographie	50

Liste de figures

Figure N°	Titre de la figure	Page
1.1	<i>Différentes modalités biométriques</i>	12
1.2	<i>Catégories des méthodes biométriques</i>	14
1.3	<i>La reconnaissance de visage</i>	15
1.4	<i>La reconnaissance de l’empreinte digitale</i>	15
1.5	<i>Géométrie de la main</i>	16
1.6	<i>L’iris</i>	17
1.7	<i>La signature</i>	18
1.8	<i>La reconnaissance vocale</i>	19
1.9	<i>Image de frappe au clavier</i>	19
1.10	<i>La démarche (capteur de sol)</i>	20
1.11	<i>L’ADN</i>	21
1.12	<i>Image du système de configuration des veines</i>	21
1.13	<i>Cartographie thermique du visage d’un homme</i>	22
1.14	<i>Diagramme Cas d’utilisation</i>	24
1.15	<i>Diagramme de séquence</i>	25
2.1	<i>Francis Galton</i>	28
2.2	<i>Organigramme du système d’identification par empreinte digitale</i>	30
2.3	<i>Points singuliers globaux</i>	32
2.5	<i>La terminaison et la bifurcation</i>	33
2.6	<i>Architecture d’un système biométrique basé sur l’empreinte</i>	34
2.7	<i>Conversion niveaux de gris</i>	35
2.8	<i>Binarisation</i>	36
2.9	<i>Squelettisation de l’empreinte digitale</i>	36
2.10	<i>Calcul de minutie</i>	37
3.1	<i>Quelques images de la base de données SOCOFing</i>	41

Résumé

Dans le contexte actuel où la sécurité prend une place croissante, les technologies d'identification biométrique s'imposent comme des solutions de référence. Ce mémoire porte sur l'étude du fonctionnement des systèmes de reconnaissance par empreintes digitales. Nous explorons les étapes fondamentales de ce type de système : le prétraitement, l'extraction des caractéristiques et la classification. Chaque phase est détaillée et mise en œuvre à l'aide d'une base de données réelle afin d'illustrer concrètement le processus de reconnaissance.

Introduction générale

À l'ère du numérique, les avancées technologiques rapides et l'augmentation des menaces informatiques ont placé la sécurité des systèmes d'information au cœur des priorités. Dans ce contexte, concevoir des mécanismes d'identification à la fois fiables, performants et résistants aux attaques est devenu un enjeu fondamental pour les chercheurs et les professionnels de la cybersécurité.

L'identification des individus est en effet un pilier essentiel de la protection des systèmes informatiques et des infrastructures sensibles. Elle consiste à confronter les données fournies par un utilisateur à une base de référence afin de vérifier son identité. Cette démarche permet notamment de contrôler l'accès à des espaces restreints ou à des services sécurisés. À titre d'exemple, dans des zones à accès réglementé, seules les personnes préalablement enregistrées peuvent être autorisées. De même, les forces de l'ordre exploitent ces technologies à des fins judiciaires, notamment pour reconnaître des suspects ou authentifier des empreintes. Parmi les techniques d'identification, l'empreinte digitale occupe une place de choix en raison de sa fiabilité et de sa longue histoire. Elle était déjà utilisée dans la Chine ancienne, où l'empereur Ts-In-She, dès le II^e siècle av. J.-C., validait certains documents à l'aide de ses empreintes. Cette méthode s'est perpétuée en Chine et au Japon jusqu'au XIX^e siècle, notamment dans le cadre de transactions commerciales.

L'étude scientifique des empreintes digitales a débuté au XVII^e siècle. En 1684, Nehemiah Grew en proposa une première analyse descriptive. Peu après, Marcello Malpighi les observa au microscope, avant que Johannes Purkinje, en 1823, n'établisse une classification des motifs en neuf types distincts. Ces premières recherches furent approfondies au XIX^e siècle : William James Herschel observa leur stabilité tout au long de la vie, tandis qu'Henry Faulds mit en évidence leur unicité. En 1892, Francis Galton confirma scientifiquement que les empreintes digitales permettent d'identifier de manière fiable les individus, jetant ainsi les bases de la biométrie moderne.

Historiquement associée à l'anthropométrie, la biométrie s'est d'abord imposée dans les milieux policiers et judiciaires. Grâce à l'efficacité des empreintes digitales, ces méthodes ont été largement

adoptées pour l'identification des criminels. Aujourd'hui encore, elles restent incontournables dans de nombreux dispositifs de sécurité.

L'identification biométrique, fondée sur l'analyse de traits physiologiques ou comportementaux, connaît ainsi une croissance significative. Les progrès dans les domaines du traitement du signal, de l'intelligence artificielle et de l'imagerie ont fortement contribué à cette expansion. De plus, les événements géopolitiques majeurs du début du XXI^e siècle, tels que les attentats du 11 septembre 2001, ont suscité un intérêt accru des gouvernements pour ces technologies, dans le but de renforcer les dispositifs de sécurité à l'échelle nationale et internationale.

Ce mémoire propose une exploration approfondie de la biométrie, en mettant l'accent sur la reconnaissance par empreintes digitales. Nous commencerons par introduire les concepts fondamentaux et les différentes modalités biométriques, ainsi que l'architecture générale d'un système de reconnaissance. Ensuite, nous nous concentrerons sur l'empreinte digitale, en détaillant les étapes de traitement nécessaires à son exploitation : prétraitement, extraction des caractéristiques et classification. Enfin, nous présenterons le système que nous avons développé, les résultats obtenus à partir de bases de données réelles, et une évaluation critique de ses performances.

La structure du mémoire est organisée comme suit :

- **Chapitre 1 :** Vue d'ensemble de la biométrie, son évolution, ses fondements théoriques et ses différentes modalités. Une attention particulière sera portée sur l'architecture d'un système biométrique et à ses domaines d'application.
- **Chapitre 2 :** Étude spécifique de l'empreinte digitale comme modalité biométrique, avec une description des étapes de traitement de l'image et des algorithmes utilisés.
- **Chapitre 3 :** Présentation du système développé, des données utilisées, des résultats expérimentaux et d'une analyse critique des performances observées.

Chapitre 1 : Introduction à la Biométrie



1.1 Introduction

Dans un contexte marqué par la mondialisation numérique et l'intensification des échanges, assurer une identification fiable des individus constitue un enjeu stratégique majeur en matière de sécurité. Face à cette exigence, les technologies biométriques s'imposent comme une réponse efficace, en exploitant les caractéristiques physiques propres à chaque personne pour garantir une vérification d'identité rigoureuse [8], [9].

Autrefois réservée à la fiction et popularisée par le cinéma, la biométrie fait désormais partie intégrante de la vie courante. Elle est utilisée tant dans les dispositifs de sécurité institutionnels que dans les équipements personnels, tels que les smartphones ou les systèmes domotiques. Dans un tel contexte d'adoption généralisée, il devient essentiel de clarifier les principes fondamentaux de cette technologie, d'examiner les différentes modalités existantes et d'évaluer leur pertinence en fonction des besoins et des environnements d'application.

1.2 Définition de la biométrie :

Le terme biométrie tire ses origines du grec ancien, *bios* signifiant « vie » et *metron* signifiant « mesure ». Il désigne un ensemble de techniques permettant de mesurer, d'analyser et d'exploiter les particularités propres à chaque individu dans le but de l'identifier ou de confirmer son identité[9], [20]. Ces technologies se déclinent principalement en deux grandes catégories : la biométrie physique, qui repose sur des attributs corporels immuables tels que les empreintes digitales, l'iris ou les traits du visage, et la biométrie comportementale, qui étudie des gestes ou des habitudes spécifiques, comme la dynamique de la signature manuscrite ou la frappe au clavier. Tandis que la biométrie physique peut être utilisée à la fois pour l'identification et l'authentification, la biométrie comportementale est généralement réservée à la vérification d'identité.

Sur le plan pratique, la biométrie est définie comme un processus d'identification automatisé, fondé sur des données personnelles distinctives, mesurables et difficilement reproductibles. Qu'elles soient physiologiques ou comportementales, ces données permettent de distinguer de manière fiable un individu au sein d'un groupe donné.

Face à l'augmentation des exigences sécuritaires, les systèmes biométriques sont de plus en plus présents dans les infrastructures modernes. Ils sont aujourd'hui intégrés dans divers domaines, allant

de l'émission de documents officiels à la surveillance des frontières, en passant par le contrôle d'accès à des espaces sensibles, le vote électronique ou la sécurisation des transactions bancaires.

En tant qu'alternative moderne aux moyens d'identification traditionnels tels que les mots de passe, les codes PIN ou les cartes d'identité, les technologies biométriques offrent une fiabilité supérieure. En exploitant des caractéristiques intrinsèques à la personne, elles permettent de valider une identité de façon directe et infalsifiable, réduisant ainsi considérablement les risques d'usurpation, de perte ou de contrefaçon.

Ainsi, la biométrie s'impose progressivement comme une solution incontournable pour garantir l'identité réelle de l'utilisateur, en apportant un niveau de sécurité et de confiance nettement supérieur aux méthodes classiques[6].

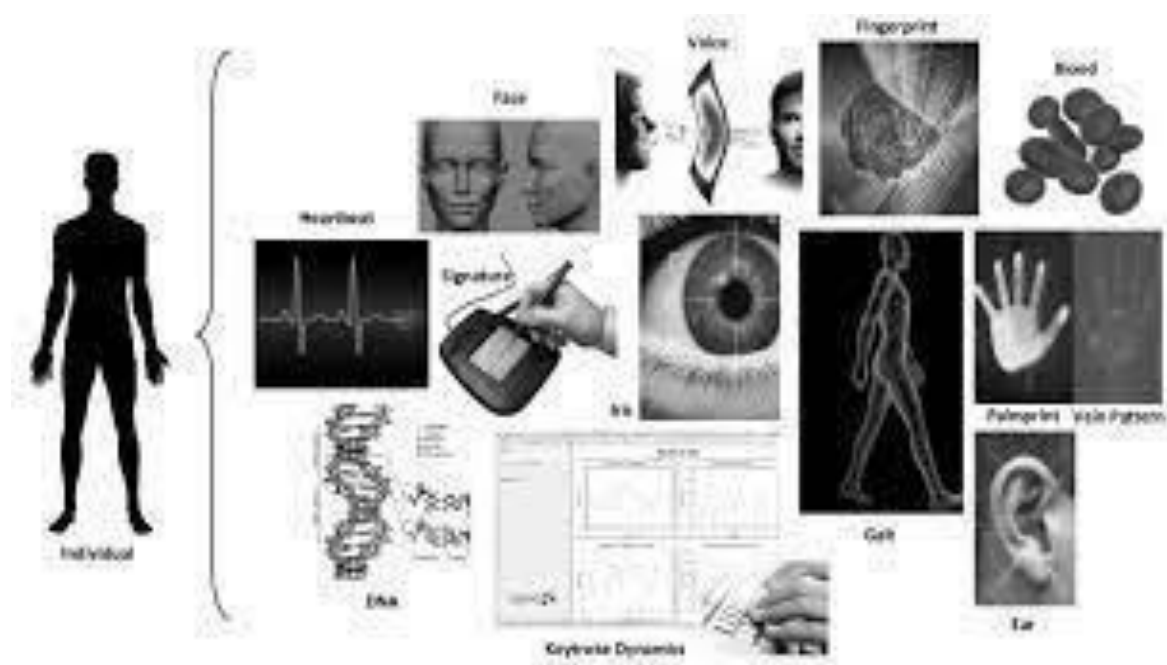


Figure 1.1 : Différentes modalités biométriques https://www.researchgate.net/figure/Some-examples-of-biometric-modalities-20_fig4_335083341

La biométrie repose sur un ensemble de méthodes bien établies, visant à identifier ou authentifier un individu à partir de ses caractéristiques personnelles, qu'elles soient physiques ou comportementales. Parmi les techniques physiologiques les plus répandues figurent la reconnaissance des empreintes digitales, l'analyse du visage en 2D ou en 3D, la lecture de l'iris et de la rétine, la reconnaissance vocale ainsi que l'imagerie du réseau veineux de la main[9], [13]. Ces approches sont complétées par des techniques comportementales, qui s'appuient sur des habitudes propres à chaque utilisateur, telles que la dynamique de la signature, le rythme de frappe au clavier, les gestes sur interfaces tactiles ou encore la manière de marcher.

