République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 8 Mai 1945 Guelma

Faculté des Sciences et de la Technologie

Département d'Electronique et Télécommunications

Mémoire en vue de l'obtention du

Diplôme de Master

==========

Identification des personnes par les veines des doigts

==========

Filière : **Electronique**

Spécialité : Instrumentation

Présenté par :

SLIMANI Amani

Sous la direction de :

Dr. BENDJOUDI Salim

Juin 2024

Remerciements

D'abord je tiens à remercier Dieu de m'avoir donné le courage et la capacité de terminer ce mémoire de fin d'étude.

Je tiens à exprimer ma plus profonde gratitude à mon encadreur BENDJOUDI SALIM, Professeur à l'Université 8 Mai 1945 de Guelma. C'est avec beaucoup d'humilité et d'appréciation que je reconnais son immense contribution dans la direction de ce travail et dans ses conseils et son soutien inestimables. L'honneur qu'il m'a fait et sa disponibilité sans faille tout au long du processus ont été vraiment inestimables.

J'exprime ma plus profonde gratitude à mes parents bien-aimés et au reste de ma famille, dont le soutien indéfectible a été une source constante de force. Leurs conseils et leur motivation ont contribué à faire de moi la personne que je suis aujourd'hui, et pour cela, je leur en suis vraiment reconnaissant.

Avec la plus grande gratitude, j'adresse mes sincères remerciements à mes chers amis qui ont toujours été à mes côtés. Leur fidélité inébranlable et leurs encouragements indéfectibles ont été pour moi une source de force inestimable.

Dédicace

Je dédie ce travail à :

- *A ma famille, elle qui m'a doté d'une éducation digne, son amour a fait de moi ce que je suis aujourd'hui.*
- *À mon encadreur « Dr. BENDJOUDI.S » envers qui je dois le plus grand respect et la profonde gratitude.*
- *À tous les éducateurs estimés qui m'ont accompagné dans mon parcours académique et m'ont permis de m'épanouir dans mes études.*
- *A tous mes amis et collègues de la promo 2024 de Master.*

Résumé

Les caractéristiques des veines sont difficiles à extraire avec précision, car les images des veines des doigts prises par la lumière proche infrarouge sont toujours de qualité inférieure. Ce mémoire présente une méthode de représentation des caractéristiques des veines du doigt qui repose sur la mesure de la quantification de phase locale (LPQ). Étant donné que les réseaux veineux sont composés de diverses caractéristiques de texture et d'orientation, on utilise un opérateur de description des caractéristiques de texture à différentes échelles sur l'image des veines du doigt afin de minimiser les effets de la déformation géométrique liée à la posture et à la position différentes des doigts lors de l'acquisition de l'image.

Afin de remédier aux conséquences néfastes du flou de l'image provoqué par une illumination inégale, une mise en place d'une quantification de phase locale permet d'extraire les caractéristiques des veines. Enfin, on combine les deux types de caractéristiques de texture de l'image des veines en utilisant des histogrammes concaténés pour obtenir une caractéristique précise des veines, connue sous le nom d'histogramme de quantification de phase locale (LPQ). Ainsi, la formation de l'image de la veine est codée non seulement dans le domaine des fréquences, mais aussi entre différentes orientations et échelles. Les expériences rigoureuses que nous menons sur une base de données publique, SDUMLA-HMT, montrent que le système proposé peut améliorer de manière prometteuse les performances de la reconnaissance des veines du doigt.

Mots clés : Identification, authentification, veines du doigt, FVR, LPQ, Classificateur KNN

ملخص

من الصعب استخراج ملامح الأوردة بدقة، لأن صور أوردة الأصابع التي يلتقطها ضوء الأشعة تحت الحمراء القريبة تكون دائمًا نظرًا لأن .(LPQ) ذات جودة أقل. تقدم هذه الأطروحة طريقة لتمثيل خصائص أوردة الإصبع بناءً على قياس قياس الطور المحلي الشبكات الوريدية تتكون من مختلف خصائص الملمس والتوجه، فإن المشغل الذي يصف خصائص الملمس على مقاييس مختلفة على صورة أوردة الإصبع يستخدم لتقليل آثار التشوه الهندسي المرتبط بالوضعية والموقع المختلفين للأصابع عند الحصول على الصورة.

من أجل معالجة العواقب الضارة لطمس الصورة الناجم عن الإضاءة غير المتكافئة، يتم استخدام قياس الطور المحلي لاستخراج خصائص الأوردة. أخيرًا، يتم دمج نوعين من خصائص الملمس لصورة الوريد باستخدام مخطط نسيجي مختصر للحصول على وبالتالي، فإن تكوين صورة الوريد يتم ترميزه ليس .(LPQ) سمة دقيقة للأوردة، تُعرف باسم مخطط النسيج الكمي للمرحلة المحلية فقط في مجال التردد، ولكن أيضًا بين الاتجاهات والمقاييس المختلفة. تُظهر التجارب الصارمة التي نجريها على قاعدة بيانات عامة، ، أن النظام المقترح يمكن أن يحسن أداء التعرف على وريد الأصابع بطريقة واعدةSDUMLA-HMT

KNN و LPQ و FVR الكلمات الرئيسية: تحديد الهوية والمصادقة وأوردة الأصابع و

Summary

Vein features are difficult to extract accurately, as near-infrared light images of finger veins are always of inferior quality. This dissertation presents a method for representing finger vein features based on the measurement of local phase quantization (LPQ). Since vein networks are composed of various textural and orientation features, a texture feature description operator at different scales is used on the finger vein image to minimize the effects of geometric distortion related to different finger posture and position during image acquisition.

To overcome the adverse effects of image blurring caused by uneven illumination, local phase quantization is used to extract vein features. Finally, the two types of vein image texture features are combined using concatenated histograms to obtain a precise vein feature, known as the local phase quantization (LPQ) histogram. In this way, vein imaging is encoded not only in the frequency domain, but also between different orientations and scales. Our rigorous experiments on a public database, SDUMLA-HMT, show that the proposed system can promisingly improve finger vein recognition performance.

Keywords : Identification, authentication, finger vein, FVR, LPQ, KNN Classifier

Table des Matières

Table des Matières

Chapitre 3: Traits biométriques

Chapitre 4: Identifications par les veines des doigts

Table des Matières

Chapitre 5: Les outils et techniques utilisés

Chapitre 6: Résultats

Introduction Générale

Introduction générale

Avec notre progression vers une société de l'information mondialisée et envahissante, l'existence de l'individu normal s'est en même temps transformée en une vie de plus en plus complexe et de plus en plus imprévisible, et ce, en raison de l'évolution des technologies de l'information et de la communication (TIC).

Dans notre société contemporaine, où l'innovation en matière d'information dans le domaine électronique et de l'intelligence artificielle connaît une croissance véloce, la sécurité est devenue un enjeu capital. D'où la popularité de la vérification biométrique, car celle-ci propose une méthodologie fiable et extrêmement sécurisée pour l'authentification des personnes. La vie des individus moyens est en même temps devenue menacée par des événements odieux qui peuvent survenir n'importe où et à n'importe quel moment dans le monde. Les horreurs peuvent se propager dans le monde entier en un instant, augmentant et intensifiant le risque.

Il en résulte un besoin soudain et intense de systèmes d'authentification personnelle capables d'empêcher l'usurpation d'identité et d'autres qui permettent de prévenir les crimes de falsification d'identité ou d'autres formes de contraventions tels que les retraits d'argent (en espèces ou par carte de crédit), la falsification des passeports et des permis de conduire, l'entrée sur des territoires étrangers, l'accès à des informations personnelles et l'atteinte à la vie privée des gens, l'accès aux équipements informatiques personnels d'autrui, et un large éventail d'autres applications etc. En tant que tels, les systèmes biométriques, qui sont très précis et utilisent une partie de notre corps, sont devenus la réponse idéale à ces besoins de sécurité accrus et sont déjà adoptés dans le monde entier. Selon les prévisions de l'International Biometrics Group (IBG), le marché mondial de la biométrie devrait dépasser les ***51 milliards de dollars d'ici fin 2024 et 104.22 milliards de dollars d'ici 2029***. Les systèmes biométriques les plus répandus, sont les dispositifs d'authentification par empreintes digitales et l'iris.

Ces systèmes biométriques conventionnels ont leurs propres défauts, tels que la sensibilité à l'âge, à la santé et à l'expression faciale dans la reconnaissance des visages, par exemple la falsification à l'aide d'un doigt factice muni d'une empreinte digitale copiée dans la reconnaissance des empreintes digitales, la résistance psychologique des individus à la lumière directe dans les yeux pour la reconnaissance de l'iris, et la falsification de la voix enregistrée pour la reconnaissance de la voix dans le cas de la reconnaissance vocale. La biométrie des veines du doigt a offert des solutions prometteuses à ces défis grâce à ses

Caractéristiques uniques telles que la résistance à la falsification, à une précision élevée, à l'unicité et la cohérence, à la non-infraction et l'absence d'erreur, l'imagerie non invasive et sans contact, la rapidité d'authentification, les dispositifs de capture petits et abordables et l'identification du corps vivant.

Récemment, la biométrie des veines du doigt a suscité un intérêt croissant de la part de nombreux chercheurs et un développement considérable a été observé au cours des deux dernières décennies. En tant que technique biométrique récemment apparue, la reconnaissance des personnes par leurs veines et en particulier celles du doigt a été reconnue comme l'une des technologies biométriques les plus efficaces et les plus fiables pour l'authentification et la sécurité des personnes. La société japonaise (Hitachi Ltd.) explore la technologie des veines du doigt depuis 1997 et a été la première à mettre au point et à commercialiser un système d'identification par les veines du doigt. En 2004, Hitachi a développé des applications ATM et les a commercialisées en 2005. A travers ce modeste mémoire nous tentons de souligner les bénéfices et les désavantages des divers traits biométriques et pourquoi nous avons sélectionné parmi eux la biométrie des veines du doigt. Puis nous focalisons notre étude sur les éléments suivants : la description générale des veines du doigt,ses différentes étapes : l'acquisition des images, leurs prétraitement, l'extraction des caractéristiques, l'appariement, l'analyse de quelques travaux de recherche actuels et nous décrivons également quelques bases de données courantes utilisées dans le domaine de la recherche. Enfin nous couronnons ce modeste travail par une simulation d’authentification basée sur les veines des doigts et nous achevons notre travail par une conclusion.

Chapitre I : Identification et authentification

1.1 Introduction

Le concept d'identification et d'authentification est utilisé pour défaire des difficultés tels que la protection des systèmes d'information. Pour apprécier pleinement ce concept, il faut comprendre les problèmes que l'identification et l'authentification ont permis de résoudre.
Permettre à des personnes d'accéder à n'importe quelle ressource peut avoir des résultats dévastateurs. La fraude, le vol, les abus et d'autres activités criminelles seront imposés à la ressource. Aux États-Unis et en Inde des milliards de dollars d'aides sociales sont réclamé par double emploi d'identité, une méthode par laquelle les bénéficiaires utilisent plusieurs identités pour obtenir des avantages sociaux supplémentaires non autorisés.
Prenons l'exemple d'un établissement médical dépourvu de système d'authentification. Si ses médicaments coûteux, l'utilisation de ses équipements médicaux et des informations médicales sur ses patients sont exhibés ou révélés, cela va permettre à des activités malveillantes de se produire.
C'est pourquoi ces ressources nécessitent une protection maximale. Au fil des années, trois caractéristiques clés ont été identifiées pour aider les professionnels de la sécurité à protéger les ressources électroniques précieuses. Ces trois caractéristiques sont les suivantes

- Confidentialité
- Intégrité
- Disponibilité

Pour protéger ces trois caractéristiques des ressources électroniques, il est nécessaire d'adopter des approches consistantes et admissibles en matière d'identification et d'évaluation. Nous allons maintenant examiner brièvement ces trois caractéristiques.

1.2 Les caractéristiques clés

1.2.1 Confidentialité

La confidentialité consiste à préserver les informations dans le système d'information afin d'éviter tout accès non autorisé. Ces informations peuvent être des données médicales relatives à un patient, des renseignements militaires ou des informations financières essentielles comme les soldes des comptes des employés.

Confidentialité - La sécurité des informations dans le système afin d'éviter tout accès aux personnes non autorisées Tipton [1]. Il peut s'agir d'informations médicales concernant un patient, de renseignements militaires ou d'informations financières de base telles que le salaire d'un employé. Dans son article, Tipton [1] signale les six menaces les plus courantes qui pèsent sur la confidentialité. Ces menaces sont les suivantes :

- Les piratages informatiques ;

- Déguisements ;
- Activité d'un utilisateur non autorisé ;
- Téléchargements non autorisés des fichiers non protégés ;
- Réseaux locaux ;
- Chevaux de Troie ;

Par exemple, les secrets commerciaux sont un élément vital pour toute entreprise. Un ancien employé mécontent peut révéler des secrets à une entreprise concurrente, ce qui peut entraîner une perte d'activité et de bénéfices. La confidentialité des informations doit donc être protégée.

1.2.2 Intégrité

Intégrité - Empêcher les ressources électroniques de subir des modifications accidentelles ou intentionnelles ou la possibilité de contester la validité des informations fournies par la ressource. La falsification d'informations financières ou d'accords juridiquement contraignants sont des situations typiques où ce type d'abus peut se produire.

Lorsqu'il est question d'intégrité, la plupart des gens pensent uniquement à l'intégrité de l'information. Bien que cela soit vrai, lorsqu'il est question de systèmes d'information, le concept d'intégrité s'applique à la fois aux données et aux systèmes. L'intégrité des données vise à préserver la signification des informations, en ce qui concerne l'exhaustivité et la cohérence de leurs représentations au sein du système, ainsi que leur correspondance avec leurs représentations extérieures au système Mayfield et al. [2].

1.2.3 Disponibilité

Disponibilité - Les informations et les services qui peuvent être obtenus par les organisations et les individus doivent être accessibles lorsque ces "utilisateurs" en ont besoin. Ces utilisateurs peuvent être une personne ou un autre système informatique. Le commerce en ligne, les services bancaires en ligne ainsi que d'autres plateformes de systèmes d'information disponibles sur un réseau doivent être protégés contre l'indisponibilité.

Prenons l'exemple d'EBay, le site de vente aux enchères en ligne qui compte des centaines de millions d'utilisateurs actifs et dont le bénéfice net enregistré au quatrième trimestre 2023 s’est élevé à un chiffre d'affaires de 2562 millions de dollars. EBay subirait des pertes considérables en termes de crédibilité si son site web était hors ligne ne serait-ce qu'une journée.

La sécurisation d'un système d'information contre l'indisponibilité est donc essentielle pour tous les systèmes fournissant un service.

L'identification et l'authentification sont nécessaires pour mettre en œuvre la mise en place de la confidentialité, de l'intégrité et de l'i*nactivité*. Combinées, ces approches protègent contre l'utilisation non autorisée des données et des systèmes au seul personnel autorisé et la garantie que ces systèmes et ces informations sont conservés dans leur état d'origine.

La section suivante explique comment ces trois approches sont combinées pour mettre en œuvre efficacement l'identification et l'authentification des ressources électroniques.

1.3 Le Processus d'identification et d'authentification

Après avoir identifié le problème et les domaines dans lesquels l'authentification est nécessaire, examinons plus en détail ce que sont l'identification et l'authentification.

L'identification et l'authentification sont des procédures utilisées pour identifier l'identité réelle d'une personne.

Dans le monde physique, il est facile de s'identifier face à face. En revanche, dans le monde virtuel, il est plus difficile de confirmer son identité. N'importe qui peut prétendre être Slimani Amani derrière son ordinateur, mais une vérification est nécessaire pour que l'ordinateur vous fasse confiance.

L'identification est un processus par lequel vous communiquez votre identité au système. Dans un monde physique, les gens vous identifient à l'aide de vos attributs physiques. Dans un monde virtuel et dans la plupart des systèmes d'information modernes, l'utilisateur présente un identifiant unique. Cet identifiant unique peut être une adresse électronique, un numéro d'assurance ou simplement un nom d'utilisateur créé en combinant votre nom de famille, et le premier caractère de votre prénom par exemple le nom d'utilisateur de Slimani Amani pourrait être slimania ou aslimani.

Cet identifiant unique n'est pas un secret et n'importe qui peut le connaître. Au cours de la procédure d'identification, l'utilisateur fournit généralement l'identifiant unique au système de sécurité. Le système vérifie si l'identifiant unique existe dans le système. S'il n'existe pas, la demande d'utilisation du système est rejetée. Toutefois, si l'identifiant existe, le système demandera à l'utilisateur de prouver que cet identifiant lui appartient effectivement. Le processus consistant à prouver son identité est connu sous le nom d'authentification.

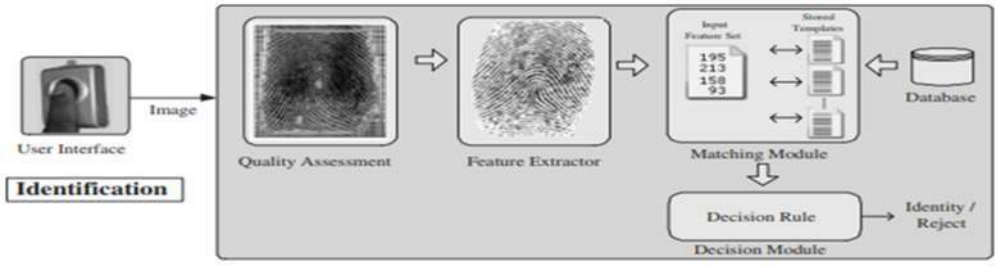


Figure 1-1 : illustre le processus d'identification

Comme c'est indiqué ci-dessus, les identifiants uniques ne sont pas nécessairement secrets, de sorte que n'importe qui peut les utiliser sans l'autorisation de leur propriétaire. Afin d'empêcher l'utilisation malveillante des identifiants uniques, l'utilisateur qui présente l'identifiant doit prouver que cet identifiant lui appartient. La plupart des systèmes de sécurité demandent souvent à l'utilisateur de fournir un objet pour vérifier son identité. L'authentification est donc un processus de vérification d'une identité revendiquée en fournissant des preuves.

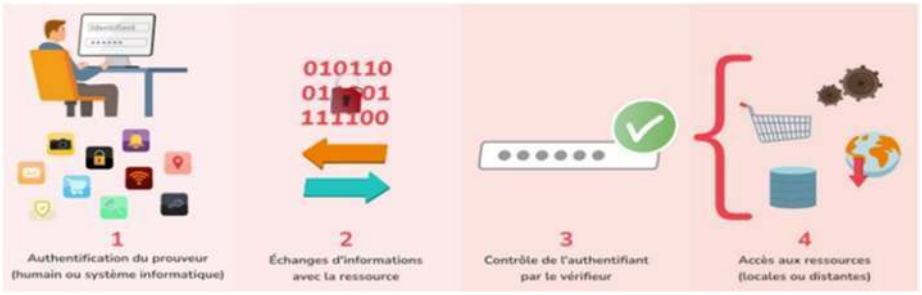


Figure 1-2 : illustre le processus d'authentification

L'objet fourni par l'utilisateur est souvent appelé " références ". Contrairement aux identifiants uniques, les références sont des secrets qui n'appartiennent et ne sont connus que du propriétaire de l'identifiant. Les types d'identifiants ne sont pas toujours les mêmes, car ils peuvent varier d'un système à l'autre. Parmi les exemples de références, on peut citer un mot de passe secret, des codes PIN et des certificats.

L'identification est un processus par lequel vous communiquez votre identité au système. Dans un monde physique, les gens vous identifient à l'aide de vos attributs physiques. Dans un monde virtuel et dans la plupart des systèmes d'information modernes, l'utilisateur présente un identifiant unique. Cet identifiant unique peut être une adresse électronique, un numéro d'assurance ou simplement un nom d'utilisateur créé en combinant votre prénom et le premier caractère de votre nom de famille, par exemple le nom d'utilisateur de Slimani Amani pourrait être aslimani ou slimania. Cet identifiant unique n'est pas un secret et n'importe qui peut le connaître. Au cours de la procédure d'identification, l'utilisateur fournit généralement l'identifiant unique au système de sécurité. Le système vérifie si l'identifiant unique existe dans le système. S'il n'existe pas, la demande d'utilisation du système est rejetée. Toutefois, si l'identifiant existe, le système demandera à l'utilisateur de prouver que cet identifiant lui appartient effectivement. Le processus consistant à prouver son identité est connu sous le nom d'authentification.

En utilisant un identifiant unique, un système peut identifier chaque utilisateur. Ces identifiants uniques ne sont pas secrets et peuvent être connus de tous. Ces identifiants

Uniques sont générés au cours du processus d'enregistrement, processus par lequel l'utilisateur est présenté au système.

Les identificateurs uniques ne sont pas des secrets et sont souvent connus d'un certain nombre de personnes. Pour déterminer si l'utilisateur est le propriétaire autorisé de l'identifiant, le système lui demandera de fournir un jeton d'authentification pour prouver son identité. Ces jetons d'authentification sont des secrets et ne sont connus ou possédés que par le propriétaire autorisé. Ces jetons se présentent sous la forme de mots de passe, de cartes à puce ou même de données biométriques. Comme c'est indiqué précédemment, les jetons d'authentification se présentent sous différentes formes. La section suivante examinera brièvement l'évolution des méthodes d'authentification dans un monde numérique.

1.4 Introduction aux mécanismes d'authentification

Au début des années 1960, l'un des premiers mécanismes d'authentification par ordinateur a été créé dans le cadre du système compatible de partage du temps (CTSS) Woodward et al. 2003 [3]. Le concepteur du système a introduit le concept d'un "code privé" que les étudiants devaient mémoriser. Ce code était similaire aux serrures à combinaison de leurs casiers d'école.

