République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE MOULOUD MAMMERI DETIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Filière : **Electronique**
Spécialité : **Instrumentation et systèmes embarqués**

Thème :

Identification des empreintes digitales basée sur une méthode holistique

Réaliser par :

ADLI Slimane
AMOUCHAS Hocine

Encadré par :

KHERCHAOUI Sonia

Membres du jury :

Mm OUSLIMANI Farida

Mm OUDJMIA Souad

Promotion : 2023/2024

Remerciements

On remercie Allah le tout puissant qui nous a donné le courage, la sagesse et la patience afin de réussir ce modeste travail

Je tiens à exprimer ma profonde gratitude à ma professeure encadrante ***KHARCHAOUI Sonia*** *Votre guidance, votre patience et vos précieux conseils ont été essentiels à la réalisation de ce mémoire. Vous avez su m'inspirer et me motiver tout au long de ce projet, et vos enseignements resteront gravés dans ma mémoire. Merci pour votre dévouement et votre soutien indéfectible.*

Avec toute ma reconnaissance,

Je tiens à exprimer ma profonde gratitude aux membres du jury Mm Ouslimani et Mm Oudjmia pour leur temps, leur attention et leurs précieux commentaires. Votre expertise et vos conseils ont grandement contribué à l'amélioration de ce mémoire. Merci pour votre engagement et votre bienveillance tout au long de ce processus.

J'adresse mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions.

Je remercie mes très chers parents, qui ont toujours été là pour moi.

Je remercie mes frères, pour leurs encouragements.

Enfin, je remercie mes amis et camarades qui ont toujours été là pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une grande aide.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

DÉDICACES

A ma très chère mère Djamila
Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père Arezki
Tu es mon bras droit , tu as toujours été à mes côtés pour me soutenir et m'encourager.

Que ce travail traduit ma gratitude et mon affection.
A mes très chers frères et sœurs (Mouh , Ahcene ,Sofiane)Puisse Dieu vous donne santé, bonheur, courage et surtout réussite
À ma chère grand-mère,

Ton amour, ta sagesse et ta bienveillance ont marqué ma vie de manière indélébile. Bien que tu ne sois plus parmi nous, ton souvenir continue de m'inspirer chaque jour. Ce mémoire est dédié à ta mémoire, en hommage à tout ce que tu as fait pour moi. Tu resteras toujours dans mon cœur.
Avec tout mon amour et ma gratitude

À mes chers amis,(Slimane,Melissa,Katia,Mouh,Said)
Votre soutien, votre amitié et vos encouragements ont été inestimables tout au long de ce parcours. Sans vous, ce mémoire n'aurait pas été possible. Je vous suis profondément reconnaissant pour votre présence et votre aide constante. Ce travail est dédié à vous, en signe de ma gratitude et de mon affection.

[HOCINE]

Dédicaces

A ma très chère mère Malika

Quoi que je fasse ou que je dise, je ne saurai point te remercier
comme il se doit. Ton affection me couvre, ta bienveillance me
guide et ta présence à mes côtés a toujours été ma source de force
pour affronter les différents obstacles.

A mon très cher père

Tu es mon bras droit , tu as toujours été à mes côtés pour me soutenir et m'encourager.
Que ce travail traduit ma gratitude et mon affection.

A mes très chers frères et sœurs (Mahdi , Amine , Lyes et Rima)Puisse Dieu vous donne santé, bonheur, courage et surtout réussite

À ma chère grand-mère,

Ton amour, ta sagesse et ta bienveillance ont marqué ma vie de manière indélébile. Bien que tu ne sois plus parmi nous, ton souvenir continue de m'inspirer chaque jour. Ce mémoire est dédié à ta mémoire, en hommage à tout ce que tu as fait pour moi. Tu resteras toujours dans mon cœur.

Avec tout mon amour et ma gratitude

À mes chers amis,(Hocine,Melissa,Katia,Idir,Said)

Votre soutien, votre amitié et vos encouragements ont été inestimables tout au long de ce parcours. Sans vous, ce mémoire n'aurait pas été possible. Je vous suis profondément reconnaissant pour votre présence et votre aide constante. Ce travail est dédié à vous, en signe de ma gratitude et de mon affection.

[SLIMANE]

Chapitre 1 :Généralité sur la biométrie

Chapitre 2 :Etat de l'art sur l'empreinte digitale

CHAPITRE 3 :Systéme d'identification des empreintes digitales Implémenté

CHAPITRE 4 :Résultats obtenus

Introduction générale

L'identification biométrique a émergé comme une solution incontournable dans les systèmes de sécurité et d'authentification modernes. Parmi les diverses méthodes biométriques, l'identification des empreintes digitales se distingue par son efficacité, sa fiabilité et sa facilité d'utilisation. Les empreintes digitales, avec leurs motifs uniques de crêtes et de sillons, offrent une méthode robuste pour identifier et authentifier les individus, ayant trouvé des applications dans des domaines variés tels que l'application de la loi, Contrôle d'accès aux bâtiments.

L'unicité et la permanence des empreintes digitales en font un outil précieux pour l'identification biométrique. Chaque individu possède des empreintes digitales distinctes qui ne changent pas au cours de sa vie, ce qui permet d'assurer une haute précision dans les processus d'identification. Cette caractéristique est particulièrement avantageuse dans les scénarios où une identification fiable et rapide est cruciale, comme dans les systèmes de contrôle d'accès sécurisés et les enquêtes criminelles.

Cependant, malgré son efficacité, l'identification des empreintes digitales n'est pas exempte de défis. Les variations dans la qualité des empreintes capturées, les déformations dues à la pression ou à l'angle de contact, et la présence de bruit ou de salissures peuvent affecter la précision des systèmes de reconnaissance. De plus, la gestion et la protection des données biométriques soulèvent des préoccupations importantes en matière de sécurité et de confidentialité.

Ce mémoire explore les techniques et méthodes utilisées pour améliorer la précision et la robustesse des systèmes d'identification des empreintes digitales. Nous examinerons en détail les caractéristiques distinctives des empreintes digitales, les technologies de capture, ainsi que les algorithmes de traitement et de comparaison. En particulier, nous nous concentrerons sur les approches holistiques, telles que les Local Binary Patterns (LBP), les cartes de distance et les machines à vecteurs de support (SVM), afin de proposer des solutions innovantes pour surmonter les défis actuels.

Les Local Binary Patterns (LBP) sont utilisés pour capturer les motifs de texture des empreintes digitales, offrant une représentation efficace pour la reconnaissance. Les cartes de distance permettent de mesurer les similarités entre les empreintes digitales en tenant compte des variations et des déformations. Enfin, les machines à vecteurs de support (SVM) sont employées pour classifier les empreintes digitales de manière précise et robuste.

Ce mémoire vise à explorer en profondeur les mécanismes de l'identification des empreintes digitales, à évaluer les récentes avancées technologiques, et à proposer des solutions pour renforcer la fiabilité et l'efficacité de ces systèmes. Notre objectif ultime est de contribuer au développement de systèmes biométriques plus solides, sécurisés et précis, répondant aux besoins croissants en matière de sécurité et d'authentification dans divers domaines d'application. Les sections suivantes de ce mémoire sont organisées comme suit :

Chapitre 1 : Dans ce chapitre, nous allons suivre l'évolution de la reconnaissance biométrique, mettre le point sur le concept et les bases de la reconnaissance automatique ainsi que sur les différentes modalités et une étude détaillée d'un système biométrique sera dressée avec ses domaines d'application.

Chapitre 2 : Nous présentons l'empreinte digitale comme modalité biométrique, et ses caractéristiques exploitées dans les différents types de reconnaissance ainsi que le processus général de sa reconnaissance.

Chapitre 3 : On exposera aussi les méthodes utilisées pour le prétraitement, l'extraction des caractéristiques, et la classification des données.

Chapitre 4 : Dans ce chapitre, nous donnons le principe de notre système de reconnaissance des empreintes digitales, la base de données utilisée et les résultats obtenus ainsi que des discussions.

Chapitre 1
Généralité sur la biométrie

1 Introduction

Face à la fraude documentaire et au vol d'identité, aux menaces du terrorisme ou de la cybercriminalité, et face à l'évolution logique des réglementations internationales, de nouvelles solutions technologiques sont mises en œuvre progressivement.

Parmi ces technologies, la biométrie s'est rapidement distinguée comme la plus pertinente pour identifier et authentifier les personnes de manière fiable et rapide, en fonction de caractéristiques biologiques uniques.

Figure (1) : exemple de dispositif d'identification des empreintes digitales.

Aujourd'hui, de nombreuses applications font appel à cette technologie. Ce qui était autrefois réservé à des applications sensibles telles que la sécurisation de sites militaires est devenu une application grand public en développement rapide [1].

2 La biométrie

La biométrie est la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu et permettant l'authentification de son identité.

Au sens littéral et de manière plus simplifiée, la biométrie signifie la "mesure du corps humain".

Nous distinguons deux catégories de technologies biométriques :

2.1 Les mesures physiologiques

Les mesures physiologiques peuvent être morphologiques ou biologiques.

Ce sont surtout les empreintes digitales, la forme de la main, du doigt, le réseau veineux, l'œil (iris et rétine), ou encore la forme du visage, pour les analyses morphologiques.

Figure (2) : deux aspectes très répondus de la biométrie l'identification par l'empreinte digital et par le gabarit du visage.

En matière d'analyses biologiques, on trouve le plus souvent l'ADN, le sang, la salive, ou l'urine utilisés dans le domaine médical, pour des investigations criminelles ou même dans le domaine du sport pour des contrôles de dopage.

2.2 Les mesures comportementales

Les mesures les plus répandues sont la reconnaissance vocale, la dynamique des signatures (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison), la dynamique de frappe au clavier d'un ordinateur, la façon d'utiliser des objets, la démarche, le bruit des pas, la gestuelle…

Les différentes techniques utilisées font l'objet de recherches régulières, de développements et bien entendu, d'améliorations constantes. Toutefois, les différentes sortes de mesures n'ont pas le même niveau de fiabilité. On estime que les mesures physiologiques ont l'avantage d'être plus stables dans la vie d'un individu.

2.3 Les technique d'identification les plus utilisées

2.3.1 Identification par l'empreinte digitale

La reconnaissance d'empreintes digitales est la technique biométrique la plus ancienne et c'est l'une des plus matures. Cependant les empreintes digitales sont une mesure biométrique assez mal acceptée par les utilisateurs à cause de l'association qui est souvent faite avec la criminologie. Cette méthode sera détaillée dans le chapitre 2.

2.3.2 Identification par l'iris

La reconnaissance de l'iris est une technologie des plus récente puisqu'elle ne s'est véritablement développée que dans les années 80, principalement grâce aux travaux de J. Daug-man [15]. L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d'un même individu sont différents. L'iris n'est pour l'instant pas modifiable par intervention chirurgicale. La reconnaissance de l'iris est donc aussi considérée comme une des méthodes biométriques les plus fiables qu'il soit.

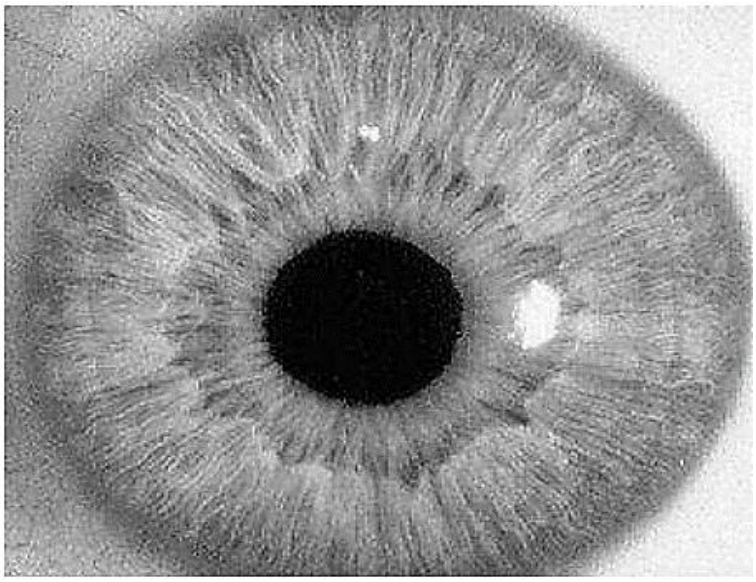


Figure (3) : L'iris de l'œil humaine

La capture de l'iris se fait par une caméra standard. Du fait des contraintes sur l'éclairage de l'œil, le capteur doit être assez proche de celui-ci (un mètre maximum) ce qui restreint les applications d'une telle technologie. L'éclairage de l'œil doit être uniforme et il faut éviter les

reflets. Bien que la reconnaissance de l'Iris soit moins contraignantes que la reconnaissance de la rétine, les gens ont également du mal à accepter cette biométrie .

