République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 8Mai 1945 – Guelma

Faculté des sciences et de la Technologie

Département d'Electronique et Télécommunications

Mémoire de fin d'étude

pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**

Filière : **Electronique**

Spécialité : **Instrumentation**

La vérification des personnes par leurs signatures manuscrites en hors ligne

---

Présenté par :

FERAGA Hamza

BOUHALITE Djamel

Sous la direction du :

Dr. BENDJOUDI Salim

Juillet 2021

Remerciement

Nous remercions Dieu tout puissant de nous avoir donné la force et la patience pour mener ce travail à terme. Nous exprimons notre profonde gratitude à Mr. BENJOUDI Salim pour avoir assumé la responsabilité de nous encadrer, nous orienter et de nous conseiller tout au long de la réalisation de ce travail ainsi pour la confiance qu'il nous a accordé. Nous remercions vivement les membres du jury pour l'honneur qu'ils nous ont fait en acceptant d'être rapporteurs de notre mémoire. A ceux qui nous ont apporté, de près ou de loin, orientation, soutien et aide dans la réalisation et la concrétisation de ce travail.

Dédicaces

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères frères et sœurs Pour leurs encouragements permanents, et leur soutien moral.

A toute ma famille et A tous mes amis pour leur soutien tout au long de mon parcours universitaire.

Merci de m'Avoir soutenu et Aimé durant Toutes ces Années et d'être si fier de moi.

Hamza.

A mon très cher père, A ma très chère mère pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien tout au long de mes études,

A toute ma grande famille, A toute ma petite famille et A tous mes amis pour leur soutien tout au long de mon parcours universitaire.

Merci de m'Avoir soutenu et Aimé durant Toutes ces Années et d'être si fier de moi.

Djamel.

Résumé

La vérification de signature hors ligne est un système de vérification automatique qui peut traiter des images numérisées de signatures. La vérification de signature utilise des mesures en niveaux de gris avec différentes caractéristiques de premier plan. La vérification de signature est effectuée à l'aide de vecteurs de caractéristiques de reconnaissance de formes locales. Le modèle binaire local amélioré (LBPM) et le descripteur BSIF extraient des informations de la structure locale en établissant la relation entre le pixel central et les pixels voisins. Le travail (mémoire) utilise les caractéristiques du modèle binaire local modifié (LBPM) et ceux du descripteur BSIF pour la vérification de la signature. Cette procédure de vérification des signatures est testée sur les deux bases de données MCYT et GPDS. La précision de la méthode proposée est vérifiée au moyen du classificateur le plus proche voisin (KNN).

Abstract

Offline signature verification is an automatic verification system that can process scanned images of signatures. Signature verification uses grayscale measurements with different foreground features. Signature verification is performed using local pattern recognition feature vectors. The Local Enhanced Binary Model (LEBM) and BSIF descriptor extract local structure information by establishing the relationship between the center pixel and neighboring pixels. The work (dissertation) uses the features of the modified local binary model (LBPM) and those of the BSIF descriptor for signature verification. This signature verification procedure is tested on both MCYT and GPDS databases. The accuracy of the proposed method is verified using the nearest neighbor classifier (KNN).

الملخص

التحقق من التوقيع في وضع عدم الاتصال هو نظام تحقق تلقائي يمكنه معالجة الصور الممسوحة ضوئيًا للتوقيعات. يستخدم التحقق من صحة التوقيع قياسات تدرج الرمادي بخصائص بارزة مختلفة. يتم إجراء التحقق من التوقيع باستخدام متجهات ميزة التعرف على الأنماط المحلية. يستخرج النموذج الثنائي المحلي المحسن (LBP) وواصف BSIF المعلومات من البنية المحلية عن طريق إنشاء العلاقة بين البكسل المركزي والبكسلات المجاورة. تستخدم الوظيفة (الذاكرة) خصائص النموذج الثنائي المحلي المعدل (LBP) وتلك الخاصة بواصف BSIFللتحقق من صحة التوقيع. يتم اختبار إجراء التحقق من التوقيع على قاعدتي البيانات MCYT وGPDS يتم التحقق من دقة الطريقة المقترحة باستخدام أقرب مصنف جار(KNN) .

Tables de matières

Liste de figures

Chapitre 01

chapitre 02

chapitre 03

Liste de tableaux

Chapitre 01

Chapitre 04

Liste des acronymes

Chapitre 01

ADN : Acide Désoxyribo Nucléique

ECG : électrocardiogramme

EMG : électromyogramme

IRM :imagerie par résonance magnétique

SAS : Système d'authentification de signature

OCON: one-class / one-network

RBF: fonction de base radiale (Radial Basis Function)

MLP : Multi Layer Perceptron

SVM : La machine à vecteur de support (Support Vector Machine)

HMM :modèles de Markov cachés (Hidden Markov Model)

OC-SVM: One Class Support Vector Machine

Introduction générale

1. Introduction

Les exigences de sécurité de la société d'aujourd'hui ont placé la biométrie au centre d'un débat permanent sur son rôle clé dans une multitude d'applications [1-3].

Actuellement, dans le monde les signatures sont la forme la plus largement acceptée de vérification biométrique de l'identité. Cependant, elles ont l'inconvénient d'être facilement falsifiées ou volées par ceux qui prétendent à l'identification ou à l'intention d'un individu. La vérification des signatures permet d'identifier l'original et la fausse signature.

La biométrie mesure les caractéristiques physiques ou comportementales uniques des personnes dans le seul but est de reconnaître ou d'authentifier l'identité de ces individus. Les caractéristiques physiques courantes sont les empreintes digitales ou palmaires, la géométrie de la main, les caractéristiques faciales, la rétine, l'iris ou l'oriel. Les caractéristiques comportementales comprennent la voix (qui est également une composante physique), modèle de frappe, la démarche et la signature. Les technologies de la signature et de la voix sont des exemples de cette catégorie de biométrie et sont les plus développées [4].

La signature manuscrite est reconnue comme l'un des attributs personnels les plus largement acceptés pour la vérification de l'identité.

La signature est un symbole de consensus et d'autorisation, particulièrement dans l'environnement des cartes de crédit et des chèques bancaires, et a été depuis longtemps une cible privilégiée des malfaiteurs.

Il existe une demande croissante pour que le traitement de l'identification individuelle soit plus rapide et plus précis, et la conception d'un système

automatique de vérification automatique de signature constitue un véritable défi. Plamondon et Srihari [5] ont noté que les systèmes de vérification automatique de signature occupent une place très spécifique parmi les autres systèmes d'identification automatique :

"D'une part, ils diffèrent des systèmes basés sur la possession de quelque chose (clé, carte, etc.) ou la connaissance de quelque chose (mots de passe, informations personnelles, etc.), car ils reposent sur un geste spécifique, bien appris. D'autre part, ils diffèrent également des systèmes basés sur les propriétés biométriques d'un individu (empreintes digitales, empreintes vocales, empreintes rétiniennes, etc.), car la signature reste le moyen d'identification personnelle le plus accepté socialement et légalement."

Une comparaison de la vérification de signature avec d'autres technologies de reconnaissance (empreintes digitales, visage, voix, rétine et iris) révèle que la vérification de signature présente plusieurs avantages en tant que mécanisme de vérification d'identité. Tout d'abord, l'analyse de la signature ne peut être appliquée que lorsque la personne est/était consciente et disposée à écrire de la manière habituelle, bien qu'il soit possible que des individus soient forcés de soumettre l'échantillon de leur signature. Pour donner un contre-exemple, une empreinte digitale peut également être utilisée lorsque la personne est dans un état inconscient (par exemple droguée). La falsification d'une signature est réputée d'être plus difficile que celle d'une empreinte digitale, étant donné la disponibilité de méthodes d'analyses sophistiquées [6]. Malheureusement, la vérification de signature est un problème de discrimination très difficile car une signature manuscrite est le résultat d'un processus complexe dépendant des conditions physiques et psychologiques du signataire, ainsi que des conditions du processus de signature [7]. Le résultat définitif est qu'une signature est une entité variable importante et que sa vérification, même pour des experts humains, n'est pas une question triviale.

Les défis scientifiques et les applications précieuses de la vérification de signature ont attiré de nombreux chercheurs universitaires et industriels (privé ou étatique) par le problème de vérification de signatures. Sans aucun doute, la vérification automatique de la signature joue un rôle important dans l'ensemble des techniques biométriques dont l'objectif est la vérification des identités des personnes [8,9].

Dans la présente étude, nous nous concentrons sur les caractéristiques basées sur les informations déduites sur le niveau de gris des images contenant des signatures manuscrites en particulier celles qui fournissent des informations sur la distribution de l'encre le long des traces délimitant la signature. Les méthodologies d'analyse de texture sont préconisées à cette fin puisqu'elles assurent l'invariance à la rotation et à luminance. Par conséquent, les défis scientifiques et les précieuses applications dédiées à la vérification des signatures ont attiré de nombreux chercheurs universitaires et du secteur industriel privé et étatique par cette problématique de la vérification des signatures et le développement de vrais systèmes de vérification et d'authentification des individus avec cette modalité.

Il existe deux grandes méthodes de vérification de signature. L'une est une méthode en ligne qui consiste à mesurer des données dynamiques et séquentielles, telles que la vitesse d'écriture, l'inclinaison et la pression du stylo, à l'aide d'un dispositif spécial. L'autre est une méthode hors ligne qui utilise un scanner optique ou une caméra numérique pour numériser les écritures manuscrites consignées sur du papier. Il existe deux approches principales pour la vérification de signature hors ligne : *l'approche statique* et *l'approche pseudo-dynamique*. La statique implique des mesures géométriques de la signature tandis que la pseudo-dynamique tente d'estimer les informations dynamiques à partir de l'image statique [10]. Les systèmes en ligne utilisent des dispositifs d'entrée spéciaux tels que les tablettes, tandis que les approches hors ligne sont

beaucoup plus difficiles car les seules informations disponibles sont une image bidimensionnelle statique obtenue en scannant des signatures pré-écrites sur un papier ; les informations dynamiques du mouvement de la pointe du stylo (stylet), telles que les coordonnées de la pointe du stylo, la pression, la vitesse, l'accélération, ainsi que la levée et la descente du stylo, peuvent être capturées par une tablette en temps réel, mais pas par un scanner d'images. La méthode hors ligne doit donc appliquer des techniques complexes de traitement d'image pour segmenter et analyser la forme de la signature afin d'en extraire des caractéristiques [11]. Par conséquent, la vérification en ligne de la signature est potentiellement plus fructueuse. Néanmoins, les systèmes hors ligne présentent un avantage signifiant en ce qu'ils ne nécessitent pas l'accès à des dispositifs de traitement spéciaux lors de la production des signatures. En fait, si l'on insiste sur la précision des systèmes de vérification, la méthode hors ligne a beaucoup plus de domaines d'application pratique que celle en ligne. Par voie de conséquence, un nombre croissant de recherches a étudié la méthodologie d'extraction de caractéristiques pour la reconnaissance et la vérification de signatures hors ligne [12].

Chapitre 1: La biométrie

1.1 Introduction

Face à la fraude et au vol d'identité, à la menace de terrorisme ou de la cybercriminalité et à l'évolution logique des réglementations internationales, de nouvelles solutions technologiques sont progressivement mises en place.

Parmi ces technologies, basées sur des caractéristiques physiologiques et comportementales uniques, la biométrie est rapidement devenue la technologie la plus fiable et la plus importante pour identifier et authentifier rapidement et de manière fiable le personnel.

Aujourd'hui, de nombreuses applications utilisent cette technologie. Des fonctions autrefois réservées à des applications sensibles (comme la protection de sites militaires) sont devenues des applications grand public à croissance rapide.

La biométrie est une science qui traite des caractéristiques physiques ou comportementales spécifiques de chaque personne et permet de vérifier son identité. Littéralement et de manière plus simplifiée.

La technologie biométrique est divisée en deux catégories : la mesure physiologique et la mesure comportementale.

Les mesures physiologiques peuvent être morphologiques ou biologiques. Ce sont principalement les empreintes digitales, les formes des mains, des doigts, les réseaux veineux, les yeux (iris et rétine) ou les formes de visage pour l'analyse morphologique. En termes d'analyse biologique, on retrouve le plus souvent de l'ADN, du sang, de la salive ou de l'urine utilisés dans le domaine médical, ou juridique dans les enquêtes criminelles et même dans le domaine sportif dans le contrôle du dopage des sportifs.

Les mesures comportementales les plus courantes sont la reconnaissance vocale, la dynamique de frappe sur un clavier d'ordinateur, comment utiliser les objets,

la démarche, les pas, les gestes et surtout la signature dans ses deux modes dynamique (en ligne : vitesse de déplacement du stylet, accélération, pression appliquée, inclinaison), ou statique (en hors ligne).

Ces différentes technologies biométriques utilisées font régulièrement l'objet de recherches, de développements et d'amélioration continue. Cependant, certains types de mesures n'ont pas le même niveau de fiabilité.

La biométrie peut identifier ou authentifier une personne sur la base de ses données identifiables et vérifiables, qui lui sont spécifiques et uniques.

L'authentification consiste à déterminer l'identité d'une personne. Il s'agit de saisir des données biométriques de la personne, par exemple en prenant une photo de son visage, en enregistrant sa voix ou en capturant l'image de son empreinte digitale. Ces données sont ensuite comparées aux données biométriques de plusieurs autres personnes de la base de données.

La vérification d'identité (également appelée vérification) est le processus de comparaison des données caractéristiques d'une personne avec le modèle de référence biométrique d'une personne (« modèle ») pour déterminer la similitude. Le modèle de référence est préenregistré et stocké dans une base de données dans le dispositif de sécurité ou les effets personnels. Nous sommes là pour vérifier que la personne présentée est bien la personne qu'elle revendique être [13].

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 [14-16]. La figure **1.1** illustre un exemple de quelques modalités biométriques.

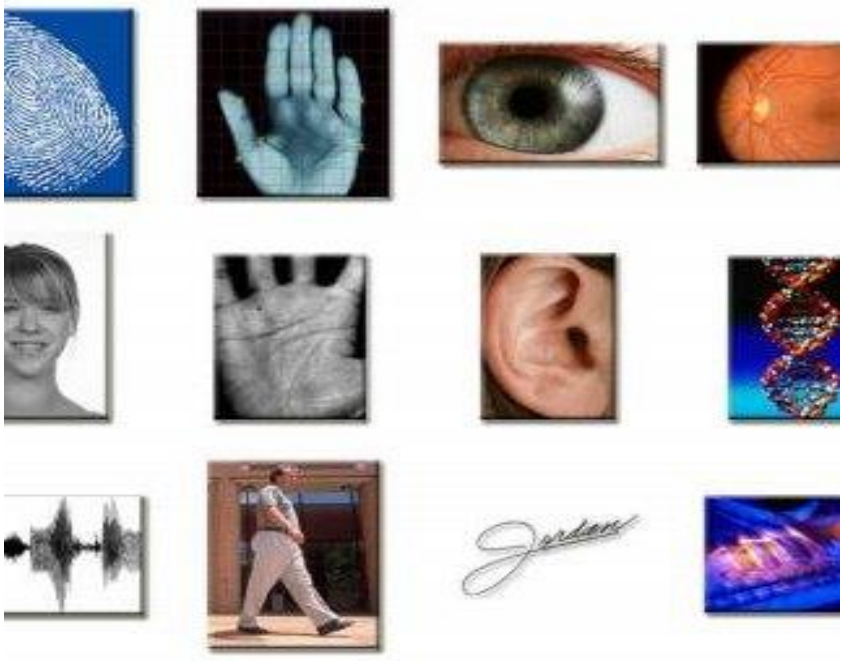


Figure 1.1: Exemples de modalités (physiologiques et comportementales)

1.3 Les modalités biométriques

Il existe plusieurs modalités qui ont été utilisées dans les différents systèmes biométriques, Bien qu'il existe un très grand nombre de modalités biométriques, nous pouvons les scinder en deux grandes catégories

a) La biométrie physiologique : peuvent être morphologiques ou biologiques :
b) Les mesures morphologiques : Comme les empreintes digitales, la forme de la main, du doigt, le réseau veineux de la main ou des doigts, l'œil (iris ou la rétine), ou encore la forme du visage…
c) Les mesures biologiques : Comme l'ADN, le sang, la salive, ou l'urine utilisés dans le domaine médical, ou dans les investigations criminelles...
d) La biométrie comportementale : Les plus répandues sont la reconnaissance vocale, la dynamique de frappe au clavier d'un ordinateur, la démarche, la gestuelle et surtout les signatures dynamiques (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison) ou statiques, …

1.3.1 Les modalité physiologiques (morphologiques)

Ces types de modalité regroupent des caractéristiques spécifiques de la structure ou de la forme d'une partie du corps humain. Nous pouvons citer quelques-unes des exemples les plus connues

1.3.1.1 L'empreinte digitale

L'être humain a utilisé ses 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[17]. Une empreinte digitale est le motif de crête et de vallées sur la surface des bouts des doigts. L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les policiers et les gendarmes utilisent cette technique depuis plus d'un siècle. Aujourd'hui, les empreintes digitales sont recueillies sur les scènes de crime et sont ensuite comparées à

celles contenues dans les bases de données nationales ou même internationales (*Interpole*) [18].

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 la main d'un être humain. Ces empreintes sont uniques pour chaque individu. Même les vrais jumeaux n'ont pas des empreintes digitales identiques.

Figure 1.2 : L'empreinte digitale

.