Aujourd'hui, ce "code privé" est connu sous le nom de mot de passe et est visible sur la plupart des systèmes informatiques. Même avec les avancées modernes, les mots de passe sont le type d'identifiant le plus couramment utilisé. Cependant, les mots de passe sont facilement compromis Imperva [4], Cluley [5]. Les avancées de la puissance de calcul facilitent la détection de mots de passe courts, d'où la nécessité de mots de passe plus complexes. Cependant, les mots de passe complexes sont difficiles à retenir et sont souvent écrits, ce qui compromet encore davantage la sécurité du système.

Des méthodes alternatives ont été développées pour surmonter les problèmes posés par les mots de passe. Ces méthodes d'authentification alternatives peuvent consister en des jetons qui fournissent à l'utilisateur un mot de passe à usage unique (OTP) ePass [6], Haller [7] et Rubin [8] ou en une technologie d'empreintes digitales électroniques.

Ces méthodes d'authentification sont regroupées en trois approches, à savoir ;

- Une connaissance de l'utilisateur ;
- Un truc que l'utilisateur possède *;*
- Quelque moyen que l'utilisateur est *;*

La section suivante explique chaque approche plus en détail

1.5 Approches d'authentification

1.5.1 Quelque chose que l'utilisateur connaît

Il existe *une* perception selon laquelle les personnes peuvent être reconnues en présentant des informations que seule cette personne connaît. Cette perception peut être observée dans un scénario simple, lorsque vous appelez votre banque. Celle-ci vous pose généralement un certain nombre de questions afin de vérifier votre identité. Ces questions peuvent varier, mais elles sont généralement du type : quel est votre numéro d'assurance ou de téléphone *?* Quelle est votre date de naissance *?* Il s'agit là d'un exemple classique d'identification basée sur la connaissance. On parle souvent d'identification basée sur la connaissance lorsque l'utilisateur possède des informations telles que des mots de passe, des codes PIN ou un numéro d'assurance.

Les systèmes de mots de passe sont une forme courante d'identification basée sur la connaissance et constituent la forme d'authentification la plus répandue. Un mot de passe consiste en une série secrète de caractères conformes à certaines règles prédéfinies Zviran et al. [9]. Les mots de passe peuvent fournir une sécurité efficace s'ils sont mis en œuvre correctement. Cependant, avec la puissance de calcul actuelle, *les mots de passe doivent être suffisamment complexes pour* offrir une protection adéquate. Un mot de passe complexe se compose de plusieurs caractères numériques, alphabétiques et symboliques, tels que ZAbat@&sw79%§£24. Plus le mot de passe est complexe, plus il est difficile de s'en souvenir. Les gens écrivent souvent ces mots de passe complexes, ce qui rend les systèmes de mots de passe moins sûrs.

Zviran et al. [9] définit cinq séries de règles à appliquer lors de la création d'un mot de passe :

- *Mots de passe* sans dictionnaire et sans nom ;
- *Des mots de passe* suffisamment longs avec différents types de caractères ;
- Vieillissement du mot de passe et non réutilisation ;
- Complexe mais facile à mémoriser ;
- Les mots de passe ne doivent pas être partagés ni écrits.

Bien que les mots de passe offrent une sécurité suffisante pour la plupart des systèmes, certains systèmes d'information nécessitent un degré de sécurité plus élevé pour surmonter la faiblesse inhérente aux méthodes basées sur les mots de passe.

1.5.2 Quelque chose que l'utilisateur a

Un objet que l'utilisateur possède est souvent appelé authentification *par* jeton. L'authentification par jeton est utilisée pour prouver l'identité d'un utilisateur en fournissant un objet physique que seul le propriétaire autorisé de cet objet possède. Ces jetons peuvent consister en un large éventail d'objets, tels *que des certificats de naissance*, *des cartes de* sécurité, etc.

Les passeports sont la forme la plus courante d'authentification par jeton *dans le monde physique*. *Dans le monde virtuel*, deux types de jetons sont généralement utilisés, à savoir Zviran et al. [9] :

- Jetons de mémoire
- Jetons intelligents

-Les jetons de mémoire : stockent des informations uniques telles que des identifiants et des mots de passe complexes. Ces jetons ne traitent aucune information. Pour lire et traiter ces informations, un matériel spécial est nécessaire. Les cartes à puces magnétiques sont le type de jeton de mémoire le plus utilisé.

Ces cartes se trouvent souvent dans les cartes d'étudiant et les anciennes cartes de crédit. Ces cartes sont peu coûteuses à produire, mais elles peuvent être reproduites sans effort Ramsbrock et al. [10].

- **Les jetons intelligents** : sont le contraire des jetons à mémoire. Dotés de microprocesseurs intégrés, ils peuvent stocker et traiter des informations. En règle générale, les jetons de carte à puce sont utilisés pour l'authentification basée sur la connaissance, où le code PIN de l'utilisateur est stocké et vérifié sur la carte. Les cartes à puce ont la capacité d'effectuer une cryptographie complexe, ce qui rend ce type d'authentification possible. C'est une technologie attrayante.

Bien que l'authentification par jeton offre un niveau de sécurité élevé, le jeton ne garantit pas la preuve de la propriété puisque le jeton peut être volé ou reproduit.

1.5.3 Quelque chose que l'utilisateur est

Ce type d'authentification est basé sur la technologie biométrique. La technologie biométrique est un processus d'identification automatique utilisant certaines caractéristiques anatomiques, comportementales et physiologiques associées à l'utilisateur (Zviran et al. [9]. L'authentification par empreinte digitale est le type de biométrie le plus courammentutilisé.

L'authentification biométrique offre des niveaux élevés de sécurité et de commodité à l'utilisateur. L'accent est mis sur ce que l'utilisateur est plutôt que sur ce qu'il sait ou possède. La technologie biométrique se divise en deux catégories principales : comportementale et physiologique. La biométrie comportementale est basée sur des actions humaines telles que la reconnaissance de la signature ou de la voix. En revanche, la biométrie physiologique est basée sur les attributs physiques de l'utilisateur, tels que les empreintes digitales ou vasculaires des doigts.

1.5.4 Authentification multimodale

Les méthodes d'authentification décrites ci-dessus ne doivent pas être utilisées isolément. Ces méthodes d'authentification sont souvent combinées pour offrir une plus grande sécurité.

L'authentification multimodale combine deux ou plusieurs approches d'authentification existantes pour offrir une sécurité plus forte. L'authentification multimodale peut prêter à confusion. Demander à l'utilisateur un mot de passe et de répondre à une série de questions est toujours une authentification à un seul facteur puisque le mot de passe et les réponses relèvent de l'approche "quelque chose que l'utilisateur connaît". Demander à *l'utilisateur* de fournir certaines connaissances (quelque chose que l'utilisateur connaît*)* et de présenter un jeton (quelque chose que l'utilisateur possède) est un exemple d'une véritable authentification.

Les jetons RSA sont un choix populaire d'authentification multimodale. Ces jetons combinent "quelque chose que l'utilisateur connaît" et "quelque chose que l'utilisateur possède". Les cartes à puce sont de plus en plus utilisées par les banques pour remplacer les cartes de crédit. Les cartes magnétiques périmées. Ces banques stockent des codes PIN ou des modèles biométriques sur ces cartes à puce, ce qui permet à leurs clients de bénéficier d'une authentification multimodale.

1.6 Résumé

Ce chapitre a introduit les concepts d'identification et d'authentification en les décrivant brièvement dans le contexte du monde réel. Dans le monde virtuel, l'identification est une méthode permettant de se présenter au système en tant qu'utilisateur, tandis que l'authentification est utilisée pour vérifier que l'on est bien l'utilisateur déclaré.

Trois domaines clés ont été définis, à savoir la confidentialité, l'intégrité et la disponibilité, qui constituent les principales raisons pour lesquelles nous avons besoin d'une identification et d'une authentification.

L'authentification était le thème principal de ce chapitre. Il a été mentionné que l'authentification se présente sous différentes formes, à savoir

- Quelque chose que l'utilisateur connaît - comme les mots *de* passe
- Quelque chose que l'utilisateur possède, *comme* des cartes bancaires ;
- Ce que l'utilisateur est - par exemple des données biométriques (empreintes digitales).

Pour renforcer les méthodes d'authentification, les méthodes susmentionnées peuvent être combinées afin de fournir un niveau de sécurité plus élevé. Les cartes à puce modernes utilisées avec des gabarits biométriques sont un bon exemple de cette combinaison ; quelque chose que l'utilisateur possède est associé à quelque chose qu'il est.

Dans le chapitre suivant, l'authentification biométrique sera examinée en détail. Les différentes formes de ce type d'authentification ainsi que leurs avantages et inconvénients seront mis en évidence.

Trois axes principaux ont été identifiés, à savoir la confidentialité, l'intégrité et la disponibilité, qui sont les raisons principales de notre besoin d'identification et d'authentification.

La question de l'authentification était le sujet central de ce chapitre. On a dit que l'authentification peut prendre plusieurs formes, à savoir

- Un élément que l'utilisateur sait - tel que les mots de passe
- Un élément que l'utilisateur détient - tel que des cartes bancaires ;
- Quelles sont les caractéristiques de l'usager - comme par exemple ses données biométriques (empreintes digitales) ;

Afin de renforcer les procédures d'authentification, il est possible de combiner les méthodes mentionnées précédemment pour obtenir un degré de confiance plus élevé. Les cartes à puce modernes utilisées avec des gabarits biométriques sont un bon exemple de cette combinaison ; un truc que l'usager possède est associé à quelque chose qu'il est.

Chapitre II : La biométrie

2.1 Introduction

La biométrie est définie comme l'utilisation de caractéristiques biologiques, physiologiques ou comportementales pour identifier une personne [1]. Le mot biométrie est dérivé des mots grecs bios, qui signifie vie, et metron, qui signifie mesure. La biométrie repose sur l'utilisation de caractéristiques mesurables, robustes et distinctives. Le terme « robuste » est utilisé pour décrire la variabilité de la caractéristique dans le temps [2].

Ce chapitre commence par un bref historique sur la biométrie, suivi d'une présentation des systèmes biométriques automatisés. Ces systèmes automatisés peuvent être constitués de plusieurs types de données biométriques.
Chaque biométrie sera étudiée sous l'angle de sa fonctionnalité, de ses bénéfices et de ses défauts.

2.2 Histoire de la biométrie

Hollywood est souvent connu pour avoir présenté les dernières technologies sur ses grands écrans. En 2008, le film de James Bond Quantum of Solace a introduit la technologie des écrans tactiles [3] et des tablettes mobiles, mais ces gadgets ne sont apparus sur le marché qu'en 2010.

Ce n'est pas la première fois qu'Hollywood sort des films qui présentent des technologies nouvelles et souvent inédites. En 2002, des films tels que "***Minority Report***" et "***Die another day***" ont montré l'utilisation de la technologie biométrique [4]. L'identification est effectuée dans ces films à l'aide de la reconnaissance des yeux et des empreintes palmaires.

Les nombreuses personnes qui ont regardé ces films ont pensé que le concept de la biométrie est une nouvelle technologie qui n'a jamais existé avant. Or, ces personnes se sont trompées lourdement. La biométrie est une vieille coutume utilisée pour vérifier l'identité des personnes.

Les références au concept de la biométrie remontent à 2550 av. J.-C. dans l'ancienne Égypte. Voyons comment la biométrie a été mise en œuvre dans l'Antiquité. Lors de la construction de la grande pyramide de Gizeh, la pyramide de Khéops comptait plus de 20 000 ouvriers sur le chantier. La gestion d'une main-d'œuvre de plus de 20 000 personnes peut entraîner de nombreux problèmes logistiques. L'un de ces problèmes s'est posé lors de la gestion des approvisionnements en nourriture. Pour gérer l'approvisionnement en nourriture, les administrateurs ont mis au point un système dans lequel chaque travailleur est affecté à un entrepôt de nourriture. Une fois par mois, le travailleur se rend à l'entrepôt auquel il a été affecté

Afin de percevoir son allocation alimentaire mensuelle. Pour garder une trace de chaque travailleur, les administrateurs enregistraient le nom, l'âge, le lieu d'origine, la profession et la dernière date à laquelle ce travailleur avait reçu son allocation. Les informations enregistrées ont été utilisées pour vérifier l'identité du travailleur à chaque tentative de collecte.

Toutefois, ce système s'est avéré inefficace. Les travailleurs demandaient l'allocation alimentaire sous de multiples fausses identités. Pour éviter les fraudes, les administrateurs ont commencé à enregistrer les caractéristiques physiques et comportementales des travailleurs, telles que la taille, la couleur des yeux et même le teint [5].

Dans l'ancienne Babylone et en Chine, des empreintes digitales ont été retrouvées sur des tablettes d'argile. Ces empreintes digitales étaient utilisées pour effectuer des transactions commerciales [6]. La figure 2-1 (c) montre des tablettes d'argile sur lesquelles figurent des empreintes digitales.

En 1858, Sir William James Herschel, premier magistrat du district de Hooghly à Jungipoor, en Inde, a utilisé pour la première fois les empreintes digitales et palmaires pour conclure des contrats avec la population locale. La figure 2-1 (a) montre le contrat entre Sir Herschel et les habitants. L'intention initiale était d'utiliser ces empreintes pour "effrayer (l'utilisateur) de toute idée de répudier sa signature". Cependant, au fil du temps, Sir Herschel a rassemblé un plus grand nombre de ces empreintes et il était fermement convaincu que ces dernières pouvaient être utilisées pour prouver ou réfuter l'identité de l'utilisateur [7].

Alphonse Bertillon, officier de la préfecture de police de Paris, en France, a mis au point un système de classification, connu sous le nom d'anthropométrie ou de système Bertillon, qui utilise les mesures des parties du corps. Le système de Bertillon comprend des mesures telles que la longueur et la largeur de la tête, la longueur du majeur, la longueur du pied gauche et la longueur de l'avant-bras, du coude à l'extrémité du majeur. Bertillon a également mis au point un système de photographie des visages, que l'on a appelé les « mugshots » figure 2-1 (b)

Bertillon a noté que même si les délinquants criminels utilisaient souvent différents pseudonymes, ils ne pouvaient pas changer certains éléments de leur corps [8].

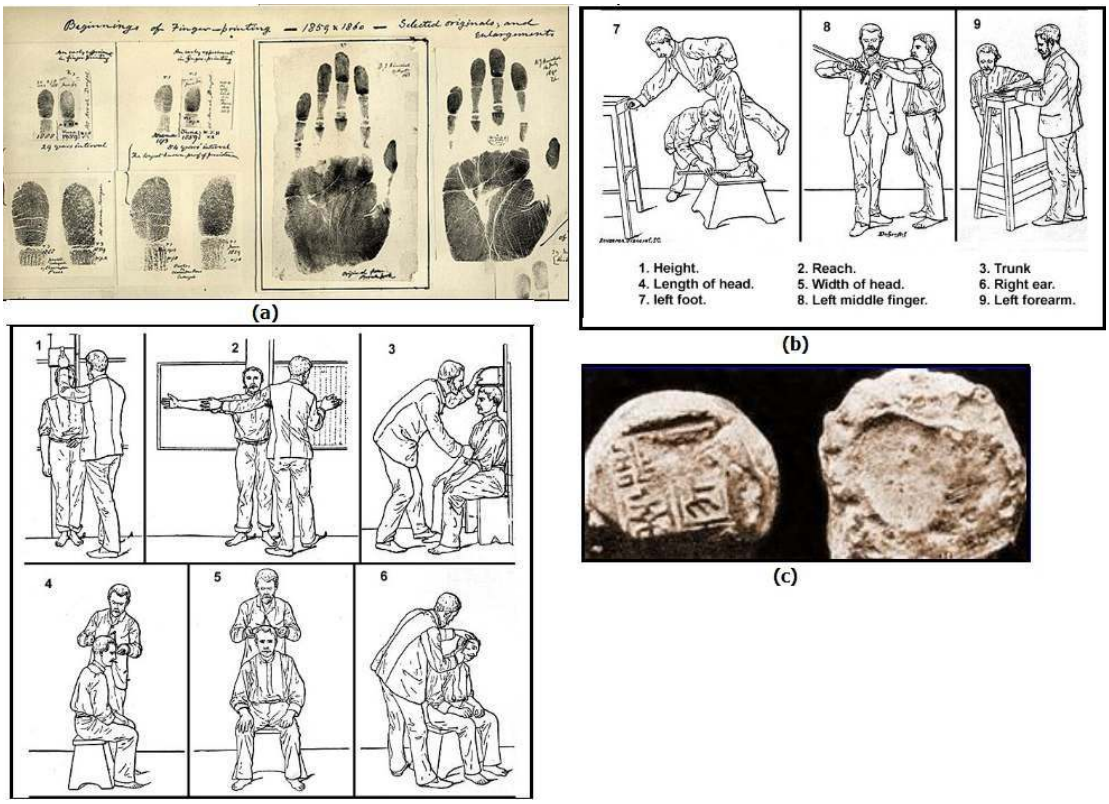


Figure 2-1 : Anciennes applications biométriques

(a) - Empreintes digitales et palmaires prises par Sir Herschel pour des transactions commerciales.

(b) - Illustration du système de bertillonnage, qui consiste à mesurer des parties du corps.

(c) - Empreintes digitales gravées sur des tablettes d'argile dans la Babylone et la Chine anciennes Au centre

Les documents chinois de la dynastie Qin (221-206 av. J.-C.) contiennent des informations sur l'utilisation des empreintes des mains comme éléments de preuve lors d'enquêtes sur des cambriolages. Des sceaux d'argile portant des empreintes de crêtes de frottement ont été utilisés sous les dynasties Qin et Han (221 av. J.-C. - 220 apr. J.-C.).

Sir Francis Galton a travaillé toute sa vie sur les empreintes digitales. Il a déclaré qu'il n'y avait pas deux empreintes digitales identiques Motorola [9]. Galton a également inventé le concept de "minuties", qui est encore utilisé aujourd'hui pour comparer les empreintes digitales. Les minuties sont des points d'intérêt trouvés sur une empreinte digitale qui la rendent unique. Ces points d'intérêt sont formés par la terminaison ou la bifurcation des crêtes cutanées de frottement sur chaque doigt et sont définis comme l'un des éléments suivants :

- Fin de crête - le point où une crête se termine ;
- Bifurcation - le point où une crête unique se divise en deux (2) crêtes.

En 1879, Edward Henry a mis au point la première méthode de classification pour l'identification des empreintes digitales, appelée système de classification Henry. Ce système classe chaque empreinte selon qu'elle présente un "arc", un "verticille" ou une "boucle" Motorola [9]. Le système de classification Henry est encore utilisé aujourd'hui dans le cadre du processus de classification. Ce système de classification de Henry est utilisé jusqu'au aujourd'hui.

La biométrie des empreintes digitales n'est pas la seule à avoir fait l'objet de recherches au fil des ans.

- En 1936, Frank Burch a proposé une méthode d'identification utilisant les motifs de l'iris.
- En 1965, North American Aviation a mis au point le premier système de reconnaissance de signature.
- 1974, le premier système commercial de géométrie manuelle.
- 1976, le premier prototype de système de reconnaissance du locuteur.
- 1988, le premier système de reconnaissance faciale semi-automatique utilisant des images vidéo.

Au milieu des années 1960 et 1970, des scientifiques ont travaillé sur des méthodes permettant d'automatiser le processus de capture et d'identification des empreintes digitales. Au début des années 1980, un système automatisé entièrement fonctionnel a été inventé, qui effectue une comparaison avec une base de données électronique - le système automatisé d'identification des empreintes digitales (AFIS) [9].

Les systèmes automatisés ont été créés pour réduire le temps de saisie et de recherche de plusieurs mois et semaines à quelques heures et minutes.
Nous poursuivrons notre étude de la biométrie en étudiant les raisons pour lesquelles elle devrait être utilisée.

2.3 Avantages de la biométrie

La biométrie est devenue un choix de plus en plus populaire pour de nombreuses organisations, et ce pour de bonnes raisons. La technologie biométrique offre de nombreux avantages par rapport à ses homologues - les mots de passe et les jetons. Examinons les principales raisons d'utiliser la technologie biométrique.

2.3.1 Commodité pour les utilisateurs finaux - L'un des principaux arguments de vente de tout système biométrique est la commodité qu'il offre à l'utilisateur final. Les mots de passe, les

jetons, les cartes et même les clés exigent de l'utilisateur qu'il se souvienne des mots de passe ou qu'il possède un de ces gadgets. En revanche, les systèmes biométriques n'exigent pas de l'utilisateur final qu'il possède des informations ou qu'il transporte un objet, car la technologie repose sur un identifiant unique intégré dans les caractéristiques de la personne même. Par conséquent, la technologie évite à l'utilisateur de devoir se souvenir d'un mot de passe, de porter une carte, un jeton ou, dans le pire des cas, de se souvenir de plusieurs mots de passe pour différents systèmes au sein d'une organisation.

2.3.2 Commodité pour l'administration informatique - Dans les organisations qui mettent en œuvre l'authentification par mot de passe ou par jeton, les administrateurs informatiques et le personnel d'assistance sont confrontés à la tâche décourageante de gérer ces systèmes. Les mots de passe sont oubliés, expirés ou même compromis. Ces administrateurs doivent gérer la réinitialisation des mots de passe ou le remplacement des jetons perdus ou volés. L'audit du système peut également devenir un défi ; remonter d'un événement particulier du système à un utilisateur peut devenir une tâche difficile, car les mots de passe et les jetons sont souvent partagés entre collègues et peuvent être compromis. Les systèmes biométriques offrent une plus grande facilité aux administrateurs informatiques pour gérer l'authentification des utilisateurs. Avec la biométrie, il n'y a rien à réinitialiser ou à remplacer et chaque événement peut être suivi en termes de "qui a fait quoi".