Pour renforcer la fiabilité et la performance globale des systèmes biométriques, une approche dite multimodale est de plus en plus adoptée. Elle consiste à combiner plusieurs modalités biométriques dans un même dispositif[4], afin de compenser les limites individuelles de chaque méthode et d'assurer une reconnaissance plus précise, même en cas de conditions défavorables ou de données partielles. Les systèmes biométriques sont fréquemment intégrés à d'autres technologies de sécurité, telles que les cartes à puce, le chiffrement des données ou encore les techniques d'anonymisation, dans le but de renforcer leur fiabilité et d'assurer une protection accrue des informations sensibles.

Ces solutions présentent plusieurs avantages notables, qui expliquent leur adoption croissante dans des environnements variés [8] :

1. **Sécurité** : Elles permettent de limiter considérablement les risques de fraude en s'appuyant sur des données uniques et difficilement falsifiables, réduisant ainsi les incertitudes liées à l'identité de l'utilisateur.
2. **Fiabilité** : Elles renforcent la confiance des utilisateurs et des responsables systèmes, grâce à la constance et à la robustesse des mécanismes d'authentification biométrique.
3. **Simplicité d'usage** : Elles offrent une expérience utilisateur optimisée, reposant sur une interaction intuitive et sans contrainte matérielle complexe.
4. **Rentabilité** : En automatisant les processus d'identification, elles contribuent à la réduction des coûts de gestion et de maintenance, tout en augmentant l'efficacité des systèmes.

1.3 modalités biométriques :

Il existe plusieurs modalités biométriques utilisées dans divers secteurs. On peut distinguer trois catégories (figure 1.2) :

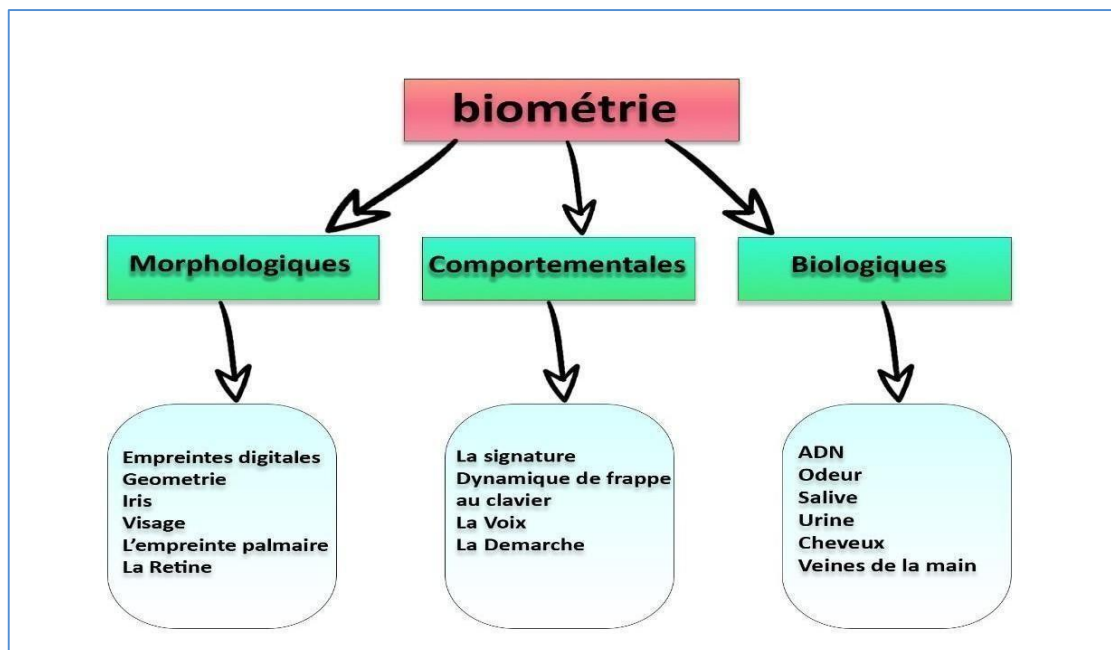


Figure 1.2 : Catégories des méthodes biométriques.

1.4. Méthodes biométriques :

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, on peut en distinguer deux catégories :

1.4.1. Analyse morphologique

Ce type de biométrie repose sur l'analyse de traits corporels distinctifs, considérés comme uniques, invariants dans le temps et propres à chaque individu. Parmi ces caractéristiques figurent notamment la structure de l'iris, le schéma vasculaire de la rétine, la morphologie de la main, les empreintes digitales, la configuration du visage, ou encore la répartition thermique du corps captée par imagerie infrarouge. Chacune de ces modalités offre un haut degré de fiabilité en matière d'identification.

a) Reconnaissance de visage

La reconnaissance faciale repose sur l'analyse de l'anatomie du visage à travers des paramètres mesurables tels que la distance interoculaire, la configuration du nez, la disposition des lèvres, ainsi que la forme du menton et des oreilles. Ces données morphologiques sont traitées par des algorithmes spécialisés qui comparent les caractéristiques extraites à celles enregistrées dans une base de données. Cette méthode est utilisée à la fois pour authentifier un individu ou pour établir son identité de manière automatisée. [9]



Figure1.3: La Reconnaissance de visage.(
<https://www.forbes.com/sites/steveandriole/2020/01/28/happy-data-privacy-day--now-read-the-new-york-times-privacy-project-about-total-surveillance/>)

b) Empreintes digitales

Parmi les méthodes d'identification biométrique, l'analyse des empreintes digitales figure parmi les plus anciennes et les plus répandues auprès du grand public. Elle occupe une place centrale dans les systèmes fondés sur des données physiologiques en raison de sa fiabilité éprouvée [10]. Chaque empreinte digitale possède une configuration propre à l'individu, considérée comme stable et inaltérable tout au long de la vie. Cette unicité explique son utilisation historique dans les contextes judiciaires et les systèmes d'identification. Sur le plan morphologique, une empreinte se compose d'un ensemble complexe de crêtes et de sillons. Ces structures forment des motifs qui, même analysés localement, conservent une signature distincte propre à chaque doigt [11].



Figure 1.4 : La reconnaissance de l'empreinte digitale.(
<https://researchoutreach.org/articles/moisture-regulation-finger-pad-ridges-ensure-optimal-grip/>)

c) Géométrie de la main

La reconnaissance par géométrie de la main s'appuie sur l'analyse de multiples paramètres anatomiques, tels que la forme générale de la main, les dimensions des doigts (longueur, largeur), la disposition des articulations et les mesures entre segments. Cette méthode utilise principalement des dispositifs à imagerie infrarouge pour capturer ces données. Reconnue pour sa simplicité d'utilisation et son caractère non intrusif, cette technique est bien acceptée par les utilisateurs. Elle présente également l'avantage de générer des fichiers légers, bien moins volumineux que ceux produits par les systèmes basés sur les empreintes digitales, avec des tailles allant généralement de 10 à 20 octets contre 250 à 1000 octets pour ces dernières. Toutefois, cette modalité présente certaines limites. La morphologie de la main peut se modifier avec le temps, en particulier en raison du vieillissement ou de blessures, ce qui affecte la stabilité des données. De plus, les dispositifs nécessaires à la capture sont relativement encombrants, ce qui complique leur intégration dans des systèmes portables [12].

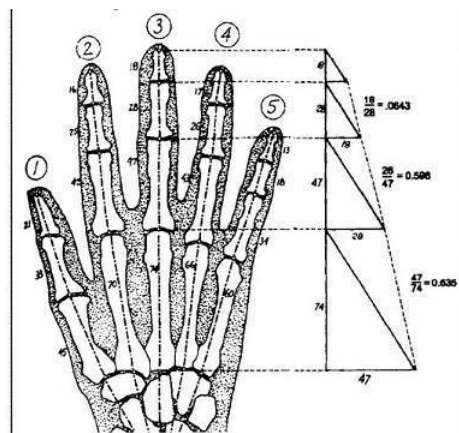


Figure 1.5 : Géométrie de la main. (<https://pin.it/5gGRumQGF>)

d) 1. L'Œil

Parmi les modalités biométriques les plus précises, l'analyse de l'œil notamment de l'iris et de la rétine occupe une place importante. L'iris, situé à l'avant de l'œil et reconnaissable à sa couleur, conserve une structure stable dès la fin de l'adolescence, ce qui en fait un identifiant fiable à long terme. Sa richesse en motifs complexes crêtes, sillons et textures uniques permet une encodation efficace pour les processus de reconnaissance. L'iris offre un haut niveau de sécurité, car il est extrêmement difficile à reproduire artificiellement[1], [13] . Par exemple, une image falsifiée ne pourrait pas tromper un capteur sophistiqué, notamment à cause de l'absence de

réaction pupillaire à la lumière, un phénomène que seuls les iris vivants présentent [13].

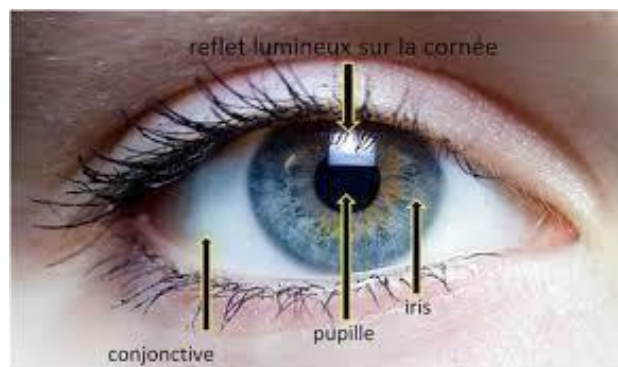


Figure 1.6 : L'iris (<https://ndgperception.weebly.com/i-le-fonctionnement-de-loeil.html>)

2. Rétine, fine membrane située au fond de l'œil, est utilisée en biométrie en raison de la complexité et de l'unicité de son réseau vasculaire. Ce maillage de vaisseaux sanguins constitue une signature biométrique extrêmement fiable, propre à chaque individu.

La reconnaissance rétinienne s'effectue à l'aide d'un dispositif d'éclairage spécifique, qui impose à l'utilisateur de positionner son œil très près du capteur. Cette exigence technique, plus contraignante que celle de l'analyse de l'iris réalisable à distance, limite son emploi dans les systèmes d'identification de personnes. En revanche, cette méthode trouve des applications intéressantes dans des domaines spécialisés, notamment dans la traçabilité animale, comme l'identification des bovins [13].

1.4.2. Analyse comportementale :

La biométrie comportementale repose sur l'observation et l'analyse de schémas d'action propres à chaque individu. Elle englobe diverses méthodes, telles que la reconnaissance de la voix, l'étude des habitudes de frappe au clavier, l'analyse de la signature manuscrite, ou encore l'examen de la démarche. Ces comportements, bien que subtils, présentent des caractéristiques suffisamment distinctives pour permettre une identification fiable.

Parallèlement, une autre branche de la biométrie se concentre sur les marqueurs biologiques. Elle exploite des éléments comme l'ADN, les fluides corporels (sang, salive, urine) ou encore l'empreinte olfactive de l'individu, qui constituent autant de signatures biologiques uniques pouvant servir à l'authentification [14].

a) **Signature**

La signature manuscrite constitue un moyen d'identification largement accepté et profondément enraciné dans les pratiques quotidiennes. Chaque personne développe, au fil du temps, un style graphique distinctif qui peut être capturé et modélisé pour permettre une reconnaissance biométrique. Cette spécificité en fait un critère exploitable[3] dans les systèmes d'authentification. En outre, la signature conserve une forte valeur juridique et administrative à l'échelle internationale, où elle est fréquemment utilisée comme preuve d'identité ou de consentement dans divers documents officiels.



Figure 1.7: La signature.(<https://www.xavierstuder.com/2023/10/voici-swisscom-sign-la-signature-numerique-du-geant-bleu/>)

a) **Reconnaissance vocale**

La reconnaissance vocale s'appuie sur une combinaison de caractéristiques physiologiques, telles que le timbre, la fréquence ou l'intonation de la voix, ainsi que de facteurs comportementaux, comme le rythme ou la vitesse d'élocution. Cette dualité confère à la voix une signature vocale propre à chaque individu.

Considérée comme l'une des approches les plus intuitives de la biométrie, cette méthode est particulièrement bien acceptée par les utilisateurs[9]. Son principal atout réside dans son caractère non intrusif : elle ne requiert aucun contact physique avec le système, ce qui facilite son intégration dans des environnements variés et en améliore l'ergonomie.



