الجمهورية الجزائرية الديمقراطية الشعبية

Populaire et démocratique algérienne République

وزارة التعليم العالي و البحث العلمي

Ministère de l'enseignement supérieur et de la recherche scientifique

المركز الجامعي لعين تموشنت

Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent

Institut de Technologie

Département de Génie Electrique

Projet de fin d'études

Pour l'obtention du diplôme de Master en :

Domaine : TECHNOLOGIE

Filière: Télécommunications

Spécialité : Réseaux et Télécommunications.

Thème

Identification des personnes par la biométrie de la main

Présenté Par :

1) ABDELAZIZ Miloud
2) CHILI Ahmed

Devant le jury composé de :

BENOSMANE	Mourad	C.U.B.B.T	MCB	President
BOUTKHIL	Malika	C.U.B.B.T	MAA	Encadrante
SOUIKI	Sihem	C.U.B.B.T	MCB	Examinaterice

Année universitaire2019/2020

Remerciements

Au terme de ce travail, Nous tenons à exprimer nos profonde gratitude à notre professeur et encadrante Mme BOUTKHIL Malika et notre co-encadrante Mme Bentaieb Samia qui n'a pas cesser de nous prodiguer tout au long de la période du projet, pour le choix de sujet, le temps qu'elle nous a consacré et pour son précieux aide. Un grand remerciement pour son humour et sa gentillesse.

Nous adressons aussi nos vifs remerciements aux membres de jury pour avoir bien voulu examiner et juger notre travail.

Nous nous ne laisserons pas cette occasion passer, sans remercier tous les enseignants et le personnel de l'Université CUAT, et particulièrement ceux de la section Réseaux & Télécommunications pour leurs aides et leurs précieux conseils

Enfin, on remercie tous ceux qui ont contribué de près ou de loin au bon déroulement de ce projet.

Dédicace

Avant tout, je remercie le grand Dieu, qui nous a aidés à élaborer ce modeste travail.

Je dédie ce modeste travail :

A toi MA MERE pour ton courage, tes combats et tes sacrifices afin que je puisse achever mes études.

A toi MON PERE, l'homme à qui je dois ma réussite, mon bonheur, et tout le respect; Que tu trouves ici l'expression de mon affection et une récompense des sacrifices consentis pour moi.

A mes très chers frères et sœurs.

A Tous mes amis surtout: DJAMEL, AMINAIKHLAS, HOUARI, ABDELKADER, MOHAMED, FAYCEL, MILOUD, MUSTAPHA, MEHDI, ARBI,…. Egalement à tous ceux que je connais.

A mon binôme AYMEN ainsi qu'à toute sa famille dont l'apport dans notre travail est inestimable.

A tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers. A toute la promotion RT.

Dédicace

Avant tout, je remercie le grand Dieu, qui nous a aidés à élaborer ce modeste travail.

Je dédie ce modeste travail :

A toi MA MERE pour tes conseils, a toi qui a tout souffert, sans me faire souffrir, que tu trouves dans ce mémoire le témoignage de ma reconnaissance et de mon affection pour tous tes sacrifices, l'extrême amour et la bonté que tu m'a offert pour me voir réussir. Que tu en sois remerciée à tout jamais.

A toi MON PERE, l'homme à qui je dois ma réussite, mon bonheur, et tout le respect; Que tu trouves ici l'expression de mon affection et une récompense des sacrifices consentis pour moi.

A mes très chers frères et sœurs.

A Tous mes amis surtout : NADIR HABBACHA, AMINAIKHLAS,…. Egalement à tous ceux que je connais de loin ou de prêt.

A mon binôme MILOUD ainsi qu'à toute sa famille dont l'apport dans notre travail est inestimable.

A tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers. A toute la promotion RT.

Résumé :

Les systèmes biométriques unimodaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents et notamment à la détérioration de la qualité de l'entrée biométrique. L'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.
Nous avons utilisé l'algorithme SIFT pour l'extraction de caractéristiques, En profitant de sa robustesse grâces a l'invariabilité a l'échelle et à la rotation, de plus de sa rapidité.
Le processus de reconnaissance multimodal permet de renforcer les systèmes biométriques
sur les plans de sécurité, fiabilité et pertinence. En effet. le taux de reconnaissance global pour la méthode proposée est de 100%, ce qui est beaucoup mieux que le système unimodale où le taux de reconnaissance est de 65%.

Mots Clés :

reconnaissance, biométrie, ,SIFT ,empreinte digitale.

Abstract :

The uni-modal biometric systems suffer from several problems which are due to the origin of the use of a single biometric trait susceptible to noise, poor capture, poverty in terms of confidential biometric points and in particular the deterioration of the quality of the biometric entry. Introduction of biometric systems multi-modal is a solution to these problems.
We used SIFT algorithm for the extraction of characteristics, taking advantage of its robustness thanks to the invariability, scale and the rotation, more of its speed.
The multi-modal recognition process makes it possible to strengthen the biometric. systems under terms of security, reliability and relevance. Indeed, 100% were the overall recognitionrate for the proposed method while the former mentioned system we're rated as 65%.

Keywords :

recognition, biometrics, , SIFT, fingerprint.

Sommaire

CHAPITRE II

Transformation de caractéristique visuelles invariantes a l'échelle

CHAPITRE III

Résultat expérimental de SIFT algorithme

Liste des figures

Liste des tableaux

INTRODUCTION GENERALE

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance; aujourd'hui, la croissance internationale des communications (déplacement Physique, transaction financière, accès aux Services…) implique le besoin de s'assurer La conception d'un système d'identification fiable, efficace et robuste.

La lutte contre les fraudes d'informations personnelles, continue et les constructeurs de distributeurs automatiques s'engagent sur la voie de nouvelles technologies comme la biométrie. Il y a donc un intérêt grandissant pour les systèmes d'identification et d'authentification biométriques.
La biométrie utilise pour identifier une personne, ses propres caractéristiques physiques qui ne peuvent pas être changées, ni perdues ni encore volées.

En effet, les caractéristiques physiques d'un individu sont universelles (exister chez tous les individus), uniques (permettre de différencier un individu par rapport à un autre), permanentes (ne changent pas au fil du temps), enregistrables (collecter les caractéristiques d'un individu avec l'accord de celui-ci).

Dans le présent travail nous allons étudier un système d'Identification des personnes par la biométrie de la main, notre document est divisé en trois parties :

1. dans la première partie nous présentons une introduction a la biométrie et aux systèmes biométriques.
2. Dans la seconde nous allons voir l'algorithme SIFT (scale-invariant feature transform).

3. dans la dernière partie en va exposer les Résultats expérimental de SIFT algorithme

CHAPITRE I

Introduction à la Biométrie et aux Systèmes Biométriques

1. Introduction :

La biométrie est la science qui permet de reconnaître l'identité d'une personne sur la base de ses caractéristiques physiologiques, chimiques ou comportementales, telles que: le visage, l'iris, l'odeur, la façon de marcher ou la signature électronique…etc. Avec la nécessité de techniques solides de reconnaissance humaine dans les applications critiques, telles que: le contrôle d'accès sécurisé, le passage des frontières internationales et les applications légales, la biométrie se positionne comme une technologie viable qui peut être intégrée dans les systèmes de management d'identité à grande échelle. Les systèmes biométriques fonctionnent en vertu du principe que la plupart des caractéristiques biologiques de l'être humain soient distinctives pour chaque individu, puissent être acquises d'une manière fiable à l'aide des capteurs convenables et peuvent être représentées dans un format numérique. Ainsi, ces systèmes peuvent être considérés comme des moteurs de reconnaissance des formes et peuvent être incorporés dans divers marchés.

Dans ce chapitre, nous introduisons tout d'abord quelques notions et définitions de bases liées à la biométrie, nous décrivons le principe de fonctionnement d'un système biométrique ainsi que les outils d'évaluations utilisés pour mesurer leurs performances, nous donnons un bref aperçu des modalités biométriques les plus répandues, tout en accordant une attention particulière à la reconnaissance par signature parmi les autres modalités.[1]

2. Généralités et notions de bases en biométrie:

Les méthodes classiques d'authentification biométriques sont basées soit sur *une connaissance* à priori de la personne (ex., un mot de passe ou un code d'activation) ou sur *la possession* d'un objet (ex., une pièce d'identité, un badge ou une clef). Cependant, ce type de présentation d'identité peut être facilement perdu, partagé, oublié par son utilisateur ou deviné par d'autres personnes. Aujourd'hui, *la biométrie* est un domaine émergeant ou la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changé, perdues ou volées.

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. **La figure I.1** illustre un exemple de quelques modalités biométriques. **[1]**

Figure I.1 : Exemples de modalités (physiologiques et comportementales) [1]

3. Les modalités biométriques :

Il existe plusieurs modalités qui ont été utilisées dans plusieurs systèmes biométriques, Bien qu'il existe un très grand nombre de modalités biométriques, nous pouvons distinguer deux grandes catégories **figure I.2** :

a) La biométrie physiologique ou morphologique : Utilisant les caractéristiques physiologiques de l'individu (visage, main, oreille, empreinte digitale, la rétine …)

b) La biométrie comportementale : qui se base sur l'analyse de comportements d'un individu (la signature, la démarche, la voix …).

Nous allons aussi introduire quelques modalités cachées qui sont en cours d'expansion. **[1]**

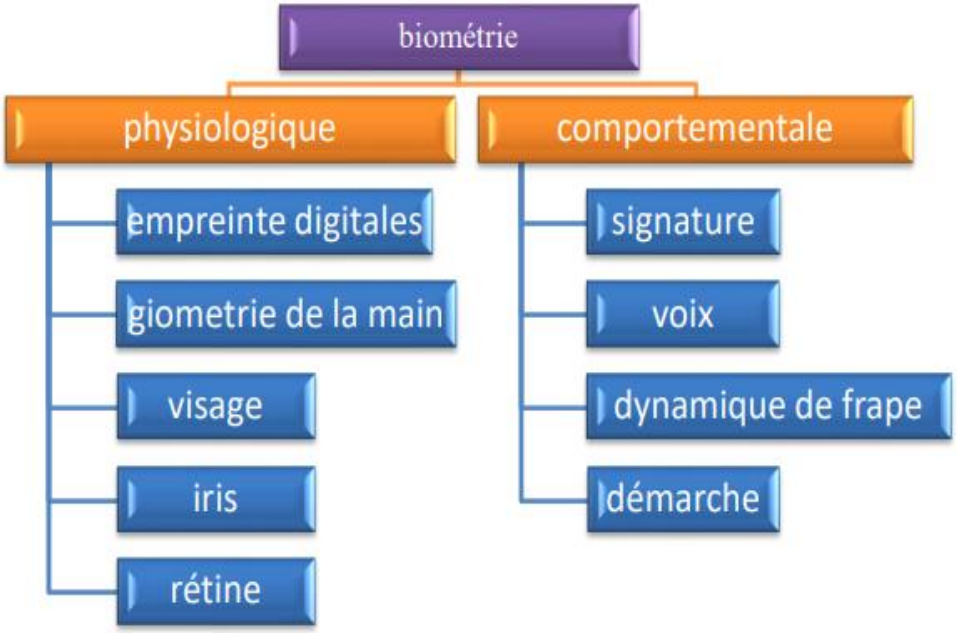


Figure I.2 : Catégories des méthodes d'identification biométriques. **[1]**

3.1. Modalités comportementale:

Dans ces techniques de reconnaissance, on s'intéresse aux caractéristiques physiques en activité des individus qui peuvent être typiques et permettent de distinguer une personne d'une autre, Dans la suite, nous présenterons quelques modalités de ce type avec leurs modes d'utilisations :

i. La signature :

L'identification par signature comme technique était parmi les premières utilisées dans le demain de la biométrie et le moyen le plus accepté et le plus utilisé pour authentifier des documents. Elle a été acceptée comme une méthode d'authentification légale par les

Les systèmes de vérification de signatures se base sur deux catégories selon le type d'acquisition des données : en ligne ou online, hors-ligne ou offline. Les systèmes online traitent les signatures, qui sont produites à l'aide d'une tablette à digitaliser, comme étant un signal dynamique et font l'extraction de plusieurs caractéristique comme les points de pauses, la pression, la direction, la vitesse pendant la signature et l'angle d'inclinaison.