1.3.1.2 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 [19]. 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 l'inconvénient majeur de cette modalité. De plus, ce capteur coute très cher par rapport à ceux des 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

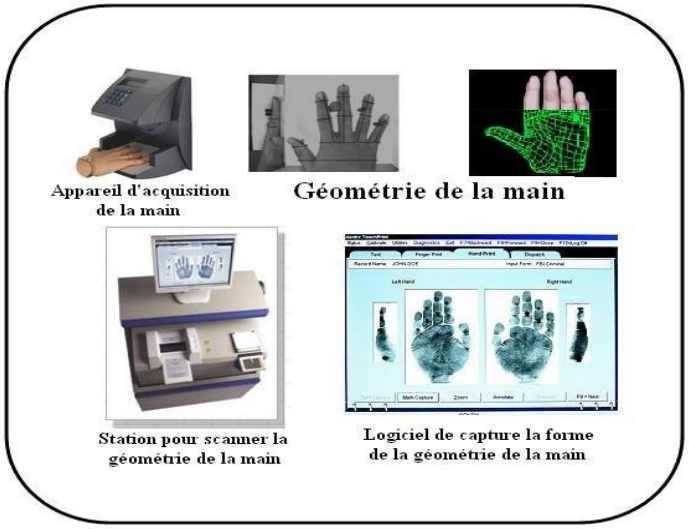


Figure 1.3 : La géométrie de la main

1.3.1.3 La rétine

Cette modalité est bien adaptée aux applications de haute sécurité (sites militaires, salles de coffres forts, etc.). Lors de l'acquisition de cette modalité, l'utilisateur place son œil à proximité d'un capteur où un rayon lumineux illumine le fond de l'œil pour extraire des points repères. La détermination des caractéristiques de la rétine consiste en l'extraction de la distribution géographique des vaisseaux sanguins [20]. Cette mesure est riche en matière de caractéristique plus de 400 [21]. 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 a réduit l'utilisation de cette modalité.

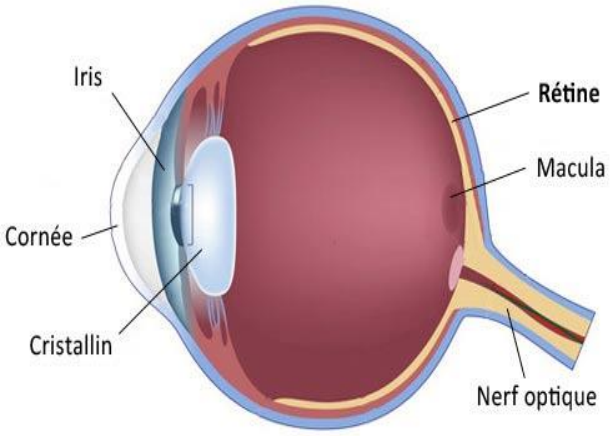


Figure 1.4 : La rétine

1.3.1.4 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 [22]. Les caractéristiques qui servent à la reconnaissance du visage sont : les yeux, la bouche, la forme du visage (contour), etc… [23-24].

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 sont extraites (le tour du visage, la position des oreilles, les coins de la bouche, l'écartement des yeux et la taille de la bouche, etc…) à partir de la photo d'un individu. Ces systèmes sont capables de faire face aux techniques de *spoofing* [25], comme le port de lunettes, la barbe, le maquillage, etc.

Figure 1.5 : Le visage

1.3.1.5 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 [26], donc elle est considérée comme la modalité la plus précise pour l'identification et l'authentification des personnes [27]. Son seul inconvénient est son coût assez élevé, ce qui ne la rend pas autant répondu dans les 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 [29] 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 [23], [28].

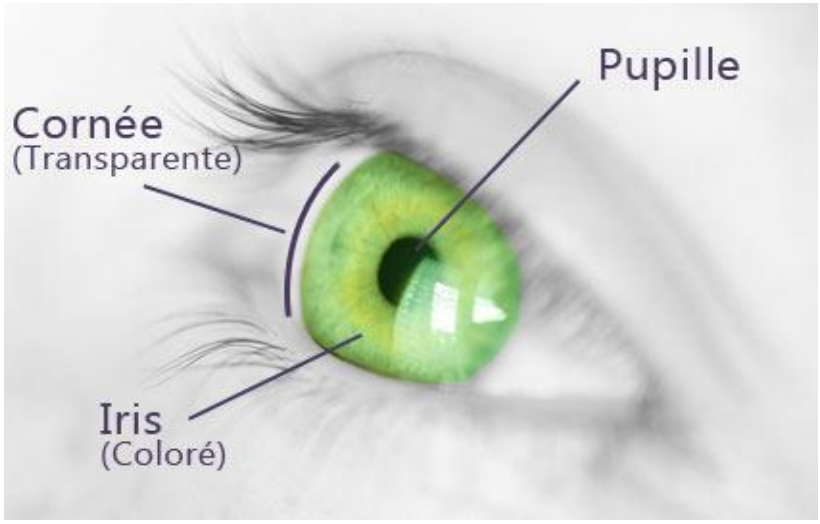


Figure 1.6: L'iris

1.3.1.6 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 [23], [29].

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 dans les systèmes multimodaux. Les recherches ont légèrement évolué pour développer des technologies automatisées d'identification par oreille. Cependant, des efforts significatifs sont encore exigés pour améliorer l'identification par l'oreille, la segmentation et la possibilité d'identification dans le but de faire un déploiement dans la surveillance et dans les autres applications commerciales [23].

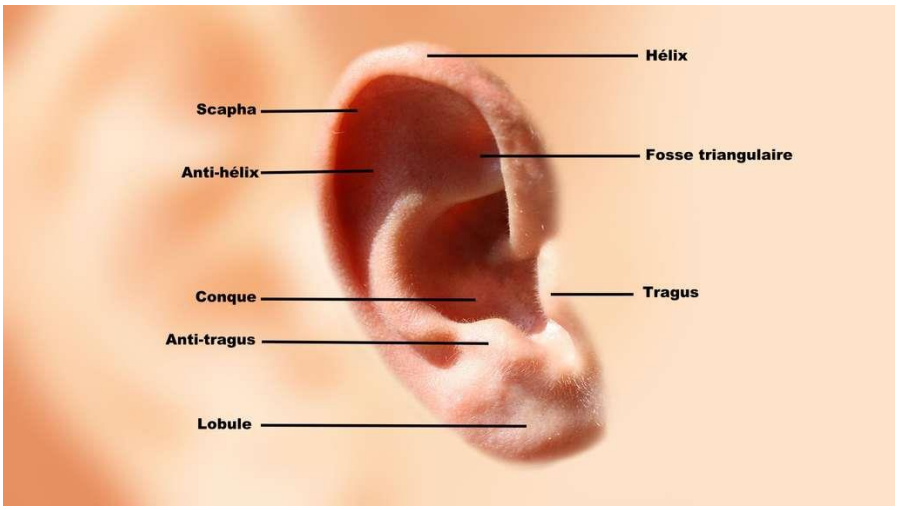


Figure 1.7 : L'oreille

1.3.2 Les modalités comportementales

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

1.3.2.1 La signature

L'identification par la 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 (les chèques, les actes, etc.…). Elle a été acceptée comme une méthode d'authentification légale par les gouvernements et dans les transactions commerciales. Les systèmes de vérification de signatures se base sur deux catégories selon le type d'acquisition des données : en ligne (*online)* [23], [30], ou en hors-ligne (*offline)* [23], [31].

Les systèmes de vérification des signatures en ligne 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 caractéristiques comme les points de pauses, la pression, la direction, la vitesse d'écriture pendant la signature et l'angle d'inclinaison. Ces caractéristiques dynamiques sont spécifiques à chaque individu. D'autre part, les systèmes de vérification des signatures en hors ligne

traitent la signature à partir de leurs images scannées. Ces systèmes sont assez complexes dû à l'absence de caractéristiques dynamiques stables.

Figure 1.8 : La signature

1.3.2.2 La dynamique de frappe au clavier

Cette modalité est une caractéristique comportementale qui 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 [23], [32].

La différence avec ces systèmes se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux [32], soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence). Ces techniques sont assez satisfaisantes, mais restent néanmoins statistiques.

Figure 1.9 : La dynamique de frappe au clavier

1.3.2.3 La démarche

Elle se réfère à la manière dont une personne marche et c'est l'une des rares modalités biométriques qui peut être utilisée 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 candidat [23], [33].

Les gens montrent 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 [34] ce qui aide de manière significative à les identifier.

Cette modalité est notamment appropriée pour les applications de vidéo surveillance. Les performances des systèmes à base de la démarche ne sont pas assez acceptables, car elles sont affectées par le changement de l'environnement.

Figure 1.10 : La démarche

1.3.2.4 La voix

La voix est considérée comme une combinaison entre les caractéristiques biométriques physiques et comportementales [23], [35]. 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 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 partir 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 de 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 [35]. 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.

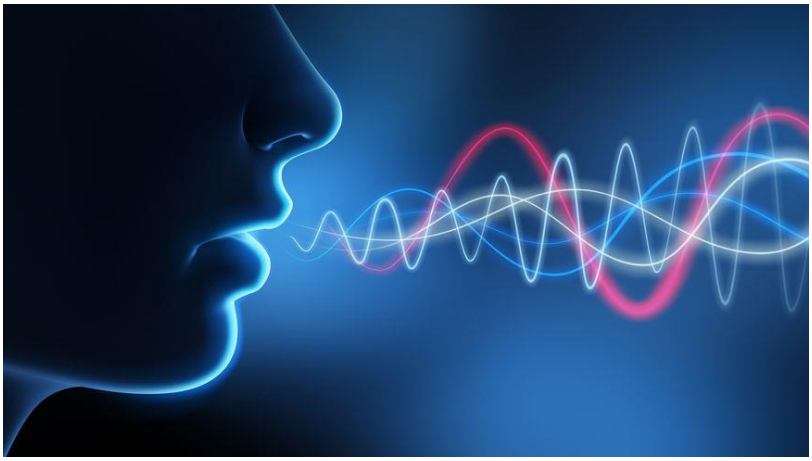


Figure 1.11 : La voix

1.4 Les caractéristiques biométriques

Ces caractéristiques dites biométriques ont un caractère personnel et ne peuvent pas être facilement volées, falsifiées, ou partagées. Ainsi, elles sont plus fiables et sécurisées pour la reconnaissance de personnes que les méthodes traditionnelles basées sur la connaissance ou la possession. Chaque caractéristique, physiologique ou comportementale, peut être utilisée comme une modalité biométrique [36]. Quoiqu'il en soit, ces techniques biométriques doivent avoir les propriétés suivantes :

- ***Universalité*** : toutes les personnes à identifier doivent la posséder.
- ***Unicité*** : l'information doit être aussi dissimilaire que possible entre les différentes personnes.
- ***Permanence*** : l'information collectée doit être présente pendant toute la vie d'un individu.
- ***Collectabilité*** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.
- ***Acceptabilité*** : acceptation par les utilisateurs.

Chaque modalité biométrique a ses forces et ses faiblesses, et doit posséder effectivement ces propriétés avec des degrés différents. Le choix et l'utilisation d'une modalité biométrique dépend généralement des besoins de l'application à mettre en place.

1.5 Architecture d'un system biométrique :

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres d'un individu : physiques, biologiques ou comportementales [37].

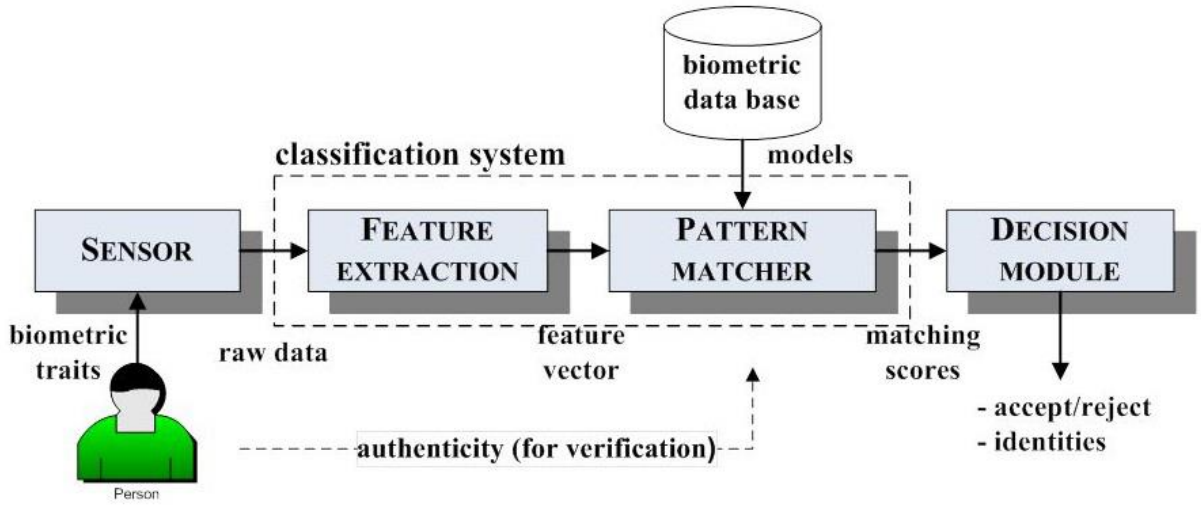


Figure 1.12 : Architecture d'un système biométrique

Il doit regrouper quatre modules principaux [37] :

1.5.1 Le module de capture

Responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreinte digitales, une caméra de sécurité, etc..).

1.5.2 Le module d'extraction de caractéristiques

Prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des donnés.

Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes.

1.5.3 Le module de correspondance

Compare l'ensemble des caractéristiques extraites avec le modèle préenregistré dans la base de données du système et détermine le degré de similitude (ou divergence) entre les deux.

1.5.4 Le module de décision

Vérifie l'identité affirmée par un utilisateur ou détermine d'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés.

1.6 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 affectant la reconnaissance du speaker), changements des conditions ambiantes (ex., le changement du niveau d'illumination lors de la 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 [14].

1.7 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. La figure **1.13**, représente 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 limitées. 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. L'empreinte et la signature manuscrite représentent un compromis en matière de performance. C'est l'une des raisons pour laquelle on a choisi l'une de ces modalités dans notre étude.

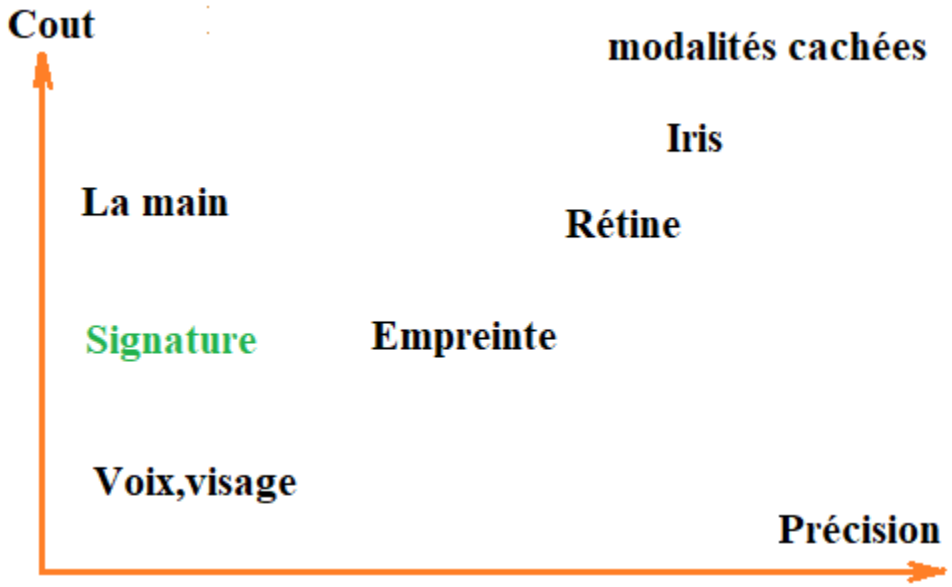


Figure 1.13 : Classement des modalités biométriques selon le coût et la précision

Ainsi, dans le tableau suivant, en plus de la précision et du cout de chaque modalité, on a ajouté d'autres paramètres de comparaison qui sont la simplicité d'utilisation et son acceptation par l'utilisateur.

La simplicité d'utilisation peut être définie comme étant la quantité d'énergie fournie par un individu pour être reconnue par un système. L'acquisition de certaines modalités ne nécessite parfois aucun effort de la part

de l'utilisateur (visage, empreinte…). Pour d'autres modalités, la tâche se complique de façon significative. L'acquisition de l'image de l'iris ou du cerveau par exemple est très délicate, car ça nécessite des positions bien précises. Par conséquent, cela nécessite un effort considérable de la part de l'utilisateur.

L'acceptation d'une modalité par un utilisateur est liée à des paramètres sociaux, psychologiques et parfois sanitaires. La signature par exemple est une pratique quotidienne, c'est pourquoi elle est la plus acceptée des modalités biométriques. Quant à l'iris, les gens hésitent toujours à l'utiliser à cause des rayons laser qui traversent les yeux de l'individu et qui peut provoquer des problèmes de santé. Les modalités cachées ont aussi du mal à être acceptées à cause de forts risques sanitaires qui peuvent être engendrés par leurs utilisations.