Figure 1.8 : La reconnaissance vocale.(<https://industrywired.com/elearning-mobile-app-how-children-benefit-from-this-modern-approach/>)

b) **Frappe du clavier**

Cette technique d'authentification biométrique repose sur l'analyse du rythme de frappe au clavier, propre à chaque individu. Il s'agit d'une solution purement logicielle ("Software-Only"), qui renforce la sécurité des mots de passe en les rendant beaucoup plus difficiles à imiter. Lors de l'enregistrement, l'utilisateur doit saisir son mot de passe une dizaine de fois. Un algorithme analyse alors le temps d'appui sur chaque touche et l'intervalle entre les frappes, puis établit un profil de frappe unique, qui servira de référence. Lors des connexions ultérieures, la saisie du mot de passe est comparée au profil enregistré. L'accès est accordé en fonction du niveau de correspondance entre les deux profils. Selon le seuil de tolérance défini par l'administrateur, le système peut être plus ou moins strict dans l'autorisation de l'accès [15].



Figure 1.9 : image de de frappe au clavier.(<https://www.tribuneindia.com/news/delhi/delhi-computer-trainer-surpasses-master-blaster-sachin-tendulkars-number-of-guinness-world-records/>)

c) **Démarche**

L'évolution constante des technologies biométriques a ouvert la voie à des approches innovantes, parmi lesquelles figure la reconnaissance fondée sur la silhouette et la démarche d'un individu. Cette méthode s'appuie sur l'analyse de la façon dont une personne se déplace, en prenant en compte des paramètres tels que la vitesse de marche, l'accélération, et la

coordination des mouvements corporels. L'identification s'effectue à partir de séquences d'images capturant le mouvement, permettant ainsi de modéliser un schéma de déplacement propre à chaque individu. La démarche étant intimement liée à la structure musculaire et à la morphologie corporelle, elle présente un haut degré de singularité, bien que certains facteurs externes (comme les vêtements) puissent en altérer la fiabilité. Étroitement liée à la morphologie corporelle et à la configuration musculaire de l'individu, la démarche constitue un trait distinctif difficilement reproductible. Elle peut donc servir de critère pertinent pour l'identification biométrique. Toutefois, sa précision peut être compromise par certains facteurs externes, notamment le port de vêtements amples ou encombrants, qui altèrent la perception des mouvements [16].

L'analyse de la marche repose sur deux grandes catégories de paramètres :

- **Les paramètres cinématiques**, qui incluent les mouvements des articulations, notamment au niveau du genou et de la cheville, ainsi que les angles formés pendant la marche.
- **Les paramètres spatiotemporels**, tels que la longueur et la largeur des pas, ainsi que la vitesse de déplacement [17].

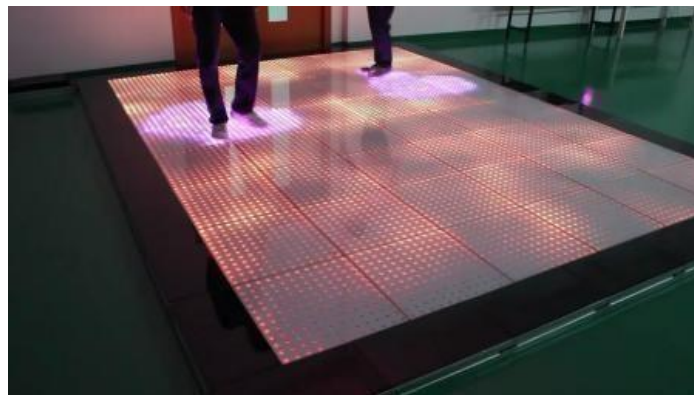


Figure 1.10 : la démarche (capteur de sol). (<https://pin.it/1wpKJIEi1>)

1.4.3. Analyse biologique :

Elle est basée sur l'identification de traits biologiques particuliers.

a) Veines de la main

Il est communément admis que la structure veineuse de la main présente une configuration unique à chaque individu. Le sang oxygéné est transporté vers les extrémités par les artères, puis revient vers le cœur par les veines. Or, le sang pauvre en oxygène possède des propriétés

d'absorption différentes de celles du sang artériel, en particulier dans les longueurs d'onde proches de l'infrarouge (environ 760 nanomètres).

Ainsi, en exposant la main à une source infrarouge, le réseau veineux devient visible sous forme de motifs sombres, permettant sa capture sous forme d'image. Ce motif biométrique distinct, une fois numérisé, peut être enregistré dans une base de données et utilisé ultérieurement à des fins d'authentification sécurisée [16].



Figure 1.12 : Image de système configuration des veines.(
<https://www.fdesouche.com/page/15/?q=zemmour/page/4930/>)

b) ADN

L'empreinte génétique, fondée sur l'analyse de l'ADN, est largement reconnue comme l'un des moyens d'identification les plus fiables disponibles à ce jour. Elle est notamment utilisée dans les tests de filiation, où elle permet d'atteindre des taux de certitude avoisinant les 99,999 %. Malgré cette précision remarquable, l'exploitation de l'ADN présente des limitations importantes en matière de délai. En effet, le processus d'analyse est complexe et peut s'étendre sur plusieurs semaines, ce qui le rend peu adapté aux besoins d'identification instantanée dans des contextes opérationnels [18].



Figure 1.11 : L'ADN. (https://www.nichd.nih.gov/sites/default/files/inline-files/NICHD_SP_Response_June_2019.pdf)

1.4.4 Modalité expérimental :

a) Cartographie thermique

La cartographie thermique repose sur l'utilisation d'une caméra infrarouge pour enregistrer la distribution de chaleur émise par une partie du corps, comme le visage, la main ou un doigt. Cette répartition thermique, influencée par la vascularisation sous-cutanée, présente des motifs distinctifs propres à chaque individu, pouvant également révéler le réseau veineux facial. Bien que cette approche offre un potentiel intéressant en matière d'identification biométrique, elle demeure pour l'instant au stade de la recherche expérimentale et n'est pas encore largement déployée dans les systèmes opérationnels [13].

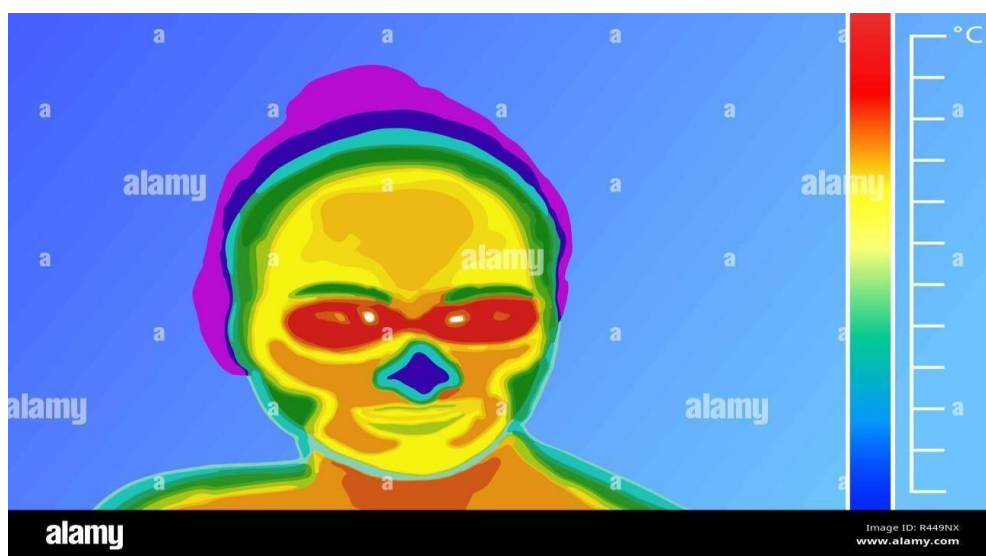


Figure 1.13 Cartographie thermique de visage d'un homme - Thermographie infrarouge

<https://www.alamy.com/thermal-imager-medical-scan-human-face-vector-illustration-the-image-of-a-men-arm-using-infrared-thermograph-scale-is-degrees-fahrenheit-image231903982.html>.

1.5 Fonctionnement d'un système biométrique

Les systèmes biométriques reposent sur l'analyse quantitative de caractéristiques biologiques propres à chaque individu, dans le but d'établir ou de vérifier son identité de manière fiable. Contrairement aux méthodes d'authentification traditionnelles, telles que les mots de passe ou les cartes d'accès, qui peuvent être oubliés, volés ou usurpés, la biométrie exploite des traits physiques ou comportementaux inhérents à l'utilisateur, offrant ainsi une sécurité renforcée.

Deux principaux modes de fonctionnement peuvent être distingués dans un système biométrique [19] :

1.5.1 Authentification

L'authentification biométrique consiste à vérifier si les données biométriques présentées par une personne correspondent à un modèle de référence préalablement enregistré. Ce modèle est stocké soit

dans une base de données centrale, soit sur un dispositif sécurisé, comme une carte à puce. Lors de la vérification, le système compare les nouvelles données à celles existantes afin de confirmer l'identité déclarée de l'utilisateur. Ce processus repose sur la question : « Êtes-vous bien la personne que vous prétendez être ?

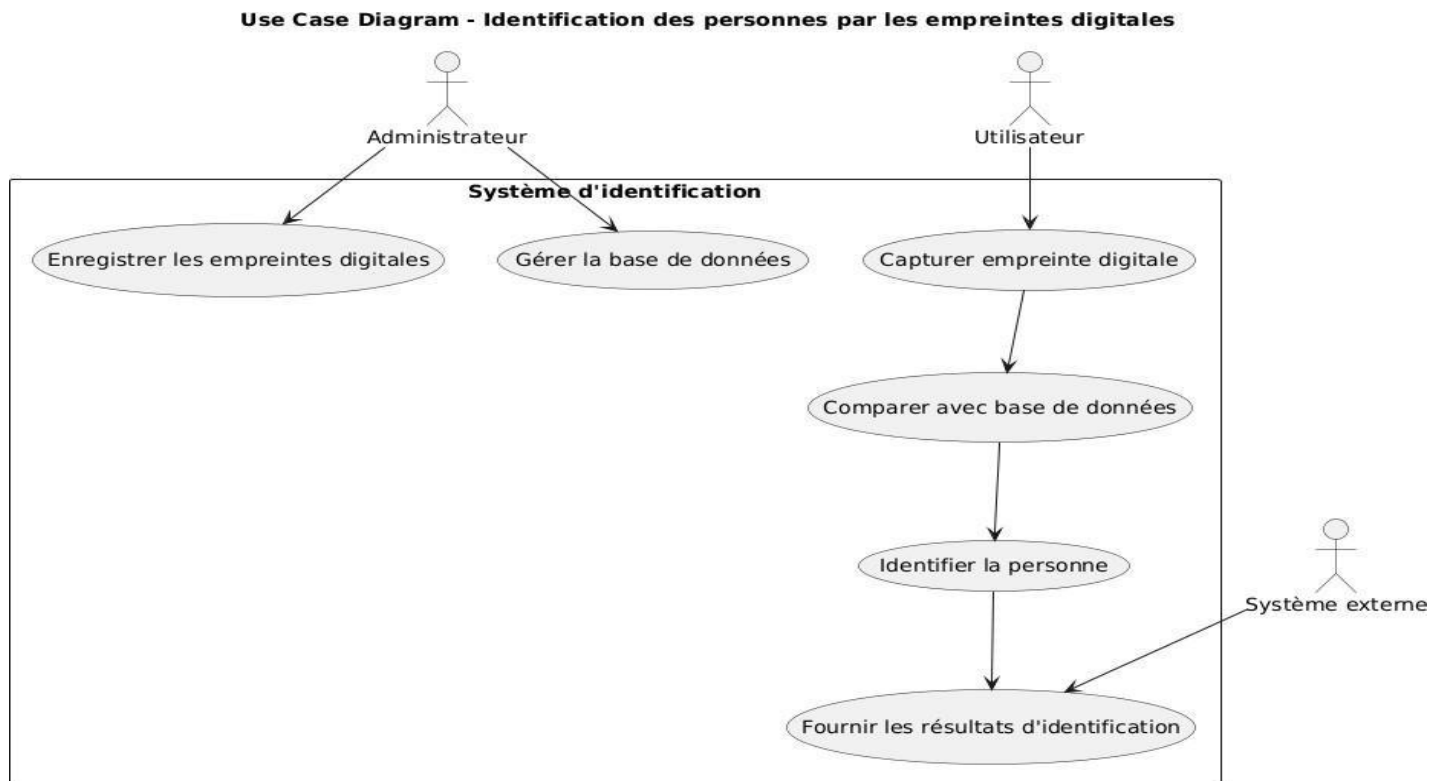


Figure1.14. Diagramme Cas d'utilisation

1.5.2 Identification

L'identification biométrique a pour objectif de déterminer l'identité d'un individu en s'appuyant sur la capture d'un trait distinctif, tel qu'une empreinte digitale, une image faciale ou un enregistrement vocal. Une fois acquises, ces données sont confrontées à un ensemble de profils biométriques préalablement enregistrés dans une base de données. Contrairement à l'authentification, qui vérifie une identité déclarée, l'identification consiste à rechercher une correspondance parmi plusieurs enregistrements afin d'identifier l'individu. Ce processus repose sur une interrogation implicite : « *Qui êtes-vous ?* »