2.3.3 Amélioration de la sécurité - Woodward et al. [10] a déclaré que les systèmes biométriques "devraient réduire le risque de compromission, c'est-à-dire la probabilité qu'un adversaire puisse présenter un identifiant approprié et obtenir un accès non autorisé". Le partage de mots de passe avec des collègues et la perte de jetons peuvent facilement compromettre les systèmes d'information. L'utilisation d'un identifiant biométrique unique élimine les problèmes liés au partage des informations d'identification. La reproduction des identifiants biométriques est très difficile, voire impossible.

2.3.4 Prévention de la fraude - Bubeck et al. [6] affirme que les systèmes biométriques offrent deux avantages importants : la détection et la dissuasion de la fraude. Par exemple, unepersonne peut revendiquer plusieurs identités pour bénéficier d'une subvention gouvernementale. Sans la biométrie, il serait extrêmement difficile d'identifier l'activité frauduleuse compte tenu des grandes quantités de données stockées dans un tel système. La biométrie peut donc contribuer à la prévention de la fraude.

La présence d'une telle caractéristique dans un système a un effet psychologique sur les personnes, car elle les dissuade de tenter de s'enregistrer plus d'une fois, étant donné qu'elles prennent conscience du fait que leurs caractéristiques physiologiques/comportementales uniques sont utilisées pour les identifier Bubeck et al. [6]. La biométrie a donc un effet dissuasif sur la fraude.

2.3.5 Faible coût - Au fil des ans, l'amélioration du matériel et des logiciels biométriques a permis de réduire le coût de l'authentification biométrique à un niveau commercial. Grâce à cette baisse des coûts, de nombreux organismes privés et gouvernements ont mis la biométrie à la disposition du public. Cela permet aux utilisateurs finaux de se familiariser avec ces nouvelles technologies. Les fabricants d'ordinateurs intègrent des capteurs biométriques et des logiciels dans les claviers, les souris et les ordinateurs portables. HP a intégré depuis les années 80 des scanners d'empreintes digitales à ses ordinateurs portables. Logitech propose des scanners d'empreintes digitales avec ses claviers et, plus récemment, Lenovo a intégré un logiciel de reconnaissance faciale qui utilise la webcam intégrée de l'ordinateur portable, comme l'illustre la figure 2-2.

Figure 2-2 : Reconnaissance faciale dans les produits commerciaux
Logiciel de reconnaissance faciale que Lenovo utilise pour la connexion à Windows.

Bien que la biométrie présente de nombreux avantages, elle a aussi ses inconvénients que nous abordons dans la section suivante.

2.4 Inconvénients de la biométrie

Bien que la biométrie offre de nombreux avantages à la société, elle soulève des questions qu'il convient d'aborder. Il existe sept problèmes concernant la biométrie, à savoir Woodward [10], NBSP [11] ; Nous allons maintenant examiner chaque question plus en détail.

2.4.1 Vie privée

Lorsque les données biométriques sont saisies, l'utilisateur final donne des informations sur lui-même qui peuvent être utilisées pour l'identification. Le fait de donner ses informations

Biométriques sur soi-même peut constituer un risque pour le droit à la vie privée. D'un autre côté, l'utilisation d'informations biométriques peut présenter des avantages en termes de sécurité. Un bon exemple est celui de la période précédant le 11 septembre (9/11). De nombreuses personnes remettaient en question le droit à la vie privée que la biométrie pouvait envahir. En revanche, après le 11 septembre, les gens se sont interrogés sur l'aspect sécuritaire de la biométrie.

Examinons les deux préoccupations importantes liées à la protection de la vie privée.

2.4.1.1 Divulgation à des tiers - Avez-vous déjà reçu un appel téléphonique, un courriel ou un SMS d'une entreprise voulant vous vendre ses produits ? Vous êtes-vous déjà demandé où elle avait obtenu vos coordonnées ? Ce n'est un secret pour personne que les organisations qui disposent de vos informations (avec ou sans votre consentement) les vendent à des tiers. Il est à craindre que les données biométriques subissent le même sort. Une fois les données biométriques collectées, les données brutes peuvent être copiées et reproduites facilement. Ces données peuvent être partagées entre d'innombrables bases de données des secteurs public et privé. Prenons l'exemple suivant. Ma banque locale met en place un système de biométrie faciale et d'empreintes digitales afin que toutes mes transactions financières soient plus sûres. J'enregistre mon visage et mes empreintes digitales auprès de ma banque locale. Lorsque j'entre dans la banque, je présente mon visage à la caméra. Lors de toute transaction financière, j'utilise mes empreintes digitales pour finaliser la transaction.

Au bout d'un certain temps, j'ai commencé à recevoir des informations commerciales de la part de sociétés de prêt et de cartes de crédit qui me demandaient de me présenter dans leur agence parce que j'étais déjà préenregistré biométriquement dans leurs systèmes. En effet, ma banque a vendu à ces sociétés, en même temps que mes coordonnées, mes images faciales et d'empreintes digitales avec les données brutes et les modèles. Plus tard, alors que je fais des achats dans un magasin, leurs caméras me reconnaissent et alertent un vendeur qui me propose sa carte de magasin.

2.4.1.2 Informations supplémentaires obtenues - Des recherches récentes ont suggéré que les données biométriques peuvent être utilisées à d'autres fins que l'identification. Les données biométriques saisies peuvent fournir des informations sur la santé et les antécédents médicaux d'une personne. Les recherches du Dr Howard Chen [12] dans le domaine de la dermatoglyphie - L'étude des motifs des crêtes de la peau et des parties des mains et des pieds - indiquent que "certains troubles chromosomiques sont connus pour être associés à des anomalies

Dermatoglyphiques caractéristiques". Le Dr Chen mentionne spécifiquement le syndrome de Down, le syndrome de Turner et le syndrome de Klinefelter comme des troubles chromosomiques qui provoquent des empreintes digitales inhabituelles chez une personne. Certains troubles non chromosomiques, tels que la leucémie et le cancer du sein, ont également été associés à des empreintes digitales inhabituelles.

Dans son article Courtney Ostaff [13] souligne que de nombreux problèmes de santése manifestent dans nos yeux. La consommation de drogues comme la cocaïne et l'alcool, les maladies infectieuses comme le paludisme, le sida, la varicelle, les maladies chroniques comme l'insuffisance cardiaque, le cholestérol, l'hypertension et même la grossesse se manifestent dans les yeux. En examinant l'iris et la rétine, les experts pensent pouvoir déterminer l'état de santé d'une personne.

Bien que des recherches supplémentaires doivent être menées dans ce domaine, la simple perception que la biométrie pourrait divulguer des informations sensibles découragera les gens d'utiliser un système biométrique avantageux.

Nous avons abordé le premier inconvénient de la biométrie, à savoir la protection de la vie privée. Poursuivons l'examen des autres aspects de la biométrie.

2.4.2 Atteinte à l'intégrité physique

Les gens pensent que des maladies telles que la conjonctivite peut résulter d'un contact avec des dispositifs semblables à des jumelles que des étrangers ont touchées. D'autres pensent que l'exposition d'organes vitaux tels que les yeux peuvent endommager la vision, ce qui n'est pas le cas. Il n'existe aucun cas documenté de biométrie causant un préjudice réel à une personne.

Les activités criminelles peuvent conduire à des membres coupés, comme l'empreinte d'un doigt ou d'une paume.

2.4.3 Détournement de fonction

Également appelé « détournement de mission », il s'agit du processus par lequel l'objectif initial d'obtention de l'information est élargi à d'autres objectifs que celui qui avait été défini à l'origine. Le détournement de fonction peut se produire avec ou sans la connaissance ou l'accord d'une personne.

Au départ, lors de la mise en œuvre, le système biométrique serait utilisé dans un but limité et spécifique - pour lutter contre la fraude ou protéger les transactions financières, etc. Au fil du temps, le système biométrique sera utilisé à des fins supplémentaires qui n'ont pas été annoncées ou qui n'étaient même pas prévues lors de la conception initiale.

Prenons l'exemple précédent : j'ai enregistré mon visage et mes empreintes digitales auprès de ma banque locale. Plus tard, au cours du scénario, la police est confrontée au meurtre horrible du directeur de la succursale de la banque, dont la seule preuve est une empreinte digitale latente sur l'arme du crime. La police commence son enquête en recherchant une correspondance d'empreintes digitales dans sa base de données. En l'absence de correspondance, elle demande au nouveau directeur de l'agence de lui remettre la base de données d'empreintes digitales de la banque.

2.4.4 Objections culturelles

Les systèmes biométriques peuvent ne pas être acceptés par tous. Il existe de nombreuses objections culturelles, religieuses et philosophiques. Certains chrétiens pensent quela biométrie est une "marque de la bête". Cette objection se fonde sur les révélations du NouveauTestament :

Les secteurs privé et public doivent tenir compte des réactions des clients pour que le système soit accepté.

En Californie, des groupes religieux se sont plaints du fait que les appareils de géométrie de la main apposaient "la marque de la bête" sur les mains des personnes inscrites Woodward [10]. En Alabama, deux personnes se sont opposées à la fourniture d'un numéro de sécurité sociale (SSN) pour demander un permis de conduire. Ces personnes ont fondé leur refus sur des convictions religieuses qui les empêchent d'avoir un numéro de sécurité sociale. En revanche, la Californie, le Texas, le Colorado, Hawaï et la Géorgie ont mis en place avec succèsun système permettant d'obtenir les empreintes digitales du conducteur pour son permis de conduire.

2.4.5 Fausses données biométriques

Une attaque utilise un faux justificatif d'identité pour tenter d'accéder à un système ou à un bâtiment. Des recherches récentes ont montré que les dispositifs biométriques peuvent être usurpés à l'aide de diverses méthodes. L'une d'entre elles consiste à fournir un échantillon biométrique artificiel ou simulé. Le professeur Tsutomu Matsumoto a relevé (Woodward et al.

[10], Gregory et al. [14], Matsumoto et al. [15]**)** deux méthodes de création d'une empreinte digitale artificielle. Les deux méthodes utilisent de la gélatine pour recréer le doigt d'une personne, ce qui est souvent appelé "gummy fingers" (doigts gommeux).

La détection du caractère vivant est l'une des méthodes proposées pour lutter contre ces attaques. Les tests de vivacité biométrique sont des tests automatisés réalisés pour déterminer si l'échantillon biométrique présenté au système biométrique provient d'un être humain vivant - pas n'importe quel être humain vivant, cependant, mais l'être humain vivant qui a été enregistré à l'origine dans le système.

2.4.6 Attaques par répétition

Les attaques par réémission se produisent lorsqu'un pirate a trouvé un moyen de retransmettre des données d'authentification biométrique connues sur le réseau de manière à tromper le système et à l'amener à l'admettre.

Lors d'une attaque par relecture, l'attaquant est en mesure d'enregistrer une connexion réussie. Les données biométriques non cryptées envoyées sur le réseau peuvent être interceptées par l'attaquant. L'attaquant rejouera ensuite ces données pour tenter d'obtenir un accès.

Par exemple, lors de la reconnaissance vocale, le pirate peut enregistrer les données biométriques (la voix légitime) par le biais d'un microphone caché et la rejouer plus tard.

2.4.7 Informations d'identification volées

Bien qu'il soit assez difficile de voler un trait biométrique, il est arrivé que des parties du corps soient volées à des utilisateurs légitimes pour tromper un système biométrique. Comme le rapporte le BCC, Gregory et al. [14], les membres d'un gang en Malaisie ont coupé le doigt du propriétaire d'une voiture pour franchir le système de sécurité des empreintes digitales de la Mercedes Classe S du propriétaire.

En Afrique du Sud, les retraités utilisent leurs empreintes digitales pour réclamer leur chèque de pension mensuel. Lors d'une fraude au système d'empreintes digitales Woodward et al. [10], un couple a expliqué au receveur des postes que le vieil l'homme âgé les accompagnant était leur oncle et ont déclaré : "Il est très paresseux, il ne se donne pas la peine de rester éveillé pour réclamer sa pension, Il est peut-être ivre ou même malade." Le receveur des postes a commencé à avoir des soupçons lorsqu'il a remarqué que les yeux du vieil homme étaient complètement fermés et immobiles. Puis, lorsqu'il a remarqué la façon dont le jeune homme

manœuvrait la main du vieil homme sur le comptoir pour prendre ses empreintes digitales, le receveur des postes leur a dit que la pension de vieillesse n'avait pas été versée et qu'il n'y avait pas d'autre solution.

Les demandeurs doivent être en pleine possession de leur corps et de leur esprit pour obtenir leur argent, et il convoque son superviseur.

À ce moment-là, le couple a crié après le receveur des postes et s'est brusquement enfui, laissant le vieil homme s'effondrer sur le sol. Le receveur explique : "Lorsque je me suis rendu de l'autre côté du guichet, j'ai constaté que le vieil homme était glacé et qu'il était manifestement mort depuis de nombreuses heures, et j'ai donc appelé la police.

Il est important de noter qu'une fois qu'un trait biométrique est compromis, il ne peut être remplacé ou réinitialisé, contrairement aux mots de passe.

Nous passons maintenant à la section suivante, qui étudie les caractéristiques biométriques.

2.5 Caractéristiques biométriques

Il existe différents types de systèmes biométriques. Chaque système peut être basé sur un trait biométrique différent : l'iris, les empreintes digitales ou même la reconnaissance faciale. Ces systèmes peuvent sembler différents, mais l'architecture qui les sous-tend est assez similaire. Tous les systèmes biométriques fonctionnent en enregistrant les utilisateurs en mesurant et en stockant leurs caractéristiques biométriques particulières, puis en comparant les données biométriques stockées avec les données des sujets non vérifiés pour déterminer s'ils doivent être autorisés à accéder à un système ou à un lieu Gregory al. [14].

Examinons les caractéristiques Woodward et al. [10] d'un trait biométrique, qui révèlent certains attributs que tous les systèmes d'authentification basés sur la biométrie devraient posséder.

2.5.1 Robustesse

La robustesse fait référence à la capacité d'une caractéristique biométrique particulière à être présentée de manière répétée à un système biométrique pour une mesure automatisée réussie Woodward et al. [10]. Un système biométrique doit être basé sur une caractéristique biométrique qui change lentement (voire pas du tout) au fil du temps. La reconnaissance de l'iris est un bon exemple de biométrie robuste, ce qui n'est pas le cas de la reconnaissance vocale.

2.5.2 Unicité

L'unicité est la capacité d'une caractéristique biométrique particulière d'une personne à être différente des autres dans la population utilisatrice et la différence peut être mesurée Woodward et al. [10]. L'unicité d'un trait biométrique peut être classée en trois catégories : génétique, phénotypique et comportementale.

I. ***Génétique -*** caractéristiques telles que la couleur des cheveux et des yeux, héritées des parents de l'utilisateur final. En théorie, certaines caractéristiques génétiques sont très difficiles à modifier.

II. ***Phénotypique -*** Il s'agit de traits biométriques développés au cours des stades embryonnaires de la vie. Ces traits sont une sorte d'aléatoire sur la feuille de route génétique permettant une plus grande distinction dans la population générale pour certaines caractéristiques biométriques telles que les motifs de l'iris, les empreintes digitales et les réseaux vasculaires Woodward et al. [10].

III. ***Comportementales -*** Il s'agit de caractéristiques biométriques qui sont apprises ou développées au fil du temps. Les caractéristiques biométriques telles que la signature et la voix entrent dans cette catégorie.

2.5.3 Universalité

Il s'agit de savoir si chaque personne possède les caractéristiques mesurées. L'universalité peut être résumée en une seule question : Est-ce que toutes les personnes de votre groupe cible possèdent cette caractéristique biométrique ? Tout le monde dans votre organisation peut avoir au moins un doigt pour la biométrie des empreintes digitales, mais la biométrie basée sur la démarche peut être difficile à mesurer si vous avez un membre du personnel qui se déplace en fauteuil roulant.

2.5.4 Possibilité de collectionner

Il s'agit de la facilité avec laquelle la biométrie est collectée. La biométrie par empreintes digitales obtient de bons résultats car le processus de collecte est rapide et non invasif. En revanche, la collecte de l'ADN est un processus intrusif. Les systèmes basés sur la démarche exigent de l'utilisateur final qu'il marche sur une certaine distance et le balayage de la rétine exige de l'utilisateur final qu'il s'approche très près du scanner.

2.5.5 Performance

Il s'agit de la quantité d'équipement, de temps et de calculs nécessaires au traitement d'une comparaison Gregory al. [14]. Les systèmes biométriques à base d'empreintes digitales sont assez performants car la technologie des empreintes digitales est légère et précise. Les systèmes biométriques basés sur l'ADN sont coûteux, lents, gourmands en ressources et en main-d'œuvre.

2.5.6 Précision

Dans quelle mesure la comparaison est-elle correcte ? Le système présente-t-il un taux élevé de fausses acceptations (nombre de personnes acceptées qui devraient être rejetées) ? La biométrie de l'iris et de la rétine a un taux d'acceptation erronée très faible.

2.5.7 Acceptabilité

Les utilisateurs finaux sont-ils à l'aise avec le système ? La biométrie par l'ADN obtiendra un score très faible pour des raisons de protection de la vie privée. La rétine met les gens mal à l'aise en plaçant leur œil très près de quelque chose qui semble intrusif. Cependant, certaines personnes ne verront pas d'inconvénient à passer leur doigt sur un lecteur d'empreintes digitales.

2.5.8 Contournement

Est-il facile de tromper le lecteur biométrique ? Certains dispositifs à empreintes digitales peuvent être falsifiés en utilisant des doigts gommés. Les dispositifs rétiniens dépendent des motifs vasculaires derrière l'œil, qui n'existent que lorsque l'utilisateur est vivant.

Nous passons maintenant à la section suivante, qui traite de l'architecture d'un système biométrique et des composants utilisés pour traiter un trait biométrique.

2.6 Architecture du système

Chaque système biométrique est composé de quatre éléments essentiels, à savoir l'acquisition des données, le traitement du signal, la politique de décision et le stockage Woodward et al. [10]. La figure 2.3 illustre un système biométrique de haut niveau.

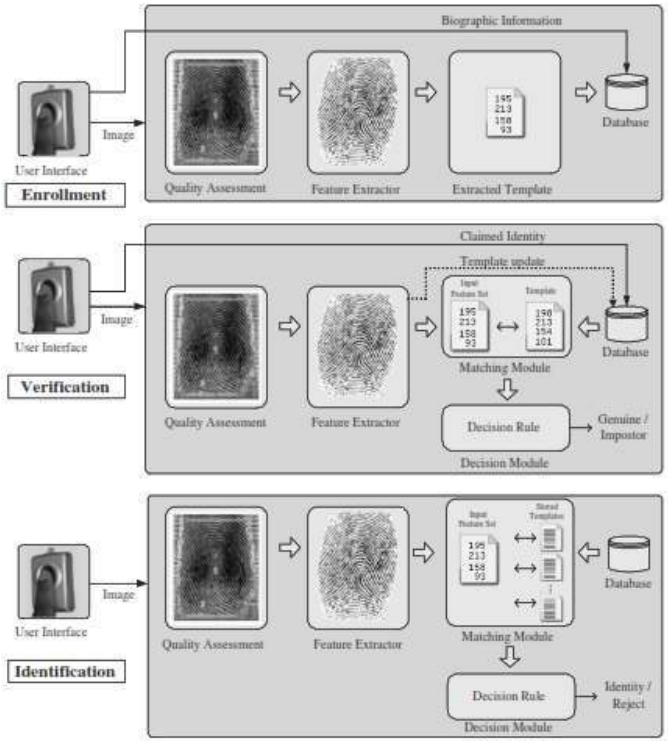


Figure 2-3 : Architecture des systèmes biométriques : Étapes d'inscription et reconnaissanced'un système biométrique fonctionnant en modes de vérification et d'identification. La ligne en pointillé dans le module de ver vérification est une opération facultative permettant de mettre à jour le gabarit d'un utilisateur particulier

Chaque système biométrique comporte quatre éléments essentiels. Ces éléments sont indépendants des caractéristiques biométriques

Chacun de ces modules est constitué de multiples sous-composants. Afin d'avoir une vision globale d'un système biométrique, analysons brièvement le rôle de chaque composant.

2.6.1 Composants d'un système biométrique

Acquisition des données : Au cours de cette phase, les données biométriques sont présentées au système. Le lecteur biométrique capture une représentation numérique de la biométrie qui est ensuite envoyée au module de traitement du signal.

Traitement du signal : À ce stade, l'échantillon biométrique ou les données brutes sont reçus par le processeur du signal. Les données biométriques seront traitées pour l'appariement ou l'enrôlement. L'échantillon biométrique est soumis à des étapes de segmentation et d'extraction de caractéristiques afin de créer un modèle. Le résultat de la segmentation et de l'extraction des caractéristiques est un score de qualité. Le score de qualité reflète la qualité de

L'échantillon biométrique et de l'enregistrement. Le degré de réussite de l'extraction des caractéristiques. Lors de l'inscription, le score de qualité est utilisé pour déterminer si l'utilisateur peut être inscrit. D'autre part, lors de l'authentification, le modèle nouvellement créé est comparé aux modèles existants pour produire le score de correspondance, qui indique le degré de précision des modèles.

Politique de décision : L'étape finale du processus. La politique de décision prend en compte les paramètres de sortie (score de qualité/correspondance) de la phase de traitement du signal qui est utilisée pour déterminer la décision finale (les scores sont acceptables ou non). Les résultats sont comparés à un seuil défini par le système pour déterminer si le processus a réussi ou échoué.