Tableau 1.1: Comparaison entre les modalités biométriques en matière de simplicité et acceptabilité

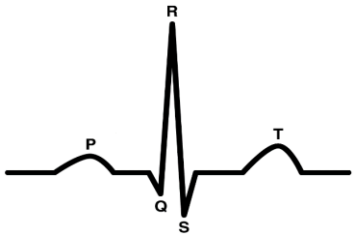
Type	**Modalité**	**Précision**	**Simplicité d'utilisation**	**Acceptation par l'utilisateur**
Morphologique	Empreinte	Haute	Moyenne	Haute
	Iris	Haute	Moyenne	Moyenne
	Rétine	Haute	Basse	Basse
	visage	Basse	Haute	Haute
	Voix	Moyenne	Haute	Haute
	Géométrie de la main	Moyenne	Haute	Moyenne
Comportementale	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 rayons X	Haute	Basse	Basse

1.8 Modalités cachées

Ces modalités sont un concept biométrique particulièrement robuste. En comparaison aux modalités biométriques classiques qui sont à la base des caractéristiques évidentes de l'être humain, les modalités cachées considèrent plutôt les caractéristiques intrinsèques et non visibles du corps humain [39].N'importe quel signal physiologique ou organe humain est potentiellement un candidat pour des applications biométriques [40]. Dans la première catégorie, nous pouvons employer l'électrocardiogramme (ECG), l'électromyogramme (EMG). Dans la deuxième catégorie, nous pouvons considérer, comme exemple, la morphologie ou la texture du cerveau humain. Voici quelques exemples de ces modalités :

1.8.1 Electrocardiogramme ECG

L'ECG est un signal représentant l'activité cardiaque d'un individu. 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.



La biométrie par ECG a fait l'objet d'un certain nombre de travaux [41-43]. Son utilisation 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 [44]. D'autres basées sur l'intégration des caractéristiques analytiques et d'apparence extraite des signaux ECG [45].

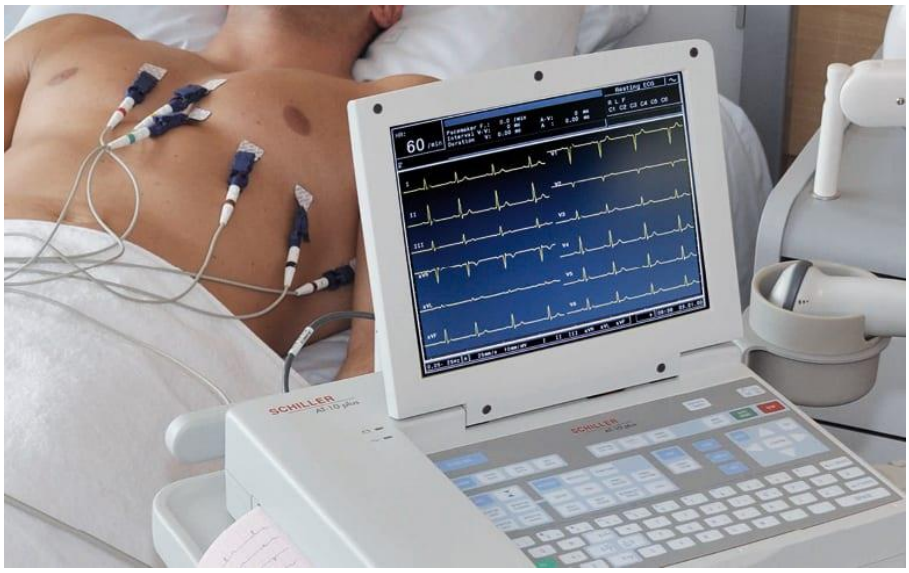


Figure 1.14 : Biométrie par ECG

.

1.8.2 Electromyogrammes EMG

Les signaux électromyogrammes (EMG) sont des signaux bioélectriques enregistrés au niveau des muscles. Ils fournissent des informations diverses sur l'état des nerfs périphériques.

Le signal d'EMG a plusieurs applications cliniques. Son utilisation en tant que modalité biométrique cachée peut être particulièrement intéressante. Dans ce contexte, quelques expériences récentes ont été relatés dans les publications [39-40]et [45]. En particulier, ces travaux ont mis l'accent sur l'analyse des signaux électromyographie de surface (SEMG) [46]. 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 **1.15).** 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 les individus.

Figure 1.15 : Biométrie par l'EMG

1.8.3 Biométrie du cerveau avec des images IRM

Dans des applications médicales, l'IRM (imagerie par résonance magnétique) est une technique de formation image non envahissante employée pour visualiser des images en 2D ou 3D des organes du corps humain (par exemple le cerveau, les muscles, ou le cœur) avec une résolution relativement élevée. Ceci est rendu possible avec l'utilisation d'un champ électromagnétique puissant et constant, produit par un supraconducteur.

La Biométrie par le cerveau [47]cherche à caractériser le cerveau humain à travers des images IRM 2D et 3D [48]. Depuis les images IRM 2D, on peut faire la reconstruction en 3D du cerveau pour avoir des informations sur sa 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 le ***Brain Code*** ou code du cerveau à travers une segmentation de la zone d'intérêt du cerveau [49].

L'avantage principal de ce type de modalité cachée est le fait que le cerveau est totalement protégé contre toutes sortes de changements. Il est

difficile d'imaginer qu'un individu modifie la structure de son propre cerveau pour usurper l'identité d'un autre individu. Cependant, l'inconvénient principal de cette modalité est la non-disponibilité de systèmes d'IRM robuste consacrés à la biométrie.

Figure 1.16 : Biométrie du cerveau avec des images IRM

1.8.4 Biométrie avec des images de rayon X

La radiographie est une technique d'imagerie de transmission par 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. La radiographie est utilisée en radiologie médicale, en radiologie industrielle et en radiothérapie.

La radiographie médicale permet le développement d'images en 2D des os humains. Avec ce type d'images, des structures d'os sont clairement accentuées.

L'application de ce type de technologie dans la biométrie est envisageable en exploitant des images radiographiques de la main par exemple (figure **1.17**) où le but est de caractériser les phalanges à l'aide de quelques outils de traitement d'images [39].

Figure 1.17 : Biométrie de la main avec des images à rayon X

1.9 Les limite de la biométrie.

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux : le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent.

Prenons le cas le plus simple, celui des empreintes digitales (mais la même chose s'applique à toute donnée physique). Suivant les cas, nous présentons plus ou moins de transpiration, la température des doigts n'est pas régulière. Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Dans la majorité des cas, les mesures du capteur et du logiciel associé retourneront un résultat différent de la mesure initiale de référence. Or, il faut pourtant bien réussir à se faire reconnaître. En pratique, cela sera réalisé dans la plupart des cas car le système est amené à autoriser une marge d'erreur entre la mesure et la référence.

De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sûr sur la

façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle. De plus, les experts techniques mettent au passif cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, confronté à une personne qui a subtilisé un mot de passe ou une signature manuscrite, le titulaire du mot de passe ou de la signature peut facilement les remplacer ou les révoquer. La chose semble plus complexe pour une empreinte digitale ou une image rétinienne. Si un tiers s'approprie une identité biométrique du type empreintes digitales ou identité visuelle, il peut au moyen de ces identités biométriques passer tout type d'actes au nom de la victime. Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Les experts en sécurité sont partagés sur la question, même si, en majorité, ils semblent considérer que cette révocation est possible. Tous reconnaissent cependant la difficulté à mettre au passif cette protection technique.

Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, etc…. Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure. Si la biométrie se généralise dans notre environnement, il est dangereux de penser qu'il s'agit de la réponse à tous les problèmes de sécurité. La biométrie, de par ses limites fonctionnelles, techniques et juridiques n'est en aucun cas synonyme de technologie miracle et de sécurité absolue [50].

1.9.1 Les limites fonctionnelles

Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne

peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.

1.9.2 Les limites techniques

Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau [50].

1.10 Applications biométriques

La biométrique peut être utilisée dans plusieurs applications qui nécessitent la sécurité ou pour connaître l'identité de la personne. Ces applications peuvent être divisées en trois groupes principaux qui sont :

- **Applications commerciales** : telles que l'accès au réseau informatique, au téléphone mobile, à l'accès internet, au commerce électronique, à la sécurité des données électroniques, des cartes de crédit, etc.
- **Applications juridiques** : telles que la recherche criminelle, l'identification terroriste, etc.
- **Les demandes gouvernementales** : telles que le passeport, la carte nationale, le permis de conduire, la sécurité sociale, etc… [51].

1.11 Conclusion

A travers ce premier chapitre, nous avons défini la biométrie, ses propriétés, le principe de fonctionnement des systèmes biométriques, les différentes modalités ainsi que les 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 les travaux futurs, par l'application et le développement des descripteurs de texture locaux appropriés.

Chapitre 2: Etat de l'art sur la signature

2.1 Introduction

Les signatures manuscrites étaient la première méthode disponible avant même l'avènement des ordinateurs. Les signatures manuscrites sont utilisées depuis longtemps pour la vérification d'identité en finance. Beaucoup de travail a été fait dans le domaine de la reconnaissance et de la vérification des signatures manuscrites [52].

L'étude de la signature manuscrite est un cas particulier de l'expertise des documents manuscrits. En effet, l'information disponible pour analyser une signature est relativement réduite, comparée aux textes manuscrits. En outre, une signature plus que toute autre forme d'écriture, est le résultat d'un geste spontané et quasi-automatique.

L'habilité du scripteur constitue un élément important de l'authentification. Le scripteur débutant appuie lentement sur le papier, demeure stationnaire avant d'aborder le tracé de la signature et produit des traits irréguliers. Dans le cas du scripteur habile, la plume est en mouvement avant de toucher le papier et produit des traits réguliers. Ainsi l 'habilité du scripteur influence la qualité du tracé.

Les variations naturelles dans le tracé sont des caractéristiques intrinsèques de la signature authentique. En effet, deux signatures parfaitement identiques, indiquent que nous sommes probablement en présence d'une falsification. Ces variations sont affectées par plusieurs facteurs tels que l'état de santé et émotionnel de l'individu, l'âge et la fréquence de l'écriture [53-55]. De plus, une étude effectuée par Evette et Totty [56] démontre la variabilité dans les proportions d'une signature. Il est donc nécessaire de toujours isoler les spécimens dans le temps et de comparer les signatures litigieuses avec des authentiques provenant d'une même période [57].

L'utilisation de la signature manuscrite comme moyen d'un bon engagement entre le niveau de sécurité (fiabilité), la facilité d'utilisation et le prix (la signature ne nécessite pas de coûts supplémentaires pour le capteur) [58].

Quant à la reconnaissance des signatures, on peut parler de la reconnaissance des signatures manuscrites hors ligne et en ligne :

a) Le système de traitement des signatures en ligne « *Online* »

La signature est obtenue à partir d'une tablette numérique reliée à un ordinateur. Cette méthode permet d'exploiter des informations dynamiques telles que la vitesse, la pression et/ou l'inclinaison du stylo. Ces systèmes sont surtout utilisés pour contrôler l'accès à des zones protégées ou pour vérifier l'identité lors d'une transaction en ligne (pourvu qu'on ait les dispositifs de saisie adéquats). Ces systèmes ne peuvent pas être utilisés pour vérifier des signatures déjà apposées sur des documents (chèques bancaires par exemple)[58].

b) Le système de traitement des signatures hors ligne « offline »

Ne nécessite qu'une image de signature, qui doit être analysée d'une manière ou d'une autre. Ces systèmes n'exigent pas la présence de la personne pour son identification.

La signature est numérisée à partir d'un support physique tel un chèque ou tout autre document. Cependant, ces systèmes permettent de vérifier les signatures à un temps différé [58].

2.2 Système d'authentification de signature (SAS)

La conception de tels systèmes nécessite généralement deux phases principales : l'apprentissage et le test. Le système d'authentification par

signature (SAS) conçu à des fins d'identification ou de vérification de scripteurs peut être illustré par la figure 2.1.

En gros, l'apprentissage d'un SAS est réalisé en apprenant au système plusieurs échantillons de signature afin de pouvoir authentifier une signature interrogée (inconnue) en phase de test. Dans le pipeline des deux phases, quatre étapes principales sont nécessaires : acquisition de données pour l'acquisition de signature des échantillons, prétraitement pour améliorer et mettre en évidence les informations contenues dans les signatures, génération de caractéristiques qui extrait les informations pertinentes des signatures dans un vecteur de caractéristique set, enfin, le processus de classification qui détermine l'authenticité d'un signature soit en la vérifiant, soit en l'identifiant [59].

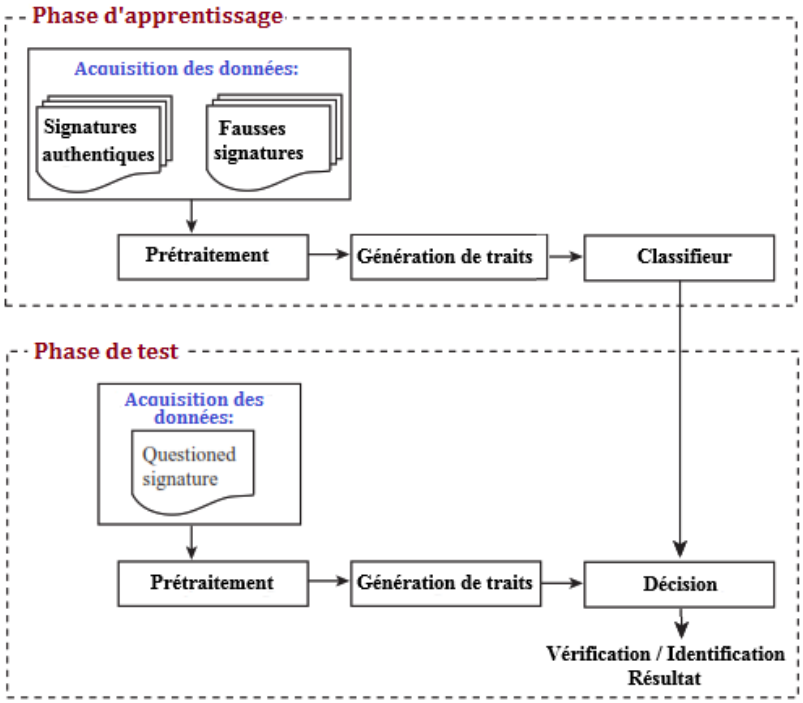


Figure 2.1 : Système d'authentification par signature

La structure d'un tel système est généralement composé de deux phases principales : l'apprentissage et le test. En général, l'entrainement d'un SAS

consiste à apprendre de multiples échantillons de signatures afin d'être en mesure d'authentifier une signature inconnue lors de la phase de test.

De plus amples détails sur les méthodes utilisées pour chacune de ces étapes sont donnés dans les sections suivantes.

2.3 L'acquisition des données

La première étape d'un système d'authentification de signature (SAS) est l'acquisition de données (en d'autres termes, l'acquisition de signatures). Comme le montre la figure 2.2, il existe deux approches pour développer de tels systèmes : en ligne (dynamique) et hors ligne (statique).

(a) Signature en ligne sur une tablette(b) Signature hors ligne sur une feuille de papier

Figure 2.2 : Acquisition de la signature en ligne et hors ligne

L'approche de vérification des signatures en ligne permet une acquisition en temps réel, dans laquelle les utilisateurs s'inscrivent sur un matériel spécialisé à l'aide d'un stylet instrumenté. Toutefois, dans ce cas, le processus de signature ne peut être naturel car les utilisateurs doivent adapter leur écriture au dispositif numérique. C'est pourquoi, certains travaux ont tenté de surmonter ce problème en produisant des stylos électroniques capables de détecter des informations dynamiques, telles que les positions, la vitesse, l'accélération, la pression et l'inclinaison du stylo (Shimizu et al, 2004 ; Malik et al, 2012).

Dans les systèmes hors ligne, les souscripteurs signent sur une feuille de papier, qui est ensuite numérisée avec un scanner optique ou un appareil photo

numérique. Ainsi, la signature est représentée comme une image en niveaux de gris. De toute évidence, les systèmes en hors ligne sont moins précis que les systèmes en ligne, car les informations dynamiques sont perdues. Néanmoins, ils ont des domaines d'application plus pratiques, comme l'approbation de documents juridiques ou officiels, la signature de lettres et l'exécution de transactions bancaires. De ce fait, l'approche hors ligne est considérée comme une tâche difficile, qui a suscité beaucoup d'intérêt (Ruiz-del Solar et al., 2008, Favorskaya et Baranov, 2014 ; Pal et al, 2016.) et c'est pour cela, que notre étude s'est porté sur l'authentification des signatures manuscrites en hors ligne [**8**].

2.4 Prétraitement

L'étape de prétraitement vise à améliorer la qualité des images des signatures. Cette étape est très décisive, car un mauvais prétraitement peut entraîner une perte d'informations. Par conséquent, le bon choix peut faciliter l'extraction des caractéristiques pertinentes lors de l'étape suivante. Dans les sections suivantes, nous présentons quelques techniques élémentaires de prétraitement pour l'authentification des signatures manuscrite shors ligne.

Les plus courantes sont : la suppression du bruit, la binarisation, la normalisation de la taille, l'extraction de la signature et la représentation de la signature. Rappelons que l'utilisation de chacune d'entre elle dépend de la qualité de la signature ainsi que du schéma de génération de caractéristiques adopté. Actuellement, la binarisation et l'extraction de signature sont employées dans cette étude.

2.4.1 Suppression du bruit

Le processus de numérisation peut produire du bruit dans l'image de la signature numérisée, comme des pixels noirs sur un fond blanc ou des pixels blancs ~~uniques~~ sur un fond noir. Le plus souvent, un filtre de suppression du

bruit, tel qu'un filtre médian, est appliqué pour purifier l'image initiale (Baltzakis et Papamarkos, 2001). De même, certaines autres opérations morphologiques peuvent être utilisées pour combler les petits trous et/ou supprimer les petites composantes générées principalement par un fond bruyant (Huang et Yan, 1997) [59].