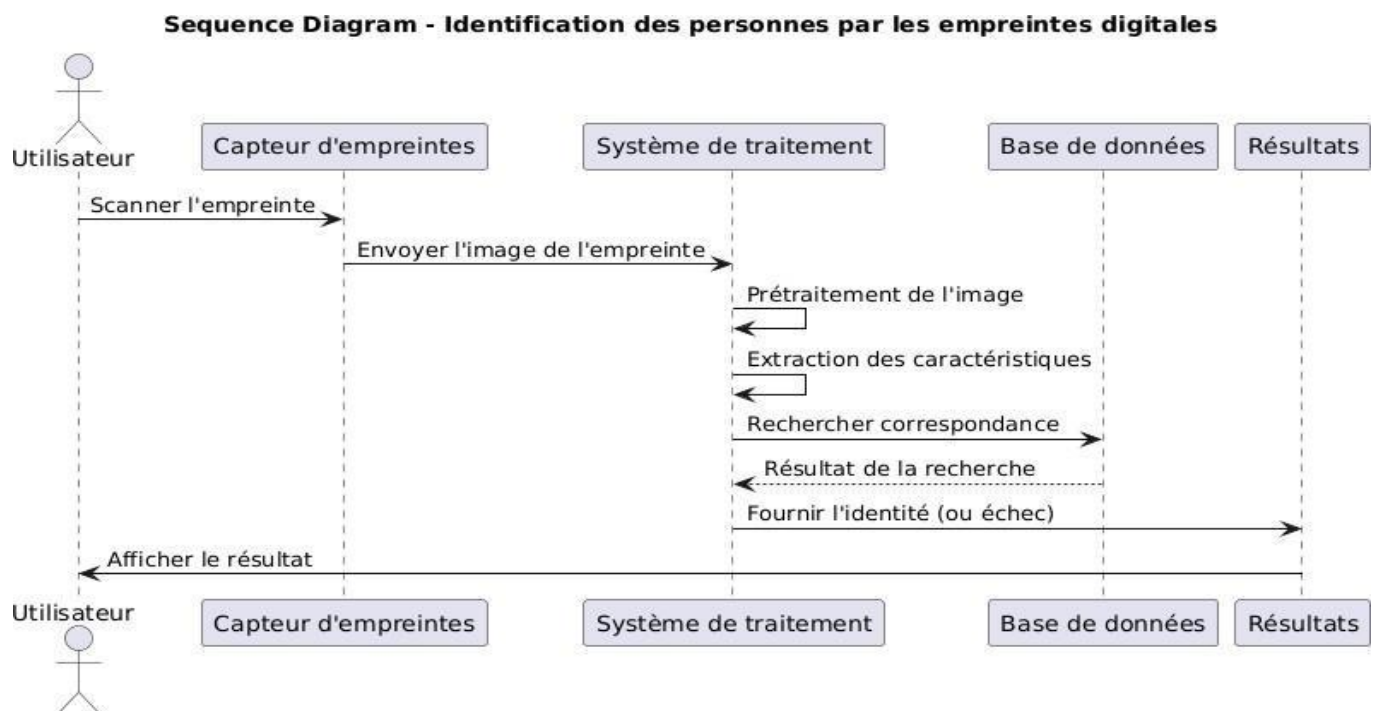


Figure1.15. Diagramme de séquence.

1.6 Conclusion

La biométrie désigne un ensemble de technologies permettant l'identification ou l'authentification des individus à partir de leurs caractéristiques personnelles, qu'elles soient d'ordre physique (comme les empreintes digitales, l'iris, le visage ou la morphologie de la main) ou comportemental (comme la signature, la voix ou la démarche). Ces données sont collectées et analysées par des systèmes automatisés à l'aide de dispositifs spécialisés tels que des capteurs optiques, des caméras ou des scanners.

Contrairement aux méthodes classiques d'identification mots de passe, codes PIN, cartes ou clés qui peuvent être oubliés, copiés ou détournés, les traits biométriques présentent l'avantage d'être propres à chaque individu et difficiles à falsifier. Cette singularité confère à la biométrie un niveau de sécurité élevé, en faisant l'un des moyens d'authentification les plus fiables d'aujourd'hui.

Néanmoins, son adoption soulève plusieurs enjeux, notamment en matière de protection de la vie privée et de confiance dans les performances des systèmes. Si les utilisateurs sont souvent prêts à accepter certaines limitations au nom de la sécurité, ils demeurent peu tolérants face aux erreurs récurrentes, telles que les faux rejets ou les mauvaises reconnaissances. Ces limites techniques, encore observées dans les systèmes monomodaux, justifient le recours croissant à des approches multimodales, qui combinent plusieurs types de données biométriques afin d'accroître la fiabilité et la précision des résultats. Le chapitre qui suit aborde la thématique de notre projet et qui est la reconnaissance par empreintes digitales.

Chapitre 02 : Reconnaissance par Empreintes Digitales



2.1 Historique :

L'utilisation des empreintes digitales pour l'identification remonte à l'une des plus anciennes pratiques biométriques connues. Ce procédé est étudié sous le nom de dactyloscopie, qui désigne l'analyse des dessins formés par les crêtes papillaires des doigts [22].

En 1892, Francis Galton, anthropologue britannique, réalise une première classification scientifique des empreintes en se basant sur plus de 2 500 cas. Plus tard, en 1898, Edward Richard Henry, inspecteur général de la police à Londres, met au point un système de classement fondé sur la configuration globale des empreintes, facilitant ainsi leur identification[10].

Parmi toutes les méthodes biométriques, l'empreinte digitale est celle que le public connaît le mieux. Son usage dans l'identification débute notamment avec les travaux d'Alphonse Bertillon dans les années 1880, qui permettent de reconnaître les récidivistes sans recours à des méthodes physiques brutales. Toutefois, c'est grâce aux recherches de Galton que cette méthode s'impose comme une solution fiable, puisqu'il prouve scientifiquement que les motifs des crêtes sont uniques à chaque individu, immutables tout au long de la vie, et impossibles à reproduire.

Les systèmes d'empreinte digitale reposent sur les motifs formés par les crêtes et sillons présents sur l'épiderme. Ces motifs, bien que riches en informations, sont trop complexes pour être exploités dans leur intégralité. C'est pourquoi seuls les points caractéristiques les plus marquants, appelés minuties (comme les bifurcations, les îlots ou les lignes interrompues), sont extraits. Une empreinte complète peut en contenir une centaine, mais en pratique, on en utilise en moyenne une quarantaine, voire une douzaine selon les exigences légales, ce seuil étant basé sur la fameuse « règle des 12 points » qui garantit un risque d'erreur extrêmement faible même dans des bases très vastes.

Concernant les techniques de capture, plusieurs types de capteurs sont disponibles : optiques (CCD/CMOS), capacitifs, thermiques ou ultrasoniques. Ces capteurs sont souvent couplés à des mécanismes de validation pour s'assurer que l'image provient bien d'un doigt humain vivant. Ces vérifications peuvent inclure des mesures de conductivité, rythme cardiaque, pression sanguine, ou même des analyses sous-cutanées.

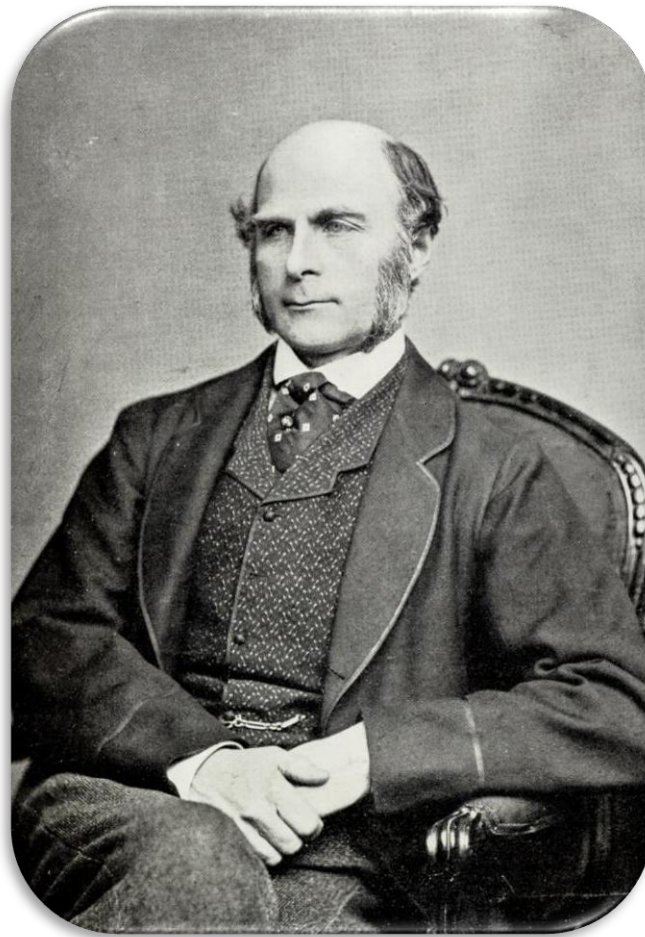


Figure 2.1 : Francis Galton.

2.2. Définition et structure

La reconnaissance des empreintes digitales constitue une application majeure de la biométrie. Elle est couramment exploitée dans de nombreux domaines, en particulier dans les systèmes de sécurité destinés à l'identification individuelle [23].

Parmi les techniques biométriques disponibles, l'analyse des empreintes digitales est aujourd'hui la plus utilisée. Cette popularité s'explique par la structure particulière des empreintes : un ensemble de lignes parallèles comportant des points spécifiques appelés minuties, qui confèrent à chaque empreinte un motif à la fois unique, constant et universel.

Avec les progrès technologiques, la numérisation des empreintes s'effectue désormais via des capteurs sophistiqués, remplaçant les anciennes méthodes basées sur l'encre. Ces capteurs peuvent s'appuyer sur divers mécanismes de détection tels que la pression, la température, ou encore les champs électriques. On distingue généralement deux types de dispositifs : les capteurs matriciels, qui capturent une image fixe, et les capteurs à balayage, qui analysent l'empreinte en mouvement.

Le processus débute par la capture de l'image à l'aide d'un lecteur spécialisé. À partir de cette image, on extrait des caractéristiques biométriques distinctives afin de générer une signature numérique propre à l'individu. Ce modèle constitue une base solide pour l'authentification et offre une fiabilité élevée lorsqu'il est bien conçu.

Les approches de comparaison des empreintes se divisent en deux grandes familles :

- **Les méthodes fondées sur les minuties** : elles identifient les points clés de l'empreinte et analysent leur position, leur orientation et leur type (terminaison, bifurcation, etc.) [24].
- **Les méthodes de corrélation** : elles comparent l'aspect général de deux images d'empreintes pour détecter des similitudes globales[24].