Stockage : Une fois le gabarit biométrique créé lors de l'enrôlement, il doit être stocké en vue d'une utilisation ultérieure. Il existe différentes méthodes de stockage : local (sur le dispositif), réseau (base de données) et stockage portable (cartes à puce). Si la capacité de stockage n'est pas limitée, des données telles que les journaux d'audit peuvent être stockées.

Nous avons abordé le rôle que joue chaque composant dans le système biométrique. Pour que ces composants atteignent leurs objectifs et pour simplifier la compréhension des méthodes utilisées pour atteindre ces objectifs, chaque composant est constitué de plusieurs sous-composants.

2.6.1.1. Authentification

Le processus d'authentification est beaucoup plus simple que l'inscription. Dans ce scénario, un seul échantillon biométrique est capturé à des fins de comparaison. Bien qu'un échantillon de bonne qualité soit préférable pour le système, il n'est pas obligatoire. Le système rejettera très probablement l'utilisateur si un échantillon de mauvaise qualité est fourni, mais cette décision est basée sur un certain nombre de facteurs examinés dans la section relative à la politique de décision.

Le processus d'authentification comporte deux volets : l'identification et la vérification.

- L'identification, également appelée comparaison entre plusieurs personnes, est un processus qui permet de déterminer le propriétaire des données biométriques fournies. À qui appartiennent ces données biométriques ?

- La vérification, également appelée correspondance biunivoque, permet deconfirmer que les données biométriques appartiennent bien à un utilisateur donné. Ces données biométriques appartiennent-elles à SLMANI Amani ?

Nous allons maintenant passer à la deuxième composante, le traitement du signal.

2.6.1.2 Composante 2 - Traitement du signal

L'objectif de la phase de traitement du signal est de créer un modèle biométrique à partir de l'échantillon biométrique de l'utilisateur. Des scores numériques seront également produits à la fin de ce processus. Ces scores sont utilisés dans le cadre de la politique dedécision d'acceptation ou de rejet de la demande d'inscription ou d'authentification. La phase de traitement du signal se décompose en trois étapes essentielles, à savoir la segmentation, l'extraction des caractéristiques et la création d'un modèle.

Nous allons maintenant étudier ces étapes plus en détail.

2.6.1.2.1 Étape 1 - Segmentation

La segmentation est le processus qui vise à éliminer les informations d'arrière-plan non pertinentes des données biométriques ; il s'agit d'une étape souhaitable et nécessaire avant de procéder à l'extraction des caractéristiques. La figure 2-4 illustre le processus de séparation des informations d'arrière-plan et des informations faciales Woodward et al. [10]. La segmentation améliore les performances des algorithmes suivants, leur permettant de localiser et d'extraire plus efficacement les caractéristiques pertinentes (avec moins de données à traiter). Au cours du processus de création du modèle, il y a généralement aussi des étapes de normalisation des données. La normalisation est le processus d'ajustement ou de mise à l'échelle des données de manière à ce que leur plage de valeurs soit toujours comprise dans une plage conviviale et connue. La normalisation est utile à diverses fins et peut être appliquée aux données brutes ainsi qu'aux plaques d'immatriculation « finies ». Fondamentalement, la normalisation permet d'éliminer les surprises qui pourraient autrement affecter les procédures de mise en correspondance.

Le résultat du traitement du signal d'un système biométrique est généralement le score de qualité et le score de concordance. Ces informations sont utilisées par l'application décisionnelle, conformément à la politique de seuil définie par l'utilisateur final (ou l'administrateur du système), pour déterminer s'il existe une correspondance ou une inscription acceptable.

La figure 2-4 illustre le processus de segmentation pour la reconnaissance faciale. Les images de la ligne ci-dessous représentent uniquement les informations biométriques pertinentes.

Figure 2-4 : Segmentation faciale

2.6.1.2.2 Étape *2 - Extraction des caractéristiques*

L'étape d'extraction des caractéristiques est responsable de la localisation et de l'extraction des données biométriques souhaitées. Prenons l'exemple d'un échantillon d'empreinte digitale segmenté. L'algorithme d'extraction des caractéristiques doit localiser les points caractéristiques et les crêtes de l'empreinte digitale. La figure 2-5 illustre l'exemple d'une empreinte digitale où les points caractéristiques importants sont localisés.
Une fois les données localisées, l'algorithme n'utilisera que les données qui ont été localisées.

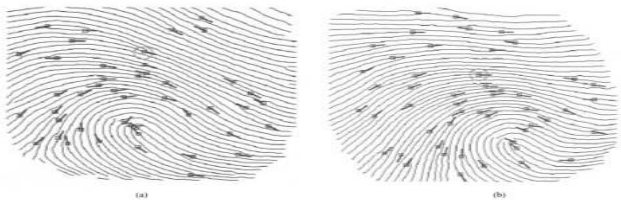


Figure 2-5 : Fig. 15. Résultats de l'application de l'algorithme de mise en correspondance à un ensemble de points caractéristiques et à un modèle. (a) jeu de points caractéristiques d'entrée. (b) Jeu de points caractéristiques du modèle [17].

L'extraction des caractéristiques consiste à trouver des données uniques pour le trait biométrique.

2.6.1.2.3 Étape 3 - Création d'un modèle

Un modèle est un petit fichier dérivé des caractéristiques distinctives des données biométriques d'un utilisateur Bubeck et al. [16]. Les modèles ne sont généralement pas l'image réelle ou l'échantillon biométrique numérique, mais une représentation mathématique des caractéristiques biométriques importantes. Une fois l'étape d'extraction des caractéristiques terminée, les caractéristiques extraites sont converties en modèle.

Dans la plupart des cas, les algorithmes qui effectuent la conversion sont la propriété des fournisseurs.

Les gabarits d'empreintes digitales peuvent faire l'objet d'une ingénierie inverse afin de recréer l'image biométrique originale d'une personne à partir du gabarit biométrique. Cette affirmation a été confirmée par les recherches de Jain [18, 19], qui a réussi à créer une image d'empreinte digitale en utilisant uniquement le gabarit.

Deux types de modèles biométriques peuvent être créés.

- *Modèle d'inscription* - Ce modèle est créé lors de l'inscription et stocké pour des comparaisons ultérieures.
- *Modèle de correspondance* - Ce modèle est créé au cours de la procédure d'authentification. Le modèle de correspondance est souvent utilisé uniquement à des fins de comparaison et est ensuite supprimé. Toutefois, les systèmes d'apprentissage anticipé enregistrent ces modèles. Ces modèles sont utilisés pour créer un nouveau modèle principal à des fins de comparaison. Ces systèmes apprennent en permanence et s'améliorent au fur et à mesure de l'acquisition d'échantillons.

Le résultat de la phase de traitement du signal est un score de qualité. Ce score indique le degré de réussite du processus d'extraction des caractéristiques. Lors de l'authentification, la phase de traitement du signal renvoie un score de correspondance en même temps que le score de qualité. Le score de correspondance indique le degré de similarité du modèle.

Nous poursuivons avec la troisième composante, la politique de décision, à la page suivante.

2.6.1.3 Volet 3 - Politique décisionnelle

Une fois le traitement du signal terminé, il envoie un score de qualité et/ou de correspondance à la politique de décision. La tâche de la politique de décision est simple : comparer ces scores à un seuil. Si les scores sont supérieurs au seuil, l'utilisateur est accepté, sinon il est rejeté. Bien qu'il puisse sembler s'agir d'une simple décision oui/non, la politique de décision est un élément critique et fait l'objet d'une grande attention de la part des industries commerciales.

Il existe deux seuils. L'un pour la qualité et l'autre pour le score de correspondance. Pour comprendre comment ces seuils sont calculés, nous devons nous familiariser avec les systèmes métriques utilisés dans les systèmes biométriques.

Il existe trois mesures importantes liées aux systèmes biométriques.

- FTER - Taux de non-inscription
- FRR - Taux de faux rejets
- FAR - Taux d'acceptation erronée

2.6.1.3.1 FTER - Taux de non-inscription

L'échec de l'inscription désigne la probabilité que le système ne soit pas en mesure d'extraire des caractéristiques distinctives, cohérentes et reproductibles de l'échantillon présenté au cours de la procédure d'inscription Bubeck et al**.** [16]. L'enregistrement échoue lorsque la phase de traitement du signal ne parvient pas à créer un modèle en raison de la mauvaise qualité de l'échantillon biométrique. L'échantillon de mauvaise qualité peut être influencé par de nombreux facteurs tels que la profession, l'âge, l'appartenance ethnique ou le mode de vie. Le ***FTER*** peut être calculé à l'aide de la formule suivante :

Équation 2-1 Taux de non-inscription

$$FTER = \frac{Nombre\ d'inscriptions\ non\ réussies}{Nombre\ total\ d'inscriptions\ effectuées} \quad \textbf{(2.1)}$$

Lors de l'inscription, la phase de traitement du signal renvoie le score de qualité. Si le score de qualité est supérieur au FTER (seuil de qualité), l'inscription est réussie.

Exemple : Réglage du seuil de qualité

Supposons que nous voulions que notre système rejette éventuellement 10 personnes pour 100 personnes qui s'inscrivent : = 10⁄100 = 0,1

Le seuil de qualité est maintenant fixé à 0,1. Le seuil est toujours compris entre zéro et un. Plus le seuil est proche d'un, plus le système est strict en ce qui concerne la qualité de l'échantillon biométrique. Les personnes inscrites (échantillon biométrique) qui ne répondent pas à ces critères stricts seront rejetées. Ce rejet peut entraîner une insatisfaction du système et une mauvaise expérience pour l'utilisateur. Lors de la définition du FTER, quelques facteurs tels que le trafic, la fréquence, la taille de la population et l'environnement doivent être pris en compte.

2.6.1.3.2 FAR - Taux d'acceptation erronée

Le taux de fausse acceptation, également appelé erreur de type II, est la probabilité que le système fasse correspondre le modèle de vérification d'un utilisateur avec le modèle d'inscription d'un autre utilisateur Bubeck et al. [16]. La plupart des systèmes biométriques tentent de maintenir le FAR aussi bas que possible, de sorte que le système ne permette pas à un imposteur d'entrer dans le système en tant qu'utilisateur légitime. La formule FAR est définie comme suit :

Équation 2-2 Taux de fausse acceptation

$$FAR = \frac{Nombre\ de\ fausses\ reconnaissances}{Nombre\ total\ de\ demandes\ d'authentification} \quad \textbf{(2.2)}$$

2.6.1.3.3 FRR - Taux de faux rejets

Le taux de faux rejet, également appelé erreur de type I, est la probabilité que le modèle de vérification d'un utilisateur ne corresponde pas à son modèle d'inscription Bubeck et al. [16]. Dans ce cas, un utilisateur légitime se voit refuser l'accès au système. Un FRR trop élevé peut entraîner la frustration et l'insatisfaction de l'utilisateur. La formule du FRR est définie comme suit :

Équation 2-3 Taux de faux rejets

$$FRR = \frac{Nombre\ de\ faux\ rejets}{Nombre\ total\ de\ demandes\ d'authentification} \quad \textbf{(2.3)}$$

Le FAR et le FRR sont l'inverse l'un de l'autre. Lorsque vous augmentez votre FAR, le FRR diminue.

Le seuil de correspondance est basé sur le FAR. La définition du FAR est influencée par de nombreux facteurs tels que l'environnement, les utilisateurs et la taille de la population. Dans un environnement hautement sécurisé, le FAR doit être bas, ce qui réduit les chances qu'un imposteur pénètre dans le système. Cependant, nous sacrifions la satisfaction de l'utilisateur puisqu'un plus grand nombre d'utilisateurs seront rejetés.

2.6.1.4 Composant 4 - Stockage

La gestion des modèles est un sujet important. Il faut tenir compte de la conception actuelle et future du système afin de déterminer quelle est la meilleure méthode pour stocker ces gabarits. Prenons l'exemple d'un système biométrique qui stocke ces modèles sur une carte à puce. Le système n'est en mesure d'effectuer qu'une vérification univoque. Le système ne

pourra pas vérifier s'il y a des "doublons" ou procéder à une identification de personne à personne.

Examinons quelques méthodes de stockage courantes dans les systèmes biométriques.

2.6.1.4.1 Stockage local

Les modèles sont stockés sur le dispositif biométrique. Cette méthode de stockage est souvent utilisée pour l'accès physique à un lieu par un petit nombre de personnes en raison des limitations de stockage.

Le stockage local offre une solution robuste et sûre ; il n'est pas sensible aux pannes de réseau ou aux compromis. Toutefois, la gestion des modèles est difficile ; l'inscription, la mise à jour ou la suppression doivent être effectuées sur l'appareil et les modèles ne peuvent pas être partagés entre les appareils.

2.6.1.4.2 Stockage en réseau

Le stockage en réseau offre un référentiel central pour tous les modèles. Les référentiels centraux sont souvent utilisés pour un grand nombre de modèles et éventuellement pour des correspondances entre plusieurs modèles. Grâce à leur grande capacité, des informations supplémentaires peuvent également être stockées, telles que les journaux d'audit qui peuvent aider les administrateurs à déterminer les tentatives d'imposture. La gestion des modèles peut être effectuée à partir d'une seule station, de même que les événements de reprise après sinistre tels que les sauvegardes. Le référentiel central doit résider dans un environnement sécurisé afin d'éviter toute compromission.

2.6.1.4.3 Portable

Les modèles sont stockés sur un dispositif portable tel que les cartes à puce et les dispositifs USB. Du point de vue de l'utilisateur, ce type de stockage est très intéressant, car il protège la vie privée de l'utilisateur ; l'utilisateur peut choisir qui peut avoir accès à ces données. Lorsque cette méthode de stockage est envisagée, les modèles doivent être stockés de manière hautement sécurisée afin d'éviter toute altération non autorisée.

Jusqu'à présent, nous avons couvert une grande partie des informations concernant les systèmes biométriques. La section suivante présente un résumé des informations que nous avons étudiées. Après ce résumé, nous examinerons les différentes caractéristiques biométriques.

2.7 Résumé

Dans les paragraphes 3.1 à 3.6, nous avons couvert l'histoire de la biométrie ainsi que l'importance de l'utilisation de la technologie biométrique. Cependant, la technologie biométrique est confrontée à des défis de la part de la société. Ces défis ont été abordés au point 3.4.

Tous les traits biométriques doivent posséder un ensemble d'attributs. Des attributs tels que l'unicité, l'universalité et la possibilité de collecte constituent un trait biométrique, comme nous l'avons vu au point 3.5.

Ces attributs nous ont amenés à étudier l'architecture d'un système biométrique. Quatre composants essentiels ont été identifiés dans tous les systèmes biométriques.

Ces quatre composantes sont les suivantes

1. ***Acquisition des données -*** Comment le trait biométrique est-il capturé ?
2. ***Traitement du signal -*** Comment les caractéristiques biométriques sont-elles extraites ?
3. ***Politique de décision -*** Utilisée pour déterminer si l'échantillon biométrique est acceptable pour l'inscription ou si deux gabarits biométriques répondent à l'exigence de concordance.
4. ***Stockage -*** Comment le gabarit biométrique est-il stocké en vue de correspondances ultérieures ?

Chacune de ces quatre composantes a été explorée pour révéler ses sous-composantes, qui sont utilisées pour accomplir leur tâche.

La section suivante (3.8) explore les différents traits biométriques, à savoir les empreintes digitales, la voix et la reconnaissance de l'iris. Chaque caractéristique biométrique sera étudiée en termes de fonctionnalité, de matériel utilisé, ainsi que de forces et de faiblesses.

2.7 Résumé

Dans les paragraphes 3.1 à 3.6, nous avons couvert l'histoire de la biométrie ainsi que l'importance de l'utilisation de la technologie biométrique. Cependant, la technologie biométrique est confrontée à des défis de la part de la société. Ces défis ont été abordés au point 3.4.

Tous les traits biométriques doivent posséder un ensemble d'attributs. Des attributs tels que l'unicité, l'universalité et la possibilité de collecte constituent un trait biométrique, comme nous l'avons vu au point 3.5.

Ces attributs nous ont amenés à étudier l'architecture d'un système biométrique. Quatre composants essentiels ont été identifiés dans tous les systèmes biométriques.

Ces quatre composantes sont les suivantes

1. ***Acquisition des données -*** Comment le trait biométrique est-il capturé ?
2. ***Traitement du signal -*** Comment les caractéristiques biométriques sont-elles extraites ?
3. ***Politique de décision -*** Utilisée pour déterminer si l'échantillon biométrique est acceptable pour l'inscription ou si deux gabarits biométriques répondent à l'exigence de concordance.
4. ***Stockage -*** Comment le gabarit biométrique est-il stocké en vue de correspondances ultérieures ?

Chacune de ces quatre composantes a été explorée pour révéler ses sous-composantes, qui sont utilisées pour accomplir leur tâche.

La section suivante (3.8) explore les différents traits biométriques, à savoir les empreintes digitales, la voix et la reconnaissance de l'iris. Chaque caractéristique biométrique sera étudiée en termes de fonctionnalité, de matériel utilisé, ainsi que de forces et de faiblesses.

Chapitre III :
Traits biométriques

La plupart des gens pensent d'abord aux empreintes digitales lorsqu'ils prononcent le mot "biométrie". La reconnaissance des empreintes digitales est la caractéristique biométrique la plus ancienne et la plus largement utilisée. Cette large adoption et mise en œuvre de la biométrie des empreintes digitales fait que la plupart des gens associent la biométrie à la reconnaissance des empreintes digitales.

La reconnaissance des empreintes digitales est l'une des nombreuses caractéristiques biométriques existantes. Les êtres humains peuvent être identifiés par leurs doigts, leurs mains, leurs yeux ou même leur voix. Ces caractéristiques biométriques peuvent être classées en biométries physiques, comportementales et ésotériques.

La biométrie physique est basée sur des attributs physiques uniques de l'anatomie humaine. Les empreintes digitales, l'iris et la reconnaissance faciale entrent dans cette catégorie.

Biométrie comportementale - il s'agit de caractéristiques biométriques qui sont apprises ou développées au fil du temps, comme les signatures ou la voix.

La biométrie ésotérique est une nouvelle biométrie émergente qui en est encore au stade expérimental. Les données biométriques telles que l'ADN, la reconnaissance de l'oreille et de la démarche sont des données biométriques ésotériques.

Cette section du chapitre est consacrée à l'étude des caractéristiques biométriques de chaque catégorie.

3.1 Reconnaissance des empreintes digitales

La biométrie des empreintes digitales est basée sur les motifs que l'on trouve à l'extrémité de chaque doigt. Ces motifs, souvent appelés empreintes digitales, se développent au cours des stades fœtaux de l'anatomie humaine. Il n'existe pas deux empreintes digitales identiques, même chez les vrais jumeaux.

Les empreintes digitales sont composées de multiples crêtes et sillons. Les crêtes sont la partie haute de la peau de frottement, tandis que les sillons sont la partie basse et peu profonde de la peau de frottement.

Le caractère unique de chaque empreinte digitale est déterminé par les motifs formés par les crêtes et les sillons, ainsi que par les points caractéristiques. Les points caractéristiques sont des caractéristiques locales des crêtes qui apparaissent lorsqu'une crête se divise (bifurcation) ou se termine [1]. Ces points de minutie sont utilisés pour créer le modèle biométrique à des fins de comparaison.

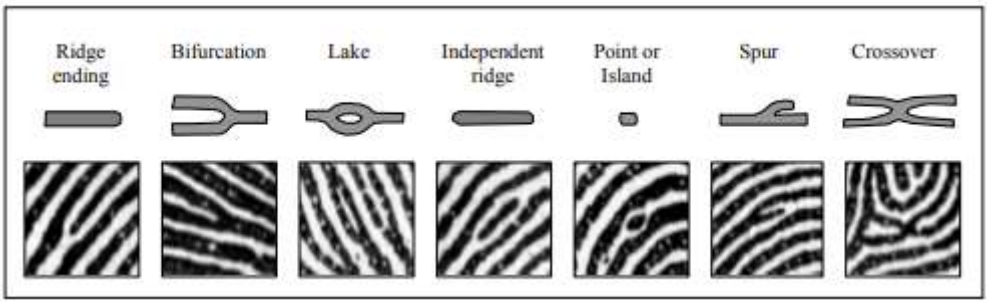


Figure 3-1 : Les sept types de points caractéristiques de l'empreinte digitale [1].

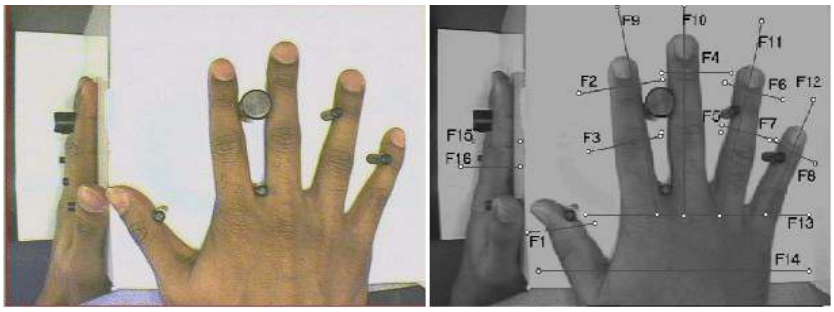
Les empreintes digitales sont considérées comme uniques en raison de leurs points caractéristiques. Les points caractéristiques sont souvent des points où les crêtes sont interrompues. Les extrémités des crêtes et les bifurcations sont deux points caractéristiques courants.