Ces caractéristiques dynamiques sont spécifiques à chaque individu D'autre part, les systèmes offline traitent la signature à partir d'une image provenant d'un scanner.

Ces systèmes sont assez complexes du a l'absence de caractéristiques dynamiques stables. Dans notre travail on a travaillé sur deux bases offlines MCYT-75 et GPDS. [1]

ii. La dynamique de frappe au clavier :

Cette modalité est une caractéristique comportementale n'est pas unique pour chaque individu, Les paramètres suivants sont généralement pris en compte par les systèmes de reconnaissance de cette modalité : la position de l'utilisateur par rapport au clavier et le type du clavier utilisé, la vitesse de frappe, la suite de lettres, la mesure des temps de frappe, la pause entre chaque mot et la reconnaissance de mot(s) précis. La différence avec ces systèmes se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux, soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence). Ces techniques sont assez satisfaisantes, mais restent néanmoins statistiques. **[1]**

iii. La démarche :

Elle se réfère à la manière dont une personne marche et c'est l'une des rares modalités biométriques qui peuvent être utilisées pour reconnaître des personnes à distance. On cherche ici à identifier un individu par sa façon de marcher et de bouger tout en analysant des images vidéo de la promenade du

Les gens montrent de différents traits tout en marchant comme le maintien du corps, la distance entre les deux pieds, la position des joints tels que les genoux et les chevilles et les angles de balancement ce qui aide de manière significative à les identifier. Cette modalité est notamment appropriée pour les applications de vidéosurveillance. Les performances des systèmes à base de la démarche ne sont pas assez acceptables, car elles sont affectées par le changement de l'environnement. **[1]**

iv. La voix :

La voix est considérée comme une combinaison entre les caractéristiques biométriques physiques et comportementale. Les caractéristiques physiques de la voix d'un individu sont basées sur la forme et la taille des appendices (ex., les tractus vocaux, la bouche, les cavités nasales et les lèvres) qui sont utilisées dans la synthèse du son. Ces caractéristiques physiques de la parole humaine sont invariantes pour chaque individu, par contre, l'aspect comportemental de la parole se change au cours du temps en raison de l'âge, des conditions médicales (ex., rhume) et de l'état émotionnel. La voix n'a pas été connue comme une modalité très distinctive et n'est pas appropriée pour une identification à grande échelle.

Un système de reconnaissance vocale de type texte-dépendant est basé sur l'expression d'une phrase fixe et prédéterminée. Par contre, un système de reconnaissance vocale de type texte-indépendant identifie un individu à la base de ce qu'il parle. L'implémentation des systèmes de type texte-indépendant est plus difficile

par rapport aux systèmes de type texte-dépendant, mais elle offre plus de sécurité et protection contre les attaques malveillantes. L'inconvénient des systèmes de reconnaissance vocale est que les caractéristiques de la parole sont sensibles à certains facteurs comme le bruit. La reconnaissance vocale est plus appropriée dans les applications qui se basent sur le téléphone malgré la dégradation de la qualité de la voix, typiquement, à travers le canal de transmission. **[1]**

3.2. Modalité physiologique (morphologique):

Ces types de reconnaissance mesurent une caractéristique spécifique de la structure ou de la forme d'une partie du corps humain. Nous pouvons citer les exemples les plus connus :

i. L'empreinte digitale :

L'être humain a utilisé les empreintes digitales, depuis plusieurs décennies, en criminalistique et en identification biométrique. Le taux d'identification à l'aide d'empreintes digitales a été montré d'être très élevé. Une empreinte digitale est le motif de crête et de vallées sur la surface au bout d'un doigt. L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les corps policiers utilisent cette technique depuis plus de 100 ans. Aujourd'hui, les empreintes digitales sont recueillies sur une scène de crime et sont ensuite comparées à celles contenues aux base de donné.

L'empreinte digitale est une impression produite par la transpiration, la graisse, l'huile ou l'encre présente dans les lignes de crêtes non uniformes contenues dans la partie supérieure de chaque doigt de main d'un être humain. Ces empreintes sont uniques pour chaque individu. Même des jumeaux parfaits n'ont jamais des empreintes digitales identiques. **[1]**

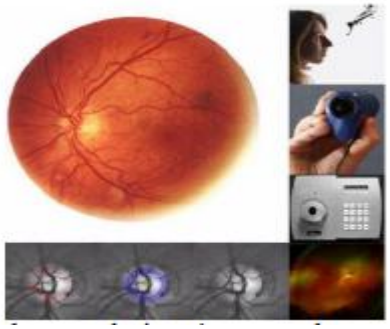
ii. La géométrie de la main :

La biométrie par cette modalité extrait près d'une centaine de paramètres comme les épaisseurs, les longueurs, les surfaces et les largeurs des doigts de la main. La géométrie de la main n'est pas connue comme une modalité très distinctive, ainsi les systèmes de reconnaissances basés sur cette modalité ne peuvent pas être utilisés pour identifier un individu à partir d'une grande population. En outre, les informations de la géométrie de la main sont variantes durant la période de croissance des enfants.

L'acquisition de cette modalité ne nécessite aucune lecture d'empreintes et la mesure des épaisseurs des doigts s'effectue à l'aide de miroirs ce qui veut dire que l'acquisition s'effectue en trois dimensions. La taille du capteur est le major inconvénient de cette modalité. De plus, ce capteur coute très cher par rapport aux autres modalités. Tous ces inconvénients réduisent l'utilisation de cette technique biométrique. Il existe aussi des

systèmes d'authentification qui se basent uniquement sur la mesure de quelques doigts au lieu de la main entière; ces appareils sont plus petits que ceux utilisés pour la géométrie de la main. **[1]**

iii. La rétine :



Cette technologie est bien adaptée aux applications de aute sécurité (sites militaires, salles de coffres forts, etc). ors de l'acquisition, l'utilisateur place son œil à proximité u capteur où un rayon lumineux illumine le fond de l'oeil our extraire des points repères. La détermination des aractéristiques de la rétine consiste à l'extraction de la istribution géographique des vaisseaux sanguins. Cette iesure est richesse de caractéristique plus de 400

Cependant, la rétine n'est pas appropriée pour une grande population à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres). En outre, des risques liés à la santé sont signalés, ce qui réduit l'utilisation de cette modalité. **[1]**

iv. Le visage :

La reconnaissance par cette modalité s'effectue de façon spontanée dans la vie quotidienne des êtres humains. L'authentification par le visage est la technique la plus commune et la plus populaire puisqu'elle correspond à ce que nous utilisons naturellement pour reconnaître une personne. Les caractéristiques qui servent à la reconnaissance du visage sont : les yeux, la bouche, la forme du visage (contour), etc

Dans un système de reconnaissance faciale, la photo d'une personne est prise volontairement ou involontairement à l'aide d'une caméra. Puis, un ensemble de caractéristiques propres à chaque individu est extrait (le tour du visage, la position des oreilles, les coins de la bouche, l'écartement des yeux et la taille de la bouche) à partir de la photo. Ces systèmes sont capables de faire face aux techniques de spoofing comme le port de lunettes, la barbe, le maquillage, etc. **[1]**

v. L'iris :

L'iris est la région annulaire de l'œil délimitée par la pupille et la sclérotique. La texture complexe de l'iris comporte des informations très distinctives et utiles pour différencier et reconnaître les individus, donc elle est considérée comme la modalité la plus précise pour l'identification et l'authentification .Son seul inconvénient est son coût assez élevé, ce qui ne la rend pas autant répondu pour des applications quotidiennes.

Alors, son utilisation s'est limitée dans des endroits où la sécurité est primordiale et même critique comme dans les bases nucléaires par exemple. La reconnaissance par l'iris est utilisée aussi dans le secteur financier pour les employés et les clients, dans les hôpitaux et dans les grands aéroports. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris est prise par une caméra. Ensuite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données. **[1]**

vi. L'oreille :

Au cours de plusieurs années, l'oreille humaine a été utilisée comme un moyen d'identification en médecine légale. L'oreille humaine possède une richesse d'information qui se situe sur une surface 3D incurvée, cette richesse d'information a attiré l'attention des scientifiques légaux.

Les images d'oreilles peuvent être acquises simultanément avec les images du visage et employées ensemble pour améliorer d'une manière significative la précision de la reconnaissance. Il est possible aussi d'employer l'oreille et le visage comme une pièce complémentaire d'information.

Les recherches ont légèrement évolué pour développer des technologies automatisées d'identification par oreille. Cependant, des efforts significatifs sont encore exigés pour améliorer la détection d'oreille, la segmentation et la possibilité d'identification dans le but de faire un déploiement dans la surveillance et dans les autres applications commerciales. **[1]**

4. Comparaison entre les modalités biométriques :

D'après la description précédente des différentes modalités biométriques, on a pu constater que chacune d'entre elles présente des avantages et des inconvénients et que certaines applications nécessitent de choisir une modalité à l'égard d'une autre. Ce choix s'effectue essentiellement en tenant compte d'un nombre de paramètres comme l'origine de l'application, son coût, les performances espérées du système et l'acceptation de la modalité par l'utilisateur.

Dans **la figure I.3,** on a effectué un classement des différentes modalités biométriques selon deux axes : la performance et le coût. Les systèmes à base de la voix ou du visage ne sont pas couteux, mais leurs performances restent limites. Les modalités de la biométrie cachée sont incontestablement les modalités les plus performantes. En revanche, les systèmes à base de ces modalités sont très coûteux à cause du prix élevé des dispositifs d'acquisition. **[1]**

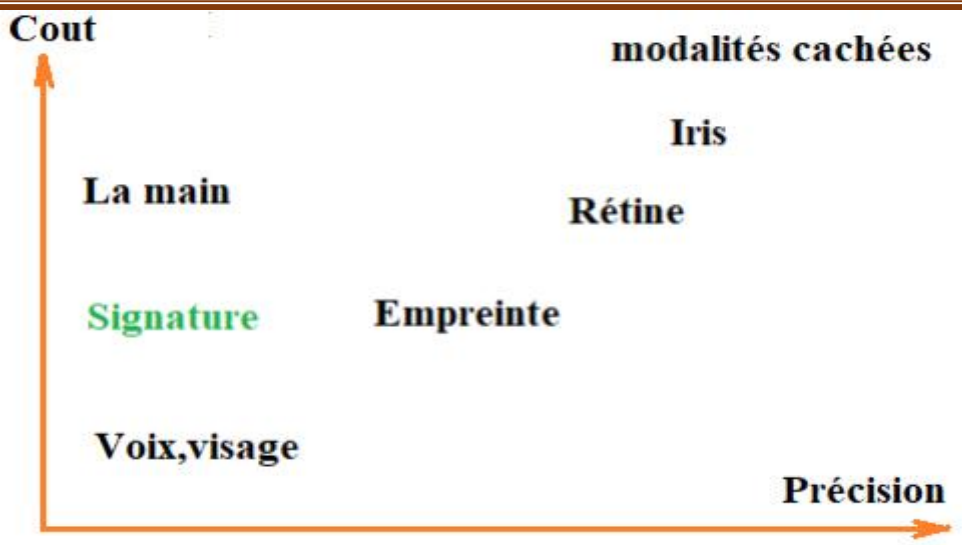


Figure I.3 : Classement des modalités biométriques selon le cout et la précision. **[1]**

5. Architecture fonctionnelle d'un système biométrique :

Un système biométrique est généralement composé de deux principaux modes **(voir la Figure I.4)** qui sont le mode d'apprentissage appelé également mode d'enregistrement ou d'enrôlement et le mode de reconnaissance (vérification ou identification). Le premier mode consiste à enregistrer dans une base de données les caractéristiques physiques ou comportementales d'un individu sous forme d'un "Modèle" biométrique appelé aussi "Template" ou "Signature". Le deuxième mode consiste à tester les mêmes caractéristiques et à les comparer avec les modèles biométriques stockés dans la base de données. Si les données testées correspondent à un modèle biométrique enrôlé, l'individu est donc considéré comme reconnu. **[1]**