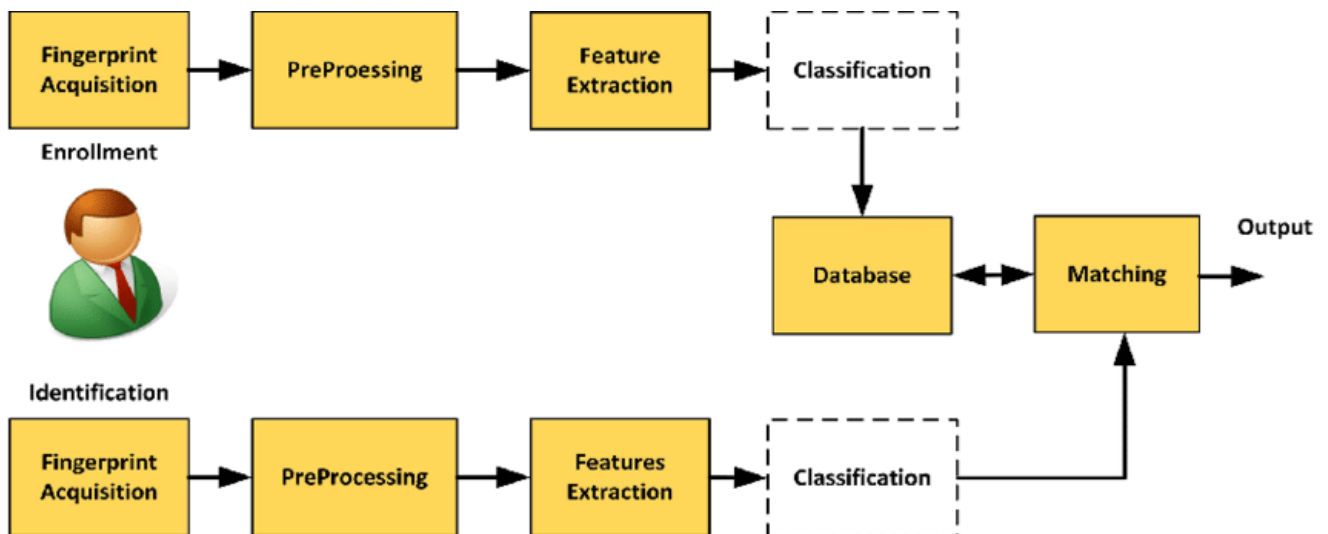


Figure 2.2 : Un organigramme du système d'identification par empreinte digitale (composants de base)
https://www.researchgate.net/figure/A-flowchart-of-fingerprint-identification-system-basic-components_fig4_291098892.

Néanmoins, l'approche fondée sur l'analyse des minuties présente certaines limites, notamment lorsque la qualité de l'image capturée est insuffisante. Dans ces conditions, il devient difficile d'identifier avec précision les points caractéristiques nécessaires à une reconnaissance fiable. Un autre inconvénient de cette méthode réside dans le fait qu'elle néglige la structure globale des lignes papillaires (crêtes et sillons).

À l'opposé, les techniques basées sur la corrélation exploitent l'aspect global de l'empreinte, ce qui leur permet de compenser les lacunes des méthodes traditionnelles. Toutefois, ces approches sont plus sensibles aux variations de position de l'empreinte (comme les déplacements ou les rotations) et offrent en général une précision inférieure à celle des systèmes utilisant les minuties.

C'est pourquoi, pour bénéficier des avantages respectifs de ces deux approches, il est fréquent de les combiner dans une solution hybride, dans le but de renforcer la précision et la robustesse du système de reconnaissance [24].

2.3 Empreinte digitale

Dans cette section, nous allons définir ce qu'est une empreinte digitale et expliquer son fonctionnement.

2.3.1 Explication d'empreinte digitale

Les empreintes digitales correspondent aux marques résultant des crêtes dermiques situées sur la surface des doigts. Ces motifs, propres à chaque individu, présentent une unicité remarquable qui en fait un moyen d'identification particulièrement fiable (voir figure 2.2).

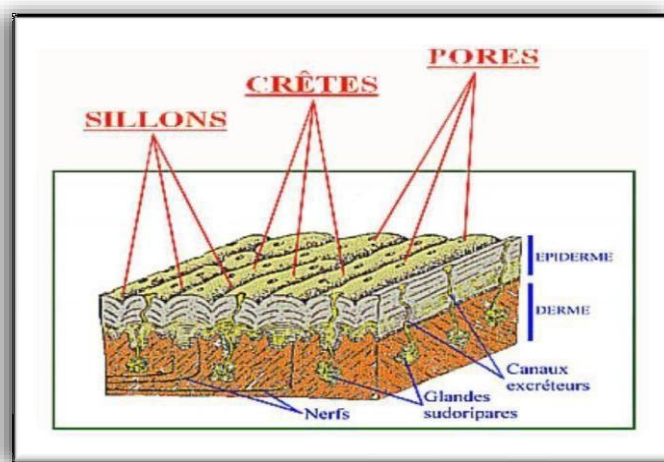


Figure 2.2 : Dessin d'une Empreinte

https://www.memoireonline.com/08/21/12173/m_Etude-des-methodes-de-reconnaissances-dempreinte-digitale-a-laide-du-deep-learning4.html.

2.3.1 Propriétés d'empreinte digitale

Lorsqu'il s'agit de distinguer deux empreintes digitales présentant une structure similaire, l'analyse repose sur l'identification de certaines caractéristiques distinctives, appelées points singuliers globaux. Ces repères jouent un rôle fondamental dans la définition de l'agencement global de l'empreinte et facilitent considérablement la comparaison :

Le centre (ou core) : Ce point désigne la zone centrale de l'empreinte, là où les crêtes dermiques atteignent une courbure maximale. Il correspond généralement à la zone de concentration des lignes de crêtes, souvent située au cœur du motif.

- **Le delta** : Il s'agit d'un point où les lignes de crêtes forment un motif de type triangulaire, facilement perceptible. Ce repère marque la séparation entre deux flux de crêtes qui divergent à partir de ce point (voir figure 2.3).

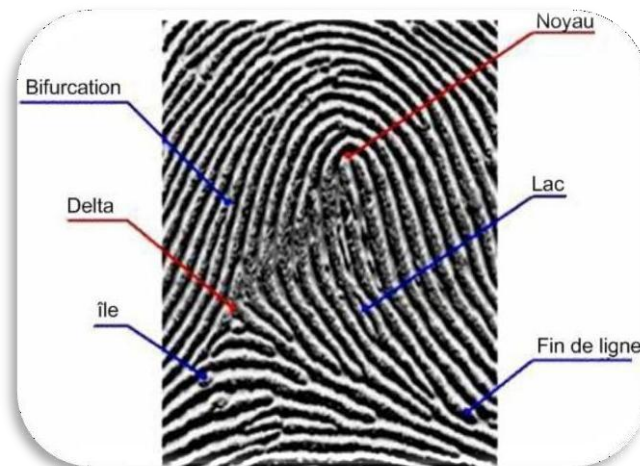


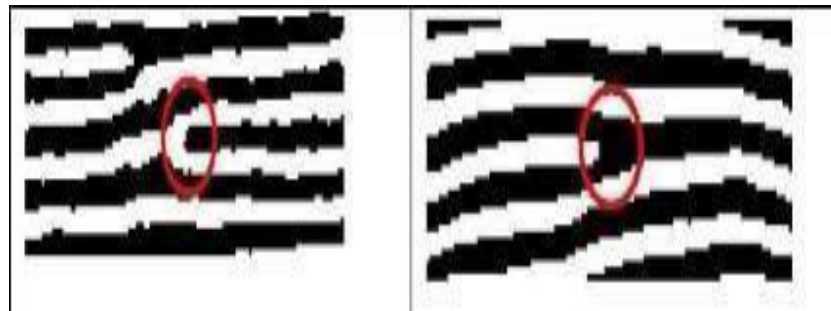
Figure 2.3 : points singuliers globaux

b) Points singuliers locaux

Les minuties désignent les irrégularités localisées le long des lignes papillaires d'une empreinte digitale. Elles constituent des marqueurs cruciaux dans le processus d'identification, car leur répartition et leur forme varient d'un individu à l'autre, y compris entre des empreintes très proches. Bien que la littérature en recense jusqu'à seize types, les systèmes de reconnaissance automatisée s'appuient généralement sur un nombre restreint de minuties, principalement les plus discriminantes :

- **Terminaison** (droite ou gauche) : point où une ligne de crête s'interrompt brusquement.
- **Bifurcation** (droite ou gauche) : lieu où une ligne de crête se divise en deux branches distinctes.
- **Île** : courte ligne isolée entre deux terminaisons, souvent interprétée comme deux terminaisons très proches.
- **Lac** : formation fermée au sein des crêtes, semblable à une boucle engendrée par deux bifurcations.

Parmi l'ensemble des minuties, les terminaisons et les bifurcations sont les plus fréquemment exploitées, en raison de leur facilité de détection par les systèmes automatisés d'analyse d'empreintes digitales (voir figure 2.5).



a : Terminaison.

b : Bifurcation.

Fig2.5. La terminaison et la bifurcation

2.4 Processus de reconnaissance

Un système biométrique fondé sur les empreintes digitales opère généralement selon deux étapes principales (voir figure 2.6) :

2.4.1. Phase d'enrôlement (ou d'apprentissage) :

Durant cette première étape, l'empreinte digitale d'un individu est capturée, puis soumise à un traitement permettant d'en extraire des caractéristiques uniques. Ces informations sont ensuite transformées en un modèle biométrique qui sera conservé dans une base de données pour servir de référence lors des futures vérifications[24].

2.4.2. Phase de vérification ou d'identification :

À ce stade, l'empreinte digitale de l'utilisateur est de nouveau capturée et analysée pour en extraire les mêmes types de caractéristiques. Le modèle ainsi obtenu est ensuite comparé à ceux enregistrés précédemment dans la base. Si une correspondance est établie, l'identité de l'individu est confirmée ou l'accès est autorisé ; dans le cas contraire, la demande est rejetée[24].

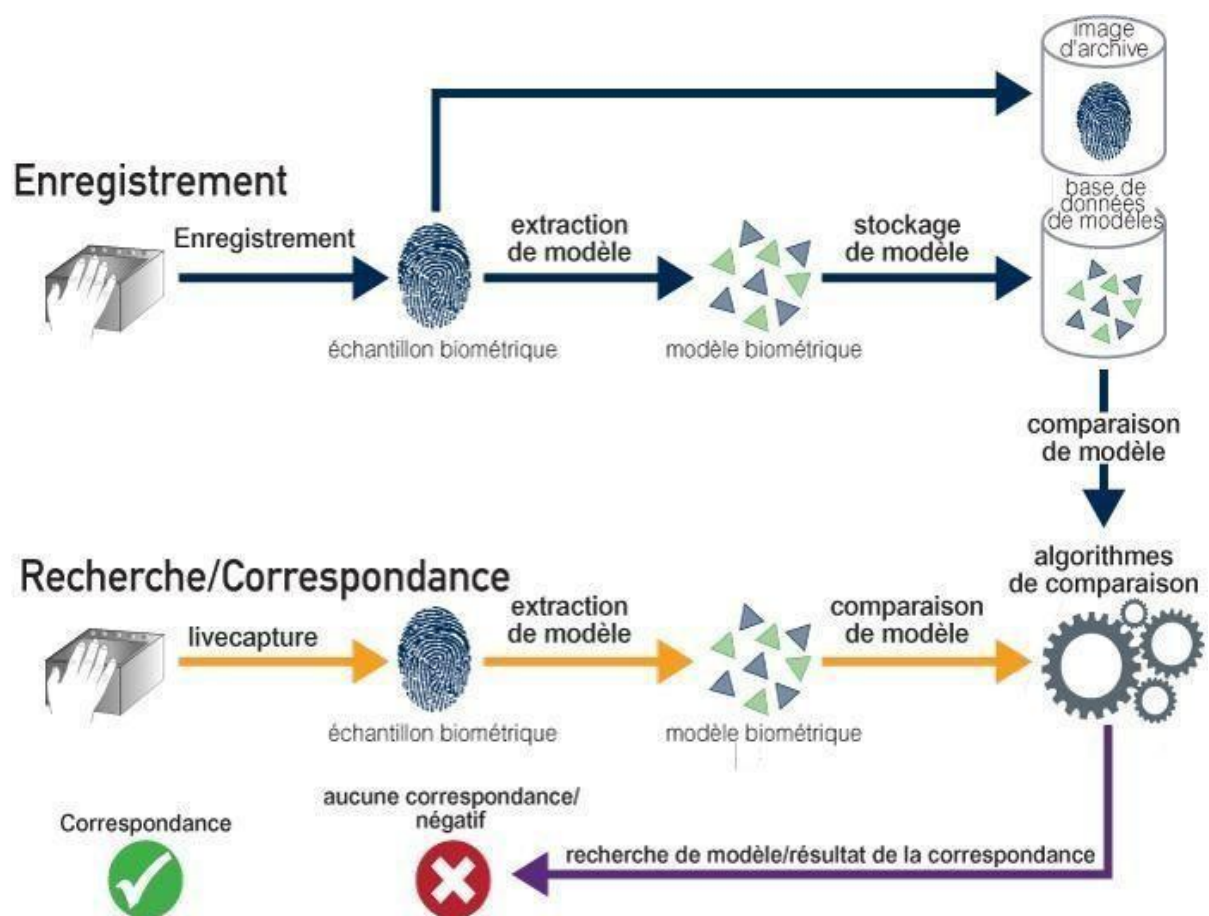


Fig2.6. Architecture d'un système biométrique basé sur l'empreinte(https://www.researchgate.net/figure/Les-processus-biometriques-Aware-2017_fig1_353247361).