3.2 Géométrie de la main

La reconnaissance de la géométrie de la main est basée sur l'extraction des mesures de plusieurs caractéristiques clés de la main humaine. L'idée principale de la géométrie de la main est conceptualisée à partir du système Bertillon où les mesures des parties du corps étaient utilisées pour identifier les personnes. La longueur, la largeur et la surface de la main sont quelques-unes des mesures prises au cours du processus de reconnaissance.

Les scanners de géométrie de la main se composent d'une caméra CCD (dispositif à couplage chargé), d'une source lumineuse, d'un miroir unique et d'une surface plane avec des piquets. Les chevilles sur la surface sont utilisées comme points de contrôle pour assurer un placement approprié de la main. Au cours du processus de capture, une image tridimensionnelle (3D) de la main est prise. L'image 3D est utilisée pour déterminer l'épaisseur de la main. Cet effet 3D est obtenu grâce à l'utilisation d'un seul miroir. La figure 3-2 (a) montre l'image du miroir pour créer l'effet 3D.

Au cours du processus de capture, la première image est prise du dessus, ce qui permet de capturer la partie supérieure de la main. La deuxième image utilise le miroir pour obtenir une image latérale de la main.



(a) (b)

Figure 3-2 : Scanner de géométrie de la main

La figure "a" comprend l'image du miroir. Le miroir est utilisé pour capturer une image 3D de la main, qui est utilisée pour mesurer l'épaisseur de la main.

La figure "b" illustre les seize axes le long desquels les valeurs des caractéristiques sont calculées. Ces axes ne servent de points de calcul des mesures (+/-) 90.

Une fois ces images obtenues, le système prend pas moins de 90 mesures de la main. Ces mesures comprennent la longueur des doigts, la distance entre les articulations, la hauteur de la main et de chaque doigt, ainsi que la surface de la paume. La figure 3-2 (b) montre les mesures qui sont prises.

Ces mesures sont utilisées pour créer le modèle biométrique en vue d'une comparaison ultérieure. En moyenne, le gabarit biométrique a une capacité de neuf (9) octets, ce qui en fait une solution intéressante pour les dispositifs de stockage limités tels que les cartes à puce.

Les systèmes de géométrie de la main utilisent principalement des images noir et blanc (binaires) de la main. En utilisant ces modèles binaires, le système peut ignorer les détails de la surface tels que les empreintes digitales, les lignes, les cicatrices, la couleur et même les tatouages. Bien que l'image binaire ait fait ses preuves, des recherches ont été menées sur des systèmes utilisant des images en couleur.

L'approche de Golfarelli [2] suggère d'utiliser la couleur bleue de la surface du scanner. La surface bleue permet une segmentation. Anil Jain, l'un des auteurs de l'Encyclopédie de la biométrie [2] explique que "la peau humaine, quelle que soit la race, a une très faible part de composante bleue.

L'élimination de la composante bleue dans le modèle de couleur rouge, vert et bleu (RVB) permet d'éliminer facilement toutes les informations d'arrière-plan.

La plupart des scanners de géométrie de la main utilisent des chevilles comme points de contrôle. Toutefois, les systèmes sophistiqués demandent à l'utilisateur de presser ses doigts contre les chevilles pour confirmer que la main est "vivante" et non fausse NBSP [3]. Ce type de détection de la vivacité est utilisé pour empêcher l'usurpation du scanner. Chen al. [4] a démontré deux méthodes qui peuvent être utilisées pour falsifier un scanner de géométrie de la main sans détection de la vivacité. La première méthode utilise du plâtre pour fabriquer de fausses mains (voir figure 3-3 (a)) tandis que la seconde méthode fabrique une fausse main à partir d'images de silhouettes capturées par le scanner (voir figure 3-3 (b)). Les deux méthodes ont démontré avec succès comment un système de géométrie de la main peut être falsifié.

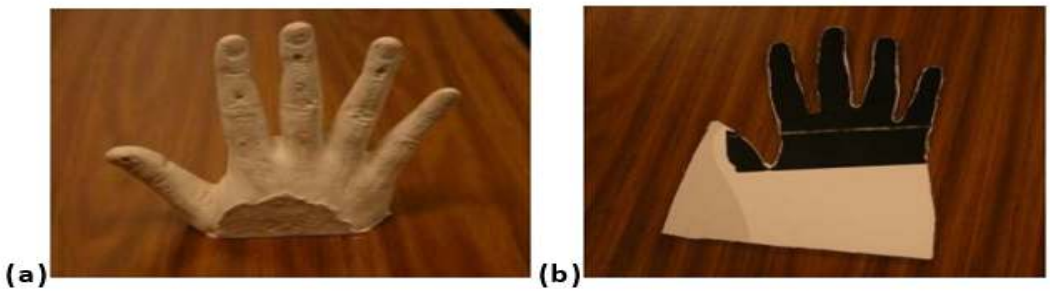


Figure 3-3 : Fausses mains utilisées pour tromper les scanners de géométrie de la main [4]

Fausses mains créées par Chen et al. [4] qui ont été utilisées avec succès pour usurper le système. Figure "a" - Fausse main en plâtre. Figure "b" - Fausse main sur papier 2D, réalisée à partir des images obtenues par le scanner de géométrie de la main.

Bien que les chevilles existent dans la plupart des systèmes, elles ne sont pas obligatoires dans les systèmes à géométrie manuelle. Des recherches ont été menées sur les systèmes sans piquets Govindaraju et al. [5]. Ces systèmes utilisent le poignet comme point de départ, ce qui permet de localiser les extrémités des doigts et les points de la vallée.

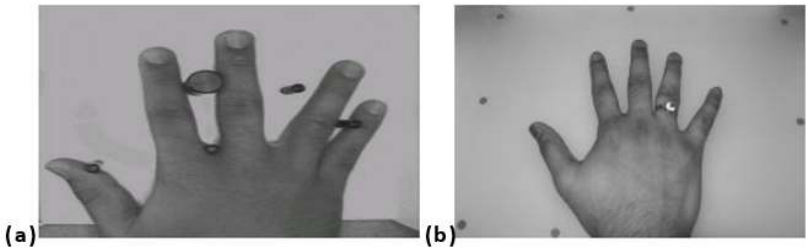


Figure 3-4 : Scanner à cheville ou sans cheville [5]

La figure "a" illustre un scanner de géométrie de la main qui utilise des chevilles pour positionner la main, tandis que la figure "b" illustre un scanner sans chevilles.

Examinons le processus d'inscription des systèmes de géométrie de la main. Comme indiqué au début de cette sous-section, les systèmes de géométrie de la main prennent une image en 3D de la main en prenant deux photos, l'une du dessus de la main et l'autre du côté de la main. Au cours de la procédure d'inscription, le système prend trois clichés de chacune de ces deux photos. Bien que ce processus dépende du système, il dure généralement entre 30 secondes et 1 minute. La géométrie de la main est suffisamment distincte pour la vérification (un pour un), mais pas assez pour l'identification.

Les bagues, les gants et même les bandages peuvent entraîner de fausses acceptations ou de faux rejets. Toutefois, certains systèmes ignorent la zone de l'anneau ainsi que les ongles (longs ou courts) afin d'éviter ces fausses acceptations ou rejets. Si un utilisateur ne peut pas utiliser sa main droite pour la vérification, sa main gauche (si elle est enregistrée) doit être retournée, car la plupart des systèmes sont conçus pour utiliser uniquement la main droite.

Ruud Bolle et al. [6] a souligné que la plupart des systèmes de géométrie de la main doivent apprendre les changements mineurs de la forme de la main et mettre à jour en permanence le modèle de vérification. À la naissance, les mains humaines sont symétriques. Au fur et à mesure que le corps vieillit, les mains changent de forme en raison des conditions naturelles et environnementales. Les personnes deviennent gauchères ou droitières, ce qui fait qu'une main est plus grande que l'autre. La main "préférée" a tendance à être plus susceptible de se blesser lors d'activités sportives ou professionnelles.

Les mains d'une jeune personne changent rapidement à mesure qu'elle mûrit, tandis que celles d'une personne âgée changent avec le processus naturel de vieillissement ou l'arthrite. Une perte ou un gain de poids extrême peut également avoir une influence sur le système.

Les systèmes de géométrie manuelle améliorent la sécurité, la précision et la commodité. Ces systèmes sont souvent utilisés dans les zones de contrôle d'accès à faible niveau de sécurité, dans les systèmes de gestion du temps et des présences ou dans la surveillance des ressources.

La mise en œuvre la plus remarquable d'un système de géométrie de la main se trouve à Disney World à Orlando, en Floride Woodward et al. [7]. Ce système biométrique a été mis en place pour résoudre le problème des billets promotionnels. Disney a permis aux visiteurs

d'acheter des billets promotionnels en réalisant des économies considérables par rapport au coût des cartes journalières. Ces billets pouvaient être utilisés de manière interchangeable par les amis et la famille. Les voyagistes ont découvert cette vulnérabilité, ce qui les a amenés à acheter ces billets et à les délivrer pour une seule journée et à empocher le prix de la journée. Disney a choisi de mettre en œuvre la biométrie à géométrie de la main parce qu'elle pouvait être utilisée rapidement et sans formation.

3.3 Reconnaissance de l'iris

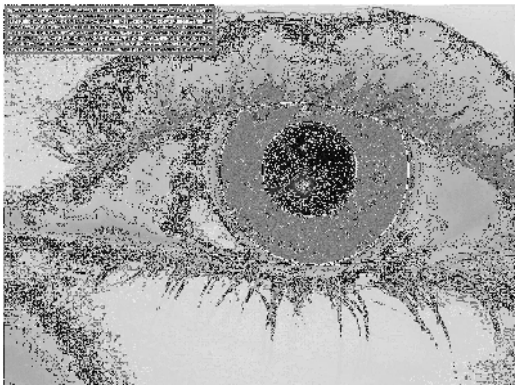


Figure 3-5 : Isolement d'un iris en vue de son codage et "IrisCode" qui en résulte [8]

L'iris, tel que défini par Anil Jain et al. [22], est l'anneau coloré qui entoure la pupille. Chaque iris est constituée de motifs de texture complexes avec de nombreux attributs tels que des rayures, des piqûres et des sillons. L'iris, qui se développe au cours de la croissance prénatale, est responsable de la régulation de la taille de la pupille, contrôlant ainsi la quantité de lumière pénétrant dans l'œil.

Bien que la coloration et la structure de chaque iris soient génétiquement liées, les détails des motifs de l'iris ne le sont pas. Les iris sont uniques pour chaque individu, même chez les vrais jumeaux. Les iris gauche et droit sont différentes. L'iris est un organe interne bien protégé, difficile à usurper chirurgicalement. Selon les recherches, l'iris est extrêmement stable tout au long de la vie d'une personne, sauf en cas de traumatisme ou de blessure.

Les scanners d'iris utilisent une caméra CCD (diode à couple chargé) avec un imageur infrarouge pour éclairer l'œil et capturer une image haute résolution en noir et blanc. "L'image sera utilisée pour identifier plus de 200 caractéristiques uniques qui donnent l'impression de diviser l'iris de manière radiale, des anneaux, des sillons, des taches de rousseur et des couronnes « (Bohm et al). Ces 200 caractéristiques sont utilisées pour créer le modèle d'iris d'environ 512 octets.

Figure 3-6 : Iris utilisé pour l'identification [8]

Figure "a" - Image de l'iris capturée à l'aide d'un scanner d'iris. Le cercle blanc autour de l'iris est l'iris localisé utilisé lors du processus de segmentation. Figure "b" - Structure de l'iris composée de plus de 200 points.

La reconnaissance de l'iris est généralement mise en œuvre dans un environnement contrôlé - la luminosité de l'environnement doit être contrôlée pour obtenir des résultats corrects. Pendant le processus de capture, l'utilisateur doit se tenir à une distance de 3 à 10 pouces de la caméra et regarder directement dans l'objectif. La plupart des scanners de l'iris exigent un positionnement précis de l'œil et, pour cette raison, la reconnaissance de l'iris présente le taux le plus élevé d'échec à l'inscription (FTER). L'utilisation de lunettes et de lentilles de contact sans motif est autorisée pendant le processus de capture.

Ces craintes doivent être prises en compte lors de la mise en œuvre d'un système de reconnaissance de l'iris afin que le marché cible accepte le système.

La reconnaissance de l'iris est souvent utilisée dans des environnements hautement sécurisés. Les applications suivantes ont mis en œuvre avec succès la reconnaissance de l'iris.

- L'aéroport international de Charlotte-Douglas utilise la reconnaissance de l'iris pour l'accès physique des travailleurs aux zones non publiques de l'aéroport NBSP [10], Woodward et al. [7].

- Lors des Jeux olympiques d'hiver de Nagano, au Japon, un système de reconnaissance de l'iris a été mis en place pour restreindre l'accès aux fusils utilisés dans le biathlon [10].

- Les Émirats arabes unis utilisent la reconnaissance de l'iris depuis plus d'une vingtaine d'années pour contrôler les nouveaux détenteurs de visas. Ce système vise à détecter les personnes précédemment expulsées NBSP [10], Gregory et al. [11].

- Les Nations unies utilisent la reconnaissance de l'iris pour le contrôle des réfugiés [10].

• Le Child Project aux États-Unis est un système basé sur l'iris utilisé pour identifier et ramener les enfants disparus.

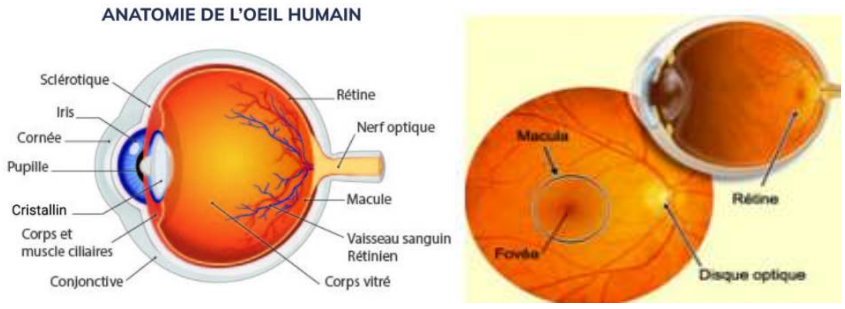
3.4 Reconnaissance de la rétine

La reconnaissance de la rétine est basée sur des motifs vasculaires uniques situés à l'arrière de l'œil. La rétine est la couche de cellules nerveuses située à l'arrière du globe oculaire qui sert d'écran de projection pour les images passant par la cornée, l'iris et le cristallin. La figure 3-12 (a) montre l'emplacement de la rétine dans l'œil.

Ces nerfs sont reliés (via les nerfs optiques) au cerveau et transmettent les informations que le cerveau interprète comme étant la vision.

On pense que les motifs du réseau vasculaire de la rétine sont créés par un processus biologique aléatoire. La rétine est unique d'une personne à l'autre, même chez les vrais jumeaux, et elle est stable tout au long de la vie.

Le balayage de la rétine est réalisé en éclairant la rétine avec une lumière infrarouge de faible intensité diffusée à travers l'ouverture pupillaire et en visualisant les motifs vasculaires formés à travers le cercle de balayage de la région annulaire. La figure 3-7 illustre une rétine capturée.



(a) (b)

Figure 3-7 : Reconnaissance de la rétine

L'image "a" est une représentation visuelle de l'anatomie d'un œil. L'image montre l'emplacement de la rétine dans l'œil. L'image "b" est une capture de l'anatomie de la rétine à l'aide d'une caméra infrarouge.

Pendant le processus de balayage, l'utilisateur doit aligner un œil sur l'objectif, à une distance d'environ 2 à 3 pouces du scanner. L'usager doit rester immobile pendant 1 à 2 secondes nécessaires à l'éclairage, à la mise au point et à la capture d'une image rétinienne. Lorsque

l'utilisateur aligne son œil sur la lentille, il remarque une lumière verte intégrée à la lentille de l'appareil de balayage.

Une fois que le processus de balayage a commencé, cette lumière verte se déplace sur un cercle complet de 360 degrés, capturant des images des vaisseaux sanguins de la rétine à travers la pupille. Comme la rétine n'est capturée qu'à travers la pupille, seule une partie de la rétine est capturée. La figure 3-8 illustre la partie de la rétine qui est capturée.

Ce processus capture généralement 3 à 5 images de la rétine et dure plus d'une minute.

Comparé à d'autres techniques biométriques, ce délai est long. Une fois terminée, l'image circulaire est convertie en une structure linéaire similaire à un code-barres (Woodward et al. [13] pour créer un modèle de 96 octets. Ces modèles contiennent souvent jusqu'à 400 points uniques trouvés sur la rétine, contre 30 à 40 pour les empreintes digitales.

Figure 3-8 : Zone de balayage pour la capture de la rétine

Les motifs de la rétine existent dans l'ensemble de l'œil, mais seuls les motifs formés dans la zone de balayage sont capturés par le scanner à travers la pupille Jain et al. [9].

La rétine étant un organe interne protégé, elle est moins susceptible de changer d'environnement, d'être modifiée ou défigurée par la chirurgie. Les scanners de la rétine sont assez difficiles à falsifier à l'aide d'un faux œil, car ils s'appuient sur le sang qui existe dans le réseau vasculaire. Contrairement à d'autres systèmes biométriques tels que la reconnaissance faciale, la reconnaissance de la rétine ne peut être utilisée qu'au moment et à l'endroit choisis par l'utilisateur. La reconnaissance de la rétine est souvent considérée comme l'un des systèmes biométriques les plus performants, offrant des taux de réussite proches de zéro et des correspondances positives très concluantes. Toutefois, les faux rejets peuvent être assez fréquents, mais ils sont dus à la méconnaissance du système ou à des problèmes d'alignement des yeux.

L'un des principaux problèmes liés à la reconnaissance de la rétine est l'inconvénient et la nature intrusive du système. Le processus de balayage exige que l'œil de l'utilisateur soit à une distance de 2 à 3 pouces de la lentille et que l'utilisateur reste immobile pendant une minute - tout mouvement peut entraîner de faux rejets ou des problèmes d'inscription. Les utilisateurs doivent faire preuve d'un grand respect et d'une grande coopération pour utiliser le système.

Le système de reconnaissance de la rétine ne fonctionne pas bien avec des lunettes qui doivent être enlevées, car le verre peut créer des reflets indésirables. Les blessures et les maladies (telles que le glaucome et le diabète) peuvent affecter le processus de reconnaissance et nécessiter un réenregistrement.

Les systèmes de reconnaissance rétinienne sont souvent utilisés dans des environnements de haute sécurité, généralement pour le contrôle d'accès, l'entrée de sécurité ou même l'accès aux portes. Les scanners sont souvent déployés en tant qu'unité murale.

3.5 Reconnaissance de la signature

La reconnaissance de signature est utilisée pour mesurer des caractéristiques comportementales, souvent apprises au fil du temps. La reconnaissance de signature mesure la manière dont un client produit sa signature, qui est principalement utilisée lors de la vérification (comparaison un à un).

Divers facteurs sont pris en considération lors de l'analyse de la signature, notamment les caractéristiques de la signature elle-même (le produit statique) et la manière dont la signature est créée (le produit dynamique).

Le processus dynamique analyse une série de mouvements qui contiennent des données biométriques uniques telles que les rythmes personnels, l'accélération et le déroulement du processus Motorola, 2006 [12].
Les tablettes numériques et les PDA sont utilisés avec un stylet pour capturer la signature. Les écrans tactiles modernes sont de plus en plus souvent utilisés sans stylet, comme la signature d'un iPhone (voir figure 3-9).

Figure 3-9 : Signature effectuée sur un écran tactile

La signature elle-même (produit statique) fournit des informations sur la géométrie, la courbure et la forme qui sont utilisées pour le processus de reconnaissance. La falsification étant un problème majeur dans les produits de reconnaissance de signature, la signature statique ne peut être utilisée seule pour l'identification. Le processus dynamique fournit des détails uniques sur la manière dont la signature a été générée et est pratiquement impossible à reproduire. La direction du trait, la vitesse, la montée et la descente du stylo, ainsi que la pression sont mesurées au cours du processus dynamique. La figure 3-10 illustre les différentes mesures effectuées au cours du processus dynamique.

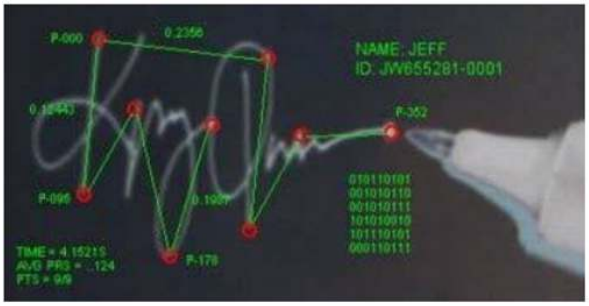


Figure 3-10 : Processus de signature dynamique

Diverses mesures prises lors de la création de la signature (processus dynamique) Gupta et Rick Joyce ont réalisé une série d'expériences afin de détecter les falsifications dans le processus de reconnaissance des signatures Woodward et al. [7] p105, ils ont relevé six caractéristiques au cours du processus dynamique. Ces caractéristiques sont les suivantes :

1. Temps total ;
2. Nombre de changements de signe de la vitesse dans la direction x ;
3. Nombre de changements de signe de la vitesse dans la direction y ;
4. Nombre de changements de signe d'accélération dans la direction x ;
5. Nombre de changements de signe d'accélération dans la direction y ;

6. Temps total d'écriture

L'expérience a fait appel à des professionnels qui pratiquent la falsification. Gupta et Rick ont noté que les faussaires étaient capables de reproduire la signature statique, mais que cela n'avait aucune incidence sur la façon de reproduire la manière dont la signature avait été produite.

