

Université Kasdi Merbah - Ouargla
Faculté des Nouvelles Technologies de l'Informatique et de la Communication
Département de l'informatique et des technologies de l'information



Mémoire de Master

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Administration et Sécurité des Réseaux

Thème

Système Biométrique Multimodal Utilisant Filter Bloom

Encadrer :

Dr.Azzaoui Nadjjet

Examineur :

Dr.Khelili Farida Khalida

Président :

Dr.Cheradid Abdelatif

Présenté par :

Aounallah Nour Elhouda

Chera Salsabil

Année universitaire : 2024/2025

Table des matières

Liste des abréviations	11
1 Les systèmes biométriques	14
1.1 Introduction	14
1.2 Définition d'un système biométrique	14
1.3 Types de systèmes biométriques	14
1.3.1 Système biométrique unimodal	14
1.3.2 Système biométrique multimodal	15
1.4 Modalités biométriques	15
1.4.1 Biométrie physiologique	16
1.4.2 Biométrie comportementale	18
1.5 Architecture d'un système biométrique	20
1.5.1 Capteur	20
1.5.2 Prétraitement	20
1.5.3 Extraction des caractéristiques	20
1.5.4 Générateur de gabarits	20
1.5.5 Matcher	21
1.5.6 Dispositif d'application	21
1.6 La fonctionnement des systemes biometriques	21
1.6.1 Authentification	21
1.6.2 Identification	22
1.6.3 Vérification	22
1.7 Domaine d'application	23
1.7.1 Reconnaissance visage	24
1.7.2 Reconnaissance d'empreinte digitale	24
1.7.3 Reconnaissance de l'iris	24
1.7.4 Reconnaissance de pume de la main	24
1.7.5 Reconnaissance de viox	25
1.8 Avantages et limites	25
1.8.1 les avantages :	25
1.8.2 Les limites	25
1.9 Performance des systèmes	26
1.10 Conclusion	27
2 Les Travaux relatifs aux systèmes biométriques	28
2.1 Introduction	28
2.2 Les Travaux relatifs	28
2.2.1 les Systèmes biométriques Unimodaux	28

2.2.2	Systèmes biométriques Multimodaux	32
2.3	Discussion et Analyse	37
2.4	Dataset	37
2.4.1	Discussion et Analyse de Dataset	39
2.5	conclusion	40
3	Réalisation d'un systeme biometrique multimodel utilisant un filtre de bloom	41
3.1	Introduction	41
3.2	Présentation du système proposée	41
3.3	Environnement de travail	42
3.3.1	les bibliothèque de Python	42
3.3.2	les methodes	43
3.3.3	Dataset	46
3.3.4	langage de programmation	48
3.4	l'implementation	49
3.4.1	l'extraction des caractéristique :	49
3.4.2	la Fusion Biométrie	51
3.4.3	Le Filtrage par Bloom Filter	52
3.5	les interfaces de L'application	53
3.5.1	L'enregistrement des personnes	53
3.5.2	Galerie des utilisateurs enregistrés	54
3.5.3	Affichage de la liste des utilisateurs	55
3.5.4	Définir L'identification des personnes.	56
3.5.5	Reconnaissance facile	57
3.5.6	Reconnaissance d'empreintes digitales	58
3.5.7	Reconnaissance visage	59
3.5.8	Reconnaissance d'empreinte digitale	60
3.6	Resultat	61
3.6.1	Équations Utilisées	61
3.6.2	Résultats Totales	62
3.6.3	Les statistiques du système	62
3.6.4	Résultats d'interface	63
3.7	conclusion	65
	Conclusion Générale	66

Liste des tableaux

2.1	les travaux baseés sur Empreinte digitale	29
2.2	les travaux baseés sur Visage	30
2.3	les travaux baseés sur Iris	31
2.4	les travaux baseés sur Pume de la main	32
2.5	les travaux baseés sur l’empreinte digitale et iris	34
2.6	les travaux baseés sur visage et iris	35
2.7	les travaux baseés sur l’oreille et du visage	36
2.8	Dataset	39
3.1	Résultat	63

Table des figures

1.1	Système biométrique unimodal	15
1.2	Système biométrique multimodal	15
1.3	Visage	16
1.4	Iris	17
1.5	Emprunte Digitale	17
1.6	la paume de la main	18
1.7	La voix	18
1.8	la Signateur	19
1.9	Frappe au clavier	19
1.10	Architecture d'un système biométrique	20
1.11	Modules d'un système biométrique	21
1.12	Authentification	22
1.13	Identification	22
1.14	Vérification	23
1.15	Application d'un système biométrique	23
3.1	Diagramme de système proposée	42
3.2	LBP	44
3.3	Histogram of Oriented Gradients (HOG) de l'extraction de visage	45
3.4	Convolutional Neural Network(CNN)	46
3.5	Dataset de visage	47
3.6	Dataset d'empreinte digitale	48
3.7	Python 3.8	48
3.8	Diagramme d'empreinte digitale	50
3.9	Diagramme de Visage	51
3.10	Code d'utilisation du Filter Bloom dans le système	52
3.11	Les données personnelles	53
3.12	Galerie	54
3.13	Affichage de la liste des utilisateurs	55
3.14	L'identification des personnes	56
3.15	Base de données contenant les visages enregistrés	57
3.16	Base de données d'empreintes digitales	58
3.17	Reconnaissance visage	59
3.18	Reconnaissance d'empreinte digitale	60
3.19	la précision de la reconnaissance sur plusieurs mois	62
3.20	La reconnaissance d'empreinte digitale	63
3.21	La reconnaissance de visage	64

ألهاء

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تتحقق الغايات، له الشكر أولاً وآخرًا، ظاهرًا وباطنًا، أن وفقني لإنجاز هذا العمل المتواضع.

وكم كنت أتمنى أن يكون والدي الغالي، رحمه الله، حاضرًا معي لحظة تخرجي، فقد كان سندي الأول، وكان لا يملّ من تشجيعي على الدراسة والاجتهاد، ينتظر هذا اليوم بفرغ الصبر، لكن شاءت إرادة الله أن يرحل قبل أن يرى ثمرة تعب. أسأل الله أن يتغمّده بواسع رحمته ويجعل هذا العمل في ميزان حسناته.

أخصّ بالشكر والامتنان زوجي العزيز، الذي كان لي نعم السند والداعم في كل مراحل دراستي، لم ييخل عليّ بالدعم المعنوي والمادي، ووقف إلى جانبي في كل التحديات.

ولا يسعني أيضًا إلا أن أعبر عن محبتي وامتناني لعائتي الصغيرة والكبيرة، وعلى رأسهم أمي الحبيبة، نبع الحنان ومصدر القوة، التي كانت دعواتها نورًا يضيء دربي، وصبرها دافعًا لأكمل الطريق.

كما أتقدم بالشكر والعرفان إلى أخواتي العزيزات : أسماء، رانيا، شهد، انتصار، ندى، وأم الخير، على كل كلمات التشجيع، وكل لحظة دعم ومحبة، فقد كنّ دومًا قريبات من قلبي، داعمات لي في كل خطوة.

إلى كل من ساندني بكلمة أو دعاء أو ابتسامة خلال هذا المشوار، أقول : شكرًا من القلب.

ألهاء

الحمد لله حُبًّا وشُكْرًا وامتنانًا، ما كنتُ لأفعل هذا لولا فضل الله، فالحمد لله على البدء، وعلى الختام.

أهدي هذا النجاح لنفسي الطموحة، إلى ذلك الحلم الذي طال انتظاره، ففتحقق بفضل الله، وأصبح واقعًا أفخر به.

إلى من زين اسمي بأجمل الألقاب، إلى من دعمني بلا حدود، وأعطاني بلا مقابل، إلى من علّمني أن الدنيا كفاح، وسلاحها العلم والمعرفة، إلى من غرس في روحي مكارم الأخلاق، إلى داعمي الأول في مسيرتي، وسندي، وقوتي، وملاذي بعد الله، إلى فخري واعتزازي أبي.

وإلى من جعل الله الجنة تحت قدميها، إلى من لم تخلُ دعواتها من اسمي، إلى من أفنت عمرها لأحقق طموحي، إلى الداعمة الأولى والأبدية، إلى من تحمّلت عني الألم، وساندتني في ضعفي، إلى سرّ قوتي ونجاحي أمي.

وإلى شركاء الطفولة، إلى أعزّ الناس وأقربهم إلى قلبي، إخوتي الأحبة زكريا، عبد القادر، وهيفاء.

وإلى من كانوا لي عونًا وسندًا في هذا الطريق شروق

إلى رفاق السنين، وأصحاب الشدائد والأزمات، ما سلكنا البدايات إلا بتيسيره، وما بلغنا النهايات إلا بتوفيقه، وما حققنا الغايات إلا بفضلِهِ. الحمد لله من قبل ومن بعد.

Résume

Les systèmes biométriques permettent l'identification automatique à partir des mesures biologiques d'un individu. nous proposons dans notre mémoire de master, un système de reconnaissance biométrique multimodal fusionner deux modalité :visage et empreinte digitale, pour améliorer la vérification et l'identification de l'identité des personnes de manière plus précise et efficace. ce système se distingue par l'utilisation du filtre de Bloom (Bloom Filter), qui offre une approche efficace et optimisée pour le traitement des données biométrique.

Le système traite les visages à l'aide de la reconnaissance faciale pour extraire des vecteurs (128 dimensions) et les comparer à la distance euclidienne. Les empreintes digitales sont améliorées, puis leurs caractéristiques sont extraites à l'aide de LBP et d'histogrammes, puis comparées à SSIM et à la comparaison d'histogrammes. Toutes les données personnelles (y compris le visage et les empreintes digitales) sont stockées dans SQLite avec un numéro d'identification unifié. Pour améliorer les performances de recherche, un filtre Bloom est utilisé uniquement pour les empreintes digitales (et non pour les visages) afin de filtrer les hashtags non spécifiés auparavant.

Le système a été développé en Python, s'appuyant sur des algorithmes d'apprentissage profond pour extraire les caractéristiques des images. Les résultats expérimentaux ont montré que la combinaison du visage et des empreintes digitales à l'aide d'un filtre Bloom permet d'obtenir de meilleures performances. cette approche permet d'augmenter les performances du système en comparaison avec les systèmes classiques ne reposant que sur une modalité biométrique unique.

Mots clé : Système biométrique multimodal, Reconnaissance visage, Reconnaissance d'empreinte digitale, Filtre de Bloom.

الملخص

تُعد الأنظمة البيومترية وسيلة فعّالة لتحديد هوية الأفراد تلقائيًا اعتمادًا على خصائصهم البيولوجية. في هذا المشروع، نقترح نظامًا بيومترًا متعدد الوسائط يجمع بين طريقتي التعرف على الوجه وبصمة الإصبع، بهدف تحسين دقة وكفاءة التحقق من الهوية. يعتمد النظام على استخدام مرشح بلوم، الذي يُمثل آلية فعّالة لمعالجة وتصفية البيانات البيومترية، مع تقليل استهلاك الذاكرة وتحسين سرعة البحث.

يعالج النظام صور الوجوه من خلال استخراج متجهات الخصائص (١٢٨ بعدًا) باستخدام خوارزميات التعلم العميق، ثم يقارنها اعتمادًا على المسافة الإقليدية. أما بصمات الأصابع، فتُعالج وتُستخرج خصائصها باستخدام خوارزمية الأنماط الثنائية المحلية، بالإضافة إلى تحليل المدرج التكراري، ثم تُقارن النتائج باستخدام مؤشر التشابه البنيوي ودرجة تطابق المدرجات.

تُخزّن البيانات الشخصية والبيومترية في قاعدة بيانات تحت معرف موحد لكل شخص. ويُستخدم مرشح بلوم خصيصًا لمعالجة بصمات الأصابع، حيث يتيح تصفية سريعة للأوسمة دون الحاجة إلى مقارنة مباشرة لكل الصور.