2.4.2 Binarisation

La binarisation a pour but de transformer les images des signatures de l'échelle de gris en des images en noir et blanc, afin de faciliter l'extraction des entités des signatures de leur arrière-plan. Pour réaliser une bonne binarisation, déférents algorithmes ont été proposés dans la littérature. On peut citer deux types : la binarisation globale et la binarisation locale. La première utilise un seul seuil pour l'ensemble de l'image. Par exemple, Ammar et al. (1988) ; Kiani et al. (2009) ont utilisé la méthode d'Otsu pour binariser les images de signature. Cette méthode de seuillage sélectionne automatiquement le seuil optimal séparant deux classes de pixels (ceux de l'avant-plan et de l'arrière-plan) en recherchant la somme minimale des mesures de dispersion (variance intra-classe). Par contre, Bansal et al. (2008) ont utilisé un algorithme de binarisation locale appelé la méthode Niblack, dans laquelle la valeur du seuil est calculée localement pour chaque région de l'image en considérant la moyenne locale et l'écart type local [59].

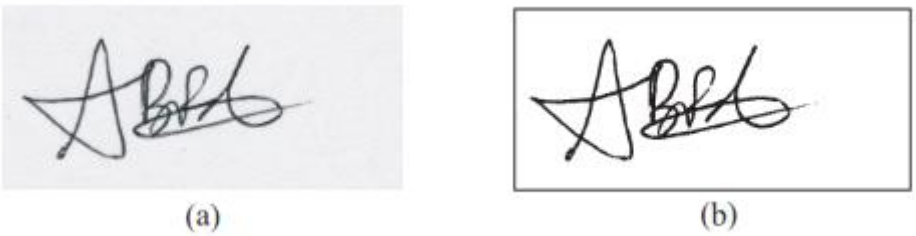


Figure 2.3 : Exemple de binarisation de signature (a) Image de la signature originale (b) signature binarisée

2.4.3 Normalisation de la taille

La hauteur et la largeur des images de signature peuvent varier d'une personne à l'autre et parfois, même la même personne peut avoir des signatures de tailles différentes. Ainsi, la normalisation des images de signature à une même taille fixe en la réduisant peut permettre un traitement plus rapide lors de la génération des caractéristiques. En général, une normalisation linéaire est effectuée en définissant une taille de cadre fixe (largeur/hauteur) pour ajuster la taille de l'image tout en gardant le rapport hauteur/largeur inchangé (Baltzakis et Papamarkos, 2001 ; Pourshahabi et al., 2009 ; Soleymanpour et al., 2010).

2.4.4 Extraction de signature

L'extraction de la signature (cette opération est également appelée segmentation) consiste à trouver la boîte englobante des signatures. Le défi dans ce cas est surtout lorsque la signature est écrite sur un fond complexe comme dans le cas des chèques bancaires qui contiennent un fond pictural en couleur, plusieurs logos et de nombreuses directives pré-imprimées (Dimauro et al., 1997 ; Djeziri et al.,1998 ; Hafemann et al, 2015). Dans notre travail, les signatures sont toutes écrites sur un fond homogène et, par conséquent, la segmentation élimine juste le fond environnant. La figure 2.4 illustre cette prétraitement.

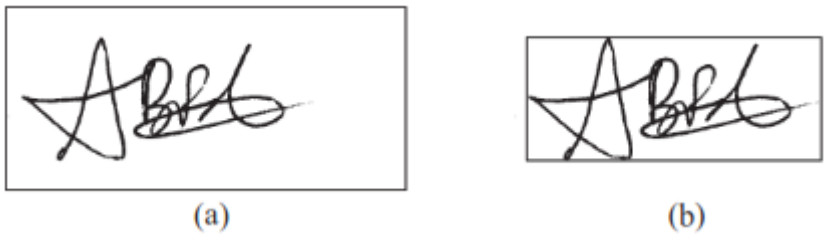


Figure 2.4 : Exemple d'extraction de la signature (a) Image originale de la signature (b) Signature extraite

2.4.5 Représentation de la signature

La représentation de la signature est une technique de prétraitement qui transforme l'image de la signature en une autre forme plus représentative. Plutôt

que d'extraire les caractéristiques directement de l'image en niveau de gris, le descripteur est alors fondé sur cette représentation. Les plus courantes dans la littérature sont : la squelettisation, la représentation du contour, la distribution de l'encre et de la frontière directionnelle. (Voir figures 2.5 et 2.6).

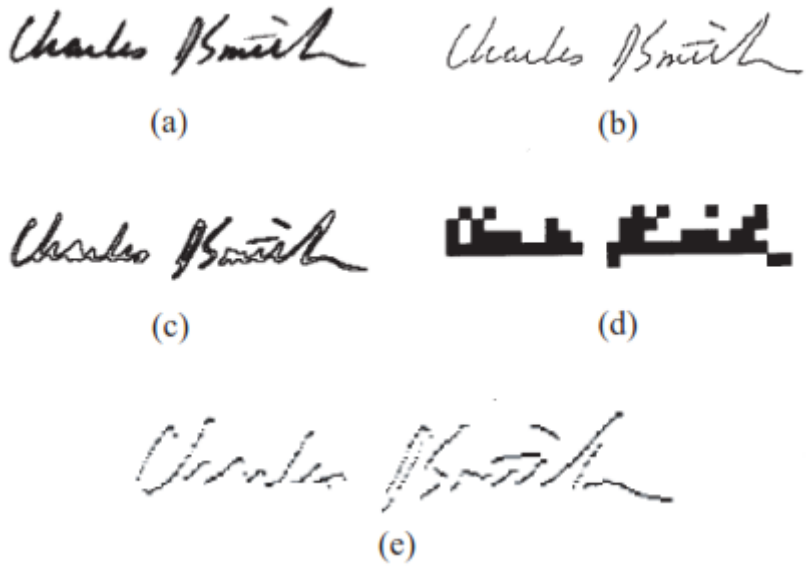


Figure 2.5 : Représentation de la signature (a) Original, (b) Squelette, (c) Contour, (d) Distribution de l'encre (e) Frontière directionnelle

Figures 2.6 :Représentation des contours (a) Originale, (b) Dilatée, (c) Remplie, (d) Contour de la signature

La squelettisation, également appelée amincissement, est une représentation structurelle des signatures qui élimine les différences d'épaisseur des stylos en rendant l'image épaisse d'un pixel (Ozgunduz et al., 2005). La représentation du contour extrait le contour de la signature qui donne une information globale sur sa forme (Huang et Yan, 1997). Elle peut également être extraite au moyen d'opérations morphologiques en dilatant l'image de la signature et en la remplissant afin de simplifier le processus d'extraction des contours (Ferrer et al.,

2005). Une autre représentation vise à décrire la distribution de l'encre de plusieurs traits de signature gros et fins (Huang et Yan, 1997). Elle est réalisée en appliquant une grille virtuelle sur l'image de la signature. Puis une cellule de la grille est remplie si son nombre de pixels appartenant à la signature est supérieur à 50% du total des pixels de la grille. Pour terminer, la frontière directionnelle est une représentation structurelle qui décrit l'information directionnelle des pixels du contour. Elle est calculée en gardant seulement les pixels noirs de l'image de la signature avec les voisins de la frontière blanche (Huang et Yan, 1997) [59].

2.5 Génération de traits caractéristiques

Après avoir accompli les étapes d'acquisition et de prétraitement des données, l'étape suivante consiste à mettre en évidence les informations pertinentes au sein des images de signature en extrayant des traits discriminants. Selon l'information mise en évidence, ces caractéristiques (aussi appelées descripteurs) peuvent être considérées comme : statiques ou pseudo-dynamiques (Hafemann et al., 2015). Les traits statiques sont plus appropriés pour décrire la forme de la signature et leur calcul est simple. Toutefois, les gestes de l'écriture manuscrite ne sont pas correctement caractérisés. Ainsi, les caractéristiques pseudo-dynamiques tentent de récupérer les informations dynamiques à partir d'images de signatures statiques. D'autre part, on peut distinguer les caractéristiques globales et locales. Les caractéristiques globales décrivent l'image de signature dans son ensemble, tandis que les caractéristiques locales extraient les traits de régions spécifiques de l'image de signature. Comme ces dernières extraient des informations plus fines et plus détaillées, elles sont réputées pour être plus précises que les caractéristiques globales, ce qui en fait une approche plus attrayante qui a été adoptée dans plusieurs travaux de recherche (Kiani et al., 2009 ; Yilmaz et al., 2011 ; Ferrer et al., 2012). En outre, il convient de noter que les techniques de caractéristiques globales peuvent

également être appliquées à des régions spécifiques pour fournir des caractéristiques locales et vice versa (Impedovo et Pirlo, 2008). Dans les deux types de caractérisation, statique/pseudo-dynamique et globale/locale, les traits caractéristiques sont généralement classés en plusieurs catégories qui sont décrites dans ce qui suit.

2.5.1 Les traits caractéristiques statiques

Habituellement, les caractéristiques statiques impliquent des mesures géométriques liées à l'occupation de l'espace graphique (Pellegrini et al., 2014). De plus, ils sont connus pour être invariants aux rotations, translations et distorsions. On peut citer la hauteur, la largeur et la surface de l'image de signature comme caractéristiques fondamentales de cette catégorie (Baltzakis et Papamarkos, 2001). D'autres descripteurs plus élaborés sont : le calibre, la proportion, l'espacement et l'alignement par rapport à la ligne de base (Oliveira et al., 2005). Le calibre fait référence au rapport hauteur/largeur de l'image de la signature. La proportion décrit la symétrie d'une image de signature en mesurant la variation de hauteur des lettres. La signature peut être soit proportionnelle (c'est-à-dire que toutes les lettres ont à peu près la même hauteur), soit disproportionnée (c'est-à-dire que la hauteur des lettres est hétérogène) ou mixte, dans laquelle on peut distinguer deux parties proportionnelles. L'espacement révèle les écarts entre les caractères ou les combinaisons de traits dans l'image de la signature. Une signature peut être espacée ou concentrée sans espace entre les caractères. Enfin, l'alignement sur la ligne de base représente l'orientation d'une signature selon une ligne de base de référence. La ligne de base est définie en mettant un trait sous la signature afin de relier ses zones médiane, supérieure et inférieure. Ensuite, l'angle d'inclinaison est défini par une ligne horizontale qui traverse la ligne de base. Selon cette mesure, on peut désigner un alignement ascendant, descendant ou rectiligne [59].

2.5.2 Les traits pseudo-dynamiques

Le terme pseudo-dynamique "désigne les informations dynamiques résultant du processus de signature qui peuvent être reconstruites à partir d'une image de signature statique. En plus des caractéristiques statiques, Oliveira et al. (2005) ont introduit de nouvelles caractéristiques géométriques pseudo-dynamiques pour les caractérisations de signature en ligne. Précisément, trois ensembles de caractéristiques qui sont calculées localement en appliquant une grille uniforme sur les images de signature ont été proposés.

La densité des pixels est calculée en comptant le nombre de pixels noirs sur chaque cellule de l'image. Il est important de souligner que la densité peut nous renseigner sur la pression apparente des traits de signature locaux. Un autre descripteur calculé localement est la distribution des pixels qui calcule quatre mesures sur chaque cellule de l'image. Ces mesures représentent la largeur du trait calculée en fonction de quatre zones sur chaque cellule. Enfin, la progression effective qui détermine le niveau de tension qui fournit des informations sur la vitesse, la continuité et l'uniformité des traits. Pour cela, le trait le plus significatif sur chaque cellule (c'est-à-dire le plus long) est utilisé pour calculer le nombre de fois que le trait change de direction. Peu de changements font référence à un trait tendu, sinon il est supposé être un trait mou.

D'autre part, outre les caractéristiques géométriques, de nombreuses autres caractéristiques peuvent également être considérées comme pseudo-dynamiques. Par exemple, les informations dynamiques peuvent être reconstituées à l'aide de transformations mathématiques, de caractéristiques statistiques ou de textures ou alors de caractéristiques de gradients [59].

2.6 Approches de vérification de signature

La dernière étape importante de ce système est la vérification : Cette étape compare les signatures de test entrantes avec le modèle de signature de l'utilisateur qui se trouve dans la base de données. Les approches les plus courantes sont les suivantes [60].

2.6.1 Modèle de distance euclidienne

Le modèle de distance euclidienne est l'un des classificateurs les plus appropriés pour obtenir la mesure de la distance entre deux vecteurs de taille égale sur un plan bidimensionnel [61].

Il est utilisé pour calculer la distance entre les caractéristiques extraites comme si nous avions une paire de vecteurs de taille égale pour calculer la distance (d) entre deux vecteurs X(x1,x2, x3, ...,xn) etY(y1,y2,y3,…,yn) en utilisant l'équation suivante :

$$(d) = \sqrt{\sum_{i=1}^{n}(X_i - Y_i)^2} \quad (1)$$

Le modèle de distance euclidienne a été utilisé comme classificateur dans les publications [61-64].

2.6.2 Réseaux neuronaux

Un réseau neuronal est plus efficace si l'on dispose d'un grand nombre d'échantillons. Les réseaux neuronaux sont très adaptés à la modélisation des aspects globaux des signatures manuscrites. Dans [65], un réseau de neurones a été utilisé pour classer les caractéristiques extraites de 3000 images de signatures. Le réseau est entraîné par des échantillons authentiques et faux échantillons générés artificiellement à partir de signatures de référence d'inscription, ce qui permet un contrôle précis de l'entraînement et, en même temps, réduit considérablement le nombre d'échantillons d'inscription requis

pour obtenir une bonne performance. Dans l'article [66], une nouvelle technique de reconnaissance et de vérification de signatures hors ligne est développée. La technique proposée se base sur des caractéristiques globales, de grille et de texture. Pour chacun de ces ensembles de caractéristiques, une structure de classification spéciale OCON (one-class / one-network) à deux étages de Perceptron a été mise en œuvre. La distance euclidienne et le réseau neuronal sont utilisés dans la première étape comme classificateur. Les résultats du classificateur de la première étape alimentent une structure de réseau neuronal à fonction de base radiale (RBF) de la deuxième étape, qui prend la décision finale. Un système de vérification et de reconnaissance hors ligne est présenté dans [67]. Dans ce système, un réseau neuronal à perceptron multicouche (MLP) utilise des caractéristiques telles que l'algorithme de rétro-propagation, l'algorithme FF, la méthode centroïde et la base de données de sérialisation pour stocker des échantillons de signatures qui peuvent être extraits par traitement d'image. En outre, le réseau neuronal a été formé à l'aide de l'algorithme de propagation inverse.

2.6.3 Machines à vecteurs de support

La machine à vecteur de support (SVM), développée par Vapnik en 1998, est une nouvelle technique dans le domaine de la théorie de l'apprentissage statistique. L'objectif de la méthode proposée dans [68] est de mesurer les caractéristiques de niveau de gris d'une image lorsqu'un arrière-plan complexe la déforme en utilisant un classificateur de réseau de neurones et un SVM.

Une machine à vecteur de support à une classe (OC-SVM) est proposée dans [69] sur la base de paramètres indépendants du souscripteur. Le système HSVS ne prend en compte que les signatures authentiques et les signatures falsifiées comme contre-exemples pour la conception du système.

L'OC-SVM est efficace lorsque des échantillons importants sont disponibles pour fournir une classification précise. Une technique efficace d'extraction de

caractéristiques est proposée dans [70] pour la vérification à l'aide d'un classificateur à deux classes, à savoir RBF-SVM (machine à vecteurs de support avec noyau RBF) ou MLP. Dans la publication [71], cinq caractéristiques géométriques uniques et huit caractéristiques Camastra sont extraites de chaque carré. Le SVM est utilisé comme classificateur.

2.6.4 Modèle flou

Diverses règles floues sont utilisées pour juger du type de signature lue, fausse ou authentique. Un système de reconnaissance et de vérification de signature arabe hors ligne en deux phases est décrit dans [72]. Ce système a utilisé un modèle flou dans une phase de vérification pour la prise de décision ; une fois que les points d'intérêt sont sélectionnés, le système attribue des notes floues à ces points en fonction de leur degré de correspondance. La vérification de signature hors ligne utilisant la logique floue est proposée par [73].

2.6.5 Modèle de Markov caché

Les approches de vérification de signature en ligne et hors ligne peuvent utiliser des modèles de Markov cachés (HMM). La reconnaissance de signature hors ligne utilisant un HMM est proposée dans la publication [74]. Dans l'article [75], une comparaison des classificateurs SVM et HMM pour la vérification de signature hors ligne est présentée.

2.7 Conclusion

Dans ce chapitre, nous avons donné l'état de l'art pour l'authentification des signatures manuscrites en hors ligne, et expliqué les différentes techniques utilisées dans chaque phase des systèmes d'authentification (acquisition, prétraitement, génération de caractéristiques et classification). Nous avons clôturé ce chapitre par une discussion des approches de vérifications des signatures. La plupart des travaux de recherche en cours sur le thème de

l'authentification des individus par leurs signatures manuscrites se consacrent à l'obtention de bonnes représentations des traits caractéristiques des signatures, c'est-à-dire à la conception de bons extracteurs de caractéristiques afin d’améliorer les étapes de génération et de classification des traits caractéristiques des signatures.