L'un des avantages des produits de reconnaissance de signature est qu'ils sont conviviaux et non invasifs. De nombreuses personnes sont déjà habituées à apposer leur signature pour autoriser des transactions. Il n'y a donc pratiquement aucun problème de respect de la vie privée. Cet avantage permet également d'utiliser les produits de reconnaissance de signature partout où des signatures conventionnelles sont utilisées. Le remplacement des signatures à base d'encre peut réduire la fraude et les abus dans les applications de commerce électronique.

Les systèmes avancés de reconnaissance de signature sont dotés d'une fonction d'apprentissage pour tenir compte des changements naturels ou des dérives qui se produisent dans la signature d'un individu au fil du temps.

Bien que les produits de reconnaissance de signature soient faciles à utiliser et peu invasifs, la reconnaissance de signature ne s'est pas imposée sur le marché, contrairement à la biométrie par empreintes digitales.

Les caractéristiques physiques de l'équipement de signature peuvent affecter la robustesse et les performances de ces systèmes. Le poids, le diamètre et le frottement de la surface du stylet peuvent influencer la manière dont une signature est créée.

La fatigue et les circonstances psychologiques sont des facteurs humains qui jouent un rôle dans la répétabilité. Les individus ont tendance à être plus prudents et conscients lorsqu'ils signent des documents importants tels que des prêts immobiliers. En revanche, les documents ordinaires et ennuyeux, tels que les factures, sont signés à la hâte. Des difficultés surviennent également lorsque la signature de l'utilisateur change substantiellement à chaque fois.

Les algorithmes utilisés pour la création de modèles imposent des limites à la longueur de la signature. Les signatures ne peuvent être ni trop longues ni trop courtes. Lorsqu'une signature longue est présentée, trop de données comportementales sont capturées, ce qui rend difficile l'identification de points de données cohérents et uniques. Les signatures trop courtes ne fournissent pas suffisamment de données, ce qui peut entraîner une augmentation du nombre de FAR.

Les questions d'environnement jouent un rôle important. Les mêmes conditions d'environnement doivent être utilisées pour l'inscription et la vérification. Si l'utilisateur a été inscrit alors qu'il était debout, il doit être vérifié alors qu'il était debout. Les modèles d'inscription et de vérification tendent à être sensiblement différents si les conditions ne sont pas les mêmes. Les utilisateurs peuvent également avoir des difficultés à s'habituer à l'utilisation d'une table de signature.

La reconnaissance de signature peut être utilisée dans de nombreuses situations, qu'il s'agisse de l'ouverture d'une session informatique, de l'accès aux données, de la vérification des cartes de crédit ou de diverses applications POS (point de vente). L'utilisation la plus notable de la reconnaissance de signature est celle de la Chase Manhattan Bank, la première banque connue à avoir adopté la technologie de vérification de signature.

3.6 Résumé

Ce chapitre a étudié le domaine de la biométrie. Depuis des milliers d'années, l'homme utilise les caractéristiques uniques du corps humain pour s'identifier. L'identification des individus par leurs parties du corps est inscrite dans notre ADN. En tant qu'êtres humains, nous utilisons les structures faciales pour nous identifier les uns les autres. L'utilisation de la biométrie comme forme d'identification présente de nombreux avantages. Les individus n'ont plus à se souvenir de mots de passe complexes ou à porter des jetons tels que des cartes à puce. Pour les administrations, la biométrie offre une sécurité accrue, empêche le partage des mots de passe ou la fraude.

Toutefois, pour qu'un système biométrique soit efficace, l'utilisateur final doit accepter le fait que ses caractéristiques physiques puissent être utilisées pour l'identifier. Toute question relative à la protection de la vie privée doit être abordée avec les utilisateurs finaux. D'autres problèmes liés à la biométrie peuvent découler d'un manque de connaissance du système ; des problèmes tels que des dommages physiques ou l'utilisation de données biométriques à des fins autres que celles prévues à l'origine. Bien que la biométrie soit une méthode d'identification sûre, le système développé doit empêcher l'entrée de données biométriques falsifiées.

Le corps humain possède de nombreuses caractéristiques, mais toutes ne peuvent pas être utilisées pour une identification unique. Pour qu'une caractéristique soit considérée comme un identifiant biométrique, elle doit présenter les attributs suivants : robustesse, unicité, collectabilité, performance, précision et acceptabilité.

Quel que soit le trait biométrique utilisé dans un système (empreinte digitale/iris), chaque système biométrique se compose de quatre étapes utilisées au cours du processus d'identification : l'acquisition des données, le traitement du signal, la politique de décision et le stockage. L'étape d'acquisition des données permet d'obtenir le trait biométrique sous forme numérique, comme l'image d'une empreinte digitale. L'étape suivante, le traitement du signal, permet de trouver les caractéristiques biométriques et de supprimer toutes les données indésirables. Une fois les caractéristiques biométriques trouvées, des attributs uniques sont extraits. Ces attributs sont utilisés pour créer une représentation mathématique de la caractéristique biométrique, appelée modèle biométrique.

Avec le modèle, le système produit deux scores de performance : la qualité et la correspondance. Le score de qualité est utilisé pour déterminer si la phase de traitement du signal a trouvé suffisamment d'attributs uniques dans la biométrie, tandis que le score de correspondance est utilisé pour comparer deux modèles biométriques. Le score de correspondance indique dans quelle mesure les modèles sont identiques l'un à l'autre. Si l'un de ces scores est inférieur au seuil.

Chapitre V :
Les outils et techniques utilisés

Dans ce chapitre, nous exposerons les méthodes et les outils de bases adoptés dans notre système biométrique proposé.

5.1 Extraction des caractéristiques des veines du doigt

5.1.1 Basée sur la quantification de la phase locale [1]

La quantification de phase locale est un opérateur de description de texture locale dans le domaine des fréquences. La quantification de phase locale fonctionne sur la base de la transformée de Fourier à court terme et présente l'avantage d'être invariante en cas de changement d'illumination. L'image floue spatiale $g(x)$ peut être exprimée par une convolution de l'image originale $f(x)$ avec la fonction d'étalement du point □(x) du flou, qui peut être exprimée comme suit **[2]** :

$$g(x) = f(x) * □(x) \quad (1)$$

Sa représentation dans le domaine des fréquences est l'expression de Fourier :

$$G(u) = F(u) \cdot H(u) \quad (2)$$

La relation correspondante de l'angle de phase est exprimée comme suit :

$$\angle G(u) = \angle F(u) + \angle H(u) \quad (3)$$

Si nous supposons que la fonction d'étalement du point h(x) est centralement symétrique, c'est-à-dire que h(x)=h(-x), la transformée de Fourier H(u) sera toujours une valeur réelle. Les fonctions gaussiennes ou Sinc approximatives doivent être sélectionnées de manière à ce que H(u) soit positive sur toutes les bandes de fréquence.

Étant donné que les caractéristiques de la texture sont locales plutôt que globales, le descripteur correspondant doit également être en mesure de décrire ces caractéristiques locales. Ainsi, au lieu de calculer la transformée de Fourier de l'image entière, nous estimons la transformée de Fourier de chaque image locale. Pour l'image originale, nous utilisons la transformée de Fourier à court terme pour transformer chaque pixel de la région de voisinage

N_λ de taille $M \times M$

$$F(u, x) = \sum_{y \in N_x} f(x - y) e^{-j2\pi u^T y} = W_u^T f_x \quad (4)$$

Où u représente la fréquence et fx est le vecteur composé de tous les pixels de Nλ. Wu est le vecteur de base en u dans la transformée de Fourier à court terme. Quatre sous-ensembles de points de fréquence sont considérés pour calculer les coefficients de Fourier locaux dans LPQ : u1 = [a,0] ^{T}, u2 = [0, a] ^{T}, u3 = [a, a] ^{T}, u4 = [a, -a] ^{T}. Le scalaire a est généralement évalué sur une petite plage de sorte que H(ui) soit toujours positif. La valeur de a couramment utilisée est 1/M **[3]**. Chaque pixel de l'image est représenté par un vecteur comme suit :

$$F_x = [F(u_1, x), F(u_2, x), F(u_3, x), F(u_4, x)] \quad (5)$$

Fx est un vecteur complexe dans le domaine des fréquences, et les parties réelles et imaginaires de chaque composante peuvent être marquées comme suit :

$$G(x) = [R_e\{F_x\}, Im\{F_x\}] \quad (6)$$

Des informations texturales insensibles au flou peuvent alors être obtenues en fonction de la valeur de G(x) comme suit **[4]** :

$$f_{LPO}(x) = \sum_{j=0} q_j 2^j \quad (7)$$

où la plage de j est comprise entre 0 et 7. $f_{LPO}(x)$ est la valeur LPQ de la fenêtre W × W. q_j est la $j^{ième}$ composante de $G(x)$, donnée par :

$$q_i = \begin{cases} 1 & G_j \geq 0 \\ 0 & G_j < 0 \end{cases} \quad (8)$$

La figure 1 présente une procédure de calcul du protocole de représentation LPQ. Les valeurs résultantes peuvent être directement encodées pour produire l'image LPQ, et la figure 2 présente une description d'images de veines digitales à l'aide de LPQ.

Les vecteurs de caractéristiques obtenus par l'opérateur LPQ sont présentés sous la forme d'un histogramme statistique, qui ignore souvent les informations de structure intrinsèque de l'image. Afin de remédier à ce défaut, nous utilisons la méthode des blocs pour diviser l'imageoriginale en M sous- régions S0, S1, ..., SM-1 qui ne se chevauchent pas et sont de même taille, et nous appliquons l'opérateur LPQ pour extraire les caractéristiques de la texture des veines dans chaque bloc d'image. L'histogramme de l'opérateur LPQ dans la sous-image est exprimé comme suit :

$$H_L(j) = \left[H_L^0(j), H_L^1(j) \cdots, H_L^{255}(j)\right] | H_L^i(j) = \sum_{x,y \in S_j} B\left(f_{LPQ}(x, y) = i\right) \quad (9)$$

où $j \in [0, M-1]$ *et* $B(y)$ *est un indicateur booléen*:

$$B(y) = \begin{cases} 1 & lorque \ \ y \ est \ vrai \\ 0 & Sinon \end{cases} \quad (10)$$

Enfin, les histogrammes précédents de tous les sous-blocs d'image sont concaténés pour former l'histogramme LPQ final. La figure 3 présente une procédure simplifiée d'extraction de la caractéristique LPQ pour une image de veine digitale.

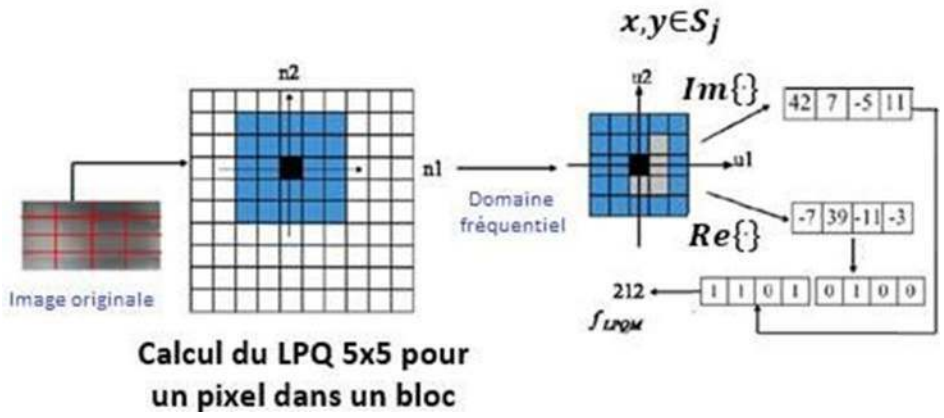


Figure 5-1 : Une illustration du calcul LPQ **[1]**

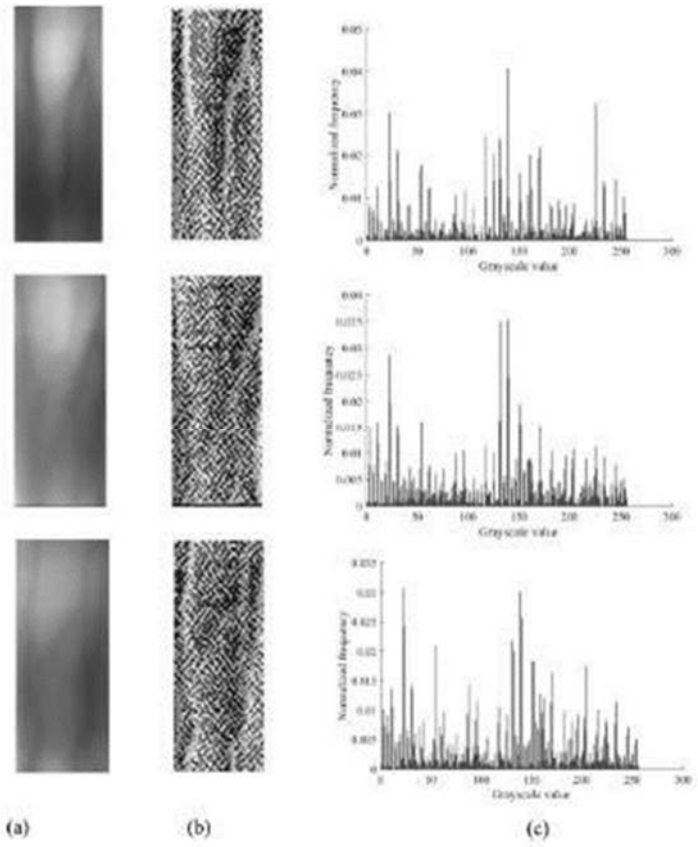


Figure 5-2 : La présentation de quelques images de veines de doigts à l'aide de la technique LPQ et de l'histogramme correspondant (a) images ROI (b) images LPQ (c) histogramme de la caractéristique LPQ **[1]**

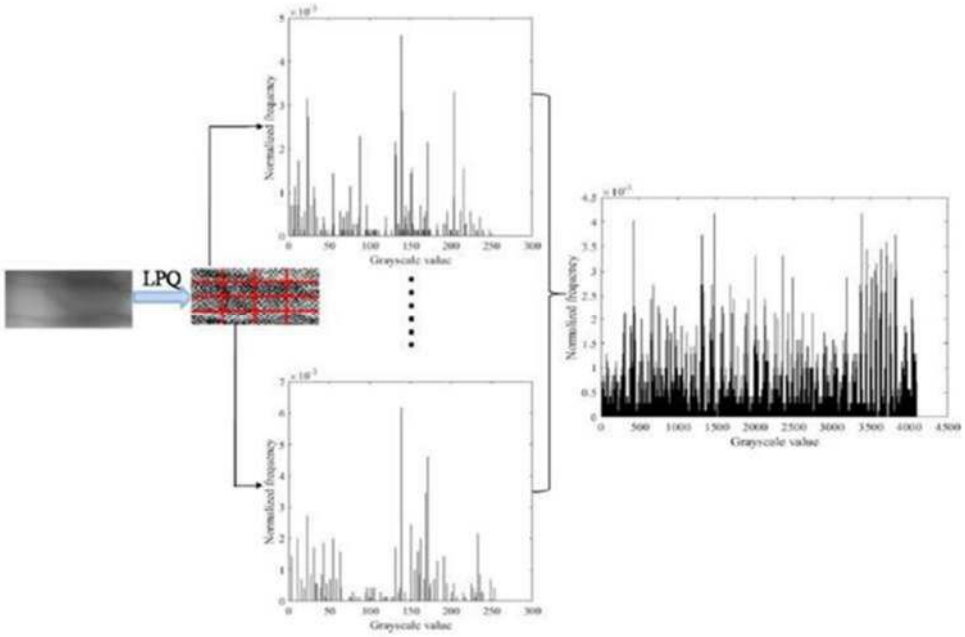


Figure 5-3 : La procédure simplifiée d'extraction de la caractéristique LPQ d'une image de veine de doigt **[1]**

5.2 Apprentissage

Cette phase implique l'intégration des individus dans le système, ce qui requiert la sauvegarde des paramètres extraits dans une base de données bien organisée pour faciliter la reconnaissance et les prises de décision futures. En quelque sorte, il s'agit de la mémoire du système. Il est possible de distinguer deux types d'apprentissage : l'apprentissage supervisé et l'apprentissage non supervisé.

5.2.1 Apprentissage supervisé

L'apprentissage supervisé constitue une subdivision de l'apprentissage automatique et de l'intelligence artificielle. Il se caractérise par l'utilisation de ensembles de données annotés pour entraîner des algorithmes permettant de classifier les données ou de prédire les résultats avec précision. Le but est d'attribuer une signification aux données en fonction d'une question particulière. L'apprentissage supervisé est couramment appliqué pour résoudre des problèmes de classification et de régression, tels que l'identification de la catégorie d'un article de presse ou la prédiction du chiffre d'affaires pour une date ultérieure **[5].**

5.2.2 Apprentissage non supervisé

Les algorithmes d'apprentissage automatique non supervisés sont déployés dans des cas où les données d'entraînement ne sont ni catégorisées ni annotées. Le modèle en question analyse les données d'apprentissage afin d'inférer une fonction permettant de décrire une structure cachée

à partir de ces données. Le système ne parvient jamais à déterminer la sortie correcte de manière certaine. Au lieu de cela, il déduit des informations des ensembles de données pour déterminer la sortie attendue **[6].**

5.3 La classification

La dernière étape dans un système de reconnaissance est la classification. Son objectif est de donner une classe ou une catégorie à chaque objet (ou individu) à classer, en utilisant des données statistiques pour cela. En reconnaissance de forme, elle utilise fréquemment l'apprentissage automatique et est largement employée. Il existe différentes méthodes de classification :

5.3.1 Machine à Vecteurs de support (SVM)

La classification supervisée implique l'acquisition d'une règle de classification à partir d'un ensemble de données préalablement classées. Une fois que la règle est maîtrisée, il devient possible de l'appliquer pour classifier de nouvelles données dont la catégorisation est inconnue. Les Support Vector Machines (SVM), connues également sous le nom de machinesà vecteurs de support, représentent une méthode de classification supervisée relativement récente, ayant été introduite en 1992 par Vladimir Vapnik, Bernhard Boser et Isabelle Guyon. Leur efficacité remarquable dans diverses applications pratiques suscite un intérêt croissant. L'objectif de l'algorithme des Machines à Vecteurs de Support (SVM) est de résoudre les problèmes de classification binaire. Il est communément désigné sous l'appellation de problème de discrimination à deux niveaux. Un défi consiste à identifier la catégorie àlaquelle un individu, considéré comme un membre d'un ensemble, appartient parmi deux options possibles **[7]**.

5.3.2 Arbre de décision (ADD)

En matière d'apprentissage automatique, les arbres de décision représentent un modèle de classification largement répandu. Leurs atouts résident dans leur interprétation relativement simple et leur capacité à classifier de manière fiable de vastes ensembles de données. Diverses méthodes ont été proposées dans la littérature pour acquérir des connaissances sur les arbres de décision. Les techniques gloutonnes se caractérisent par leur large adoption. Ces méthodes divisent de façon récurrente le jeu de données en deux sous-ensembles. Cette partition est fondée sur un élément sélectionné de façon peu conventionnelle. Une fois que le critère d'arrêt est satisfait, le processus de partitionnement récursif est interrompu, tel que défini par des conditions telles qu'un seuil minimum d'observations dans un nœud terminal ou l'homogénéité des observations dans ce nœud. Bien que ces méthodes se révèlent efficaces en application,

elles offrent une classification précise pour divers types de données, sans toutefois garantir une précision absolue. Par conséquent, les arbres générés à l'aide de ces méthodes peuvent être extrêmement complexes, moins précis qu'ils pourraient l'être, et il peut également être difficile d'imposer de nouvelles contraintes sur ces structures **[8]**.

5.3.3 Définition de K voisin plus proche (K-NN)

Le kNN, abréviation de "k plus proches voisins", représente un algorithme d'apprentissage automatique appartenant à la catégorie des méthodes d'apprentissage supervisé simples et faciles à implémenter. Il peut être employé pour résoudre des problèmes de classification et de régression **[9]**.

La classification kNN soulève au moins deux questions non résolues concernant la mesure de similarité entre deux données. Et la décision relative à la valeur de k. Diverses méthodes ont été proposées pour aborder cette question. La question initiale porte sur diverses mesures de distance telles que la distance euclidienne, la distance de Mahalanobis, la distance de Minkowski et leurs différentes variantes. La première question aboutit à la conclusion commune selon laquelle les applications nécessitent des mesures de distance variées. Cet article se concentre sur la deuxième problématique, qui concerne la sélection de la valeur k enutilisant exclusivement la distance euclidienne pour évaluer la similarité (ou distance) entre deux points de données. Les approches précédentes de classification kNN ont adopté une approche consistant à déterminer la valeur de k en utilisant une constante fixe pour l'ensembledes données de test, ou en réalisant une validation croisée pour estimer la valeur de k pour chaque point de données de test. Fréquemment, cette situation conduit à une faible précision de prédiction dans les applications de classification réelles, étant donné que ces méthodes ne prennent pas en compte la distribution des données **[9]**.

5.3.4 Principe de la méthode des k plus proches voisins

Une fois que l'algorithme a achevé la phase d'apprentissage, pour prédire une nouvelle observation inconnue, il recherche dans l'ensemble de données d'apprentissage l'observation la plus similaire. Ensuite, l'algorithme assigne la nouvelle observation inconnue à l'étiquette correspondante dans l'ensemble de données d'apprentissage.

En employant le paramètre k dans le concept de "k plus proches voisins", il devient envisageable de prendre en compte un nombre déterminé de voisins de l'ensemble d'apprentissage, au lieu de se restreindre à un unique voisin le plus proche de l'observation inconnue. En définitive, il nous est possible de faire des prédictions en se basant sur la classe sociale dominante de ce quartier **[10]**.