2.3.3 Identification par la rétine

La reconnaissance de la rétine est une méthode assez ancienne puisque les premières études remontent aux années 30. Les motifs formés par les veines sous la surface de la rétine sont uniques et stables dans le temps. Ils ne peuvent être affectés que par certaines maladies. Pour ces raisons, la reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sures.

Figure (4) : Détail d'une rétine

Les systèmes d'acquisition de la rétine sont couteux. L'image est obtenue en projetant sur l'œil un rayon lumineux de faible intensité dans les fréquences visibles ou infrarouges. L'œil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes ce qui demande une grande coopération de sa part. Les personnes hésitent en général à approcher un organe aussi sensible que l'œil près de l'appareil de mesure ce qui explique pourquoi cette méthode est mal acceptée par le grand public [2].

2.3.4 Reconnaissance faciale

Elle se base sur une photographie du visage décomposée en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière non sujette à modification (haut des joues, coins de la bouche, distance entre différents points, formes….). Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou de lunettes, expression faciale inhabituelle, changement avec l'âge….)[5].

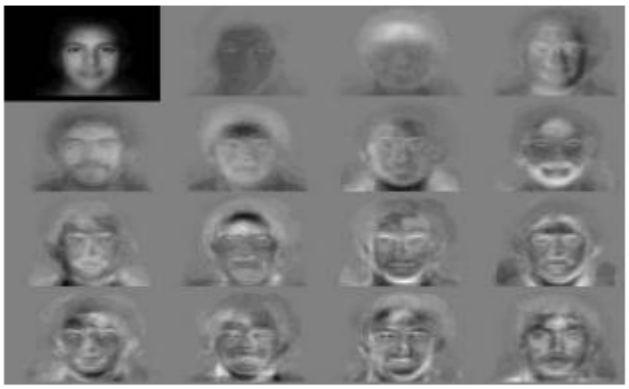


Figure (5): photographie du visage décomposé en plusieurs images

2.3.5 Identification par la voix

Elle est basée essentiellement sur la tonalité, la fréquence vocale et la distance entre la formation des lettres, et dépend grandement de la qualité d'enregistrement et de la méthode utilisée. nous distinguons les systèmes à texte prédéterminé où l'utilisateur doit répéter un texte qu'il ne choisit pas, et les systèmes où la personne peut parler librement. De plus, on doit tenir compte de la variabilité de la voix du locuteur dans le temps comme dans le cas de maladie (rhume,…), et des états émotionnels. Cette technique peut être utilisée sans obtenir le consentement de la personne identifiée [2].

2.3.6 Identification par la dynamique de frappe sur un clavier

Un système basé sur la dynamique de frappe sur un clavier ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ mille fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un t de passe. Initialement l'utilisateur doit composer son mot de passe à quelque reprise afin que soit constitué un gabarit de référence [2].

2.3.7 Authentification par la dynamique du tracé de la signature

Elle est basée sur l'analyse et le calcul de la dynamique d'une signature. Ce système est basé sur des critères précis comme la pression, l'accélération, la souplesse, les courbes. La falsification est possible en passant par une phase d'apprentissage, la signature peut varier selon le stress de l'utilisateur [2].

2.3.8 Analyse de traces biologiques

Ces procédés se basent sur des prélèvements (salive, urine, sang, ADN, odeur). Certaines de ces technique sont très prometteuses (iris) et commencent à émerger, d'autre sont encore au stade expérimental (analyse comportementale). Mais l'utilisation des empreintes digitales reste la méthode la plus aboutie actuellement [2][25].

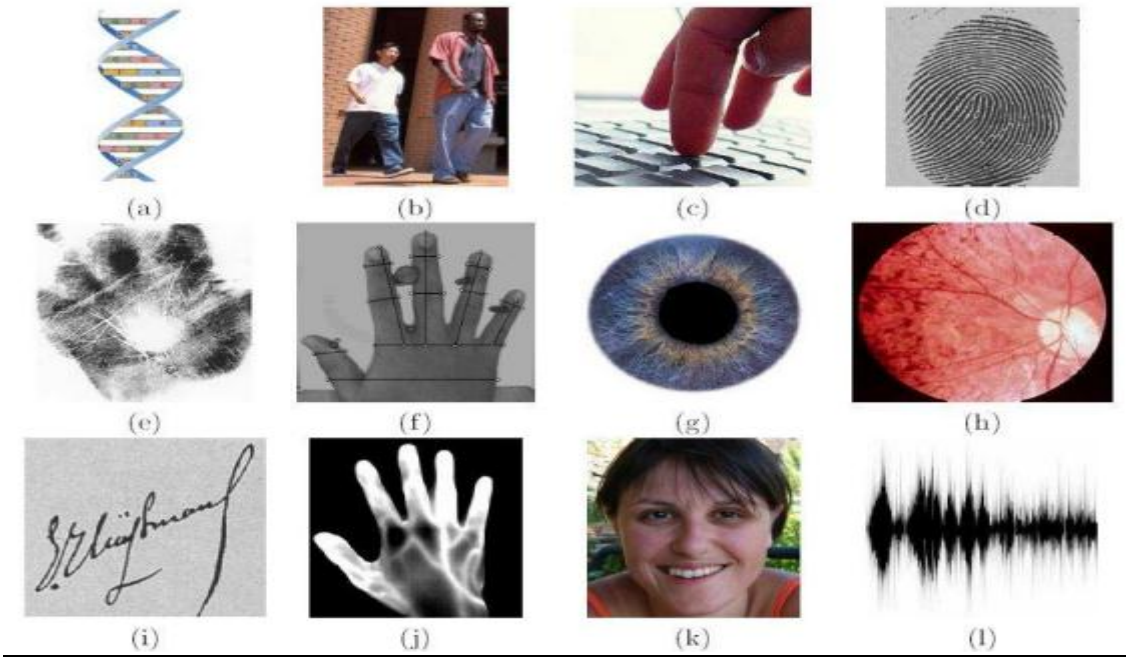


Figure (6) : Les principales caractéristiques biométriques : (a) ADN, (b) Démarche, (c) Dynamique de la frappe au clavier, (d) Empreinte digitale, (e) Empreinte palmaire, (f) Géométrie de la main, (g) Iris, (h) Rétine, (i) Signature, (j) Thermographie de la main, (K) visage, et (l) voix.

3 Conclusion :

En conclusion, ce chapitre a offert un aperçu général de la biométrie et de ses différentes méthodes d'identification, y compris les empreintes digitales, la reconnaissance faciale, la reconnaissance de l'iris et la reconnaissance vocale. Nous avons vu comment la biométrie dépasse les méthodes traditionnelles grâce à des solutions d'identification plus sécurisées et précises.

Parmi ces techniques, l'identification par empreintes digitales se distingue par sa fiabilité et son adoption répandue, en raison de son équilibre entre sécurité, coût et facilité d'utilisation. La reconnaissance faciale offre une analyse sans contact, la reconnaissance de l'iris est extrêmement précise, et la reconnaissance vocale permet une identification pratique et non intrusive.

Les progrès technologiques continuent d'améliorer ces systèmes biométriques, bien que des préoccupations liées à la protection de la vie privée et à l'éthique demeurent.

Ce chapitre pose les bases pour notre étude approfondie de l'identification par empreintes digitales. Le prochain chapitre examinera spécifiquement les caractéristiques, les techniques de capture et les algorithmes de comparaison associés à cette méthode biométrique.

Chapitre 2

Etat de l’art sur l’empreinte digitale

1 Introduction

L'identification des empreintes digitales a longtemps été au cœur des systèmes de sécurité et de contrôle d'accès, offrant une méthode fiable et précise pour l'authentification des individus. Traditionnellement, cette identification repose sur des méthodes minutieuses, mettant en évidence les caractéristiques spécifiques des empreintes digitales, telles que les crêtes et les vallées, ou sur des approches basées sur les points singuliers, où seuls certains points clés sont extraits pour la comparaison. Cependant, ces méthodes traditionnelles peuvent présenter des défis dans des situations où les empreintes digitales sont partiellement endommagées ou altérées, ou lorsque les ensembles de données sont vastes et hétérogènes.

Face à ces défis, une approche émergente et prometteuse dans le domaine de l'identification des empreintes digitales est la méthode holistique. Contrairement aux méthodes traditionnelles qui se concentrent sur des caractéristiques spécifiques ou des points singuliers, la méthode holistique prend en compte l'ensemble de l'empreinte digitale dans sa totalité, en utilisant des techniques de traitement d'image et d'analyse des motifs pour extraire des informations globales et complexes. Cette approche offre un potentiel significatif pour améliorer la robustesse et la précision de l'identification des empreintes digitales, même dans des conditions difficiles.

2 Historique

Les premières traces d'utilisation d'empreintes digitales ont été découverte en Egypte et date de l'époque des pyramides il y a plus de 4000 ans. Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient surement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable. C'est en 1856 que l'anglais William Herschel, après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, commença à comprendre que les empreintes étaient uniques et constates dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, invariance, minuties, classification….) et en 1901 la technique d'identification au moyen des empreintes fut adoptée officiellement en Angleterre dans le système judiciaire.

Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires [2]. Le premier fichier d'empreintes est mis en place en

Argentine en 1891.De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable.

2.1 Définition de l'empreinte digitale

Une empreinte digitale est une impression unique et distinctive formée par les crêtes et les vallées présentes sur la surface des doigts et des pouces humains. Ces impressions digitales sont des motifs biologiques uniques à chaque individu, même entre des jumeaux identiques. Les empreintes digitales sont généralement utilisées pour l'identification et l'authentification biométriques dans une variété de domaines, y compris la sécurité, la criminalistique, les systèmes de contrôle d'accès et les dispositifs de déverrouillage des appareils électroniques.

Sur le plan anatomique, les empreintes digitales sont formées par les crêtes papillaires et les sillons présents sur la peau des doigts. Ces crêtes et sillons forment des motifs complexes qui sont généralement divisés en trois types principaux : les arcs, les boucles et les tourbillons. Ces motifs uniques sont établis pendant la période de développement fœtal et restent relativement inchangés tout au long de la vie d'un individu, à l'exception de petites variations dues à des blessures, des cicatrices ou d'autres altérations de la peau.

Les empreintes digitales sont acquises à l'aide de capteurs d'empreintes digitales, qui enregistrent les détails des crêtes et des vallées à travers un processus d'imagerie ou de balayage. Ces informations sont ensuite traitées et analysées pour extraire des caractéristiques distinctives, telles que les bifurcations, les points de terminaison et les segments de crête, qui sont utilisées pour représenter de manière unique chaque empreinte digitale.

En raison de leur caractère unique et permanent, les empreintes digitales sont largement utilisées pour l'identification et l'authentification des individus dans les systèmes de sécurité et les applications biométriques. L'analyse des empreintes digitales est également une composante essentielle des enquêtes criminelles, permettant l'identification des suspects et la résolution d'affaires judiciaires en comparant les empreintes digitales relevées sur le lieu d'un crime avec celles stockées dans les bases de données criminelles [15].

2.2 Caractéristiques des empreintes digitales

Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles forment un motif unique pour chaque individu (Figure 7), nous distinguons :

- Les crêtes (ou les stries), ce sont les lignes en contact avec une surface au toucher. Les crêtes contiennent en leur centre un ensemble de pores régulièrement espacés.
- Les vallées : sont les creux entre deux crêtes.

Chaque empreinte possède un ensemble de points singuliers globaux (les centres ou noyaux et les deltas) et locaux (les minuties). Les centres correspondent à des lieux de convergences des crêtes tandis que les deltas correspondent à des lieux de divergence. Les minuties peuvent prendre seize configurations différentes comme le montre la figure 8. Mais en général les algorithmes ne s'intéressent qu'aux bifurcations et terminaisons qui permettent d'obtenir les autres types par combinaison.

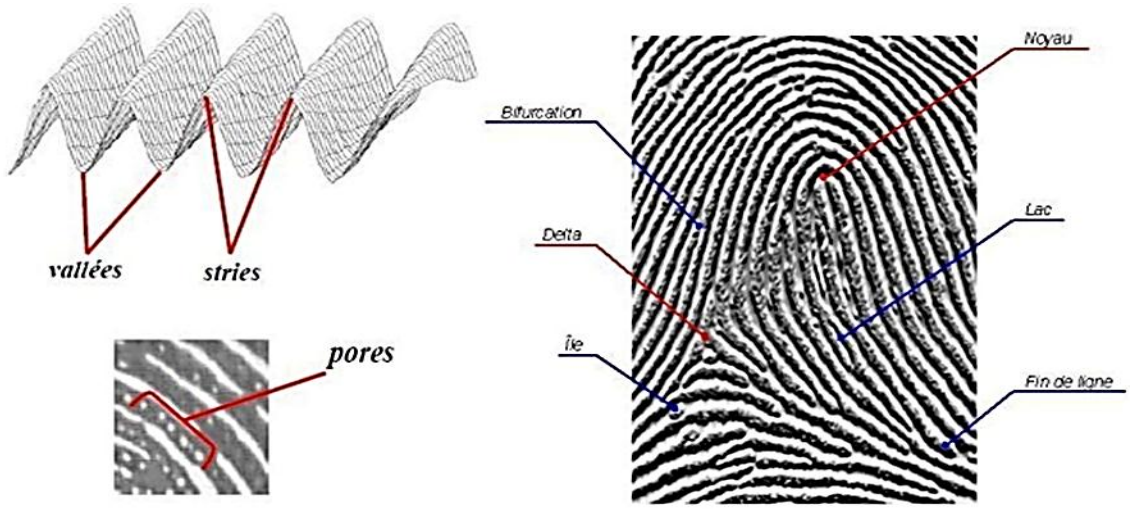
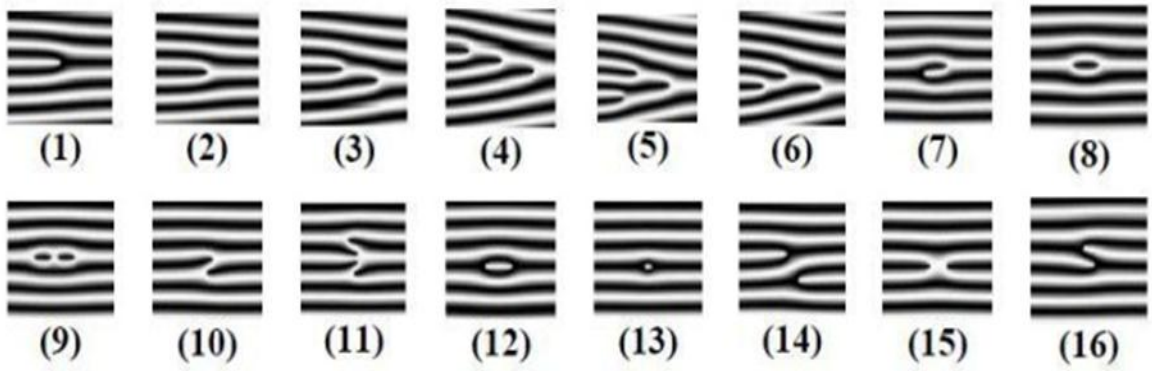


Figure (7) : Caractéristiques d'une empreinte digitale



1.	terminaison	9.	boucle double
2.	bifurcation simple	10.	pont simple
3.	bifurcation double	11.	pont jumeau
4.	bifurcation triple I	12.	intervalle
5.	bifurcation triple II	13.	point isolé
6.	bifurcation triple III	14.	traversée
7.	crochet	15.	croisement
8.	boucle simple	16.	tête bêche

Figure (8) : Les différents types de minutie (crêtes en noir)

Parmi les types des minuties rapportés dans la figure (Figure 9), deux types sont les plus utilisés pour extraire une signature mathématique extrêmement fiable pour l'identification, ce sont les fins de crêtes, (fin d'une ride), et la bifurcation, le point sur la ride où deux branches dérivent.

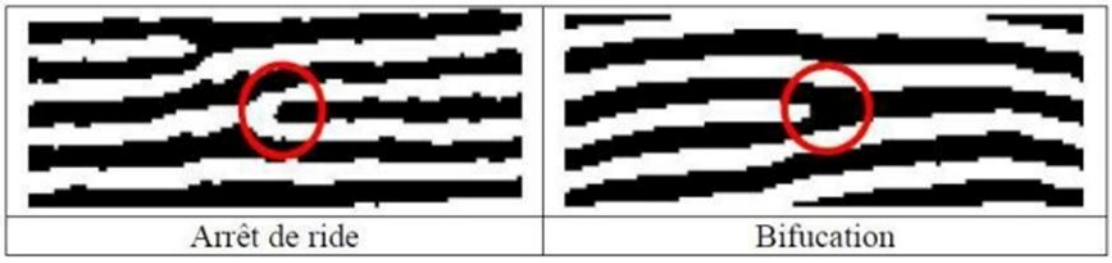


Figure (9) : Deux types de minuties les plus utilisés

La position et le nombre de centres et des deltas permettent de classifier les empreintes en catégorie selon leur motif général. On distingue principalement trois grandes familles (voir Figure 10). Ces trois types d'empreintes regroupent 95% des doigts humains, il existe aussi des dessins beaucoup plus rares comme les doubles boucles :

- Les boucles (loop) représentent 60% des empreintes rencontrées.
- Les spires (whorl) représentent 30% des empreintes rencontrées.
- Les arches (arch) représentent 5% des empreintes rencontrées.

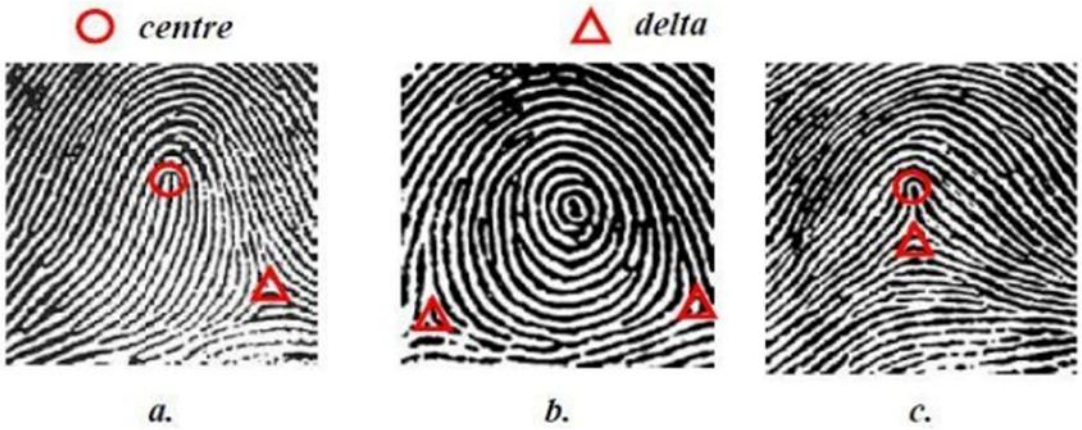


Figure (10) : Les classes d'empreintes : boucle (a), spire (b), arche (c)

Ces trois formes d'empreintes digitales peuvent être déclinées en sous-parties : Boucle à droite, boucle à gauche, double tourbillon (boucle).

L'ensemble formé par la disposition des points singuliers constitue un motif unique pour chaque individu, en effet l'empreinte digitale se forme aux alentours de la treizième semaine de grossesse, le motif général est influencé par les gènes héréditaires, la vitesse de croissance des doigts, l'alimentation du fœtus ou encore la pression sanguine, qui dépend de la taille du cordon ombilical, mais l'apparition des détails (minuties) est créée de manière accidentelle par des pressions variables aléatoire sur les surfaces tactiles.

C'est ce processus qui rend chaque empreinte unique. Même de vrais jumeaux n'ont pas les mêmes empreintes, car le diamètre du cordon ombilical n'est jamais le même pour les deux enfants [12]. De plus les empreintes une fois formées ne changent plus au cours de la vie d'une personne, ces deux caractéristiques en font un moyen de reconnaissance très efficace [6].

2.3 Structure d'un système complet de reconnaissance d'empreintes

Un système automatique complet de reconnaissance d'empreintes digitales est une chaîne de processus qui à partir de l'empreinte digitale d'un utilisateur produit un résultat déterminant l'accès de l'utilisateur à des ressources protégées. La conception de ce type de

système a fait l'objet de nombreuses recherches, proposant diverses méthodes de traitement [3]. Malgré ces variations, les systèmes suivent toujours la même structure générale (Figure 11).

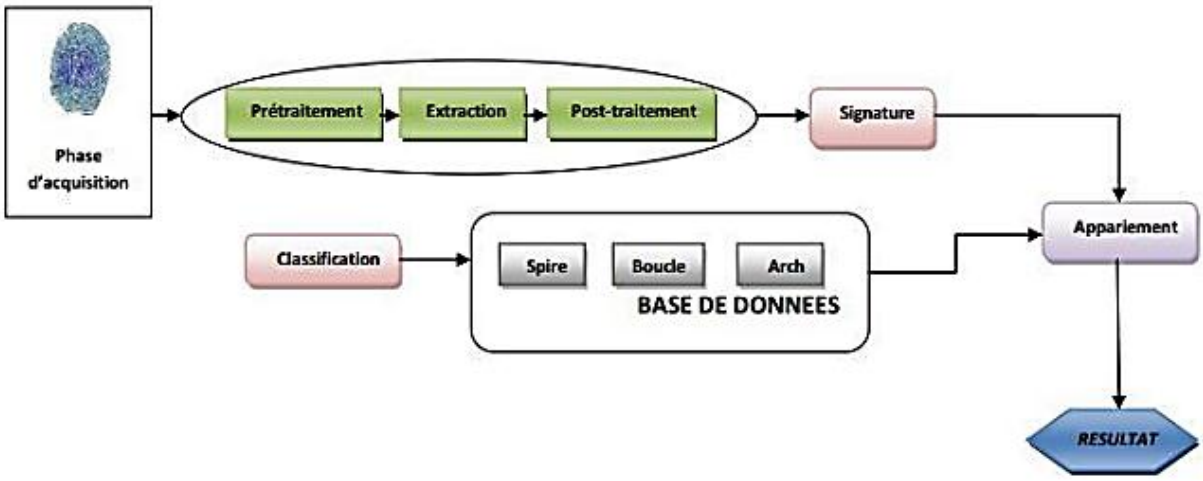


Figure (11): Architecture générale d'un système complet de reconnaissance d'empreintes [3]

La première étape consiste à obtenir une image de l'empreinte digitale de l'utilisateur (acquisition). Cette image subit ensuite un prétraitement pour extraire les informations pertinentes (signature). Un traitement supplémentaire peut être appliqué pour éliminer les erreurs potentielles apparues durant la chaîne de traitement. Si le système est utilisé pour créer une base de données (stockage), la signature peut être compressée puis stockée grâce à une technique de classification.

Pour un système d'identification, les empreintes stockées dans la base de données qui pourraient correspondre à celle de l'utilisateur (modèle identique) sont désarchivées et comparées une par une (appariement). Si une correspondance est trouvée, le système renvoie des informations personnelles concernant l'utilisateur. Dans le cas d'un système de vérification, une seule comparaison est effectuée et un résultat binaire (acceptation ou rejet) est renvoyé, permettant de déterminer si l'utilisateur est autorisé ou non.

2.4 Les capteurs

2.4.1 Les capteurs optiques d'empreinte

La méthode optique est l'une des plus courantes pour la reconnaissance d'empreintes digitales. Elle utilise un appareil-photo CCD (Dispositif Charge Couplé) qui se compose de diodes sensibles à la lumière appelées photo sites. Le doigt est placé sur une surface en verre, et le CCD capture l'image en utilisant une rangée de LED pour illuminer les creux et les bosses du doigt. Les systèmes optiques sont avantageux en raison de leur coût faible, mais ils sont faciles à contourner. Un autre problème est la présence d'empreintes latentes, c'est-à-dire les traces laissées par les empreintes précédentes sur le capteur [4].

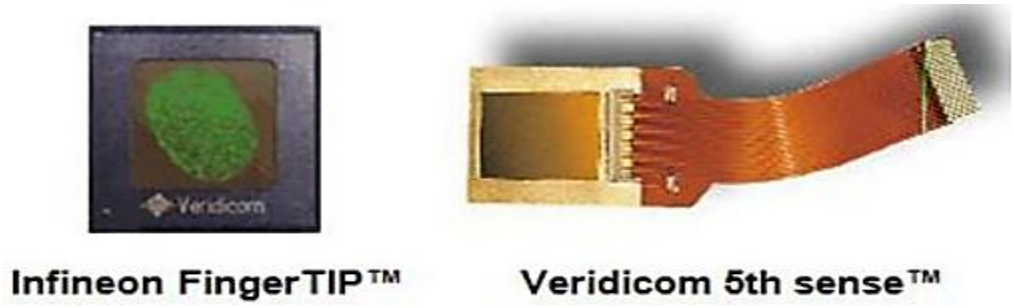


Figure (12) : Les capteurs optiques d'empreinte [4]

2.4.2 Les capteurs électriques-thermique

La méthode de reconnaissance d'empreintes digitales consiste à faire glisser le doigt le long du capteur, qui mesure la différence de température entre les creux de la peau et l'air dans les bosses. Cette méthode produit des images de haute qualité même avec des empreintes de mauvaise qualité, comme des doigts secs. La technologie thermique fonctionne bien dans des conditions environnementales difficiles et aide à nettoyer le capteur, empêchant les empreintes résiduelles. Cependant, elle a l'inconvénient d'augmenter la consommation électrique en raison du chauffage du capteur [4].

Figure (13): Les capteurs électriques-thermique [4]

2.4.3 Capteurs capacitifs

La méthode capacitive est l'une des plus populaires pour la reconnaissance d'empreintes digitales. Elle utilise des condensateurs électriques pour mesurer les creux et les bosses de l'empreinte, composés de cellules minuscules avec deux plaques conductrices recouvertes d'un revêtement protecteur. L'avantage principal est qu'elle nécessite une véritable empreinte digitale. Cependant, cette méthode rencontre des difficultés avec les doigts secs et humides. [4]

Figure (14) : Capteurs capacitifs [4]

2.4.4 Capteurs de champ-électrique

Ce capteur utilise un champ électrique pour mesurer au-delà de la couche extérieure de la peau où l'empreinte digitale commence. Cette technologie peut fonctionner dans des conditions extrêmes, même avec un doigt sale ou sec. Le champ électrique crée une représentation des creux et des bosses de la couche épidermique du doigt, et les signaux sont mesurés par un amplificateur de sous-pixel. Les capteurs travaillent ensemble pour produire une image plus claire de l'empreinte digitale par rapport aux technologies optiques ou capacitives. Cependant, ils ont une résolution d'image plus faible et une zone d'image plus petite, ce qui entraîne un taux d'erreur élevé [4].

Figure (15) : Capteurs de champ-électrique [4]

3 Conclusion

En résumé, ce chapitre nous a présenté les empreintes digitales et leurs états de l’art. En comprenant les caractéristiques uniques de ces empreintes et en examinant les différents types de capteurs utilisés pour les reconnaître, nous avons acquis une compréhension approfondie de cette technologie cruciale dans le domaine de la sécurité et de la biométrie. De la structure des empreintes digitales à celle des capteurs, nous avons exploré les fondements de cette science, ouvrant la voie à des avancées continues dans le domaine de la sécurité des données et de l'authentification. Ce chapitre nous a non seulement éclairés sur les progrès actuels, mais a également suscité notre curiosité pour les développements futurs dans ce domaine en constante évolution.

1 Introduction

L'identification des empreintes digitales est une technique biométrique largement utilisée pour des applications de sécurité et de criminalistique. Ce chapitre détaille les étapes de la programmation d'un système d'identification des empreintes digitales en utilisant MATLAB, depuis l'acquisition de l'image et traitant l'image empreinte entière jusqu'à la classification via un modèle SVM (Support Vector Machine).

2 Système d'identification des empreintes digitales

2.1 L'Acquisition de l'Image

L'acquisition de l'image constitue la première étape et une des plus cruciales dans le processus d'identification des empreintes digitales. Elle établit la base sur laquelle toutes les étapes subséquentes de traitement, d'extraction de caractéristiques et de classification reposent.

Assurer que l'image acquise conserve l'intégrité des détails biométriques évite les problèmes de déformation ou de perte de données cruciales. La préservation des détails authentiques des empreintes est fondamentale pour des analyses biométriques fiables. L'acquisition d'images doit également prendre en compte la sécurité et la confidentialité des données biométriques.

Une acquisition correcte et de haute qualité est essentielle pour garantir une identification précise et fiable. Voici plusieurs raisons expliquant l'importance de cette étape :

2.1.1 Qualité de l'Image

La réduction des erreurs est cruciale dans les applications de sécurité et de criminalistique où des décisions importantes dépendent de :

- La clarté et la haute résolution de l'image empreinte permettent de capturer les détails fins des crêtes et des vallées des empreintes digitales. Les détails précis sont essentiels pour distinguer des caractéristiques uniques et pour assurer une correspondance exacte lors de la phase de comparaison.
- Les images de mauvaise qualité (floues, bruitées ou mal éclairées) compliquent les étapes de prétraitement et d'extraction des caractéristiques. Une image de haute qualité minimise le besoin de traitement intensif pour corriger les défauts, réduisant ainsi le risque de perte d'information critique.
- Les algorithmes de correspondance et de classification reposent sur des caractéristiques distinctes des empreintes digitales.

- Une image de haute qualité améliore la fiabilité de l'extraction des minuties (points caractéristiques) et des motifs, augmentant ainsi les taux de correspondance correcte.
- Une acquisition de haute qualité réduit les erreurs d'identification telles que les faux positifs (identification incorrecte) et les faux négatifs (non-reconnaissance d'une empreinte correcte).

2.2 Préparation pour le Prétraitement

Une image correctement acquise avec des niveaux de gris équilibrés et un contraste approprié facilite les étapes de prétraitement comme le filtrage et la binarisation. Moins de prétraitement nécessaire permet de conserver l'intégrité des caractéristiques originales des empreintes digitales.

Des images uniformes et cohérentes en termes de qualité et de format permettent des traitements standardisés, améliorant ainsi la performance des algorithmes de traitement d'images et de classification.

En résumé, l'acquisition de l'image est une étape fondamentale qui conditionne la qualité et la fiabilité de l'ensemble du processus d'identification des empreintes digitales. Une acquisition de haute qualité permet de maximiser la précision de l'identification, de réduire les erreurs et de faciliter les étapes de traitement ultérieures. Elle assure également que les données biométriques sont préservées dans leur forme la plus authentique et sécurisée, renforçant ainsi la confiance dans les systèmes d'identification des empreintes digitales.

2.2.1 L'égalisation de l'histogramme:

L'égalisation de l'histogramme est une technique efficace pour améliorer le contraste des images, rendant les détails plus visibles et l'image globalement plus informative. Bien qu'elle ait des limitations, elle reste un outil précieux dans le traitement et l'analyse d'images.

L'égalisation d'histogramme consiste à élargir la distribution des valeurs des pixels d'une image de manière à accroître l'information de perception. L'histogramme d'une image d'empreinte digitale est de type bimodal (Figure (16)), l'histogramme après l'égalisation occupe toute la gamme de 0 à 255 et l'effet de visualisation est par conséquent amélioré (Figure (16))[33].

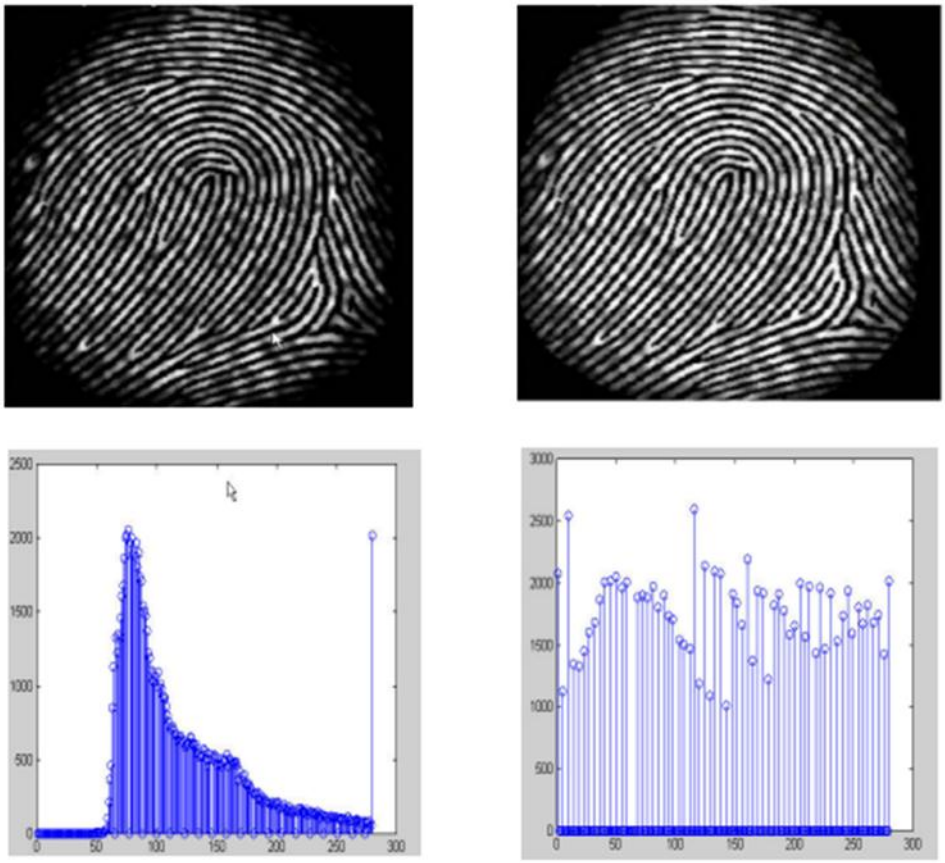


Figure (16) : L'image de l'empreinte et son histogramme (a) avant l'égalisation (b) après l'égalisation.

2.2.2 Le seuillage d'image :

Le seuillage d'image est une technique de binarisation d'image, consistant à remplacer les niveaux de gris d'une image par un ensemble de pixels prenant la valeur 255 (blanc) ou 0 (noir) selon que sa valeur initiale est inférieure ou supérieure à une valeur définie comme seuil[32].

2.2.3 Le filtrage:

Le filtrage en prétraitement d'images consiste à transformer une image pour améliorer sa qualité et faciliter les étapes suivantes d'analyse. Il permet de réduire le bruit, d'accentuer les contours, de lisser les variations d'intensité et d'améliorer le contraste. Les types de filtrage couramment utilisés incluent le filtre médian (réduit le bruit impulsionnel), le filtre gaussien (lisse l'image et réduit le bruit gaussien), et le filtre passe-haut (met en évidence les détails fins et les contours). Ces techniques sont essentielles pour préparer les images pour des analyses avancées, telles que l'extraction de caractéristiques et la classification.

Nous avons fait le choix de suivre de méthode de traitement et d'extraction des caractéristiques soient :

2.3 Identification des empreintes digitales par la carte des distances

2.3.1 Binarisation de l'Image

La binarisation est le processus qui consiste à convertir une image en niveaux de gris en une image binaire, où chaque pixel est représenté soit en noir soit en blanc. Cette transformation est cruciale dans le traitement des empreintes digitales, car elle simplifie l'image pour les étapes ultérieures d'extraction de caractéristiques et de comparaison.[26]

2.3.1.1 Objectif de la Binarisation

L'objectif principal de la binarisation est de distinguer les crêtes (ridges) des vallées (valleys) dans les empreintes digitales dans les méthodes classiques. En transformant l'image en niveaux de gris en une image binaire, nous facilitons l'identification des caractéristiques clés des empreintes, comme les minuties (points de terminaison et bifurcations des crêtes) .

Image en niveau de gris image binarisée

Figure(17): Binarisation

2.3.1.2 Méthode Utilisée

Pour binariser une image en niveaux de gris, on utilise généralement une méthode de seuillage global. La méthode d'Otsu est l'une des techniques les plus populaires pour déterminer automatiquement le seuil de binarisation optimal.

1. On part d'une image déjà en niveaux de gris.
2. Un seuil est calculé pour diviser les pixels de l'image en deux classes : ceux à convertir en blanc et ceux à convertir en noir.
3. Les pixels de l'image sont comparés au seuil calculé et convertis en noir ou blanc en conséquence.

La méthode d'Otsu :

La méthode d'Otsu est une technique de seuillage global[17] utilisée en traitement d'images pour convertir une image en niveaux de gris en une image binaire. Cette méthode, développée par Nobuyuki Otsu, cherche à déterminer automatiquement un seuil optimal qui minimise la variance intra-classe et maximise la variance inter-classe des niveaux de gris. En d'autres termes, elle cherche le seuil qui sépare les pixels en deux groupes distincts de manière à ce que la dispersion des niveaux de gris soit la plus faible possible au sein de chaque groupe, tout en maximisant la différence entre les groupes. Cette méthode est particulièrement utile pour segmenter les objets d'intérêt dans une image de fond en une étape simple et efficace.

2.3.2 Carte de Distance

La carte de distance est une transformation d'image qui assigne à chaque pixel de fond (noir) une valeur représentant la distance à son pixel de premier plan (blanc) le plus proche. Ce concept est essentiel dans le traitement d'images binaires pour diverses applications telles que la reconnaissance de formes, la segmentation, et l'analyse des structures.

- L'objectif principal de la carte de distance est de quantifier les distances entre les pixels de fond et les pixels de premier plan, fournissant ainsi une représentation utile pour l'extraction et l'analyse des caractéristiques géométriques des objets dans une image.
- Nous avons utilisé 4 types de carte de distance pour l'extraction de caractéristiques qui sont :

2.3.2.1 Types de Distances

Il existe plusieurs types de distances qui peuvent être utilisées pour calculer la carte de distance, chacune ayant ses propres propriétés et applications [18]. Les principaux types de distances sont :

A. Distance Euclidienne

La distance euclidienne est la distance "en ligne droite" entre deux points dans un espace euclidien. C'est la mesure de la longueur du segment de ligne droite qui relie deux points [18].

- Formellement, la distance euclidienne entre deux pixels (i, j) et (x, y) est calculée comme suit :
- distance $= \sqrt{(\mathrm{i} - \mathrm{x})^2 + (\mathrm{j} - \mathrm{y})^2}$

Propriétés :

- Représente la distance géométrique réelle.
- Utilisée dans des analyses où la distance directe est pertinente, par exemple, dans les applications de géométrie ou de physique.

Applications :

- Analyse géométrique des formes.
- Reconnaissance de formes et d'objets.
- Extraction de caractéristiques dans les images d'empreintes digitales.

B. Distance de Manhattan (City Block)

Aussi connue sous le nom de distance L1, la distance de Manhattan mesure la distance entre deux points en se déplaçant uniquement le long des axes orthogonaux (à angles droits)[18].

- La formule pour calculer la distance de Manhattan entre deux pixels (i, j) et (x, y) est:
- Distance = $| i - x | + | j - y |$

Propriétés :

- La distance est mesurée le long des chemins parallèles aux axes de la grille.
- Appropriée pour les environnements structurés en grille, comme les villes.

Applications :

Planification de trajectoires dans les environnements urbains.

- Jeux vidéo et simulations où le mouvement est restreint à des directions orthogonales.
- Analyse d'images dans des contextes structurés.

C. Distance de Chebyshev (Chessboard)

Aussi connue sous le nom de distance L∞, la distance de Chebyshev mesure la distance entre deux points comme étant la plus grande des distances le long des axes x et y[18].

- La formule pour calculer la distance de Chebyshev entre deux pixels (i, j) et (x, y) est :
- Distance de Chebyshev= $max(|i - x|, |j - y|)$

Propriétés :

- Permet les mouvements en diagonale aussi bien qu'orthogonaux.
- La distance entre deux points est le nombre minimal de mouvements de roi nécessaires sur un échiquier.

Applications :

- Jeux de stratégie comme les échecs, où le mouvement en diagonale est permis.

- Traitement d'images où les objets peuvent se déplacer librement dans toutes les directions.

D. Distance Quasi-Euclidienne

La distance quasi-euclidienne est une approximation de la distance euclidienne, qui utilise une table de distances pré-calculées pour réduire la complexité de calcul. Cette méthode offre une bonne approximation de la distance euclidienne réelle avec des calculs moins intensifs [18].

.distance Quasi-Euclidienne= $|i - x| + (\sqrt{2} - 1)\,|j - y|$

Propriétés :

- Rapide à calculer par rapport à la distance euclidienne exacte.
- Donne des résultats proches de ceux obtenus avec la distance euclidienne.

Applications :

- Situations où la précision de la distance euclidienne est souhaitée, mais où les ressources de calcul sont limitées.
- Traitement d'images en temps réel et applications de reconnaissance où la vitesse est cruciale.

Remarque 1: Chacune de ces distances offre des perspectives et des avantages différents en fonction des besoins spécifiques de l'application. La compréhension et l'utilisation appropriée de ces différentes cartes de distance permettent d'optimiser les processus de traitement d'images pour des tâches variées allant de la reconnaissance de formes à l'analyse géométrique des objets.

Remarque 2 : une fois la matrice carte des distance est obtenue, nous la transformons en vecteur qui est en-fait le vecteur caractéristique qui sera transmis au classifieur choisit.

2.4 Identification des empreintes digitales par les motifs binaires locaux LBP

Avant d'appliquer les LBP nous devons :

- Redimensionner chaque image empreinte en une image 256*256.
- Partitionner l'image empreinte en plusieurs imagettes 32*32.

2.4.1 Motifs binaires locaux (LBP)

Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris [27].

Le concept du LBP est simple [10], il attribue un code binaire à un pixel en fonction de son voisinage. Ce code, qui décrit la texture locale d'une région, est calculé en comparant les niveaux de gris des pixels voisins avec celui du pixel central. Pour générer un motif binaire,

chaque voisin prend la valeur "1" si sa valeur est supérieure ou égale à celle du pixel central, sinon il prend la valeur "0" (Figure18). Les pixels de ce motif binaire sont ensuite multipliés par des poids et sommés pour obtenir le code LBP du pixel central. Ainsi, pour toute l'image, on obtient des pixels dont l'intensité varie entre 0 et 255, comme dans une image en niveaux de gris sur 8 bits. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut utiliser un histogramme de dimension 255 comme descripteur de texture.

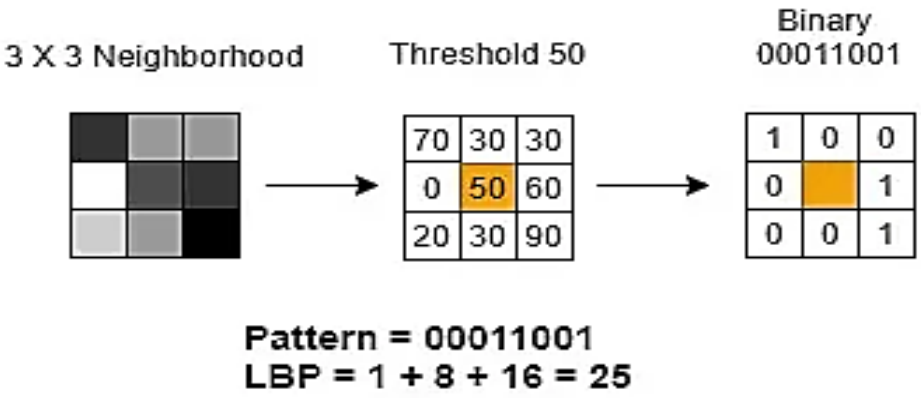


Figure (18): Algorithme pour calculer un motif binaire local (LBP)

Le LBP de base est défini par cette formule :

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} S(g_p - g_c) \times 2^p$$

Où : $\boldsymbol{gc}$ est le niveau de gris du pixel central de coordonnées $(\boldsymbol{xc}, \boldsymbol{yc})$.

$\boldsymbol{gp}(p = 0,1,\ldots,7)$ est le niveau de gris de chaque pixel environnant.

Si $\boldsymbol{gp}$ est plus petit que $\boldsymbol{gc}$

Le résultat binaire du pixel prend la valeur 0, sinon (supérieure ou égale), il sera mis à 1.

Avec : S(x) une fonction définie comme suit :

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

- pour chaque pixel central, on regarde ses voisins dans un certain rayon (habituellement de 3x3 pixels).
- Chaque voisin reçoit un '1' si sa valeur est supérieure ou égale à celle du pixel central, sinon un '0'.

- Les bits obtenus sont alors convertis en une valeur décimale qui représente le LBP du pixel central.

Remarque : Les Local Binary Patterns (LBP) sont une technique simple mais puissante pour l'analyse de textures et la reconnaissance de motifs dans les images. Leur efficacité et leur simplicité ont conduit à leur adoption dans de nombreuses applications en vision par ordinateur(classification de texture, reconnaissance faciale, en détection d'objets…)

2.5 La classification

Une fois que le vecteur caractéristique est obtenu il est transmis au classifieur qui est dans notre cas les machines à vecteur à support.

Nous avons fait le choix d'utiliser le même classifieur pour les deux méthodes de traitement et d'extraction de caractéristiques. Nous avons utilisé une commande MATLAB pour les SVM

2.6 Les Machines à Vecteurs de Support SVM (support vector machine)

Les Machines à Vecteurs de Support (SVM) sont une classe d'algorithmes d'apprentissage supervisé (apprentissage machine) utilisés principalement pour les problèmes de classification et de régression. Elles ont été introduites par Vladimir Vapnik[22] et son équipe dans les années 1990 et ont depuis connu un large succès en raison de leur robustesse et de leur capacité à gérer des espaces de grande dimension.

2.6.1 Principe

Les SVM cherchent à trouver l'hyperplan optimal qui sépare les données de différentes classes avec la plus grande marge possible. Un hyperplan dans un espace n-dimensionnel (où n est le nombre de caractéristiques) est une surface qui divise l'espace en deux sous-espaces. En classification binaire, les SVM cherchent le meilleur hyperplan qui sépare les points de données de deux classes différentes avec la plus grande marge, c'est-à-dire la distance maximale entre les points de données les plus proches (appelés vecteurs de support) de chaque classe et l'hyperplan [21][23].

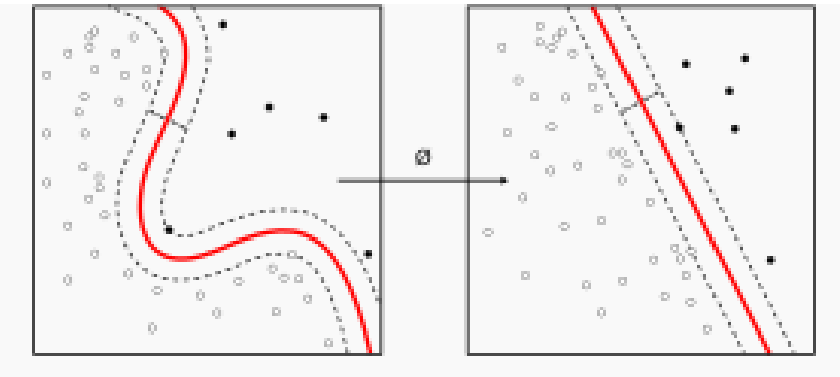


Figure (19): Machine à vecteurs de support

L'idée fondamentale des SVM repose sur l'utilisation de fonctions noyau (kernels), qui permettent une séparation optimale des points dans différentes catégories. Cette méthode utilise un ensemble de données d'apprentissage pour établir un hyperplan qui sépare au mieux les points.

Les SVM visaient à séparer linéairement des objets appartenant à deux classes différentes à l'aide d'un hyperplan optimal. Cette méthode a ensuite été étendue pour traiter des cas multi classes.

L'ensemble d'apprentissage constitué d'objets caractérisés par un vecteur de k composantes chacun, appartenant à deux classes différentes : une classe positive étiquetée +1 et une classe négative étiquetée -1. De même soit également $yi \in \{1, -1\}$ la variable représentant les étiquettes des deux classes. L'objectif des SVM est de déterminer la frontière linéaire définie par l'équation $\boldsymbol{wx} + \boldsymbol{b}$ entre les objets positifs et les objets négatifs, comme illustré à la Figure 2 où **w** représente le vecteur normal à ce séparateur linéaire et $\boldsymbol{b}$ le biais. Déterminer un hyperplan revient à définir le couple de valeurs (**w**,**b**) qui le caractérise. Étant donné que plusieurs solutions sont possibles, quel critère détermine donc la séparation optimale ?

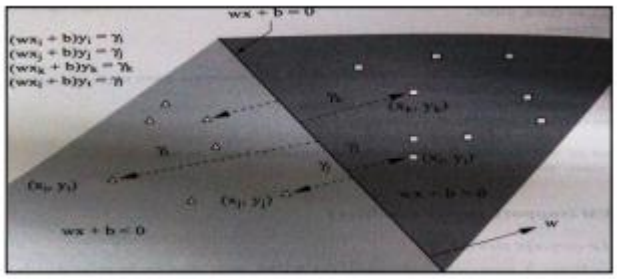


Figure (20): Séparation linéaire des objets carrés et triangles par un hyperplan[24]

2.6.2 Multi-classes

À l'origine, les SVM étaient principalement conçus pour les problèmes à deux classes, mais plusieurs approches permettant d'étendre cet algorithme aux cas à N classes ont été proposées. La généralisation vers les cas multi-classes peut être réalisée de trois manières différentes [23]. Les deux premières méthodes reposent sur une multiplication des classifieurs bi-classes, tandis que la dernière propose une approche globale

Un-contre-tous : Cette approche consiste à utiliser la méthode de discrimination binaire et à apprendre N fonctions de décision $\{fm\}m = 1 \ldots N$ pour discriminer chaque classe par rapport à toutes les autres (chaque classe est opposée à toutes les autres). Ainsi, N problèmes binaires sont posés. L'affectation d'un nouveau point x à une classe Ci se fait par la relation : $i = \ argmaxm = 1..N\ Fm(x)$

Un-contre-un : La deuxième méthode est celle dite "un contre un". Au lieu d'apprendre N fonctions de décision, chaque classe est discriminée par rapport à une autre. Ainsi $,N(N-1)/2$ Fonctions de décision sont apprises et chacune d'elles contribue à l'affectation d'un nouveau point x. La classe de ce point x devient ensuite la classe majoritaire après le vote.

2.6.3 Avantages et inconvénients des SVM

Avantages :

1. **Grande précision de prédiction** : Les SVM offrent une haute précision dans les résultats prédictifs, ce qui les rend particulièrement efficaces pour des tâches de classification et de régression.
2. **Efficacité sur des ensembles de données de petite taille** : Les SVM fonctionnent bien avec des petits ensembles de données, car ils sont capables de trouver un hyperplan optimal avec une quantité limitée de données.
3. **Utilisation d'un sous-ensemble de points d'entraînement** : Les SVM peuvent être plus efficaces que d'autres algorithmes car ils se basent uniquement sur un sous-ensemble des points d'entraînement (appelés vecteurs de support) pour déterminer l'hyperplan de séparation. Cela permet de réduire la complexité computationnelle dans certains cas.

3 Inconvénients :

1. **Inadapté pour des ensembles de données volumineux** : Pour des jeux de données très volumineux, l'entraînement des SVM peut être très long et coûteux en termes de temps de calcul, rendant l'algorithme moins pratique.
2. **Sensibilité au bruit et aux outliers** : Les SVM sont moins performants sur des ensembles de données contenant beaucoup de bruit et d'outliers, car ces anomalies peuvent influencer significativement l'hyperplan de séparation, dégradant ainsi la qualité de la classification.

4 Conclusion

Dans ce chapitre on a détaillé le processus de développement d'un système d'identification des empreintes digitales à l'aide de MATLAB. Chaque étape, de l'acquisition initiale de l'image à la classification finale par SVM, a été examinée en soulignant son importance critique dans la chaîne de traitement des empreintes digitales.

L'acquisition de l'image a été identifiée comme une étape fondamentale déterminant la qualité et la fiabilité du processus d'identification. Une image de haute qualité est cruciale pour

préserver les détails biométriques nécessaires à une correspondance précise et fiable. Ensuite, le prétraitement de l'image, comprenant des techniques comme l'égalisation de l'histogramme et la binarisation, vise à optimiser les images pour une extraction efficace des caractéristiques.
Concernant l'extraction des caractéristiques, deux approches ont été discutées : la carte des distances, permettant de quantifier les distances entre les pixels d'arrière-plan et ceux de premier plan, et les motifs binaires locaux (LBP), une méthode robuste pour caractériser les textures dans les empreintes digitales. Chaque méthode offre des avantages distincts selon les besoins spécifiques, des LBP rapides et simples à la précision géométrique de la carte des distances.
Enfin, la classification par SVM a été choisie pour sa robustesse et sa capacité à séparer efficacement les données de différentes classes. Les SVM sont particulièrement adaptés à la classification biométrique en raison de leur capacité à gérer des données complexes et à établir des frontières de décision précises.
En résumé, ce chapitre démontre comment une combinaison réfléchie de techniques d'acquisition d'images, de prétraitement, d'extraction de caractéristiques et de classification peut aboutir à un système d'identification des empreintes digitales précis, fiable et sécurisé.

1 Introduction

Ce chapitre est dédié à la présentation des résultats obtenus pour la validation de notre système. La description de la base de données utilisée FVC est tout d'abord présentée. Deux variante du système (via la carte de distance et par les LBP) sont évalués les résultats obtenus sont présentés sous forme de matrice de confusions.

2 La base de données FVC

Pour la base des empreintes digitales nous avons utilisé la base FVC2002 (Fingerprint Vérification Compétition) [28], base qui a été collectée par l'université de Bologne. Cette base est devisée en quatre petites bases (DB1,DB2,DB3,DB4) et deux groupe dans chacune SET A SET B chaque base collecté utilise différents capteur , le table ci-dessus explique la différence entre ces bases

	Capteurs	Taille de l'image	SET A (personnes x doigts)	SET B (x personnes x doigts)	Résolution
DB1	Capteur optique 'touch view II' Par identix	388x374 (142 Kpixels)	100*8	10*8	500 DPI
DB2	Capteur optique 'F2000'de Biometrica	296x560 (162 Kpixels)	100*8	10*8	500 DPI
DB3	Capteur capacitif '100 SC' de précise biometrics	300x300 (88 Kpixels)	100*8	10*8	500 DPI
DB4	Génération d'empreintes synthétiques	288x384 (108 Kpixels)	100*8	10*8	Environ 500 DPI

Tableau (1) : Les bases de données FVC 2002

3 Environnement de développement

Nous avons utilisé MATLAB pour implémenté notre système d'identification par empreintes digitales. MATLAB est un langage de programmation de quatrième génération et un environnement d'analyse numérique. MATLAB permet de faire du calcul matriciel, de développer et d'exécuter des algorithmes [30],

Nous avons utilisé la version '9.3.0.948333 (R2017b) Update 9' de MATLAB et sur un environnement WINDOWS avec in processor Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.50 GHz et une RAM de 8,00 Go.

4 Matrice de confusion

Les résultats obtenus sont présentés sous forme de matrices de confusions. Une matrice de confusion est un tableau qui résume des prédictions pour un problème de classification particulier. Il compare les données réelles de la variable cible avec les données prédites par le modèle [29]. Les prédictions correctes et fausses sont affichées et réparties par quatre catégories (voir la figure 21) expliquées comme suite :

1. True Positive (TP) : la prédiction et la valeur réelle sont positives.

Exemple : Une personne malade et prévu malade.

2. True Negative (TN) : la prédiction et la valeur réelle sont négatives.

Exemple : Une personne saine et prévu saine.

3. False Positive (FP) : la prédiction est positive alors que la valeur réelle est négative.

Exemple : Une personne saine et prévu malade.

4. False Negative (FN) : la prédiction est négative alors que la valeur réelle est négative.

Exemple : Une personne malade et prévu saine.

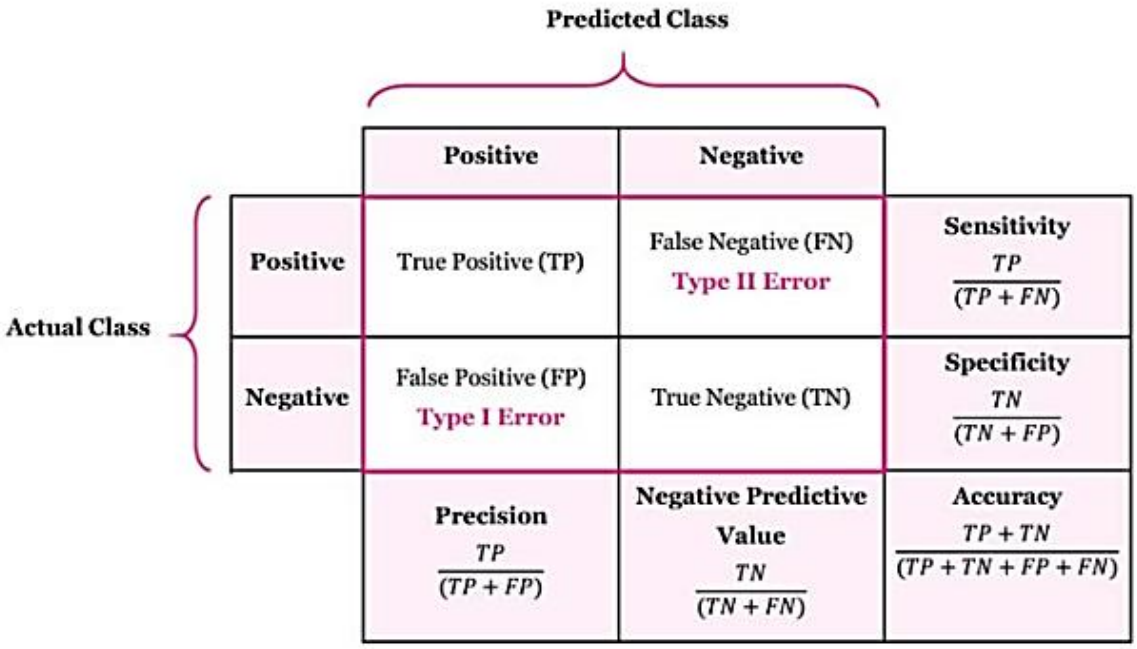


Figure 21 : matrice de confusion [29]

5 Organigramme du système d'identification des empreintes digitales via la carte de distance

Image d'empreinte en niveaux de gris :

Il s'agit de l'image brute de l'empreinte digitale, déjà convertie en niveaux de gris. Cela signifie que chaque pixel de l'image est représenté par une valeur d'intensité unique, simplifiant ainsi les étapes de traitement ultérieures.

Prétraitement avec égalisation d'histogramme :

Cette étape améliore le contraste de l'image d'empreinte digitale. L'égalisation d'histogramme redistribue les intensités des pixels pour exploiter toute la plage de valeurs possibles. Cela rend les caractéristiques de l'empreinte plus distinctes et facilite les étapes suivantes.

Binarisation avec la méthode d'Otsu :

La binarisation convertit l'image de l'empreinte en une image binaire (noir et blanc). La méthode d'Otsu est un algorithme qui détermine automatiquement un seuil de binarisation optimal en minimisant la variance intra-classe des niveaux de gris. Les crêtes deviennent noires et les vallées blanches.

Calcul de la carte de distance :

La carte de distance transforme l'image binaire en une carte où chaque pixel contient la distance par rapport au pixel de la crête la plus proche. Différentes méthodes peuvent être utilisées :

a. Euclidienne : Distance directe entre deux points (distance la plus courte).

b. Cheesboard : Distance en termes de mouvements de la pièce "roi" aux échecs (mouvement en ligne droite ou en diagonale).

c.City Block : Distance de Manhattan, c'est-à-dire distance en termes de déplacement uniquement horizontal et vertical.

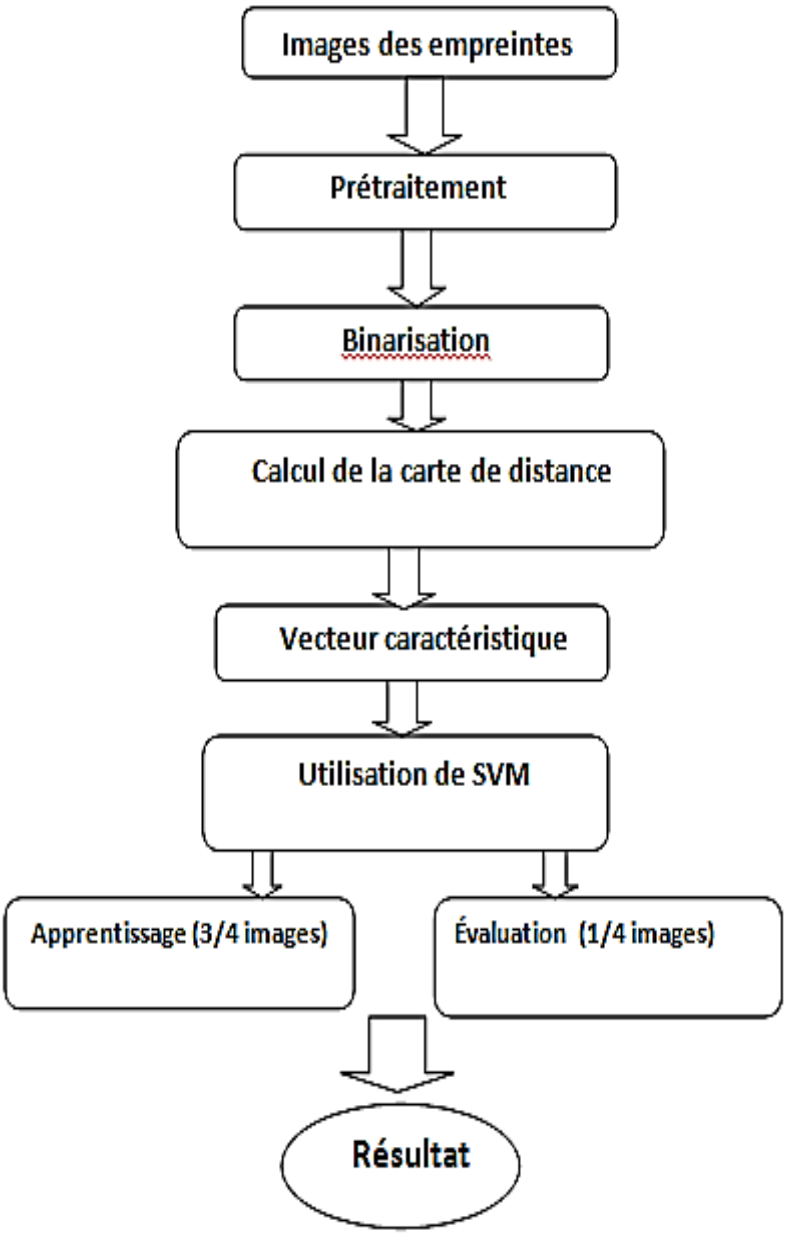
d. Quasi-Euclidienne : Approximation de la distance euclidienne.

Classification avec SVM (Support Vector Machines) :

Les SVM sont utilisés pour la classification des empreintes digitales. Un modèle SVM est entraîné à partir des caractéristiques extraites (par exemple, les valeurs de la carte de distance). Vous avez utilisé 3/4 des images d'empreintes pour l'apprentissage (phase de training) et 1/4 pour l'évaluation (phase de testing). Les SVM séparent les différentes classes d'empreintes en maximisant la marge entre les différents groupes de données dans l'espace des caractéristiques.

Résultats - Taux de bonne identification :

Après la classification, les performances du système sont évaluées. Le taux de bonne identification indique le pourcentage d'empreintes digitales correctement identifiées par le système. C'est une mesure clé pour évaluer l'efficacité du système de reconnaissance d'empreintes digitales.


Images des empreintes
Prétraitement
Binarisation
Calcul de la carte de distance
Vecteur caractéristique
Utilisation de SVM
Apprentissage (3/4 images)
Évaluation (1/4 images)
Résultat

6 Organigramme du système d'identification des empreintes digitales Via les LBP

Image d'empreinte en niveaux de gris :

Il s'agit de l'image brute de l'empreinte digitale, déjà convertie en niveaux de gris. Cela signifie que chaque pixel de l'image est représenté par une valeur d'intensité unique, simplifiant ainsi les étapes de traitement ultérieures.

Prétraitement avec égalisation d'histogramme :

Cette étape améliore le contraste de l'image d'empreinte digitale. L'égalisation d'histogramme redistribue les intensités des pixels pour exploiter toute la plage de valeurs possibles. Cela rend les caractéristiques de l'empreinte plus distinctes et facilite les étapes suivantes.

Redimensionnement des images à 256x256 :

L'image d'empreinte est redimensionnée à une taille standard de 256x256 pixels. Cela uniformise les dimensions des images d'empreintes digitales pour simplifier les étapes de traitement suivantes.

Partitionnement des images en imagettes 32x32 :

L'image redimensionnée est divisée en plus petites sections (imagettes) de 32x32 pixels. Cette division permet de traiter des portions locales de l'image, ce qui peut améliorer l'extraction des caractéristiques locales.

Extraction des caractéristiques par les LBP (Local Binary Patterns) :

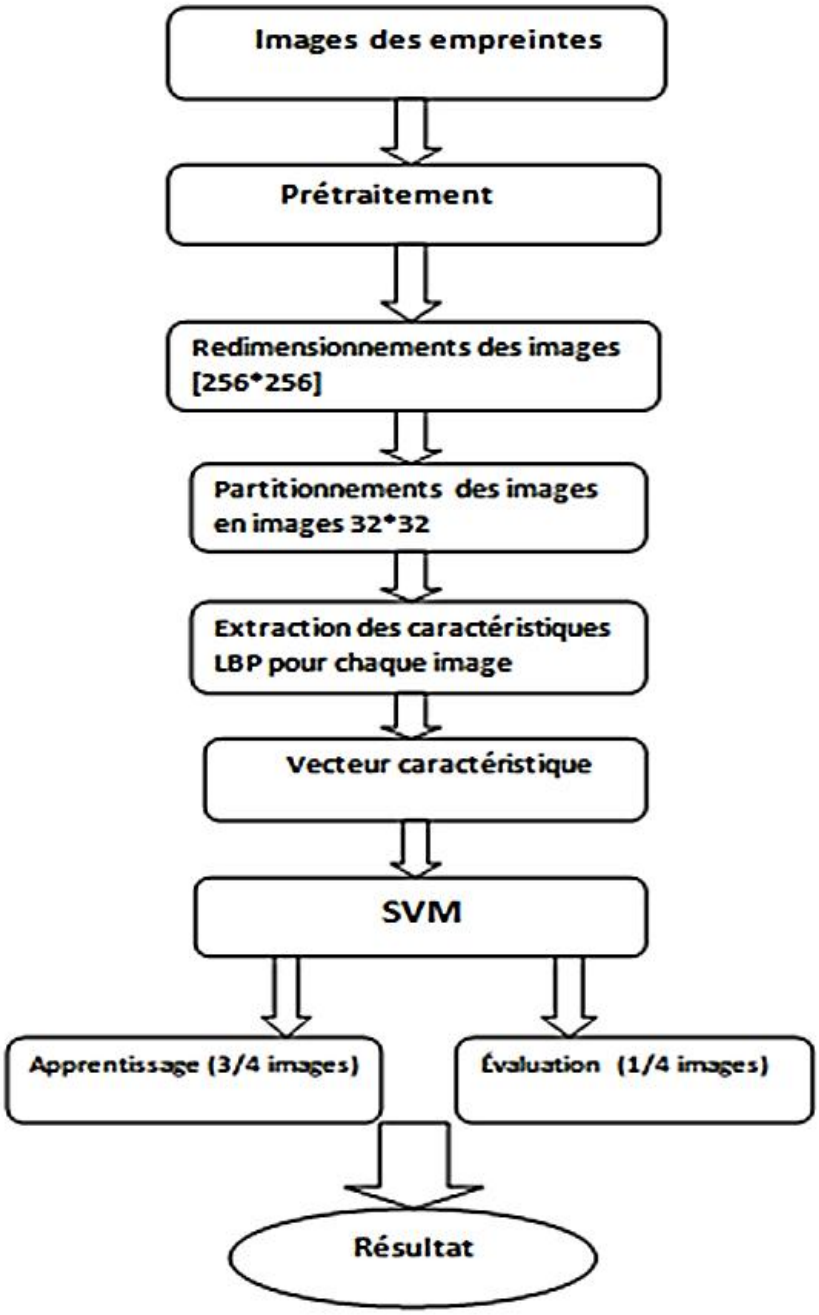
Les LBP sont utilisés pour extraire des caractéristiques texturales des imagettes. Cette méthode encode la texture locale en comparant chaque pixel avec ses voisins et en générant un code binaire. Les histogrammes des LBP sont ensuite calculés pour chaque imagette, fournissant une représentation compacte et discriminative de la texture locale.

Classification avec SVM (Support Vector Machines) :

Les SVM sont utilisés pour la classification des empreintes digitales. Un modèle SVM est entraîné à partir des caractéristiques extraites (par exemple, les histogrammes des LBP). Vous avez utilisé 3/4 des images d'empreintes pour l'apprentissage (phase de training) et 1/4 pour l'évaluation (phase de testing). Les SVM séparent les différentes classes d'empreintes en maximisant la marge entre les différents groupes de données dans l'espace des caractéristiques.

Résultats - Taux de bonne identification :

Après la classification, les performances du système sont évaluées. Le taux de bonne identification indique le pourcentage d'empreintes digitales correctement identifiées par le système. C'est une mesure clé pour évaluer l'efficacité du système de reconnaissance d'empreintes digitales.



7 Les résultats obtenus

Nous avons évalué le système avec ses deux variantes sur un ensemble d'images d'empreintes digitales de 13 personnes avec huit empreintes par personne de la base de données FVC2002.

7.1 Système d'identification des empreintes digitales Via la carte de distance

1. Par la carte distance euclidienne

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
P1	1	0	0	0	0	0	0	0	0	0	0	1	0
P2	0	2	0	0	0	0	0	0	0	0	0	0	0
P3	0	2	0	0	0	0	0	0	0	0	0	0	0
P4	1	0	0	1	0	0	0	0	0	0	0	0	0
P5	0	0	0	1	0	0	0	0	0	0	1	0	0
P6	0	0	0	0	0	2	0	0	0	0	0	0	0
P7	0	0	0	0	0	0	1	0	0	0	0	0	1
P8	0	0	0	0	1	0	0	0	0	0	1	0	0
P9	0	0	0	0	1	0	0	0	1	0	0	0	0
P10	0	0	0	0	1	0	0	0	0	1	0	0	0
P11	0	0	0	0	0	0	0	0	0	0	2	0	0
P12	0	1	0	0	0	0	0	0	0	0	0	1	0
P13	0	0	0	0	0	0	0	0	0	0	0	0	2

Tableau (2) : Résultats par la carte de distance euclidienne

Taux de bonne identification = **53.8462%**

La matrice de confusion pour la méthode Euclidienne montre une performance notablement moyenne avec un taux de précision de 53.8462%. Cela indique une nécessité d'améliorer la méthode ou d'explorer d'autres approches pour obtenir de meilleurs résultats de classification.

2. Par la carte distance Cityblock

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
P1	1	0	0	0	0	0	0	0	0	0	0	0	1
P2	0	1	0	0	0	0	0	0	0	1	0	0	0
P3	0	2	2	0	0	0	0	0	0	0	0	0	0
P4	1	0	0	0	0	0	0	1	0	0	0	0	0
P5	0	0	0	1	1	0	1	0	0	0	0	0	0
P6	0	0	0	0	0	1	1	0	0	0	0	0	0
P7	0	0	0	0	1	0	0	0	0	0	0	0	0
P8	0	0	0	0	0	0	0	2	0	0	0	0	0
P9	0	0	0	0	0	0	1	0	1	0	0	0	0
P10	0	0	0	0	0	0	0	0	0	2	0	0	0
P11	0	0	0	0	0	0	0	0	0	1	1	0	0
P12	0	0	0	0	0	1	0	0	0	0	1	0	0
P13	0	0	0	0	0	0	0	0	0	0	0	0	2

Tableau (3) : Résultats par la carte de distance **Cityblock**

Taux de bonne identification = **57.6923%**

La matrice de confusion pour la méthode City Block montre une performance modérée avec un taux d'exactitude de 57.6923%.

3. Par la carte distance cheessboard

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
P1	2	0	0	0	0	0	0	0	0	0	0	0	0
P2	0	2	0	0	0	0	0	0	0	0	0	0	0
P3	0	0	1	0	0	1	0	0	0	0	0	0	0
P4	1	0	0	0	0	0	0	1	0	0	0	0	0
P5	0	0	0	0	0	0	0	0	1	0	0	0	1
P6	0	0	0	0	0	2	0	0	0	0	0	0	0
P7	0	0	0	0	0	0	1	1	0	0	0	0	0
P8	0	0	0	0	0	0	0	2	0	0	0	0	0
P9	0	0	0	0	1	0	0	0	1	0	0	0	0
P10	0	1	0	0	0	0	0	0	0	1	0	0	0
P11	0	0	0	0	0	0	0	0	0	0	2	0	0
P12	0	0	0	0	0	0	0	0	0	0	0	2	0
P13	0	0	0	0	0	0	1	0	0	0	0	0	1

Tableau (4) : Résultats par la carte de distance **cheessboard**

Taux de bonne identification = 65.3846**%**

La matrice de confusion pour la méthode de Chessboard montre une performance solide avec un taux d'exactitude de 65.3846%.cette méthode pourrait être appropriée pour cette tâche spécifique de classification de personnes.

4. Par la carte de distance quasi-euclidienne

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
P1	1	0	0	0	0	0	0	0	0	0	0	1	0
P2	0	1	0	0	1	0	0	0	0	0	0	0	0
P3	0	0	1	0	0	1	0	0	0	0	0	0	0
P4	0	0	0	2	0	0	0	0	1	0	0	0	0
P5	0	0	0	0	1	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	2	0	0	0	0	0	0	0
P7	0	0	0	0	0	0	2	0	0	0	0	0	0
P8	0	0	0	0	0	0	0	2	0	0	0	0	0
P9	0	0	0	0	1	0	0	0	1	0	0	0	0
P10	0	1	0	0	0	0	0	0	0	1	0	0	0
P11	0	1	0	0	0	0	0	0	0	0	1	0	0
P12	0	0	0	0	0	0	0	0	0	0	0	2	0
P13	0	0	0	0	0	0	1	0	0	0	0	0	1

Tableau(5) : Résultats par la carte de distance **quasi-euclidienne**

Taux de bonne identification = **69.2308%**

La matrice de confusion montre que le modèle utilisant la distance quasi-Euclidienne pour la classification a un taux de bonne identification de 69.2308%.

7.2 Système d'identification des empreintes digitales LBP (local binary pattern)

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
P1	1	0	0	0	0	0	0	0	0	0	0	1	0
P2	0	2	0	0	0	0	0	0	0	0	0	0	0
P3	0	0	2	0	0	0	0	0	0	0	0	0	0
P4	0	0	0	2	0	0	0	0	0	0	0	0	0
P5	0	0	0	0	2	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	2	0	0	0	0	0	0	0
P7	0	0	0	0	0	0	2	0	0	0	0	0	1
P8	0	0	0	0	0	0	0	2	0	0	0	0	0
P9	0	0	0	0	0	0	0	0	2	0	0	0	0
P10	0	0	0	0	0	0	0	0	0	2	0	0	0
P11	0	0	0	0	0	0	0	0	0	0	2	0	0
P12	0	0	0	0	0	0	0	0	0	0	0	2	0
P13	0	0	0	0	0	0	0	0	0	0	0	0	2

Tableau (6) : Résultats par Les LBP

Taux de bonne identification = **92.3077%**

La matrice de confusion montre que le modèle utilisant les LBP pour la classification a un taux de bonne identification de 92,3077%

7.3 Discussion

Le tableau suivant compare les résultats obtenus par les deux variantes de notre système avec les résultats obtenus par une méthode classique basée sur la caractéristique des empreintes digitales (minutie, terminaison, centre….)

méthodes	Taux %
Euclidienne	53.8462%
cityblock	57.6923%
chessboard	65.3846%
quasi-Euclidienne	69.2308%
LBP	92.3077%
Classique	97%

Tableau (7) : comparaison des résultats obtenus

8 Conclusion

Les LBP se démarque nettement avec un taux d'exactitude exceptionnel de 92.3077%, démontrant sa capacité supérieure à capturer et à distinguer les motifs ou textures dans les données. En revanche, les méthodes de distances plus simples comme Euclidienne et

Cityblock montrent des performances relativement inférieures, indiquant qu'elles peuvent ne pas être suffisamment robustes pour des tâches de classification complexes impliquant des nuances subtiles entre les classes.

La méthode quasi-Euclidienne et Chessboard se positionnent respectivement à 69.2308% et 65.3846%, montrant des améliorations significatives par rapport aux méthodes plus simples, mais restant en deçà de LBP.

La méthode classique [34] reste la référence pour les applications nécessitant une haute précision tandis que les LBP représentent une alternative très performante.

En résumé, choisir la bonne méthode de classification, adaptée aux spécificités des données et à la complexité de la tâche, est essentiel pour garantir des performances optimales du modèle. L'utilisation de méthodes plus sophistiquées comme LBP peut conduire à des résultats considérablement meilleurs dans des domaines où la précision et la discrimination fines des classes sont primordiales.

La reconnaissance biométrique est l'identification des personnes est basée sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologies. Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte digitale par ce qu'elle est permanente et unique. Les chercheurs essayent toujours de développer les systèmes de reconnaissance à travers des outils mathématiques habituellement complexes pour faire la discrimination entre les individus. Les objectifs suivis dans ce mémoire proposent une démarche qui consiste à améliorer la performance de l'identification et vérification biométriques via l'empreinte digitale par plusieurs méthodes avec un ensemble d'opérations.

Notre système est constitué de trois étapes, le prétraitement, l'extraction des caractéristiques et la classification. Le prétraitement est fait par la conversion en niveaux de gris et l'égalisation de l'histogramme. Enfin, la classification est effectué par le calcul du distance euclidienne entres les vecteurs de caractéristiques des images de test et celle des images de la base de données.

En fin, le système proposé est appliqué sur une base de donnés connue dans le domaine des empreintes digitale et les résultats obtenus, sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

Comme travail futur, nous proposons de concentrer sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

La reconnaissance biométrique est l'identification des personnes est basée sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologies. Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte digitale par ce qu'elle est permanente et unique. Les chercheurs essayent toujours de développer les systèmes de reconnaissance à travers des outils mathématiques habituellement complexes pour faire la discrimination entre les individus. Les objectifs suivis dans ce mémoire proposent une démarche qui consiste à améliorer la performance de l'identification et vérification biométriques via l'empreinte digitale par plusieurs méthodes avec un ensemble d'opérations.

Notre système est constitué de trois étapes, le prétraitement, l'extraction des caractéristiques et la classification. Le prétraitement est fait par la conversion en niveaux de gris et l'égalisation de l'histogramme. Enfin, la classification est effectué par le calcul du distance euclidienne entres les vecteurs de caractéristiques des images de test et celle des images de la base de données.

En fin, le système proposé est appliqué sur une base de donnés connue dans le domaine des empreintes digitale et les résultats obtenus, sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

Comme travail futur, nous proposons de concentrer sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

Références

[1] https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie(1)

https://fr.wikipedia.org/wiki/Empreinte_digitale(2)

[2] OULD AMER DJAMEL, mémoire fin d'etude " Extraction de la signature d'une empreinte digitale par la détection locale des minuties", 2011.

[3] N. Yager and A. Amin, "Fingerprintverificationbased on minutiaefeatures: areview', Pattern Analysis and Applications, Vol. 7, No. 1, pp. 94-113, April 2004

[4] X. Xia and L. O'Gorman, "Innovations in fingerprint capture devices", Pattern Recognition, Vol. 36, pp.361-369, 2003.

[5] N. Galy, " Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage. Micro et nanotechnologies,Microélectronique" Institut National Polytechnique de Grenoble - INPG, 2005.

[6] http://www.biometrie-tpevh.blogspot.com

[7] L. CHUNG ERN, G. SULONG, "Fingerprint Classification Approaches", International Symposiom on SignalProcessing and its Applications, Vo. 1, p.347-350, Kuala Lumpur, Malaisie, 13-16 Aout 2001.

[8] A. JAIN, S. PANKANTI, "Fingerprint Classificationand Recognition", The Image and VideoProcesssingHandbook, AcademicPress, Avril, 2000.

[9] A. JAIN, S. PANKANTI, "Advances in FingerprintTechnology", 2nde edition, Elsevier Science, New ,York, 2001.

[10] A. JAIN, S. PANKANTI, "Automated Fingerprint Identification and Imaging Systems", Advances inFingerprintTechnology, 2nde edition, Elsevier ´Science, New-York, 2001.

[11] S. PRABHAKAR, "Fingerprint Classification and MatchingUsing a Filterbank", Michigan State University, 2001

[12] D. MAIO, D. MALTONI, R. CAPPELLI, J.L. WAYMAN A.K. JAIN, FVC2000: fingerprint verification competition, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 3, p. 402-412, Mars 2002

[13] https://en.wikipedia.org/wiki/Fingerprint_Verification_Competition

[14] Maltoni, D., Maio, D., Jain, A. K., &Prabhakar, " S. Handbook of Fingerprint Recognition". Springer,2009.

[15] J. DAUGMAN, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 15, p. 1148-1161, 1993

[16] Maltoni, D., Maio, D., Jain, A. K., &Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer.

[17]https://fr.wikipedia.org/wiki/M%C3%A9thode_d%27Otsu#:~:text=En%20vision%20par%20ordinateur%20et,gris%20en%20une%20image%20binaire.

[18]MathWorks. (2024). MATLAB Documentation. Retrieved from https://www.mathworks.com/help/matlab/

[19] Zhang, D., Kong, W.-K., You, J., & Wong, M. (2003). Online Palmprint Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9), 1041–1050. doi:10.1109/TPAMI.2003.1227981

[20] onzalez, R. C., &Woods, R. E. (2018). *Digital Image Processing*. Pearson.
MathWorks. (2024). Image ProcessingToolbox Documentation.

[21] https://fr.wikipedia.org/wiki/Machine_%C3%A0_vecteurs_de_support

[22] Vapnik, V. (1995). *The Nature of Statistical Learning Theory*. Springer.

[23] Amine Nait-Ali, mémoire fin d'étude ‘’Traitement du signal et de l'image pour la biométrie’’, L'OUASIR, 2012

[24] J. V. Kittler., "Combiningclassifiers A theoreticalframework", IEEE Transactions on Pattern Analysis and Machine Intelligence, 1(1) :18–27, 1998.

[25] Pierre Buyssens., "Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e transactions", Université de Caen Basse-Normandie, 2011.

[26] https://fr.wikipedia.org/wiki/Binarisation

[27] https://fr.wikipedia.org/wiki/Motif_binaire_local

[28] http://bias.csr.unibo.it/fvc2004/download.asp

[29] https://datascientest.com/matrice-de-confusion

[30] https://www.lemagit.fr/definition/MATLAB

[31] https://brightcape.co/les-svm-support-vector-machine/

[32] Senthilkumaran N et Vaithegi S, « Image Segmentation By UsingThresholding Techniques For Medical Images », Computer Science & Engineering: An International Journal, vol. 6, no 1,2016 février 29

[33] hafstoufik ‘’reconnaissance biométrique’’universitè Badji mokhtar Annaba , 2016

[34] Q. Li, C. Jin, W. Kim, J. Kim, S. Li, and H. Kim, "Multi-featurebased score fusion method for fingerprint recognition accuracyboosting," AnnualSummit and Conference on Asia-Pacific International Journal of ScientificResearch in Science, Engineering and Technology (ijsrset.com) 197 Signal and Information Processing Association, pp. 1–4, 2017.

Resumè :

Ce mémoire traite de l'identification des empreintes digitales, une méthode essentielle pour l'authentification et la sécurité des accès. Le premier chapitre introduit la biométrie, expliquant son importance, ses applications et ses différents types, ainsi que les critères de performance des systèmes biométriques et les défis associés à leur utilisation. Le deuxième chapitre présente un aperçu des méthodes et techniques existantes pour l'identification des empreintes digitales, couvrant l'histoire, les approches de capture et d'analyse, ainsi que les principaux algorithmes de traitement et de reconnaissance.

Le troisième chapitre décrit en détail la méthodologie adoptée. Le prétraitement des images d'empreintes digitales inclut l'égalisation d'histogramme pour améliorer le contraste et la binarisation pour simplifier le traitement. Pour l'extraction de caractéristiques, les cartes de distance sont utilisées pour représenter les structures des crêtes et des vallées, tandis que le LBP (Local Binary Pattern) capture les motifs de texture locaux. La classification est effectuée à l'aide de SVM (Support Vector Machine), un algorithme de classification efficace pour différencier les empreintes digitales basées sur les caractéristiques extraites.

Les résultats obtenus démontrent que l'approche proposée, combinant ces techniques de prétraitement et d'extraction de caractéristiques avec les SVM pour la classification, offre une performance satisfaisante. Les résultats sont analysés en termes de précision, de taux de faux rejet et de taux de faux acceptation, prouvant l'efficacité de la méthode.

En conclusion, ce mémoire démontre que l'utilisation de techniques avancées de prétraitement et d'extraction de caractéristiques, combinées avec des algorithmes de classification robustes comme les SVM, peut améliorer significativement la précision et la fiabilité des systèmes d'identification des empreintes digitales. Des suggestions pour des travaux futurs incluent l'exploration de nouvelles techniques de machine learning et l'intégration de méthodes de fusion multi-biométriques pour une identification encore plus précise.

voici quelques mots clés pour ce mémoire :

1. Identification des empreintes digitales
2. Biométrie
3. Égalisation d'histogramme
4. Binarisation
5. Cartes de distance
6. Local Binary Pattern (LBP)
7. Support Vector Machine (SVM)
8. Prétraitement des images
9. Extraction de caractéristiques
10. Classification
11. Taux de faux rejet (FRR)
12. Taux de faux acceptation (FAR)
13. Techniques de machine learning
14. Systèmes biométriques
15. Authentification et sécurité