2.5. Technologies employées

Le prétraitement d'une empreinte digitale constitue une étape fondamentale visant à améliorer la qualité de l'image avant l'extraction des caractéristiques. Plusieurs techniques sont mises en œuvre pour optimiser cette phase. Ci-après, nous présentons quelques méthodes parmi les plus fréquemment utilisées.

2.5.1. Conversion en niveaux de gris

La conversion en niveaux de gris consiste à transformer une image en couleurs en une représentation monochrome, où chaque pixel est défini par une valeur unique d'intensité lumineuse[24].

Dans sa forme standard, une image en niveaux de gris présente une profondeur de couleur de $k = 8$ bits (voir figure 2.7), ce qui permet à chaque pixel de prendre une valeur comprise entre 0 et 255 :

- 0 correspond à un noir absolu,
- 255 à un blanc pur.

Pour certaines applications de haute précision, notamment dans le domaine professionnel, une profondeur plus élevée peut être requise. Des images en 14 bits ou 16 bits sont alors utilisées, offrant un éventail plus large de niveaux d'intensité et, par conséquent, une meilleure finesse dans la représentation des détails.



a : L'empreinte originale. b: L'empreinte en gris.

Fig2.7. Conversion Niveaux de gris

2.5.2 Seuillage (Binarisation)

Au cours de cette étape, l'image en niveaux de gris est convertie en une image binaire à l'aide d'un procédé de seuillage, plus spécifiquement une méthode de binarisation adaptative (voir figure 2.8). L'objectif principal de cette opération est de différencier les crêtes (les lignes sombres) du fond en attribuant une valeur binaire à chaque pixel :

- **0** pour les pixels correspondant aux crêtes,
- **1** pour ceux représentant les vallées ou le fond.

Cette étape est parfois désignée sous le terme de **segmentation** dans la littérature[24]. Toutefois, il est important de ne pas la confondre avec la segmentation plus générale, qui consiste à séparer la région d'intérêt (ROI) du fond de l'image. Cette dernière opération est souvent réalisée lors de la création d'un masque afin d'isoler les zones pertinentes de l'empreinte.



A) Image en niveaux de gris B) image Binarisée.

Fig2.8.Binarisation

2.5.3 Squelettisation

La squelettisation constitue une étape cruciale du prétraitement, visant à réduire la quantité d'information présente dans l'image tout en préservant la structure fondamentale des motifs. Elle permet d'obtenir une représentation simplifiée et homogène de l'empreinte, facilitant ainsi l'extraction des minuties telles que les terminaisons et les bifurcations.

Cette opération s'effectue sur une image binaire [25]. Bien que les crêtes soient visibles dans une image binaire classique, leur épaisseur peut varier, ce qui complique l'analyse. La squelettisation permet de réduire l'épaisseur de toutes les lignes à un seul pixel[16], offrant ainsi une représentation schématique et normalisée de l'empreinte (voir figure 2.9).



Figure 2.9. Squelettisation de l'empreinte digitale.

2.6. Limites et solutions

Les étapes précédentes de binarisation et de squelettisation ont considérablement simplifié le processus d'extraction des minuties. À ce stade, l'image obtenue est une version squelettisée en noir et blanc, dans laquelle :

- Un pixel noir (représentant une crête) a une valeur de 1,
- Un pixel blanc (représentant le fond) a une valeur de 0,
- La largeur des stries est réduite à un seul pixel.

L'extraction des minuties repose principalement sur le calcul du nombre de transitions (passages de 0 à 1 ou de 1 à 0) dans le voisinage immédiat d'un pixel donné. Ce nombre, appelé **Crossing Number** (CN), permet d'évaluer la connectivité du point sur le squelette.

En divisant ce nombre de transitions par deux, il devient possible de déterminer le type de minutie correspondant au pixel :

- Un CN égal à 1 indique généralement une terminaison de crête,
- Un CN égal à 3 indique une bifurcation,
- D'autres valeurs permettent d'identifier des cas plus complexes ou de rejeter des points non pertinents.

Cette méthode, à la fois simple et efficace, constitue le fondement de nombreux algorithmes d'extraction automatique des minuties[24].

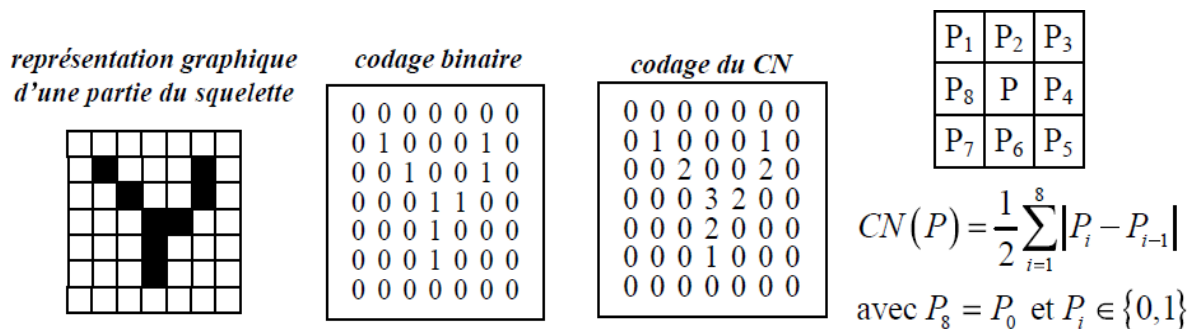


Figure 2.10. Calcul de minutie.

Ainsi, pour chaque pixel PPP appartenant à une strie (c'est-à-dire un pixel ayant une valeur de 1 dans l'image binaire squelettisée), le calcul du **Crossing Number** (CN) peut aboutir à l'une des cinq situations suivantes :

Le Crossing Number (CN) est une méthode simple et efficace pour détecter les points caractéristiques (minuties) d'une empreinte digitale à partir d'une image binaire (noir et blanc).

Principe :

Le CN d'un pixel central est calculé comme suit :

$$CN = \frac{1}{2} \sum_{i=1}^8 |P_i - P_{i+1}|$$

où P1,P2,...,P8P_1, P_2, ..., P_8P1,P2,...,P8 sont les pixels du voisinage 8-connecté autour du pixel central, et P9=P1P_9 = P_1P9=P1 pour refermer le cycle.

Interprétation :

- CN = 1 → Terminaison de ligne (ridge ending)
- CN = 3 → Bifurcation
- CN = 0 ou CN > 3 → Autres cas, souvent ignorés ou considérés comme bruit

CN	Signification
1	Terminaison
3	Bifucation
2	Point normal
>3	Intersection/bruit

2.7 Classification

La classification constitue la phase finale du processus de reconnaissance des empreintes digitales. Elle consiste à comparer les vecteurs de caractéristiques extraits d'une empreinte à ceux présents dans une base de données, afin de déterminer s'il existe une correspondance.

a) Algorithme d'apprentissage (CNN pour la classification)

Dans notre approche, nous utilisons un Réseau de Neurones Convolutif (CNN) pour la classification automatique des données biométriques. Contrairement aux machines à vecteurs de support (SVM), les CNN sont capables d'apprendre des caractéristiques hiérarchiques directement à partir des données brutes (comme les images d'empreintes digitales), sans nécessiter d'extraction manuelle de caractéristiques.

Le modèle CNN développé comporte les éléments suivants [17]:

- **Des couches convolutives** pour détecter des motifs locaux, tels que des bordures et des textures.
- **Des couches de pooling** (MaxPooling, AveragePooling) pour réduire la dimension spatiale.
- **Des couches fully-connected** (ou denses) en fin de réseau, responsables de la décision de classification.
- **Une fonction d'activation softmax** en sortie, permettant d'obtenir les probabilités associées à chaque classe.

Avantages par rapport aux SVM :

- Meilleure adaptation aux données complexes, telles que les images et les signaux.
- Apprentissage automatique des caractéristiques, éliminant le besoin de normalisation manuelle.
- Robustesse aux variations, telles que les légères translations ou rotations.

b) Méthode de similarité (Distance cosinus ou Loss contrastive)

- Plutôt que d'utiliser une distance euclidienne classique pour comparer les vecteurs, nous exploitons une approche basée sur :

1. Embeddings (représentations CNN) :

- La dernière couche avant la classification (généralement un vecteur de 128 à 512 dimensions) sert de signature pour l'empreinte digitale.
- Deux images similaires auront des embeddings proches dans l'espace latent.

2. Mesure de similarité :

- **Distance cosinus** : Elle mesure l'angle entre deux vecteurs, ce qui la rend particulièrement adaptée pour des embeddings normalisés.

$$\text{similarité} = \frac{X \cdot Y}{\|X\| \cdot \|Y\|}$$

- **Loss contrastive** (si entraînement par paires) : Pénalise les embeddings de mêmes classes trop éloignés.

2.8 Conclusion

Dans ce chapitre, nous avons fourni une présentation approfondie des divers processus informatiques impliqués dans l'identification des empreintes digitales. Ces techniques, bien que performantes et relativement simples à mettre en œuvre, présentent encore certaines limitations lorsqu'elles sont appliquées dans des contextes réels.

Malgré les avancées significatives des systèmes de reconnaissance d'empreintes digitales, rendues possibles par les progrès technologiques et algorithmiques, ce domaine demeure en constante évolution. Plusieurs défis persistent, notamment :

- La sensibilité des systèmes aux empreintes de mauvaise qualité,
- Le temps de traitement requis pour l'identification,
- La robustesse face aux variations, telles que la rotation, la translation ou la pression.

Ces limitations font l'objet de nombreuses recherches visant à améliorer la précision, la rapidité et la fiabilité des systèmes biométriques basés sur les empreintes digitales.

Chapitre 3: Implémentation et résultats



3.1 Introduction

L'étude expérimentale de ce travail porte sur la reconnaissance des individus par leurs empreintes digitales, en utilisant les méthodes décrites au chapitre 2. Notre programme a été testé sur la base de données SOCOFing (Sokoto Coventry Fingerprint Dataset), une collection d'empreintes digitales largement utilisée dans la recherche biométrique. Ce chapitre détaille le fonctionnement de chaque bloc du système, les caractéristiques de la base de données SOCOFing, ainsi que l'environnement de travail utilisé[15].

3.2 Base de données SOCOFing

La base de données SOCOFing est une référence dans le domaine de la reconnaissance d'empreintes digitales, comprenant des images de haute qualité capturées dans des conditions variées[15]. Voici ses principales caractéristiques :

- **Nombre total d'images** : 6 000 empreintes digitales.
- **Individus uniques** : 600 personnes (300 hommes / 300 femmes).
- **Empreintes par personne** : 10 (6 doigts + 4 scans répétés).
- **Taille moyenne des images** : $\sim 300 \times 300$ pixels.

a. Structure de Nommage des Fichiers

- **Format** : ID_Gender_Hand_FingerNumber.png
 - **ID** : 001 à 600 (identifiant unique de la personne).
 - **Gender** : M (Homme) ou F (Femme).
 - **Hand** : Left (main gauche) ou Right (main droite).
 - **FingerNumber** : thumb, index, middle, ring, little (ou 1 à 5).

b. Conditions de Capture (Simulées)

- **Variabilité** :
 - Différents niveaux de pression et d'orientation.
 - Imperfections réalistes (blessures mineures, résidus).
- **Annotations** : Fichiers séparés avec coordonnées des minuties (bifurcations, terminaisons).

c. Compatibilité Logicielle

- **Systèmes d'exploitation** : Tous (Linux, Windows, macOS).
- **Outils recommandés** : Bibliothèques Python (OpenCV, TensorFlow), MATLAB.

d. Environnement de Stockage

- **Taille totale** : ~ 150 Mo (compressé).