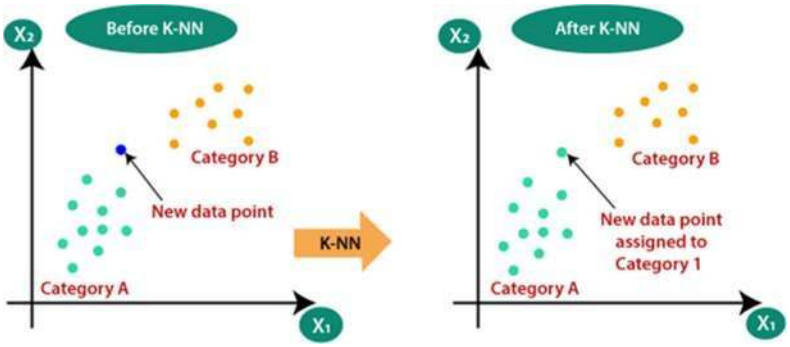


Figure 5-4 : L'algorithme k-NN et son principe de fonctionnement

5.4.1 La distance euclidienne

Il est envisageable de déterminer la distance entre deux points en effectuant la racine carrée de la somme des carrés des écarts entre leurs coordonnées**.**

$$d(\vec{u},\vec{v}) = \|\vec{u}-\vec{v}\| = \sqrt{\sum_{i=1}^{n}(u_i - v_i)^2}$$

5.4.2 La distance Manhattan

Pour calculer la distance de Manhattan entre deux points, on calcule les valeurs absolues des différences entre leurs coordonnées.

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

5.4.3 La distance Hamming

Hamming Distance

$$D_H = \sum_{i=1}^{k} |x_i - y_i|$$

$$x = y \Rightarrow D = 0$$

$$x \neq y \Rightarrow D = 1$$

X	Y	Distance
Male	Male	0
Male	Female	1

Notons qu'il y a d'autres mesures de distance selon le contexte d'utilisation de l'algorithme, mais la distance euclidienne reste la plus utilisée **[11].**

5.4.4 Similarité cosinus

La similarité cosinus est une mesure de similarité utilisée pour quantifier la similarité entre deux vecteurs dans un espace vectoriel. Elle est calculée en utilisant le cosinus de l'angle entreles deux vecteurs. Cette mesure est souvent utilisée dans les systèmes de recommandation pour trouver des éléments similaires **[12].**

5.4.4.1 Calcul de la similarité cosinus

Pour calculer la similarité cosinus entre deux vecteurs, nous utilisons la formule suivante :

$$Similarité(U,V) = cos(\theta) = \frac{U \cdot V}{\|U\| \cdot \|V\|} = \frac{\sum_{i=1}^{n} U_i V_i}{\sqrt{\sum_{i=1}^{n} U_i^2 \sum_{i=1}^{n} V_i^2}}$$

5.4.4.2 Interprétation de la similarité cosinus

La similarité cosinus donne une valeur comprise entre -1 et 1. Une valeur de 1 indique une similarité maximale entre les vecteurs, tandis qu'une valeur de -1 indique une dissimilarité maximale. Une valeur de 0 indique une absence de similarité.

5.4.4.3 Distance cosinus

Contrairement à la similarité cosinus, la distance cosinus mesure la différence entre deux vecteurs plutôt que leur similarité. La distance cosinus est calculée en soustrayant la similarité cosinus de 1. Ainsi, plus la similarité cosinus est élevée, plus la distance cosinus est faible.

5.4.4.4 Calcul de la distance cosinus

Pour calculer la distance cosinus entre deux vecteurs, nous utilisons la formule suivante...

Distance cosinus = 1 - similarité cosinus

5.4.4.5 Interprétation de la distance cosinus

La distance cosinus donne une valeur comprise entre 0 et 2. Une valeur de 0 indique une distance minimale entre les vecteurs, ce qui signifie qu'ils sont très similaires. Une valeur plus élevée indique une distance plus grande entre les vecteurs, ce qui signifie qu'ils sont moins similaires.

5.4.4.6 Utilisation de la similarité et de la distance cosinus

La similarité et la distance cosinus sont largement utilisées dans les systèmes de recommandation et d'analyse de données. Voici quelques exemples d'applications de ces mesures :

5.4.4.7 Exemples d'applications

Outre les systèmes de recommandation, la similarité et la distance cosinus sont également utilisées dans d'autres domaines tels que l'analyse de texte, la clustering de données, larecherche d'informations, etc. Ces mesures permettent de quantifier la similarité ou la différence entre des vecteurs dans un espace multidimensionnel.

5.4.4.8 Conclusion

Dans cette section, nous avons exploré les concepts de similarité et de distance cosinus. Nous avons examiné les différentes distances de mesure utilisées en analyse de données, telles que

la distance euclidienne, la distance de Manhattan et la distance de Minkowski. Ensuite, nous avons discuté de la similarité et de la distance cosinus, en expliquant comment les calculer et comment les interpréter. Enfin, nous avons abordé les utilisations de la similarité et de la distance cosinus dans les systèmes de recommandation et d'autres applications.

6 La WLDA (ou la LDA blanchie) (Whitened Linear Discriminant Analysis) [13]

Au fil des années, de nombreux algorithmes d'analyse discriminante linéaire (LDA : Linear Discriminant Analysis)) ont été proposés pour la réduction des données à forte dimension dans une grande variété de problèmes [10]. Mais une limitation inhérente de la LDA classique est le problème dit de "petite taille d'échantillon (3S : Small Sample Size)", c'est-à-dire qu'elle échoue lorsque toutes les matrices de dispersion sont singulières. Denombreuses extensions de la LDA ont été proposées dans le passé pour surmonter les problèmes 3S. Cependant, aucune des méthodes avancées n'a pu résoudre complètement ce problème des 3S dans la mesure où elles permettent de conserver toutes les caractéristiques discriminantes avec un faible coût de calcul. Mais le blanchiment des données suivi par l'application de la LDA, a permis à la LDA blanchie de trouver les caractéristiques les plus discriminantes sans avoir à faire face au problème des 3S. Dans la WLDA, seul le calcul des valeurs propres simples est effectué au lieu du calcul des valeurs propres généralisés, ce qui explique le faible coût de calcul de la WLDA.

Dans cette section, nous avons expliqué que le blanchiment des données suivi par l'application de la LDA permet de transformer le problème de calcul des valeurs propres généralisées de la LDA en un calcul de valeurs propres simples, ce qui réduit le coût de calcul.En plus, la WLDA a fait preuve de sa capacité de conserver toutes les informations discriminantes contrairement aux travaux précédents.

7. Base de données des veines du doigt [14]

La reconnaissance des veines du doigt est un domaine de recherche récemment développé. Nous incluons dans SDUMLA-HMT une base de données de veines de doigts qui, à notre connaissance, est la première base de données ouverte de veines de doigts. L'appareil utilisé pour capturer les images des veines du doigt a été conçu par le Joint Lab. for Intelligent Computing and Intelligent Systems de l'université de Wuhan. Au cours du processus de capture, il a été demandé à chaque sujet invité de fournir des images de son index, de son majeur et de son annulaire des deux mains. La collecte pour chacun des 6 doigts est répétée 6 fois pour obtenir 6 images de veines digitales. Quelques exemples d'images sont présentés à lafigure 5.

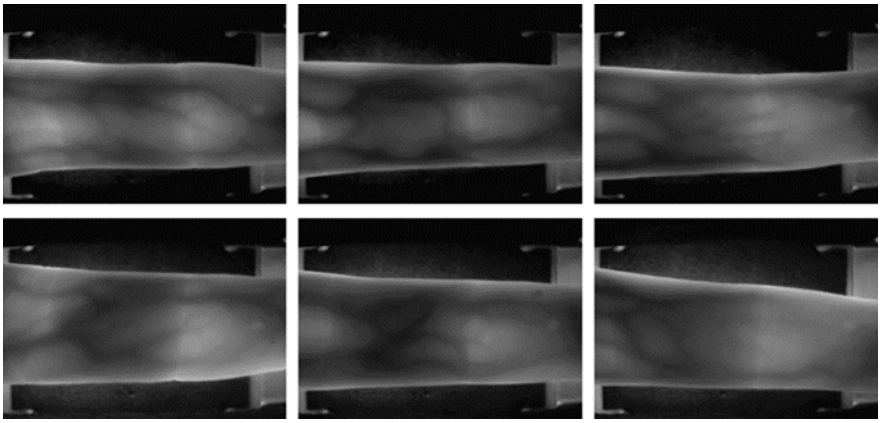


Figure 5-5 : Exemples d'images dans la base de données des veines du doigt

La base de données des veines du doigt est composée de 6×6×106=3 816 images. Chaque image est stockée au format "bmp" avec une taille de 320×240 pixels. La taille totale de notre base de données est d'environ 0,85 Goctets.

Résultats

1. Introduction :

Dans ce chapitre, nous présenterons les résultats que nous avons obtenus pour nous assurer de la validité de notre système. D'abord nous commençons par la description de la base de données utilisée. Ensuite, nous faisons plusieurs expériences sur cette base pour étudier l'effet de notre système sur elle. Ensuite nous présentons les résultats que nous avons obtenus avec le descripteur LPQ. Grâce à ces résultats, nous pourrons certainement en mesure d'évaluer les performances de notre système.

2. La base de données

La base SDUMLA-HMT a été collecté durant l'été 2010 à l'université de Shandong, à Jinan, en Chine. 106 sujets, dont 61 hommes et 45 femmes âgés de 17 à 31 ans, ont participé au processus de collecte de données, dans lequel les 5 traits biométriques - visage, veines du doigt, démarche, iris et empreintes digitales - sont collectés pour chaque sujet. SDUMLA-HMT comprend donc cinq sous bases de données, à savoir une base de données sur les visages, une base de données sur les veines des doigts, une base de données sur la démarche, une base de données sur l'iris et une base de données multi-capteurs sur les empreintes digitales. Il convient de noter que dans les cinq sous bases de données, tous les traits biométriques correspondant à l'identité d'une personne sont capturés à partir du même sujet. Nous détaillerons juste après, la sous base les veines des doigts à laquelle nous nous intéressons.

2.1 Sous base de données des veines du doigt

La reconnaissance des veines du doigt est un domaine de recherche en plein essor. Dans SDUMLA-HMT se trouve une sous base de données sur les veines du doigt qui, à notre connaissance, est la première base de données à accès libre sur les veines du doigt.

L'appareil utilisé pour capturer les images des veines du doigt a été conçu par le laboratoire commun d'informatique et de systèmes intelligents de l'université de Wuhan. Lors du processus de capture, il a été demandé à chaque sujet de fournir des images de ses deux index, majeurs et de ses annulaires c'est- à-dire de ses deux mains gauche et droite, et la collecte pour chacun des 6 doigts a été répétée 6 fois pour obtenir 6 images de veines digitales. Quelques exemples d'images ont été présentées sur la figure 5.5. La sous base de données des veines du doigt est composée de 6×6×106=3 816 images. Chaque image est stockée au format "bmp" avec une

taille de 320×240 pixels. La taille totale de cette sous base de données est d'environ 0,85 G octets.

2.2 Extraction des régions d'intérêt (ROI)

Nous avons retenu l'algorithme de Lee pour extraire les ROIs de la base de donnée retenue : ceci est fait grâce à la fonction :

[outMask, edges] = lee_region(x, leeH, leeW)

Cette fonction ***lee_region()*** est utilisée pour extraire une sous-région d'une image ou d'un ensemble de données. Voici une description de cette fonction.

✓ **Les paramètres d'entrée**

- x : Il s'agit des images d'entrée de la sous base des veines que nous souhaitons traiter.
- leeH : Il s'agit de la hauteur de la région Lee que nous souhaitons extraire dans notre cas :

leeH =4.

- leeW : Il s'agit de la largeur de la région que nous souhaitons extraire dans notre cas

LeeW = 20 ou 40.

✓ **Les paramètres de sortie**

- outMask : Ceci est le masque de sortie qui représente la sous-région de Lee extraite.
- edges : Il s'agit de la sortie qui contient les bords de la sous-région de Lee extraite.

La fonction lee_region() utilise certainement les techniques de traitement d'image, telles que la détection et la segmentation des contours, pour identifier et extraire la région Lee des données d'entrée. La sortie outMask est un masque binaire qui met en évidence la région Lee, et la sortie edges contient les limites de la région extraite.

Nous donnons ci-dessous quelques image ROI extraites avec cette fonction Lee_region

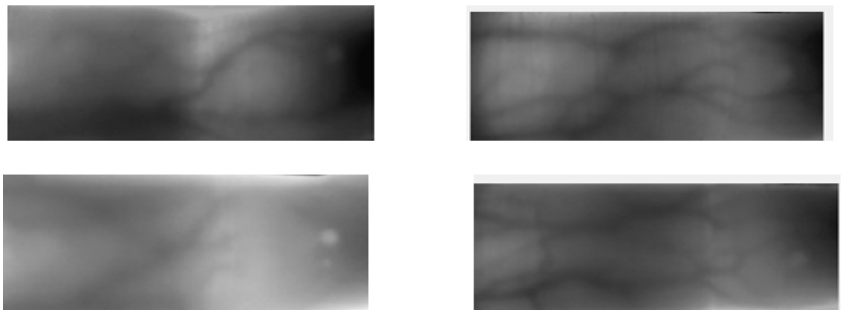


Figure 6.1 : Quelques images ROI de la base de données SDUMLA-HMT

2.3 Séparation des bases de données :

Afin de mener à bien le bon fonctionnement de notre système de reconnaissance du FV, il est indispensable de partager l'ensemble des images en deux groupe l'un pour l'apprentissage et l'autre pour les tests.

Cependant, nous ne disposons pas de deux bases de données. Pour ces tests, nous avons réparti la base de la manière suivante :

3. Résultats

Résultats des simulations

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 4
	LEFT INDEXE	
	PP1	PP2
LPQ5	0,8962	0,9654
LPQ7	0,9182	0,9780
LPQ9	0,9151	0,9560
LPQ11	0,8962	0,9057
LPQ13	0,8585	0,8636

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 4
	Idexe Gauche	
	PP1	PP2
LPQ5	0,8899	0,9528
LPQ7	0,9182	**0,9717**
LPQ9		
LPQ11	0,8899	0,9025
LPQ13	0,8836	0,8931

	LeeH = 40	LeeW= 20
	nn1=1	mm1=2
	PP1	PP2
LPQ5	0,8396	0,9340
LPQ7	0,8962	0,9528
LPQ9	0,8962	0,9340
LPQ11	0,8742	0,9119
LPQ13	0,8679	0,8774

	LeeH = 4	LeeW= 20
	nn1=4	mm1=4
	Idexe Gauche	
	PP1	PP2
LPQ5	0,8145	**0,8616**
LPQ7	0,8208	0,8428
LPQ9	0,8208	0,8176
LPQ11	0,7893	0,7862
LPQ13	0,783	0,7736

	LeeH = 4	LeeW= 20
	nn1=2	mm1=4
	LEFT INDEXE	
	PP1	PP2
LPQ5	0,8459	0,9403
LPQ7	0,8931	0,9686
LPQ9	0,8962	0,9403
LPQ11	0,8553	0,8774
LPQ13	0,8491	0,8648

	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	PP1	PP2
LPQ5	0,7390	0,8836
LPQ7	0,7673	0,8899
LPQ9	0,7579	0,8774
LPQ11	0,7296	0,8302
LPQ13	0,7327	0,7799

P 5 1	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	Left Middle	
	PP1	PP2
LPQ5	0,7390	0,8836
LPQ7	0,7673	0,8899
LPQ9	0,7579	0,8774
LPQ11	0,7296	0,8302
LPQ13	0,7327	0,7799

P 5 2	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,8113	0,9340
LPQ7	0,8333	**0,9371**
LPQ9	0,8113	0,8931
LPQ11	0,7956	0,8648
LPQ13	0,7704	0,8333

P 4 4	LeeH = 4	LeeW= 20
	nn1= 1	mm1=1
	Left Middle	
	PP1	PP2
LPQ5	0,8836	0,9434
LPQ7	0,9182	0,9623
LPQ9	0,9088	0,9277
LPQ11	0,8836	0,8931
LPQ13	0,8585	0,8648

	LeeH = 4	LeeW= 20
	nn1=4	mm1=1
	LEFT INDEXE	
	PP1	PP2
LPQ5	0,6667	0,8176
LPQ7	0,6981	**0,8270**
LPQ9	0,7264	0,7956
LPQ11	0,695	0,7516
LPQ13	0,624	0,7484

	LeeH = 4	LeeW= 40
	nn1= 1	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,7233	0,7327
LPQ7	0,8176	**0,8805**
LPQ9	0,805	0,8585
LPQ11	0,7642	0,8365
LPQ13	0,7642	0,8208

Résultats des simulations

	LeeH = 4	LeeW= 40
	nn1=2	mm1=2
	Left Middle	
	PP1	PP2
LPQ5	0,8050	0,9371
LPQ7	0,8333	0,9340
LPQ9	0,8145	0,8994
LPQ11	0,7673	0,8449
LPQ13	0,7547	0,8208

	LeeH = 4	LeeW= 40
	nn1=2	mm1=4
	Majeur gauche	
	PP1	PP2
LPQ5	0,8585	0,9308
LPQ7	0,8711	**0,9340**
LPQ9	0,8711	0,9151
LPQ11	0,8113	0,8459
LPQ13	0,7956	0,8113

ANNULAIRE GAUCHE

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 1
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.7170	0.7421
LPQ7	0.7767	0.8711
LPQ9	0.7925	0.8805
LPQ11	0.8208	**0.9057**
LPQ13	0.8082	0.8585

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 2
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.7956	0.8994
LPQ7	0.8585	**0.9560**
LPQ9	0.8679	0.9434
LPQ11	0.8899	0.9528
LPQ13	0.8616	0.9025

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 5
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8742	0.9528
LPQ7	0.9088	**0.9811**
LPQ9	0.9245	0.9686
LPQ11	0.9465	**0.9811**
LPQ13	0.8962	0.9277

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 6
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8962	0.9686
LPQ7	0.9182	**0.9717**
LPQ9	0.9151	0.9686
LPQ11	0.9308	**0.9717**
LPQ13	0.8931	0.9308

ANNULAIRE GAUCHE

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 40
	PP1	PP2
LPQ5		
LPQ7		
LPQ9		
LPQ11		
LPQ13		

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 1
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.7264	0.7075
LPQ7	0.7767	**0.8774**
LPQ9	0.7925	0.8711
LPQ11	0.8082	0.9182
LPQ13	0.8082	0.8522

	LeeH = 40	LeeW= 20
	nn1= 1	mm1= 4
	PP1	PP2
LPQ5		
LPQ7		
LPQ9		
LPQ11		
LPQ13		

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 4
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8648	0.9497
LPQ7	0.9088	**0.9686**
LPQ9	0.9151	**0.9780**
LPQ11	0.9277	0.9654
LPQ13	0.8836	0.9214

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 7
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8994	0.9591
LPQ7	0.9214	**0.9780**
LPQ9	0.9214	**0.9780**
LPQ11	0.9403	0.9717
LPQ13	0.8962	0.9308

Résultats des simulations

	LeeH = 4	LeeW= 20
	nn1= 1	mm1=1
	Idexe Gauche	
	PP1	PP2
LPQ5	0,7767	0,7516
LPQ7	0,8270	**0,9088**
LPQ9	0,8553	0,8836
LPQ11	0,8302	0,8805
LPQ13	0,8208	0,8145

	LeeH = 4	LeeW= 40
	nn1=2	mm1=2
	Idexe Gauche	
	PP1	PP2
LPQ5	0,7952	0,9214
LPQ7	0,8428	**0,9340**
LPQ9	0,8459	0,9245
LPQ11	0,8333	0,8805
LPQ13	0,8270	0,8491

	LeeH = 4	LeeW= 20
	nn1=1	mm1=2
	Idexe Gauche	
	PP1	PP2
LPQ5	0,8396	0,9340
LPQ7	0,8962	**0,9528**
LPQ9	0,8962	0,9340
LPQ11	0,8742	0,9119
LPQ13	0,8679	0,8774

	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	Idexe Gauche	
	PP1	PP2
LPQ5	0,7358	0,8491
LPQ7	0,7642	0,8836
LPQ9	0,7579	**0,8931**
LPQ11	0,7516	0,8459
LPQ13	0,739	0,805

	LeeH = 4	LeeW= 20
	nn1=2	mm1=2
	PP1	PP2
LPQ5	0,8113	0,9340
LPQ7	0,8333	0,9371
LPQ9	0,8113	0,8931
LPQ11	0,7956	0,8648
LPQ13	0,7704	0,8333

	LeeH = 4	LeeW= 20
	nn1=2	mm1= 4
	PP1	PP2
LPQ5	0,8585	0,9371
LPQ7	0,8679	0,9403
LPQ9	0,8616	0,9057
LPQ11	0,8239	0,8648
LPQ13	0,8019	0,8113

	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,8585	0,9371
LPQ7	0,8679	**0,9403**
LPQ9	0,8616	0,9057
LPQ11	0,8293	0,8648
LPQ13	0,8019	0,8113

	LeeH = 4	LeeW= 20
	nn1=2	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,7138	0,8396
LPQ7	0,7421	**0,8491**
LPQ9	0,7329	0,8176
LPQ11	0,7044	0,7799
LPQ13	0,6824	0,7296