Chapitre 3: Les outils et techniques utilisés

Dans ce chapitre, nous exposerons les méthodes et les outils de bases adoptés dans nos systèmes biométriques proposés.

3.1 Introduction

Les systèmes de vérification de signature visent à vérifier l'identité des individus en reconnaissant leur signature manuscrite. Ils s'appuient sur la reconnaissance d'un geste précis et bien appris, afin d'identifier une personne. Ceci contraste avec les systèmes basés sur la possession d'un objet (par exemple une clé, une carte à puce) ou la connaissance de quelque chose (par exemple un mot de passe), et diffère également d'autres systèmes biométriques, tels que l'empreinte digitale, puisque la signature reste la plus socialement et légalement le moyen d'identification le plus accepté (Plamondon et Srihari (2000)) [76]. Dans la vérification de signature hors ligne (statique), la signature est acquise une fois le processus d'écriture terminé, en scannant un document contenant la signature et en la représentant sous forme d'image numérique (Impedovo & Pirlo (2008)) [77]. Par conséquent, les informations dynamiques sur le processus de génération de signature sont perdues (par exemple, la position et la vitesse du stylo au fil du temps), ce qui rend le problème très difficile. Définir des extracteurs de caractéristiques discriminantes pour les signatures hors ligne est une tâche difficile. La question « Qu'est-ce qui caractérise une signature » est un concept difficile à mettre en œuvre en tant que descripteur de fonctionnalité. La plupart des efforts de recherche dans ce domaine ont été consacrés à la recherche d'une bonne représentation des signatures, c'est-à-dire à la conception d'extracteurs de caractéristiques adaptés à la vérification de signature, ainsi qu'à l'utilisation d'extracteurs de caractéristiques créés à d'autres fins (Hafemann et al. (2017b)) [78]. Des travaux récents utilisent des caractéristiques de texture, telles que les motifs binaires locaux (LBP) (Hu & Chen (2013)) [79], et le Gray-Level Co-occurrence Matrix (GLCM) (Hu & Chen (2013) [79].(Yılmaz &Yanıkoˇglu (2016)) [80] ; des caractéristiques directionnelles telles que

l'histogramme des gradients orientés (HOG) (Yılmaz &Yanıko˘glu(2016)) [80] et directionnel (Rivard et al. (2013) [81], Eskander et al. (2013)) [82],des extracteurs de caractéristiques spécifiquement conçus pour les signatures, comme l'estimation des traits par ajustement des courbes de Bézier (Bertolini et al. (2010)) [83], entre autres. Aucun extracteur de caractéristiques n'est apparu comme particulièrement adapté à la vérification de signature, et les travaux les plus récents utilise une combinaison de plusieurs de ces techniques.

La difficulté de trouver une bonne représentation des signatures se reflète sur les performances de classification des systèmes de vérification des signatures, en particulier pour distinguer les signatures authentiques des contrefaçons qualifiées. Les contrefaçons qui sont faites ciblant un individu particulier. Lorsque nous considérons les expériences menées sur de grands ensembles de données publics, tels que le GPDS (Vargas et al. (2007)) [84], les meilleurs résultats rapportés atteignent des taux d'erreur égaux d'environ 7%, même lorsque le nombre d'échantillons pour la formation est d'environ 10-15%, avec les pires résultats en utilisant moins d'échantillons par utilisateur. Pour résoudre à la fois le problème de l'obtention d'une bonne représentation des caractéristiques pour les signatures, ainsi que l'amélioration des performances de classification.

3.2 Description du système

La Figure 3.1 illustre les principales étapes du système de vérification hors-ligne de signature proposé.

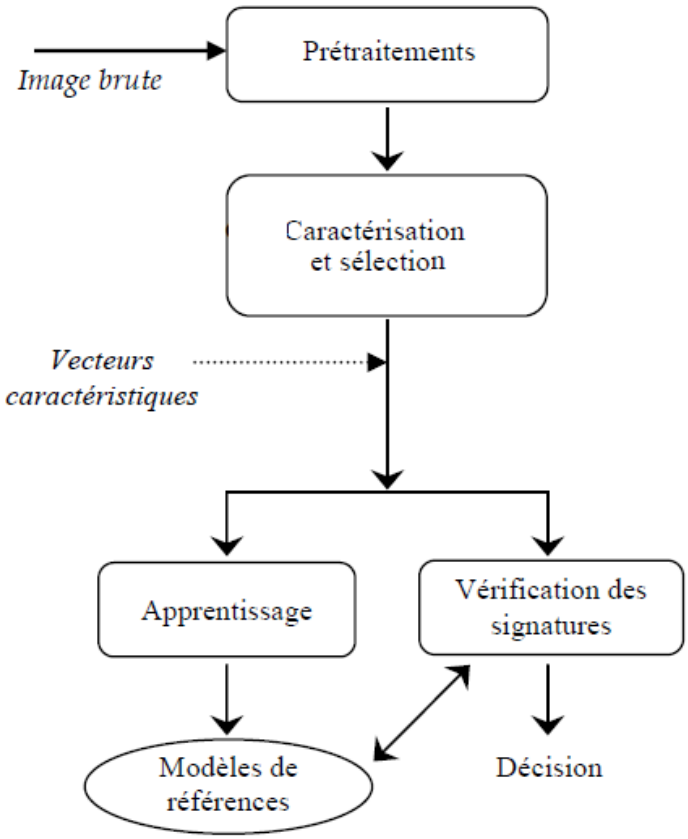


Figure 3.3 : Schéma global du système proposé

3.2.1 Acquisition et prétraitements

Les images des signatures sont numérisées à une résolution de 600 dpi, moyennant un scanner. Après une étape de binarisation, l'image signature subit quatre étapes de prétraitements :

• **Lissage :** Les signatures binaires passent tout d'abord par une étape de lissage pour réduire au maximum les discontinuités introduites dans l'image au cours de l'acquisition et la binarisation. Un filtre médian a été utilisé dans le but de rétablir la régularité et la continuité du contour de la signature (figure 3.2).

• **Extraction des signatures :** Etant donné que les signatures sont numérisées par page (15 signatures par page), un module d'extraction des signatures a été développé la méthode est basée sur les projections horizontales et verticales (figure 3.2).

• **Normalisation de l'orientation :** L'inclinaison des signatures est définie comme étant l'angle entre l'axe correspondant à la direction principale de la forme de la signature et l'axe horizontal. L'objectif de ce prétraitement est de transformer la signature de façon à ce que l'axe de direction principale devienne horizontal. Ceci permet de réduire considérablement la variabilité des signatures.

La méthode mise en œuvre consiste en premier lieu à déterminer l'angle entre l'axe horizontal et la ligne de base de la forme. Par la suite nous procédons à une rotation de l'image de façon à ce que l'angle d'inclinaison soit égal à zéro (figure 2.3).

• **Normalisation de la taille :** C'est la dernière étape des prétraitements, elle a pour objectif la réduction de la variabilité de l'image signature en normalisant la hauteur des signatures tout en gardant la proportionnalité entre la hauteur et la largeur. La largeur est alors calculée par la formule suivante [10] :

$$\boldsymbol{P = h \cdot \frac{H}{L}} \qquad \textbf{(1)}$$

La figure 3.2 présente un exemple de signature de la base et les résultats des différents prétraitements appliqués.

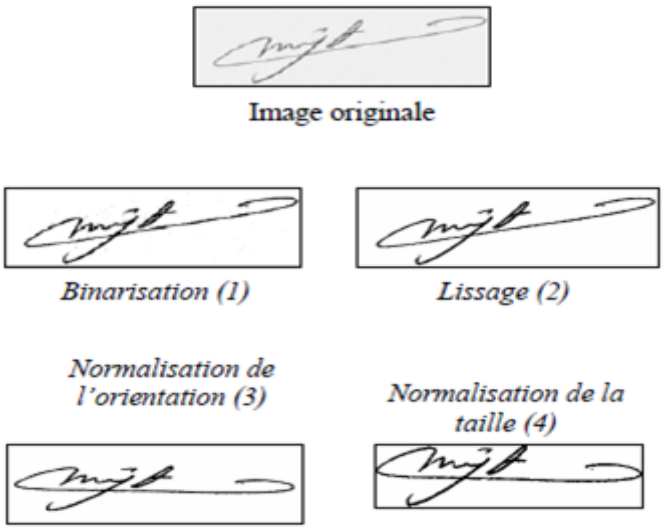


Figure 3.2: Résultats des différentes étapes de prétraitements sur une signature d'une base de données

3.3 Motifs binaires locaux (LBP: Local Binary Pattern)

Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris [86]. Ils consistent à attribuer à chaque pixel $\boldsymbol{P}$ de l'image $\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j})$ à analyser, une valeur caractérisant le motif local autour de ce pixel. Ces valeurs sont calculées en comparant le niveau de gris du pixel central $\boldsymbol{P}$ aux valeurs des niveaux de gris des pixels voisins.

Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement (figure 3.3). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255.

L'opérateur de motif binaire local décrit l'environnement du pixel $(\boldsymbol{x},\boldsymbol{y})$ en générant un code binaire à partir des dérivées binaires d'un pixel comme mesure complémentaire du contraste local de l'image. L'opérateur LBP original prend les huit pixels voisins en utilisant la valeur du niveau de gris central $I(\boldsymbol{x},\boldsymbol{y})$ comme seuil. L'opérateur génère un code binaire 1 si le voisin est supérieur ou égale au niveau central, sinon il génère un code binaire 0. Les huit codes binaires voisins peuvent être représentés par un nombre de 8 bits.

Les résultats de l'opérateur LBP pour tous les pixels de l'image peuvent être accumulés pour former un histogramme, qui représente une mesure de la texture de l'image. La figure 3.1 montre un exemple d'opérateur LBP.

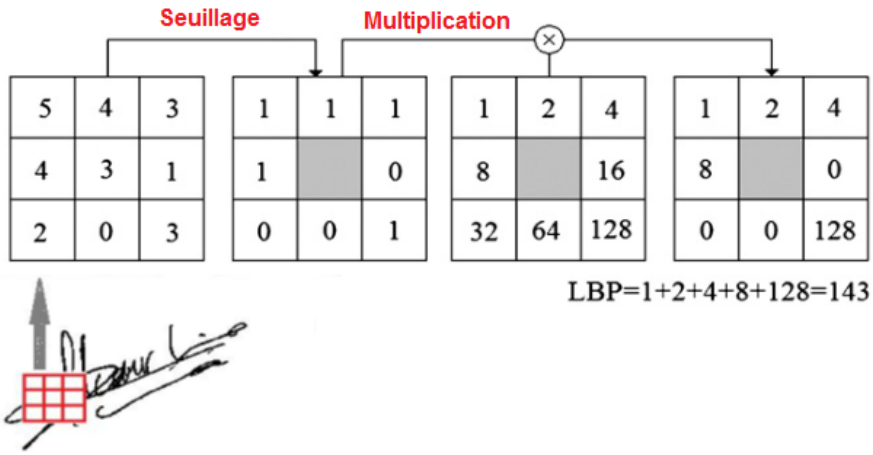


Figure 3.1 : Calcul du code LBP du pixel (x, y). Dans ce cas, I (x, y) = 3, et son code LBP est ***LBP (x, y) =143***.

L'opérateur LBP ci-dessus a été étendu dans un opérateur généralisé de niveau de gris et invariant en rotation. L'opérateur LBP est déduit d'un ensemble de voisins à symétrie circulaire de ***P*** éléments situés sur un cercle de rayon ***R***. Le paramètre ***P*** contrôle la quantification de l'espace angulaire de rotation et ***R*** détermine la résolution spatiale de l'opérateur.

Le code LBP du pixel central $(\boldsymbol{x}, \boldsymbol{y})$ avec ***P*** voisins et un rayon **R** est défini comme suit :

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

Ou $s(l) = \begin{cases} 0 & l \geq 0 \\ 1 & l < 0 \end{cases}$, la fonction échelon unitaire, g_c la valeur de niveau de gris du pixel central : $g_c = I(x,y)$, et g_p le niveau de gris du pième voisin, défini comme

$$g_p = I\left(x + Rsin\frac{2\pi p}{P}, y - Rcos\frac{2\pi p}{P}\right) \qquad (3)$$

Si le p-ième voisin ne se situe pas exactement dans la position du pixel, son niveau de gris est estimé par interpolation. Un exemple peut être illustré par la figure 2.

Dans une étape ultérieure, [38] défines un opérateur $LBP_{P,R}$ invariant à la rotation comme suit :

$$LBP_{P,R}^{riu2}(x,y) = \begin{cases} \sum_{p=0}^{p-1} s(g_p - g_c) & si \quad U(x,y) \leq 2 \\ P+1 & Si\ non \end{cases} \tag{4}$$

où

$$U(x,y) = \left|s(g_p - g_c) - s(g_{p-1} - g_c)\right|, \quad avec \ \ g_p = g_0 \tag{5}$$

En analysant les équations ci-dessus, $U(x,y)$ peut être calculé comme suit :

1. calculer la fonction $f(p) = s(g_p - g_c), 0 < p < P$ en considérant que $g_p = g_0$;
2. Obtenir sa déviation : $f(p) - f(p-1), 1 \leq p \leq P$;
3. Calculer la valeur absolue : $|f(p) - f(p-1)|, 1 \leq p \leq P$
4. Obtenir $U(x,y)$ comme l'intégration ou la somme $\sum_{p=1}^{P}|f(p) - f(p-1)|$.

Si les niveaux de gris des pixels voisins (x,y)sont uniformes ou réguliers, comme dans le cas de la figure 3, à gauche, $f(p)$ sera une séquence de "0" ou "1" avec seulement deux transitions.

Dans ce cas, $U(x,y)$ sera égal à zéro ou à deux et le code $LBP_{P,R}^{riu2}$ est calculé comme la somme $\sum_{p=0}^{P-1} f(p)$.

Inversement, si les niveaux de gris environnants le pixel (x,y) varient rapidement, comme dans le cas de la figure 3, à droite, $f(p)$ sera une séquence contenant plusieurs transitions "0"-"1" ou "1"-"0" et $U(x,y)$ sera supérieur à 2.

Ainsi, dans le cas bruyant, une valeur constante égale à P+1 est attribuée à $LBP_{P,R}^{riu2}$, ce qui le rend plus robuste au bruit que les opérateurs LBP précédemment définis.

La propriété d'invariance à la rotation est garantie car lors de la sommation de la séquence $f(p)$ pour obtenir le $LBP_{P,R}^{riu2}$, elle n'est pas pondérée par 2^p. Comme $f(p)$ est une séquence de 0 et 1, $0 \leq LBP_{P,R}^{riu2}(x,y) \leq P+1$. Comme mesure texturale, nous utiliserons ses P+2 histogramme des codes $LBP_{P,R}^{riu2}(x,y)$.

Parmi les trois codes LBP décrits dans la section précédente, $LBP, LBP_{P,R}\ et\ LBP^{riu2}_{P,R}$, nous utiliserons dans notre travail le $LBP^{riu2}_{P,R}$, en raison de ses propriétés d'invariance rotationnelle.

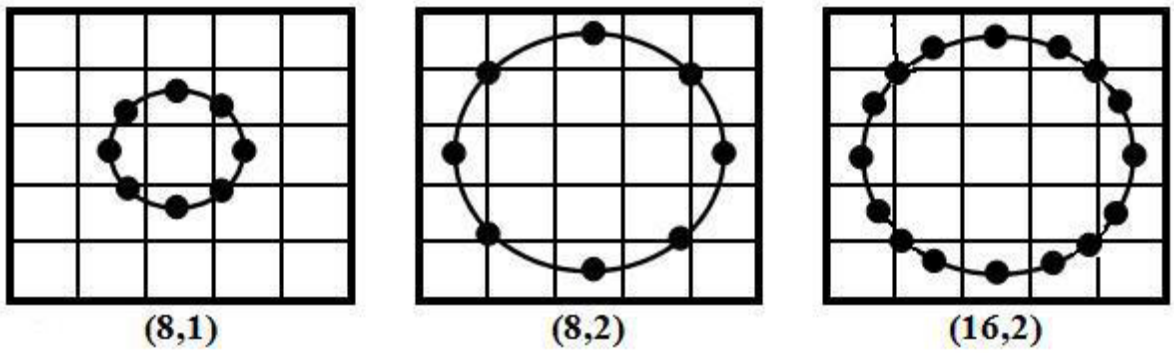


Figure 3.2: LBP multi-échelle. Exemples de voisinages obtenus pour différentes valeurs de (P, R), source Ojala et al

La propriété la plus importante de l'opérateur LBP dans les applications du monde réel réside dans son invariance contre les changements monotones du niveau de gris causés, par exemple, par des variations d'éclairage. Une autre propriété aussi importante réside dans sa simplicité de calcul, qui permet d'analyser des images compliquées en temps réel [87].

3.4 Caractéristiques statistiques et binarisées de l'image (BSIF : Binarized Statistical Image Features)

Le nouveau descripteur BSIF a été initialement proposé en 2012 par J. Kannala et E. Rahtu [88] à partir d'une inspiration des techniques LBP et LPQ. Ces deux méthodes qui décrivent le voisinage de chaque pixel par un code binaire obtenu en effectuant au préalable une convolution de l'image avec un ensemble de filtres linéaires, puis en binarisant les réponses des filtres. Les bits de la chaîne de code correspondent aux réponses binarisées des différents filtres.