- **Accès** : Téléchargeable librement sur [Kaggle](#) ou dépôts universitaires.

La figure 3.1 donne des exemples de cette base de données.



Figure 3.1 : Quelques images de la base de données SOCOFing.

3.3 Diviser les Données

La base de données a été divisée en deux ensembles distincts pour répondre aux besoins d'apprentissage et d'évaluation du système :

3.3.1 Apprentissage

- **Composition** :
 - 4 premières images de chaque individu.
 - Total : 204 images (51 personnes $\times$ 4 images).
- **Objectif** :
Permettre au modèle d'apprendre les caractéristiques discriminantes des empreintes digitales.

3.3.2 Test

- **Composition** :
 - 4 dernières images de chaque individu
 - Total : 204 images (51 personnes $\times$ 4 images)
- **Objectif** :
Évaluer objectivement les performances du système sur des données jamais vues durant l'apprentissage.

Remarque : Ce partitionnement équilibré (50%/50%) a été choisi pour garantir une évaluation représentative, bien qu'il n'existe pas de règle standard absolue en la matière.

3.4 Environnement

L'expérimentation a été menée sur une station de travail Lenovo dotée des caractéristiques suivantes :

- **Processeur** : Intel® Core™ i7-10700KF (3.80 GHz)
- **Mémoire vive** : 16 Go
- **Stockage** : Disque dur 500 Go

- **Système d'exploitation** : Microsoft Windows 11 (64 bits)

3.4.1 Outils de développement :

Lors de l'élaboration de notre système, nous avons utilisé le langage de programmation Python, qui est un langage de programmation interprété, de haut niveau, largement utilisé pour le développement d'algorithmes et l'analyse de données. Il est apprécié pour sa simplicité syntaxique et la richesse de ses bibliothèques.

Python permet de manipuler efficacement des tableaux de données (notamment avec la bibliothèque NumPy), de tracer des courbes (Matplotlib, Seaborn), de développer des interfaces utilisateur (Tkinter, PyQt), et d'implémenter des algorithmes complexes. Il offre également de nombreuses bibliothèques dédiées au traitement d'images, telles que OpenCV, Pillow, et scikit-image. Python peut s'interfacer avec d'autres langages comme le C, C++, et Java, ce qui le rend très flexible dans les projets de développement.

3.5. Le système :

L'interface graphique de notre application, développée en Python à l'aide de la bibliothèque Tkinter, permet à l'utilisateur de tester une image d'empreinte digitale à l'aide d'un modèle de réseau de neurones convolutifs (CNN). L'interface est simple, intuitive et se compose de plusieurs éléments essentiels et qui sont comme suit :

- **Zone d'affichage d'image** : située au centre de la fenêtre, elle permet de visualiser l'image d'empreinte digitale sélectionnée. Un texte indicatif « Image Test » y est affiché par défaut avant le chargement.
- **Bouton “Charger une Image”** : permet à l'utilisateur de sélectionner une image d'empreinte à partir de son système de fichiers. Une fois l'image choisie, elle est affichée dans la zone prévue à cet effet.
- **Bouton “Tester l'Image”** : ce bouton lance le traitement de l'image à l'aide du modèle CNN intégré dans l'application. Ce traitement permet par exemple de reconnaître, classer ou valider l'empreinte selon les fonctionnalités implémentées.

Notre interface a été conçue dans un souci de simplicité afin de faciliter les tests et la démonstration du fonctionnement de notre système de reconnaissance d'empreintes digitales.

3.5.1 Importation des bibliothèques :

Le script débute par l'importation des modules nécessaires à la manipulation des images, à la construction du modèle de deep learning, à l'évaluation des performances, et aussi à la création de l'interface graphique. On retrouve notamment OpenCV pour le traitement d'image, TensorFlow/Keras pour le réseau de neurones convolutif (CNN), scikit-learn pour le calcul de similarité, et PyQt5 pour l'interface.

```

1  import sys
2  import os
3  import numpy as np
4  import cv2
5  import matplotlib.pyplot as plt
6  from sklearn.metrics import accuracy_score
7  from tensorflow.keras.models import Sequential
8  from tensorflow.keras.layers import Conv2D, MaxPooling2D, Flatten, Dense, Dropout
9  from tensorflow.keras.utils import img_to_array
10 from sklearn.metrics.pairwise import cosine_similarity
11
12 from PyQt5.QtWidgets import (
13     QApplication, QWidget, QLabel, QPushButton, QVBoxLayout, QFileDialog, QMessageBox
14 )
15 from PyQt5.QtGui import QPixmap, QImage
16 from PyQt5.QtCore import Qt

```

3.5.2 Prétraitement des images

Les empreintes digitales sont d'abord converties en images normalisées. Cette phase garantit que chaque image soit dans le même format, facilitant l'apprentissage et la comparaison. L'image est convertie en niveaux de gris, redimensionnée à 128x128 pixels, puis normalisée dans l'intervalle [0, 1].

```

23 def preprocess_image(image_path): 3 usages
24     image = cv2.imread(image_path, cv2.IMREAD_GRAYSCALE)
25     image = cv2.resize(image, dsize=(IMG_SIZE, IMG_SIZE))
26     image = image.astype("float32") / 255.0
27     image = np.expand_dims(image, axis=-1)
28     return image
29

```

3.5.3 Définition du modèle CNN (encodeur)

Le réseau de neurones utilisé est un CNN qui transforme une image d'empreinte en un vecteur de caractéristiques de 64 dimensions. Ce vecteur sert à représenter numériquement l'empreinte pour les comparaisons ultérieures.

```

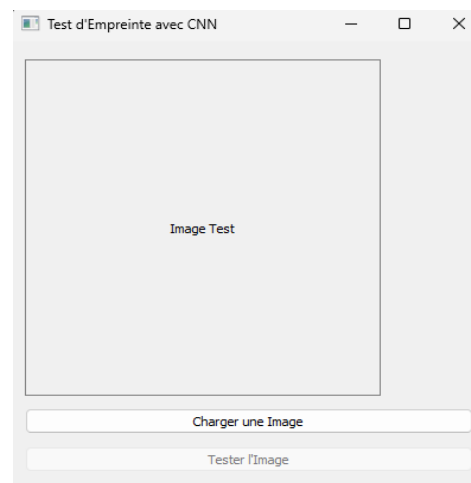
31 def build_encoder(): 1 usage
32     model = Sequential([
33         Conv2D(32, (3, 3), activation='relu', input_shape=(IMG_SIZE, IMG_SIZE, 1)),
34         MaxPooling2D(2, 2),
35         Conv2D(64, (3, 3), activation='relu'),
36         MaxPooling2D(2, 2),
37         Flatten(),
38         Dense(128, activation='relu'),
39         Dropout(0.3),
40         Dense(64, activation='linear')
41     ])
42     return model
43

```

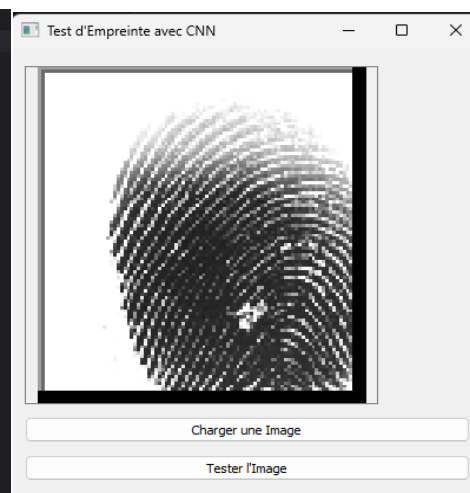
3.5.4 Chargement de l'empreinte

Une fois l'application lancée, l'utilisateur peut procéder au chargement d'une image d'empreinte digitale en cliquant sur le bouton « Charger une Image ». Cette action ouvre une boîte de dialogue lui permettant de parcourir ses fichiers et de sélectionner l'image à tester.

Après sélection, l'image est immédiatement affichée dans la zone centrale de l'interface. Comme illustré dans la figure ci-dessus, l'empreinte digitale apparaît en niveaux de gris, ce qui permet à l'utilisateur de vérifier visuellement l'image avant de lancer le traitement.



```
46 class FingerprintApp(QWidget):
47     def __init__(self):
48         super().__init__()
49         self.setWindowTitle("Test d'Empreinte avec CNN")
50         self.setGeometry(200, 200, 400, 400)
51
52         self.encoder = build_encoder()
53         self.encoder.summary()
54
55         self.input_label = QLabel("Image Test")
56         self.input_label.setAlignment(Qt.AlignCenter)
57         self.input_label.setFixedSize(300, 300)
58         self.input_label.setStyleSheet("border: 1px solid gray;")
59
60         self.btn_load = QPushButton("Charger une Image")
61         self.btn_load.clicked.connect(self.load_image)
62
63         self.btn_test = QPushButton("Tester l'Image")
64         self.btn_test.clicked.connect(self.test_image)
65         self.btn_test.setEnabled(False)
66
67         layout = QVBoxLayout()
68         layout.addWidget(self.input_label)
69         layout.addWidget(self.btn_load)
70         layout.addWidget(self.btn_test)
71
72         self.setLayout(layout)
73
74         self.test_image_path = None
```



Ce chargement dynamique permet de garantir que l'image choisie est bien conforme et exploitable par le modèle. Il constitue une étape essentielle avant de passer à l'analyse proprement dite via le bouton « Tester l'Image ».

La classe FingerprintApp hérite de QWidget et contient tous les éléments nécessaires à l'interface utilisateur. Elle affiche une image, permet à l'utilisateur d'en charger une nouvelle, et propose un bouton pour lancer le test d'identification.

3.5.5 Chargement de la base de données

Lors de l'initialisation, toutes les images présentes dans un répertoire donné sont chargées et encodées. Chaque image est traitée par le CNN pour générer un vecteur de caractéristiques, et chaque vecteur est associé à une étiquette extraite du nom de fichier.

```
78     def load_database(self): 1 usage
79         self.all_images = [os.path.join(DATASET_PATH, f) for f in os.listdir(DATASET_PATH) if f.endswith(".BMP")]
80         self.all_images.sort()
81
82         self.features = []
83         self.labels = []
84
85         for path in self.all_images:
86             img = preprocess_image(path)
87             img = np.expand_dims(img, axis=0)
88             vec = self.encoder.predict(img, verbose=0)[0]
89             self.features.append(vec)
90
91             label = path.split("\\")[-1].split("__")[0]
92             self.labels.append(label)
```

3.5.6 Lancement du test

Après le chargement de l'image, l'utilisateur peut cliquer sur le bouton « Tester l'Image » pour lancer le processus d'analyse. Cette étape déclenche l'algorithme de reconnaissance basé sur un réseau de neurones convolutifs (CNN), qui compare l'empreinte testée à celles enregistrées dans la base de données.

Une nouvelle fenêtre s'ouvre automatiquement, affichant deux empreintes côte à côte : À gauche, l'empreinte testée, identifiée ici comme appartenant à « Person9 » ; À droite, l'empreinte la plus similaire retrouvée dans la base, également identifiée comme étant celle de « Person9 ».

En bas de la fenêtre, le programme affiche le résultat du test avec deux informations essentielles : Prédiction correcte : Oui, ce qui indique que l'empreinte a été reconnue avec succès ; Similarité : 100 %, représentant le taux de correspondance entre l'image testée et la meilleure correspondance trouvée.