	LeeH = 4	LeeW= 20
	nn1= 1	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,7358	0,7107
LPQ7	0,8176	**0,8774**
LPQ9	0,8019	0,8711
LPQ11	0,7799	0,8522
LPQ13	0,7736	0,8050

	LeeH = 4	LeeW= 20
	nn1= 1	mm1=1
	Majeur gauche	
	PP1	PP2
LPQ5	0,8302	0,9214
LPQ7	0,8679	**0,9528**
LPQ9	0,816	0,9277
LPQ11	0,8396	0,8962
LPQ13	0,8302	0,8679

	LeeH = 4	LeeW= 40
	nn1= 1	mm1=2
	Majeur gauche	
	PP1	PP2
LPQ5	0,8382	0,9214
LPQ7	0,8648	**0,9528**
LPQ9	0,8679	0,9214
LPQ11	0,9239	0,8679
LPQ13	0,8270	0,8522

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 4
	Majeur gauche	
	PP1	PP2
LPQ5	0,8774	0,8528
LPQ7	0,9214	**0,9654**
LPQ9	0,9088	0,9403
LPQ11	0,8742	0,8616
LPQ13	0,8459	0,8491

Résultats des simulations

	LeeH = 4	LeeW= 40
	nn1=4	mm1=2
	Majeur gauche	
	PP1	PP2
LPQ5	0,7484	0,8711
LPQ7	0,7830	**0,8868**
LPQ9	0,7704	0,8459
LPQ11	0,7327	0,7987
LPQ13	0,7201	0,7673

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 1
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.7170	0.7421
LPQ7	0.7767	0.8711
LPQ9	0.7925	0.8805
LPQ11	0.8208	**0.9057**
LPQ13	0.8082	0.8585

LeeH = 4 LeeW= 20

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 3
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8428	0.9245
LPQ7	0.8711	**0.9560**
LPQ9	0.9025	0.9528
LPQ11	0.9151	0.9434
LPQ13	0.8836	0.9119

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 4
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8616	0.9497
LPQ7	0.9057	**0.9811**
LPQ9	0.9182	0.9717
LPQ11	0.9340	0.9654
LPQ13	0.8868	0.9277

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 7
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8931	0.9686
LPQ7	0.9151	**0.9874**
LPQ9	0.9245	0.9748
LPQ11	0.9465	0.9780
LPQ13	0.8994	0.9340

	LeeH = 4	LeeW= 20
	nn1= 1	mm1= 8
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5		
LPQ7		
LPQ9		
LPQ11		
LPQ13		

LeeH = 4 LeeW= 40

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 2
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8113	0.9057
LPQ7	0.8553	0.9560
LPQ9	0.8742	**0.9623**
LPQ11	0.8836	0.9591
LPQ13	0.8491	0.9025

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 3
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8428	0.9151
LPQ7	0.8742	0.9245
LPQ9	0.8994	**0.9560**
LPQ11	0.9057	0.9403
LPQ13	0.8774	0.9057

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 5
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8836	0.9591
LPQ7	0.9151	0.9717
LPQ9	0.9182	0.9717
LPQ11	0.9403	**0.9748**
LPQ13	0.8931	0.9277

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 6
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.8962	0.9717
LPQ7	0.9182	0.9717
LPQ9	0.9182	**0.9811**
LPQ11	0.9308	0.9717
LPQ13	0.8899	0.9308

	LeeH = 4	LeeW= 40
	nn1= 1	mm1= 8
	ANNULAIRE GAUCHE	
	PP1	PP2
LPQ5	0.9025	0.9717
LPQ7	0.9340	**0.9811**
LPQ9	0.9308	0.9748
LPQ11	0.9434	0.9717
LPQ13	0.8994	0.9277

Résumé

	LeeH = 4	LeeW= 20
	nn1= 1	
	ANNULAIRE GAUCHE	
	mm1	PP2
LPQ7	1	0.9057
LPQ7	2	0.9560
LPQ7	3	0.9560
LPQ7	4	0.9811
LPQ7	5	0.9811
LPQ7,11	6	0.9717
LPQ 7	7	0.9874
LPQ7	8	0.9811

	LeeH = 4	LeeW= 40
	nn1= 1	
	ANNULAIRE GAUCHE	
	mm1	PP2
LPQ11	1	0.9182
LPQ9	2	0.9623
LPQ9	3	0.9560
LPQ9	4	0.9780
LPQ11	5	0.9748
LPQ 9	6	0.9811
LPQ 7,9	7	0.9780
LPQ7	8	0.9811

	LeeH = 4	LeeW= 20
	nn1= 1	
	Idexe Gauche	
	mm1	PP2
LPQ7	1	0.9088
LPQ7	2	0,9528
LPQ7	3	0.9654
LPQ7	4	0.9717
LPQ7	5	0.9780
LPQ7	6	0.9748
LPQ5, 7	7	0.9780
LPQ7	8	0.9843

Conclusion Générale

Ce modeste travail de recherche présenté dans notre mémoire s'inscrit dans le domaine global de la biométrie, en mettant l'accent sur l'identification automatique des individus à partir des veines du doigt. L'identification et l'authentification jouent un rôle important dans notre vie quotidienne. Au cours du mémoire, l'identification et l'authentification ont été explorées dans le monde électronique. On a expliqué que l'identification et l'authentification protègent trois caractéristiques principales : la confidentialité, l'intégrité et la disponibilité. Afin de protéger ces caractéristiques, trois méthodes d'authentification sont utilisées, à savoir ; quelque chose que l'utilisateur connaît, quelque chose que l'utilisateur a, et quelque chose que l'utilisateur est.

La reconnaissance des veines du doigt, en tant que technologie biométrique émergente, a attiré une attention considérable dans le domaine de l'authentification biométrique en raison de ses avantages uniques. Effectivement, l'efficacité de l'emploi des motifs veineux réside dans l'impossibilité de sa falsification, en raison de leur positionnement sous la peau. Ainsi, après avoir exposé les concepts fondamentaux de l'identification et de l'authentification, de la biométrie et des différents modalités biométriques ainsi que leur fonctionnement, nous avons consacré un chapitre à la biométrie par les veines du doigt exposé quelques paramètres et des outils mathématiques pour analyser et extraire les caractéristiques.

On considère cette dernière modalité comme une méthode biométrique récemment employée pour une identification plus précise et plus sûre, le motif de veine du doigt étant l'une des modalités biométriques les plus distinctives, même pour les vrais jumeaux. Effectivement, l'efficacité de l'emploi des motifs veineux réside dans l'impossibilité de sa falsification, en raison de leur positionnement à l'intérieur de la peau. Ainsi, après avoir exposé les concepts fondamentaux de l'identification et de l'authentification, de la biométrie et des différents modalités biométriques ainsi que leur fonctionnement, nous avons consacré un chapitre à la biométrie par les veines du doigt, puis nous avons exposé sommairement les quelques outils utilisés pour mener à bien nos simulations que nous avons mené sur l'une des bases de données multimodales publique (SDUMLA-HMT).

Références Bibliographiques

Références Bibliographiques

CHAPITRE I

[1] TIPTON, Harold F. Purposes of information security management. *Handbook of Information Security Management*, 1998, p. 019-021.

[2] MAYFIELD, Terry, ROSKOS, J. Eric, WELKE, Stephen R., *et al.* Integrity in automated information systems. *National Security Agency, Tech. Rep*, 1991, vol. 79.

[3] WOODARD JR, J. D., ORLANS, N. M., et HIGGINS, P. T. Biometrics: Identity Assurance in the Information Age. 2003.

[4] IMPERVA, A. Consumer password worst practices. *Application Defense Center*, 2010.

[5] CLULEY, Graham. Sizing up the malware threat–key malware trends for 2010. *Network Security*, 2010, vol. 2010, no 4, p. 8-10.

[6] ePass ePass OTP authentication system white paper, Germany: RS-Computer, 2008).

Vertriebs GmbH & Co. KG.

[7] HALLER, Neil et METZ, Craig. Rfc1938: A one-time password system. 1996.

[8] RUBIN, Aviel D. Independent one-time passwords. *computing Systems*, 1996, vol. 9, no 1, p. 15-27.

[9] ZVIRAN, Moshe et ERLICH, Zippy. Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems*, 2006, vol. 17, no 1, p. 4.

[10] RAMSBROCK, Daniel, MOSKOVCHENKO, Stepan, et CONROY, Christopher. Magnetic swipe card system security. *A case study of the University of Maryland, College Park*, 2006.

CHAPITRE II

[1] NEWMAN, Robert. *Security and Access Control Using Biometric Technologies: Application, Technology, and Management*. Course Technology Press, 2009.

[2] ROBERTS, Chris. Biometric technologies-fingerprints. *Publisher name and location are missing*, 2006, p. 1-23.

[3] https://blog.garrytan.com/quantum-of-solaces-multitouch-ui-video-wall-g

[4] https://biometrics.mainguet.org/movies/movies_2008.htm#QuantumOfSolace

[5] Mainguet F-J. (2009). Biometric movies. Available from: https://biometrics.mainguet.org/movies/movies_2009.htm

[6] Brubeck U. & Sanchez D (n.d). Biometrics authentication – Technology and evaluation. San Diego: San Diego State University

[7] The history of fingerprints June 2024. https://onin.com/fp/fphistory.html

[8] BLACKBURN, Duane, MILES, Chris, et WING, Brad. Biometrics foundation documents. *National*

[9] WEI, Gang et LI, Dongge. *Biometrics: applications, challenges and the future*. Springer US, 2006.

[10] WOODARD JR, J. D., ORLANS, N. M., et HIGGINS, P. T. Biometrics: Identity Assurance in the Information Age. 2003.

[11] Biometric Technology Application Manual Volume 1, Section 3 p24-25 https://www.yumpu.com/en/document/view/10178385/biometric-technology-application-manual-volume-one-planet-#

[12] CHEN, Hong, VALIZADEGAN, Hamed, JACKSON, Carrie, *et al.* Fake hands: spoofing hand geometry systems. *Biometric Consortium*, 2005.

[13] OSTAFF Courtney. Retinal scans do more than let you in the door. *PhysOrg. com. Retrieved on April*, 2005, vol. 7, p. 2007.

[14] GREGORY, Peter et SIMON, Michael A. *Biometrics for dummies*. John Wiley & Sons, 2008.

[15] MATSUMOTO, Tsutomu, MATSUMOTO, Hiroyuki, YAMADA, Koji, *et al.* Impact of artificial" gummy" fingers on fingerprint systems. In: *Optical security and counterfeit deterrence techniques IV*.
SPIE, 2002. p. 275-289.

[16] BUBECK, U. M. et SANCHEZ, Dina. Biometric authentication: Technology and evaluation. *Term Project CS574*, 2003.

[17] JAIN, Anil K., HONG, Lin, PANKANTI, Sharath, *et al.* An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 1997, vol. 85, no 9, p. 1365-1388.

[18] Jain K.A, Shah J & Ross A. (2007), From Template to Image: *Reconstructing Fingerprints from Minutiae Points*, IEEE transactions on pattern analysis and machine intelligence, VOL. 29, NO. 4

[19] ROSS, Arun, SHAH, Jidnya, et JAIN, Anil K. From template to image: Reconstructing fingerprints from minutiae points. *IEEE transactions on pattern analysis and machine intelligence*, 2007, vol. 29, no 4, p. 544-560.

CHAPITRE III : Traits biométriques

[1] MALTONI, Davide, MAIO, Dario, JAIN, Anil K., et al. Handbook of fingerprint recognition. London: springer, 2009.

[2] LI, Stan Z. *Encyclopedia of Biometrics: I-Z*. Springer Science & Business Media, 2009.

[3] NSTC Archives
https://obamawhitehouse.archives.gov/administration/eop/ostp/nstc/docsreports/archives

[4] CHEN, Hong, VALIZADEGAN, Hamed, JACKSON, Carrie, *et al.* Fake hands: spoofing hand geometry systems. *Biometric Consortium*, 2005.

[5] GOVINDARAJU, Pavan K. Rudravaram Venu. Peg-Free hand geometry verification system. *USA: New York*.

[6] JAIN, Anil K., BOLLE, Ruud, et PANKANTI, Sharath (ed.), Biometrics: Personal identification in network security, USA: New York & Michigan, Kluwer Academic Publishers 2003 by The McGraw-Hill

[7] WOODARD JR, J. D., ORLANS, N. M., et HIGGINS, P. T. Biometrics: Identity Assurance in the Information Age. 2003. P106

[8] John Daugman OBE FREng, Professor of Computer Vision and Pattern

[9] JAIN, Anil K., BOLLE, Ruud, et PANKANTI, Sharath (ed.). *Biometrics: personal identification in networked society*. Springer Science & Business Media, 2006.

[10] Biometric Technology Application Manual Volume 1, Section 3 p24-25
https://www.yumpu.com/en/document/view/10178385/biometric-technology-application-manual-volume-one-planet-#

[11] GREGORY, Peter et SIMON, Michael A. *Biometrics for dummies*. John Wiley & Sons, 2008.

[12] Motorola 2006 P7
https://www.annualreports.com/HostedData/AnnualReportArchive/m/NYSE_MSI_2006.pdf

CHAPITRE IV

[1] Puneet Gupta, Phalguni Gupta, An accurate finger vein based verification system, Digital Signal Process. 38 (2015) 43–52.

[2] Y. Lu, S. Yoon, S. Wu, D.S. Park, Pyramid Histogram of Double Competitive Pattern for Finger Vein Recognition, IEEE Access 6 (2018) 56445–56456.

[3] UHL, Andreas, BUSCH, Christoph, MARCEL, Sébastien, *et al.* ***Handbook of vascular biometrics***. Springer Nature, 2020.

[4] ZAYED, Hossam L., HAMID, Heba M. Abdel, KAMAL, Yasser M., *et al.* A comprehensive survey on finger vein biometric. *Journal of Advances in Information Technology*, 2023, vol. 14, no 2, p. 2-8.

[5] Z. Liu, Y. Yin, H. Wang, S. Song, and Q. Li, "Finger vein recognition with manifold learning," Journal of Network and Computer Applications, vol. 33, pp. 275–282, 2010.

[6] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, et al., "Finger vein biometrics: taxonomy analysis, open challenges, future directions, and the recommended solution for decentralized network architectures," IEEE Access, vol. 8, pp. 9821–9845, January 2020.

[7] HASHIMOTO, Junichi. Finger vein authentication technology and its future. In : *2006 Symposium on VLSI Circuits, 2006. Digest of Technical Papers.* IEEE, 2006. p. 5-8.

[8] Hitachi, Hitachi Develops Finger Vein Authentication Technology for Steering Wheels, October 25, 2007.

[9] KONO, Miyuki, UEKI, Hironori, et UMEMURA, Shin-ichiro. Near-infrared finger vein patterns for personal identification. *Applied Optics*, 2002, vol. 41, no 35, p. 7429-7436.

[10] KOLIVAND, Hoshang, ASADIANFAM, Shiva, AKINTOYE, Kayode Akinlekan, *et al.* Finger vein recognition techniques: a comprehensive review. *Multimedia Tools and Applications*, 2023, vol. 82, no 22, p. 33541-33575.

[11] LI, Stan Z. Encyclopedia of Biometrics: I-Z. Springer Science & Business Media, 2009.

[12] MENG, Xianjing, YANG, Gongping, YIN, Yilong, *et al.* Finger vein recognition based on local directional code. *Sensors*, 2012, vol. 12, no 11, p. 14937-14952.

[13] XIE, Song, FANG, Liyong, WANG, Ziqian, *et al.* Review of personal identification based on near infrared vein imaging of finger. In : *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*. IEEE, 2017. p. 206-213.

[14] LIU, Zhi et SONG, Shangling. An embedded real-time finger-vein recognition system for mobile devices. *IEEE Transactions on consumer Electronics*, 2012, vol. 58, no 2, p. 522-527

[15] Hitachi LTD, "Finger vein authentication," White Paper, pp. 1–4, 2006.

[16] YANG, Jinfeng et SHI, Yihua. Finger–vein ROI localization and vein ridge enhancement. *Pattern Recognition Letters*, 2012, vol. 33, no 12, p. 1569-1579.

[17] K. Wang, A. S. Khisa, X. Q. Wu, and Q. S. Zhao, "Finger vein recognition using LBP variance with global matching," in Proc.the Wavelet Analysis and Pattern Recognition (ICWAPR), 2012 International Conference, Guangdong, China, pp. 196–201, 2012.

[18] H. Qin and M. A. El-Yacoubi, "Finger-vein quality assessment by representation learning from binary images," in Proc. The International Conference on Neural Information Processing, Istanbul, Turkey, 2015, Springer, pp. 421–431.

[19] RAMYA, V., VIJAYA KUMAR, P., et PALANIAPPAN, B. A novel design of finger vein recognition for personal authentication and vehicle security. *J. Theor. Appl. Inf. Technol*, 2014, vol. 65, no 1, p. 67-75.

[20] HOSHYAR, Azadeh Noori et SULAIMAN, Riza. Review on finger vein authentication system by applying neural network. In : *2010 International Symposium on Information Technology*. IEEE, 2010. p. 1020-1023.

[21] EZHILMARAN, D. et JOSEPH, P. Rose Bindu. A study of feature extraction techniques and image enhancement algorithms for finger vein recognition. *International Journal of PharmTech Research*, 2015, vol. 8, no 8, p. 222-229.

[22] XI, Xiaoming, YANG, Lu, et YIN, Yilong. Learning discriminative binary codes for finger vein recognition. *Pattern Recognition*, 2017, vol. 66, p. 26-33.

[23] SHAHEED, Kashif, LIU, Hangang, YANG, Gongping, *et al.* A systematic review of finger vein recognition techniques. *Information*, 2018, vol. 9.

[24] YANG, Gongping, XI, Xiaoming, et YIN, Yilong. Finger vein recognition based on (2D) 2 PCA and metric learning. *BioMed Research International*, 2012, vol. 2012, no 1, p. 324249.

[25] MANTRAO, N. et SUKHPREET, K. An efficient minutiae matching method for finger vein recognition. *Int. J. Adv. Res. Comput. Sci. Softw. Eng*, 2015, vol. 5, p. 657-660.

[26] DAVIS, V. et DEVANE, S. Diagnosis of brain hemorrhage using artificial neural network. *International Journal of Scientific Research in Network Security and Communication*, 2017, vol. 5, no 1, p. 20-23.

CHAPITRE V

[1] MA, Hui, HU, Na, et FANG, Chunxin. The biometric recognition system based on near-infrared finger vein image. *Infrared Physics & Technology*, 2021, vol. 116, p. 103734.

[2] T. Ahonen, E. Rahtu, V. Ojansivu, et al., Recognition of blurred faces using Local Phase Quantization, in: International Conference on Pattern Recognition, IEEE, 2008, pp. 1–4.

[3] Z. Lei, T. Ahonen, Matti Pietikainen, et al., Local frequency descriptor for low-resolution face recognition, in: IEEE International Conference on Automatic Face & Gesture Recognition, IEEE Computer Society, 2011, pp. 161–166.

[4] P.G. Freitasa, L.P. Eira, S.S. Santos, M.C.Q. Fariasb, Image quality assessment using BSIF, CLBP, LCP, and LPQ operators, Theoret. Comput. Sci. 805 (2020) 37–61.

[5] https://blent.ai/blog/a/apprentissage-supervise-definition

[6] https://blent.ai/blog/a/apprentissage-supervise-definition

[7] BOULET-ST-JACQUES, David. Les algèbres amassées : Définitions de base et résultats. *Cahier de Mathématique de l'Université de Sherbrooke (CaMUS)*, 2012, vol. 2, p. 135-150. https://savoirs.usherbrooke.ca/bitstream/handle/11143/16093/2_francoeur_CaMUS_2010_vol.1.pdf

[8] VERHAEGHE, Hélène, NIJSSEN, Siegfried, PESANT, Gilles, *et al.* Apprentissage d'arbres de décision optimaux grâce à la programmation par contraintes. In : *Seizième journées Francophones de Programmation par Contraintes (JFPC21)*. 2021. https://webusers.i3s.unice.fr/jfpc_2021/assets/agenda/JFPC_2021_final/JFPC2021_B1.pdf

[9] https://datascientest.com/knn

[10] MATHIEU-DUPAS, Eve. Algorithme des k plus proches voisins pondérés et application en diagnostic. In : *42èmes Journées de Statistique*. 2010.

[11] ELMOHRI, Madani et BOUCHERIT, ISMAIL. Utilisation du modèle LBP pour l'extraction des caractéristiques des images veines des doigts. 2020.

[12] https://medium.com/@santannalouis208/la-similarit%C3%A9-cosinus-en-ia-nlp-d554d3b14efa

[13] NHAT, Vo Dinh Minh, LEE, Sung Young, et YOUN, Hee Yong. Whitened LDA for face recognition. In: Proceedings of the 6th ACM international conference on Image and video retrieval. 2007. p. 234-241.

[14] YIN, Yilong, LIU, Lili, et SUN, Xiwei. SDUMLA-HMT: A multimodal biometric database. In : *Biometric Recognition: 6th Chinese Conference, CCBR 2011, Beijing, China, December 3-4, 2011. Proceedings 6*. Springer Berlin Heidelberg, 2011. p. 260-268.

CHAPITRE VI

[1] YIN, Yilong, LIU, Lili, et SUN, Xiwei. SDUMLA-HMT: A multimodal biometric database. In : *Biometric Recognition: 6th Chinese Conference, CCBR 2011, Beijing, China, December 3-4, 2011. Proceedings 6*. Springer Berlin Heidelberg, 2011. p. 260-268.

[2] LEE, Eui Chul, LEE, Hyeon Chang, et PARK, Kang Ryoung. Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction. *International Journal of Imaging Systems and Technology*, 2009, vol. 19, no 3, p. 179-186.