Toutefois, l'objectif principal du BSIF est d'extraire une représentation significative d'une image à partir de ses caractéristiques statistiques en se basant

sur un apprentissage automatique d'un ensemble fixe de filtres à l'aide d'un ensemble réduit d'images naturelles pour construire un code binaire pour chaque pixel par projection linéaire des patchs locaux de l'image sur un sous-espace dont les vecteurs de base sont instruits à partir d'images naturelles par l'analyse en composantes indépendantes (ICA : Independent Component Analysis,) et en utilisant la binarisation des coordonnées dans cette base par le seuillage [89].

3.4.1 La philosophie du descripteur BSIF

Le BSIF calcule une chaîne de codes binaires pour les pixels d'une image donnée. La valeur du code d'un pixel est considérée comme un descripteur local du motif d'intensité de l'image dans l'environnement du pixel. De plus, les histogrammes des valeurs de code des pixels permettent de caractériser les propriétés des textures des patchs (dans les sous-régions) des images. Ainsi, le descripteur BSIF peut être utilisé dans les tâches de reconnaissance de texture de la même manière que les motifs binaires locaux (LBP) [90].ou les valeurs quantifiées de phase locale (LPQ) [91].

La valeur de chaque bit de la chaîne de code binaire est calculée en binarisant la réponse d'un filtre linéaire avec un seuil nul. Chaque bit est associé à un filtre différent et la longueur désirée de l'élément détermine le nombre de filtres utilisés. L'ensemble des filtres est entrainé à partir d'un ensemble de patchs d'images naturelles en maximisant l'indépendance statistique des réponses des filtres [92]. Par conséquent, les propriétés statistiques des patchs d'images naturelles déterminent les descripteurs et c'est pourquoi, on les nomme descripteurs d'images statistiques binarisées (BSIF). L'apprentissage des filtres linéaires est abordé en détail dans la publication de Hyva¨rinen [92].

3.5 Analyse Discriminante Linéaire(LDA)

L'algorithme LDA est né des travaux de *Belhumeuretal.* De l'Université Yale(New Haven, USA),en1997. Il est aussi connu sous le nom de *Fisherfaces*.

Contrairement à l'algorithme PCA, l'algorithme LDA effectue une véritable *séparation de classes*(figure 3.5).

Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'images d'apprentissage en plusieurs classes: une classe par personne et plusieurs images par classe. Le LDA analyse les vecteurs propres de la matrice de dispersion des données ,avec pour objectif de maximiser les variations interclasses tout en minimisant les variations intra-classes.

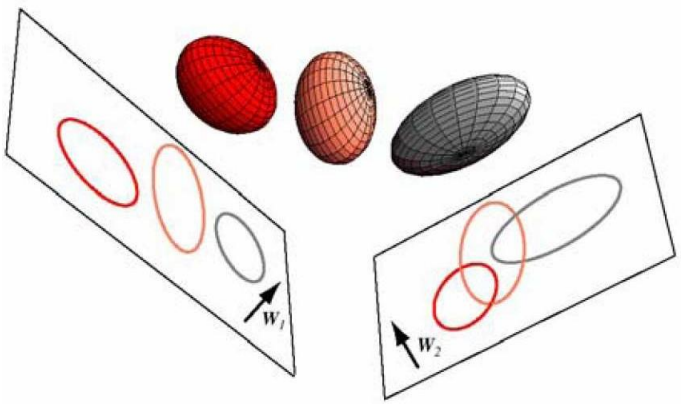


Figure 3.3 : Illustration du principe de séparation optimale des classes par le LDA. Trois distributions 3D sont projetées sur deux sous-espaces 2D décris par les vecteurs W1et W2.Puisque le parmi les classes, on voitbienqueW1estici le vecteur optimal [Baht03].

Tout comme dans le PCA, on rassemble les images de la base d'apprentissage dans une grande matrice d'imagesΓoù chaque colonne représente une image Γ_i,puis on calcule l'image moyenne Ψ.

Ensuite ,pour chaque classe C_i,on calcule l'image moyenne Ψ_{Ci} :

$$\boldsymbol{\Psi_{C_i} = \frac{1}{q_i}\sum_{k=1}^{q_i}\Gamma_k} \qquad \textbf{(6)}$$

Avec q_i,le nombre d'images dans la classe C_i.

Chaque image$\Gamma_i$de chaque classe C_i est ensuite recentrée par rapport à la moyenne. On obtient alors une nouvelle imageΦ_i:

$$\boldsymbol{\Phi_i = \Gamma_i - \Psi_i} \qquad \textbf{(7)}$$

Vient ensuite le calcul de nos différentes matrices de dispersion. On notera c le nombre total de classes (i.e. le nombre d'individus), qi le nombre d'images dans la classe Ci et M le nombre total d'images.

1. La Matrice de Dispersion Intra-classe ($\boldsymbol{s_w}$)

$$\boldsymbol{s_w} = \sum_{i=1}^{c} \sum_{\Gamma_k \in C_i} (\Gamma_k - \boldsymbol{\Psi_{Ci}})(\Gamma_k - \boldsymbol{\Psi_{Ci}})^T \quad \textbf{(8)}$$

2. La Matrice de Dispersion Interclasse ($\boldsymbol{s_b}$)

$$\boldsymbol{s_b} = \sum_{i=1}^{c} q_i (\boldsymbol{\Psi_{Ci}} - \boldsymbol{\Psi})(\boldsymbol{\Psi_{Ci}} - \boldsymbol{\Psi})^T \quad \textbf{(9)}$$

3. La Matrice de Dispersion Totale ($\boldsymbol{s_T}$)

$$\boldsymbol{s_T} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} \boldsymbol{q_i} (\boldsymbol{\Gamma_i} - \boldsymbol{\Psi})(\boldsymbol{\Gamma_i} - \boldsymbol{\Psi})^{\boldsymbol{T}} \quad \textbf{(10)}$$

Une fois ces matrices calculées ,nous devons trouver une projection optimale *W* qui minimise la dispersion intra-classe , relative à la matriceS_W,tout en maximisant la dispersion interclasse, relative à la matriceS_b.

En d'autres termes, nous devons trouver *W* qui maximise le *critère d'optimisation de Fisher* **J** (T):

$$\boldsymbol{W} = \arg \underbrace{\boldsymbol{max}}_{\boldsymbol{T}} \big(\boldsymbol{J}(\boldsymbol{T})\big)$$

$$\Longrightarrow \boldsymbol{max}\big(\boldsymbol{J}(\boldsymbol{T})\big) = \frac{|\boldsymbol{T^T S_b T}|}{|\boldsymbol{T^T S_w T}|} \boldsymbol{T} = \boldsymbol{W} \quad \textbf{(11)}$$

W peut être trouvée en résolvant le problème généralisé aux valeurs propres [Golu04]:

$$\boldsymbol{S_b W} = \boldsymbol{\lambda_w S_w W} \quad \textbf{(12)}$$

Une fois $\boldsymbol{W}$ trouvée, le même schéma que le PCA concernant la projection des images apprises ainsi que la projection d'une image test appliqué.

Ainsi, la projection vectorielle d'une image apprise réajustée par rapport à la moyenne Φ_i est définie par:

$$g(\boldsymbol{\Phi_i}) = W^T \boldsymbol{\Phi_i}$$

La phase de reconnaissance d'une image test $\boldsymbol{\Phi_t}$ s'effectue en projetant $\boldsymbol{\Phi_t}$ sur W^T:

$$g(\boldsymbol{\Phi_i}) = W^T \boldsymbol{\Phi_i}$$

Enfin, on effectue une mesure de distance entre l'image testet l'image projetée sur l'espace vectoriel engendré par$\boldsymbol{W^T}$.Par exemple ,pour la distance euclidienne, on calcule la distance d_{ti}:

$$\boldsymbol{d_{t_i}} = \|\boldsymbol{g(\Phi_t) - g(\Phi_i)}\|$$

d'où

$$\boldsymbol{d_{t_i}} = \sum \sum_{\boldsymbol{k=1}}^{\boldsymbol{c}} \big(\boldsymbol{g(\Phi_t) - g(\Phi_i)}\big)^{\mathbf{2}} \quad \textbf{(13)}$$

Finalement ,une image test est dans la classe dont la distance est minimale par rapport à toutes les autres distances de classe.

En résumé ,l'algorithme LDA permet d'effectuer une véritable séparation de classes, selon un critère mathématique qui minimise les variations entre les images d'un même individu (variations intra-classe) tout en maximisant les variations entre les images d'individus différents (variations interclasses).

Cependant ,pour des problèmes «sous-échantillonnés» en reconnaissance du visage, c'est-à-dire lorsque le nombre d'individu sà traiter est plus faible que la résolution de l'image, il est difficile d'appliquer le LDA qui peut alors faire apparaître des matrices de dispersions singulières(non inversibles).Afin de contourner ces problèmes ,certains algorithmes basés sur le LDA ont récemment été mis au point (par exemple ,les algorithmes ULDA,OLDA,NLDA et WLDA).

3.6 Comparaison

Comme de nombreux systèmes de reconnaissance automatique decibles , la performance des systèmes de vérification de signature hors ligne repose sur la précision avec la quelle les système peut faire correspondre ou rejeter correctement des échantillons précédemment non vus aux modèles contenus dans sa base de données.

Dans un système de vérification de signature hors ligne, la performance est évaluée en termes de taux de fausses acceptations (FAR) et de taux de faux rejets (FRR).

- ***FAR*** (**F**alse **A**cceptance **R**atio) :

Le taux de fausse acceptation est donné par le nombre de fausses signatures acceptées par le système par rapport au nombre total de comparaisons effectués [85].

$$FAR = \frac{\text{Nombre de Fausses Signatures Acceptées}}{\text{Nombre Total de Comparaisons Effectuées}} \times 100$$

- **FRR** (**F**alse **R**ejection **R**atio) :

Le taux de faux rejets est le rapport entre le nombre de signatures authentiques rejetées par le système et le nombre total de signatures authentiques testées.

$$FRR = \frac{\text{Nombre de Signatures Authentiques Rejetées}}{\text{Nombre Total de Signatures Authentiques Testées.}} \times 100$$

3.7 Conclusion

Dans ce chapitre, nous avons présenté les descripteurs de texture locaux les plus récents, à savoir :le LBP, le BSIF et la LDA. Finalement on a parlé des taux d'évaluation des performances des systèmes d'authentification à savoir le ***FRR*** et le ***FAR*** pour mesurer leur efficacité afin d'obtenir de meilleurs résultats. Il est nécessaire de développer un système général pour classifier chaque style de signature et d'améliorer ses performances.

Chapitre 4: Analyse statistique de texture et protocole expérimental

L'analyse statistique de texture nécessite le calcul de caractéristiques de texture à partir de la distribution statistique de combinaisons observées d'intensités à des positions spécifiées les unes par rapport aux autres dans une image. Le nombre de points d'intensité (pixels) dans chaque combinaison est identifié, ce qui conduit à la classification des statistiques de texture comme étant de premier ordre, de second ordre ou d'ordre supérieur.

Les systèmes biométriques basés sur la vérification de signature, en conjonction avec l'analyse texturale, peuvent révéler des informations sur la distribution des pixels d'encre, qui reflète les caractéristiques personnelles du signataire, c'est-à-dire la tenue du stylo, la vitesse d'écriture et la pression. Mais nous ne pensons pas que les seules informations sur la distribution de l'encre soient suffisant pour l'identification du signataire. Ainsi, dans le cas spécifique des traits de la signature, nous avons également pris en compte, pour l'analyse texturale, les pixels du contour du trait. Nous entendons par là les pixels du trait qui se trouvent dans la bordure du fond de la signature. Ces pixels contiennent des informations statistiques sur la forme de la signature. Ces données de distribution peuvent donc être considérées comme une combinaison d'informations texturales et de forme.

4.1 Caractéristiques statistiques de premier ordre [93].

Les caractéristiques statistiques de premier ordre, représentées dans un histogramme, tiennent compte de la valeur individuelle du niveau de gris de chaque pixel d'une image $\boldsymbol{I(x,y), 1 \leq x \leq N, 1 \leq y \leq M,}$ mais la disposition spatiale n'est pas prise en compte, c'est-à-dire que différentes caractéristiques spatiales peuvent avoir le même histogramme de niveau. Une manière classique de paramétrer l'histogramme consiste à mesurer sa moyenne et son écart type.

De toute évidence, la capacité discriminante des statistiques de premier ordre est vraiment faible pour la vérification automatique de signatures, surtout lorsque l'utilisateur et le faussaire utilisent un instrument d'écriture similaire. En

fait, la plupart des chercheurs normalisent l'histogramme, de manière à réduire le bruit pour le traitement ultérieur de la signature.

4.2 Matrices de cooccurrence de niveau de gris

La méthode de la matrice de cooccurrence des niveaux de gris (GLCM) permet d'extraire des caractéristiques statistiques de texture de second ordre à partir de l'image [94]. Cette approche a été utilisée dans un certain nombre d'applications, y compris l'analyse du type d'encre [95], par exemple [96-98].

La GLCM d'une image $I(x, y)$ est une matrice $P(i, j\Delta_{x,}\Delta_y), 0 \leq i \leq G - 1{,}0 \leq j \leq G - 1$, où le nombre de lignes et de colonnes est égal au nombre de niveaux de gris G.

L'élément de la matrice$P(i, j|\Delta_x, \Delta_y)$ est la fréquence relative avec laquelle deux pixels avec des niveaux de gris i et jsont séparés par une distance de pixel (Δ_x, Δ_y). Par souci de simplicité, nous désignerons dans toute la suite, la matrice GLCM par $P(i, j)$.

Pour une estimation statistiquement fiable de la fréquence relative, nous avons besoin d'un nombre suffisamment grand d'occurrences pour chaque événement. La fiabilité de $P(i, j)$ dépend du nombre de niveaux de gris G et de de la taille l'image $I(x, y)$. Dans le cas d'images contenant des signatures, au lieu de la taille de l'image, elle dépend du nombre de pixels des traits de la signature. Si la fiabilité statistique n'est pas suffisante, nous devons réduire G pour garantir le nombre minimum de pixels transitions par composant de la matrice $P(i, j)$, tout en perdant la précision de la description de la texture. Le nombre de niveaux de gris G peut être réduit facilement en quantifiant l'image$I(x, y)$.

Les mesures classiques de caractéristiques extraites de la matrice GLCM (voir Haralick [96] et Conners et Harlow [94]) sont les suivantes :

L'homogénéité de la texture H, le Contraste de la texture C, l'Entropie de la texture E et la Corrélation de la texture O.

4.3 Motifs binaires locaux

Parmi les trois codes LBP décrits dans la section précédente, $LBP, LBP_{P,R}\ et\ LBP_{P,R}^{riu2}$, nous utiliserons dans la suite de notre travail le $LBP_{P,R}^{riu2}$, en raison de ses propriétés d'invariance rotationnelle.

4.4 Analyse texturale pour la vérification de signatures

L'analyse de la trace d'écriture dans les signatures devient un domaine d'application de l'analyse texturale. Les caractéristiques texturales de l'image en niveau de gris peuvent révéler des caractéristiques personnelles du signataire (c'est-à-dire les changements de pression et de vitesse, la tenue du stylo, etc.), complétant ainsi les caractéristiques classiques proposées dans la littérature. Dans cette section, nous décrivons un schéma de base pour l'utilisation de l'analyse texturale dans la vérification automatique de signatures.

Dans ce travail, nous avons utilisé une procédure de postérisation simple pour éviter l'influence du fond.

4.5 Élimination du fond

Les caractéristiques utilisées dans notre système caractérisent la distribution des niveaux de gris dans une image de signature mais nécessitent également une procédure d'élimination de l'arrière-plan. Les niveaux de gris correspondant à l'arrière-plan ne constituent pas une information discriminante mais l'ajout de bruit peut affecter négativement la caractérisation.

Dans ce travail, nous avons utilisé une simple procédure de postérisation pour éviter l'influence du fond [93]. Évidemment, toute autre procédure de segmentation efficace serait également utile. La postérisation se produit lorsque la profondeur de bits apparente d'une image a été tellement réduite qu'elle a un impact visuel. Le terme "postérisation" est utilisé parce qu'il peut influencer l'image d'une manière similaire à la gamme de couleurs d'une affiche produite en série, où le processus d'impression utilise un nombre limité de couleur d'encres.

Soit $I(x,y)$ une image à 256 niveaux de gris et $\boldsymbol{nL}$ le nombre de niveaux de gris pris en compte pour la postérisation. L'image postérisée $\boldsymbol{I_P(x,y)}$ est définie comme suit :

$$\boldsymbol{I_P(x,y) = round\left(roud\left(\frac{I(x,y)n_L}{255}\right)\frac{255}{n_L}\right)} \quad \textbf{(1)}$$

où round(.) arrondit les éléments aux entiers les plus proches. Le round intérieur effectue l'opération de postérisation, et le round extérieur garantit que le niveau de gris résultant de $\boldsymbol{I_P(x,y)}$ est un entier.

Dans les résultats présentés dans ce document, avec les bases de données ***MCYT*** et ***GPDS***, nous avons utilisé une valeur de $\boldsymbol{nL = 3}$ pour obtenir une image postérisée à 4 niveaux de gris, les niveaux de gris étant 0, 85, 170, et 255. Perceptivement , les valeurs valides peuvent être $\boldsymbol{nL = 3}$ou $\boldsymbol{4}$. Avec des valeurs de $\boldsymbol{nL = 1}$ ou $\boldsymbol{2}$, la signature est à moitié effacée et ce n'est pas une segmentation valide. Avec une valeur de $\boldsymbol{nL = 3}$, les traits de la signature sont bien préservés et le fond apparaît presque propre. Avec des valeurs de $\boldsymbol{nL} > 3$, principalement dans le Corpus MCYT, de plus en plus de bruit de fond de type poivre et sel apparaît dans le fond. Afin d'éviter un post-traitement de l'image et d'éliminer le bruit de sel et de poivre, la valeur de $\boldsymbol{nL = 3}$a été retenue.

Les images des deux corpus sont constituées de traits sombres sur un fond blanc. Dans l'image postérisée, le fond apparaît blanc (niveau de gris égal à 255) et les traits de la signature apparaissent plus sombres (niveaux de gris égaux à 0, 85 ou 170). Par conséquent, pour obtenir la valeur$\boldsymbol{I_{bw}(x,y)}$signature binarisée (traits noirs et fond blanc)nous appliquons une simple opération de seuillage, comme suit :

$$\boldsymbol{I_{bw}(x,y) = \begin{cases} 255 & si\ \ I_p(x,y) = 255 \\ 0 & si\ non \end{cases}} \quad \textbf{(2)}$$

L'image$\boldsymbol{I_{bw}(x,y)}$en noir et blanc est utilisée comme masque pour segmenter la signature originale et la signature segmentée est obtenue comme suit :

$$\boldsymbol{I_s(x,y) = \begin{cases} 255 & si\ \ I_{bw}(x,y) = 255 \\ 0 & si\ non \end{cases}} \quad \textbf{(3)}$$

À ce stade, une segmentation complète entre l'arrière-plan et le premier plan est réalisée.

4.6 Déplacement de l'histogramme[1]

Cette section vise à réduire l'influence des différents stylos d'écriture à encre sur la signature segmentée. Nous y parvenons en déplaçant l'histogramme des pixels de la signature vers zéro, en gardant le fond blanc avec un niveau de gris égal à 255. En s'assurant que la valeur du niveau de gris du pixel le plus sombre de la signature est toujours égale à 0, la gamme dynamique reflétera uniquement les caractéristiques du style d'écriture. Ceci peut être réalisé en soustrayant la valeur minimale du niveau de gris des pixels de l'image de la signature, comme suit :

$$I_G(x,y) = \begin{cases} I_S(x,y) & si\ \ I_S(x,y) = 255 \\ I_S(x,y) - min\{I_S(x,y)\} & si\ non \end{cases} \quad (4)$$

4.7 Bases de données et protocole expérimental

Nous avons utilisé deux bases de données pour tester les caractéristiques proposées basées sur les niveaux de gris. Toutes deux ont été numérisées à 600 dpi, ce qui garantit une représentation suffisante de la texture grise. Les principales différences entre elles sont les stylos utilisés. Dans la base de données MCYT, tous les signataires, authentiques et faussaires, ont utilisé le même stylo sur la même surface. En revanche, dans la base de données GPDS, tous les utilisateurs ont signé avec leurs propres stylos sur des surfaces différentes. Ainsi, des résultats similaires avec les deux bases de données indiqueront une mesure de l'indépendance de l'encre des caractéristiques proposées.

4.7.1 Corpus GPDS-100

Le corpus de signatures GPDS-100 contient 24 signatures authentiques et 24 contrefaçons de 100 individus [99], ce qui produit 100 x 24=2400 signatures authentiques et la même chose pour les fausses. Les signatures authentiques ont

été prises en une seule session pour éviter les difficultés de programmation. Les répétitions de chaque signature authentique et de chaque spécimen de contrefaçon ont été collectées à l'aide du propre stylo de chaque participant sur des feuilles de papier blanches de format A4, comportant deux tailles de boîte différentes : la première boîte fait 5 cm de large et 1,8 cm de haut et la seconde boîte fait La moitié des spécimens authentiques et faux ont été inscrits dans chaque taille de boîte. Les faux ont été rassemblés sur un formulaire comportant 15 cases. Chaque formulaire de faux montre 5 images de différentes signatures authentiques choisies au hasard. Le faussaire a imité chacune d'elles 3 fois pour les 5 signatures. Les faussaires disposaient d'un temps illimité pour apprendre les signatures et réaliser les fausses signatures.

La moitié des spécimens authentiques et faux ont été inscrits dans chaque taille de case. Les faux ont été rassemblés sur un formulaire comportant 15 cases. Chaque formulaire de faux montre 5 images de différentes signatures authentiques choisies au hasard. Le faussaire a imité chacune d'elles 3 fois pour les 5 signatures. Les faussaires disposaient d'un temps illimité pour apprendre les signatures et réaliser les faux.

L'ensemble du processus de signature était supervisé par un opérateur. Une fois les formulaires de signature collectés, chaque formulaire a été scanné avec un appareil Canon en utilisant une échelle de gris de 256 niveaux et une résolution de 600 dpi. Toutes les images de signature ont été enregistrées au format PNG.

4.7.2 Corpus MCYT

Le sous-corpus hors ligne de la base de données de signatures MCYT [100] a été utilisé. L'ensemble du corpus comprend des données d'empreintes digitales et de signatures en ligne pour 330 contributeurs provenant de 4 sites espagnols différents. Des falsifications habiles sont également disponibles dans le cas des données de signature. Les faussaires reçoivent les images de signature des clients à falsifier et, après entraînement, il leur est demandé d'imiter la

forme. Les données de signature ont toujours été acquises avec le même stylo à encre et les mêmes modèles de papier sur une tablette à stylo. Par conséquent, les images de signature sont également disponibles sur papier. Les modèles de papier de 75 signataires (et leurs contrefaçons qualifiées) ont été numérisés avec un scanner à 600 dpi. Le sous-corpus hors ligne qui en résulte comporte 2250 images de signatures, avec 15 signatures authentiques et 15 contrefaçons par utilisateur. Ce corpus de signatures est accessible au public à l'adresse http://atvs.ii.uam.es.

4.8 Protocole expérimental

4.8.1 Évaluation des paramètres

Dans la présente partie, nous examinons les paramètres les plus pertinents du descripteur BSIF PATCH proposé. Tout d'abord, nous analysons le nombre ***b*** de filtres BSIF et la dimension k×k correspondante du filtre. Ensuite, nous examinons la dimension $W \times W$ du patch utilisé lors de la génération des histogrammes locaux qui génèrent le vecteur caractéristique final. La performance du système proposé est évaluée en fonction du taux d'identification. Dans cette expérience [101].

4.8.2 Performances vis-à-vis des paramètres du filtre BSIF

D'après la description donnée ci-dessus, il existe deux paramètres du filtre BSIF à échelle unique. Le premier est sa taille (c'est-à-dire l'échelle). Le second est la longueur du filtres (c'est-à-dire la longueur de la chaîne de bits).Les deux paramètres ont une influence sur les performances du descripteur BSIF; leurs choix optimaux améliorent les performances de l'algorithme proposé. Pour discerner les paramètres optimaux pour la méthode BSIF, nous avons mené différentes expériences en utilisant le jeu de filtres fourni par J. Kannala et all [102]. Pour chaque combinaison du nombre et de la taille du filtre, nous affectons un nombre X au filtre et nous le notons par BSIF_X. Par exemple, le

filtre BSIF_1a une taille de 11× 11etle nombre de filtres est égal à 10. Le tableau 4.2 récapitule ces types de filtres et leurs paramètres pour différentes combinaisons de longueur de chaîne de bits et de taille de filtre.

Tableau 4.1 : Les filtres BSIF et leurs paramétrages

Filtres BSIF	3×3	5×5	7 × 7	9 × 9	11 × 11	13 × 13	15 × 15	17 × 17
5	33	40	48	56	4	12	20	28
6	34	41	49	57	5	13	21	29
7	35	42	50	58	6	14	22	30
8	36	43	51	59	7	15	23	31
9	-	44	52	60	8	16	24	32
10	-	37	45	53	1	9	17	25
11	-	38	46	54	2	10	18	26
12	-	39	47	55	3	11	19	27

Dans les tableaux 4.2a et 4.2b ,nous présentons les taux d'identification du système proposé, en utilisant le descripteur BSIF à échelle unique. Nous avons utilisé différentes combinaisons de taille et de nombre de filtres afin d'évaluer convenablement le descripteur BSIF lors de l'identification des personnes à travers leurs signatures manuscrites hors ligne et de sélectionner ses paramètres optimaux, nous avons établi différentes combinaisons avec la taille du filtre et le nombre de ces derniers. Puis nous les appliquons aux trois signatures de chaque individu de la première session des bases de données GPDS et MCYT pour l'apprentissage et à toutes les autres signatures de la deuxième session pour les tests du classificateur K-NN.

Sur la base de nos expériences, 4 filtres BSIF à échelle unique ont été retenus pour les expériences suivantes. Tous ont fourni des taux d'identification supérieurs à 93% et 96% sur les deux bases de données. Ces filtres sont BSIF_2, BSIF_12, BSIF_47, BSIF_55. Il est à noter aussi que quatre filtres sélectionnés font une analyse sur des grandes fenêtres (7 × 7 à 13 × 13) avec un nombre de filtres égal à 11 ou 12. Sur la base de ce paramètre, de nombreuses expériences

ont été menées pour évaluer l'effet des autres paramètres sur la performance de notre méthode.

4.8.3 Performances vis à vis de la taille du patch.

Le troisième paramètre est la taille des patchs (patch size) dans lesquels les images sont décomposées pour calculer la longueur de d'histogramme local.

Nous avons divisé l'image de N × N pixels en zones carrés égales de taille W × W et nous avons testé la méthode pour quelques valeurs de W afin de sélectionner la meilleure partition. Pour déterminer la taille appropriée de l'image de patch, plusieurs expériences ont été opérées avec des valeurs différentes. Le tableau 4.3 résume les taux d'identification en fonction de la taille du patch. La taille du patch est égale à (N × N) / L, avec L variant de 2 à 3.

Les résultats affichés dans le tableau 4.3 sont obtenus au moyen des filtres BSIF préalablement sélectionnés. Il est clair que la précision est meilleure quand il y a un plus grand nombre de patchs d'image, car dans ce cas on peut extraire des détails plus pertinents des images initiales des signatures

Tableau 4.2a : Les taux d'identification de la méthode proposée sur la base de données MCYT en fonction de la taille des patchs et des filtres BSIF sélectionnés

MCYT	BSIF_47	BSIF_55	BSIF_2	BSIF_10
L=1	**0,9520**	**0,9573**	**0,9360**	**0,9307**
L=2	**0,9680**	**0,9653**	**0,9680**	**0,9733**
L=3	**0,9520**	**0,9707**	**0,9733**	**0,9707**

Tableau 4.2b : Les taux d'identification de la méthode proposée sur la base de données GPDS en fonction de la taille des patchs et des filtres BSIF sélectionnés

GPDS	BSIF_47	BSIF_55	BSIF_2	BSIF_10
L=1	**0,9600**	**0,9733**	**0,9778**	**0,9800**
L=2	**0,9844**	**0,9844**	**0,9800**	**0,9822**
L=3	**0,9889**	**0,9800**	**0,9822**	**0,9800**

Conclusion générale

Ce mémoire a pour vocation de répondre à une problématique de sécurisation ou plus exactement l'identification des souscripteurs à travers leurs signatures manuscrites en hors ligne. Deux descripteurs texturaux le LBP et le BSIF ont été choisis parmi l'assortiment existant dans l'état de l'art en fonction de leur capacité à discriminer les signataires via la capture des modèles locaux basés sur leur voisinage, la propriété multi-résolution, la cooccurrence des paires de pixels. Dans notre étude nous avons considéré les deux corpus de données standards MCYT et GPDS très citées dans la littérature de l'état de l'art. Les performances d'identification des souscripteurs ont été testées avec le classifieurs bien connus et de descripteurs texturaux. Les résultats ont été analysés avec le classificateur de k-plus proche voisin (KNN). La performance de ce système est comparable à celle d'autres systèmes de vérification et d'identification de signatures hors ligne, comme l'indiquent les résultats des simulations obtenus avec les deux bases de données hors ligne citées précédemment. Nous pouvons énumérer quelques perspectives de ce travail :

- ✓ L'utilisation des grandes bases de signature (étatiques),
- ✓ L'utilisation les bases de signature arabes,
- ✓ L'utilisation d'autres descripteurs texturaux,
- ✓ L'utilisation d'autre classifieurs tels que le SVM dans ses différentes versions ou le Deep Learning.

Bibliographie

[1] K. Bowyer, V. Govindaraju, N. Ratha, Introduction to the special issue on recent advances in biometric systems, IEEE Transactions on Systems, Man and Cybernetics—B 37 (5) (2007) 1091–1095.

[2] D. Zhang, J. Campbell, D. Maltoni, R. Bolle, Special issue on biometric systems, IEEE Transactions on Systems, Man and Cybernetics—C 35 (3) (2005) 273–275.

[3] S. Prabhakar, J. Kittler, D. Maltoni, L. O'Gorman, T. Tan, Introduction to the special issue on biometrics: progress and directions, PAMI 29 (4) (2007) 513–516.

[4] S. Liu, M. Silverman, A practical guide to biometric security technology, IEEE IT Professional 3 (1) (2001) 27–32.

[5] R. Plamondon, S. Srihari, On-line and off-line handwriting recognition: a comprehensive survey, IEEE Transactions on Pattern Analysis and Machine Intelligence 22 (1) (2000) 63–84.

[6] K. Franke, J.R. del Solar, M. Ko¨ pen, Soft-biometrics: soft computing for biometric-applications, Tech. Rep. IPK, 2003.

[7] S. Impedovo, G. Pirlo, Verification of handwritten signatures: an overview, in: ICIAP '07: Proceedings of the 14th International Conference on Image Analysis and Processing, IEEE Computer Society, Washington, DC, USA, 2007, pp. 191–196, doi: http://dx.doi.org/10.1109/ICIAP.2007.131.

[8] R. Plamondon, in: Progress in Automatic Signature Verification, World Scientificfic Publications, 1994.

[9] M. Fairhurst, New perspectives in automatic signature verification, Tech. Rep.1, Information Security Technical Report, 1998.

[10] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, J. Ortega-Garcia, An off-line signature verification system based on fusion of local and

global information, in: Workshop on Biometric Authentication, Springer LNCS-3087, 2004, pp. 298–306.

[11] Y. Kato, M. Yasuhara, Recovery of drawing order from single-stroke hand- writing images, IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(9) (2000).

[12] S. Lee, J. Pan, Offline tracking and representation of signatures, IEEE Transactions on Systems, Man and Cybernetics 22 (4) (1992) 755–771.

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

[14] Hedjaz Hezil. Identification de personnes par signature manuscrite. Thèse de doctorat 3ème cycle en LMD. université 8 mai 1945 Guelma Algérie .2018. (https://dspace.univ-guelma.dz/jspui/handle/123456789/496).

[15] Benzaoui, A., Hadid, A. and Boukrouche, A. (2014) 'Ear biometric recognition using local texture descriptors', *IET Biometrics*, Vol. 23, No. 3, pp.9–17.

[16] Bharadi, V.A. and Kekre, H.B. (2010) 'Off-line signature recognition systems', *International Journal of Computer Application*, Vol. 1, No. 27, pp.48–56.

[17] F. Ahmed and D. Mohamed: *A review on fingerprint classification techniques*. In Proceedings of the International IEEE Conference on Computer Technology and Development (ICCTD). Vol.2, pp.411-415, Kota Kinabalu (Malaisie), 2009.

[18] Nicolas MORIZET Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris. Thèse de doctorat Soutenue le 18 Mars 2009 à l'Ecole Nationale Supérieure des Télécommunications de Paris Spécialité : Signal et Images.

[19] Billeb, S.; Rathgeb, C.; Reininger, H.; Kasper, K.; Busch, C., "Biometric template protection for speaker recognition based on universal background models," in Biometrics, IET, vol.4, no.2, pp.116-126, 2015.

[20] Caetano Garcia, D.; de Queiroz, R.L., "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," in Information Forensics and Security, IEEE Transactions on, vol.10, no.4, pp.778-786, April 2015.

[21] Borah, Tripti Rani; Sarma, Kandarpa Kumar; Talukdar, Pran Hari, "Retina recognition system using adaptive neuro fuzzy inference system," in Computer, Communication and Control (IC4), 2015 International Conference on, pp.1-6, 10-12 Sept. 2015.

[22] Raja, K.B.; Raghavendra, R.; Busch, C., "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information," in Information Forensics and Security, IEEE Transactions on, vol.10, no.10, pp.2048-2056, Oct. 2015.

[23] Benzaoui, A., Hadid, A. and Boukrouche, A. (2014) 'Ear biometric recognition using local texture descriptors', *IET Biometrics*, Vol. 23, No. 3, pp.9–17.

[24] Soldera, J.; Alberto Ramirez Behaine, C.; Scharcanski, J., "Customized Orthogonal Locality Preserving Projections with Soft-Margin Maximization for Face Recognition," in Instrumentation and Measurement, IEEE Transactions on, vol.64, no.9, pp.2417-2426, Sept. 2015.

[25] Muwei Jian; Kin-Man Lam, "Simultaneous Hallucination and Recognition of Low-Resolution Faces Based on Singular Value Decomposition," in Circuits and Systems for Video Technology, IEEE Transactions on, vol.25, no.11, pp.1761-1772, Nov. 2015.

[26] J. Daugman: *How Iris Recognition Works?* IEEE Transactions on Circuits and Systems for Video Technology. Vol.14, No.01, pp.21-30, 2004.

[27] Guoqiang Li; Busch, C.; Bian Yang, "A novel approach used for measuring fingerprint orientation of arch fingerprint," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on, vol., no., pp.1309-1314, 26-30 May 2014.

[28] Ying Li Han; Tae Hong Min; Rae-Hong Park, "Efficient iris localisation using a guided filter" IET Image Processing, Volume 9, Issue 5, May 2015, p. 405 –412.

[29] B. Arbab-Zavar and M.S. Nixon: *On Guided Model-Based Analysis for Ear Biometrics*. Computer Vision and Image Understanding (Elsevier). Vol.115, No.04, pp.487-502, 2011.

[30] Huang, S.; Elgammal, A.; Lu, J.; Yang, D., "Cross-Speed Gait Recognition Using Speed-Invariant Gait Templates and Globality–Locality Preserving Projections," in Information Forensics and Security, IEEE Transactions on, vol.10, no.10, pp.2071-2083, Oct. 2015.

[31] Ansari, A.Q.; Hanmandlu, M.; Kour, J.; Singh, A.K., "Online signature verification using segment-level fuzzy modelling," in Biometrics, IET, vol.3, no.3, pp.113-127, Sept. 2014.

[32] Wenxiong Kang; Qiuxia Wu, "Pose-Invariant Hand Shape Recognition Based on Finger Geometry," in Systems, Man, and Cybernetics: Systems, IEEE Transactions on, vol.44, no.11, pp.1510-1521, Nov. 2014.

[33] Orcan Alpar, Keystroke recognition in user authentication using ANN based RGB histogram technique, Engineering Applications of Artificial Intelligence, Volume 32, June 2014, Pages 213-217.

[34] Haifeng Hu, "Multiview Gait Recognition Based on Patch Distribution Features and Uncorrelated Multilinear Sparse Local Discriminant Canonical Correlation Analysis," in Circuits and Systems for Video Technology, IEEE Transactions on, vol.24, no.4, pp.617-630, April 2014.

[35] Basmajian JV, de Luca CJ. Muscles Alive – The Functions Revealed by Electromyography. The Williams & Wilkins Company; Baltimore, 1985.

[36] Mohamad El-Abed. ‘’Evaluation de système biométrique’’. Cryptographie et sécurité [cs.CR]. Université de Caen, 2011.

[37] Benchennane Ibtissam, ‘’Etude et mise au point d’un procédé biométrique multimodal pour la reconnaissance des individus ‘’. Thèse de doctorat, Faculté de Génie Electrique, Université USTO, 2016.

[38] Hafs Toufik**.** Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne. Université Badji Mokhtar – Annaba. 2016.

[39] Manoj Kumar, M.; Puhan, N.B., "Off-line signature verification: upper and lower envelope shape analysis using chord moments," in Biometrics, IET , vol.3, no.4, pp.347-354, 2014.

[40] Nait-ali A., “Beyond classical biometrics: when using hidden biometrics to identify individuals”, 3rd European Workshop on Visual Information Processing, Invited paper, Paris, pp. 241–256, 4–6 July, 2011.

[41] Nait-ali A., “Hidden biometrics: towards using biosignals and biomedical images for security applications”, 7th international Workshop on Systems, Signal Processing and their Applications, Invited paper, Tipaza, pp. 352–356, 2011.

[42] Plataniotis K., Hatzinakos D., Lee J., “ECG biometric recognition without fiducial detection”, Proceedings of Biometrics Symposiums (BSYM ’06), Baltimore, MD, USA, September 2006.

[43] Chantaf S., Naït-ali A., Karasinski P., Khalil M., “ECG modeling using wavelet networks: application to biometrics”, International Journal of Biometrics, vol. 2, no. 3, pp. 236–248, 2010.

[44] Chantaf S., Biométrie par signaux physiologiques, PhD Thèse, Université Paris-Est Créteil, France, 2011.

[45] Biel L., Pettersson O., Philipson L., WIDE P., “ECG analysis: a new approach in human identification”, IEEE Transactions on Instrumentation and Measurement, vol. 50, no. 30, pp. 808–812, 2001.

[46] Wang Y., Plataniotis K., Hatzinakos D., "Integrating analytic and appearance attributes for human identification from ECG signal", Proceedings of Biometrics Symposiums (BSYM '06), Baltimore, MD, USA, September 2006.

[47] Basmajian JV, de Luca CJ. Muscles Alive – The Functions Revealed by Electromyography. The Williams & Wilkins Company; Baltimore, 1985.

[48] Nait-ali A., Fournier R., "Signal and Image Processing for Biometrics", John Wiley & Sons, ISBN 978-1-84821-385-2, 2012.

[49] Aloui K., Biométrie du cerveau humain, PhD Thesis, Université Paris-Est Créteil, France, 2012.

[50] Guermoui Mawloud, Doctorat en Sciences, Classification de personnes par utilisation des techniques de l'intelligence artificielle. Université de Batna -2-. 2017.I.7 Les limite de la biométrie.

[51] Zoubida Leila. These de Doctorat de 3ème cycle. Université Djilali Liabes Faculté des Sciences Exactes Sidi Bel Abbes, 2017/2018. Biometric Applications.

[52] Hedjaz HEZIL. Identification de personnes par signature manuscrite. Thèse de doctorat 3ème cycle en LMD. Université8 mai 1945 Guelma Algérie .2018.
(https://dspace.univ-guelma.dz/jspui/handle/123456789/496)

[53] J.Mathyer, "The Expert Examination of Signature", Journal of criminallaw, Criminology and police science, Vol.5, N° 3, Mai-Juin 1961.

[54]Harrison, Wilson R. "Suspect documents. their scientific examination." (1958).

[55]Saferstein, Richard, and Adam B. Hall, eds. Forensic science handbook. Vol. 1. Upper Saddle River, NJ: Prentice Hall, 2002.

[56]Evett, Ian W., and R. N. Totty. "A study of the variation in the dimensions of genuine signatures." Journal of the forensic science society 25.3 (1985): 207-215.

[57]Lahyane Adil. Vérification des signatures manuscrites. Mémoire Présenté à L'Université du Québec à Trois-Rivières. Février 2002. http://depot-e.uqtr.ca/id/eprint/2535/1/000693522.pdf

[58]Mehalaine Abdelkrim. Boukhors Walid, reconnaissance multimodale d'empreinte digitalet de signature manuscrite. Mémoire Master académique. Université Larbi Ben M'hidi OumEl Bouaghi. Algérie. 2016/ 2017.

[59]Yasmine Serdouk,Vérification et identification de la signature à l'aidede système Immunitaireartificielle. Thèse de doctorat (LMD). Université des sciences et technologieHouari Boumediene, Algérie, le 21 juin2017.

[60]Communications on Applied Electronics (CAE) – ISSN: 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 4– No.8, April 2016 – www.caeaccess.org. A Survey on Handwritten Signature Verification Approaches.

[61]Abuhaiba, I. S. 2007. Offline signature verification using graph matching. Turk J Elec Engin, vol.15, pp. 89-104.

[62]Afsardoost, S., Siamak Y., and Mohammad A. K. 2008. Offline signature verification using geometric center features. In Signal Processing International Conference, IEEE (ICSP 2008), pp. 1491-1494.

[63] Daramola, S., and Ibiyemi, S. 2010. Novel feature extraction technique for offline signature verification system. International Journal of Engineering Science and Technology, vol. 2, pp. 3137-3143.

[64] Jana, R., Rituparna S., and Debaleena D. 2014. Offline signature verification using Euclidian distance. International Journal of Computer Science and Information Technologies, vol.5, no. 1 pp.707-710.

[65]Huang, K., and Yan, H. 2002. Offline signature verification using structural feature correspondence. Pattern Recognition, vol.35, pp. 2467- 2477.

[66]Baltzakis, H., and Papamarkos, N. 2001. A new signature verification technique based on a two-stage neural network classifier. Engineering Applications of Artificial intelligence, vol. 14, pp.95-103.

[67]Suryawanshi, R., Kale, S., Pawar, R., Kadam, S., and Ghule, V. R. 2016. Offline signature cognition and verification using artificial neural network. IJARCCE, vol. 5, pp. 352-354.

[68] Candes, E. J., and Donoho, D. L. 2000. Curvelets: A surprisingly effective nonadaptive representation for objects with edges. Stanford University Ca Dept of Statistics.

[69]Guerbai, Y., Chibani, Y. and Hadjadji, B. 2015. The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. Pattern Recognition, vol. 48, pp. 103-113.

[70]Kumar, R., Sharma, J. D., and Chanda, B. 2012. Writer independent offline signature verification using surroundedness feature. Pattern Recognition Letters, vol.33, pp. 301-308.

[71]Anjali.R, and Manju R. M. 2013. Offline signature verification based on SVM and neural network. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, pp. 2320– 3765.

[72]Ismail, M. A. and Gad, S. 2000. Offline Arabic signature recognition and verification. Pattern Recognition, vol. 33, pp.1727-1740.

[73] Singh, P., and Patel, R. 2013. Offline signature verification using fuzzy logic. International Journal of software & Hardware Research in Engineering vol.1, pp.97-101.

[74]Daramola, S. A., and Ibiyemi, T. S. 2010. Offline signature recognition using hidden markov model (HMM). International journal of computer applications, vol.10, pp.17-22.

[75] Justino, E. J., Bortolozzi, F., and Sabourin, R. 2005. A comparison of SVM and HMM classifiers in the off-line signature verification. Pattern recognition letters, vol.26, pp.1377-1385.

[76]Plamondon, R. &Srihari, S. N. (2000). Online and off-line handwriting recognition: a comprehensivesurvey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*,22(1), 63–84. doi: 10.1109/34.824821.

[77]Impedovo, D. & Pirlo, G. (2008). Automatic Signature Verification: The State of the Art. *IEEETransactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*,38(5), 609–635. doi: 10.1109/TSMCC.2008.923866.

[78]Hafemann, L. G., Sabourin, R. & Oliveira, L. S. (2017b). Offline handwritten signature verification—literature review. *Image Processing Theory, Tools and Applications (IPTA),2017 Seventh International Conference on*, pp. 1–8.

[79] Hu, J. & Chen, Y. (2013). Offline Signature Verification Using Real Adaboost Classifier Combination of Pseudo-dynamic Features. *Document Analysis and Recognition, 12thInternational Conference on*, pp. 1345–1349. doi: 10.1109/ICDAR.2013.272.

[80] Yılmaz, M. B.&Yanıkoˇglu, B. (2016). Score level fusion of classifiers in off-line signature verification.*Information Fusion*, 32, Part B, 109–119. doi:10.1016/j.inffus.2016.02.003.

[81] Rivard, D., Granger, E. & Sabourin, R. (2013). Multi-feature extraction and selection in writerindependentoff-line signature verification. *International Journal on Document Analysisand Recognition (IJDAR)*, 16(1), 83–103. doi: 10.1007/s10032-011-0180-6.

[82]Eskander, G., Sabourin, R. & Granger, E. (2013). Hybrid writer-independent-writer-dependentoffline signature verification system. *IET Biometrics*, 2(4), 169–181. doi: 10.1049/ietbmt.2013.0024.

[83]Bertolini, D., Oliveira, L. S., Justino, E. &Sabourin, R. (2010). Reducing forgeries in
writer-independent off-line signature verification through ensemble of classifiers. *Pattern*
Recognition, 43(1), 387–396. doi: 10.1016/j.patcog.2009.05.009.

[84] Vargas, J., Ferrer, M., Travieso, C. & Alonso, J. (2007). Off-line Handwritten Signature
GPDS-960 Corpus. *Document Analysis and Recognition, 9th International Conferenceon*, 2, 764–768. doi: 10.1109/ICDAR.2007.4377018.

[85]Une Approche de Vérification Hors Ligne de Signatures Manuscrites.[1] ImenAbroug Ben Abdelghani,[2]Anouar Ben Khalifa,[3]NajouaEssoukri Ben Amara.1Ecole Nationale d'Ingénieurs de Tunis .3 Ecole Nationale d'Ingénieurs de Monastir .5019,Monastir-Tunisie.
https://www.researchgate.net/publication/323203256_Une_Approche_de_Verification_Hors_Ligne_de_Signatures_Manuscrites

[86] T. Ojala, M. Pietikäinen, and D. Harwood: *A comparative study of texture*

measures with classifiction based on featured distribution. Pattern Recognition (Elsevier). Vol.29, No.1, pp.51-59, 1996.

[87] Hedjaz HEZIL. Identification de personnes par signature manuscrite. Thèse de doctorat 3ème cycle en LMD. Université 8 mai 1945 Guelma Algérie .2018. (https://dspace.univguelma.dz/jspui/handle/123456789/496).

[88] Kannala, Juho et Rahtu, Esa. Bsif: Binarized statistical image features. In: Proceedings ofthe 21st international conference on pattern recognition (ICPR2012). IEEE, 2012. p. 1363-1366.

[89] A. Hyva¨rinen et al. Natural Image Statistics. Springer, 2009.

[90] T. Ojala et al. Multiresolution gray-scale and rotation invariant texture classification withlocal binary patterns. TPAMI, 7(24):971–987, 2002

[91] V. Ojansivu and J. Heikkila¨. Blur insensitive texture classification using local phasequantization. In ISP, 2008.

[92] A. Hyva¨rinen and E. Oja. Independent component analysis: algorithms and applications.Neural Networks, 2000.

[93] Vargas, J. F., et al. "Off-line signature verification based on grey level information using texture features." Pattern Recognition 44.2 (2011): 375-385.

[94] R.W. Conners, C.A. Harlow, A theoretical comparison of texture algorithms, IEEE Transactions on Pattern Analysis and Machine Intelligence 2 (3) (1980) 204–222.

[95] K. Franke, O. Bu¨ nnemeyer, T. Sy, Ink texture analysis for writer identification, in: IWFHR '02: Proceedings of the Eighth International Workshop on Frontiers in Handwriting Recognition (IWFHR'02), IEEE Computer Society, Washington, DC, USA, 2002, p. 268.

[96] R.M. Haralick, Statistical and structural approaches to texture, Proceedings of the IEEE 67 (5) (1979) 786–804.

[97] D. He, L. Wang, J. Guibert, Texture feature extraction, Pattern Recognition Letters 6 (4) (1987) 269–273.

[98] M. Trivedi, C. Harlow, R. Conners, S. Goh, Object detection based on gray level cooccurrence, Computer Vision, Graphics and Image Processing 28 (3) (1984)199–219.

[99] M. Ferrer, J. Alonso, C. Travieso, Offline geometric parameters for automatic signature verification using fixed-point arithmetic, IEEE Transactions on Pattern Analysis and Machine Intelligence 27 (6) (2005) 993–997.

[100] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, J. Ortega-Garcia, An off-line signature verification system based on fusion of local and global information, in: Workshop on Biometric Authentication, Springer LNCS-3087,2004, pp. 298–306.

[101] J. Kannala and E. Rahtu, "BSIF: binarized statistical image features," in Proc. 21st IEEE Int. Conf. Pattern Recognit., pp. 1363–1366 (2012).

[104]Bendjoudi Salim,Amélioration d'un système de reconnaissance biométriquedes Individus : application sur l'empreinte Palmaireet/ou l'empreinte des articulations des doigts, Thèse de doctorat. Université 8 mai 1945 Guelma Algérie 2020.

Résumé

La vérification de signature hors ligne est un système de vérification automatique qui peut traiter des images numérisées de signatures. La vérification de signature utilise des mesures en niveaux de gris avec différentes caractéristiques de premier plan. La vérification de signature est effectuée à l'aide de vecteurs de caractéristiques de reconnaissance de formes locales. Le modèle binaire local amélioré (LBPM) et le descripteur BSIF extraient des informations de la structure locale en établissant la relation entre le pixel central et les pixels voisins. Le travail (mémoire) utilise les caractéristiques du modèle binaire local modifié (LBPM) et ceux du descripteur BSIF pour la vérification de la signature. Cette procédure de vérification des signatures est testée sur les deux bases de données MCYT et GPDS. La précision de la méthode proposée est vérifiée au moyen du classificateur le plus proche voisin (KNN).

Abstract

Offline signature verification is an automatic verification system that can process scanned images of signatures. Signature verification uses grayscale measurements with different foreground features. Signature verification is performed using local pattern recognition feature vectors. The Local Enhanced Binary Model (LEBM) and BSIF descriptor extract local structure information by establishing the relationship between the center pixel and neighboring pixels. The work (dissertation) uses the features of the modified local binary model (LBPM) and those of the BSIF descriptor for signature verification. This signature verification procedure is tested on both MCYT and GPDS databases. The accuracy of the proposed method is verified using the nearest neighbor classifier (KNN).

الملخص

التحقق من التوقيع في وضع عدم الاتصال هو نظام تحقق تلقائي يمكنه معالجة الصور الممسوحة ضوئيًا للتوقيعات. يستخدم التحقق من صحة التوقيع قياسات تدرج الرمادي بخصائص بارزة مختلفة. يتم إجراء التحقق من التوقيع باستخدام متجهات ميزة التعرف على الأنماط المحلية. يستخرج النموذج الثنائي المحلي المحسن (LBP) وواصف BSIF المعلومات من البنية المحلية عن طريق إنشاء العلاقة بين البكسل المركزي والبكسلات المجاورة. تستخدم الوظيفة (الذاكرة) خصائص النموذج الثنائي المحلي المعدل (LBP) وتلك الخاصة بواصف BSIFللتحقق من صحة التوقيع. يتم اختبار إجراء التحقق من التوقيع على قاعدتي البيانات MCYT وGPDS يتم التحقق من دقة الطريقة المقترحة باستخدام أقرب مصنف جار(KNN) .