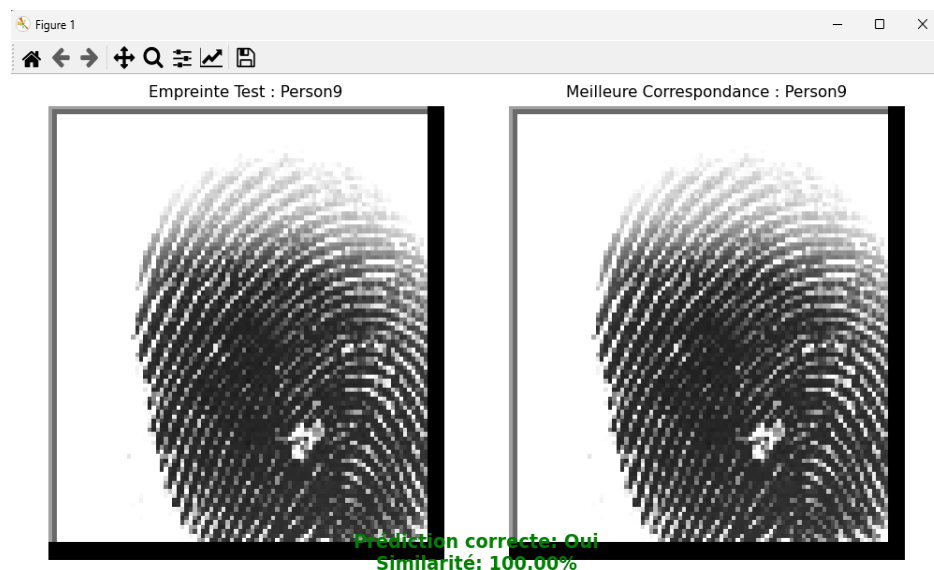
Ce retour visuel et chiffré permet à l'utilisateur de valider rapidement la fiabilité du système et d'évaluer la performance du modèle CNN.

Une fois la comparaison effectuée, deux images sont affichées : celle testée par l'utilisateur et celle de la base la plus proche. Un message indique si l'identification est correcte ainsi que le score de similarité, exprimé en pourcentage.

```

162 # Afficher l'image testée
163 test_image_display = cv2.imread(self.test_image_path, cv2.IMREAD_GRAYSCALE)
164 axs[0].imshow(test_image_display, cmap='gray')
165 axs[0].set_title(f"Empreinte Test : {test_label}")
166 axs[0].axis("off")
167
168 # Afficher la meilleure correspondance
169 best_match_path = self.all_images[best_match_index]
170 best_match_image = cv2.imread(best_match_path, cv2.IMREAD_GRAYSCALE)
171 axs[1].imshow(best_match_image, cmap='gray')
172 axs[1].set_title(f"Meilleure Correspondance : {best_match_label}")
173 axs[1].axis("off")
174
175 # Afficher le texte avec la similarité et la prédiction
176 result_text = f"Prédiction correcte: {correct}\nSimilarité: {similarity_score:.2f}%"
177 fig.text(x=0.5, y=0.01, result_text, ha='center', fontsize=14, fontweight='bold', color='green' if correct == "Oui" else 'red')
178
179 plt.tight_layout()
180 plt.show()

```



3.6 Résultats obtenus :

L'application de notre programme sur la base de données **SOCOFing**, qui contient des empreintes digitales de plusieurs individus, et dont nous avons utilisé un CNN pour l'apprentissage et la reconnaissance des empreintes, a permis d'obtenir les résultats suivants :

Images d'apprentissage	Images de test	Nombre total de personnes	Nombre de personnes reconnues	Taux de reconnaissance
204	204	51	51	100%

Les résultats obtenus sont très satisfaisants. En effet, notre système a permis d'atteindre un taux de reconnaissance de **100 %**, ce qui témoigne de la fiabilité et de l'efficacité du modèle CNN utilisé. Ce résultat répond pleinement à notre objectif initial : la mise en œuvre d'un système performant pour la reconnaissance des individus à partir de leurs empreintes digitales.

3.7. Conclusion

Dans ce chapitre, nous avons présenté en détail notre système de reconnaissance des empreintes digitales, basé sur l'utilisation d'un réseau de neurones convolutif (CNN). Ce système se décompose en trois étapes principales : le prétraitement, l'extraction de caractéristiques, et la classification.

Dans un premier temps, les images d'empreintes sont soumises à un prétraitement comprenant une binarisation par seuillage, suivie d'une squelettisation afin de simplifier la structure des crêtes et de faciliter l'analyse des minuties.

Ces images prétraitées sont ensuite utilisées comme données d'entrée du CNN, qui se charge automatiquement de l'extraction des caractéristiques discriminantes. Grâce à sa capacité à détecter des motifs complexes, le réseau apprend à identifier les minuties et autres éléments significatifs des empreintes digitales.

Enfin, la classification est réalisée par le CNN lui-même. Le modèle compare les empreintes de test avec celles présentes dans la base de données et identifie l'individu correspondant, en se basant sur la distance minimale entre les vecteurs caractéristiques appris pendant l'entraînement.

Conclusion générale

La reconnaissance biométrique est un procédé d'identification des individus basé sur l'analyse de caractéristiques physiques, comportementales ou biologiques. Parmi les différentes modalités biométriques, l'empreinte digitale est l'une des plus fiables et répandues, en raison de son caractère unique et permanent. Dans cette optique, les chercheurs s'efforcent de développer des systèmes de reconnaissance de plus en plus performants, en s'appuyant notamment sur des méthodes mathématiques et des algorithmes d'apprentissage automatique avancés.

Ce mémoire s'inscrit dans cette démarche en proposant un système de reconnaissance d'empreintes digitales visant à améliorer les performances en matière d'identification et de vérification. Le système proposé repose sur trois étapes essentielles : le prétraitement, l'extraction des caractéristiques et la classification.

Dans un premier temps, les images sont soumises à un prétraitement impliquant une conversion en niveaux de gris et une égalisation d'histogramme afin d'optimiser la qualité visuelle de l'empreinte. Ensuite, l'extraction des minuties s'effectue à travers une squelettisation suivie du calcul du Cross Number (CN) permettant de localiser les points caractéristiques de l'empreinte.

L'innovation principale de notre approche réside dans l'utilisation d'un réseau de neurones convolutif (CNN), qui assure à la fois l'extraction automatique des caractéristiques profondes et la classification. Ce type de réseau est particulièrement adapté à la reconnaissance visuelle, car il est capable d'apprendre des représentations complexes à partir des images d'empreintes.

Le système a été évalué à l'aide de la base de données Socofing, une référence dans le domaine de la reconnaissance d'empreintes digitales. Les résultats obtenus ont montré un taux de reconnaissance élevé, témoignant de la fiabilité et de l'efficacité de la méthode proposée. Le système répond ainsi pleinement à l'objectif initial, qui est de concevoir une solution robuste pour l'identification des individus.

En perspective, il serait pertinent d'approfondir l'évaluation des performances sur des bases de données plus larges et plus diversifiées, en explorant également l'intégration multimodale, c'est-à-dire la combinaison de plusieurs traits biométriques (visage, iris, voix...) pour renforcer la précision et la sécurité du système.

Bibliographie

1. **Daugman, J.** (2004). "How iris recognition works." *IEEE Transactions on Circuits and Systems for Video Technology*. Cette référence explore la biométrie oculaire et les algorithmes associés à la reconnaissance de l'iris.
2. **Pinto, R., & Morais, H.** (2018). "A survey of biometric systems: Techniques, applications, and performance evaluation." *Pattern Recognition*. Cet article propose un état des lieux des systèmes biométriques et des défis rencontrés lors de leur mise en œuvre.
3. **Ménard, L.** (2008). "Reconnaissance biométrique : une étude des différents types de systèmes." *L'Université de la Réunion*. Ce travail se concentre sur les différentes techniques de reconnaissance biométrique, notamment les empreintes digitales, la reconnaissance faciale et la reconnaissance vocale.
4. **Pérez-Medina, J., & García-Serrano, A.** (2017). "Multimodal biometric systems for user authentication." *Springer Briefs in Computer Science*. Ce livre aborde les systèmes biométriques multimodaux pour l'authentification des utilisateurs.
5. **Jain, A.K., & Nandakumar, K.** (2011). "Biometric template protection: A survey." *ACM Computing Surveys (CSUR)*. Cet article traite des défis de la protection des modèles biométriques, abordant les questions de sécurité et de confidentialité.
6. **National Institute of Standards and Technology (NIST).** (2003). "Biometric Recognition: Challenges and Opportunities." *NIST Special Publication*. Ce rapport de recherche par le NIST fournit une vue d'ensemble complète sur les défis, la précision et les applications des systèmes biométriques.
7. **Gollan, T., et al.** (2005). "Biometric recognition: A security solution for the global market." *International Journal of Security and its Applications*. Cet article traite des applications de la biométrie dans les solutions de sécurité à l'échelle mondiale.
8. **Sullivan, P., & Winter, R.** (2013). "The future of biometric identification systems." *Journal of Information Security*. Cet article explore les technologies émergentes dans le domaine de la biométrie et leur impact sur les systèmes de sécurité.
9. **Wikipedia.** (2023). "Biometrics." [En ligne]. <https://en.wikipedia.org/wiki/Biometrics>. Une ressource générale pour obtenir des informations de base sur les différents types de biométrie, les applications, ainsi que des liens vers des publications et des recherches associées.
10. **Abes, A. Ben Khalif et F.** Identification d'individus par reconnaissance. Mémoire de fin d'étude, Université Kasdi Merbah, Ouargla. Université Kasdi Merbah, Ouargla : s.n., 2008.
11. **John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas.** Biometrics A Look at Facial Recognition. documented briefing by RAND Public Safety and Justice for the Virginia State Crime Commission. 2003.

12. **ResearchGate**. Schéma du processus de reconnaissance par empreinte digitale (acquisition, traitement, extraction des caractéristiques, etc.) . [En ligne]. https://www.researchgate.net/figure/A-flowchart-of-fingerprint-identification-system-basic-components_fig4_291098892
13. **Jain, A. K., Ross, A., & Prabhakar, S. (2004)**. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology.
Lien : <https://ieeexplore.ieee.org/document/1287575>
14. **Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009)**. Handbook of Fingerprint Recognition. Springer.
Lien Springer : <https://link.springer.com/book/10.1007/978-1-84882-254-0>
15. **Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018)**. *Sokoto Coventry Fingerprint Dataset*. arXiv
16. **Zhang, T. Y., & Suen, C. Y. (1984)**. A fast parallel algorithm for thinning digital patterns. <https://ieeexplore.ieee.org/document/4767851>
17. **Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012)**. ImageNet Classification with Deep Convolutional Neural Networks. In Advances in Neural Information Processing Systems (NeurIPS). https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf
18. **LeCun, Y., Bengio, Y., & Hinton, G. (2015)**. Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
19. **Wikipédia Fingerprint recognition** https://en.wikipedia.org/wiki/Fingerprint_recognition
20. **Wikipédia Biometrics** <https://en.wikipedia.org/wiki/Biometrics>
21. **Wikipédia ConvolutionalNeuralNetwork** https://en.wikipedia.org/wiki/Convolutional_neural_network

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة عبد الحميد بن باديس-مستغانم-
كلية العلوم الدقيقة والإعلام الآلي

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

الطالب(ة): مستغانم رقم التسجيل

الجامعي: 20203703867

الحامل لبطاقة التعريف الوطنية رقم: 21357166 والصادرة بتاريخ:

2021/09/21

عن مستغانم

المسجل ب: كلية العلوم الدقيقة والإعلام الآلي / قسم: الرياضيات والإعلام الآلي

شعبة: الإعلام الآلي / التخصص:

الذكاء الاصطناعي والتدريب الآلي

والمكلف بإنجاز مذكرة ماستر بعنوان:

تخصيص هوية الأشخاص عن طريق بصمات الأصابع

أصرح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات العلمية
والنزاهة الأكاديمية المطلوبة في إنجاز البحث ، وأتحمل المسؤولية الشخصية عن كل
المحتوى المتضمن في البحث المذكور أعلاه .

التاريخ: 2025/06/21

إمضاء المعني



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة عبد الحميد بن باديس - مستغانم -
كلية العلوم الدقيقة والإعلام الآلي

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

الطالب(ة): بلكريس محمد رقم التسجيل الجامعي: 202037029671
الحامل لبطاقة التعريف الوطنية رقم: 100000963003270008 والصادرة بتاريخ: 05/07/2020
عن مستغانم

المسجل ب: كلية العلوم الدقيقة والإعلام الآلي / قسم: الإعلام الآلي
شعبة: الإعلام الآلي / التخصص: الذكاء الاصطناعي والآليات الذكية
والمكلف بإنجاز مذكرة ماستر بعنوان:

التعرف عن طريق البصمة

أصريح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات العلمية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث ، وأتحمل المسؤولية الشخصية عن كل المحتوى المتضمن في البحث المذكور أعلاه .

التاريخ: 24/06/2024

إمضاء المعني

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها.