الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

Université Larbi Tébessi – Tébessa –
Faculté des Sciences Exactes et Sciences de la Nature et de la Vie

Département : Informatique

MEMOIRE

DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME DE MASTER

Spécialité : Informatique

Option : Systèmes d'information

THEME

Une approche biométrique pour la sécurité d'information

Présenté par le binôme :

- **Maafi Wafaa**
- **Bouguessa Nour El Houda**

Devant le jury :

Laouar Mohamed Ridda	Prof	Université de Tébessa	Président
Hakim Bendjenna	Prof	Université de Tébessa	Encadreur
Abdallah Meraoumia	Prof	Université de Tébessa	Co-Encadreur
Laimeche Lakhdar	MCA	Université de Tébessa	Examinateur

Année Universitaire 2023 / 2024

Remerciement

Merci et louange à Dieu Tout-Puissant d'abord pour la bénédiction de la patience et la capacité d'accomplir le travail. Louange à Dieu pour ces bénédictions. Nous exprimons nos remerciements à Dieu d'abord qui nous a donné la force et la puissance pour finaliser ce mémoire.

En second lieu, nous tenons à remercier du fond du cœur, nos encadreurs Mr Meraoumia Abdallah et Mr Hakim Bendjenna pour avoir dirigé ce travail avec beaucoup de patience, d'avoir toujours été présents quand on avait besoin, de nous avoir offert tous leurs précieux conseils et de nous avoir encouragé et motivé à donner le meilleur de nous-mêmes.

Nous espérons que ce travail sera à la hauteur de leurs espérances.

Nous remercions également le jury qui a accepté de juger notre travail ainsi que tous les enseignants qui ont contribué à notre formation.

Enfin, nous remercions aussi tous nos familles, amis et collègues qui nous ont soutenu et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

M. Wafaa et B. Nour

بـاسم الله خـالـقـي ومسيـر أمـوري، وعصمت أمـري، لـك كـل الـحمـد والامـتـنـان

من قال أنا لها نالها أنا وإن أبت رغما عنها أتيت بها ونلتها

إلى من كلله الله بالوقار..... إلى من علمني العطاء دون انتظار.... إلى من أحمل اسمه بكل افتخار

والدي العزيز

إلى ملاذي في الحياة..... إلى معنى الحب والحنان .....إلى ملاكي الطاهر وسر الوجود .....إلى من كان دعائها نورا لدربي ..... وحنانها بلسم لجراحي .....إلى جنتي

أمي الحبيبة

إلى فقيدة الروح .....إلى من اشتقت وجودها ..... اللهم تغمدها بالرحمة والسكينة

خالتي العزيزة

إلى خيرة ايامي وصفوتها ..... إلى من مددت لهم يدي في ضعفي وامنو بي ...الى من وقفوا خلفي مثل ظلي

الثابت إلى رفيقات الروح أخواتي {سميرة، وردة، سعيدة}

إلى مصدر الأمان ... إلى ضلعي الثابت الذي لا يميل .... إلى إخوتي دمتم لي سندا {عباس، هيثم}

إلى قطع السكر .... إلى فلذات الروح ..... إلى أميرتي وفرساني الصغار

{اية. مازن، حيدر. تيم}

إلى رفيقات الخطوة الأولى .... إلى من هونوا تعب الطريق .... إلى أخوات الروح وصديقات الأيام ...

{سلسبيل، وفاء، دنيا، ريان، شاهيناز}

إلى الذين يبهجهم نجاحي ولكل من كان لي عونا وسندا لرفقاء السنين وأصحاب الشدائد والأزمات كل باسمه ومقامه انا ممتنة

Bouguessa Nour El Houda

فـرحيـن بـمـا اتـا هم الله مـن فـضلـه

من قال أنا لها "نالها" ماكنت لافعلها لولا توفيق من الله

لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون، لم يكن الحلم قريبا ولا الطريق كان محفوفا بالتسهيلات لكني فعلتها ونلتها

الحمد لله حبا وشكرا وامتنانا، الذي بفضله ها أنا اليوم أنظر إلى حلما طال انتظاره وقد أصبح واقعا أفتخر به

إلى ذلك الرجل العظيم إلى من كان لي عمودي الفقري الذي ساندني بكل حب في ضعفي الذي اخرج اجمل مافى داخلى و شخصى دائما للوصول إلى طموحاتي

إلى أول من أنتظر هذه اللحضات ليفتخر بي إلى قدوتي ومراسي من أعطاني

ولم يزل يعطيني بلا حدود إلى سندي ومسندي والضوء الذي ينير حياتي إلى والدي وسيدي ورفيق عمري "والدي العزيز ادامك الله"

إلى ملاكي الطاهر، وقوتي بعد الله، داعمتي الأولى والأبدية "امي" أهديك هذا الإنجاز الذي لولا تضحياتك لما كان له وجود، ممتنة لإن الله قد اصطفاك لي من البشر أما يا خير سند وعوض

إلى من قيل فيهم "سَنَشُدُّ عَضُدَكَ بِأَخِيك"

سندي والكتف الذي أستند عليه دائماً .... إلى (أخوتي يعقوب وشعيب)

إلى رفاق الخطوة الأولى والخطوة ما قبل الأخيرة، إلى من كانوا خلال السنين العجاف سحابا ممطرًا، وأمدوني دائماً بالقوة وكانوا موضع الإتكاء في كل عثراتي (أصدقاء العمر نور سلسبيل دنيا ريان)

شكرا لكل من ساندني وساعدني على طوال رحلتي الدراسية كل باسمه ومقامه انا ممتنة

Maafi Wafaa

Table des Matières

Liste des tableaux

Page

Liste des Figures

Résumé : *La protection des informations est récemment devenue un élément essentiel pour préserver les actifs tangibles et intangibles des organisations, en sécurisant les systèmes informatiques, les données et les réseaux. La biométrie joue un rôle clé en authentifiant les individus et en contrôlant l'accès aux données sensibles, surtout dans notre société interconnectée. Cette recherche propose un système d'authentification biométrique qui combine biométrie et protection des modèles biométriques pour identifier les personnes à distance et sécuriser la transmission de leurs gabarits biométriques. En utilisant le modèle d'apprentissage autonome de degré zéro (ALMMo-0) comme classificateur, le système extrait les caractéristiques biométriques des empreintes des articulations des doigts en utilisant les méthodes HOG et BSIF, et chiffre les gabarits avec la transformation sinus. En utilisant une base d'images de segments de doigts (ROI), nos résultats expérimentaux révèlent une amélioration significative et une précision considérable dans la capacité de reconnaissance du système, démontrant ainsi une performance excellente des techniques utilisées.*

Mots clés : *Protecting information, Biometrics,authentication, biometric templates, classifier, extracts biometric features, dataset, improvement, accuracy, recognition capability, ALMMo-0, HOG, BSIF.*

Abstract: *Protecting information has recently become a crucial element in preserving both tangible and intangible assets of organizations, by securing IT systems, data, and networks. Biometrics plays a key role in authenticating individuals and controlling access to sensitive data, especially in our highly interconnected society. This research proposes a biometric authentication system that combines biometrics and protection of biometric templates to remotely identify individuals and ensure the confidentiality of their biometric templates. Using the Zero-Order Autonomous Learning Multi-Model System (ALMMo-0) as a classifier, the system extracts biometric features from finger joint prints using HOG and BSIF methods, and encrypts templates using sinusoidal transformation. Using a dataset of finger image segments (ROI), our experimental results reveal significant improvement and considerable accuracy in the system's recognition capability, demonstrating excellent performance of the techniques employed.*

Index term*: Protection of information, biometrics, authentication, learning model, feature extraction, image database, biometric templates, improvement, accuracy, recognition capability, ALMMo-0, HOG, BSIF.*

ملخص *حماية المعلومات أصبحت مؤخراً عنصراً أساسياً للحفاظ على الأصول الملموسة وغير الملموسة للمنظمات، من خلال تأمين الأنظمة المعلوماتية والبيانات والشبكات. تلعب التقنيات البيومترية دوراً أساسياً في التحقق من هوية الأفراد وضمان أمان الوصول إلى البيانات الحساسة، خاصة في مجتمعنا المتصل بشكل كبير. يقدم هذا البحث نظاماً للتحقق من الهوية بواسطة التقنيات البيومترية يجمع بين التحقق من الهوية وحماية نماذج الهوية البيومترية لتمكين تحديد الأفراد عن بُعد وضمان سرية نقل نماذجهم البيومترية. باستخدام نموذج الفصل الذاتي من الدرجة الصفرية (ALMMo-0) كمصنف، يستخرج النظام الخصائص البيومترية من بصمات مفاصل الأصابع باستخدام طرق HOG وBSIF، ويشفر النماذج باستخدام تقنية التحويل الجيبي. باستخدام قاعدة بيانات لصور مقاطع من أصابع اليد، تكشف نتائج التجارب الخاصة بنا عن تحسين كبير ودقة ملحوظة في قدرة النظام على التعرف، مما يظهر أداء ممتاز للتقنيات المستخدمة.*

الكلمات المفتاحية *: حماية المعلومات, التقنيات البيومترية, التحقق, نموذج الفصل الذاتي, استخراج السمات, بصمات اصابع اليد, قاعدة بيانات للصور, تحسين, دقة, القدرة على التعرف، ALMMo-0، HOG، BSIF.*

Introduction Générale

Introduction Générale

La sécurité de l'information est un aspect crucial de la sécurité nationale et de la réussite organisationnelle, englobant la protection des actifs de valeur, tangibles et intangibles [1,2]. Cela implique la sécurisation des systèmes informatiques, des données, des réseaux et la gestion des informations afin d'empêcher l'accès, la modification ou le transfert non autorisés d'informations [3,4]. Les organisations s'appuient largement sur les technologies de l'information, rendant essentielle la compréhension et la mise en œuvre des principes de sécurité de l'information pour protéger les systèmes et les données [5]. Le domaine de la sécurité de l'information couvre divers aspects tels que la sécurité des réseaux, la sécurité des données et la gestion des identités, dans le but de préserver la confidentialité, l'intégrité et l'accessibilité des informations tout en prévenant les cybermenaces et les attaques grâce à des technologies avancées telles que l'apprentissage automatique.

Le domaine de la biométrie joue un rôle essentiel dans la sécurité de l'information en authentifiant les individus et en contrôlant l'accès aux données sensibles, garantissant ainsi l'intégrité des informations dans une société de plus en plus interconnectée [6]. La technologie biométrique consiste à vérifier ou à identifier des individus en fonction de leurs caractéristiques intrinsèques uniques [7]. Elle joue un rôle crucial dans divers secteurs tels que la sécurité, les soins de santé et les stratégies nationales [8]. Les applications biométriques vont de la sécurisation de l'accès aux appareils et aux locaux à l'amélioration de la vérification d'identité dans les transactions financières et les documents de voyage [9]. Le domaine de la biométrie continue d'évoluer, les recherches en cours visant à améliorer la précision de l'identification et à explorer de nouvelles modalités [10]. Dans l'ensemble, la biométrie constitue un outil essentiel pour améliorer la sécurité, l'authentification et la gestion de l'identité dans divers domaines technologiques et sociétaux.

L'authentification et l'autorisation d'accès à distance sont des mécanismes permettant de contrôler l'accès des utilisateurs aux systèmes distants. Un scénario spécifique consiste à accorder un accès à distance à un réseau en utilisant un modèle client-serveur qui combine des mécanismes cryptographiques avec la biométrie. Dans cette configuration, le terminal client

agit comme un hôte biométrique, équipé d'un dispositif de capture et d'une unité de traitement pour mesurer les caractéristiques biométriques et générer le vecteur de caractéristiques. Ce scénario d'accès inclut généralement des mécanismes pour détecter l'activité et empêcher les attaques par relecture biométrique. L'identification à distance de l'identité, ainsi que la protection des données transmises, sont cruciales. Ainsi, l'intégration de la biométrie avec la cryptographie est essentielle pour protéger à la fois les données et l'identité des personnes contre le vol. Dans ce mémoire, un crypto-système biométrique a été proposé pour identifier les personnes à distance et protéger la transmission de leurs gabarits biométriques. Le crypto-système proposé utilise le système multimodèle d'apprentissage autonome d'ordre zéro (*Zero-Order Autonomous Learning Multi-Model System, ALMMo-0*) [11] comme un classifier. Ce dernier prend en entrée des vecteurs de caractéristiques biométriques extraits de l'empreinte de l'articulation des doigts (*Finger-Knuckle-Print, FKP*) à l'aide de deux méthodes traditionnelles: l'histogramme de gradients orientés (*Histogram of oriented gradients, HOG*) [12] et les caractéristiques d'image statistique binarisées (*Binarized Statistical Image Features, BSIF*) [13]. Pour chiffrer les gabarits biométriques, la technique *Transformation sinus* [12] a été utilisée.

Pour atteindre nos objectifs, ce mémoire est organisé en trois chapitres :

Le **premier chapitre** offre un aperçu général de la sécurité de l'information et de la biométrie, détaillant les différentes modalités biométriques, la structure et le fonctionnement des systèmes biométriques, ainsi que la biométrie multimodale.

Le **deuxième chapitre** présente une analyse complète de l'authentification biométrique à distance et des techniques associées. En outre, ce chapitre détaille la méthode proposée, y compris des explications complètes de la conception et de la mise en œuvre du système. De plus, il couvre les conditions préalables nécessaires au fonctionnement du système, garantissant une compréhension claire des composants fondamentaux requis.

Le **dernier chapitre** met en évidence la faisabilité et l'efficacité de notre travail en fournissant les résultats expérimentaux relatifs aux performances du système biométrique et à l'analyse de sécurité, accompagnés de toutes les analyses et discussions nécessaires. Ces résultats sont obtenus à partir d'une base de données comprenant les données de 165 personnes.

Enfin, une **conclusion générale** accompagnée de perspectives est présentée, offrant ainsi une synthèse et une orientation pour de futures recherches dans le domaine.

Chapitre 1

Sécurité de l'information et biométrie

Résumé

Dans ce chapitre, nous aborderons les concepts fondamentaux de la sécurité de l'information et des technologies biométriques. Nous examinerons l'importance de la protection des données et des méthodes de sécurité clés telles que le cryptage, le tatouage numérique et la stéganographie. Ensuite, nous explorerons le rôle de la biométrie dans l'amélioration de la sécurité, en introduisant différentes technologies biométriques. Enfin, nous fournirons un aperçu des systèmes biométriques multimodaux et de leur contribution à l'amélioration de l'efficacité des systèmes de sécurité.

Introduction

Au cours de la dernière décennie, l'utilisation des informations a connu une évolution significative, tant en termes de volume que de diversité. La sécurité de ces informations est devenue l'une des principales préoccupations de nos sociétés contemporaines. Son objectif est de surveiller l'accès aux informations lors de leur stockage et de leur transmission, et de prévenir toute utilisation ou modification non autorisée. Dans ce chapitre, nous introduirons le concept de sécurité de l'information, puis nous donnerons un aperçu de la biométrie et de ses technologies. Nous décrirons ensuite les principes généraux du système biométrique, utilisé pour l'identification ou la vérification.

I.1 Sécurité d'information

La sécurité de l'information, souvent désignée sous le terme *InfoSec*, est essentielle pour protéger les données sensibles, que ce soit pour les organisations ou les particuliers. Elle englobe un ensemble de méthodes et de processus visant à prévenir tout accès, utilisation ou divulgation non autorisés des informations, incluant la protection des données numériques et physiques contre toute forme d'atteinte, ainsi que la garantie de conformité aux réglementations en vigueur [13], telles que le Règlement Général sur la Protection des Données (RGPD) dans l'Union européenne [14]. Cette sécurité implique la mise en place de mesures adaptées pour assurer la confidentialité, l'intégrité et la disponibilité des informations selon les besoins et les exigences spécifiques des organisations [15]. De plus, la sécurité informatique joue un rôle crucial dans la protection de l'information, constituant ainsi un aspect important de la sécurité globale des données [16].

I.1.1 Information a sécurisée

Dans le contexte de la sécurité de l'information, il est important de reconnaître les diverses significations du terme "*Information*". En effet, il existe plusieurs définitions courantes, parmi lesquelles se distinguent les deux suivantes :

- L'information désigne l'acte de s'informer, de se renseigner, de faire connaître un fait ou de le rechercher.
- Une information désigne des données, des renseignements, ou une documentation concernant quelque chose ou quelqu'un.

En informatique et en télécommunication, l'information représente un élément de connaissance (tel que la voix, les données et les images) qui peut être conservé, traité ou transmis à l'aide d'un support et d'un mode de codification standardisé [11].

I.1.2 Intérêt de la sécurité

En général, la sécurité fait référence à une situation où les risques et les conditions pouvant causer des dommages physiques, psychologiques ou matériels sont maîtrisés afin de préserver la santé et le bien-être des individus et de la société [12]. Dans le contexte de l'information et des communications numériques, la sécurité se rapporte spécifiquement à la protection des données numériques. Ainsi, la sécurité de l'information revêt une importance capitale pour garantir la protection des données, prévenir les attaques informatiques, maintenir la confiance, respecter les réglementations, minimiser les risques financiers et préserver la réputation de l'organisation.

I.1.3 Rôle de sécurité d'information

Le rôle de la sécurité d'information est essentiel dans le domaine de la cybersécurité, bien qu'ils soient souvent confondus. La sécurité d'information se concentre sur la protection de toutes les données, quel que soit leur format, tandis que La cybersécurité concerne la préservation des systèmes, réseaux et données numériques contre les risques et les attaques éventuelles. Comprendre ces distinctions est crucial pour élaborer une stratégie de sécurité efficace et adaptée aux besoins spécifiques d'une entreprise [19, 20, 21].

La sécurité informatique et la sécurité des informations sont souvent confondues, mais ce sont deux concepts distincts. La sécurité des informations concerne la protection des données, qu'elles soient stockées électroniquement ou physiquement, tandis que la sécurité informatique se concentre exclusivement sur la protection des données numériques. La principale différence réside dans les méthodes de protection appliquées en fonction de la forme de stockage des données. [22]

I.1.4 Principes de base

La sécurité de l'information a trois objectifs fondamentaux [18]: «*la confidentialité* », « *l'intégrité* » et « *la disponibilité* ».

La confidentialité protège les données sensibles contre les accès non autorisés grâce à des mesures telles que le cryptage et l'authentification multifacteurs. L'intégrité garantit que les données ne sont pas altérées de manière non autorisée, grâce à des contrôles d'accès stricts et des sauvegardes régulières. La disponibilité assure un accès rapide et continu aux données pour les utilisateurs autorisés, en mettant en place des solutions de stockage redondantes et des plans de reprise après sinistre. L'authenticité permet de vérifier l'origine des données grâce à des méthodes telles que les signatures numériques. Ensemble, ces principes veillent à ce que les informations restent sécurisées, fiables et accessibles aux personnes autorisées [17, 14].

I.2 Méthodes de sécurité d'information

Les méthodes de sécurité de l'information englobent diverses techniques visant à protéger les données contre les menaces et les vulnérabilités. Ces techniques sont souvent combinées et adaptées en fonction des besoins spécifiques de l'organisation, des réglementations applicables et de l'évolution des menaces.

I.2.1 Cryptographie

La cryptographie, également connue sous le nom de science du secret, est l'étude des techniques permettant d'envoyer des données de manière confidentielle sur un support spécifique [23]. Elle protège les données confidentielles en sécurisant le contenu des communications plutôt que les communications en elles-mêmes. L'ensemble des processus de verrouillage appelés cryptographie (sécurité des données) vise à protéger l'accès à certaines données afin de les rendre incompréhensibles aux personnes non autorisées. En d'autres termes, la cryptographie garantit la confidentialité, l'intégrité et l'imputabilité de ces informations. Le destinataire doit être certain de l'identité de l'émetteur, et inversement [24]. L'opération de cryptage/décryptage nécessite généralement une clé. Il existe généralement deux catégories de clés distinctes :

- **Cryptographie symétrique:** La cryptographie symétrique utilise la même clé secrète (k) pour le cryptage et le décryptage. En général, ce type de cryptosystèmes est plutôt efficace, mais il est nécessaire que l'émetteur et le récepteur aient partagé de manière sécurisée la clé secrète. La cryptographie symétrique est un outil puissant pour protéger les informations, mais elle doit être utilisée avec soin pour garantir la sécurité de la clé et, par conséquent, des données chiffrées.

- **Cryptographie asymétrique:** Dans les systèmes cryptographiques asymétriques, les clés de chiffrement et de déchiffrement sont séparées et l'une ne peut pas être déduite de l'autre. L'une des deux peut donc être rendue publique et l'autre privée. Ces deux clés sont mathématiquement liées, mais il est considéré comme pratiquement impossible de dériver la clé privée à partir de la clé publique.

Comparée à la cryptographie symétrique, la cryptographie asymétrique est généralement plus lente et nécessite plus de ressources computationnelles. C'est pourquoi elle est souvent utilisée pour échanger des clés symétriques, qui sont ensuite utilisées pour chiffrer de grandes quantités de données.

I.2.2 Tatouage numérique

Le tatouage numérique, aussi appelé marquage ou watermarking, est une technique permettant d'intégrer des informations dans des médias numériques tels que des images, des vidéos ou des fichiers audio, de façon à les rendre résistants aux altérations. Son objectif est d'assurer l'identification, l'authentification ou la traçabilité des médias, ainsi que de protéger les droits de propriété intellectuelle. Il doit être robuste contre les attaques pour préserver l'intégrité des données [28].

Le tatouage numérique, souvent associé à d'autres méthodes, a pour objectif de résoudre divers problèmes de sécurité liés aux données numériques, tels que la préservation des droits d'auteur, la prévention de la redistribution non autorisée, et l'intégrité du contenu des données, etc. [29].

- **Tatouage numérique visible:** Dans le cas des tatouages visibles, la marque est facilement perceptible par l'œil humain. Autrement dit, elle est très apparente. On utilise fréquemment des logos et des images comme filigranes dans les systèmes de tatouage visible. Deux inconvénients sont associés aux techniques de tatouage visible [29].: *i)* Il est facile de retirer la marque insérée en la découpant simplement, et *ii)* La visibilité de la marque insérée peut altérer la qualité visuelle de l'image hôte

- **Tatouage numérique invisible:** Dans le cas du tatouage d'images invisible, les informations sont intégrées dans les médias numériques de manière à ce qu'elles ne soient pas perceptibles par l'œil humain. Cette technique permet d'assurer la protection des droits d'auteur, l'authentification et la traçabilité sans altérer la qualité visuelle du contenu. Les marques insérées sont résistantes aux modifications et aux tentatives de suppression, garantissant ainsi l'intégrité et la sécurité des données [29].

I.2.3 Stéganographie

La stéganographie consiste à dissimuler un message secret de grande taille dans une image, un audio ou une vidéo, appelée média cover (ou original). Le média résultant est alors appelé média stégo, qui ne diffère pas beaucoup du média d'origine, du moins à l'œil humain. Cela signifie qu'il est presque impossible de détecter l'existence du message secret dans le média stégo. Le message confidentiel peut se présenter sous forme de texte brut, de texte chiffré ou d'image.

I.3 Biométrie et la sécurité

En règle générale, le manque de sécurité constitue un défi majeur dans de nombreuses applications sensibles liées aux infrastructures économiques, sociales et institutionnelles. La protection de la vie privée, d'une part, et la lutte contre la fraude et la criminalité, d'autre part, nous obligent à mettre en place des mesures de sécurité dans divers secteurs tels que les transports, le contrôle d'accès, la surveillance des frontières, le secteur bancaire et les services publics.

I.3.1 Biométrie et cryptographie

Les forces complémentaires de la biométrie et de la cryptographie permettent d'améliorer la sécurité et l'authentification. La biométrie permet d'identifier les individus de manière unique et personnelle, tandis que la cryptographie propose des techniques solides pour protéger les données et garantir l'intégrité des communications. En associant ces deux domaines, il est possible de concevoir des systèmes plus sécurisés et fiables pour l'identification des utilisateurs, la préservation des données et la gestion des accès [32].

I.3.2 Biométrie et tatouage

Au cours des dix dernières années, de nombreuses études ont suggéré diverses approches pour gérer les droits d'auteur des images en utilisant, par exemple, des mesures cryptographiques. Toutefois, ces modèles effectuent une vérification peu fiable du propriétaire des données. En effet, il est difficile de relier l'identité de l'individu à ces droits d'utilisation dans ces systèmes. Pour remédier à cette situation, des chercheurs ont envisagé l'utilisation de la biométrie. Le tatouage biométrique implique l'ajout d'une marque à une image afin de démontrer sa propriété. Il est nécessaire de calculer la marque insérée en utilisant une méthode biométrique associée à l'identité de l'individu pour assurer une vérification d'identité sécurisée et respectueuse de la vie privée [33].

I.3.3 Biométrie et Stéganographie

Bien que la biométrie et la stéganographie soient souvent perçues comme des concepts distincts, elles peuvent converger dans certaines applications, en particulier dans le domaine de l'authentification secrète et de la transmission sécurisée des données. Dans ce contexte, la biométrie peut être utilisée pour vérifier l'identité d'un individu de manière unique et personnelle, tandis que la stéganographie peut être employée pour dissimuler des informations confidentielles au sein de médias numériques, tels que des images ou des vidéos, de manière à ce qu'elles restent indétectables pour des tiers. Cette combinaison permet de renforcer la sécurité et la confidentialité des systèmes en garantissant à la fois l'authenticité des utilisateurs et la protection des données lors de leur transmission. Ainsi, cette convergence offre des solutions innovantes pour répondre aux exigences croissantes en matière de sécurité et de confidentialité dans divers domaines, allant des transactions financières aux communications gouvernementales sensibles.

I.4 Biométrie

Alors que la technologie continue de modifier notre façon de vivre et de travailler, il est devenu essentiel d'assurer une vérification d'identité sécurisée et efficace dans de nombreux domaines d'activité [25]. La biométrie est une technologie qui permet d'identifier automatiquement une personne en analysant ses caractéristiques physiques ou comportementales uniques. Parmi les méthodes biométriques les plus utilisées pour le contrôle d'accès, on trouve la reconnaissance des empreintes digitales, en raison de sa rentabilité. D'autres méthodes d'identification biométrique incluent la reconnaissance des veines des doigts, des paumes, des visages et des iris. Pour les environnements nécessitant un niveau élevé de sécurité, la reconnaissance de l'iris est la plus précise, suivie de la reconnaissance des veines de la paume. Certains systèmes de sécurité biométrique utilisent une combinaison de ces méthodes, tandis que d'autres n'en utilisent aucune, souvent pour des raisons budgétaires [35].

I.4.1 Propriétés d'une modalité biométrique

Pour garantir l'efficacité de l'exploitation de la biométrie, il est crucial que les modalités biométriques utilisées présentent certaines caractéristiques, permettant ainsi le développement de systèmes biométriques fiables et robustes. Les propriétés indispensables pour chaque modalité biométrique sont les suivantes:

- **Universalité :** Toute la population doit posséder cette modalité ;

- **Unicité :** Deux personnes différentes doivent avoir des représentations différentes de leur biométrie;
- **Stabilité :** Une biométrie, pour servir de moyen d'authentification, doit être relativement stable dans le temps et surtout doit être stable pour une personne quelles que soient les circonstances de l'acquisition (conditions extérieures, conditions émotionnelles de la personne...);
- **Acceptabilité et facilité d'utilisation :** Désigne les contraintes liées à l'acquisition et à l'utilisation d'une modalité biométrique, elle doit être acceptée par le public;
- **Non-reproductibilité :** concerne la facilité ou non de falsifier une modalité biométrique pour éviter une utilisation frauduleuse du système;
- **Permanence :** l'information doit être constante au cours du temps;
- **Performance :** reconnaitre efficacement un individu, critère prédéterminé établi pour évaluer la performance d'un système biométrique;
- **Mesurabilité :** elle peut être mesurée avec différentes capteurs.

Le Fig. I.1 montre un certains traits biométriques couramment.

Fig. I.1: Exemple des traits biométriques.

I.4.2 Modalités biométriques

Les diverses modalités biométriques ont pour objectif commun d'authentifier l'identité d'une personne en examinant ses caractéristiques physiques (morphologiques), comportementales ou biologiques. Parmi les modalités biométriques disponibles, trois grandes catégories se distinguent :

1) Modalités biométriques physiques: Les modalités biométriques physiques (morphologiques) reposent sur l'identification de caractéristiques morphologiques spécifiques obtenues à partir de différentes parties du corps humain, telles que l'œil (pour l'iris et la rétine), la main (pour les empreintes digitales, palmaires et les articulations du doigt, ainsi que la géométrie de la main) ou le visage (Fig I.2). D'autres éléments peuvent également être inclus dans cette liste, tels que la forme de l'oreille, les vaisseaux sanguins de la main, etc. [37, 38].

Fig.I.2 : Exemple des modalités physiques

2) Modalités biométriques comportementales : Les modalités biométriques comportementales (Fig I.3) reposent sur l'étude de certains comportements d'une personne, tels que le tracé de sa signature, l'empreinte de sa voix, l'analyse de sa démarche et de sa manière d'utiliser la souris ou de taper sur un clavier [37].

Fig.I.3 : Exemple des modalités comportementales

3) Modalités biométriques biologiques : La biométrie biologique est une branche de la biométrie qui utilise les caractéristiques biologiques uniques d'un individu pour l'identifier ou l'authentifier [37] basée sur l'analyse des traces biologiques d'une personne, comme L'AND, salive, urine et l'odeur (Fig I.4)

Fig.I.4 : Exemple des modalités biologiques

I.4.3 Système biométrique

Un système biométrique est fondamentalement un système de reconnaissance de formes. Il se compose principalement de deux phases essentielles : l'enrôlement (enregistrement) et la reconnaissance (Test), voir Fig. I.5.

1) Phase d'enrôlement: Dans la première phase, l'utilisateur est encouragé à fournir plusieurs échantillons de la modalité biométrique à l'aide d'un périphérique d'acquisition. Cette étape est généralement suivie d'une phase de prétraitement visant à améliorer la qualité de la modalité acquise. Ensuite, vient la phase de l'extraction de caractéristiques, la plus cruciale, au cours de laquelle les paramètres les plus pertinents de la modalité sont extraits et stockés dans une base de données.

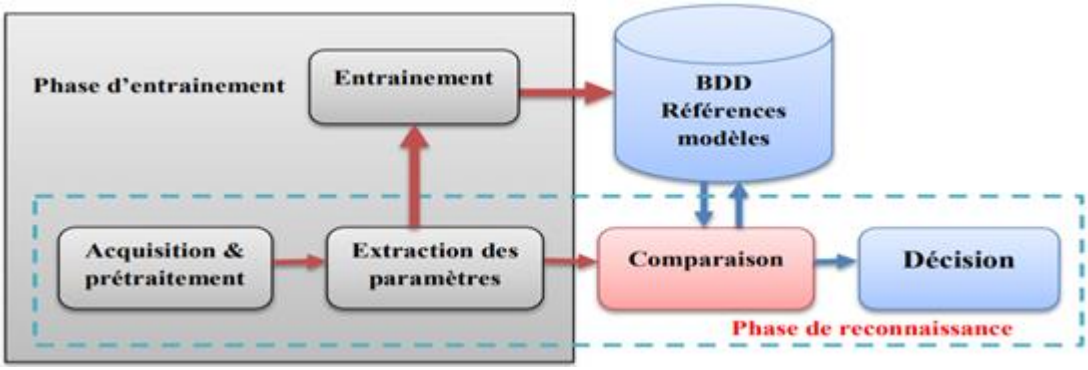

Fig. I.5 : Système biométrique typique

2) Phase de reconnaissance : Dans la phase de reconnaissance, la même modalité de la personne à authentifier (vérifier) ou à identifier est capturé, et les mêmes procédures sont exécutées. En mode d'identification, les caractéristiques sont comparées à tous ceux contenus dans la base de données. En revanche, dans le cas de vérification, les paramètres sont comparés uniquement à ceux de la personne proclamée, et la décision d'accepter ou de refuser l'authentification est annoncée par le système [35, 39].

- **Mode de vérification:** Dans le processus de vérification, également connu sous le nom d'authentification, l'individu cherchant à accéder au système déclare son identité, puis un algorithme effectue une comparaison entre un modèle biométrique associé à cette identité et des modèles biométriques préalablement enregistrés dans la base de données. Pendant la vérification, le système répond à la question "Est-ce que je suis vraiment la personne que je prétends être?" par une décision binaire, oui ou non. Ainsi, il suffit de comparer le modèle avec un seul des modèles présents dans la base de données (1:1) [41].

- **Mode d'identification :** Dans le mode d'identification, la personne désirant entrer dans le système ne déclare pas son identité. Ainsi, le système répond à la question "Qui suis-je ?" en acceptant si l'utilisateur possède un modèle dans la base de données, ou en rejetant si aucun modèle n'est trouvé. Dans cette méthode, l'utilisateur fournit un modèle biométrique qui est

ensuite comparé à tous les modèles biométriques dans la base de données lors de la phase d'enrôlement (1: N).

Le mode d'identification peut être décomposé en deux modes de fonctionnement :
L'identification en mode ensemble fermé : L'identité de la personne dont le modèle biométrique (référence) présente le degré de similitude le plus élevé avec l'échantillon biométrique présent en entrée est constituée par la sortie du système biométrique [37].

L'identification en mode ensemble ouvert : si la similarité la plus élevée entre l'échantillon biométrique testé et tous les modèles préenregistrés est inférieure (ou supérieure) au seuil de sécurité, la personne est rejetée, ce qui implique que l'utilisateur n'est pas enrôlé sinon la personne est acceptée [37].

3) Etapes de système: Un système biométrique est principalement un système de reconnaissance de formes. Ces systèmes visent à classifier des entités (modalités) en catégories (personnes) en se basant sur les observations (vecteur des caractéristiques) effectuées sur celles-ci. Un système de reconnaissance biométrique peut inclure une étape d'apprentissage consistant à apprendre à reconnaître des modalités en se basant sur leurs caractéristiques. Une fois cette étape terminée, le système sera prêt à fonctionner pour reconnaître des individus inconnus.

Quatre modules sont inclus dans un système de reconnaissance biométrique, certains étant similaires à la phase d'enrôlement et à celle de reconnaissance [42, 43] : l'acquisition, l'extraction des caractéristiques, la comparaison (mesure de similarité) et la décision. Les caractéristiques sont acquises et extraites lors de d'enrôlement et de la reconnaissance. Toutefois, la comparaison et la décision sont utilisées spécifiquement lors de la phase de reconnaissance.

- **Acquisition des données :** Il s'agit d'une interface utilisateur chargée de recueillir les informations biométriques d'une personne, telles qu'une caméra, un lecteur d'empreintes digitales, un microphone, etc.

- **Extraction des caractéristiques:** En général, un processus de prétraitement est appliqué avant la phase d'extraction des caractéristiques. Ce processus vise à éliminer les informations superflues présentes, par exemple, dans l'image initiale acquise, afin de la préparer pour l'extraction des caractéristiques biométriques. L'extraction des caractéristiques se base sur l'image prétraitée et extrait uniquement les informations pertinentes pour créer

une nouvelle représentation des données (modèles biométriques). Idéalement, cette nouvelle représentation est censée être unique pour chaque individu et relativement stable.

- **Apprentissage:** L'objectif de l'apprentissage est de fournir au système biométrique un ensemble de formes déjà assimilées. Ce groupe d'apprentissage est chargé d'adapter le système de reconnaissance pour qu'il puisse reconnaître les formes ultérieures de classe inconnue [27].

- **Comparaison :** Dans cette étape, toutes les caractéristiques biométriques extraites sont comparées aux modèles enregistrés dans la base de données du système (modèles de référence) afin d'évaluer le degré de similitude (mesuré par la mesure de similarité).

- **Décision :** L'étape de décision a pour objectif de vérifier l'identité affirmée par un utilisateur ou de déterminer l'identité d'une personne en se basant sur le degré de similarité entre les caractéristiques extraites et les modèles stockés. À ce stade, le système détermine si l'utilisateur est autorisé à accéder au système ou non.

I.5 Système biométrique multimodale

En utilisant des systèmes biométriques qui se basent sur une seule modalité biométrique (connus sous le nom de systèmes unimodaux), il est impossible d'assurer une identification précise. En réalité, les taux d'erreur associés à ces systèmes sont assez élevés, ce qui les rend inacceptables pour des applications de sécurité critiques [44]. Une solution à ce problème consiste à mettre en œuvre des systèmes biométriques multimodaux qui utilisent plusieurs modalités biométriques d'une seule personne [45].

I.5.1 Biométrie multimodale

Les individus se reconnaissent mutuellement grâce à diverses caractéristiques biologiques, physiologiques ou comportementales. Cependant, il n'est pas toujours fiable d'utiliser chaque modalité de manière isolée pour réaliser la reconnaissance [46]. En combinant les informations provenant de différentes modalités, il devient possible de réaliser une identification plus précise. Cette approche vise à surmonter les limitations des systèmes unimodaux, mentionnées ci-dessous. En créant un système biométrique multimodal, qui utilise simultanément différentes modalités biométriques, on cherche à améliorer les performances de reconnaissance [47]. L'objectif est d'augmenter la quantité d'informations discriminantes de chaque individu, ce qui renforce la capacité du système à réaliser la vérification ou l'identification.

I.5.2 Fusion des données

La fusion des données est une méthode employée pour traiter des informations provenant de différentes sources [48]. Elle consiste à combiner les données de ces différentes sources pour obtenir une décision plus précise que celle obtenue à partir de chaque source individuellement. Dans un contexte militaire, la fusion des données a été développée pour des applications telles que la localisation des cibles ennemies et la fusion d'images radar [49]. Les techniques utilisées proviennent de divers domaines tels que le traitement du signal, l'intelligence artificielle, la reconnaissance de formes, la classification, etc. En résumé, la fusion des données consiste à intégrer plusieurs ensembles de données pour en extraire une nouvelle information plus représentative de l'ensemble des données.

Actuellement, la fusion des données joue un rôle de plus en plus important dans de nombreux secteurs, facilitant ainsi l'extraction efficace d'informations de plus en plus pertinentes et précises par les scientifiques. Bien que son objectif initial ait été d'améliorer la qualité des réponses aux problèmes militaires, elle trouve désormais des applications dans un large éventail de domaines, notamment la télédétection, la prévision météorologique, la biométrie multimodale, les applications éducatives et la robotique [50]..

I.5.3 Stratégies de fusion

Le principal défi de la fusion réside dans la synthèse des informations provenant de différentes sources. Cependant, comme illustré dans la Figure I.6, il existe de multiples situations possibles pour les sources d'information qui peuvent être prises en compte dans un système biométrique multimodal [51].

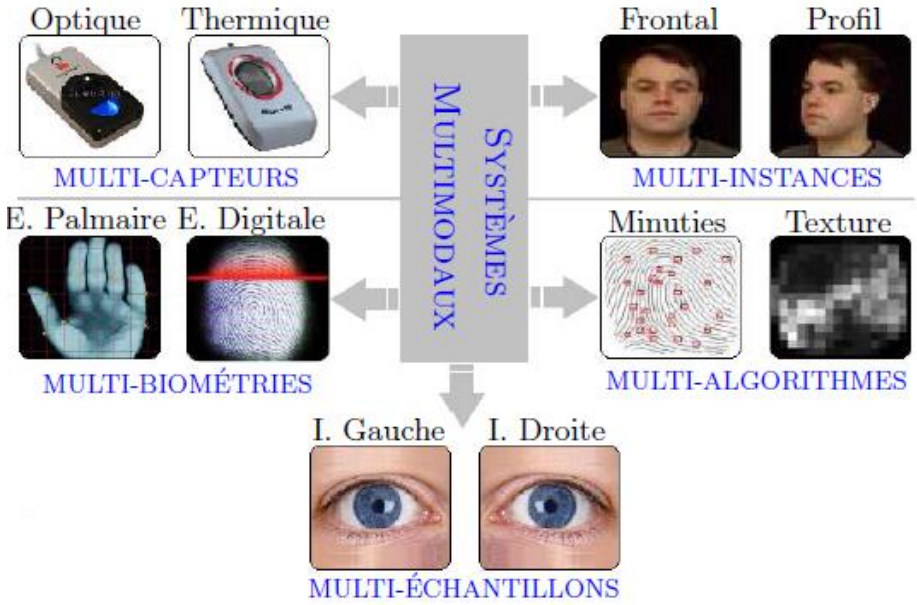

Fig.I.6 Différents systèmes biométriques multimodaux.

1) Systèmes multi-capteurs: Dans ces systèmes, une même modalité biométrique est analysée en utilisant plusieurs capteurs afin d'extraire différentes informations à partir de l'enregistrement des images. Par exemple, pour procéder à la reconnaissance faciale, un système peut enregistrer à la fois le contenu de la texture (2D) du visage d'une personne à l'aide d'une caméra CCD, et la forme de la surface du visage (3D) à l'aide d'un autre capteur. Pour l'acquisition de l'empreinte digitale, il est possible d'utiliser à la fois un capteur optique et un capteur thermique.

2) Systèmes multi-instances : Il est possible d'utiliser un seul capteur pour obtenir plusieurs instances de la même modalité biométrique afin de prendre en considération les variations qui peuvent se produire au sein de celle-ci. Prenons l'exemple d'un système de reconnaissance faciale qui peut capturer plusieurs images du visage en modifiant la pose (profil frontal, profils gauches et droits), l'expression ou l'illumination, afin de tenir compte des subtilités de la pose faciale.

3) Systèmes multi-algorithmes: Dans ces systèmes, les données biométriques sont traitées à l'aide de différents algorithmes. La diversité des algorithmes peut être présente dans le module d'extraction, où plusieurs ensembles de caractéristiques sont pris en compte, et/ou dans le module de comparaison, où différents algorithmes de comparaison sont utilisés. Par exemple, il est possible d'associer des algorithmes d'analyse de texture et de minutie pour traiter la même image d'empreinte digitale afin d'extraire différentes caractéristiques qui peuvent être utilisées pour améliorer les performances du système.

4) Systèmes multi-échantillons: Dans ces systèmes, il est possible d'utiliser un seul capteur pour obtenir plusieurs échantillons de la même modalité biométrique. Par exemple, on peut utiliser les empreintes digitales des doigts gauche et droit, ou les iris gauche et droit d'une personne pour vérifier son identité. Dans cette situation, les données sont traitées par le même algorithme, mais nécessitent différentes opérations lors de l'enregistrement, contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule opération.

5) Systèmes multi-biométries: Dans ces systèmes, diverses modalités biométriques sont associées pour établir l'identité d'une personne. Prenons l'exemple des caractéristiques de l'empreinte palmaire et de l'empreinte digitale. L'objectif de cette stratégie de fusion est d'exploiter les avantages de chaque système biométrique tout en évitant leurs inconvénients. En réalité, les systèmes qui combinent différentes informations provenant de la même biométrie permettent d'améliorer les performances en reconnaissance en réduisant l'impact de la variabilité intra-classe. Cependant, ils ne suffisent pas à résoudre efficacement tous les

problèmes des systèmes monomodaux. C'est pourquoi les systèmes multi-biométries ont suscité un grand intérêt au sein de la communauté.

I.5.4 Niveaux de fusion

La fusion peut être réalisée dans un système biométrique multimodal en utilisant les informations disponibles dans n'importe quel module du système. Il est possible de combiner différents systèmes biométriques à quatre niveaux différents [52] : au niveau capteur, au niveau des caractéristiques, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision. On peut diviser ces quatre niveaux de fusion en deux sous-ensembles: la fusion pré-classification (avant la comparaison) et la fusion post-classification (après la comparaison).

1) Fusion pré-classification: La fusion pré-classification consiste à fusionner les informations provenant de plusieurs données biométriques au niveau du capteur ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

- **Fusion au niveau du capteur (Sensor Level) :** Les systèmes biométriques multicapteurs prélevant le même exemple d'une modalité biométrique avec deux capteurs distincts. Le traitement des échantillons capturés peut être effectué avec un ou plusieurs algorithmes. Un exemple de ce niveau est la fusion de l'image de l'empreinte palmaire avec celle du visage (Fig. I.7). Un autre exemple de fusion au niveau capteur consiste à assembler plusieurs images d'empreintes digitales pour former une image finale plus complexe. La fusion au niveau capteur est relativement peu utilisée car les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue à l'avance.

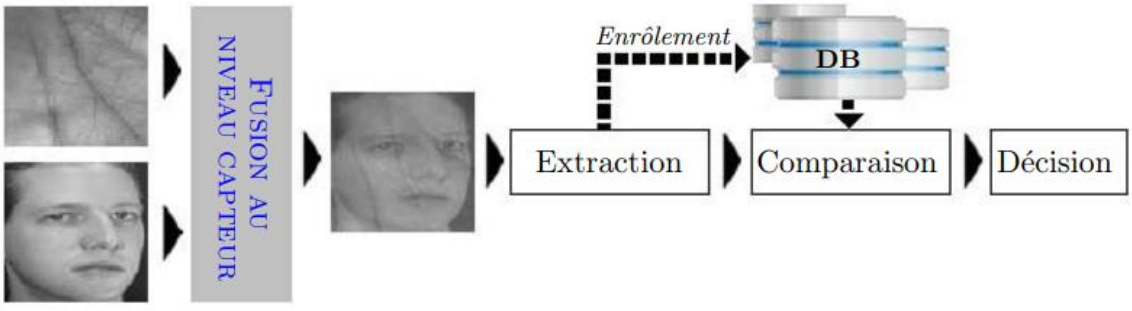

Fig.I.7 Système multimodal basé sur la fusion au niveau du capteur.

- **Fusion au niveau des caractéristiques (Feature Level) :** La fusion au niveau des caractéristiques est extrêmement utile pour la classification. À ce niveau, les informations extraites après différentes phases de traitement et d'analyse des mesures sont combinées.

Différents vecteurs de caractéristiques, provenant de plusieurs capteurs ou obtenus à l'aide de différents algorithmes d'extraction, sont fusionnés. Un exemple de ce niveau de fusion est décrit dans une étude où les auteurs proposent une méthode de fusion de caractéristiques pour combiner des données faciales et des empreintes palmaires (Fig. I.8). Dans cette méthode, la fusion est réalisée en concaténant des images obtenues par transformée de Gabor sur les images du visage et les empreintes de la main.

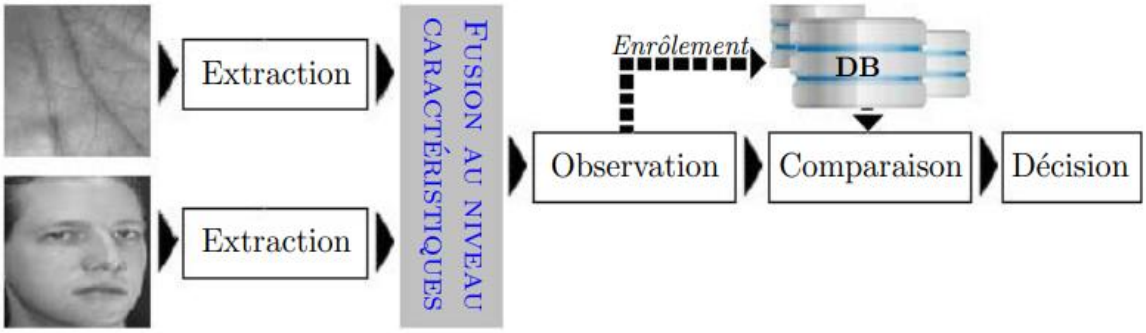

Fig.I.8 : Système multimodal basé sur la fusion au niveau des caractéristiques.

Les méthodes de fusion pré-classification sont relativement peu utilisées en raison des contraintes spécifiques qu'elles imposent, lesquelles ne peuvent être satisfaites que dans des applications très spécifiques. En revanche, la fusion post-classification est considérée comme la plus prometteuse par les chercheurs.

2) Fusion post-classification : La fusion post-classification peut s'effectuer au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion représente un problème bien documenté dans la littérature, souvent désigné sous le nom de "Multiple Classifier Système".

- **Fusion au niveau des décisions (Decision Level) :** Avec cette approche, chaque sous-système biométrique effectue de manière autonome les étapes d'extraction des caractéristiques, de comparaison et de reconnaissance. Ensuite, chaque système fournit une décision binaire sous forme de "OUI" ou "NON", représentées respectivement par 0 et 1. Le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1 (Fig. I.9). Les méthodes les plus utilisées sont les fonctions booléennes. Un grand nombre de méthodes de fusion de décision sont disponibles. La fusion au niveau des décisions est souvent préférée en raison de sa simplicité..

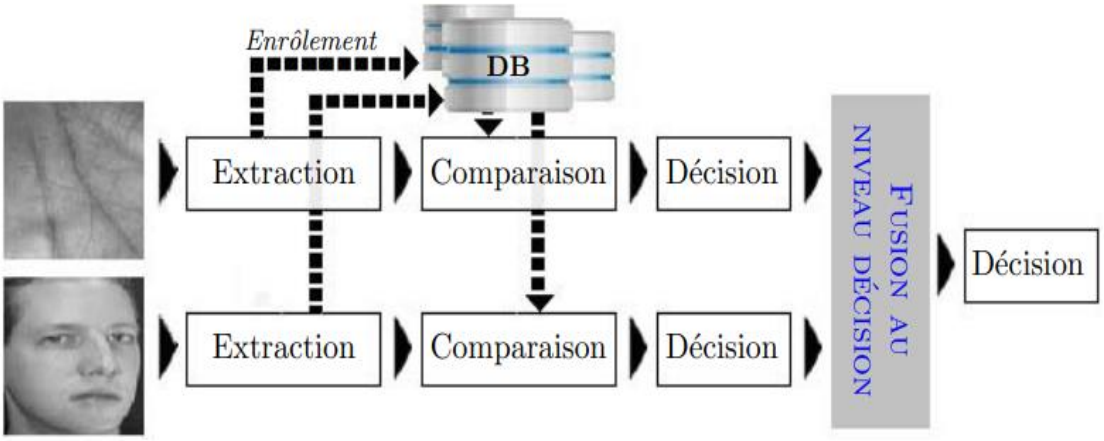

Fig.I.9 : Système multimodal basé sur la fusion au niveau des décisions.

- **Fusion au niveau score (Score Level) :** Dans la fusion au niveau des scores, les scores individuels sont combinés pour former un score unique, qui est ensuite utilisé pour prendre la décision finale. La fusion au niveau des scores [30] est le type de fusion le plus couramment utilisé car elle peut être appliquée à tous les types de systèmes avec des méthodes simples et efficaces. La Fig. I.10 illustre un système basé sur la fusion au niveau des scores. Plusieurs méthodes de fusion des scores (règles de fusion) existent. Parmi les règles les plus utilisées, on trouve la somme des scores, la somme pondérée des scores, le minimum des scores, le maximum des scores et le produit des scores.

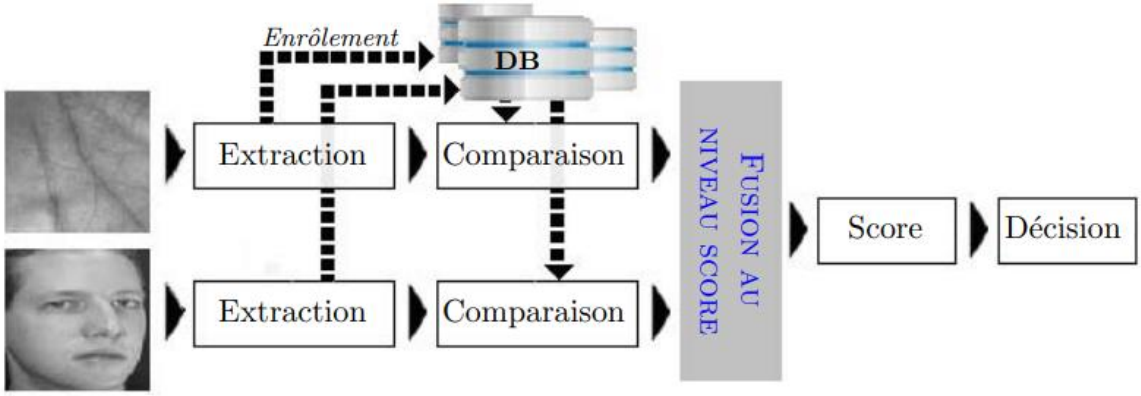

Fig.I.10 : Système multimodal basé sur la fusion au niveau score.

I.6 Conclusion

Avec l'évolution technologique et la croissance continue des activités en ligne, la sécurité des informations est devenue une préoccupation cruciale. L'authentification des individus est largement considérée comme la méthode la plus prometteuse pour garantir la sécurité des informations en limitant leur accès. Cependant, atteindre un niveau élevé de sécurité dans un

schéma d'authentification reste un défi constant. Malgré cela, la biométrie est de plus en plus utilisée dans ce contexte. Les méthodes biométriques employées dans l'authentification offrent aux systèmes un accès sécurisé à distance aux ressources sensibles.

Chapitre 2

Authentification biométrique à distance

Résumé

Ce chapitre fournit une analyse détaillée de l'authentification à distance et des techniques qui lui sont associées. Il examine les méthodes d'extraction de caractéristiques, ainsi que l'utilisation de classifieur basé sur l'apprentissage automatique non supervisé. De plus, il explore l'application de différente technique dans le domaine du traitement biométrique et étudie les opportunités qu'elles offrent pour la protection des données sensibles. En conclusion, ce chapitre propose un modèle visant à optimiser l'efficacité de l'authentification à distance et à garantir une sécurité accrue des informations.

Introduction

Les modèles biométriques sont considérés comme des données personnelles et sensibles. Pour garantir leur sécurité, de nombreux systèmes ont été mis en place afin de les protéger, préservant ainsi la vie privée et l'identité des individus. Dans ce chapitre, nous fournirons un aperçu des solutions disponibles pour protéger les modèles biométriques, en mettant l'accent sur celles basées sur les cryptosystèmes. Enfin, nous présenterons en détail la méthode proposée, qui s'appuie sur des cartes chaotiques pour chiffrer les modèles biométriques, augmentant ainsi la sécurité et la protection de la vie privée des individus.

II.1 Authentificationbiométrique à distance

Dans le monde numérique, l'authentification de l'identité à distance est essentielle pour une multitude d'applications et de services, tels que la banque en ligne, le commerce électronique, les soins de santé à distance et les réseaux sociaux. Néanmoins, les méthodes classiques d'authentification, comme les mots de passe ou les codes PIN, sont fréquemment sujettes aux piratages ou susceptibles d'être oubliées. Qui plus est, elles ne fournissent pas toujours la certitude que l'utilisateur accédant au service est bien la personne qu'elle prétend être. C'est dans ce cadre que les services d'authentification biométrique entrent en jeu. Ces systèmes exploitent les traits physiques ou comportementaux distinctifs des individus, tels que les empreintes digitales, les caractéristiques faciales, la voix ou l'iris, afin de confirmer leur identité et de leur permettre d'accéder à un service spécifique. L'authentification biométrique procure ainsi un degré de sécurités accrues et une confirmation plus fiable de l'identité des utilisateurs [57].

II.1.1 Avantages de l’authentification biométrique à distance

L'authentification biométrique transforme la vérification de l'identité à distance. En utilisant des caractéristiques biométriques uniques, elle offre un haut niveau de sécurité, de commodité, de précision et améliore l'expérience utilisateur. Les services d'authentification biométrique présentent de nombreux avantages par rapport aux méthodes classiques, tels que :

- **Haute Sécurité:** les caractéristiques biométriques sont plus difficiles à falsifier, voler ou deviner, ce qui les rend plus résistantes à la fraude et au vol d'identité. Les services d'authentification biométrique éliminent également le besoin de mémoriser ou de stocker des mots de passe, qui peuvent être facilementpiratésouperdus.

- **Confort:**les services d'authentification biométrique offrent un moyen rapide et facile d'accéder au service, sans avoir à taper, glisser ou scanner. Les utilisateursdoiventsimplement présenter leurs caractéristiques biométriques, telles que leur visage ou leurs doigts, à l'appareil, et le système les reconnaîtra automatiquement et leuraccorderal'accès.

- **Précision:** l''authentification biométrique sont plus précis que les méthodes classiques de vérification d'identité, car ils réduisent les risques de faux positifs ou de faux négatifs. Les faux positifs se produisent lorsqu'un utilisateur non autorisé se voit accorder par erreur l'accès à un système ou à un service, tandis que les faux négatifs se produisent lorsqu'un utilisateur autorisé se voit refuser par erreur l'accès à un système ou un service. L'authentification biométrique utilise des algorithmes et des technologies avancés pour garantir que les caractéristiques biométriques correspondent aux modèles stockés avec un degré élevé de confiance et de précision.

- **Expérience utilisateur:** l'authentification biométrique améliore l'expérience utilisateur en offrant un moyen personnalisé, intuitif et interactif de vérifier l'identité d'une personne. Elle peut également améliorer la satisfaction, la fidélité et la confiance des utilisateurs, car elle démontre de l'engagement du système ou du service à protéger la confidentialité et la sécurité de l'utilisateur.

II.1.2 Défis de l’authentification biométrique à distance

L'authentification biométrique révolutionne la vérification d'identité en fournissant un moyen rapide, pratique et sécurisé de vérifier l'identité d'une personne à l'aide de caractéristiques biométriques uniques. Cependant, ce moyen est également confronté à plusieurs défis qui doivent être relevés pour garantir sa fiabilité, sa facilité d'utilisation et son acceptabilité.

- **Confidentialité:** Les données biométriques sont des informations sensibles et personnelles qui peuvent révéler beaucoup sur l'identité d'un individu. Par conséquent, l'authentificationbiométrique doit respecter les droits à la vie privée des utilisateurs et protéger leurs données biométriques contre tout accès, utilisation ou divulgation non autorisés.

- **Protection des données :** les données biométriques sont vulnérables aux cyberattaques, au vol, à la perte ou à la corruption. Par conséquent, l'authentification biométrique doit mettre en œuvre des mesures strictes de protection des données pour garantir l'intégrité, la disponibilité et la confidentialité des données biométriques. Par exemple, les données biométriques doivent être cryptées, hachées ou anonymisées avant d'être transmises ou stockées, et doivent être supprimées ou détruites après utilisation.

- **Usurpation:** l'authentification biométrique peut être trompés ou contournés par des attaques d'usurpation d'identité, dans lesquelles l'attaquant soumet un échantillon biométrique faux ou volé au système. Par conséquent, l'authentification biométrique doit améliorer leurs capacités de détection et de prévention des usurpations d'identité afin de garantir l'authenticité et la validité des échantillons biométriques.

- **Scalabilité:** L'authentification biométrique doit évoluer pour s'adapter à la demande croissante et à la diversité des utilisateurs et des applications. Par conséquent, les systèmes d'authentification biométrique doivent améliorer leurs performances, leur efficacité et leur précision afin de gérer de grandes quantités de données et de transactions biométriques.

II.1.3 Types d'authentification biométrique à distance

Comme mentionné précédemment, l'authentification biométrique offre un haut niveau de sécurité, rendant la falsification ou l'usurpation très difficile. C'est pourquoi certaines technologies biométriques ont été intégrées dans de nombreux services et ont rencontré un grand succès. Ci-dessous, nous explorons certaines des technologies biométriques utilisées dans l'authentification biométrique.

- **Empreinte digitale:** Il s'agit de l'une des méthodes d'authentification biométrique les plus anciennes et les plus utilisées. La vérification des empreintes digitales est rapide, précise et économique, et peut être intégrée à divers appareils, tels que les smartphones, les ordinateurs portables ou les serrures de porte.

- **Visage:** Il s'agit d'une méthode d'authentification biométrique plus récente et plus avancée, qui utilise la technologie de reconnaissance faciale pour identifier une personne en fonction de ses caractéristiques faciales. La vérification faciale est un processus pratique, sans contact et non intrusif qui peut être effectué à l'aide d'un appareil photo ou d'un Smartphone.

- **Iris:** Il s'agit d'une méthode d'authentification biométrique hautement sécurisée et précise qui utilise le motif unique de l'iris, l'anneau coloré autour de la pupille, pour identifier une

personne. L'authentification de l’iris est sans contact, rapide et fiable, et peut être utilisée dans des applications hautement sécurisées, telles que le contrôle des frontières, les services bancaires ou les soins de santé.

- **Voix :** Il s'agit d'une méthode d'authentification biométrique comportementale, qui utilise les caractéristiques uniques de la voix d'une personne pour vérifier son identité. L'authentificationvocaleestnaturelle, simple et flexible, et peut être effectuée par téléphone, en ligne ou en personne[57].

II.2 Protection de modèle biométrique

Les données biométriques sont extrêmement sensibles et personnelles, et leur mauvaise utilisation peut entraîner de graves préjudices pour les utilisateurs, notamment l'usurpation d'identité, la fraude ou la discrimination. Pour cette raison, il est impératif de protéger les données biométriques contre tout accès, modification ou divulgation non autorisés. Cela peut être réalisé grâce à diverses mesures de sécurité telles que l'anonymisation ou encore le hachage, le cryptage. De plus, il est essentiel de recueillir, stocker et utiliser les données biométriques avec le consentement et la pleine connaissance des utilisateurs, et en respectant scrupuleusement les lois et réglementations en vigueur.

Les techniques de protection de modèle biométrique sont des méthodes employées pour sécuriser les données biométriques stockées dans un système d'authentification. Ces techniques ont pour objectif d'empêcher tout accès non autorisé, toute modification ou divulgation des informations biométriques, tout en autorisant leur utilisation légitime pour l'authentification. Le cryptage du modèle biométrique ainsi que la biométrie révocable sont parmi les moyens les plus efficaces pour protéger les modèles biométriques[60].

II.2.1 Biométrie révocable

Les modèles biométriques d'une personne sont des caractéristiques permanentes et largement immuables, ce qui pourrait conduire à une compromission biométrique permanente en cas de vol du modèle. Pour résoudre ce problème, le concept de biométrie révocable a été introduit. Ce concept permet qu'un modèle biométrique puisse être annulé et révoqué, tout comme un mot de passe, tout en restant unique à chaque application. Le concept de la biométrie révocable repose sur la transformation des données biométriques brutes, de telle sorte que les données transformées soient sûres et respectueuses de la vie privée.

1) Propriétés de la biométrie révocable: La biométrie révocable possède plusieurs propriétés clés qui assurent sa sécurité et son efficacité.

- **Non-inversibilité:**Il doit être difficile, voire impossible, de reconstruire les caractéristiques biométriques originales à partir des modèles biométriques transformés, garantissant ainsi la protection de l'informationbiométrique brute.
- **Diversité:**il doit être possible de générer plusieurs modèles biométriques à partir d'une seule donnée brute, chaque modèle biométrique étant unique pour une application ou un contexte particulier.
- **Performance:** l'efficacité du système de vérification biométrique ne doit pas être détériorée par la transformation.
- **Révocabilité:** La capacité de révoquer et de remplacer un modèle biométrique compromis par un nouveau modèle, similaire à la manière dont on réinitialise un mot de passe en cas de compromission.

La biométrie révocable permet de renforcer la sécurité des systèmes biométriques, offrant ainsi une solution viable pour protéger les données biométriques tout en maintenant la praticité et l'efficacité des méthodes d'authentification biométrique.

2) Transformation non-inversible: La technique couramment utilisée pour la révocabilité biométrique est la transformation non-inversible. Cette technique consiste à appliquer une transformation mathématique aux données biométriques d'origine pour générer une nouvelle version. Les transformations doivent être non-inversibles, ce qui signifie qu'il est difficile, voire impossible, de revenir à l'original à partir des données transformées. Si les données transformées sont compromises, une nouvelle transformation peut être appliquée pour créer une nouvelle version[58].

II.2.2 Cryptage du modèle biométrique

Le cryptage des données biométriques est une méthode de protection des informations sensibles des utilisateurs en les transformant en une forme cryptée accessible uniquement aux personnes autorisées. Cela garantit que même si les données sont interceptées, elles restent inutiles à toute entité non autorisée.

Le cryptage des données biométriques implique généralement l'utilisation d'algorithmes qui convertissent les données biométriques en une représentation mathématique, appelée modèle. Ce modèle est ensuite crypté à l'aide d'algorithmes de cryptage puissants, ce qui rend pratiquement impossible l'ingénierie inverse et la reproduction des données biométriques d'origine. Pour décrypter les données biométriques cryptées, une clé sécurisée est nécessaire. La clé doit être stockée séparément des données et contrôlée par le personnel autorisé. Des

audits réguliers doivent être effectués pour empêcher tout accès non autorisé à la clé privée[60].

II.3Système proposé

Le système proposé est un système d'identification biométrique à distance équipé d'une fonction de protection des caractéristiques biométriques. Comme tout système biométrique, notre proposition fonctionne en deux phases distinctes : la phase d'enrôlement (enregistrement) au niveau du serveur principal et la phase d'identification à distance.

II.3.1Phase d'enrôlement

Durant la phase d'enregistrement (Fig. II.1), opérant au niveau du serveur principal et pouvant se dérouler en présence de l'utilisateur ou à distance, l'empreinte de l'utilisateur est capturée et traitée pour extraire ses caractéristiques biométriques. Ensuite, le processus d'apprentissage a lieu et les paramètres du modèle d'apprentissage sont enregistrés dans la base de données du serveur, ainsi que la clé secrète, qui peut être unique pour chaque utilisateur ou publique pour tous les utilisateurs.

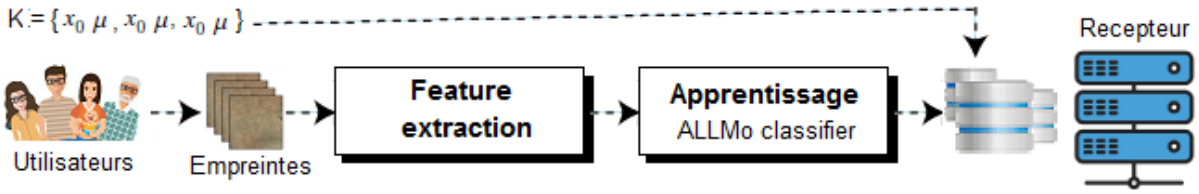

Fig. II.1 Phase d'enrôlement

En cas d'enregistrement à distance, un numéro confidentiel est transmis à l'utilisateur par un canal sécurisé, tel qu'un téléphone, par lequel le modèle biométrique est crypté puis transmis pour l'enregistrement.

II.3.2 Phase d'identification

Dans la phase d'identification(Fig. II.2), l'empreinte de l'utilisateur est capturée au niveau du terminal, tel qu'un Smartphone, puis traitée pour extraire le vecteur de caractéristiques. Ensuite, elle est cryptée et transmise au serveur. Ce dernier procède au déchiffrement des données reçues et initie un processus d'identification en ensemble ouvert afin de vérifier si l'expéditeur appartient à la base de données du système. Si tel est le cas, un processus d'identification en ensemble fermé est engagé pour déterminer l'identité de l'expéditeur.

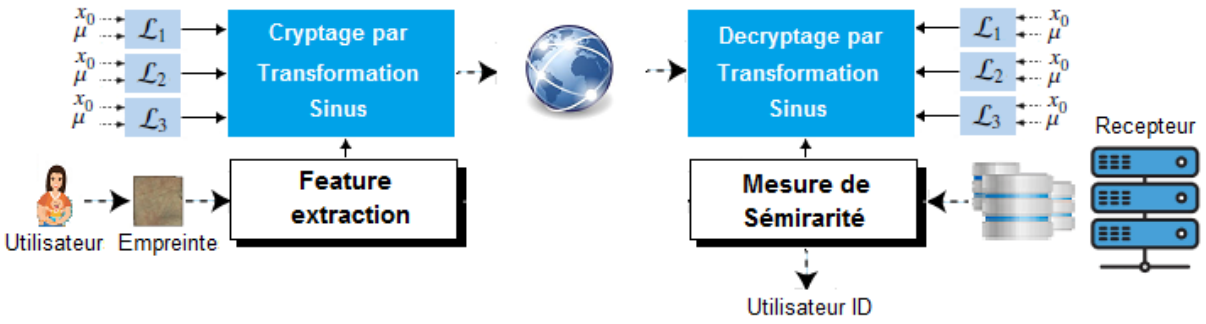

Fig. II.2 Phase d'identification

II.3.3 Fondements théoriques

L'extraction de caractéristiques est une étape cruciale dans les applications biométriques en raison de la diversité des caractéristiques présentes dans les images. Les chercheurs ont ainsi déployé d'importants efforts pour améliorer ce processus, étant donné son impact significatif sur la conception finale d'un système biométrique. Dans cette sous-section, nous aborderons notre méthode d'extraction de caractéristiques, le classifier utilisé et la méthode de cryptage.

1) Histogramme de gradient orienté : L'histogramme de gradient orienté (Histogram of Oriented Gradients-HOG) est une technique puissante de description de caractéristiques, largement utilisée en vision par ordinateur et en traitement d'images, en particulier pour la détection d'objets. Il décrit la distribution des gradients d'intensité locaux (variations des valeurs de pixels) au sein d'une image.

Les caractéristiques HOG agissent comme une représentation cartographique des contours, capturant à la fois les détails sur l'amplitude du gradient et les positions des contours dans des cellules spécifiques. Supposons que l'entrée soit une fenêtre I de dimensions $H \times W$ d'une image en niveaux de gris, ou même l'image entière, pour créer une fonction HOG, nous suivons les étapes suivantes :

Calcul des gradients: Déterminer les composantes du gradient (I_x, I_y)par :

$$\begin{cases} I_x(i,j) = I(i,j+1) - I(i.j-1) \\ I_y(i,j) = I(i-1,j) - I(i+1,j) \end{cases} i = 1 \dots H\ ,\ j = 1 \dots W \qquad (1)$$

Le gradient est ensuite transformé en coordonnées polaires avec un angle limité entre 0° et 180° degrés pour identifier les gradients opposés.

$$\begin{cases} \mu = \sqrt{I_x^2 + I_y^2} \\ \theta = \frac{180}{x}\ (\tan^{-1}(I_x, I_y))\ mod\pi \end{cases} \qquad (2)$$

Oùtan^{-1}est la tangente inverse, qui donne des valeurs comprises entre -π et π, et μ et θ désignent respectivement l'amplitude et la direction (angle) du gradient de chaque pixel.

Histogrammes d'orientation des cellules : La fenêtre est divisée en cellules voisines de taille $c \times c$ qui ne se chevauchent pas. Ensuite, pour chaque cellule, un histogramme des directions de gradient est calculé et trié dans B bins. Les bins sont numérotées de 0 à $B-1$ et chacune a une largeur de $\omega = \frac{180}{B}$.

Normalisation des blocs : Pendant cette étape, les cellules sont disposées en blocs de pixels superposés de taille $2c \times 2c$ avec un décalage vertical et horizontal de c pixels. Ensuite, les histogrammes des quatre cellules de chaque bloc sont fusionnés en un seul bloc, qui est ensuite normalisé en utilisant la norme euclidienne.

$$b_k = \left[h_{(i,j)}, h_{(i,j+1)}, h_{(i+1,j)}, h_{(i+1,j+1)}\right] \quad (3)$$

Où b_k désigne la caractéristique du bloc k et $h_{(i,j)}$, l'histogramme de la cellule *(i, j)*.Cette caractéristiques de bloc estnormaliséecomme suit :

$$\widetilde{b_k} = \frac{b_k}{\sqrt{\|b_k\|^2 + \in}} \quad (4)$$

Où ∈ est une petite constante positive qui empêche la division par zéro dans des blocs sans gradient.

Caractéristique HOG : Enfin, pour représenter l'intégralité de la caractéristique de la fenêtre, toutes les caractéristiques de bloc normalisées ($\widetilde{b_k}$) sont concaténées pour produire un vecteur de caractéristiques HOG ($\mathcal{H}$), comme indiqué ci-dessous :

$$\mathcal{H} = [\widetilde{b_1}, \widetilde{b_2}, \dots, \widetilde{b_k}, \dots, \widetilde{b_p}] \quad (5)$$

Où p est le nombre de blocs dans la fenêtre.Enfin, la fonction HOG résultante est également normalisée à l'aide de l'équation (4) [58].

2) Fonction d'image statistique binarisée: La fonction d'image statistique binarisée (BinarizedStatistical Image Features- BSIF) est méthodeinspirée des méthodologies: motifs binaires locaux (Local Binary Pattern: LBP) et quantification de la phase locale (Local Phase Quantization : LPQ). Dans cette méthode, des patchs locaux de l'image sont projetés sur un sous-espace préalablement obtenu, puis le code binaire de chaque pixel est calculé par la binarisation de tous les résultats de projection. Pour obtenir le descripteur d'image, le code binaire de chaque pixel est d'abord converti en une valeur décimale, puis la valeur de pixel d'origine est remplacée par la valeur décimale calculée. Le descripteur d'image peut être

utilisé pour obtenir le vecteur de caractéristiques de l'image analysée. Il est important de mentionner que le sous-espace de la projection est obtenu en appliquant la méthode d'analyse en composants indépendants (Independent Component Analysais: ICA) à un ensemble d'images naturelles.

Filtrage : L'objectif principal de l'étape de filtrage (convolution) est de filtrer les caractéristiques inutiles de l'image d'entrée. En pratique, ce processus utilise des filtres prédéfinis et chaque filtre est convolé avec l'image d'entrée.

Afin de décrire le cadre du système, supposons que nous ayons une image d'entrée de taille$H \times W$ et que la taille du patch, c'est-à-dire la taille du filtre de convolution (2D), soit :

$$W_i = k_1 \times k_2, \quad i = 1,2,\cdot\cdot\ \ell \tag{6}$$

Où ℓ désigne le nombre de filtres dans la couche de convolution. Il est important de noter que $k_j|_{j=1,2}$est un nombre entier impair satisfaisant les conditions suivantes : $k_j \leq h$ et $k_j \leq w$.

Les sorties de cette étape sont obtenues en filtrant l'image d'entrée (I_o) par les filtres W_i:

$$I_s^i = I_o \circledast W_i, \quad i = 1,2,\cdot\cdot,\ell \tag{7}$$

Où $\circledast$ désigne un processus de convolution 2D. Il est important de noter que pour obtenir des images filtrées de même taille que I_o, une interpolation de frontière (traitement des bords par remplissage avec des zéros) est appliquée. Enfin, en utilisant les Lfiltres, nous pouvons obtenir L images filtrées pour chaque image d'entrée.

Hachage binaire : Dans cette couche, les ℓ sorties pour l'image d'entrée, sont converties en une image à valeur entière en utilisant la quantification binaire et la conversion binaire en décimal. Le processus de quantification binaire transforme une valeur réelle en valeur binaire. En fait, le principe de seuillage est appliqué, comme suit:

$$I_s^{b,i} = \begin{cases} 1 & \text{if } I_s^i \geq 0 \\ 0 & \text{if} I_s^i < 0 \end{cases}, \quad i = 1,2,\cdot\cdot\ \ell \tag{8}$$

Dans l'étape de conversion binaire, la chaîne de binaires (ℓ-bits) autour de chaque pixel est convertie en valeur entière. Pour cela nous utilisons le polynôme de décodage suivant :

$$I_s^h = \sum_{i=1}^{\ell} I_s^{b,i} \cdot 2^i, \quad i = 1,\cdot\cdot\ \ell \tag{9}$$

Où I_s^hest le descripteur de l'image d'entrée.

Histogramme: l'histogramme de l'image descripteur I_s^hest calculé par bloc pour une forte discrimination. Pour cela, nous partitionnons d'abord le descripteur I_s^h en blocs. Ainsi, en supposant que la taille du bloc utilisé ($\mathcal{B}$) est $b_1 \times b_2$, chaque bloc ($\mathcal{B}_c$) est représenté par un

d'histogramme.Tous les histogrammes calculés sont donc concaténés en un seul vecteur pour obtenir le vecteur de caractéristiques biométriques de l'image d'entrée (I_o):

$$\mathcal{V}_o = \left[\mathcal{H}_1, \mathcal{H}_2, \cdots \mathcal{H}_{\mathcal{N}_B}\right] \quad (10)$$

Où $\mathcal{N}_B$ est le nombre blocs [59] .

3) Classificateur ALMMo-0 : Le Classificateur Autonome Multi-Modèle d'Ordre Zéro (Autonome Multi-Modèle d'Ordre Zéro-ALMMo-0) est une technique de classification de nouvelle génération basée sur l'apprentissage automatique supervisé, non supervisé et semi supervisé. Il s'agit d'une méthode innovante pour classifier des données non étiquetées.

- **Processus de fonctionnement:**Le classifier ALMMo utilise des règles floues de type AnYa et l'estimateur EDA pour effectuer la classification des données d'une manière adaptative et autonome, facilitant ainsi la gestion de problèmes complexes. Les équations et les formules mathématiques utilisées dans chaque étape du processus renforcent la rigueur et la précision du modèlecomme suit :

$$Ri: x * i \rightarrow Label\ i \quad (11)$$

où $x * i$est le point focal du $i^{ème}$ nuage de données et Labeliest l'étiquette correspondante.

- **Estimateur EDA :** L'estimateur EDA est utilisé pour révéler les propriétés de l'ensemble des données observées de manière autonome. Pour chaque échantillon de données dans l'espace euclidien, sa densité unimodale est calculée comme suit :

$$\sigma ik = Xk - || \mu k || \quad (12)$$

Où μ_k est la moyenne globale de tous les échantillons de données au $k^{ième}$instant et X_k est le produit scalaire moyen.

- **Etapes fonctionnement :** Le classificateur ALMMo est un système complexe qui se décompose en trois étapes principales :

Architecture à Modèles Multiples: Reposant sur des règles FRB où R≥CR ≥ CR≥C (nombre de classes), chaque nouvelle donnée est envoyée à tous les sous-classificateurs, qui génèrent chacun un score de confiance. La règle du "vainqueur prend tout" assigne ensuite l'échantillon à la classe la plus probable

$$Label = arg\ max\ (\lambda_i) \quad (13)$$

Étape d'Apprentissage : Les nouvelles données sont normalisées et les règles FRB AnYa correspondant à leur classe sont mises à jour. Une nouvelle règle est créée si certaines

conditions sont remplies. Les paramètres des règles sont mis à jour en fonction des caractéristiques de chaque échantillon

$$\begin{cases} Fi \leftarrow Fi + 1 \\ x_{Fi}^{*i} \leftarrow x_k^i \\ M_{fi}^{*i} \leftarrow 1 \\ r_{fi}^{*i} \leftarrow r_0 \end{cases} \quad (14)$$

Étape de Validation: Chaque échantillon de validation est envoyé à tous les sous-classificateurs FRB AnYa correspondant aux classes de l'ensemble de données. Le score de confiance de chaque règle est généré, puis l'opérateur "le vainqueur prend tout" est utilisé pour attribuer une étiquette à l'échantillon [60]:

$$IF\ (\left\|x_k^i - x_N^i\right\| \leq r_N^{*i}\ ) \quad (15)$$

$$THEN(\ x_k^i \text{ is assingned to the nearest data cloud }\ )$$

4) Cartes logistiques: le comportement dynamique des systèmes non linéaires a suscité un intérêt pratique significatif dans de nombreuses applications en raison de leur simplicité et de leur richesse. Parmi ces systèmes, les systèmes chaotiques figurent parmi les plus importants. Ils se caractérisent par une extrême sensibilité aux conditions initiales, à la périodicité, au comportement pseudo-aléatoire et à une grande complexité. En effet, dans un système chaotique, la sensibilité aux conditions initiales est sans aucun doute la caractéristique essentielle du comportement chaotique, rendant imprévisible l'évolution à long terme. De tels systèmes sont très sensibles à la moindre perturbation de l'état initial. Un système chaotique en temps discret est défini par l'équation suivante :

$$x_{n+1} = \Gamma(x_n)\ ,\quad n = 0,1,2\ \ldots \quad (16)$$

Où $x_n \in R^n$ est appelé état, et Γ trace l'état suivant x_{n+1}. A partir d'un état initial x_0, l'application répétée de cette fonction (Γ) provoque une séquence de N points ($\{x_n\}_{n=0}^{N}$) appelée orbite du système à temps discret.

Sans aucun doute, ces systèmes ont été utilisés avec succès dans des applications de sécurité de l'information, pour la génération de clés secrètes dynamiques dans des algorithmes de cryptage, de stéganographie et de tatouage numérique.Les cartes chaotiques sont l'un des systèmes les plus simples à utiliser pour générer une séquence chaotique.Dans notre proposition, nous avons utilisé plusieurs cartes logistiques 1D, chacune étant définie par :

$$\mathcal{L}_i^c(x_0, \mu_i): \qquad x_{n+1} = \mu_i \cdot x_n(1 - x_n) \quad (17)$$

Où $x_n \in [0,\ 1]$ désigne l'état initial du système et $\mu_i \in [3.57,\ 4]$ est le paramètre de contrôle. Dans de tels systèmes, x_n et μ_i peuvent être utilisés comme clé secrète de cryptographie.

5) Transformation sinus : Comme toutes les méthodes de chiffrement, cette technique permet de chiffrer l'image en utilisant une clé secrète. Nous allons d'abord introduire quelques notations qui seront utilisées dans cette section.

$\mathcal{V}_o$: Un vecteur de caractéristiques biométriques extraites de la modalité biométrique.

$$\mathcal{V}_o = [x_1, x_2, x_3, \cdots, x_n] \quad (18)$$

$\mathcal{Y}_o$: Un vecteur transformé après transformation sinusoïdale appliquée sur $\mathcal{V}_o$.

$$\mathcal{Y}_o = [y_1, y_2, y_3, \cdots, y_n] \quad (19)$$

$\mathcal{E}_o$: Un vecteur aléatoire, dans lequel e_1 est choisi aléatoirement entre [−1, 1].

$$\mathcal{E}_o = [e_1, e_2, e, \cdots, e_n] \quad (20)$$

$\mathcal{P}$: une chaîne de nombre de période dans les éléments de $\mathcal{V}_o$.

$$\mathcal{P} = p_1, p_2, p_3, \cdots, p_n \quad (21)$$

Ce processus fonctionne en deux étapes : Extraction de la période et la transformation.

Extraction de la période: Puisque nous utilisons la fonction sinus qui est périodique avec la période de 2π, nous devons savoir à quelle période $x_i$appartient. Pour chaque x_i de $\mathcal{V}_o$, on a

$$x_i = \alpha_i + p_i \cdot 2\pi \quad (22)$$

Par conséquent, nous calculons p_i par l'équation suivante :

$$p_i = \left\lfloor \frac{x_i}{2\pi} \right\rfloor \quad (23)$$

Où p_i est le nombre de période de x_i. Après cela, toutes les données de période p_i du vecteur de caractéristique $\mathcal{V}_o$ sont stockées dans la base de données pour une vérification ultérieure.

Transformation: Lorsque l'étape d'extraction de caractéristiques est terminée, le vecteur de caractéristiques $\mathcal{V}_o$ d'un utilisateur sera transformé en vecteur $\mathcal{Y}_o$. Pour chaque élément x_i dans $\mathcal{V}_o$

$$\sin(x_i + y_i) = e_i \quad (24)$$

Ainsi, nous pouvons écrire $y_i = f(x_i)$ comme suit :

$$y_i = \arcsin(e_i) - \alpha_i \quad (25)$$

Parce que $\arcsin(e_i) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ et $\alpha_i \in [0, 2\pi]$, donc la valeur de $y_i$est comprise entre $[-\frac{5\pi}{2}, \frac{\pi}{2}]$. La figure ci-contre (Fig. III.3) illustre bien l'opération de transformation.

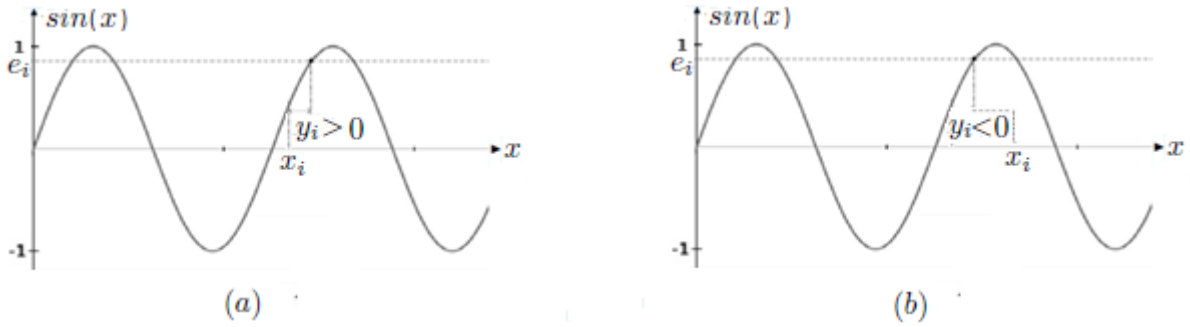

Fig. II.3 Cryptage basée sur la transformation sinus *(a)* Transformation sinus avec$y_i > 0$, et *(b)*Transformation sinus avec$y_i < 0$

En raison de la propriété périodique du sinus, pour chaque valeur de x_i, nous trouverons exactement une valeur y_i. Cependant, étant donné une valeur de yi, nous ne pouvons pas dériver exactement x_i, car il existe de nombreuses valeurs correspondant à ce y_i. En d'autres termes, cette fonction de transformation est non inversible. On peut aussi choisir une autre fonction périodique ayant la même caractéristique avec la fonction sinus (comme la fonction cosinus)[64].

II.4Conclusion

Le cryptage des données biométriques est un élément essentiel de la protection de la vie privée des utilisateurs dans le paysage numérique actuel. En mettant en œuvre des algorithmes de chiffrement puissants, en gérant les clés en toute sécurité, en utilisant l'authentification à deux facteurs et en restant vigilantes grâce à une surveillance continue, les organisations peuvent accroître la sécurité des données, instaurer la confiance et se conformer aux exigences légales et réglementaires. En donnant la priorité à la confidentialité des utilisateurs, les entreprises peuvent améliorer leurs processus d'intégration numérique et sécuriser les relations avec leurs clients.

Chapitre 3

Résultats Expérimentaux

Résumé

Les technologies biométriques sont de plus en plus employées dans diverses applications en raison de leur impact significatif sur le niveau de sécurité des systèmes d'information. Dans ce chapitre, nous présenterons les résultats de nos expérimentations sur une base de données typique d'empreintes des articulations des doigts. Ces résultats démontrent l'efficacité de notre proposition, comparable à plusieurs travaux de l'état de l'art. En présentant les performances et l'efficacité de notre cryptosystème biométrique, nous visons à fournir des informations précieuses sur ses applications potentielles et ses implications pour renforcer les niveaux de sécurité dans divers domaines.

Introduction

Ces dernières années, les applications électroniques émergentes ont joué un rôle essentiel dans la croissance rapide et continue du développement dans de nombreux pays à travers le monde. Des applications électroniques fiables doivent garantir la sécurité des informations partagées, ce qui devient de plus en plus courant et pose de nouveaux défis pour toutes les applications. Les informations échangées sont généralement sensibles et doivent être protégées. De plus, l'identité des utilisateurs qui transmettent ces informations doit être authentifiée avec précision par le destinataire. En effet, l'utilisation de cryptosystèmes biométriques est un moyen simple de répondre à ces exigences. Dans ce chapitre, nous nous concentrons sur la performance de notre système biométrique proposé, basé sur l'empreinte des articulations des doigts, ainsi que sur le niveau de sécurité qu'il atteint. Les expériences menées, basées sur une base de données biométrique récente, démontrent que notre méthode est plus efficace que plusieurs méthodes existantes.

III.1Base d'images utilisée

Pour évaluer la performance du système d'identification biométrique proposé, nous avons utilisé une base de données d'empreintes d'articulations des doigts créée par l'Université Polytechnique de Hong Kong (PolyU) [63]. Les images de cette base de données ont été capturées à l'aide d'un dispositif conçu au sein de PolyU. La base de données PolyU-FKP contient 165 personnes, dont 125 hommes. Parmi ces personnes, 143 ont un âge compris entre 20 et 30 ans, et les autres ont entre 30 et 50 ans. Les images de chaque doigt sont capturées en deux sessions, avec un intervalle de 25 jours entre les deux sessions. Six images de chaque doigt ont été collectées. Quatre doigts de chaque personne sont capturés : l'index gauche (Left Index Finger - LIF), l'index droit (Right Index Finger - RIF), le majeur gauche (Left Middle Finger - LMF) et le majeur droit (Right Middle Finger - RMF). Par conséquent, 48 images des

quatre doigts sont collectées pour chaque personne. La base de données finale rassemble un total de 7920 images en niveaux de gris des doigts, gauche et droit. La figure III.1 illustre quelques exemples d'images de cette base de données.

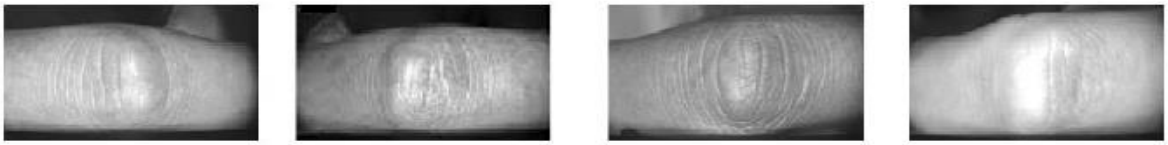

Fig. III.1 Quelques images de la base de données PolyU-FKP.

III.2Protocole d'évaluation

Dans ce travail, nous nous concentrons spécifiquement sur la tâche d'identification. Notre système, développé en mode ensemble ouvert et fermé, peut également être utilisé pour la vérification. Pour l'expérimentation réalisée dans cette phase d'identification, nous avons utilisé une base de données contenant 165 personnes (12 images par personne). Quatre images par personne, soit 660 images, sont utilisées pour construire la base de données de référence, tandis que les 1320 images restantes servent à tester les performances des systèmes proposés. Ainsi, la distribution des imposteurs et des clients est générée par 108240 et 1320 comparaisons, respectivement.

III.2.1 Méthodologie des tests

Les résultats expérimentaux présentés dans ce mémoire sont divisés en deux grandes parties. Tout d'abord, nous donnerons les résultats expérimentaux obtenus concernant l'évaluation des performances des systèmes biométriques (les performances du système biométrique ont été évaluées en mode ensemble ouvert et ensemble fermé). Cette partie est également subdivisée en deux sous-parties, l'une pour les systèmes biométriques unimodaux et l'autre pour les systèmes biométriques multimodaux. Ensuite, la deuxième partie sera consacrée à la robustesse du système de cryptage.

III.2.2 Mesure de performance

L'évaluation des performances d'un système est une étape cruciale dans sa conception et sa mise en œuvre, car elle permet de déterminer si le système est suffisamment performant pour l'application visée. Ces performances peuvent être principalement mesurées à l'aide de plusieurs métriques et visualisées à l'aide de diverses courbes de performance.

Du point de vue de la précision, qui est le critère le plus important pour évaluer la performance d'un système biométrique, deux taux d'erreur sont généralement calculés : le

taux de faux rejets (False Rejection Rate - FRR) et le taux de fausses acceptations (False Acceptance Rate - FAR). Le choix d'un seuil de décision T_0 joue un rôle crucial dans le calcul de ces erreurs. Ce seuil peut être défini selon différents critères : soit pour minimiser la moyenne des FAR et FRR, soit pour garantir que l'un des deux taux soit inférieur à un certain niveau désiré (voir Fig. III.2).

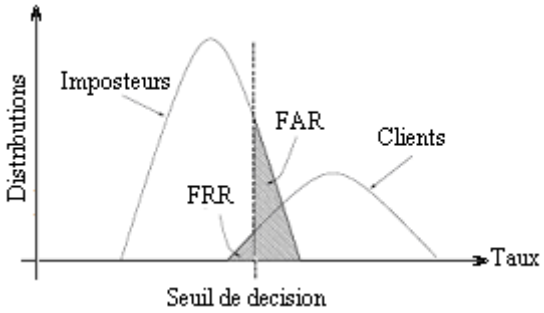

Fig. III.2 Distributions des taux (clients et imposteurs)

1) Métriques d'évaluation : Les métriques d'évaluation d'un système biométrique varient en fonction de son mode opérationnel, qu'il s'agisse d'un mode d'identification en ensemble ouvert ou mode d'identification en ensemble fermé.

☑ **Mode d'identification ensemble ouvert:** Idéalement, le système d'identification ensemble ouvert devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Soit :T_o : Seuil de décision ; N_C : Nombre d'accès client ; N_I : Nombre d'accès imposteur ;

$NFR(T_o)$: Nombre de faux rejets au seuil T_o et $NFA(T_o)$: Nombre de fausses acceptations au seuil T_o. Les FAR et le FRR sont définis comme suit :

- **Taux de faux rejet (False Reject Rate - FRR) :**Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système. Il est exprimé par la relation suivante :

$$FRR(T_O)[\%] = \frac{NFR(T_O)}{NC} \quad (1)$$

- **Taux de fausse acceptation (False Acceptance Rate - FAR) :** Ce taux représente le pourcentage de personnes qui ne devraient pas être reconnues mais qui sont tout de même acceptées par le système. Il est exprimé par la relation suivante :

$$FAR(T_O) = \frac{NFA(T_O)}{NI} \quad (2)$$

- **Taux d'égale erreur (Equal Error Rate - EER) :** Dans les cas d'un système qui fonctionne en mode vérification ou identification ensemble ouvert, le choix du seuil de

décision T_o est important car il influe directement sur les performances du système. Pour les applications, nous devons fixer T_o avec lequel les décisions d'acceptation ou de rejet de l'utilisateur seront prises. Cela correspond donc à choisir un point de fonctionnement du système. Le point de fonctionnement le plus utilisé est le taux d'équivalence des erreurs (Equal Error Rate-EER). Ce point de fonctionnement correspond au seuil qui donne des taux FAR et FRR égaux, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

$$EER(T_o) = FAR(T_o) = FRR(T_o) \quad (3)$$

Il est important de noter que les deux taux d'erreurs, mentionnés précédemment, sont utilisés dans les deux modes opératoires : vérification et identification ensemble ouvert.

☑ **Mode d'identification ensemble fermé:** Dans le cas de l'identification en mode ensemble fermé, les critères mentionnés ci-dessus ne peuvent pas être utilisés car tous les utilisateurs du système sont des clients. Il est donc plus approprié d'utiliser d'autres critères :
Soit :ρ représente le rang (ρ ∈ [1..N], *N* représente le nombre de personnes dans la base des données et N_{cr} est le nombre de clients rejetés par le système.

- **Taux de reconnaissance au rang un (Rank One Recognition-ROR) :** Dans le cas de l'identification en mode ensemble fermé, nous utilisons le taux de reconnaissance au rang un ou tout simplement taux d'identification. Ce taux donne le pourcentage de personnes reconnues par le système biométrique en fonction d'une variableρ.

$$ROR(\rho)|_{\rho=1} = 100 - \frac{N_{cr}}{N} \quad (4)$$

Le ROR représente le rapport entre le nombre de modèles correctement retrouvés par le système dans la base de données et le nombre total de modèles.

- **Rang de reconnaissance parfaite (Rank of Perfect Recognition-RPR):** Il existe une autre métrique qui joue un rôle important surtout concernant la comparaison des systèmes biométriques ce le rang de reconnaissance parfaite. Ce métrique représente le rang,ρ_n, dans le cas ou ROR = 100%.

$$ROR(\rho)|_{\rho=\rho_n} = 100\% \quad (6)$$

Nous disons qu'un système reconnait au rang ρ_n, lorsqu'il choisit, parmi ρ_n images, celle qui correspond le mieux à l'image du test. Nous pouvons donc dire que plus *RPR* augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible.

2) Courbes de performance : Les courbes de performance permettent de représenter les performances pour toutes les valeurs du seuil. Les courbes de performance d'un système biométrique varient en fonction de son mode opérationnel, qu'il s'agisse d'un mode d'identification en ensemble ouvert ou mode d'identification en ensemble fermé.

☑ **Mode d'identification ensemble ouvert:** Dans le cas de l'identification en mode ensemble ouvert, la courbe de performance les plus utilisées est :

- **Courbe de variation du FRR en fonction de FAR lorsque le seuil varie:** Cette courbe, appelée Receiver Operating Characteristic-ROC, permet de représenter graphiquement les performances d'un système de vérification ou d'identification ensemble ouvert pour les différentes valeurs de seuil T_o. L'allure de cette courbe est illustrée par la figure III.3.

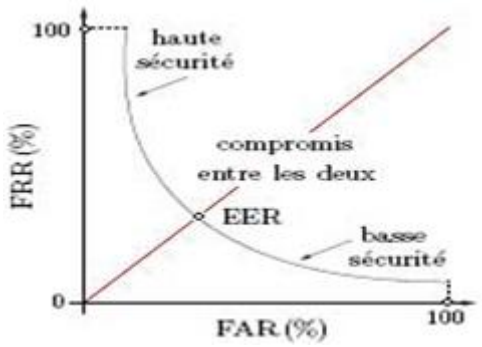

Fig. III.3 Courbe ROC (en respectant le FRR)

☑ **Mode d'identification ensemble fermé:** Dans le cas de l'identification en mode ensemble fermé, la courbe de performance les plus utilisées est :

- **Courbe des scores cumulés:** En mode d'identification ensemble fermé, le ROR est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les ρ_n premières réponses. Nous traçons alors la courbe des scores cumulés (Cumulative Match Characteristics-CMC) qui représente la probabilité que le bon choix se trouve parmi les premières réponses, comme l'illustre la figure III.4 [62].

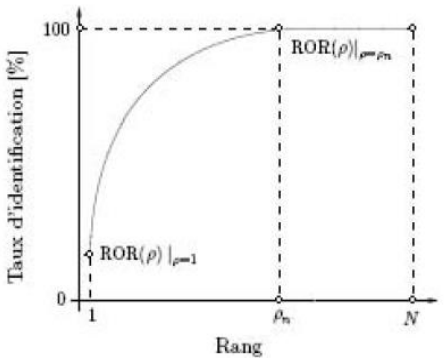

Fig. III.4 Courbe des scores cumulés (CMC).

III.3 Evaluation des performances

L'évaluation des performances d'un système est en effet cruciale dans sa conception et sa mise en œuvre, permettant de garantir son adéquation à l'application envisagée. Cette section se divise en deux parties principales : la première partie comprend des expériences préliminaires pour évaluer les performances du système biométrique, tandis que la seconde partie se concentre sur l'évaluation des performances de l'algorithme de cryptage.

III.3.1 Performances des systèmes biométriques

Les résultats expérimentaux présentés dans cette partie sont divisés en deux sous-parties. Tout d'abord, nous discuterons des résultats obtenus par rapport à différents systèmes d'identification biométrique afin de choisir les paramètres optimaux pour les deux méthodes d'extraction de caractéristiques utilisées, qui fournissent un taux d'identification élevé. La deuxième partie des résultats portera spécifiquement sur la fusion multimodale (systèmes multimodaux), exploitant les meilleurs paramètres choisis dans la première partie.

1) Résultats des tests préliminaires: En raison de l'impact significatif de la représentation des caractéristiques de l'image sur le taux d'identification du système et de la dépendance des deux méthodes d'extraction de caractéristiques (HOG et BSIF) sur des paramètres importants, nous avons réalisé un test empirique pour identifier les paramètres optimaux susceptibles d'améliorer la précision globale du système et d'optimiser ses performances. Ainsi, dans ces tests préliminaires, nous avons tenté de sélectionner le nombre de zones dans le HOG (w_h) et la taille ainsi que le nombre de filtres de convolution de BSIF (η, w_b) à partir des ensembles de valeurs suivants : $w_h = \{2, 4, 6, 8, 10, 12\}$ et $w_b = \{11 \times 11, 13 \times 13, 15 \times 15, 17 \times 17\}$, et $\eta = \{6, 8, 10, 12\}$, respectivement.Par conséquent, afin d'observer l'impact des paramètres (pour HOG et BSIF) sur les performances du système biométrique, nous présentons clairement les résultats du système d'identification ouvert (exprimés en termes de taux d'erreur égal (EER)) dans les Fig. III.5 et III.6, respectivement pour les systèmes biométriques basés sur le HOG et sur le BSIF.

Le système utilise quatre échantillons FKP (LIF, LMF, RIF et RMF) pour l'évaluation. Ainsi, à partir de ces figures et pour le mode d'identification ensemble ouvert, nous pouvons clairement voir qu'une performance excellente et très acceptable peut être obtenue en utilisant tous les paramètres possibles de HOG et BSIF, comme en montrer la valeur de EER la plus élevée qui est déjà inférieure à 3,00% (Fig. III.5). De plus, dans le système basé sur HOG, des tailles de fenêtre plus grandes entraînent généralement des valeurs EER plus faibles pour tous

les doigts ((T_o, EER) = {LIF : (0,879, 0,279%), LMF : (0,858, 0,481%), RIF : (0,863, 0,225%), RMF : (0,859, 0,381%)} pour $w_h = 10$ qui indique 100 zones HOG).

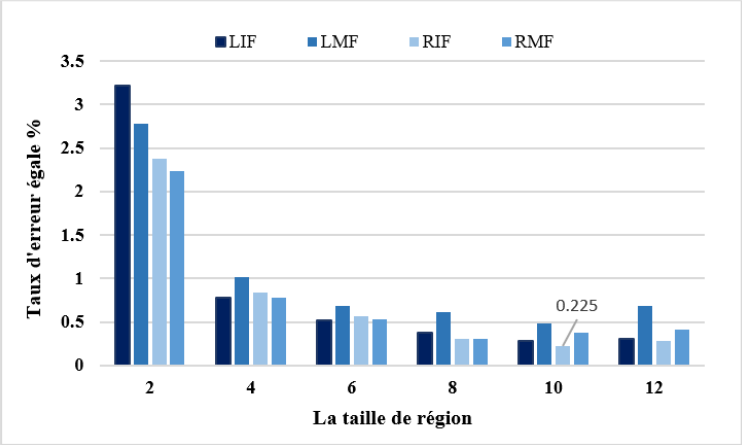

Fig III.5 Performance de système biométrique basé sur la technique HOG (ensemble ouvert)

Il est à noter que pour la technique BSIF et afin de limiter le nombre de tests, nous avons utilisé uniquement la modalité LIF pour choisir les paramètres optimaux de BSIF. De même, dans le système basé sur BSIF, un nombre accru de filtres de convolution tend à produire des valeurs EER plus faibles ((T_o, EER) = (0,838, 0,151 %) pour 12 filtres de taille 15x15), tandis qu'un nombre réduit de filtres entraîne des valeurs EER plus élevées ((T_o, EER) = (0,927, 1,765%) pour 6 filtres de taille 15x15), voir Fig. III.6. D'après ces expériences, on peut facilement conclure que l'utilisation de la technique HOG plutôt que la technique BSIF peut efficacement améliorer les performances du système.

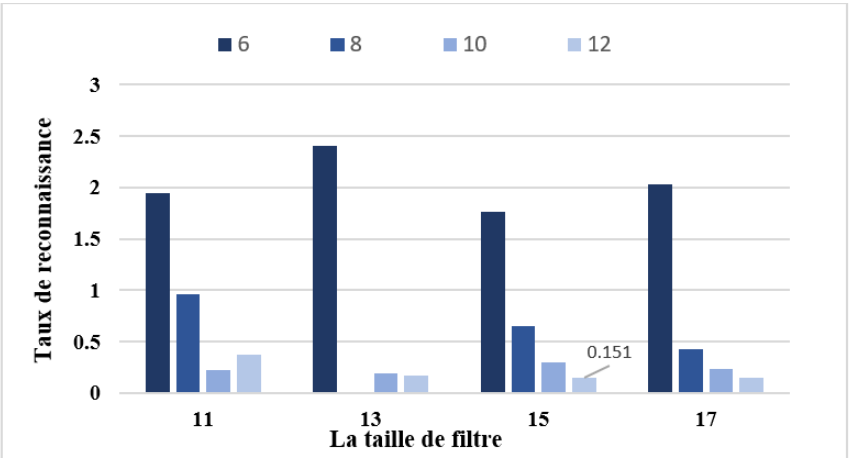

Fig III.6 Performance de système biométrique basé sur la technique BSIF (ensemble ouvert)

Nous avons également testé les performances des deux techniques dans un système d'identification opérant en mode ensemble fermé. La figure III.7 montre une comparaison entre les performances de toutes les nombres possible de zonez (w_h). D'après cette figure, avec un nombre de zones égal à 144 ($w_h = 12$), le système biométrique fonctionne avec un

taux de reconnaissance (ROR) de 98,560 %, 97,803 %, 98,484 %, et 98,333 % et des rangs de reconnaissance parfaite (RPR) égaux à 39, 65, 62, et 27, respectivement pour les modalités biométriques LIF, LMF, RIF et RMF.

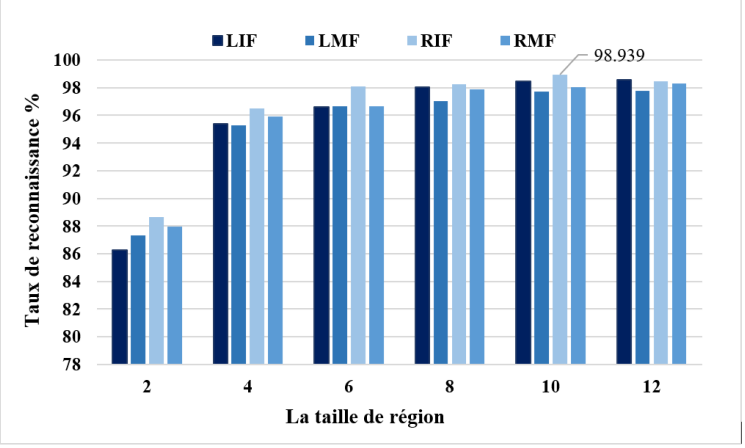

Fig III.7 Performance de système biométrique basé sur la technique HOG (ensemble fermé).

On constate sur cette figure que, pour la modalité LIF, le système donne le meilleur résultat avec un ROR égal à 98,560 % et un RPR égal à 39.

Pour le système biométrique en mode d'identification ensemble fermé, après avoir sélectionné les paramètres optimaux de BSIF (12 filtres de taille 15×15) et réexaminé tous les doigts, les résultats obtenus sont présentés dans la Fig III.8.

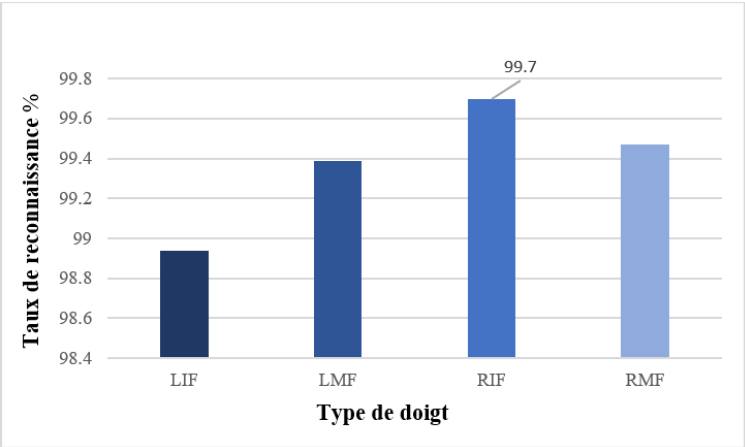

Fig III.8 Performance de système biométrique basé sur la technique BSIF (ensemble fermé).

Selon cette figure, le système biométrique fonctionne en mode d'identification ensemble fermé, basé sur n'importe quel doigt, avec une excellente efficacité, montrant un taux de reconnaissance supérieur à 98%. Cela démontre l'efficacité de la méthode d'extraction de caractéristiques basée sur BSIF. Dans ce mode, le système fonctionne avec un taux de reconnaissance (ROR) et un rang de reconnaissance parfait (RPR) de {(98.94%, 31), (99.39%,

16), (99.70%, 90) et (99.47%, 12)} pour respectivement, LIF, LMF, RIF et RMF. Après avoir sélectionné les paramètres optimaux pour les deux méthodes d'extraction de caractéristiques (HOG et BSIF), les deux sous-parties suivantes viseront à clarifier les performances des systèmes biométriques unimodaux et multimodaux.

2) Systèmes unimodaux : Le but de l'expérience dans cette partie était d'évaluer les performances du système d'identification biométrique unimodal en mode ensemble ouvert et fermé en utilisant les informations de chaque modalité (LIF, LMF, RIF et RMF). Pour ce faire, nous avons évalué les performances des quatre sous-systèmes d'identification biométriques unimodaux pour chaque méthode d'extraction de caractéristiques. Pour le système d'identification biométrique basé sur HOG, le Tableau III.1 compare les performances du système d'identification biométrique pour différentes modalités FKP.

Table III. 1 Performance de system biométrique unimodal basé sur la technique HOG

	ENSEMBLE OUVERT		ENSEMBLE FERME		Exécution	
	T_o	EER	ROR	RPR	Temps (s)	Taille de vecteur
LIF	**0.879**	**0.279**	**98.560**	**39**	0.024	900
LMF	0.858	0.481	97.803	65	0.025	
RIF	0.863	0.225	98.484	62	0.025	
RMF	0.859	0.381	98.333	27	0.024	

Les résultats expérimentaux dans ce tableau indiquent que la modalité LIF est plus performante que les autres modalités en termes d'EER et de ROR. Par conséquent, le temps de traitement est d'environ 0,025 s avec une longueur de vecteur de caractéristiques biométriques de 900 composants. Ce temps de traitement ainsi que cette longueur de vecteur conviennent à un système biométrique très rapide et léger.

Dans le cas du système d'identification biométriques basé sur BSIF, le Tableau III.2 présente une comparaison des performances du système avec différentes modalités FKP.

Table III. 2 Performance de system biométrique unimodal basé sur la technique BSIF

	ENSEMBLE OUVERT		ENSEMBLE FERME		Exécution	
	T_o	EER	ROR	RPR	Temps (s)	Taille de vecteur
LIF	0.838	0.151	98.94	31	0.211	4096
LMF	0.847	0.378	99.39	16	0.213	
RIF	0.857	0.171	99.70	90	0.213	
RMF	**0.845**	**0.151**	**99.47**	**12**	0.211	

Les résultats expérimentaux de ce tableau montrent clairement que la modalité RMF surpasse toutes les autres en termes d'EER et de ROR, conduisant à une amélioration remarquable de 45,89 % lorsque BSIF est utilisé à la place de HOG. Dans cette configuration, le temps de traitement était d'environ 0,213 s avec une longueur de vecteur de caractéristiques biométriques de 4096 composants. Ce temps de traitement, ainsi que la longueur du vecteur, sont supérieurs à ceux de la technique basée sur HOG. Cependant, compte tenu du taux d'erreur et du taux d'identification, ces valeurs sont acceptables pour les systèmes d'identification biométrique recommandés pour les applications de haute sécurité.

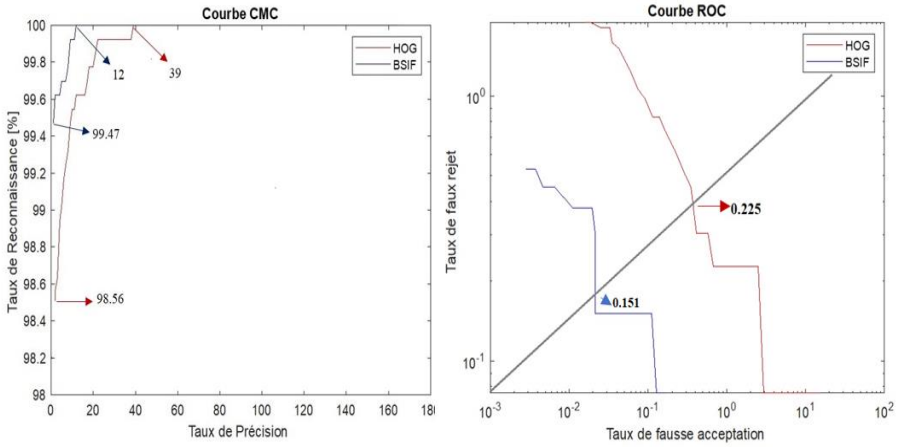

Fig III.9 Comparaison entre les performances de deux systèmes biométriques basé sur les techniques HOG et Bsif (ensemble ouvert et fermé)

Cette figure compare les performances de deux systèmes biométriques basés sur les techniques HOG et BSIF. Les paramètres optimaux pour chaque technique (voir **Table III. 1**et**Table III. 2**)ont été déterminés séparément dans les ensembles fermés et ouverts.Dans l'ensemble ouvert la méthode BSIF a obtenu un meilleur résultat avec un taux d'erreur égal (EER) de 0,151% et un seuil optimal (To) de 0,838,et la méthode HOG a obtenu un EER de 0,225% et un To de 0,863.Nous avons constaté dans l'ensemble fermé un résultat d'un taux de reconnaissance (ROR) de 99,47% et un rang de reconnaissance parfaite (RPR) de 12 pour la technique BESIF et un ROR de 98,560% et un RPR de 39 pour la technique HOG, Cela démontre l'efficacité de la technique BSIF pour l'obtention de meilleurs résultats.

3) Systèmes multimodaux : Bien que le système biométrique unimodal développé donne un résultat utile, il n'exclut pas la possibilité d'accepter une personne non autorisée ou de

refuser une personne autorisée en raison, par exemple, de la présence de bruit dans le capteur biométrique. Heureusement, la biométrie multimodale peut réduire les erreurs de reconnaissance et améliorer ainsi l'efficacité du système.

Dans nos résultats précédents, la technique HOG a montré d'excellents résultats en termes de temps de traitement et de longueur des vecteurs de caractéristiques. C'est pourquoi nous avons fusionné les résultats obtenus de tous les doigts au niveau des scores afin d'améliorer les performances du système. Dans la biométrie, la fusion au niveau des scores est considérée comme un niveau de fusion efficace en raison de sa simplicité et des résultats prometteurs obtenus, ce qui en fait le niveau le plus utile en biométrie multimodale. Avec cette technique, les différents systèmes biométriques unimodaux fonctionnent indépendamment, puis leurs résultats sont combinés pour obtenir un score scalaire utilisé pour la prise de décision. De nombreuses techniques existent pour combiner les scores obtenus à partir de sous-systèmes biométriques, mais la méthode la plus efficace est connue sous le nom de méthode basée sur des règles. Dans notre schéma de fusion, nous utilisons quatre règles simples et efficaces : la somme des scores (SUM), le score minimum (MIN), le score maximum (MAX) et la multiplication des scores (MUL).

Dans le Tableau III.3, nous présentons une comparaison des performances de tous les systèmes d'identification multimodaux en mode ensemble ouvert pour tous les types de doigts. Les résultats soulignent les avantages de l'utilisation du système multimodal avec fusion au niveau de scores correspondants. Selon les résultats du Tableau III.3, notre système d'identification montre des améliorations significatives allant jusqu'à 100,00 % pour plusieurs combinaisons, ce qui démontre les avantages remarquables de l'approche multimodale pour améliorer les performances du système biométrique.

Table III. 3 System biométrique multimodal basé sur la technique HOG (ensemble ouvert)

Règle	**SUM**		**MUL**		**MAX**		**MIN**	
Combinaison	**T_0**	**EER**	**T_0**	**EER**	**T_0**	**EER**	**T_0**	**EER**
LIF-LMF	**0.995**	**0.000**	**0.995**	**0.000**	0.954	0.008	0.856	0.318
LIF-RIF	**0.995**	**0.000**	0.99	0.002	**0.995**	**0.000**	0.861	0.207
RIF-RMF	0.893	0.018	0.884	0.020	0.963	3.651	0.852	0.227
LMF-RMF	0.870	0.052	0.861	0.057	0.862	0.059	0.858	0.331
ALL-FING	**0.837**	**0.000**	**0.890**	**0.000**	**0.969**	**0.000**	0.837	0.303

Cependant, le tableau met en évidence clairement les performances élevées de la fusion au niveau des scores. Pour confirmer sa supériorité par rapport aux autres systèmes unimodaux,

nous avons calculé le temps de traitement et la longueur du vecteur pour le multimodal, qui se sont révélés respectivement être de 0,05s et 1800, ce qui reste encore très efficace pour des applications de haute sécurité.

En ce qui concerne le système biométrique configuré en mode d'identification ensemble fermé, il est évident, d'après le Tableau III.4, que le système basé sur la combinaison LIF-RIF offre les meilleures performances (ROR = 100% et un RPR = 1), suivi par le système basé sur la combinaison ALL-FING (LIF-LMF-RIF-RMF).

Table III. 4 System biométrique multimodal basé sur la technique HOG (ensemble fermé)

Règle	**SUM**		**MUL**		**MAX**		**MIN**	
Combinaison	**ROR**	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**
LIF-LMF	99.92	2	99.92	3	99.85	2	98.86	59
LIF-RIF	**100.00**	**1**	99.92	2	**100.00**	**1**	99.39	46
RIF-RMF	99.92	2	99.92	2	99.92	3	98.79	41
LMF-RMF	99.7	25	99.70	25	99.39	28	98.33	71
ALL-FING	**100.00**	**1**	**100.00**	**1**	**100.00**	**1**	98.86	41

La plus grande amélioration des résultats (100%), par rapport au meilleur système biométrique unimodal basé sur la technique HOG et en utilisant le LIF, a été obtenue par les deux systèmes basés sur la combinaison LIF-RIF et la combinaison de tous les doigts (LIF-LMF-RIF-RMF).. Cependant, en tenant compte du temps de calcul de chaque système donné dans le Tableau III.3, le critère de choix du système peut être le compromis entre le taux d'identification et le temps de traitement. Il est à noter que tous ces résultats dépendent fortement de la taille de la base de données utilisée.

III.3.2 Performances de système de cryptage

L'objectif principal de notre système est de protéger les templates biométriques. Dans cette section, nous procéderons à une analyse de sécurité pour évaluer la robustesse de notre méthode face aux attaques potentielles. En général, pour garantir la sécurité, deux aspects de la conception du système doivent être vérifiés des critères. Le premier critère est l'impossibilité de retrouver les vecteurs biométriques par une recherche exhaustive, ce qui nécessite un espace de clés très large, tandis que le deuxième critère réside dans la production de vecteurs biométriques cryptés complètement différents lors de petites modifications de la clé secrète. Il convient de noter que notre cryptosystème biométrique fonctionne avec trois

systèmes chaotiques principaux (*logistic maps*: L_1, L_2 et L_3). En général, les paramètres qui contrôlent la sécurité de notre système sont les états initiaux de L_1, L_2 et L_3.

1) Espace clé cryptographique: L'espace de recherche des attaques est calculé en utilisant toutes les erreurs absolues moyennes entre deux séquences générées par deux clés secrètes adjacentes. L'erreur absolue moyenne pour le système chaotique est définie comme suit :

$$\mathcal{E}_\ell(\mathcal{S}, \tilde{\mathcal{S}}) = \frac{1}{\ell}\sum_{j=1}^{\ell}\left|S(j) - \tilde{S}(j)\right| \quad (7)$$

ℓ : le nombre de points dans les séquences générées.

$\mathcal{S}$(j) : le j^{ème} point de la première séquence générée par la clé secrète initiale.

$\tilde{\mathcal{S}}$(j) : le j^{ème} point de la deuxième séquence générée par la clé secrète voisine.

Cette métrique permet d'évaluer la dissemblance entre deux séquences produites par des clés secrètes très proches, assurant ainsi que même une légère variation dans la clé secrète entraîne des vecteurs biométriques totalement différents. Ce comportement est essentiel pour garantir la robustesse du cryptosystème contre les attaques par force brute, car il rend impraticable la prédiction ou la reconstruction des vecteurs biométriques à partir de clés proches.

En effet, soit $S^x, \tilde{S}^x, S^u, \tilde{S}^u$quatre séquences générées par le même système chaotique dans les conditions suivantes :

$$\begin{cases} S^x = \mathcal{L}_0^c(x_{01}, \mu) \\ \tilde{S}^x = \mathcal{L}_0^c(x_{01} + d, \mu) \end{cases} \begin{cases} S^\mu = \mathcal{L}_0^c(x_{01}, \mu) \\ \tilde{S}^\mu = \mathcal{L}_0^c(x_{01}, \mu + d) \end{cases} \quad (8)$$

Où d une très petite valeur. Ainsi, l'espace des clés pour x_0, appelés$_x$ qui vaut$1/d_x$, où d_x est la valeur de d pour laquelle$\mathcal{E}_\ell = 0$. La même chose pour l'espace des clés de μ qui appelés$_\mu$, il est égal à $1/d_\mu$, où d_u est la valeur de d pour laquelle $\mathcal{E}_\ell = 0$. Comme on a déjà mentionné, notre système utilise trois systèmes chaotiques principauxL_1, L_2 et L_3, ainsi, l'espace des clés total devient :

$$\mathcal{S}_p = s_x^1 \cdot s_u^1 \cdot s_x^2 \cdot s_u^2 \cdot s_x^3 \cdot s_u^3 \quad (9)$$

Pour tout système logistique, la valeur de $s_x$est égale à $1.201 \cdot 10^{16}$ et la valeur de $s_\mu$est égale à $0.751 \cdot 10^{16}$. Par conséquent, l'espace des clés total de notre schéma devient :

$$\mathcal{S}_p = (1.201)^3 \cdot 10^{48} \cdot (0.751)^3 \cdot 10^{48} = 0{,}73751 \cdot 10^{96} \quad (10)$$

Il est clair que notre système est très efficace car il donne un espace de clé plus important que de nombreuses méthodes de la littérature.

2) Sensibilité des clés: Dans cette section, nous avons analysé les vecteurs de caractéristiques cryptés de plusieurs clés secrètes proches pour évaluer la sensibilité de notre système à de légères variations de clé. Nous avons utilisé trois clés différentes : une clé correcte ($K_c^0 = [0.123, 3.754]$) et deux clés incorrectes proches de la clé correcte, avec des variations de $d_x = 10^{-16}(K_c^1)$ et $d_u = 10^{-16}$ (K_c^2). Pour évaluer les vecteurs de caractéristiques obtenus, nous avons calculé la corrélation entre ces vecteurs, définie comme suit :

$$\rho_c[\%] = 100 \cdot \frac{C_{ij}}{\sigma_i \sigma_j} \textit{(10)}$$

Où C_{ij} est la covariance entre deux vecteurs de caractéristiques, qui ont des écarts-types de σ_i et σ_j. De plus, pour une comparaison équitable, nous avons sélectionné aléatoirement deux personnes différentes (*i* et *j*) dans la base de données. Après avoir extrait le vecteur de caractéristiques de la première personne (*i*) en utilisant la clé correcte, nous avons extrait les vecteurs de caractéristiques des deux personnes (*i* et *j*) en utilisant toutes les clés. Ensuite, nous avons calculé la corrélation entre tous les vecteurs de caractéristiques obtenus. Les résultats sont présentés dans le Tableau III.5.

Tableau III.5 Corrélation entre les vecteurs caractéristiques produits par deux personnes

		Personne *i*			Personne *j*		
		K_c^0	K_c^1	K_c^2	K_c^0	K_c^1	K_c^2
Personne *i*	K_c^0	100.00	4. 320	5.110	18.321	3.101	2.412

De ce tableau, nous pouvons extraire deux remarques importantes :

- L'utilisation de la même clé (K_c^0) donne une corrélation totale pour la même personne. Cette corrélation devient quelque peu significative pour deux personnes différentes en raison de la similitude des traits biométriques de l'empreinte entre les deux personnes. Cependant, le système biométrique est toujours capable de différencier ces deux vecteurs de caractéristiques.
- Une légère modification d'un paramètre du système chaotique provoque une divergence notable entre les vecteurs de caractéristiques, que ce soit pour la même personne ou pour deux personnes différentes.

III.4 Conclusion

Les cryptosystèmes biométriques offrent plusieurs fonctionnalités, notamment l'identification à distance de l'identité d'un utilisateur, agissant ainsi comme un système de vérification multifacteur. De plus, ces systèmes cryptent les vecteurs de caractéristiques et les protègent contre le vol, la distorsion ou l'altération. Les tests effectués dans ce chapitre portaient à la fois sur la précision du système biométrique et sur son niveau de sécurité. En validant le système sur une base de données de 165 personnes, nous avons observé une amélioration considérable du taux d'identification, atteignant 100 % grâce à la fusion des systèmes basés sur la technique HOG. De plus, la méthode proposée a démontré un niveau de sécurité élevé (protection des vecteurs de caractéristiques), avec une robustesse dépassant 10^{96}.

Conclusion Générale

Conclusion générale

Avec le développement rapide de la technologie numérique et la transformation rapide des divers domaines vers la numérisation, en particulier dans des domaines sensibles tels que les institutions financières, la sécurité de l'information est devenue une nécessité pour gagner la confiance des clients, et pour atteindre une expansion rapide et des bénéfices accrus. En effet, les technologies biométriques, notamment avec les progrès des techniques d'intelligence artificielle, ont prouvé leur efficacité mais elles restent insuffisantes, surtout dans les applications de haut niveau de sécurité.

Le travail effectué dans cette mémoire vise à identifier automatiquement les individus en fonction de leurs descriptions vitalesles empreintes des articulations des doigts (ont été utilisées pour créer nos systèmes biométriques proposés, qu'ils soient monomodaux ou multimodaux. Après avoir exposé les concepts généraux de sécurité de l'information et de biométrie, nous avons exposé les dernières approches pour intégrer les modalités biométriques, en utilisant diverses techniques en niveaux de fusion. Nous avons également donné un aperçu des documents communs sur les empreintes digitales.

Le but principal consiste donc à élaborer un système biométrique pour assurer une identification fiable des individus. Les différentes technologies biométriques combinées permettent d'améliorer les performances du système d'identification. Toutefois, cette formation demeure vulnérable aux spécificités des méthodes utilisées. Ces trois critères sont employés afin d'évaluer l'efficacité d'un système biométrique spécifique,le taux d'identification, la taille de la base d’images et le temps de calcul sont des critères à prendre en compte. En choisissant avec prudence la méthode d'extraction, qui satisfaire à ces trois

critères.

Ce travail nous a permis de démontrer la faisabilité d'un système biométrique pour l'identification des individus à partir leurs caractéristiques physiques, comportementales ou biologiques. Parmi les méthodes couramment utilisées dans ce domaine figure l'utilisation de l'empreinte digitale à travers la base d'images FKP_ROI. Dans ce mémoire, nous avons comparé différentes méthodes d'extraction des caractéristiques, ce qui nous a permis de choisir celles qui conviennent le mieux à notre système. Nous avons ensuite opté pour les méthodes HOG et BSIF. Pour rendre notre système plus pratique, nous avons utilisé un classificateur moderne pour obtenir des résultats plus précis et fiables.Nous n'avons pas négligé la sécurité de l'information, notamment lors du partage ou de l'envoi, où nous avons employé une technologie efficace pour le chiffrer et le protéger.

En fin de compte, les résultats obtenus sont très prometteurs. En effet, nous avons atteint un taux de reconnaissance acceptable, ce qui rend notre système fiable et conforme aux objectifs initialement fixés, à savoir la mise en place d'un système permettant l'identification des individus et l'application d'une méthode efficace pour sécuriser la confidentialité des informations personnelles. Il est également important de noter que ce travail n'est pas limité à ces résultats, mais constitue une passerelle vers des modifications et des améliorations qui contribuent à l'avancement de la sécurité biométrique.

Glossaire

Les termes suivants, classés dans l'ordre alphabétique, sont utilisés dans le texte.

ADN	**:**	Acide Désoxyribo Nucléique(Nucleic Deoxyribo Acid).
ALMMO	**:**	Autonome Multi-Modèle d'Ordre Zéro (Autonomous Learning Multi-Model Classifier of 0-Order).
AnYa	**:**	Une méthodologie spécifique pour la modélisation et le contrôle flous.
BSIF	**:**	Caractéristiques d'image binarisées indépendantes (Binarized Statistical Image Features).
CCD	**:**	Dispositif à transfert de charge (Charge-Coupled Device).
CLM	**:**	Modèle Contraint Localement (Constrained Local Model).
CMC	**:**	Courbe de correspondance cumulative (Cumulative Match Curve).
DH76	**:**	l'algorithme de Diffie (Hellman, introduit en 1976).
EER	**:**	Taux d'erreurs égales (Equal Error Rate).
FAR	**:**	Taux de Fausses Acceptations (False Acceptance Rate).
FRR	**:**	Taux de Faux Rejets (False Reject Rate).
FRGC	**:**	Grand Défi de Reconnaissance Faciale (Face Recognition Grand Challenge).
HOG	**:**	Histogrammes de gradients orientés (Histograms of Oriented Gradients).
HSM	**:**	Module de Sécurité Matérielle (Hardware Security Module).
Info Sec	**:**	Sécurité de l'information (Information Security).
LIF	**:**	Index gauche (Left index finger).

LMF	**:**	Majeur gauche (Left middle finger).
MIT	**:**	Massachusetts Institute de Technologie(Massachusetts Institute of Technology).
PIN	**:**	Numéro d'Identification Personnel (Personal Identification Number).
RIF	**:**	Index droit (Right index finger).
RMF	**:**	Majeur droit (Right middle finger).
ROC	**:**	Courbe représentant les taux d'erreur (Receiver Operating Curve).
ROI	**:**	Région d'intérêt (Region Of Interest).
ROR	**:**	Taux de Reconnaissance (Rate of Recognition).
RPR	**:**	Taux de Précision et de Rappel (Rate of Precision and Recall).
USB	**:**	Bus Universel en Série (Universal Serial Bus).

Annexe A

A.1 Extraction de la région d'intérêt (ROI)

Les images biométriques brutes nécessitent un prétraitement pour en extraire une région d'intérêt (ROI), étape cruciale avant l'extraction des caractéristiques. La qualité de l'algorithme de détection des ROIs impacte directement la qualité globale du traitement de l'image. La capacité à détecter des ROIs similaires sur différentes images est essentielle pour garantir la fiabilité des systèmes biométriques. La signification des ROIs varie selon la modalité biométrique, qu'il s'agisse des zones oculaires ou labiales dans les images faciales, ou de l'iris dans les images oculaires. Ainsi, la méthode d'extraction est déterminée par la modalité biométrique utilisée.

A.2 Etapes d'extraction de ROI

L'empreinte de l'articulation du doigt présente des caractéristiques uniques à chaque individu. Elle reste invariable au fil du temps, facile à prélever, à numériser et à stocker. Après avoir établi le système de coordonnées, la partie centrale (ROI) est segmentée. Pour extraire la région d'intérêt (ROI) contenant les textures autour de l'articulation, nous utilisons un algorithme pour éliminer l'arrière-plan, réduisant ainsi la taille de l'image et améliorant la précision des résultats.

Etape 1 : Filtrage et sous-échantillonnage

La taille de chaque image de la base de données est de 768×576 pixels avec une résolution de 400 dpi. Il n'est pas nécessaire d'utiliser cette résolution pour l'extraction des caractéristiques, car une faible résolution peut bien représenter les lignes principales et secondaires autour de l'articulation. Par conséquent, l'image du doigt subit une opération de filtrage suivie d'une opération de sous-échantillonnage. L'objectif de l'opération de filtrage est de réduire le bruit dans l'image. Un filtre passe-bas (filtre gaussien) peut être appliqué pour réduire ce bruit et améliorer la qualité de l'image originale. L'opération de sous-échantillonnage permet de réduire la résolution de l'image jusqu'à 150 dpi. L'avantage de cette opération est de diminuer considérablement le coût de calcul en réduisant la quantité de données. Nous appelons ID l'image résultante. Le résultat de cette étape est illustré dans la figure.

Fig A.1 : Filtrage et sous- échantillonnage de l'image de doigt.

Etape 2 : Détermination de l'axe X

Une fois l'image de l'empreinte filtrée et sous-échantillonnée, l'algorithme détermine l'axe horizontal X en utilisant un détecteur de contours de type Canny, qui offre une bonne détection et localisation. La limite inférieure du doigt est extraite, car tous les doigts sont placés de manière uniforme lors de l'acquisition de l'image. Cette frontière est ajustée comme une ligne droite pour déterminer l'axe X. La figure suivante illustre cette procédure :

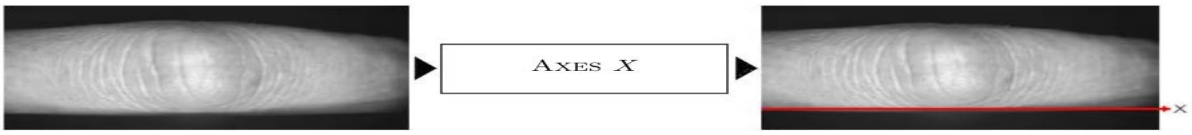

Fig A.2 : Détermination de l'axe X

Etape 3 : Extraction d'une sous-image

Les informations utiles qui peuvent être utilisées pour une identification biométrique ne réside que dans une partie de l'image du doigt. Par conséquent, nous avons d'abord coupé

Fig A.3 : Sous-image extraite avant l'extraction du ROI.

Nous avons extrait une sous-image, que nous appellerons IS, à partir de l'image originale. Les limites gauche et droite de IS sont déterminées empiriquement, tandis que les limites supérieure et inférieure sont estimées en fonction de la limite de vrais doigts. Un exemple de cette sous-image est illustré dans la figure suivante. Cette sous-image est utilisée pour calculer l'axe Y.

Etape 4 : Détection de contour

En appliquant le d´détecteur de contour de type CANNY a l'image IS, l'image des contours IE peut être obtenue. Voir la figure suivante pour un exemple.

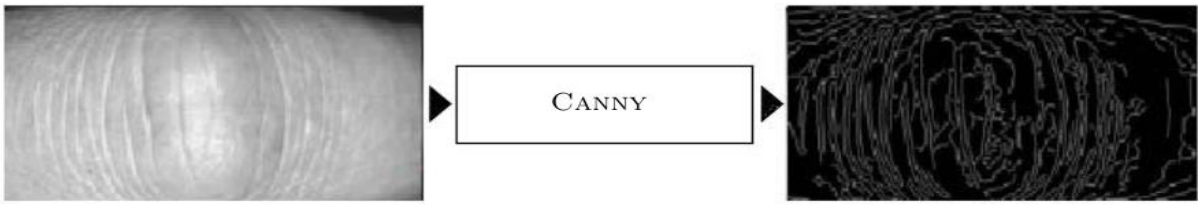

Fig A.4 : Image des contours obtenue.

Etape 5 : Codage des directions convexes

En se basant sur les caractéristiques des courbes des contours dans l'image IE, nous avons la possibilité de coder IE pour obtenir une image codée, ICD, qui illustre les directions convexes des courbes. À cette étape, chaque pixel dans IE a attribué un code représentant la direction locale (convexe) de ce pixel. En examinant les images de doigt, nous pouvons construire un modèle idéal des courbes dans l'image du doigt, tel qu'illustré dans la figure ci-dessous. Dans ce modèle, une courbe dans l'image est soit convexe vers la gauche :

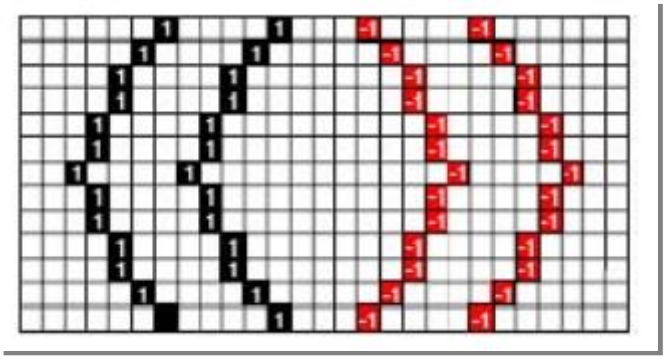

Fig A.5 : Courbes sur l'image de doigt.

Nous pouvons coder les pixels le long des courbes convexes, soit ceux qui sont convexes vers la gauche par "1", ceux convexes vers la droite par "-1", et les autres pixels (qui n'appartiennent pas à ces deux types de courbes) par "0". La figure précédente illustre les directions convexes dans ICD.

Etape 6 : Détermination de l'axe Y

Dans une image de doigt, la plupart des courbes du côté gauche de l'image sont dirigées vers la gauche, tandis que celles du côté droit sont dirigées vers la droite. Cependant, il n'y a pas

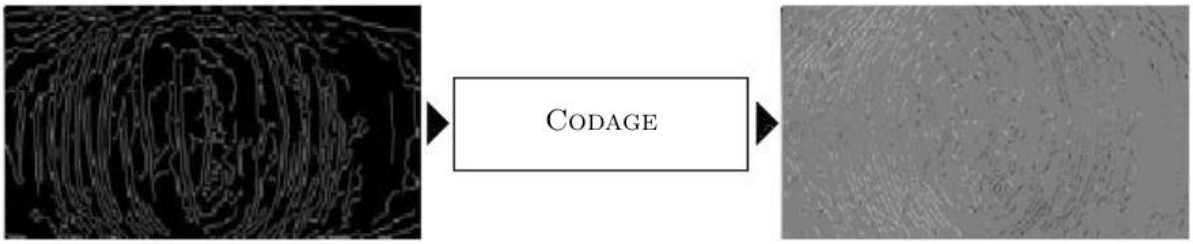

Fig A.6 : Image obtenue par l'application de codage de la direction convexe.

des directions convexes évidentes dans une petite zone autour de l'articulation. En tenant compte de cette observation, nous pouvons définir une mesure de convexité, notée %, comme suit :

$$\rho(x) = abs\left(\sum_{W} I_{CD}\right)$$

Où x est la position horizontale (représentant une colonne) de la fenêtre. W est une fenêtre symétrique par rapport à l'axe X = x. La fenêtre W est de taille d × h, avec h égale à la hauteur de l'image IS et d est choisi, dans notre travail, égal à 35. La grandeur %(x) peut atteindre son minimum autour du centre de l'articulation. La fenêtre doit parcourir un trajet qui part de la gauche et qui va balayer les différents x. L'axe Y est défini comme suit :

$$Y = \arg min_x\,[\rho(x)]$$

Cette position peut être utilisée pour définir l'axe Y. La figure suivante montre la position de l'axe Y dans l'image du doigt :

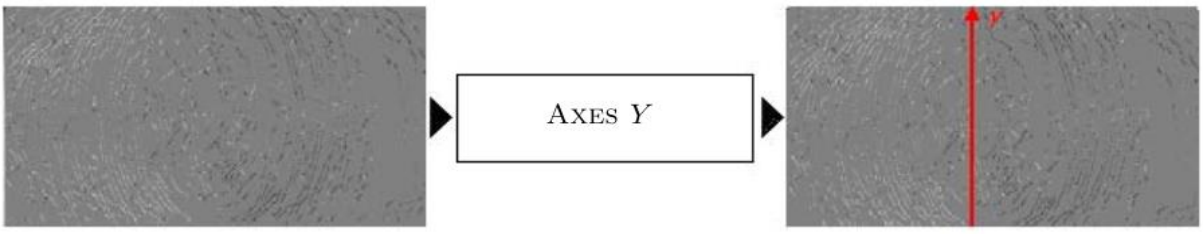

Fig A.7 : Détermination de l'axe Y.

Etape 7 : Détermination de l'axe Y

Une fois les axes X et Y localisés, nous pouvons déterminer une zone dans l'image ID, appelée IROI, qui représente la région d'intérêt. Comme le montre la figure suivante, le ROI, de taille fixe, peut être extraite à partir de l'image ID.

Fig A.8 : Localisation du ROI dans l'image de doigt.

Etape 8 : Extraction de ROI

Une région d'intérêt de l'empreinte est définie et découpée autour de l'axe Y (comme illustré dans la figure A.19). Ensuite, une région rectangulaire correspondant au ROI, avec des dimensions fixes de 110×220 pixels et contenant la majeure partie de l'empreinte, est extraite.

Fig A.9 : Extraction du ROI à partir l'image de doigt.

Après tout, nous pouvons constater que la méthode de localisation des axes X et Y, ainsi que la méthode d'extraction de la région d'intérêt (ROI), peuvent efficacement aligner les différentes images des doigts, en normalisant la zone soumise à différents traitements pour extraire les caractéristiques biométriques du doigt. Ces opérations réduisent considérablement les variations causées par les différentes positions des doigts dans le système d'acquisition [62].

Annexe B

La classification, comme méthode d'apprentissage supervisé, implique la construction d'une fonction mathématique pour déterminer si un échantillon de données appartient à un ensemble ou non. Les techniques de classification sont largement utilisées dans divers domaines tels que le traitement du langage naturel et le traitement d'images [64]. La logique floue est couramment employée dans ces tâches, avec différentes méthodes pour générer automatiquement des règles floues à partir des données. Le système d'Apprentissage Autonome à Modèles Multiples (ALMMo), introduit récemment dans le cadre de l'Analyse de Données Empiriques (EDA), extrait des données sans forme et forme automatiquement des règles linguistiques simples à partir des données observées empiriquement.

B.1 Les concepts de base

Le système ALMMo a été récemment introduit dans le cadre de l'EDA. Dans cette section, les concepts du système AnYa FRB de 0e ordre et de l'estimateur EDA seront brièvement rappelés :

B.1.1 Systèmes basés sur des règles floues AnYa de 0ème ordre

La structure d'un système ALMMo(0-Order AnYaFuzzy Rule-BasedSystems) est composée d'un ensemble de règles floues de type AnYa. Le système flou de type AnYa a été introduit par Angelov et Yager. Comparé aux deux systèmes de règles floues largement utilisés, à savoir le type Mamdani et le type Takagi-Sugeno, la partie antécédente de la règle floue AnYa est révisée et simplifiée en un vecteur, qui comprend les points focaux des nuages de données sur la figure 1, qui présente un schéma explicatif du classificateur multi-modèle sur lequel les règles sont construites. Le concept de nuage de données a également été introduit dans les références 10 et 11. Les nuages de données sont des ensembles d'échantillons de données partageant des propriétés communes regroupées autour des points focaux ressemblant à une tessellation de Voronoi. Dans AnYa, les nuages de données et les points focaux respectifs sont utilisés comme base de la partie antécédente (partie SI) de la règle floue. Une règle floue AnYa de degré 0 est exprimée comme suit :

$$Ri: x * i \rightarrow Label\ i \quad (1)$$

Oùx^{*i}est le point focal du i^{th} nuage de données ; $Label^i$ est l'étiquette correspondante. L'inférence dans la règle floue AnYa de 0e ordre peut être effectuée en suivant le principe bien connu du "vainqueur prend tout" lorsqu'il s'agit de classification.

B.1.2 Estimateur EDA

La densité unimodale du cadre EDA utilisé comme principal estimateur pour révéler les propriétés de l'ensemble des données observées de manière entièrement autonome.

Tout d'abord, considérons l'ensemble de données/flux dans l'espace de données euclidien R^d

Comme $\{x\} = \{x_1, x_2, x_3 \ldots\ldots, x_k\}$et les indices indiquent les instants auxquels les échantillons de données ont été observés. Dans cet article, la distance euclidienne est utilisée pour les dérivations mathématiques pour des raisons de simplicité, mais d'autres types de distances peuvent également être utilisés.

La densité unimodale de l'échantillon de données i^{th} au temps k^{th} est calculée comme suit :

$$D_k(x_i) = \frac{1}{1 + \frac{\|x_i - \mu_k\|^2}{\sigma_k^2}} = \frac{1}{1 + \frac{\|x_i - \mu_k\|^2}{X_k - \|\mu_k\|^2}} \qquad (2)$$

où$\mu_k$est la moyenne globale de tous les échantillons de données au k^{th} instant et $X_k$est le produit scalaire moyen ;est calculé comme$\sigma_k^i = X_k - \left\|\mu_k\right\|$, Il convient de noter que, en utilisant la distance euclidienne, la densité unimodale est sous forme d'une fonction de Cauchy dans sa nature, mais cela n'était pas une hypothèse préalable d'une distribution de Cauchy.

Pour le traitement de données en continu, le calcul récursif est très important pour améliorer l'efficacité en mémoire et en calcul. $\mu_k$et $X_k$peuvent être mis à jour de manière récursive comme suit :

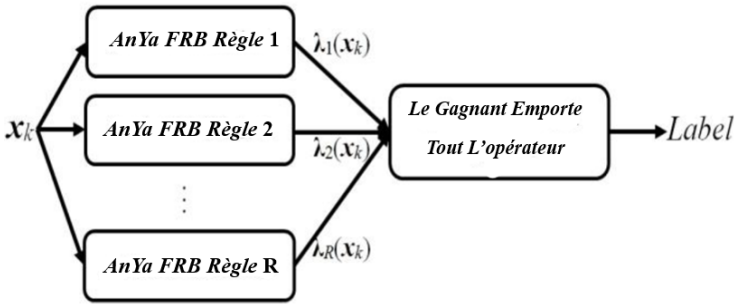

Fig B.1 : Un diagramme de cadre illustratif du classificateur multi-modèle

Les équations (3) et (4), ce qui permet de calculer la densité unimodale de manière récursive sans aucune boucle ni itération :

$$\mu_k = \frac{k-1}{k}\mu_{k_1} + \frac{1}{k}x_k;\ \ \mu_1 = \ x_1 \qquad (3)$$

$$x_k = \frac{k-1}{k}X_{k-1} + \frac{1}{K}\|x_k\|^2\ ;\ \ X_1 = \|x_1\|^2 \quad (4)$$

B.2 La structure du classificateurALMMO

Dans ce paragraphe, la structure du classificateur sera mise en évidence en décrivant ses trois étapes **:**

B.2.1Architecture à Modèles Multiples

L'architecture à modèles multiples repose sur des règles FRB où R ≥ C, C représentant les différentes classes. Chaque nouvelle donnée x_k est envoyée à tous les sous-classificateurs, qui génèrent chacun un score de confiance λ_i. La règle du "gagnant prend tout" assigne ensuite x_k à la classe la plus probable. Cette structure améliore la capacité du classificateur à gérer des problèmes complexes :

$$Label = \underset{i=1,2,\ldots\ldots R}{\arg\max}(\lambda_i) \qquad (5)$$

B.2.2Étape d'apprentissage

En raison de son architecture à modèles multiples, seules les règles FRB AnYa correspondant à la classe de l'échantillon de données nouvellement arrivé seront mises à jour. Chaque nouvel échantillon de données sera normalisé par sa norme,à savoir :

$$X \leftarrow \frac{X}{||X||} \qquad (6)$$

Supposons que le nouvel échantillon de données soit la k^{th} échantillon de la i^{th}classe, donc l'échantillon de données normalisé est désigné par x_k^iTout d'abord, la moyenne globale$\mu_{k_1}^i$ de la i^{th} classe est mise à jour en $\boldsymbol{x}_k^i$en utilisant l'équation (3). Il n'est plus nécessaire de mettre à jour le produit scalaire moyen car $X_k^i = ||x_k^i||^2 = 1$**,**puisque les données sont normalisées. Les densités unimodales de l'échantillon de données $\boldsymbol{x}_k^i$ et de tous les points focaux identifiés de lai^{th}classe, désignés par $\boldsymbol{x}_j^i$ (j $= 1, 2 \ldots\ldots F^i$), sont calculées en utilisant l'équation (2), où F^i est le nombre de points focaux.

Ensuite, le principe suivant (Condition 1) est vérifié pour voir si x_k^i générera une nouvelle règle/nuage de données :

$$IF\ (\ D_k(x_k^i) > \max_{j=1,2,\dots\dots F_i}(D_k(x_j^{*i})))$$
$$OR\ \left(D_k(x_k^i) < \min_{j=1,2,\dots\dots F_i}\left(D_k(x_j^{*i})\right)\right) \qquad (7)$$
$$THEN\ (x_k^i\ is\ a\ new\ focal\ point)$$

Si la Condition (1) est déclenchée, une nouvelle règle floue/nuage de données est formée autour de x_k^i et ses paramètres sont mis à jour comme suit :

$$\begin{cases} Fi \leftarrow Fi + 1 \\ x_{Fi}^{*i} \leftarrow x_k^i \\ M_{fi}^{*i} \leftarrow 1 \\ r_{fi}^{*i} \leftarrow r_0 \end{cases} \qquad (8)$$

Si la Condition 1 est remplie, une nouvelle règle floue/nuage de données est créée autour de x_k^iet ses paramètres sont mis à jour pour inclure le nombre de membres et le rayon de la zone d'influence. r_0 est utilisé pour stabiliser l'état initial des nouveaux nuages de données et empêche l'attraction d'échantillons trop éloignés. Si la Condition 1 n'est pas remplie, l'algorithme trouve le nuage de données le plus procèdex_k^i :

$$x_N^{*i} = \arg\min_{j=1,2,\dots\dots F^i}(\|x_k^i - x_j^{*i}\|) \qquad (9)$$

Où $x_N^{*\,i}$ représente le point focal du nuage de données le plus proche. Avant d'assigner x_k^i au nuage de données le plus proche, la Condition 2 est vérifiée pour déterminer si x_k^iest suffisamment proche du nuage de données :

$$IF\ (\|x_k^i - x_N^i\| \leq r_N^{*i}\ ) \qquad (10)$$
$$THEN(\ x_k^i\ \text{is assingned to the nearest data cloud}\ )$$

Si la Condition 2 est satisfaite, les méta-paramètres de la règle floue/nuage de données le plus proche sont mis à jour comme suit :

$$\begin{cases} x_N^{*i} \leftarrow \dfrac{M_N^{*i}}{M_N^{*i}+1} x_N^{*i} + \dfrac{1}{M_N^{*i}+1} x_k^i \\ M_N^{*i} \leftarrow M_N^{*i} + 1 \\ r_N^{*i} \leftarrow \sqrt{0.5\ \left((r_N^{*i})^2 + \left(1\_\|x_N^{*i}\|^2\right)\right)} \end{cases} \qquad (11)$$

Au contraire, si la Condition 2 n'est pas remplie, une nouvelle règle floue/nuage de données est formée autour de x_k^i en utilisant l'équation (8). Pour les nuages de données qui ne

reçoivent pas de nouveaux membres, les paramètres des autres règles floues/nuages de données restent les mêmes pour le prochain cycle de traitement.

La procédure principale de l'étape d'apprentissage du classificateur proposé est résumée à l'algorithme suivante :

While the new data sample of the i^{th} class $\boldsymbol{x}_k^i$ is available

i. $\boldsymbol{x}_k^i \leftarrow \frac{\boldsymbol{x}_k^i}{\left\|\boldsymbol{x}_k^i\right\|}$

ii. **If** ($k=1$) **Then**

1. $\boldsymbol{\mu}_1^i \leftarrow \boldsymbol{x}_1^i$
2. $F^i \leftarrow 1$
3. $\boldsymbol{x}_1^{*i} \leftarrow \boldsymbol{x}_1^i$
4. $M_1^{*i} \leftarrow 1$
5. $r_1^{*i} \leftarrow r_o$

iii. **Else**

1. Update $\boldsymbol{\mu}_{k-1}^i$ to $\boldsymbol{\mu}_k^i$ using eq. (3);
2. Calculate $D_k\left(\boldsymbol{x}_k^i\right)$ using eq. (2);
3. Update $D_k\left(\boldsymbol{x}_j^{*i}\right)$ ($j=1,2,\ldots,F^i$) using eq. (2);
4. **If** (Condition 1 (eq. (7)) is met) **Then**
   - Add a new data cloud using eq. (8);
5. **Else**
   - Find the nearest data cloud using eq. (9);
   - **If** (Condition 2 (eq. (7)) is met) **Then**
     * Update the meta-parameters of the nearest data cloud using eq. (11);
   - **Else**
     * Add a new data cloud using eq. (8);
   - **End If**
6. **End If**

iv. **End If**

End While

B.2.3 Étape de validation

Dans cette sous-section, nous décrirons la procédure du classificateur ALMMo proposé pour générer des étiquettes pour les échantillons de données de validation.

Chaque échantillon de données de validation est envoyé à tous les sous-classificateurs FRB AnYa correspondant aux C classes de l'ensemble de données. Comme chaque classe peut avoir plusieurs règles floues de type AnYa (R peut être plus grand que C), la sortie, à savoir le score de confiance de chaque règle FRB AnYa, est donnée de la manière suivante (j=1, 2...R)

$$Rule^j: \quad IF\left(x_k \sim x_j^*\right) \quad THEN \quad \left[\lambda_j = exp\left[-\frac{1}{2}\left\|x_k - x_j^*\right\|^2\right]\right] \tag{12}$$

Après que toutes les règles FRB AnYa aient généré leurs scores de confiance, l'opérateur "le vainqueur prend tout" (équation (5)) sera utilisé pour sélectionner la règle la plus confiante et attribuer à l'échantillon de données de validation l'étiquette correspondante [60].

Bibliographies

[1] Herbtonics ACV, "Informational Security (Infosec) (is)" , 01 Jan 2022.

[2] Izzat Alsmadi ," Introduction to Information Security", 01 Jan 2018.

[3] Michael Nieles, "An Introduction to Information Security", 22 Jun 2017.

[4] Bright Brabin Winsley , "Information Security: A Scientometric Study", 01 Jan 2020.

[5] Beyza Nur Akilotu, "Information Security and Related Machine Learning Applications", 01 Nov 2019.

[6] Michael C. Fairhurst, "Biometrics: A Very Short Introduction", 08 Nov 2018.

[7] "Biometrics and Applications", 01 Jun 2022.

[8] "Biometric Technologies in Healthcare Biometrics", 03 Jun 2022.

[9] Zhenan Sun, Qi Li, Yunfan Liu, Yuhao Zhu, "Opportunities and Challenges for Biometrics", 01 Jan 2021.

[10] Michael C. Fairhurst, "Biometrics: A Very Short Introduction", 08 Nov 2018.

[11] https://ww.toupie.org/Dictionnaire/Information.htm.

[12] " Sécurité et promotion de la sécurité: Aspects conceptuels et opérationnels" Bibliothèque nationale du Canada,1998.

[13] AHONA RUDRA, " Qu'est-ce que la sécurité de l'information ?", 15 Novembre 2022.

[14] "Qu'est-ce que la sécurité de l'information ?" : https://www.box.com/fr-fr/resources/what-is-information-security.

[15] "What Is Information Security ?" : https://www.cisco.com/c/fr_ca/products/security/what-is-information-security infosec.html.

[16] https://vitrinelinguistique.oqlf.gouv.qc.ca/fichegdt/fiche/8358572/securitedelinformation.

[17] https://www.info-entre-pros.com/defis-securite-information-numerique/ .

[18] André saeckel, "Les objectifs de protection de la sécurité de l'information et leur signification", 11 nov 2022.

[19] https://www.checkpoint.com/fr/cyberhub/cybersecurity/whatiscybersecurity/cybersecuriy-vs-information-security/ .

[20] "Sécurité informatique et cybersécurité : Quelles différences ?" 2022 : https://iotindustriel.com/cybersecurite/securite-informatique-et-cybersecurite-quelles-differences/ .

[21] " Cybersécurité : Différence entre la sécurité informatique et la cybersécurité", Février 5, 2024 : https://www.skills4all.com/cybersecurite-difference-entre-la-securite-informatique-et-la-cybersecurite/

[22] "Sécurité Informatique", juillet 13, 2022 : https://www.crowdstrike.fr/cybersecurity-101/it-security/

[23] Dr. Benidris Fatima zohra , " Cryptographie " , Juin, 2020.

[24] Adda Ali Pacha , Naima Hadj-Said, RIST Vol, 12 n°01 , 2002.

[25] Juliana Muñoz, "Le rôle de la biométrie dans la vérification moderne de l'identité", 12 avril 2023.

[26] "Biométrie" :https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/biometrie .

[27] BOUAZDIA Fayçal**,** "Vers des caractéristiques profondes de l'image Pourquoi ? et quand ?" , 2020.

[28] Jennifer Irish , Françoys Labonté," Comprendre les menaces et les défis – Désinformation visuelle et multimodale (DVM)" .

[29] Melouah Messaouda , Driche Imane, "Tatouage numérique des données biomédicales dans le domaine des transformée" , 2022/2023.

[30] Laimeche L, "Stéganalyse universelle basée sue les statistiques d'ordre supérieur", 2018.

[31] Daouali Somia , Oulhadj Fatima , "Sécurité de l'information par stéganographie", 2019/2020.

[32] Christophe Soutoul , DamienVergnaud , "A Survey on Crypto-Biometric Cryptosystems" :https://www.sciencedirect.com/science/article/pii/S0167404823003681

[33] Belaloui Meriem, Djaffal Souhaila, "Tatouage d'images avec des données biométriques pour la preuve de propriété",2017.

[34] Ashwini Kumar, Vikas Kumar; "Biometric-Based Steganography: A Survey": https://ieeexplore.ieee.org/document/9478120/1000.

[35] La sécurité biométrique est-elle un facteur intéressant pour le contrôle d'accès ? :

https://www.nedapsecurity.com/fr/insight/la-securite-biometrique-est-elle-un-facteur-interessant-pour-le-controle-dacces/#news-letter .

[36] Mohamad El-Abed , "Évaluation de système biométrique. Cryptographie et sécurité", 2011.

[37] Abdallah MERAOUMIA, "Modèle de Markov caché appliqué à la multi-biométrie", USTHB ,2014.

[38] https://www.alamyimages.fr/photos-images/caractéristiques-physiques.html?imgt=8&sortBy=relevant .

[39] Benouaer Aichouche, Tahrine Soumia, "Système biométrique basé sur les motifs locaux binaires orientés (LBP^{θ})", 2016.

[40] "biometric system architecture" 02 Dec, 2022 : https://www.geeksforgeeks.org/biometric-system-architecture/

[41] "Biometric, Characteristics, Measurements, and Biometric System: Why They Must Be Differentiated": https://www.fasken.com/en/knowledge/2023/10/biometric-characteristics-measurements-and-biometric-system .

[42] A. K. Jain, L. Hong, , S. Pankanti: "Biometric Identification", *Comm. ACM*, Vol. 43, No. 2,pp. 90-98, February 2000.

[43] Abdallah Meraoumia, Salim Chitroub , ahmed Bouridane," Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-Biometric System of Person Recognition", *IEEE International Conference on Communications-ICC*, Kyoto, Japan, pp. 1-5, June 2011.

[44] Jain A.K, Dass S.C , Nandakumar K, "Can soft biometric traits assist user recognition ?" , Procedings of SPIE International symposium on defense and security : Biometric technology for human identification, 2004.

[45] Ross A, "An Introduction to multibiometrics", The 15th European signal

processing conference- EUSIPCO, Poznan, Poland, pp. 51, 2007.

[46] A. Ross ,A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, Vol. 24, Issue 13, pp. 2115-2125, September, 2003.

[47] K. Nanda kumar, A. Ross, A. K. Jain, "Biometric Fusion : Does Modeling Correlation Really Matter ? ", The 3rd Int'l Conf. on Biometrics : Theory, Applications and Systems, Washington DC, Sept. 2009.

[48] Yongjin Lee, Kyunghee Lee, Hyung keun Jee, Youn-Hee Gil, Woo-Yong Choi, Dosung Ahn, Sung Bum Pan, "Fusion for Multimodal Biometric Identification", The 5th International conference on Audio and video-based biometric person authentication-AVBPA, Hilton Rye Town, N.Y. USA, pp. 1071-1079, July 2005.

[49] Suo Jidong, Liu Xiaoming, "Fusion of Radar and AIS Data", The 7th International Conference on Signal Processing-ICSP'04, Beijing, China, Vol.3, pp, 2604-2607, 2004.

[50] Berger C., Voltersen M., Eckardt R., Eberle J., Heyer T., Salepci N., Hese S., Schmullius C., Tao J., Auer S., Bamler R., Ewald K., Gartley M., Jacobson J., Buswell A., Du Q., Pacifici F., "Multi-Modal and Multi-Temporal Data Fusion", IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Vol.6, No.3, pp.1324-1340, Jun 2013.

[51] Julian Fi´errez-Aguilar, Javier Ortega-Garcia, Daniel Garcia-Romero, Joaquin Gonzalez Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification", The 4th International Conference on Audio-and Video-Based Biometric Person AuthenticationAVBPA, Guildford, UK, pp. 830-837, Jun 2003.

[52] 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 ", univ-annaba , 2016 .

[53] https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/biometrie

[54] Zhang Rui, Zheng Yan , "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification", IEEE ,27 December 2018 .

[55] Rima Ouidad Belguechi , "Sécurité des systèmes biométriques révocabilité et

protection de la vie privée. Traitement des images [eess.IV] ",Ecole nationale Supérieure en Informatique Alger, 2015.

[56] BENNACEUR Bouchra ,DJERADI Fayrouz , "Sécurité des systèmes multi biométriques ", annecy, France ,Jun 2007.

[57] Valérie Viet Triem Tong, Hervé Sibert, Jérémy Lecoeur, Marc Girault, "FingerKey, un cryptosystème biométrique pour l'authentification ", University of Dayton,16 Decembre 2022.

[58] Meriem Mebarkia , Abdallah Meraoumia , Lotfi Houam , Seddik Khemaissia **,** " X-ray image analysis for osteoporosis diagnosis: From shallow to deep analysis ",Elsevier,2023

[59] Juho Kannala and Esa Rahtu : "BSIF: Binarized Statistical Image Features", University of Oulu, Finland.

[60] Plamen Angelov, Fellow, IEEE and Xiaowei Gu, " Autonomous Learning Multi-Model Classifier of 0 Order (ALMMo-0) ", IEEE Data Science Group, School of Computing and Communications, Lancaster University, Lancaster UK, 2017.

[61] Bendjenna Riadh, " Protéger l'échange d'information via un système crypto-biométrique », Université Larbi Tebessi,2021.

[62] Abdallah MERAOUMIA, "Modéle de Markov caché appliqué à la multi-biométrie », , Universite Des Sciences Et De La Technologie Houari Bomedienne, 01/06/2014.

[63] The Hong Kong Polytechnic University, PolyU FKP Database, http ://www.comp.polyu.edu.hk/sbiometrics/FKP/polyudb.htm.

[64] KARFOUF Mohammed Ali, BEDDIAF Ali, "Reconnaissance des expressions faciales", Université Kasdi Merbah-Ouargla,2022.