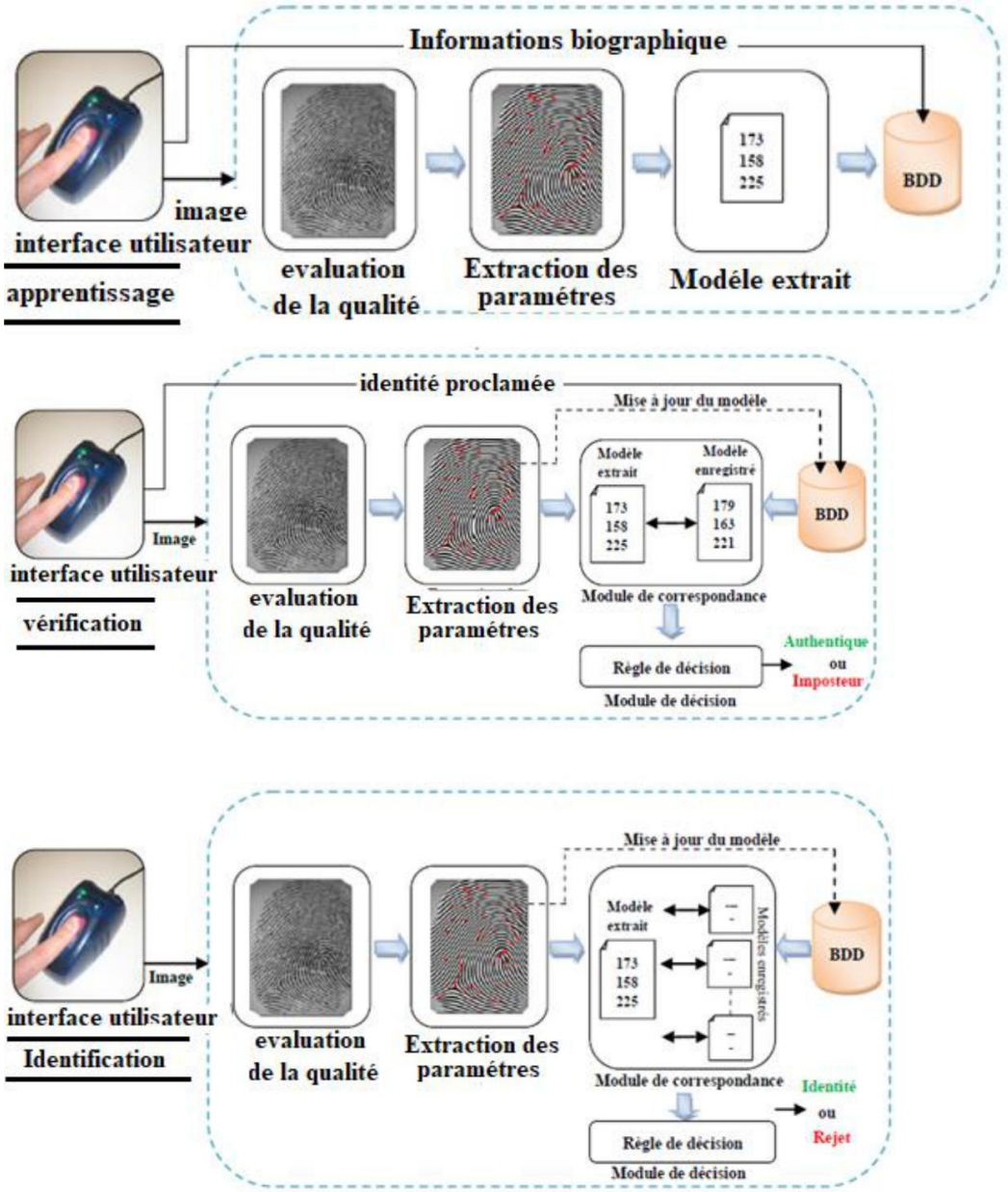


Figure I.4 : Architecture fonctionnelle d'un système biométrique. Diagramme des processus d'apprentissage, vérification et identification. **[1]**

6. Caractéristiques de la biométrie :

Comme nous l'avons dit précédemment, les modalités biométriques doivent être déterminées par quelques caractéristiques en but d'assurer leurs fiabilités, Chaque modalité possède ses propres avantages et inconvénients, le choix d'une modalité biométrique pour une application donnée dépend d'une variété de paramètres liés à la nature et les exigences de l'application et aux propriétés de la modalité , ont identifié quelques paramètres généralement employés dans une application biométrique, qui sont:

a. Universalité: tout individu, qui accède à une application, doit posséder le trait, donc la modalité doit exister chez tous les individus.

b. Unicité: Le trait biométrique doit être suffisamment différent d'une personne aux autres.

c. Stabilité: Le trait biométrique d'un individu doit être suffisamment stable et invariant au cours du temps.

d. Mesurabilité: il devrait être possible de numériser les données biométriques à l'aide d'un dispositif d'acquisition.

e. Performance: Signifie que l'authentification doit être précise et rapide.

f. Acceptabilité: Indique que la modalité biométrique utilisée doit être bien accepté par les utilisateurs du système.

Il n'existe aucun trait biométrique exceptionnel qui satisfait et répond efficacement à toutes les exigences mais à des degrés différents.

Tableau I.1 montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Le choix de la modalité est ainsi effectué selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des individus. **[1]**

Type	modalité	précision	Simplicité d'utilisation	Acceptation par l'utilisateur
morphologique	empreinte	Haute	Moyenne	Basse
	Iris	Haute	Moyenne	Moyenne
	Rétine	Haute	Basse	Basse
	Visage	Basse	Haute	Haute
	Voix	Moyenne	Haute	Haute
	Géométrie de la main	Moyenne	Haute	Moyenne
comportementale	Frappe au clavier	Basse	Haute	Moyenne
	Démarche	Basse	Moyenne	Moyenne
	Signature	Moyenne	Moyenne	Haute
cachée	ECG, EMG	Haute	Moyenne	Moyenne
	Cerveau	Haute	Basse	Basse
	Imagerie par rayon x	Haute	Basse	Basse

Tableau I.1 : Comparaison entre les modalités biométriques**. [1]**

7. Les systèmes biométriques et leurs modes de fonctionnements :

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique ou comportementale. Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : analyse basée sur la morphologie, analyse de traces biologiques, l'analyse comportementale. Après l'extraction de ces caractères, le système biométrique compare ces derniers par rapport aux modèles stockés dans la base de données et exécute une action basée sur le résultat de la comparaison. Par conséquent, un système biométrique générique peut être vu comme un processus à quatre modules principaux : un module de capture, un module de prétraitement et d'extraction des caractéristiques, un module de correspondance et un module de décision **figure I.5**. Le fonctionnement de chaque module est détaillé ci-dessous.[1]

7.1. Le module de capture : est responsable de l'acquisition des données biométriques d'un individu (cela peut être un : un lecteur, un scanner biométrique, une caméra ou un module de balayage approprié est requis pour la détection des donnée biométrique d'un individu). [1]

7.2. Le module prétraitement d'extraction de caractéristiques : les donnée biométrique obtenue lors de la première phase doit être évaluée par ce module et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes. [1]

7.3. Le module de correspondance : Le vecteur des caractéristiques, extrait, est comparé avec les modèles stockés dans la base de données pour générer des scores de correspondances. Le résultat de cette comparaison va être utilisé pour prendre une décision sur le taux de correspondance de la signature biométrique, inscrites dans la base de données (MCYT, GPDS) pour la validation ou le rejet de l'identité de l'individu à reconnaitre. Donc il compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.[1]

7.4. Le module de décision : vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés (bases de données). [1]

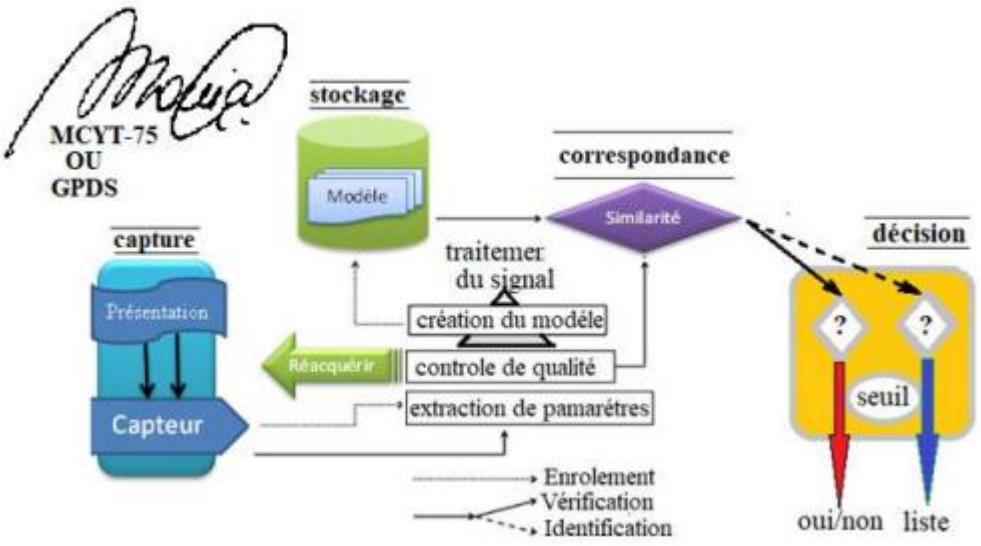


Figure I.5 : les modules principaux d'un système biométrique**. [1]**

8. Performances d'un système biométrique :

Dans les systèmes basés sur les mots de passe, une correspondance parfaite est nécessaire entre les deux chaînes de caractères pour valider l'identité d'un individu. Par contre, les systèmes biométriques rencontrent rarement deux modèles biométriques d'un même utilisateur présentant exactement les mêmes vecteurs de caractéristiques, en raison de: mauvaises conditions (ex., une empreinte digitale qui contient un bruit lié à un défaut du capteur), changements des caractéristiques biométriques de l'utilisateur (ex., une maladie respiratoire effectuant la reconnaissance du speaker), changements des conditions ambiantes (ex., le changement du niveau d'illumination en reconnaissance par visage) et variations en interaction utilisateur-capteur (ex., iris occlue ou empreinte digitale partielle). Il est donc rare d'avoir deux modèles biométriques exactement similaires provenant du même utilisateur. En effet, une correspondance parfaite entre deux vecteurs de caractéristiques peut indiquer la possibilité qu'il y ait une attaque malveillante lancée contre le système. **[1]**

9. Vérification et identification :

Un système biométrique peut fonctionner en mode vérification ou en mode identification **(voir Figure I.2).**

✓ Dans la phase de vérification, le système évalue l'identité d'une personne en comparant les données biométriques capturées avec son (ses) propre(s) modèle(s) enregistré(s) dans la base de données du système. Dans ce type d'application, un individu qui veut être reconnu par le système doit proclamer son identité, habituellement, par son numéro d'identification personnelle (PIN), par son nom d'utilisateur ou par sa carte magnétique, le système effectuera une comparaison de type un-contre-un pour déterminer si cette proclamation est vraie ou fausse. La vérification est typiquement utilisée pour une reconnaissance positive afin d'empêcher l'utilisation d'une même identité par plusieurs personnes.

✓ En mode identification, le système identifie un individu en recherchant le modèle enrôlé qui représente la meilleure correspondance parmi tous les modèles d'utilisateurs stockés dans la base de données. Par conséquent, le système effectue une comparaison de type un-contre-tous afin d'établir l'identité de cet individu. L'identification est une composante essentielle pour les applications de reconnaissances négatives; l'objectif de ce type de reconnaissance est d'empêcher l'utilisation de plusieurs identités par un seul individu. Comme les méthodes traditionnelles de reconnaissances d'individus telles que les mots de passe et les possessions peuvent fonctionner en mode positif, le mode négatif peut être uniquement établi à l'aide de la biométrie.

Dans les systèmes biométriques, la correspondance n'est pas absolue. Ceci est dû à :

- Des conditions imparfaites lors de l'acquisition des échantillons biométriques (ex. : empreinte digital bruitée).
- Des variations de la caractéristique biométrique de l'utilisateur.
- Des changements des conditions ambiantes.
- La différence dans l'interaction de l'utilisation avec les dispositifs d'acquisition (ex. : iris occlus).

Cependant, il est très rare d'obtenir un ensemble de caractéristiques exactement similaires lors de deux acquisitions d'échantillons biométriques d'un individu. En effet, une correspondance parfaite de deux échantillons déclenche une mise garde du systèmecontre une tentative de fraude par reproduction.

Le degré de similitude entre deux ensembles de caractéristiques est appelé : le taux de similarité (similarity score). Le taux de similarité d'une comparaison entre deux échantillons d'un trait biométrique du même individu est appelé : taux d'authenticité (genuine score ou authentic score). Le taux de similarité entre deux échantillons de deux individus différents est appelé : taux d'imposture (impostor score).

Comme montré sur **la figure I.6 (a),** il est question d'un compromis, défini par un seuil, entre le taux de fausses acceptations et le taux des faux rejets. C'est –à-dire qu'un taux d'authenticité en dessous du seuil généré un faux rejet, tandis qu'un taux d'imposture qui dépasse le seuil résulte une fausse acceptation.

La performance d'un système biométrique est quantifiée par le taux de deux erreurs fondamentales définies par :

- **Le Taux de Faux Rejets (False-Rejection Rate), noté FRR :** il exprime le pourcentage des utilisateurs authentiques faussement rejetés par un système biométrique. En d'autres termes, ce taux représente les données de test authentiques qui ont été incorrectement rejetées et considérées comme des imposteurs. FRR est aussi nommé: False Non-Match Rate (FNMR).
- **Le Taux de Fausses Acceptations (False-Acceptance Rate), noté FAR** : il exprime le pourcentage des utilisateurs imposteurs faussement acceptés par un système biométrique. En d'autres termes, il représente les données de test imposteurs qui ont été incorrectement acceptées et considérées comme authentiques.

En pratique, la valeur du FAR est affectée par le nombre de fausses acceptations (FA) divisé par le nombre de tests imposteurs dans la base de données (N). Tandis que, la valeur du FRR est affectée par le nombre de faux rejets (FR) divisé par le nombre de tests authentiques

(M). En plus, les deux taux FAR et FRR sont dépendants du seuil de décision θ fixé dans le module de décision. En effet, en faisant varier la valeur des deux taux d'erreurs d'une manière importante. Le calcul du FAR et FRR en fonction de θ est donné par :

$$F(\theta) = FA(\theta) / N \qquad \textbf{(I.1)}$$

$$F(\theta) = FR(\theta) / M \qquad \textbf{(I.2)}$$

Le choix optimal de la valeur du seuil de décision θ est très important puisqu'il influe directement sur la performance et la fiabilité du système biométrique. En effet, une valeur élevée du seuil θ entraîne l'apparition d'un grand nombre de faux rejets, par contre d'une faible valeur du seuil, résulte un nombre important de fausses acceptations. La valeur la plus optimale du seuil θ pour faire un équilibre entre le FRR et le FAR correspond à l'endroit où le FAR = FRR est noté par le point d'équivalence des erreurs (Equal Error Rate (EER)); ce dernier est déterminé par le point d'intersection entre la courbe des taux de fausses acceptations et la courbe des taux des faux rejets. Un exemple de détermination du point EER est illustré dans **la figure I.6 (a).**

Les deux taux FRR et FAR en différentes valeurs du seuil θ peuvent être récapitulés en utilisant la courbe : Receiver Operating Characteristic (ROC) . Cette courbe trace le taux de faux rejets en fonction du taux de fausses acceptations. Elle sera tracée d'une manière paramétrique en fonction des valeurs du seuil θ. Un exemple de détermination du point EER en utilisant la courbe ROC est illustré dans **la figure I.6 (b)** Plus cette courbe tend à rapprocher la forme du repère, plus le système est performant, c'est-à-dire qu'il possède un taux de reconnaissance global élevé. **[1]**

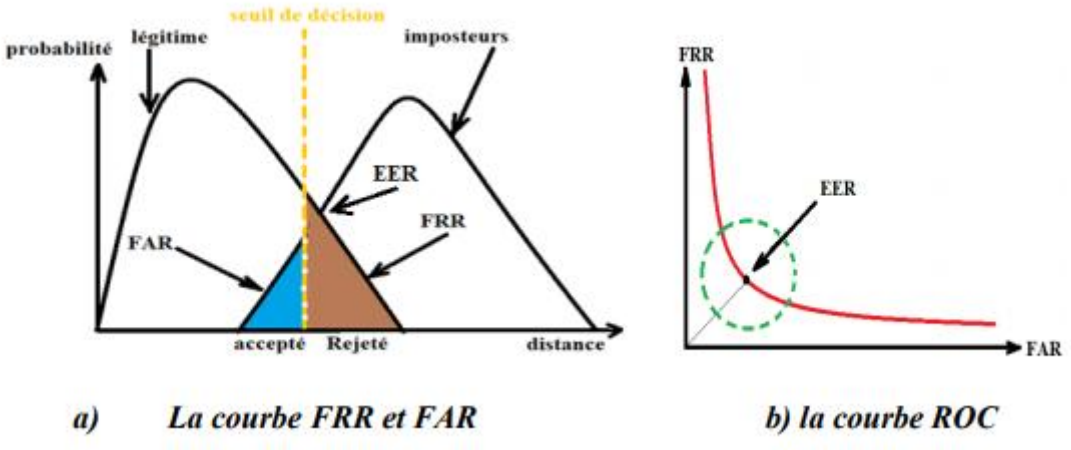


Figure I.6 : Courbes représentatives des taux de similarité FRR, FAR**. [1]**

10.Modalités cachées

Dans cette partie, nous discutons une idée qui consiste à l'utilisation de la biométrie médicale dans le cadre d'authentification, donc au lieu de reconnaître un individu en utilisant ces modalités morphologiques ou physiologiques (signature, empreinte, visage … etc.) on utilise des traits inaccessibles tel que : les motifs du cerveau, la texture de l'os, **ECG** … Ce type est en cours d'exploration, s'appelle "la biométrie cachée", les

modalités cachées considèrent plutôt les caractéristiques intrinsèques et non visibles du corps humain sois un signal physiologique ou bien un organe humain est considéré comme un candidat pour des applications biométriques. Dans la première catégorie Nous pouvons employer l'électrocardiogramme (**ECG**), l'électromyogramme (**EMG**). Ainsi, Dans la deuxième catégorie, nous pouvons considérer, comme exemple la morphologie ou la texture du cerveau humain. Nous présentons par la suite quelques idées et travaux réalisés dans ce domaine. Ce type reste inconvenable, il est difficile d'employer ce type de biométrie pour sécuriser ou accéder à des ressources informatiques. La contrainte principale dans le système d'acquisition c'est la visualisation de la forme du cerveau nécessite l'utilisation des scanners **MRI** (Magnetic Resonance Imaging) et la visualisation du squelette du corps, contenant le crâne et les autres os, nécessite l'usage des scanners de rayons **X**. **[1]**

10.1. Utilisation des images IRM en biométrie de cerveau :

Dans les applications médicales, l'IRM est une technique employée pour visualiser des organes du corps humain (cerveau, muscles, et cœur ...) avec une résolution relativement élevée. Ceci est rendu possible avec l'utilisation d'un champ électromagnétique puissant et constant, produit par un supraconducteur. L'objectif de cette section est de présenter l'utilisation des images **MRI** du cerveau humain dans l'identification des individus **figure 1.7 (a et b)** et cherche à caractériser le cerveau humain à travers des images **IRM 2D** et **3D**. **[1]**

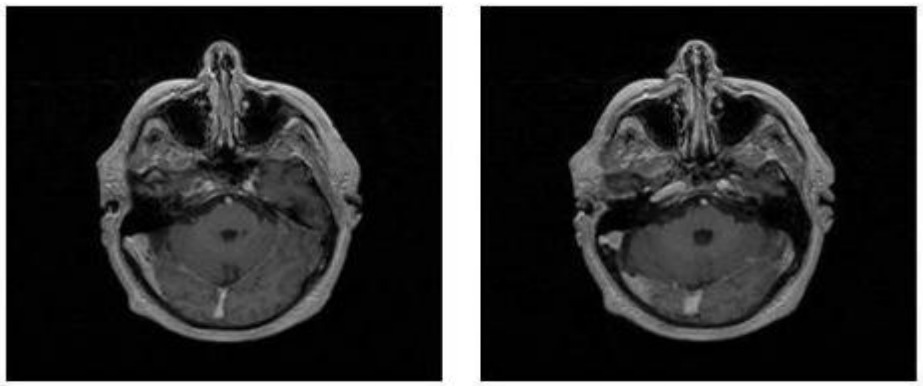


Figure I.7 : Deux images MRI du cerveau humain qui montrent une différence visuelle entre deux individus : (a) individu 01, (b) individu 02. **[1]**

Depuis les images **IRM 2D (Figure I.8.a),** on peut faire la reconstruction en **3D(Figure I.8.b)** du cerveau pour avoir des informations sur la texture. Ainsi d'autres caractéristiques géométriques du cerveau peuvent être considérées comme le rapport isopérimètre et la courbure extérieure corticale. En fait, la quantité de paramètres qui peuvent être extraits à partir d'une image du cerveau **3D** est plus grande que ce que nous pouvons extraire à partir d'autres modalités classiques. On peut aussi définir ce qu'on appelle brain code ou code du cerveau à travers une segmentation de la zone d'intérêt du cerveau **(Figure I.8.c) [1]**

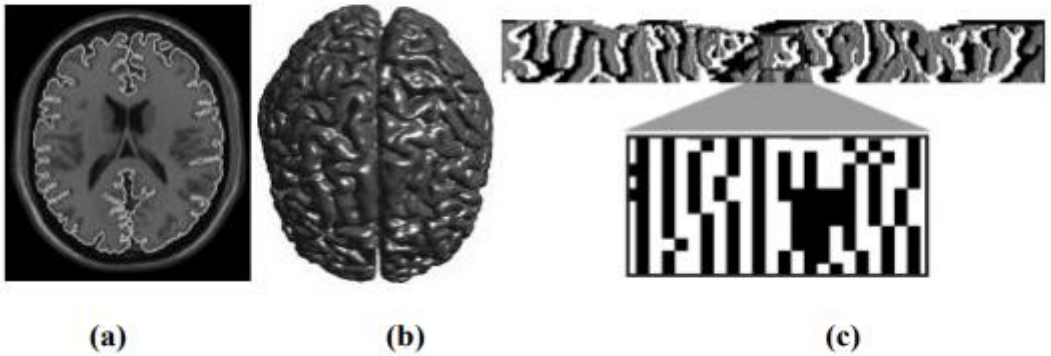


Figure I.8 : Biométrie du cerveau avec des images IRM : (a) Extraction des textures de cerveau par segmentation (b) reconstruction de 3D d'image de cerveau montrant les circonvolutions qui peuvent être employées pour identifier des individus (c) extraction du Brain Code**. [1]**

L'avantage principal de ce type de modalité cachée est le fait que le cerveau est totalement protégé contre toutes sortes de changements. Cependant, l'inconvénient principal de cette modalité est la non-disponibilité de systèmes d'**IRM** robuste consacrés à la biométrie. **[1]**

10.2. Biométrie avec des images de rayon X :

La biométrie cachée a été aussi prolongée vers l'utilisation des images de rayons **X**. Elle permet d'obtenir un cliché dont le contraste dépend à la fois de l'épaisseur et du coefficient d'atténuation des structures traversées. Nous présentons, dans les **figures I.9 (a et b),** deux images **X**-ray de poumons qui correspondent à deux individus différents. Les différences en termes de textures et en morphologies peuvent être remarquées facilement. Dans ce cas, l'extraction des caractéristiques par l'utilisation de quelques techniques appropriées de traitement d'images peut être facilement employée pour différencier entre les individus

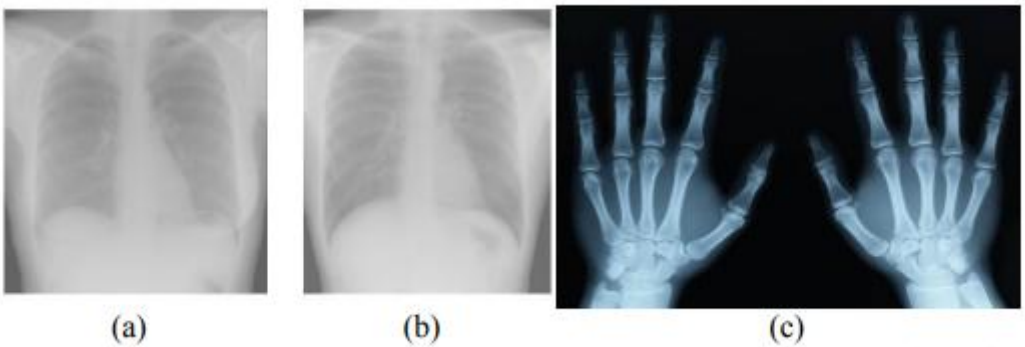


Figure I.9 : Biométrie cachée appliquée sur les images X-ray. (a) et (b) deux images X-ray des poumons de deux individus différents. (c) Biométrie de la main avec des images à rayon X.**[1]**

Une autre application potentielle de la biométrie cachée qui utilise les images **X-ray** de la main est présentée dans la **figure I.9 (c).** Cette méthode est plus efficace et robuste par rapport à la biométrie classique qui utilise les empreintes palmaires. Dans ce type d'application, les paramètres géométriques peuvent être facilement extraits et modélisés.

Pour chaque individu. **[1]**

10.3. Electrocardiogramme ECG :

L'ECG est un signal représentant l'activité du cœur. Il est principalement employé dans des applications cliniques pour diagnostiquer les maladies cardio-vasculaires. Le signal d'ECG est caractérisé par la forme de ses battements composés de cinq vagues typiques, à savoir P, Q, R, S, et T ou parfois la vague U **(figure I.10(a et b).** La biométrie par **ECG** a fait l'objet d'un certain nombre de travaux. L'utilisation de l'ECG en biométrie est relativement nouvelle. En fait, il existe plusieurs méthodes biométriques basées sur l'**ECG**. Il y a des approches qui sont basées sur l'analyse de **l'ECG.** D'autres basées sur l'intégration des caractéristiques analytiques et d'apparence extraite des signaux **ECG**. **[1]**

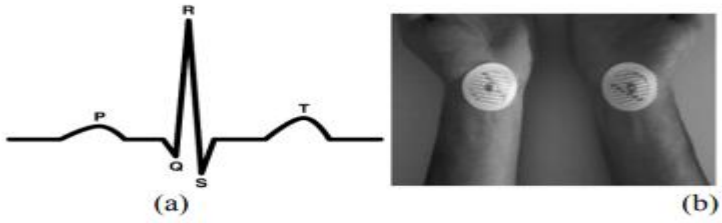


Figure I.10 : Biométrie par ECG : (a) Signal d'ECG avec le rythme régulier (b) positionnement des électrodes sur les avant-bras pour la capture d'ECG**. [1]**

10.4. Electromyogrammes EMG :

Les signaux électromyogrammes (**EMG**) sont des signaux bioélectriques enregistrés fournissent des informations diverses sur l'état des nerfs et des muscles, dans ce contexte, quelques expériences récentes ont été réalisées. Lors de l'acquisition de ces signaux, les individus sont invités à appliquer une pression manuelle d'une intensité constante sur une sonde de force pendant plusieurs secondes (**Figure I.11**). Le signal ainsi obtenu est analysé dans le domaine spectral. Puis, des paramètres sont extraits comme la puissance du signal, la fréquence moyenne, le coefficient d'aplatissement et le coefficient de dissymétrie. En effet, ces paramètres fournissent un vecteur de dispositif que nous pouvons employer pour caractériser des individus.

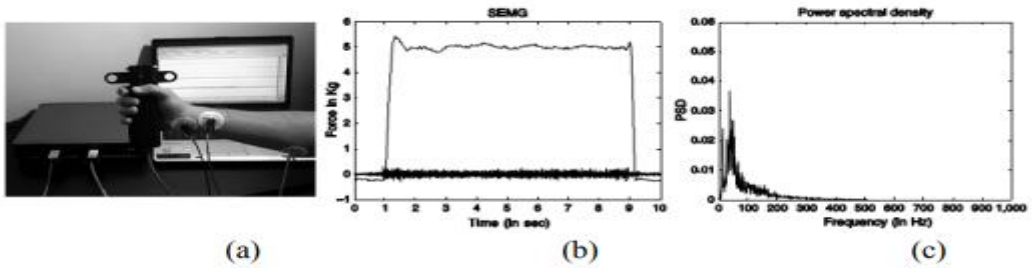


Figure I.11 : Biométrie par l'EMG: (a)Acquisition d'un signal EMG(b) L'intensité appliquée par l'utilisateur et l'EMG relatif (c)périodogramme d'EMG**. [1]**

11.Applications de la biométrie :

La nécessité des techniques d'authentification fiables est augmentée suite aux préoccupations croissantes qui concernent la sécurité et les progrès rapides en communication, réseau et mobilité. Ainsi, la biométrie est de plus en plus intégrée dans diverses applications ou bien pouvant être classées en trois groupes principaux qui sont:

a. Applications commerciales : telles que l'accès à un réseau d'ordinateurs, la sécurité des données électroniques, le e-commerce, l'accès d'internet, l'utilisation des cartes de crédit bancaire, le contrôle d'accès physique, mobile phone, la gestion des registres médicaux ou l'apprentissage à distance, etc.

b. Applications gouvernementales : telles que les cartes d'identité (ID cards), la sécurité sociale, le contrôle des frontières, le contrôle des passeports, le déboursement en assistance sociale ou en permis de conduite, etc.

c. Applications légales : telles que l'identification des corps humains, les enquêtes criminalistiques ou la détermination parentèle, etc. **[1]**

12.Conclusion :

A travers ce premier chapitre, nous avons présenté un état de l'art sur la biométrie, ses propriétés, le principe de fonctionnement des systèmes biométriques, les différentes modalités ainsi que les critères d'évaluation des performances de ce type de systèmes. Ensuite, nous avons mis en évidence une comparaison entre ces modalités biométriques, tout en accordant une attention particulière à la reconnaissance par signature, puisqu'elles constituent un bon choix, en termes de praticabilité, robustesse, acceptabilité. Finalement, nous avons terminé le chapitre par une brève présentation de la biométrie cachée comme nouvel axe de recherche en criminalistique et en sécurité biométrique, qui constitue un défi très important que nous voulons exploiter dans un futur travail, par l'application et le développement des descripteurs de texture locaux proposés. **[1]**

CHAPITRE II

Transformation de caractéristique visuelles invariantes a l'échelle(Sift)

1. Introduction :

Omniprésents, les ordinateurs effectue a longueur de journée des tâches répétitives. Ils aident ainsi l'homme a manipuler d´énormes quantités de données, souvent même plus rapidement et plus précisément que lui. Malgré cela, la capacité des ordinateurs demeure limitée lorsqu'il s'agit d'extraire automatiquement des informations d'images ou de vidéos, qui représentent pourtant des volumes déponnées extrêmement importants. Le traitement automatisé de ces données ouvrirait la voie à beaucoup d'opportunités. La discipline qui vise a automatisé la compréhension des images, la vision par ordinateur, est une branche de l'intelligence artificielle dont l'objectif est précisément de permettre à une machine de comprendre ce qu'elle voit lorsqu'on la connecte a une ou plusieurs caméras. Nos travaux se situent au cœur de cette discipline. Cette discipline a connu un intérêt grandissant avec la montée en flash du nombre d'images numériques grâce au d´développement de la vidéosurveillance et a la démocratisation des appareils photos numériques, des téléphones et des réseaux permettant leur ´échange (a peu près 5 Milliards de photos sont hébergées sur le site Flickr et 2.5 Milliards nouvelles photos par mois sont ajoutées au site Facebook).Dans ce vaste domaine qu'est la vision par ordinateur, nous nous intéressons ici a la sous-discipline qu'est la reconnaissance d'objets, et plus particulièrement a la localisation de classes d'objets dans des images (par exemple localiser toutes les personnes présentes dans une image). Ce type de technique combine des approches de traitement d'images et d'apprentissage automatique dans le but de mener à bien cette tache de reconnaissance des objets présents dans les images

2. Etat de l'art sur les approches de reconnaissance utilisant l'empreinte digitale :

Flom et Safir ont proposé l'idée du premier système biométrique basé sur l'iris Mais ils l'ont fait pour des conditions très contraintes comme, l'image doit être prise avec l'idéal Appui-tête, la personne doit regarder directement sur le système d'acquisition d'image et le manuel opérateur.

Le premier système de reconnaissance de l'iris a été développé par Daugman a utilisé des ondelettes en quadrature multi-échelles pour extraire la structure de phase de texture Informations de l'iris pour générer un iris code de 2048 bits et comparer la différence entre une paire de représentations d'iris en calculant leur distance de Hamming via le XORWildes [9], Boles et Boashash [8] sont parmi plusieurs autres qui ont proposé des algorithmes de reconnaissance de l'iris. Les auteurs de [8] ont représenté l'iris unique fonctions utilisant des passages à zéro par transformée en ondelettes.

Dans [7], Nosrati et al. Ont utilisé une méthodologie en 4 étapes pour extraire des formes circulaires d'arrière-plans. Dans un premier temps, ils effectuent un filtrage médian pour lisser l'image et supprimer le bruit de sel et de poivre. Dans l'étape suivante, un filtre laplacien est utilisé pour affiner le Bords flous et mettre en évidence les petits détails. La troisième étape implique l'application de Canny Détecteur de bord pour la segmentation d'image suivie de la 4ème étape dans laquelle Circular Hough Transform (CHT) est utilisé pour détecter les formes circulaires.

Dans [9], les auteurs ont utilisé Hough Transform pour la segmentation de l'iris, laplacienne de Gaussian (LoG) pour produire des modèles d'entités et une corrélation normalisée pour L'appariement.

3. Description de la méthode sift :

L'idée générale de cette méthode est de transformer une image en vecteurs de caractéristiques, lesquels doivent être dans l'idéal invariants aux transformations géométriques (rotation, mise à l'échelle), et dans une moindre mesure invariants à l'illumination.

Il s'agit de détecter des points remarquables (ou clés), qui vont permettre d'identifier un objet. La détection de ces points donne lieu à la mise en place des vecteurs de caractéristiques dont les composantes sont propres au point considéré.

3.1. Aperçu (overview) :

La détection et l'identification d'objets sont des sujets très importants dans le domaine de la vision par ordinateur. Comme les difficultés de ce projet que nous avons mentionnées, nous devons trouver une sorte de fonctionnalité moins sensible à la traduction d'image, à la mise à l'échelle, à la rotation, aux changements d'éclairage qui se produiront dans l'environnement de l'entrepôt. À l'échelle macroscopique, l'ensemble du travail est principalement divisé en deux étapes : la détection et l'identification des objets. Il est illustré à la figure II.1.

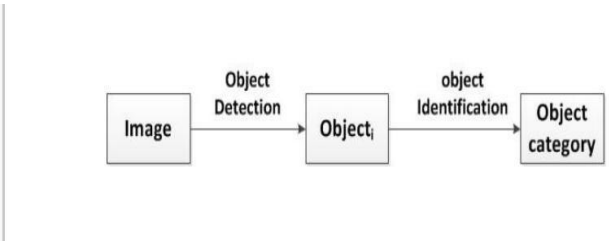


Figure II.1: L'organigramme de l'ensemble de l'approche. L'ensemble de la méthode de reconnaissance d'objets est développé en deux étapes: détection d'objet et identification d'objet.

L'organigramme de l'ensemble de l'approche. L'ensemble de la méthode de reconnaissance d'objets est développé en deux étapes : détection d'objet et identification d'objet. Pour l'ensemble du système, une image prise dans un environnement réel d'entrepôt contenant plusieurs objets à l'intérieur est donnée. À travers le processus de détection, pour chaque image, l'extraction des caractéristiques SIFT est appliquée en premier. Sur la base de ces caractéristiques extraites, une méthode de détection d'objets est développée. Dans l'étape de détection d'objet, la position de chaque objet détecté est obtenue. En fonction de la position de l'objet dans l'image, une zone de délimitation pour un objet détecté dans l'image de test est créée. À l'aide du modèle «Sac de mots», l'objet détecté sera classé dans sa classe d'appartenance. Il est illustré à la figure II.2.

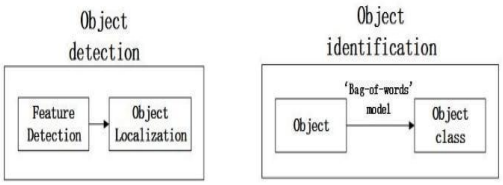


Figure II.2 : Processus de détection et d'identification d'objets.

3.2. Méthode SIFT Extraction de fonctionnalités :

SIFT Scale Invariant Feature Transforma (SIFT) est une approche pour détecter et extraire des descripteurs de caractéristiques locaux qui sont invariant pour l'illumination, la mise à l'échelle et la rotation de l'image. Cet algorithme a été proposé pour la première fois par Lowe [6]. Ces dernières années, il a été amélioré et développé. La fonction SIFT présente plusieurs avantages comme suit :

• caractéristiques naturelles des images. Ils sont invariants à l'échelle uniforme, l'orientation et partiellement invariants aux changements d'éclairage ;

• meilleure tolérance aux erreurs avec moins de correspondances ;

• avec une bonne efficacité et rapidité ;

• pratique pour combiner et générer des informations utiles. L'étape de détection de la fonction SIFT est divisée en 4 étapes :

1. Détection des extrema d'espace d'échelle :

À ce stade, dans un premier temps, l'image I (x, y) est convolutée avec des filtres gaussiens à différentes échelles comme l'équation II.1 :

$$\mathbf{L\ (x, y, \sigma) = G\ (x, y, \sigma) * I\ (x, y)\ (II, 1)}$$

Dans l'équation II.1, L (x, y, σ) est la convolution de l'image I (x, y) avec le filtre gaussien G (x, y, σ) à l'échelle σ. Les différences entre deux images gaussiennes à l'échelle kσ et σ sont prises comme l'équation II.2 montrée :

$$\mathbf{D\ (x, y, \sigma) = L\ (x, y, k\sigma) - L\ (x, y, \sigma)} \qquad \mathbf{(II.2)}$$

(2.2) la différence à ces deux échelles est appelée DoG (Différences de Gaussiennes), Image dont est présenté dans la figure II.3 :

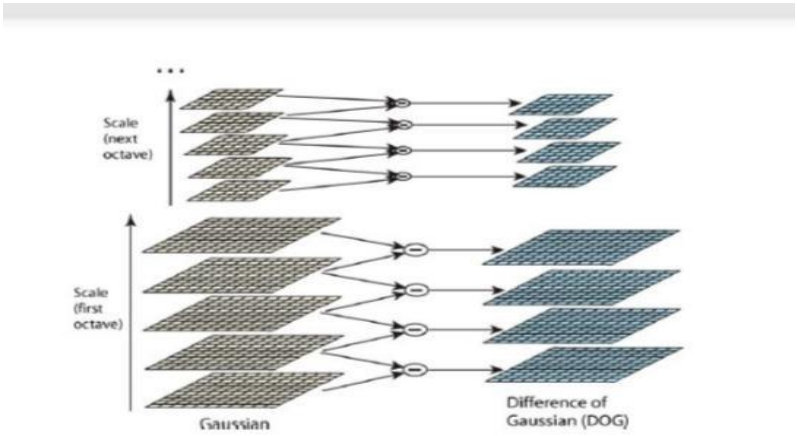


Figure II.3 : La création d'une image DoG, à partir de [16].

2. Localisation des points clés :

Après la première étape, les points clés peuvent également être appelés Les points d'intérêt sont identifiés comme des maxima ou minima locaux des images DoG à travers les échelles. Chaque pixel du

Les images DoG sont comparées à ses 8 voisins à la même échelle, comme illustré à la figure II.4. Nous devons également préciser les localisations des points-clés en supprimant les points d'une valeur prédéterminée. **1 ∂DT D (xˆ) = D + xˆ (II, 3) 2 ∂x**,Où xˆ est calculé en fixant la dérivée D (x, y, σ) à zéro.

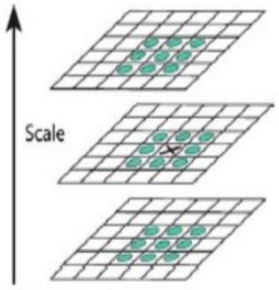


Figure II.4 : Détection des extrema locaux, d'après [16].

3. Affectation de l'orientation :

Afin d'obtenir l'invariance de l'orientation, la magnitude du gradient m (x, y) et l'orientation θ (x, y) sont précalculées en utilisant comme équation II.4, II.5 :

q m (x, y) = (L (x + 1, y) – L (x – 1, y)) 2 + (L (x, y + 1) – L (x, y – 1)) 2 (2,4) L (x, y + 1) – L (x, y – 1) θ (x, y) = arctan () L (x + 1, y) – L (x – 1, y) **(II,5)**

4. Génération de descripteur de point-clé :

Si une orientation de point-clé est sélectionnée, le descripteur de fonction est calculé comme un ensemble d'histogrammes d'orientation sur des quartiers de 4 × 4 pixels, il est illustré à la figure II.5 :

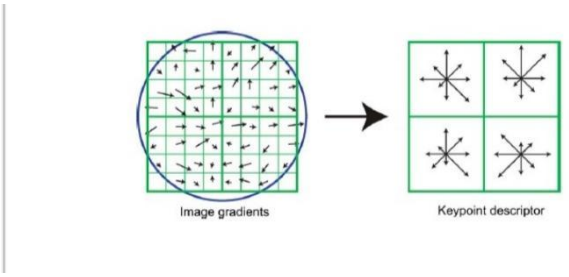


Figure II.5 : descripteur de fonction SIFT, d'après [16].

L'histogramme contient 8 cases, donc un vecteur d'entités SIFT est avec 4 × 4 × 8 = 128 éléments, et il est normalisé à la longueur unitaire. C'est le représentant du descripteur de fonctionnalités SIFT.

Comme nous avons choisi d'utiliser les fonctionnalités SIFT, pour extraire les fonctionnalités SIFT dans une image, nous utilisons VL_FEAT [5], la bibliothèque open source qui implémente la détection des fonctionnalités SIFT dans une image.

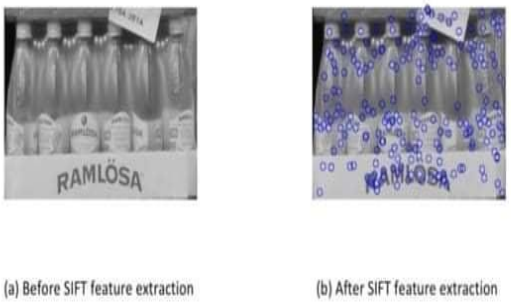


Figure II.6 : Extraction de fonctionnalités SIFT à l'aide de la bibliothèque VL_FEAT. Dans la figure de droite, les positions des points d'entités SIFT extraites sont tracées avec des marques bleues.

En utilisant cette bibliothèque et une image comme entrée, les positions des points caractéristiques dans l'image seront obtenues. Sur la figure II.6, une image de Ramlosa avec 465 × 286 pixels est donnée, les positions des points caractéristiques SIFT extraites ont été présentées sous forme de marques bleues. Pour chaque entité, son descripteur d'entité SIFT de 128 dimensions sera également extrait. :

Figure II.7: Extraction de fonctionnalités SIFT à l'aide de la bibliothèque VL_FEAT. Dans la figure de droite, les positions des points d'entités SIFT extraites sont tracées avec des marques bleues.

3.3. Correspondance des fonctionnalités :

Dans cette section, afin de décrire notre méthode de correspondance des caractéristiques, nous choisissons une image d'objet qui est appelée exemple d'image ici. Nous choisissons également une image de test comprenant l'objet de l'image d'échantillon à l'intérieur. Il est illustré à la figure II.8.

Figure II.8: Exemple d'image d'échantillon et d'image de test.

Les fonctionnalités SIFT de l'image d'exemple sont extraites et stockées. Ensuite, les fonctionnalités SIFT de l'image de test sont également extraites. Afin de mettre en œuvre la détection d'objets, la première étape consiste à trouver des paires correspondantes de points caractéristiques situés dans l'image échantillon et l'image test. Ici, une approche du plus proche voisin développée par Lowe de la distance euclidienne dans l'espace des entités (128 dimensions de SIFT). Nous appelons ces deux fonctionnalités Fb et Fc, ainsi que leurs descripteurs de fonctionnalités db et dc. Et nous calculons le rapport entre les deux distances qui est indiqué dans l'équation II.6 :

$$\text{Ratio} = \text{dis}(da,db) / \text{dis}(da, dc) \quad \textbf{(II.6)}$$

Où Dis (da, db) est la distance euclidienne entre da et db dans un espace de 128 dimensions, et Dis (da, dc) est la distance euclidienne entre da et dc.

Selon la méthode de Lowe, alors que le rapport des deux distances est inférieur à un seuil, cela signifie qu'une paire d'entités SIFT est mise en correspondance. Dans l'équation, cela signifie que les caractéristiques Fa et Fb sont appariés. Alors que le seuil de rapport est de 0,8, le résultat de la correspondance des caractéristiques SIFT a les meilleures performances [6]. Dans notre test, tout en définissant le seuil sur 0,8, la correspondance des fonctionnalités est la plus efficace. Donc, ici, dans notre implémentation, nous avons également défini le seuil de ratio comme 0.8.

Par exemple, nous prenons un exemple d'image avec une résolution de 465 × 286 pixels de Ramlosa, et une image avec une résolution de 1528 × 2288 pixels contenant Ramlosa comme image de test :

Exemple d'image d'échantillon et d'image de test. Selon l'approche de correspondance de caractéristiques décrite ci-dessus, nous pouvons trouver des paires correspondantes de caractéristiques SIFT situées dans l'image d'exemple et l'image de test de la figure II.9. Ces points caractéristiques correspondants dans deux images sont reliés par des lignes bleues :

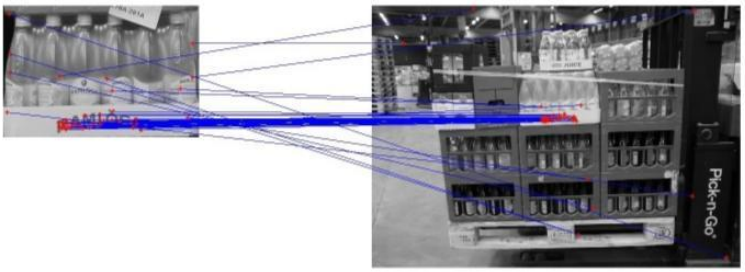


Figure II.9 : Fonction SIFT correspondant entre l'image échantillon et l'image test. Dans les deux images, les positions des points caractéristiques SIFT correspondantes sont marquées en rouge.

Mais dans l'environnement d'entrepôt, non seulement un mais plusieurs objets se trouvent sur une seule palette. Et sur une palette, il peut y avoir plusieurs objets de même catégorie, comme la figure II.10 montrée :

Figure II.10 : L'image d'exemple et plusieurs objets identiques apparaissent dans l'image de test.

Dans notre test, après avoir utilisé la méthode que nous avons décrite ci-dessus, il y a moins de trois points caractéristiques SIFT appariés situés sur l'objet qui est montré dans la figure II.10. D'après la recherche précédente [6], afin de détecter la position d'un objet, le plus petit nombre de points caractéristiques SIFT situés sur un objet cible est 3. Si nous utilisons toujours la même approche de correspondance de caractéristiques que celle décrite ci-dessus, tous les objets ne peuvent pas être détectés. Nous changeons donc un peu notre approche de correspondance des fonctionnalités. Nous faisons correspondre les caractéristiques SIFT extraites de l'image de test à celles extraites de l'image échantillon. En particulier, les fonctionnalités SIFT de l'image d'exemple sont toujours extraites et stockées dans un premier temps. Si une image de test est mise en détection, les caractéristiques SIFT de l'image de test sont également extraites. Ensuite, pour une fonctionnalité de l'image de test, nous commençons à trouver sa fonctionnalité correspondante dans l'image d'exemple.

(a) Pour une nouvelle image de test, il suffit d'extraire ses fonctionnalités

(a)Mise en correspondance des caractéristiques SIFT extraites de l'image échantillon avec celles de l'image test.

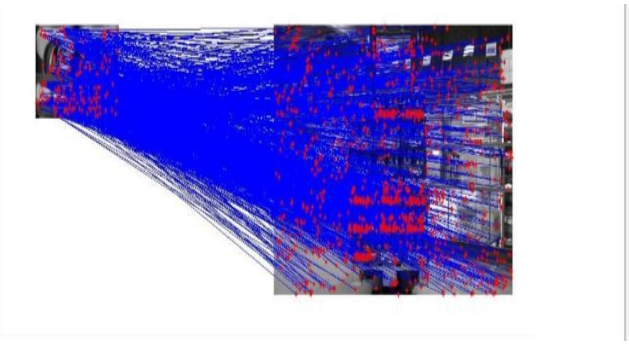


Figure II.11 : La sous-figure (a) est le résultat correspondant aux caractéristiques SIFT de l'image échantillon à celles de l'image de test, la sous-figure (b) est le résultat de la correspondance des caractéristiques SIFT de l'image test à celles de l'image échantillon.

(b) Faire correspondre les caractéristiques SIFT extraites de l'image de test à celles de l'image de l'échantillon.

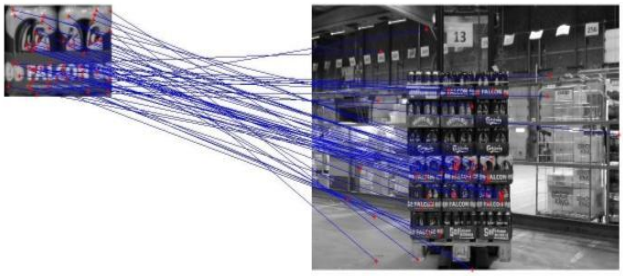


Figure II.12 : la sous-figure (b) est le résultat de la correspondance des caractéristiques SIFT de l'image test à celles de l'image échantillon.

À partir de la figure II.11, nous pouvons voir qu'après avoir changé pour faire correspondre les caractéristiques SIFT extraites de l'image de test à celles de l'exemple d'image, beaucoup plus de paires de caractéristiques correspondantes sont trouvées. Parmi tous, il existe un certain nombre de fonctionnalités mal assorties. Mais dans la zone de chaque objet cible, il y a évidemment bien plus que trois points caractéristiques. C'est pratique pour la détection d'objets. Il faut donc trouver une solution pour réduire efficacement le nombre de fonctionnalités incorrectes. Une solution à ce problème est présentée dans la section 2.3.1.

II.3 Détection d'objets basée sur la fonction SIFT

Dans la section II.2, nous décrivons principalement comment extraire des fonctionnalités SIFT à partir d'images et la méthode pour résoudre le problème de correspondance des fonctionnalités. Dans ce chapitre, une méthode de détection d'objet basée sur la fonction SIFT est décrite. L'ensemble de la procédure de détection d'objet peut être décrite comme illustré à la figure II.12

- **L'algorithme des SIFT :**

La méthodes des SIFT (scale-invariant feature transform= transformation de caractéristiques visuelles invariante à l'échelle), est une méthode développée par David Lowe en 2004 [10], permettant de transformer une image en ensemble de vecteurs de caractéristiques qui sont invariants par transformations géométriques usuelles (homothétie, rotation) et de manière moins fiables aux transformations affines et à l'illumination.

Le point fort de la méthode de Lowe est qu'elle est capable de mettre en correspondance des points distants avec des variations de caméra importantes.

- ✓ **L'algorithme des SIFT**

vient combler en grande partie les limites des méthodes d'extraction de points remarquables déjà développées avant lui par Harris, et plus tard par Mohr et Schmid.

En effet, il a contribué à l'amélioration des techniques d'extraction d'information dans une image en apportant un algorithme robuste et satisfaisant les propriétés que requièrent les procédés de vision artificielle notamment le recalage d'images, » technique consistant à trouver une transformation géométrique permettant de passer d'une image (dite source) à une autre image (dite cible) « La mise en place de la méthode de Lowe nécessite deux étapes principales. Premièrement, il est nécessaire d'extraire les caractéristiques d'un objet et de calculer ses descripteurs, c'est-à-dire, de détecter les caractéristiques qui sont les plus susceptibles de représenter cet objet, de le définir et de le discriminer par rapport aux autres. Deuxièmement, il faut mettre en place une procédure de mise en correspondance (« matching »). C'est le but ultime de la méthode.

Figure II.13 : David Lowe

4. CONCLUSION :

Au terme de cette recherche nous avons pu atteindre tous les objectifs qui nous avaient été assignés au départ qui consistait a faire la reconnaissance des objets a l'aide du Descripteur SIFT. A souligner que nos résultats sont beaucoup plus encourageants Visa a visa du cahier de charges du TP à travers les voyants de la matrice de Confusion.
Sachant qu'il est difficile de détecter les images disposant de très peu (nombre Réduit) de descripteurs comme ce sont le cas des images lices.
Cependant, comme toute œuvre humaine, ce programme n'est pas parfait. En Perspective, nous comptons améliorer notre programme avec l''évolution du cours tout en ajoutant ou bien essayant d'autres méthodes de reconnaissance des objets entre autres.

CHAPITRE III

Résultat expérimental de SIFT algorithme

1. Introduction :

Après avoir abordé l'aspect théorique dans les chapitres précédents, nous passons à la conception et à l'implémentation de notre application pour la reconnaissance des individus par l'empreinte digitale.
Nous analyserons plus en détail les étapes de conception du notre système multi biométrique pour cela on a met en place la méthode SIFT (Scale Invariant Feature Transforme).
Nous conclurons le chapitre par une analyse et discussion des résultats Expérimentaux.

2. Résultat expérimental de l'algorithme SIFT :

Dans cette section, la simulation et l'évaluation des performances de l'algorithme SIFT ont été effectuées sur un PC Pentium I-3, 2,2 GHz avec Windows 7 et 2 Go de RAM. L'implémentation a été réalisée en utilisant le logiciel Matlab. Versions utilisées : MATLAB R2013a et MATLAB R2017a, ce dernier offre plus de fonctionnalités, mais nécessite une configuration puissante de PC.

- ✓ **Base de données utilisée :**

Nos expériences ont été menées sur la sous base de données d'empreinte digitale d'humains doigts. Pour chaque personne, 3 doigts sont enregistrés : le pouce, l'index et le majeur des deux mains gauche et droite; chacun des doigts est acquis 8 fois, nous avons sélectionné les 3 doigts de la main droite.

- ✓ **Évaluation de performance :**

Dans cette section, nous présentons les résultats des expériences menées sur notre base de données.

1) Détection des extrêmes de l'espace d'échelle

La première étape de l'algorithme est l'identification de l'espace d'échelle ou de l'emplacement où les points clés sont trouvés. L'espace d'échelle est construit en appliquant progressivement l'opération de flou Gaussien sur l'image d'origine, formant ainsi des octaves (images de même taille). Et cela peut être donné par la fonction,

$$L(x, y, \delta) = G(x, y, \delta) * I(x, y) \quad \textbf{(III.1)}$$

Où * est l'opérateur de convolution, G (x, y, σ) est une échelle variable Gaussien et I (x, y) est l'image d'entrée et σ est le paramètre d'échelle (quantité de flou).La différence des images *G*aussien (DoG) est créée à partir de l'octave générée. Deux images adjacentes d'une octave sont prises et l'une est soustraite de l'autre.La prochaine paire d'images adjacentes est considérée pour l'opération et le processus est répété pour toutes les octaves. Les images

résultantes sont une approximation du Laplace invariant d'échelle de Gauss. Différence de Gaussien donnée par,

$$D(x, y, \delta) = L(x, y, k\delta) - L(x, y, \delta)$$ **(III.2)**

Dans l'image DoG résultante, chaque pixel est comparé à ses 26 voisins à l'échelle actuelle, inférieure et supérieure, si le pixel a valeur extrême (maximum ou minimum) alors c'est un candidat potentiel pour le point-clé. La première image de la première octave est créée en interpolant l'originale image

Figure III.1: la première image de la première octave est créée en interpolant l'original

2) Différence de Gaussien :

Dans l'étape suivante, nous créons la pyramide DoG comme le montre la figure III.2.

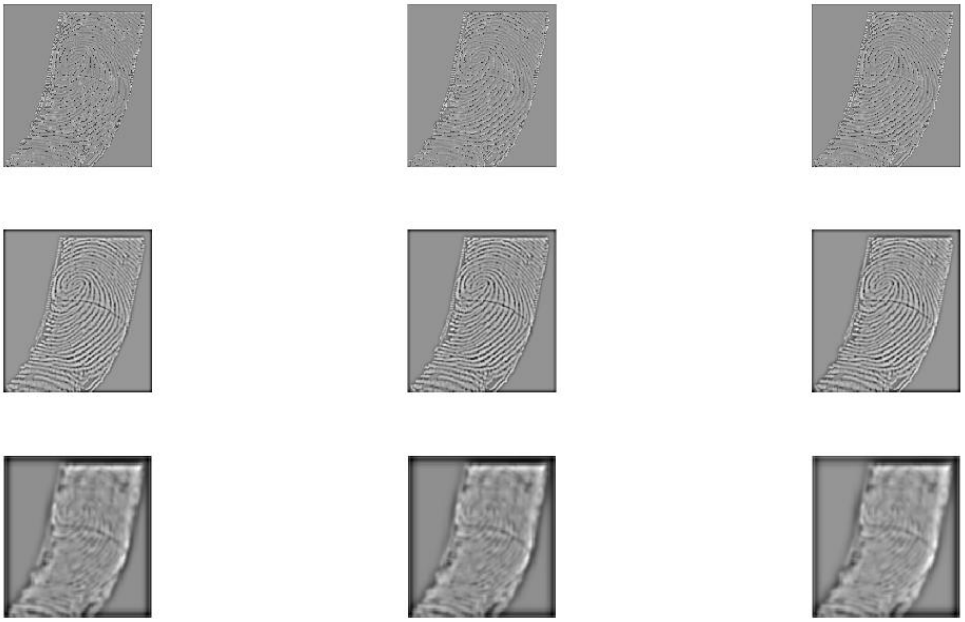


Figure III.2: la pyramide DoG

Localisation des points clés: les points clés ayant des caractéristiques de faible contraste, c'est-à-dire si l'amplitude de l'intensité du pixel est inférieure à la valeur seuil ou situés sur les bords sont supprimés.
Dans cette étape, nous rechercherons chaque pixel dans DoG map pour trouver le point extrême comme indiqué sur les figures III.3 et III.4.

3) Octaves :

Dans l'étape d'octave, les figures suivantes montrent différentes octaves de l'image d'origine.

Figure III.3: Localisation des points clés de DoG map

Dans l'étape d'octave, les figures suivantes montrent différentes octaves de l'image d'origine.

Figure III.4: Quatre images avec des octaves différentes

4) Descripteur de point-clé :

Génération d'une valeur de descripteur unique pour chaque point-clé sélectionné. Une région 16x16 autour du point clé est prise et est divisée en bloc 4x4. L'amplitude et les directions du gradient sont calculées pour chaque bloc. Les orientations sont représentées à l'aide d'un histogramme à 8 cases. Ainsi, le descripteur SIFT est calculé et représenté comme un vecteur numéroté de 128 (bloc 4x4 avec 8 rotations de bac, 4x4x8 = 128).La figure III.5 montres le descripteur de point-clé de l'image d'origine.

Figure III.5: le descripteur de point-clé de l'image d'origine

5) Algorithme de correspondance :

• Les fonctionnalités SIFT sont extraites des images d'empreintes digitales. Chaque image est représentée avec une valeur de caractéristique extraite à l'étape précédente.
• En utilisant l'approche des voisins les plus proches, la reconnaissance d'empreintes digitales est effectuée.
• Les voisins les plus proches sont l'un avec la plus petite distance euclidienne entre le vecteur de descripteur de test donné et les descripteurs d'empreintes digitales.
• Enfin, l'empreinte digitale qui reçoit la distance minimale est choisie comme la meilleure correspondance.

6) La courbe CMC :

Afin d'évaluer la performance de notre approche,nous allons choisir la courbe CMC (Cumulative Match Caractéristique), Cette courbe affiche le taux d'identification cumulé en fonction de rang de la distribution. Ceci fournit une indication du degré de proximité pour obtenir la correspondance correcte si la correspondance au rang-1 est incorrecte.
Dans la figure III.6 Courbe de correspondance cumulative (CMC) montrant les performances de correspondance avec l'empreinte digitale à l'aide des algorithmes SIFT et SURF.

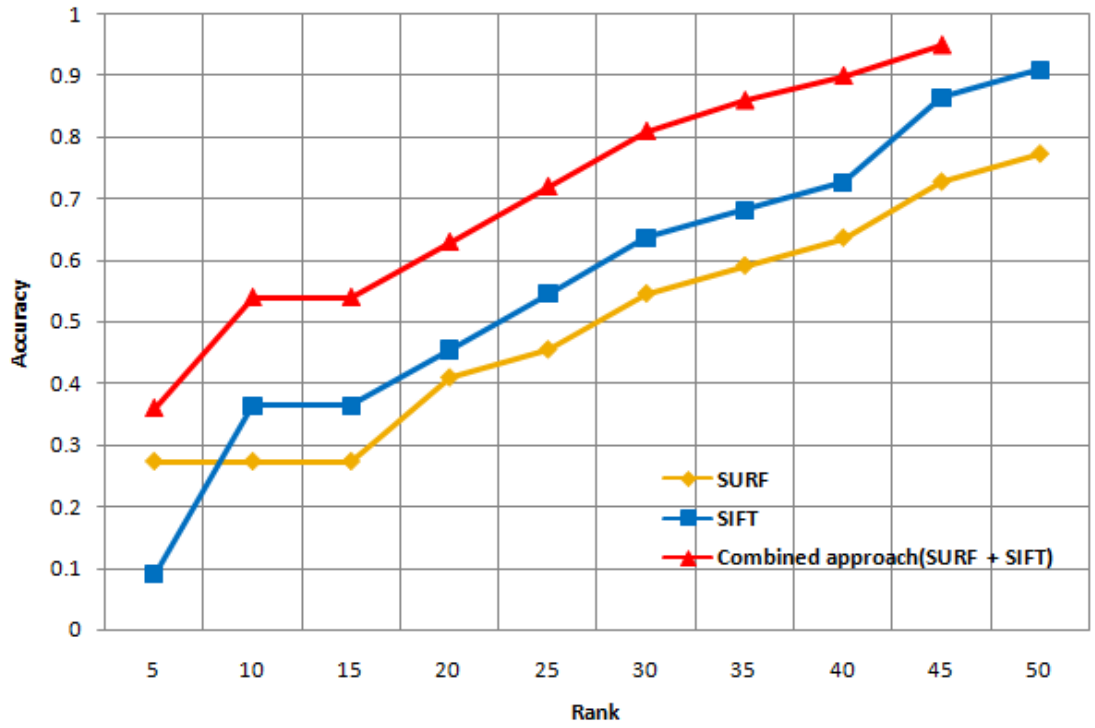


Figure III.6: Courbe de correspondance cumulative (CMC) montrant les performances de correspondance avec l'empreinte digitale

.Suite au résultat qu'on a eu dans la Courbe de correspondance cumulative (CMC), nous avons constaté que SIFT est plus performant que le SURF et donne des meilleurs résultats par rapport a d'autres algorithmes.

7) La courbe ROC :

La fonction d'efficacité du récepteur, plus fréquemment désignée sous le terme « courbe ROC» (de l'anglais receiver operating characteristic, pour « caractéristique de fonctionnement du récepteur ») dite aussi caractéristique de performance (d'un test) ou courbe sensibilité/spécificité, est une mesure de la performance d'un classificateur binaire, c'est-à-dire d'un système qui a pour objectif de catégoriser des éléments en deux groupes distincts sur la base d'une ou plusieurs des caractéristiques de chacun de ces éléments. Graphiquement, on représente souvent la mesure ROC sous la forme d'une courbe qui donne le taux de vrais positifs (fraction des positifs qui sont effectivement détectés) en fonction du taux de faux positifs (fraction des négatifs qui sont incorrectement détectés).Dans la figure III .7 Courbes ROC pour les trois algorithmes (SIFT, ZNCC avec rotations et Harris SSD) selon le nombre d'empreinte digitale.

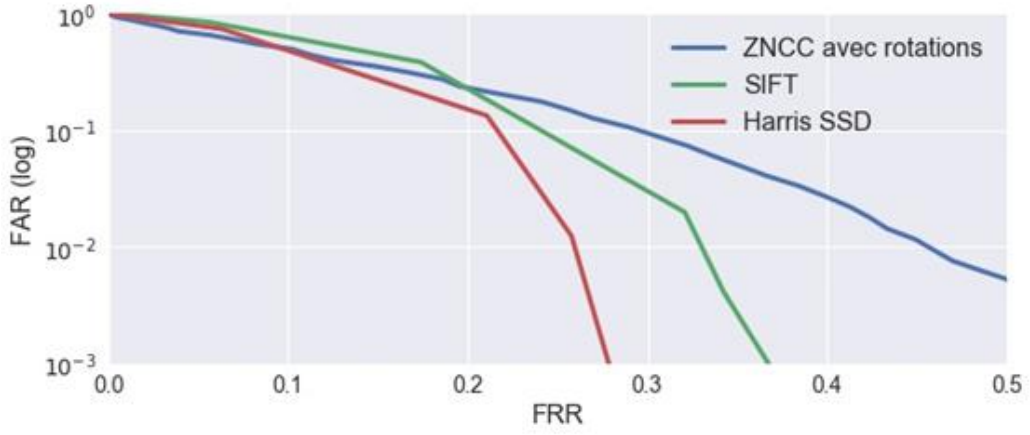


Figure III.7: Courbes ROC pour les trois algorithmes (SIFT, ZNCC avec rotations et Harris SSD) selon le nombre d'empreinte digitale

.Pour la courbe ROC on a comparé notre algorithme avec d'autre algorithmes (ZNCC, Harris SSD), l'algorithme Sift a donné meilleur résultat dans l'empreinte Digitale.

3. Avantages et inconvénients du SIFT

➢ **Les avantages :**

- Résistant aux transformations affines d'étendue limitée (fonctionne mieux pour les objets plans que pour les objets 3D complets).
- Résistant à une gamme de changements d'éclairage
- Résistant aux occlusions dans la reconnaissance d'objets, car les descripteurs SIFT sont locaux.

➢ **Inconvénients :**

- La résistance aux transformations affines est empirique – non théorie du noyau dur fournie.
- Plusieurs paramètres dans l'algorithme: taille du descripteur, taille de la région, différents seuils – théoriques le traitement de leur spécification n'est pas clair.

CONCLUSION :

Dans ce chapitre, nous avons vu les étapes de conception d'une plateforme biométrique Multimodale.
Sa représentation modulaire ainsi que la méthode utilisée pour extraire les informations nécessaires à partir des instances multiples et répétées pour chaque individu avec la modalité « Empreinte digitale ».
Par la suite on a exposé les résultats obtenu lors de la phase de test d'évaluation de notre Système on utilisant les courbes CMC et ROC.
comme on a pu arriver à augmenter la fiabilité de la reconnaissance tout en maintenant un taux de reconnaissance idéal de 100% avec une solution simple ,rapide et précise.

CONCLUSION GENERALE ET PERSPECTIVES

La biométrie, définit comme l'étude quantitative des caractéristiques biologiques, morphologiques Ou comportementales de l'humain, est un champ de recherche très actif.
A L'heure actuelle, les technologies biométriques sont basées le plus souvent sur la modalité D'empreinte digitale, qui est pour l'instant réputée parmi les plus fiables en contrepartie de leur caractère intrusif.
Les systèmes biométriques uni-modaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture,
à la pauvreté en matière de points biométriques confidents et notamment à la détérioration de la qualité de l'entrée biométrique. L'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.
Le processus de reconnaissance multimodal permet de renforcer les systèmes biométriques sur les plans de sécurité, fiabilité et pertinence.
En perspective, il est souhaitable d'ajouter un module pour contrôler la qualité des donnéesbiométriques acquises pendant la phase d'enrôlement. Ainsi d'intégrer un module destiné àla sécurisation des données biométriques.

Références

[1]Hedjaz HEZIL« Identification De Personnes Par Signature Manuscrite **», THÈSE 2018, UNIVERSITE 8 MAI 1945 – GUELMA.**

[2]Aghiles GOUNANE et **Samira SADI** « Contribution De L'approche LBP A La Classification Des Images Multispectrales. Application Aux Données TM De La Région Du Hoggar. », **Mémoire de Fin d'Etudes de MASTER ACADEMIQUE 2014**, **Université Mouloud MAMMERI de Tizi-Ouzou**.

[3] Ghoulia bouthaina et Kouidri yamina « Etude Comparative D'ensemble Des Descripteurs De Texture Pour La Reconnaissance De Visages. » **Mémoire MASTER ACADEMIQUE 2016/2017**, **UNIVERSITE KASDI MERBAH OUARGLA**.

[4]Lotfi HOUAM « Contribution À L'analyse De Textures De Radiographies Osseuses Pour Le Diagnostic Précoce De L'ostéoporose**»THÈSE2013, UNIVERSITÉ D'ORLÉANS - UNIVERSITÉ DE GUELMA**.

[5]Andrea Vedaldi and Brian Fulkerson. Vlfeat: An open and portable library of computer vision algorithms. In Proceedings of the international conference on Multimedia**, pages 1469–1472. ACM, 2010.**

[6]David G Lowe. Object recognition from local scale-invariant features. In Computer vision, 1999. The proceedings of the seventh IEEE international conference on**, volume 2, pages 1150–1157. Ieee, 1999.**

[7]Cong Geng and Xudong Jiang. Sift features for face recognition. In Computer Science and Information Technology**, 2009. ICCSIT 2009. 2nd IEEE International Conference on, pages 598–602. IEEE, 2009.**

[8]Martin A Fischler and Robert C Bolles. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography**. Communications of the ACM, 24(6):381–395, 1981.**

[9]Thomas Deselaers, Daniel Keysers, and Hermann Ney. Improving a discriminative approach to object recognition using image patches. In Pattern Recognition**, pages 326–333. Springer, 2005.**

[10]James J DiCarlo and David D Cox. Untangling invariant object recognition. Trends in cognitive sciences**, 11(8):333–341, 2007.**

[11]FATIMA ZOHRA AMARA« IDENTIFICATION BIOMÉTRIQUE PAR FUSION MULTIMODALE DE L'EMPREINTE DIGITALE», **THÈSE** 2018,**CENTRE UNIVERSITAIRE BELHADJ BOUCHAIB D'AÏN-TÉMOUCHENT**