تم تطوير هذا النظام بلغة بايثون، باستخدام مكتبات مخصصة لمعالجة الصور والتعلم الآلي. وقد أظهرت التجارب أن دمج الوجه والبصمة معًا، باستخدام مرشح بلوم، يُحسّن الأداء مقارنة بالأنظمة التقليدية الأحادية النمط.

الكلمات المفتاحية :

نظام القياسات الحيوية متعدد الوسائط، التعرف على الوجه، التعرف على بصمات الأصابع، مرشح بلوم

Abstract

Biometric systems enable automatic identification based on an individual's biological measurements. In our master's thesis, we propose a multimodal biometric recognition system that combines two modalities : face and fingerprint, to improve the verification and identification of individuals' identities more accurately and efficiently. This system is distinguished by the use of the Bloom Filter, which offers an efficient and optimized approach for processing biometric data.

The system processes faces using facial recognition to extract vectors (128 dimensions) and compare them with Euclidean distance. Fingerprints are enhanced, then their features are extracted using LBP and histograms, and then compared with SSIM and histogram comparison. All personal data (including face and fingerprints) are stored in SQLite with a unified ID number. To improve search performance, a Bloom filter is used only for fingerprints (and not for faces) to filter out previously unspecified hashtags.

The system was developed in Python, relying on deep learning algorithms to extract image features. Experimental results showed that combining face and fingerprints using a Bloom filter achieves better performance. This approach increases the system's performance compared to conventional systems relying on a single biometric modality.

Keywords : Multimodal biometric system, Face recognition, Fingerprint recognition, Bloom filter.

Liste des abréviations

ACC : Analyse de Corrélation Canonique.
ADN : Acide Désoxyribonucléique.
AFIS : Automated Fingerprint Identification System.
BD : Base de Données.
BF : Bloom Filter.
CNN : Convolutional Neural Network.
DLF : Discriminant Linéaire de Fisher.
EER : Equal Error Rate.
FNM : Face Normalization Model.
FVC : Fingerprint Verification Contest.
GAN : Generative Adversarial Network.
GLCM : Gray-Level Co-occurrence Matrix.
GUI : Graphical User Interface.
HOG : Histogram of Oriented Gradients.
KNN : K-Nearest Neighbors.
LBP : Local Binary Pattern.
MICL : Multimodal Identification and Comparison Layer.
NIG : Normal Inverse Gaussian.
NN : Neural Network.
PCA : Principal Component Analysis.
PIN : Personal Identification Number.
SN : Système Neuronale.
SSA : Singular Spectrum Analysis.
SSIM : Structural Similarity Index Measure.
SVM : Support Vector Machine.

Introduction Générale

Jour après jour on parle de plus en plus de l'absence de sécurité dans plusieurs domaines, ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance. Pour assurer cette sécurité il faut faire une vérification et l'identification des individus. Le système visuel qui sert quotidiennement par l'être humain pour identifier les personnes d'une façon automatique, bien que il soit complexe.

Malgré les différentes méthodes d'identification traditionnelles telles que la vérification de l'identité d'une personne, comme une carte d'identité, un passeport ou un numéro d'identification personnel, elles sont vulnérables au volé ou bien d'oublié et à la falsification. Pour contourner ces limitations, il y a un autre moyen de sécurité a été développé qui permet d'utiliser des informations d'individu au lieu des informations qu'il possède ou qu'il connaît. Cette nouvelle façon d'identification des individus est la biométrie.

La solution alternative aux anciens moyens de vérification d'identité c'est Les caractéristiques biométriques. et permis leur avantage elle est universelles et d'autre part elles sont mesurables et uniques : deux personnes ne peuvent pas posséder exactement la même caractéristique.

L'objectif principal de la système biométrie est la reconnaissance et identification automatiquement des individus en utilisant leurs caractéristiques physiologiques ou comportementales. Les caractéristiques physiologiques peuvent inclure le visage, l'iris, les empreintes, la géométrie de la main, les oreilles. Les caractéristiques comportementales incluent la voix, la signature, la démarche.

Cette recherche vise principalement à améliorer la précision et la fiabilité des systèmes biométriques multimodaux pour la reconnaissance des visages et des empreintes digitales en utilisant Bloom filter pour fonctionner en manière rapide et efficace.

Cette thèse est divisée en trois chapitres qui est structuré comme suit :

Chapitre 1 - Présentation de la biométrie : Ce chapitre commence par un aperçu de la biométrie, en passant en revue son importance et son rôle essentiel dans l'identification de l'identité numérique. Ensuite, nous abordons les diverses mesures biométriques et leur utilisation pour sécuriser les données et la confidentialité.

Chapitre 2 - Les Travaux relatifs aux systèmes biométriques : Le deuxième chapitre s'attache à classer sur les Travaux relatifs en deux parties les Systèmes biométriques Unimodaux, les Systèmes biométriques Multimodaux et chaque de deux avec leur modalité. En suite les Dataset utilisé dans cette recherche.

Chapitre 3 - Réalisation d'un système biométrique multimodal utilisant un filtre de bloom : dans ce chapitre on se termine par une présentation détaillée sur notre travail, nous mentionnons donc l'environnement de travail en suite l'implémentations de résultat de leur efficacité pour améliorer la précision de système biométrique multimodal.

Chapitre 1

Les systèmes biométriques

1.1 Introduction

Les systèmes biométriques sont aujourd’hui une solution incontournable dans le domaine de l’identification et de l’authentification. Utiliser des caractéristiques biométriques uniques, telles que les visages ou les empreintes digitales, pour authentifier les individus [1]. Avec le développement de l’intelligence artificielle, sa précision et sa fiabilité ont considérablement augmenté [2]. En raison de son efficacité à améliorer la sécurité et l’accès aux services. Ce chapitre présente les principes de base des systèmes biométriques, leurs composants et les principaux types de méthodes utilisées.

1.2 Définition d’un système biométrique

La biométrie fait référence à l’étude des caractéristiques physiques ou comportementales utilisées pour l’identification d’une personne. Les caractéristiques biométriques sont traitées au moyen d’un système biométrique qui permet de comparer efficacement le visage, l’iris, les empreintes digitales, etc. pour vérifier ou identifier une personne. La biométrie étant en hausse, les systèmes biométriques sont intégrés dans les domaines les plus courants de la vie quotidienne. Le plus efficace s’appelle le système d’identification biométrique automatisé – ABIS. [3].

1.3 Types de systèmes biométriques

En général, il existe deux types de systèmes biométriques [4]. :

1.3.1 Système biométrique unimodal

Un système biométrique unimodal se base sur une unique modalité biométrique, comme la reconnaissance des empreintes digitales, faciales ou de l’iris, pour confirmer ou identifier l’identité d’une personne. Toutefois, ces dispositifs ont plusieurs faiblesses, notamment au niveau de la performance lorsqu’il y a une mauvaise qualité des données, une grande similitude entre les utilisateurs ou encore en présence de tentatives d’usurpation. Ces limites peuvent nuire à la fiabilité du système dans des environnements réels [4].

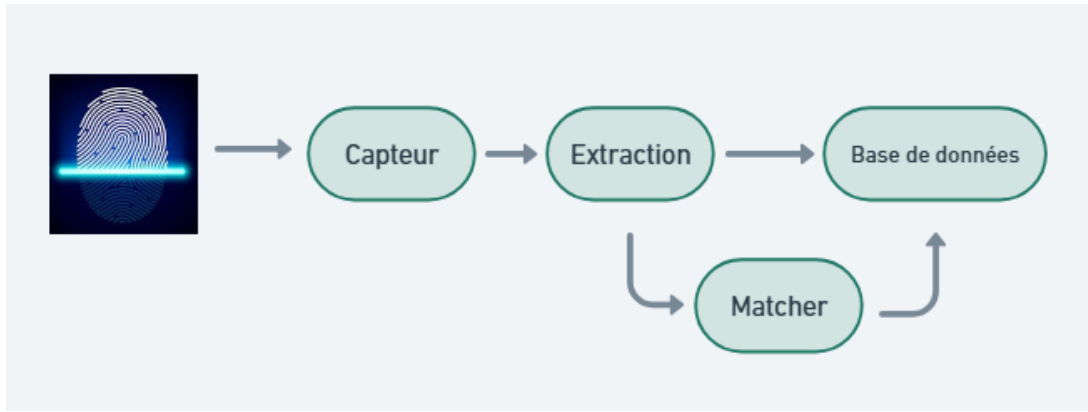


FIGURE 1.1 – Système biométrique unimodal

1.3.2 Système biométrique multimodal

Un système biométrique multimodal combine plusieurs modalités biométriques (par exemple : empreinte digitale et visage) pour surmonter les faiblesses des systèmes unimodaux. L'intégration de plusieurs sources d'information biométrique permet d'améliorer la précision, la sécurité et la robustesse du processus de reconnaissance. La fusion des scores issus de chaque modalité joue un rôle clé dans l'amélioration de la performance globale du système, en rendant les décisions plus fiables même en cas de données partielles ou bruitées [4].

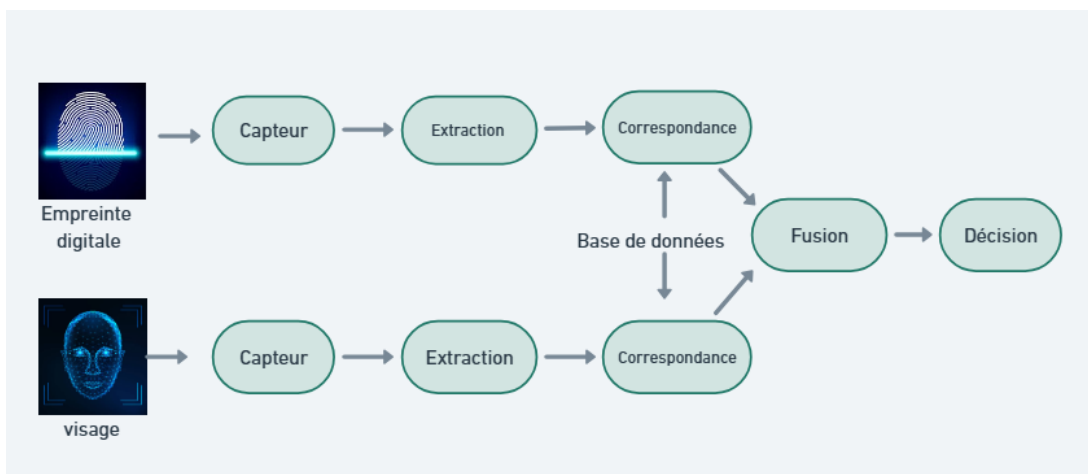


FIGURE 1.2 – Système biométrique multimodal

1.4 Modalités biométriques

Chaque caractéristique biométrique qui satisfait aux conditions précédentes, peut être utilisée pour identifier un individu, elle est appelée modalité biométrique, et se classer selon le type : physiologique ou comportementale [5]

1.4.1 Biométrie physiologique

Ces modalités sont uniques et permanentes, leur principe est basée sur l'identification de traits physiques particuliers d'une personne, tels que : Le visage, L'iris, La rétine, L'ADN, La géométrie de la main, L'empreinte palmaire, L'empreinte digitale. Ces éléments ont l'avantage d'être stables dans la vie d'un individu[5]. Quelques exemples comprennent les méthodes d'identification physique :

a.Reconnaissance du visage :

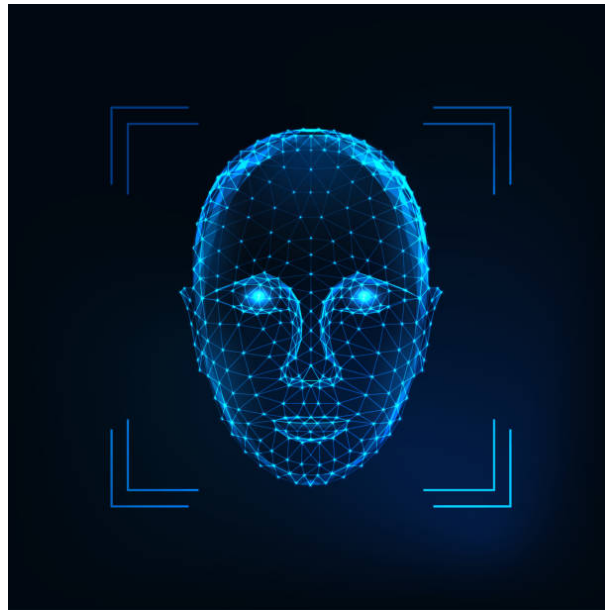


FIGURE 1.3 – Visage

Cette étape prend en compte les caractéristiques extraites de l'arrière-plan au cours de l'étape d'extraction des caractéristiques et les compare aux caractéristiques connues stockées dans une base de données spécifique. Il existe deux applications générales de la reconnaissance faciale, l'une appelée identification et l'autre appelée vérification. Au cours de l'étape d'identification, une face de test est comparée à un ensemble de faces dans le but de trouver la correspondance la plus probable. Au cours de l'étape d'identification, une face test est comparée à une face connue dans la base de données afin de prendre la décision d'acceptation ou de rejet [6] .

b.Reconnaissance de l'iris :



FIGURE 1.4 – Iris

L'analyse de l'iris détecte les motifs uniques dans les iris, les cercles colorés dans les yeux des personnes, un ensemble de pixels contenant uniquement l'iris en éclairant l'iris avec une lumière visible et proche infrarouge et enfin comparé aux modèles stockés dans une base de données pour vérification.[7] .

c.Reconnaissance des empreintes digitales :



FIGURE 1.5 – Empreinte Digitale

La technologie de reconnaissance des empreintes digitales fonctionne en capturant et en analysant des motifs uniques sur le bout des doigts. Le processus commence par la prise d'une image numérique de l'empreinte à l'aide d'un scanner dédié, puis cette image est analysée par un logiciel avancé pour extraire les caractéristiques distinctives telles que les extrémités des lignes, les branches et les motifs. Ensuite, un modèle numérique est créé qui représente l'empreinte sous une forme mathématique unique. Lorsqu'une personne tente de vérifier son identité, son empreinte digitale est prise à nouveau et un nouveau modèle est créé qui compare aux modèles stockés dans la base de données. Si une correspondance est trouvée, l'identité est confirmée et l'accès est accordé ; sinon, la demande est rejetée.

Cette méthode est rapide et fiable pour vérifier l'identité. [8] .

d.Reconnaissance de la paume de la main :



FIGURE 1.6 – la paume de la main

En utilisant la lumière infrarouge pour cartographier la structure veineuse unique de votre paume, capturant plus de 5 millions de points de données. Le scanner de la veine palmaire convertit ensuite ces points de données en un code unique crypté qui devient une identification biométrique [7] .

1.4.2 Biométrie comportementale

La biométrie comportementale met l'accent sur les actions d'une personne, en tenant compte des variantes intérieures comme l'humeur et l'état de santé. Des exemples de biométrie comportementale comprennent :

a.La voix :

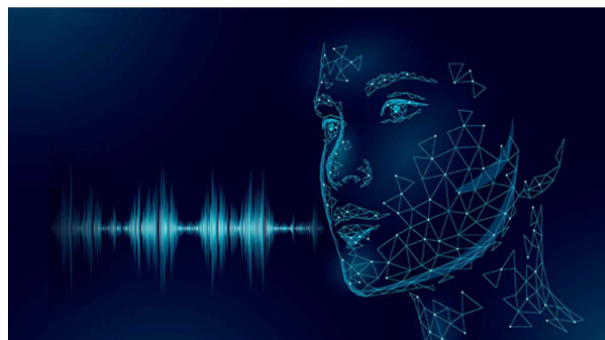


FIGURE 1.7 – La voix

La reconnaissance vocale est une technologie qui permet à un ordinateur ou à un appareil d'identifier et d'analyser la parole parlée, de sorte qu'il peut comprendre les commandes vocales ou identifier le locuteur en fonction de son empreinte vocale. Le processus commence par la capture du son via un microphone, puis le signal est traité et analysé pour extraire des caractéristiques audio, après quoi ces caractéristiques sont comparées à

des modèles pré-stockés pour reconnaître les mots ou les haut-parleurs[9].

b.la Signateur :



FIGURE 1.8 – la Signateur

Reconnaissance de la signature (pour l'identification, on utilise simplement le degré de coïncidence des deux images). Par la peinture et les caractéristiques dynamiques de l'écriture (pour l'identification, une convolution est construite, qui comprend des informations sur la peinture, les caractéristiques temporelles de l'application de peinture, et les caractéristiques statistiques de la dynamique de la pression sur la surface) [10]

c.Frappe au clavier :



FIGURE 1.9 – Frappe au clavier

Frappe au clavier désigne une méthode biométrique comportementale fondée sur les dynamiques de frappe, c'est-à-dire les comportements particuliers de chaque personne lors de l'utilisation du clavier. Ces dynamiques comprennent des éléments comme l'intervalle de temps entre les frappes, la durée pendant laquelle une touche est maintenue (temps de maintien), la rapidité de saisie, le taux d'erreurs (comme l'emploi de la touche effacer), l'utilisation du pavé numérique, la séquence d'usage des touches majuscules et parfois même l'intensité de frappe. Ces indicateurs permettent non seulement de confirmer l'identité d'un utilisateur à partir d'un échantillon réduit (par exemple, lors de la saisie d'un mot de passe), mais également de l'identifier en analysant un volume important de données et en mettant en comparaison son profil avec ceux des autres utilisateurs. [11]

1.5 Architecture d'un système biométrique

L'architecture du système biométrique comprend les principaux éléments suivants [12] :

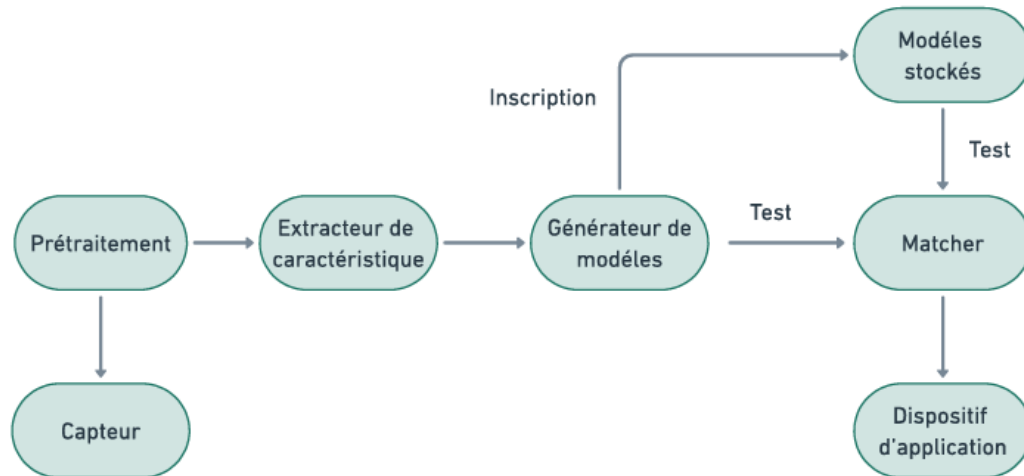


FIGURE 1.10 – Architecture d'un système biométrique

1.5.1 Capteur

Le premier composant du système biométrique qui rassemble toutes les données nécessaires à la biométrie est le capteur. C'est l'interface entre le monde réel et le système. Il s'agit généralement d'un système d'acquisition d'images, bien que cela dépende de certaines caractéristiques ou des caractéristiques nécessaires pour déterminer s'il doit être remplacé ou non.[12]

1.5.2 Prétraitement

C'est le deuxième bloc qui complète le portrait. Son but est d'améliorer l'entrée et de supprimer les artefacts capteur, fond bruit, etc.[12]

1.5.3 Extraction des caractéristiques

C'est la troisième et la plus importante étape du système biométrique. L'extraction des caractéristiques doit être faite pour les identifier à un stade ultérieur. L'objectif d'un extracteur de caractéristiques est de caractériser un objet à reconnaître par des mesures.[12]

1.5.4 Générateur de gabarits

Le générateur de modèles génère les modèles qui sont utilisés pour l'authentification à l'aide des fonctionnalités extraites. Un gabarit est un vecteur de nombres ou une image avec des tracés distincts. Les caractéristiques obtenues à partir des groupes sources se

combinent pour former un gabarit. Les modèles sont stockés dans la base de données à des fins de comparaison et servent d'entrée pour la correspondance. [12]

1.5.5 Matcher

La phase de correspondance est réalisée par l'utilisation d'une correspondance. Dans cette partie, le gabarit obtenu est remis à un matcher qui le compare avec les gabarits stockés en utilisant divers algorithmes tels que la distance de Hamming, etc. Après avoir fait correspondre les entrées, les résultats seront générés.[12]

1.5.6 Dispositif d'application

C'est un dispositif exploitant les résultats fournis par un système biométrique.[12]

1.6 La fonctionnement des systemes biometriques



FIGURE 1.11 – Modules d'un système biométrique

L'identification et l'authentification sont des processus essentiels pour vérifier l'identité d'un utilisateur et sécuriser l'accès aux ressources.

1.6.1 Authentification

L'authentification biométrique est une technologie qui s'appuie sur les caractéristiques physiologiques ou comportementales uniques des individus, comme les empreintes digitales, les traits du visage, l'iris ou les modèles vocaux, pour identifier et vérifier l'identité. Cette technologie se distingue par sa capacité à fournir un haut niveau de sécurité et de commodité par rapport aux méthodes traditionnelles telles que les mots de passe ou les cartes à puce. Trois axes principaux d'authentification biométrique ont été identifiés [13] :

Enrôlement : C'est la première étape dans un système biométrique. Elle consiste à capturer et enregistrer les données biométriques d'un individu (comme une photo du visage ou une empreinte) dans une base de données pour des comparaisons futures[14].

Échantillon en direct : Maintenant que le modèle est en place, l'utilisateur fournit un échantillon réel dans le cadre du processus d'authentification. Par exemple, ils peuvent insérer une carte contenant des données de reconnaissance faciale dans une machine et ensuite faire une photo de l'utilisateur[10].

Comparaison : Afin de terminer le processus d'authentification, l'échantillon réel de l'étape 2 est comparé au modèle. Si une correspondance est vérifiée, l'utilisateur est authentifié et peut accéder au système[14].

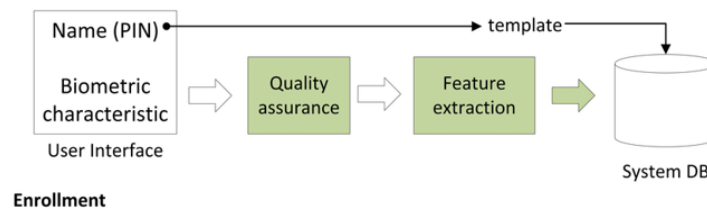


FIGURE 1.12 – Authentication

1.6.2 Identification

L'identification biométrique peut être appliquée à des scénarios numériques et physiques, et c'est une solution utilisée dans la défense, l'application de la loi et le contrôle des frontières. Avec l'identification, il existe une base de données qui contient les caractéristiques physiques d'un grand nombre de personnes par exemple, le dépôt du FBI stocke la taille, la couleur des cheveux, le poids, la couleur des yeux, les cicatrices et les tatouages de plus de 70.000.000 dossiers criminels. Avec l'authentification, les caractéristiques d'une personne sont comparées à un modèle spécifique ou Avec l'identification, cependant, les caractéristiques de la personne sont appariées à l'ensemble de la base de données[10].

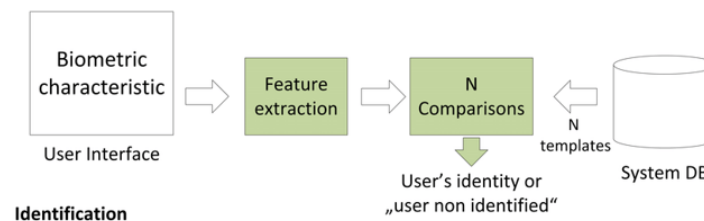


FIGURE 1.13 – Identification

1.6.3 Vérification

La vérification biométrique est souvent confondue avec l'autorisation. Pourtant, il existe une différence subtile entre les deux processus. Alors que l'authentification indique qu'une personne possède les mêmes caractéristiques biométriques qu'une personne déjà enregistrée dans le système, la vérification peut prouver de manière concluante que son identité en ligne est liée à son identité réelle.[10]

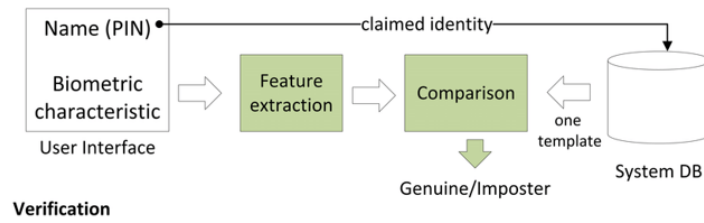


FIGURE 1.14 – Vérification

1.7 Domaine d'application

Ce système biométrique peut être appliqué dans de nombreux domaines qui ont besoin de sécurité et de protection, comme suit :



FIGURE 1.15 – Application d'un système biométrique

1.7.1 Reconnaissance visage

La reconnaissance visage est une technique permettant de reconnaître ou de valider l'identité d'une personne en observant son visage. Les logiciels de reconnaissance visage permettent d'identifier des personnes sur des photos, des vidéos ou en temps réel. Lors des contrôles de police, les agents peuvent utiliser des appareils mobiles pour identifier des personnes. Les logiciels de reconnaissance visage utilisent des algorithmes informatiques pour identifier des caractéristiques spécifiques et distinctives du visage d'une personne. Ces caractéristiques, telles que la distance entre les yeux ou la forme du menton, sont ensuite transformées en une représentation mathématique et comparées aux données d'autres visages dans une base de données de reconnaissance visage.

La technologie de reconnaissance visage est utilisée dans les aéroports, aux postes-frontières et lors d'événements sportifs tels que les Jeux olympiques. La reconnaissance visage peut également être utilisée dans des lieux privés tels que les entreprises et les stades[15].

1.7.2 Reconnaissance d'empreinte digitale

L'identification par empreintes digitales est l'une des méthodes biométriques les plus connues et utilisées. Utilisées à des fins d'identification depuis plus d'un siècle en raison de leur caractère unique et de leur constance dans le temps, les empreintes digitales ne sont devenues automatisées (c'est-à-dire biométriques) que récemment grâce aux progrès de la puissance de calcul[15].

La technologie de reconnaissance d'empreintes digitales a été utilisée dans [16] :

- Les systèmes automatisés d'imagerie d'empreintes digitales à grande échelle (AFIS) utilisés par les forces de l'ordre .
- La prévention de la fraude dans les programmes d'aide sociale .
- Le contrôle d'accès physique aux portes .
- L'accès logique aux systèmes informatiques.

1.7.3 Reconnaissance de l'iris

La reconnaissance de l'iris est un moyen biométrique d'identifier les personnes grâce à des motifs distinctifs présents dans la partie annulaire du globe oculaire entourant la pupille. Chaque iris étant unique, il s'agit d'un excellent outil de vérification biométrique. La procédure de reconnaissance de l'iris utilise une caméra numérique spécialisée. reconnaissance d'iris a été utilisée dans :

- comme le programme national d'identification des personnes.
- le programme de sécurité frontalière Aadhaar en Inde (avec plus de 1,2 milliard de paires d'iris enregistrées).
- la technologie de reconnaissance avancée du territoire national (HART) aux États-Unis (jusqu'à 500 millions d'identités).
- le système NEXUS, conçu pour accélérer le passage des frontières pour les voyageurs à faible risque et préapprouvés se déplaçant entre le Canada et les États-Unis. [17]

1.7.4 Reconnaissance de pume de la main

La reconnaissance d'empreintes palmaires a bénéficié d'un grand succès dans la recherche pour l'authentification et l'identification d'identité ces dernières années. Elle pré-

sente de nombreux avantages uniques, notamment la richesse de ses fonctionnalités, sa grande convivialité et son adéquation à la sécurité privée.[18]

1.7.5 Reconnaissance de viox

Les fonctionnalités MFCC sont largement utilisées dans la plupart des applications de traitement de la parole, telles que l'identification et la vérification des locuteurs, la reconnaissance viox et la classification du bruit. Les MFCC représentent le spectre qui modélise le conduit vocal chez l'homme, et la longueur du conduit vocal varie entre les hommes et les femmes. Des techniques d'apprentissage en profondeur sont utilisées pour créer un modèle permettant de reconnaître le genre de la voix à l'aide d'un ensemble de formation connu sous le nom de genre d'une personne, ainsi que de caractéristiques extraites de la parole.[19]

1.8 Avantages et limites

1.8.1 les avantages :

La biométrie est une technologie récente et adoptée par de grands constructeurs de matériel informatique. L'usage de la biométrie est un complément ou une alternative de l'utilisation des méthodes d'authentification comme des mots de passe, des badges ... etc. parmi les avantages de cette technique, citons [20] :

A. Vitesse et précision : L'utilisation de mots de passe et de codes pour accéder de manière sécurisée à un site physique ou virtuel est assez simple, mais générique. En revanche, la technologie de sécurité biométrique désigne les mots de passe biologiques qui ne peuvent être falsifiés. En d'autres termes, l'identification et l'authentification d'un individu donné sont fiables. La reconnaissance d'iris ou faciale est de plus en plus souvent intégrée aux processus de sécurité, du fait de la rapidité et de la simplicité de la détection.

B. Sécurité et rentabilité : Une fois le système de contrôle biométrique intégré, il n'y a plus besoin d'investissements infrastructurels supplémentaires. Les coûts d'investissement initiaux et récurrents chutent par conséquent de manière très nette. Ces systèmes contribuent en outre à prévenir les pertes dues à la fraude et aux entrées illégales. À lui seul, cet avantage permet d'économiser de l'argent et d'accroître la rentabilité.

C. Évolutif pour accompagner la croissance : Au fur et à mesure que les entreprises grandissent, la sécurité doit impérativement évoluer avec elles. L'évolutivité constitue d'ailleurs l'un des principaux avantages des contrôles biométriques. La flexibilité de ces systèmes leur permet d'accepter facilement des données supplémentaires sur les employés. En clair, la sécurité grandit avec l'entreprise.

D. L'aspect pratique : L'un des principaux avantages d'un système de contrôle biométrique tient à sa commodité. Les mots de passe n'ont pas besoin d'être réinitialisés. Une fois le test biométrique activé, la reconnaissance des empreintes digitales, de l'iris et du visage peut s'effectuer et les employés vaquer à leurs occupations. On peut même enregistrer les données et les vérifier selon les besoins.

1.8.2 Les limites

Bien que les applications biométriques soient constamment améliorées, ces derniers souffrent de plusieurs limites. Parmi les limites des systèmes biométriques[20], citons :

A. Le bruit sur la donnée capturée : Les données biométriques capturées peuvent être bruyantes ou endommagées, ces données bruitées risquent alors d'être mal appariées avec les modèles de la base de données aboutissant à un rejet incorrect d'un utilisateur autorisé. Des exemples de données bruitées sont une empreinte digitale avec une cicatrice, une voix altérée par un rhume mais généralement dues à des capteurs défectueux ou mal entretenus.

B. Les variations d'intra-classe : Les données biométriques d'un individu acquises pendant l'authentification peuvent être très différentes des données enrôlées (Template) dans la base de données. Cette variation peut être causée par une mauvaise interaction entre l'utilisateur et le capteur (changement de pose), une variation des conditions de l'environnement ambiant (changements d'éclairage) ou même par une variation de la constitution psychologique de l'individu (expression faciale).

C. Unicité : Alors qu'un trait biométrique est censé être unique et variable d'un individu à l'autre, il peut y avoir de grandes similitudes interclasses par rapport à ce trait (apparence faciale des vrais jumeaux), ce qui risque d'augmenter le taux de fausse acceptation du système.

D. Les attaques : Il est vrai que les traits biométriques sont beaucoup plus difficiles à contrer que les moyens d'identification classiques (les mots de passe et les cartes d'accès). Cependant, les impostures existent en particulier dans les modalités comportementales telles que la signature et la voix. Les traits physiologiques sont également sensibles aux attaques d'usurpation (l'utilisation de silicone pour reproduire des empreintes digitales).

1.9 Performance des systèmes

L'évaluation des performances des systèmes biométriques est un problème fondamental. Elle est généralement menée dans trois contextes :

- Évaluation technologique : Il s'agit de tester un algorithme sur un ensemble de données standardisé. L'objectif est de déterminer si le système biométrique développé répond aux prérequis. Les tests sont effectués à l'aide d'un traitement de données hors ligne et les résultats des tests technologiques sont reproductibles.

Évaluation du scénario : les tests sont effectués sur un système complet dans un environnement qui simule une application cible réelle d'intérêt. Les résultats des tests ne seront reproductibles que dans la mesure où le scénario simulé peut être contrôlé avec précision.

- Évaluation opérationnelle : Il s'agit d'un test réalisé en ligne dans des conditions réalistes. En général, les résultats des tests opérationnels ne seront pas reproductibles en raison de différences inconnues et non documentées entre les environnements opérationnels.

L'évaluation des performances du système biométrique prend généralement en compte la qualité des données d'entrée et le résultat de sortie. Pour l'évaluer, nous utilisons généralement un processus expérimental considérant le système comme une boîte noire. Dans ce cas, le fonctionnement interne des algorithmes associés n'est pas étudié. La boîte noire produit un résultat de sortie en utilisant un modèle biométrique comme entrée et un ensemble de paramètres.

1.10 Conclusion

Dans ce chapitre, nous fournissons un aperçu complet des systèmes biométriques et des types de systèmes biométriques, en nous concentrant sur l'utilisation de caractéristiques comportementales telles que la signature et la voix, et de caractéristiques physiologiques telles que les empreintes digitales et le visage, en plus des technologies biométriques avec leurs avantages et leurs limites.

Ce chapitre est essentiel pour comprendre les chapitres suivants, qui se concentreront sur la manière d'intégrer plusieurs fonctionnalités (système biométrique multimodal).

Chapitre 2

Les Travaux relatifs aux systèmes biométriques

2.1 Introduction

Les systèmes biométriques sont devenus des outils de plus en plus importants pour la sécurité de l'individu et de l'information[21], Ces systèmes utilisent les caractéristiques physiques ou comportementales de chaque individu, en raison de leur efficacité et de leur sécurité. Dans ce chapitre, nous avons passé un d'ensemble de recherches sur deux types biométriques sont :les systèmes biométriques unimodaux, qui sont basées sur une unique modalité biométrique. les systèmes biométriques multimodaux, qui combinent plusieurs modalité pour améliorer la précision et la fiabilité.

2.2 Les Travaux relatifs

Cette section, classer les Les Travaux relatifs de deux partie : les Systèmes biométriques Unimodaux .En suite les Systèmes biométriques Multimodaux.

2.2.1 les Systèmes biométriques Unimodaux

Dans cette section, nous avons réalisé une étude de plusieurs travaux de recherche traitant des systèmes biométriques unimodaux.

a.les travaux Basées sur l'empreinte digitale :

Christophe Charrier et al[22] Il réduire le nombre de minutes du modèle de référence (modèle de reconnaissance d'empreintes digitales) tout en maintenant les performances des systèmes biométriques. Une nouvelle mesure de confiance a été proposée pour chaque minute du modèle. Cet indicateur de confiance MiCI prédit l'importance et l'utilité de chaque minute par rapport aux autres parties du modèle. Cette procédure a été appliquée au cas où le modèle réduit était utilisé dans les bases de données FVC (Fingerprint Verification Contest) et SFINGE.

Zainul Abdin Jaffery[23] Ont développé un système robuste de reconnaissance automatique des empreintes digitales en utilisant une nouvelle approche appelée « Multi-Connection Hopfield Neural Network (MCHNN) ». Cette méthode vise à améliorer la

précision de reconnaissance, même dans des environnements bruités, tout en réduisant la complexité du système et la consommation de mémoire. L'étude a été évaluée sur trois bases de données (FVC-2004, NIST-4, et une base interne) et a atteint une précision de 99,65

Ali.N et al [24] Proposé un système de reconnaissance des empreintes digitales à l'aide de MATLAB 2010 , c'est une méthode d'identification biométrique personnelle les plus courantes et fiables

Auteur	Année	Travail	Méthode	Résultat
Christophe Charrier et al[22]	2023	Évaluation de la confiance des minuties d'une empreinte digitale	MiCI (Minutiae Confidence Index)	la methode MiCI proposée réduit le nombre de points du modèle tout en maintenant de bonnes performances sur les bases FVC/SFINGE.
Zainul Abidin Jaffery et al[23]	2022	A Robust Automatic Fingerprint Recognition System Using Multi-Connection Hopfield Neural Network	MC-HNN (Multi-Connection Hopfield Neural Network)	La méthode MC-HNN proposée a obtenu des résultats prometteurs avec une précision de 99,65%.
Ali.N et al [24]	2020	Fingerprint Recognition(using MATLAB)	Diviser l'image en blocs 3*3 et extraire les propriétés de l'empreinte digitale	la méthode utilisée est valide

TABLE 2.1 – les travaux basées sur Empreinte digitale

b.les travaux Baseés sur visage

Yichen Qian et al.[25] Proposer un modèle " Face Normalization Model (FNM) " pour générer une image de visage frontal neutre et réaliste pour la reconnaissance faciale,les Méthodologie utilise Modèle FNM basé sur le GAN, un réseau d'experts du visage pour maintenir l'identité faciale , une perte pixel par pixel pour stabiliser le processus d'optimisation , les discriminateurs d'attention du visage pour différencier et améliorer la qualité des images et des détails

Chen Li et al.[26] Exploiter pleinement cet avantage et rendre la reconnaissance humaine appropriée pour des applications intelligentes plus larges avec une sécurité et une commodité accrues,il a été proposé une architecture de réseau neuronal convolutif parallèle multi-échelle pour extraire des traits faciaux profonds et robustes avec une grande capacité discriminante. Des expériences abondantes sont menées sur les bases de données CMU-PIE, FERET étendue et AR.

Diaa Salama Abd Elminaam et al.[27] propose Un système complet de reconnaissance faciale (RF) utilisant l'apprentissage translationnel dans le brouillard et l'informatique en nuage. Le système avancé utilise des réseaux neuronaux convolutifs profonds

(DCNN). En raison de la représentation dominante, le DCNN es utilisé pour extraire les caractéristiques faciales pertinentes.

Auteur	Année	Travail	Méthode	Résultat
Yichen Qian et al[25]	2019	Unsupervised Face Normalization With Extreme Pose and Expression in the Wild	FNM(Face Normalization Model)	Le modèle FNM combiné à VGG-Face a atteint un taux de reconnaissance allant jusqu'à 98.4 %.
Chen Li et al[26]	2018	A Multi-Scale Parallel Convolutional Neural Network Based Intelligent Human Identification Using Face Information	MP-CNN(Multi-Scale Parallel Convolutional Neural Network)	96,61% (sur base CMU-PIE)et 95.48%(sur base FERET)et 99.46%(sur base AR)
Diaa Salama Abd Elminaam et al[27]	2020	A Deep Facial Recognition System Using Computational Intelligent Algorithms	DCNN deep convolutional neural networks	99.06%Précision sur SDUMLA-HMT, CASIA, 113 bases

TABLE 2.2 – les travaux baseés sur Visage

c.les travaux Baseés sur iris :

Kadhim et al [28] Présente Un nouveau modèle linéaire discriminant spatiotemporel synchronisé – Iris (SSLDMNet-Iris), une architecture d'apprentissage profond est présentée dans ce travail qui est conçu pour répondre aux défis associés à la reconnaissance de l'iris dans des environnements variables. Ceci a été mis en œuvre par l'extraction de la caractéristique convolutionnaire multi-échelle avec modélisation temporelle synchronisée via des unités récurrentes (GRUs), le SSLDMNet-Le modèle de l'iris peut efficacement capturer les détails complexes des textures et les motifs spatiaux globaux liés à l'iris. En outre, le modèle utilise le discriminant linéaire de Fisher (FLD) pour l'extraction des caractéristiques et l'optimisation de la séparation entre les classes tout en minimisant la variance intra-classe, augmentant ainsi la précision de reconnaissance.

Hafeez et al [29] Amélioré un système de reconnaissance de l'iris comprenant l'enregistrement d'image comme étape clé ainsi qu'une méthode de détection des arêtes pour l'extraction des caractéristiques sont proposés. La méthode PCA a également été proposée comme une méthode indépendante pour la reconnaissance de l'iris basée sur le degré de similarité.

Zhuang et al [30] Découverte Une technique efficace qui utilise un réseau neuronal convolutif (CNN) et une machine de support vectoriel (SVM) pour extraire et classer les caractéristiques respectivement pour augmenter l'efficacité de reconnaissance.

Auteur	Année	Travail	Méthode	Résultat
Kadhim et al [28]	2025	Deep Learning for Robust Iris Recognition : Introducing Synchronized Spatiotemporal Linear Discriminant Model-Iris	SSLDMNet-Iris (modèle linéaire discriminant spatiotemporel synchronisé – Iris)	SSLDMNet-Iris atteint une précision de 100% sur les ensembles de données CASIA Iris 1.0, CASIA Iris 2.0 et MMU.
Hafeez et al [29]	2022	Real-Time Human Authentication System Based on Iris Recognition	Recalage d'images + méthode de détection de contours pour l'extraction de caractéristiques + PCA (méthode proposée indépendante).	Précision jusqu'à 99,73%
Zhuang et Azam et al [30]	2020	Iris Recognition using Convolutional Neural Network	CNN + SVM(machine de support vectorie)	La méthode proposée dans cette recherche (CNN + SVM) a atteint une précision de 96,3%.

TABLE 2.3 – les travaux basées sur Iris

d.les travaux Basées sur pume de la main :

Dewi et al[31] Sont présentons une brève analyse des algorithmes de reconnaissance d'objets basés sur les réseaux de neurones convolutifs (CNN), et plus particulièrement des modèles Yolov7 et Yolov7x à 100 et 200 époques. Cette étude explore un large éventail de détecteurs d'objets, dont certains sont utilisés pour des applications de reconnaissance de positionnement de la main. De plus, nous entraînons et testons notre méthode proposée sur le jeu de données Oxford Hand à l'aide des modèles Yolov7 et Yolov7x. Des statistiques importantes, telles que le nombre de GFLOPS, la précision moyenne (mAP) et le temps de détection, sont suivies et surveillées à travers des indicateurs de performance. Nos résultats de recherche indiquent que Yolov7x à 200 époques pendant la phase d'apprentissage est l'approche la plus stable par rapport aux autres méthodes.

Al Farid et al [32] Identifier les limites des étapes de capture d'images, de segmentation et de suivi d'images, d'extraction de caractéristiques et de classification des gestes dans un système de reconnaissance des gestes de la main basé sur la vision, selon différentes orientations de caméra. Cette étude couvre les recherches menées sur les systèmes de reconnaissance des gestes de la main basés sur la vision de 2012 à 2022. Son objectif est d'identifier les axes d'amélioration et ceux nécessitant des travaux supplémentaires.

Mohammed et al [33] Développer d'un système de reconnaissance de la main capable d'extraire 21 caractéristiques de la main droite pour identifier et assigner des personnes. Le système se compose de deux parties principales : la première consiste à collecter des données, à expliquer le prétraitement de base requis et à extraire les caractéristiques géométriques de la main, telles que la longueur et la largeur des doigts, les coordonnées

de la base des doigts et la largeur de la paume, afin d'extraire les caractéristiques utilisées pour la reconnaissance. La seconde partie consiste à entraîner et à tester trois réseaux de neurones artificiels pour réaliser le processus de reconnaissance. Après avoir extrait les caractéristiques, le système utilise trois types de réseaux de neurones artificiels pour réaliser le processus de reconnaissance : les réseaux de neurones à propagation avant-arrière (NN), les réseaux de neurones d'Elman et les réseaux de neurones directs en cascade (SN).

Auteur	Année	Travail	Méthode	Résultat
Dewi et al[31]	2023	Deep Learning for Highly Accurate Hand Recognition Based on Yolov7 Model	l'ensemble de données Oxford Hand avec les modèles Yolov7 et Yolov7x.	Yolov7x Precision : 84.7%
Al Farid et al [32]	2022	A Structured and Methodological Review on Vision-Based Hand Gesture Recognition System	Reconnaissance des gestes de la main basée sur la vision	Il existe une grande variation dans la précision de l'identification, de 68% à 97%, la moyenne étant de 86,6%.
Mohammed et al [33]	2021	Biometric identity Authentication System Using Hand Geometry Measurements	Feed forward Back propagation Neural Network(NN),Elman Neural Network(NN),Cascade Forward Neural Network(NN)	Feedforward Back Propagation NN : 95%,Elman NN : 92%,Cascade Forward NN : 88%

TABLE 2.4 – les travaux baseés sur Pume de la main

2.2.2 Systèmes biométriques Multimodaux

Dans cette section, nous avons divisé les travaux relatifs selon des systèmes biométriques Multimodaux

a.les travaux Baseés sur l'empreinte digitale et iris :

mustafa et al [34] Proposent une technique de fusion décisionnelle pour la combinaison des données biométriques de l'iris et des empreintes digitales, sans aucun prétraitement. Cette approche est proposée sur la base d'une revue de la littérature existante dans ce domaine. Elle consiste à combiner les données biométriques de l'iris et des empreintes digitales à l'aide de la matrice de cooccurrence en niveaux de gris (GLCM) avec un réseau neuronal à neurones convexes (KNN) pour l'extraction des caractéristiques, la porte ET étant utilisée pour la prise de décision finale. Les résultats montrent que l'approche de fusion proposée est nettement plus performante que les approches basées sur une modalité

unique.

kamlaskar et al [35] Proposer une fusion au niveau des caractéristiques en adoptant le concept d’analyse de corrélation canonique (ACC) pour fusionner les caractéristiques de l’iris et des empreintes digitales d’une même personne. La particularité de cette approche réside dans l’extraction de caractéristiques corrélées maximisées à partir des caractéristiques des deux modalités, constituant ainsi une information discriminante efficace au sein de ces caractéristiques. Pour évaluer les performances du système proposé, les empreintes digitales de l’iris gauche et droit et du pouce des deux mains de l’ensemble de données multimodales SDUMLA-HMT sont prises en compte dans cette expérience

yadav et al [36] Présentent un algorithme d’apprentissage profond pour la reconnaissance d’un individu à l’aide des modalités biométriques de l’iris, des empreintes digitales et de la signature manuscrite. Sa structure repose sur des réseaux de neurones convolutifs (CNN), qui extraient les caractéristiques et classifient les images à l’aide d’un classificateur Softmax. Trois modèles CNN ont été combinés : un pour l’iris, un pour les empreintes digitales et un pour la signature manuscrite. Le modèle CNN a été construit selon la méthode VGG-32, la méthode d’optimisation Adam et l’entropie croisée catégorielle comme fonction de perte. Des techniques visant à éviter le surapprentissage ont été appliquées, telles que l’augmentation et la suppression d’images. Pour fusionner les modèles CNN, différentes approches de fusion ont été employées afin d’explorer leur influence sur les performances de reconnaissance. Des approches de fusion au niveau des caractéristiques et des scores ont été appliquées. Les performances du système proposé sont empiriquement évaluées grâce à plusieurs expériences menées sur le jeu de données SDUMLA-HMT, un jeu de données biométriques multimodales. Les résultats obtenus ont démontré que l’utilisation de trois traits biométriques dans les systèmes d’identification biométrique obtenait de meilleurs résultats que l’utilisation d’un ou deux traits biométriques.

Auteur	Année	Travail	Méthode	Résultat
mustafa et al [34]	2020	Multimodal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique	the Gray-Level Co-occurrence Matrix (GLCM), K-Nearest Neighbour (KNN)	accuracy de reconnaissance et de non-reconnaissance des deux classificateurs atteignait jusqu'à 90 %
yadav et al [36]	2022	A robust automatic fingerprint recognition system using multi-connection Hopfield neural network	Multi-Connection Hopfield Neural Network(MC-HNN)	accuracy Iris 98.58% ,accuracy l'empreinte digitale 98.72%
kamlaskar et al [35]	2021	Iris-fingerprint multimodal biometric system based on optimal feature level fusion model	canonical correlation analysis (CCA)	EER de 0.1050% (l'iris droit et de l'empreinte digitale gauche), EER de 1.4286% (l'iris gauche et de l'empreinte digitale droite)

TABLE 2.5 – les travaux basés sur l'empreinte digitale et iris

b.les travaux Basés sur visage et iris :

khider et al [5] présentent la conception et la mise en œuvre d'un système d'identification biométrique multimodal et hybride (multi-biométrique, multinstances, et multi-algorithme) et l'adaptation des algorithmes biométriques unimodaux, robustes et prêts à l'emploi pour un système multimodal qui intègre les points forts de ces deux modalités biométriques et d'augmenter le degré de flexibilité du système multimodal proposé et d'éliminer la limitation imposée par le trait manquant en sélectionnant un schéma de fusion approprié.

ammour et al [37] réalisée une système à l'aide d'un filtre Log-Gabor 2D multi-qui fait une résolution performant pour capturer les informations texturales à différentes échelles et orientations. Les caractéristiques faciales sont calculées à l'aide de la puissante méthode d'analyse spectrale singulière (SSA) associée à la transformée en ondelettes. L'SSA vise à décomposer les signaux ou les images en composantes interprétables et physiquement significatives. Dans cette étude, la SSA est appliquée et combinée aux caractéristiques statistiques gaussiennes inverses normales (NIG) dérivées de la transformée en ondelettes. Le processus de fusion des caractéristiques pertinentes des deux modalités est combiné à un niveau de fusion hybride. Le processus d'évaluation est réalisé sur une base de données chimérique et comprend le laboratoire de recherche Olivetti (ORL) et la technologie de reconnaissance faciale (FERET) pour le visage et la base de données d'images d'iris de l'Institut d'automatisation de l'Académie chinoise des sciences (CASIA) v3.0 (CASIA V3) pour l'iris. Les résultats expérimentaux démontrent la robustesse de cette base de données.

kadhim et al [38] Intègre des techniques de reconnaissance faciale et de l'iris pour présenter une méthodologie de reconnaissance biométrique multimodale. Le descripteur

HOG (Histogramme de Gradients Orientés) est utilisé dans le système de reconnaissance faciale pour extraire les caractéristiques faciales, tandis que le réseau de transformée par diffusion en ondelettes (WSTN) profond est appliqué dans le système de reconnaissance de l'iris pour extraire les caractéristiques de l'iris. Ensuite, pour une classification de reconnaissance personnalisée, les vecteurs de caractéristiques de chaque système de reconnaissance faciale et de l'iris sont intégrés à une régression logistique multiclasse. Ces systèmes fournissent des scores, qui sont ensuite combinés par fusion au niveau des scores afin d'optimiser l'efficacité du processus de reconnaissance humaine. La base de données multimodale réaliste (MULB) est utilisée pour évaluer les performances du système.

Auteur	Année	Travail	Méthode	Résultat
khider et al[5]	2023	Un système biométrique multimodal basé sur la fusion visage-iris	Le filtre de Gabor et le Motif binaire local (LBP) etQuantification par phase locale (LPQ)	Amélioration de la précision : de 91% (unimodal) à 98,67%. (fusion visage-iris) sur la base CASIA-Distance .
kadhim et al [38]	2024	A Multimodal Biometric System for Iris and Face Traits Based on Hybrid Approaches and Score Level Fusion	L'histogramme de gradients dirigés (HOG)et un réseau de transformée dispersive en ondelettes profondes (WSTN) et Une base de données multimédia réaliste connue sous le nom de MULB	accuracy rates of 96.45% and 95.31%, The equal error rates for the face and iris are 1.79% and 2.36% respectively.
ammour et al [37]	2020	Face-iris multimodal biometric identification system	singular spectrum analysis (SSA) ,the normal inverse Gaussian (NIG) , face recognition technology (FERET),Gabor filter,spectral regression kernel discriminant analysis (SRKDA),multi-resolution 2D Log-Gabor filter	recognition rates up to 99.16% and 99.33%

TABLE 2.6 – les travaux basées sur visage et iris

c.les travaux Basées sur l'oreille et du visage :

youbi et al [39] proposer un système de la reconnaissance de l'oreille et du visage basée sur une variante du descripteur de modèle binaire local appelé : Local Binary Pattern

multi scale (MLBP).à l'aide de City-Block distance (CTB). La méthode proposée est évaluée à partir de six bases de données de référence dont IIT Delhi I, IIT Delhi II et USTB-1 sur l'oreille et ORL, Yale et AR sur le visage

Le JURY et al [40] proposent la méthode des faces propres PCA pour le système de reconnaissance de visage et d'oreille.l'objectif est de approche d'extraction des caractéristiques géométriques basées sur un prétraitement par des filtres avec une classification basée sur les réseaux de neurones artificiel ANN.

benzaoui et al [21] Identifier un système Biométrique par Descripteurs de Texture Locaux : Application au Visage et Oreille est pour cela sont d'identifier les individus à partir des images d'intensités 2D, de visages ou d'oreilles, dans des conditions non-contrôlées.sont utiliser quatre descripteurs pour testés et comparés : LBP (Local Binary Pattern), 1DLBP (One Dimensional Local Binary Pattern), LPQ (Local Phase Quantization) et BSIF (Binarized Statistical Image Features).

Auteur	Année	Travail	Méthode	Résultat
benzaoui et al [21]	2015	Identification Bio-métrique par Descripteurs de Texture Locaux : Application au Visage et Oreille	LBP (Local Binary Pattern), 1DLBP (One Dimensional Local Binary Pattern), LPQ (Local Phase Quantization) et BSIF (Binarized Statistical Image Features)	Sommaire des travaux connexes et récents en identification des individus par visage : ORL :97% Sourire :100%,Colère :100%,cri perçant :93.24% ,avec Lunette :90.84%,Avec Echarpe :97.26% Sommaire des travaux connexes et récents en identification des individus par oreilles : Delhi-1 :98%, Delhi-2 :97.49%, USTB :98.46%
Le JURY et al [40]	2020	Identification biométrique par le visage et l'oreille	face propre PCA,apprentissage supervisé ANN	Taux de reconnaissance par Approche géométrique +ANN :83% ,Taux de reconnaissance par PCA :99,66%
youbi et al [39]	2020	Reconnaissance biométriques de personnes par le visage et l'oreille	Local Binary Pattern multi scale (MLBP),City-Block distance (CTB)	98,40% pour IIT Delhi I, 98,64% pour IIT Delhi II et 98,33% pour USTB-1, 97,90% pour ORL, 96,90% pour YALE et 99,24% pour AR.

TABLE 2.7 – les travaux basées sur l'oreille et du visage

2.3 Discussion et Analyse

En examinant les travaux antérieurs sur les systèmes biométriques, il devient clair qu'il existe des différences clés entre les systèmes unimodaux et multimodaux en termes de structure, de performances et d'applications.

Dans cette section, nous comparerons et analyserons les systèmes biométriques unimodaux et multimodaux sur la base des études précédentes que nous avons couvertes.

Les systèmes biométriques uniques s'appuient sur une seule caractéristique pour identifier les individus, comme les empreintes digitales, le visage ou la voix. Ces systèmes se caractérisent par leur conception simple, leur facilité de configuration et d'intégration dans les systèmes existants, ainsi que leur coût inférieur à celui des systèmes multibiométriques, ce qui les rend adaptés aux applications avec des budgets limités ou ne nécessitant pas une sécurité élevée. Cependant, ces systèmes souffrent de plusieurs problèmes documentés dans diverses études, notamment de faibles performances en présence d'interférences ou de mauvaise qualité des données, la possibilité de falsification ou d'usurpation d'identité et la difficulté d'identifier les changements dans les caractéristiques biométriques.

Le développement de systèmes biométriques multimodaux joue un rôle important dans le domaine de la biométrie en combinant la biométrie (empreinte digitale + visage, iris + voix, etc.). Cette combinaison améliore la précision du système et réduit considérablement les taux d'erreur. Il devient très difficile pour un attaquant d'imiter plus d'une fonctionnalité à la fois. De plus, même si une fonctionnalité échoue (par exemple, une distorsion de l'image faciale), le système peut s'appuyer sur une autre fonctionnalité (par exemple, une empreinte digitale). Malgré ces avantages, les systèmes multimodaux nécessitent des ressources plus importantes en termes de stockage et de traitement, et sont plus complexes à mettre en œuvre, ce qui limite leur utilisation à des applications spéciales ou sensibles telles que la sécurité gouvernementale ou les systèmes bancaires. Des travaux antérieurs ont montré que les systèmes multimodaux offrent de meilleures performances et une plus grande sécurité, en particulier dans les environnements qui nécessitent une grande fiabilité.

À travers cette analyse, nous constatons que les systèmes multi-biométriques représentent une évolution significative dans le domaine de la sécurité de l'identité, notamment à la lumière des défis croissants en matière de sécurité.

2.4 Dataset

Chen Li et al.[26] Des expériences abondantes sont menées sur les bases de données CMU-PIE, FERET étendue et AR

Christophe Charrier et al [22] Cette procédure a été appliquée au cas où le modèle réduit était utilisé dans les bases de données FVC (Fingerprint Verification Contest) et SFINGE.

Yichen Qian et al.[25] L'ensemble de données utilisé dans l'ensemble de visages non naturels contient 297 369 images de visages provenant de l'ensemble de données CASIA-WebFace sans contrainte, tandis que l'ensemble de visages naturels contient 5 000 images de visages (pose frontale et 20 éclairages pour 250 identités) provenant de Multi-PIE. Dans l'expérience contrainte, nous avons divisé l'ensemble d'entraînement de configuration Multi-PIE-1 en un ensemble non naturel (12 poses et 20 illuminations pour

150 identités) et un ensemble naturel (pose frontale).

Diaa Salama Abd Elminaam et al.[27] Le système proposé est évalué à l'aide de trois ensembles de données d'images faciales (SDUMLA-HMT, 113 et CASIA) à travers les mesures de performance de précision, de précision, de sensibilité, de spécificité et de temps. Les résultats expérimentaux montrent que la méthode proposée surpasse les autres algorithmes dans tous les critères.

Dewi et al[31] Les chercheurs ont formé une version test de la méthode proposée sur l'ensemble de données Oxford Hand en utilisant les modèles Yolov7 et Yolov7x. Des statistiques importantes, telles que la quantité de GFLOPS, la précision moyenne (mAP) et le temps de détection, sont suivies et surveillées via des mesures de performance.

kamlaskar et al [35] Pour évaluer les performances du système proposé, les empreintes digitales de l'iris gauche et droit et du pouce des deux mains de l'ensemble de données multimodales SDUMLA-HMT sont prises en compte dans cette expérience.

kadhim et al [38] L'ensemble de données multimodales réelles (MULB), une base de données unique que les auteurs ont collectée auprès du personnel et des étudiants de l'Université technique Al-Furat Al-Awsat de Koufa, a été utilisé pour évaluer les performances du système biométrique multimodal visage-iris proposé. En utilisant différentes proportions, nous avons réparti aléatoirement chaque sous-ensemble de données multimodales MULB en sous-ensembles d'entraînement, de validation et de test.

khider et al [5] pour évaluer l'applicabilité de la méthode proposée dans cette étude dans des environnements réels multimodal, les expériences de cette section sont réalisées sur une base de données multimodal (visage-iris) publiquement disponible appelée CASIA-Iris-Distance. La base de données complète contient un nombre total de 2567 images de 142 sujets et les images ont été acquises à une distance de 3 m de la caméra. La taille de la texture des iris extraits dans ce travail est de 240×20 . La disponibilité des différentes variations de la base de données CASIA-Iris-Distance.

Auteurs	Dataset	Résultat
Chen Li et al [26]	les bases de données CMU-PIE, FERET étendue et AR	96,61%CMU-PIE 95.48%FERET 99.46%AR
Christophe Charrier et al [22]	le modèle réduit était utilisé dans les bases de données FVC (Fingerprint Verification Contest) et SFINGE.	FVC2002DB2 AUC=0.010 et SFINGE AUC=0.029
Yichen Qian et al [25]	Ensemble de données CASIA-WebFace	Taux de reconnaissance 98.4%
Diaa Salama Abd Elminaam et al [27]	Utilisée trois ensembles de données d'images faciales (SDUMLA-HMT, 113 et CASIA)	Taux de précision 99.06%
Dewi et al[31]	Ensemble de données Oxford Hand en utilisant les modèles Yolov7 et Yolov7x	Yolov7x precision : 84.7%
kamlaskar et al [35]	les empreintes digitales de l'iris gauche et droit et du pouce des deux mains de l'ensemble de données multimodales SDUMLA-HMT sont prises	EER de 0.1050%(l'iris droit et de l'empreinte digitale gauche),EER de 1.4286%(l'iris gauche et de l'empreinte digitale droite)
kadhim et al [38]	L'ensemble de données multimodales réelles (MULB)	taux de précision de 96,45% et 95,31%
khider et al [5]	les expériences de cette section sont réalisées sur une base de données multimodal (visage-iris) publiquement disponible appelée CASIA-Iris-Distance.	Amélioration de la précision : de 91% (unimodal) à 98,67%. (fusion visage-iris)

TABLE 2.8 – Dataset

2.4.1 Discussion et Analyse de Dataset

En examinant les travaux antérieurs sur les systèmes biométriques, nous constatons que le choix de la base de données est un élément clé pour déterminer l'efficacité du modèle proposé, que ce soit dans des systèmes uniques ou multiples. Les chercheurs ont eu recours à une variété de bases de données dont la taille, le type et la qualité varient, selon la nature du système biométrique adopté.

Pour les systèmes unimodaux : Des bases de données spécialisées contenant un seul type de données, telles que CMU-PIE, Extended FERET, AR, FVC (Fingerprint Competition Verification) et SFINGE, ont été utilisées. Ces bases de données sont adaptées pour tester les performances du système dans un scénario unique, mais elles n'ont pas la capacité de simuler des scénarios multi-attributs réels. Certaines études ont montré que les performances sont considérablement affectées par les changements d'éclairage, d'angle de capture ou de qualité d'image, soulignant les limites des systèmes à attribut unique.

Pour les systèmes multimodaux : Des bases de données contenant des données biométriques combinées (par exemple, visage + empreintes digitales) ont été utilisées, telles que les bases de données CASIA Multimodal ou SDUMLA-HMT. Ces bases de données

permettent au chercheur de tester l'intégration des fonctionnalités et d'évaluer l'efficacité de la fusion.

Plusieurs études ont montré que l'utilisation de bases de données multi-fonctionnalités a contribué à augmenter la précision de la reconnaissance et à réduire les taux d'erreur, en particulier lors de la mise en œuvre de stratégies de fusion efficaces au niveau des fonctionnalités ou des décisions. Cependant, les chercheurs sont confrontés à des défis tels que la complexité du traitement, les variations de format d'image ou la nécessité d'un prétraitement supplémentaire pour unifier les données.

En analysant ces travaux, il apparaît clairement que les bases de données multi-attributs sont plus adaptées aux systèmes avancés, mais leur gestion nécessite une expertise technique plus élevée. En revanche, les bases de données uniques restent une option appropriée pour une étude initiale ou lorsque les ressources sont limitées.

Certaines études ont également créé leurs propres bases de données en raison du manque de bases de données ouvertes qui collectent de multiples caractéristiques de bonne qualité.

Le choix de la base de données dans les systèmes biométriques n'est pas seulement une question technique, mais stratégique qui affecte directement les résultats de l'étude. Par conséquent, l'analyse de la nature des données, de leur diversité, de leur qualité et de leur compatibilité avec l'objectif biométrique est l'un des points essentiels qui distingue un système efficace d'un système à l'efficacité limitée.

2.5 conclusion

à la fin de notre revue de recherche, nous avons conclu que les deux modalités biométrique (multimodaux et Unimodaux) pas assez pour la protection de système biométrique parfois elle est absente et parfois pour l'insuffisance des mécanismes, ce qui constitue un risque pour des utilisateurs, est pour cela il y a plusieurs mesures qui gèrent la performance de système. ce qui fait mettre à la nécessité de développer des systèmes biométriques multimodaux non seulement il est efficace, mais il est également capable de garantir la confidentialité, est pour cela on propose notre un système biométrique multimodal filtrer par bloom filtre .

Chapitre 3

Réalisation d'un systeme biometrique multimodel utilisant un filtre de bloom

3.1 Introduction

Les systèmes biométriques multimodaux Comme l'une des applications les plus réussies dans le domaine de l'analyse et la compréhension de l'image visage et d'empreintes digitales ,est une application intégrée qui combine l'intelligence artificielle et le traitement d'images pour gérer et identifier les identités des personnes.

3.2 Présentation du système proposée

Sybio_Blofil système biométrique multimodal basé sur la reconnaissance des empreintes digitales et la reconnaissance faciale utilisant Filter de Bloom . Le système est conçu pour combiner l'efficacité de plusieurs descripteurs tels que LBP, SSIM, HOG et les encodages faciaux afin d'assurer une identification fiable. Il intègre également un Bloom Filter pour optimiser le processus de recherche.

Lors de la reconnaissance digitale, une série d'étapes de prétraitement est appliquée à l'image (conversion en niveaux de gris, égalisation d'histogramme, filtrage gaussien), puis un descripteur LBP est utilisé pour extraire un vecteur de caractéristiques à partir de la texture locale. Ce vecteur est ensuite comparé avec ceux enregistrés à l'aide d'une mesure de similarité combinée : 60% SSIM et 40% corrélation d'histogramme.

En parallèle, la reconnaissance faciale repose sur la détection du visage via HOG, suivie de l'extraction d'un vecteur de 128 dimensions représentant les caractéristiques faciales uniques, obtenu grâce à la bibliothèque face_recognition. La comparaison se fait par distance euclidienne, avec un seuil défini pour déterminer l'identité.

Les résultats issus des deux modalités biométriques sont ensuite fusionnés sur la base d'un identifiant unique pour chaque individu. Cette fusion permet d'augmenter la robustesse et la précision du système. Pour optimiser les performances, un Bloom Filter est utilisé afin de filtrer les requêtes et limiter les comparaisons inutiles dans la base de données, réduisant ainsi le temps de traitement tout en évitant les faux négatifs.

L'architecture globale du système est illustrée dans la figure suivante, montrant les différentes étapes depuis l'acquisition des données jusqu'à la décision finale.

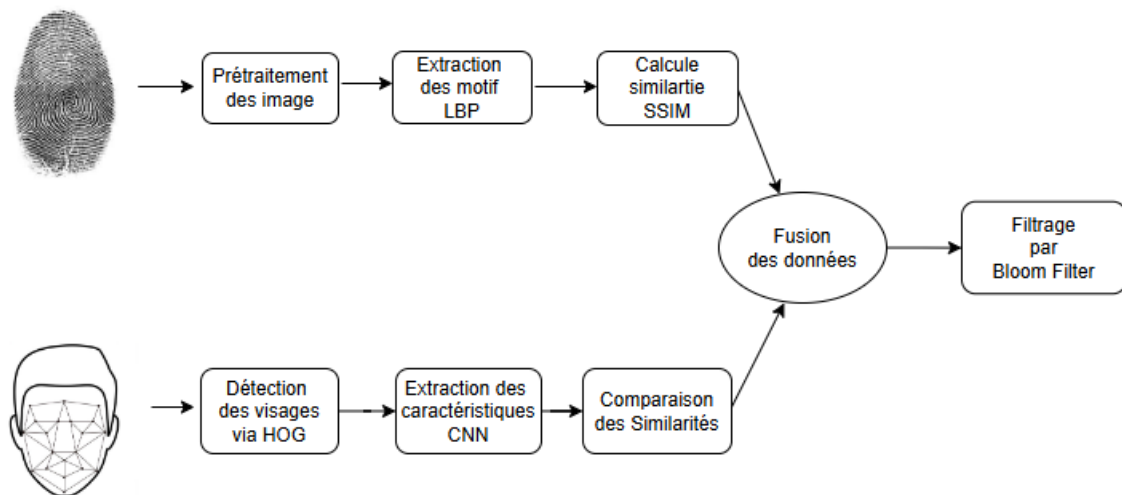


FIGURE 3.1 – Diagramme de système proposée

3.3 Environnement de travail

3.3.1 les bibliothèque de Python

1- Tkinter[41] : pour l'interface utilisateur graphique standard pour un certain nombre de langages de programmation, notamment Python, Tcl et Perl.

2- ttk : la bibliothèque ttk (Themed Tkinter) pour amélioration visuelle des composants.. Elle permet de styliser les composants standards (boutons, étiquettes, champs de texte, etc.) avec un rendu plus moderne et professionnel.

3- PIL/Pillow [42] :Le module Pillow fournit les fonctions `open()` et `show()` pour lire et afficher l'image. Pour afficher l'image, Pillow la convertit d'abord au format .png (sous Windows), la stocke dans une mémoire tampon temporaire et l'affiche pour le traitement d'images.

4- OpenCV (cv2) [43] : La bibliothèque OpenCV est une bibliothèque open source permettant de créer une architecture d'apprentissage automatique capable de suivre et de traiter des données réelles, Les applications d'OpenCV pour le traitement d'images.

5- face_recognition [44] :est une bibliothèque open source avec les dernières architectures et technologies de réseaux neuronaux profonds pour la reconnaissance faciale.

6- sqlite3 [45] : SQLite3 c'est une bibliothèque qui fourni avec le langage de programmation Python. pour la prise en charge des bases de données, qui fournit une interface SQL compatible avec DB-API 2.0. SQLite3 est un moteur de base de données léger qui

ne nécessite aucune installation ,et en utilise pour le stockage local (sans serveur) .

7- pybloom_live [46] : une bibliothèque permettant de tester efficacement l'appartenance à un ensemble pour le filtre Bloom.

8- hashlib [47] : hashlib est une bibliothèque standard de Python permettant la création de valeurs de hachage à l'aide d'algorithmes cryptographiques tels que SHA-256, utilisée pour la sécurité, et la vérification de l'intégrité des données.

9- NumPy[48] :est une bibliothèque qui Utilisé pour effectuer des calculs numériques, y compris des opérations sur des tableaux à plusieurs dimensions.

10- scikit-image [49] :est une bibliothèque qui écrivent donc du code Python, dans lequel les opérations de traitement d'images sont des fonctions scikit-image opérant sur les images. Les images sont manipulées sous forme de tableaux numériques du module NumPy, objets communs à de nombreuses bibliothèques de traitement du signal ou de visualisation (qui partagent également une interface de programmation et un style de documentation similaires).

3.3.2 les methodes

1- Local Binary Pattern (LBP) :

c'est une methode mathématique pour l'extraction des caractéristiques de la reconnaissance faciale ,Cette approche relativement nouvelle a été introduite en 1996 par Ojala et al[50].Grâce à la méthode LBP, il est possible de décrire la texture et la forme d'une image numérique. Cet opérateur fonctionne avec les huit voisins d'un pixel, en utilisant la valeur de ce pixel central comme seuil. Si un pixel voisin a une valeur de gris supérieure à celle du pixel central (ou la même valeur de gris), une valeur de 1 lui est attribuée, sinon une valeur de 0 lui est attribuée. Le code LBP du pixel central est ensuite produit en concaténant les huit uns ou zéros en un code binaire.[51]

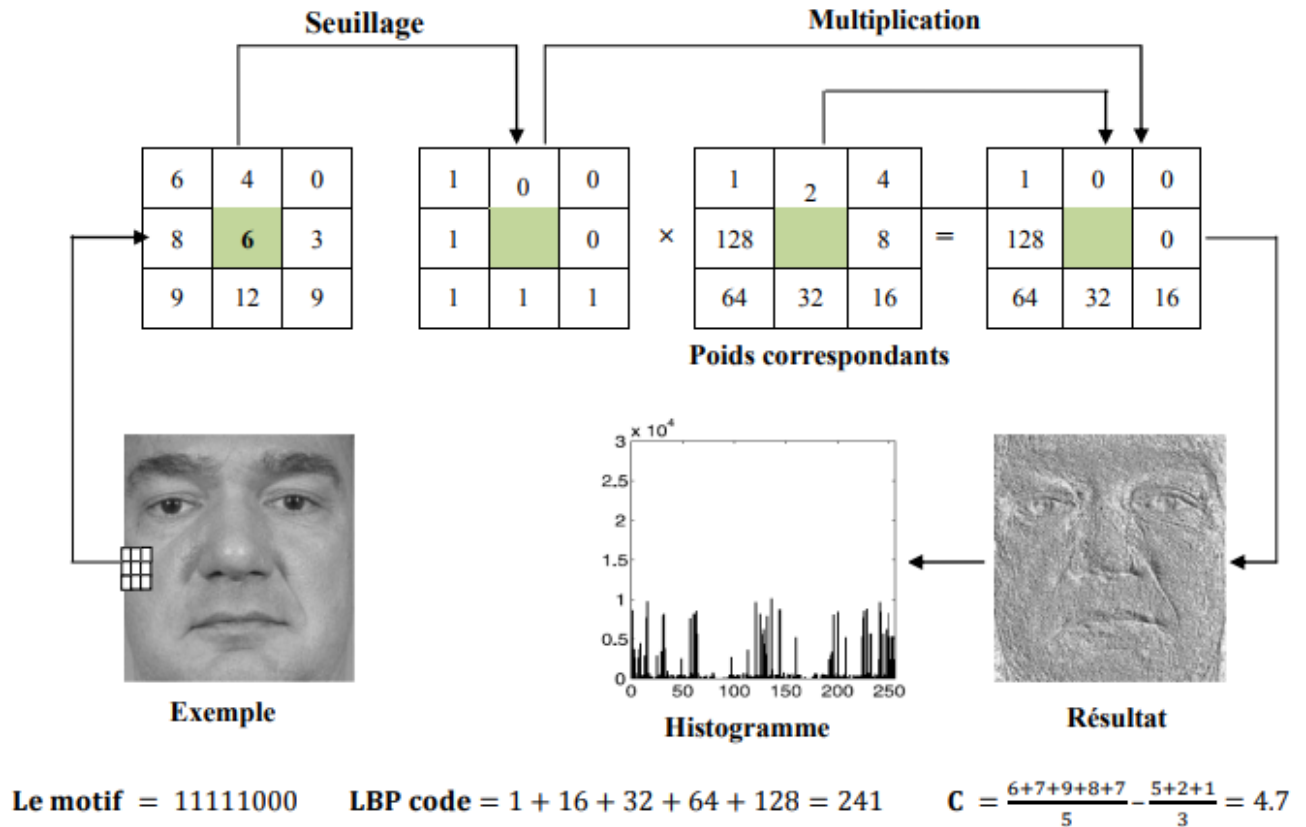


FIGURE 3.2 – LBP

2- Histogram of Oriented Gradients(HOG) :

L'histogramme de gradients orientés (HOG) est un descripteur de caractéristiques et connue utilisé pour la reconnaissance d'objets en vision par ordinateur. Il a été introduit par Navneet Dalal et Bill Triggs en 2005. HOG extrait les informations de gradient d'image locale et construit un histogramme des orientations de gradient, qui constitue un puissant descripteur de caractéristiques.[52]

Le processus d'extraction de caractéristiques HOG peut être résumé comme suit :

- 1. Prétraitement :** Conversion de l'image d'entrée en niveaux de gris.
- 2. Calcul du gradient :** Calcul des gradients horizontaux et verticaux de l'image à l'aide d'un filtre dérivé unidimensionnel, tel que le filtre dérivé du premier ordre.
- 3. Regroupement d'orientation :** Divisez l'image en petites cellules et calculez l'orientation et la magnitude du gradient pour chaque pixel de la cellule. L'orientation est quantifiée en un nombre fixe de cellules couvrant 180 degrés, et les magnitudes sont utilisées pour sélectionner les cellules d'orientation.
- 4. Normalisation par blocs :** Combinez les histogrammes des cellules voisines en blocs plus grands et normalisez ces histogrammes afin de réduire l'influence des variations d'éclairage. Le processus de normalisation consiste généralement à calculer la norme L2 de l'histogramme et à diviser chaque élément par cette norme.
- 5. Vecteur descripteur :** Concaténez les histogrammes de blocs normalisés pour former un vecteur de caractéristiques final, utilisable pour la classification ou la reconnaissance d'objets.[52]

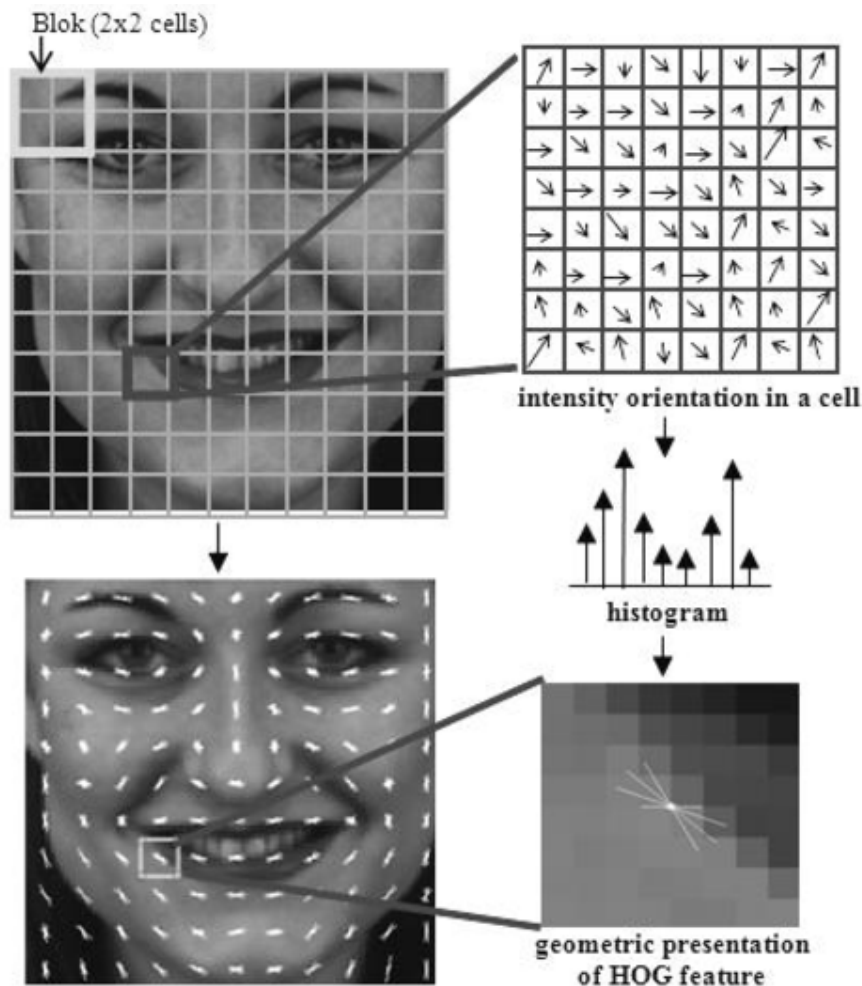


FIGURE 3.3 – Histogram of Oriented Gradients (HOG) de l'extraction de visage

3- Support Vector Machine(SVM) :

La SVM est une méthode puissante pour construire un classificateur. Elle vise à créer une frontière de décision entre deux classes permettant de prédire des étiquettes à partir d'un ou plusieurs vecteurs de caractéristiques[53], Est une techniques utilisée dans plusieurs domaine statistiques(fusion,classement,...etc.),elle été proposée par V.Vapnik en 1995. Le but de SVM (Support Vector Machine) consiste à projeter les données de l'espace d'entrée (appartenant à deux classes différentes) non-linéairement séparables dans un espace de plus grande dimension appelé espace de caractéristiques de façon à ce que les données deviennent linéairement séparables. Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la fonction de classement séparant les deux class. [54].

4- Convolutional Neural Network(CNN) :

c'est une methode qui constitués de neurones dont les pondérations et les biais sont apprenables. Chaque neurone reçoit plusieurs entrées, les additionne par une somme pondérée, les transmet à une fonction d'activation et renvoie une sortie.pour l'intégration implicite d'une phase d'extraction de caractéristiques et a été utilisé avec succès dans de nombreuses applications[55].les CNN ont des fonctionnalités telles que l'extraction de fonctionnalités les rendent plus efficaces lorsque manipulation d'images.[56]

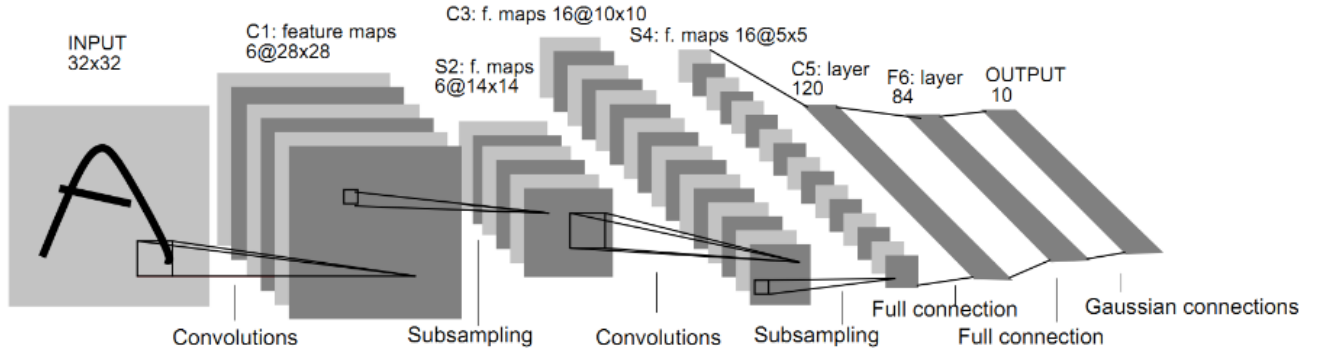


FIGURE 3.4 – Convolutional Neural Network(CNN)

5- Structural Similarity Index Measure(SSIM) :

SSIM est une mesure de similarité entre deux images numériques, elle a été développée pour mesurer la qualité visuelle d'une image compressée, par rapport à l'image originale. SSIM compare les images en trois étapes :

1. Comparaison de la luminance :

On compare la moyenne des pixels pour chaque image pour évaluer la luminosité.

2. Comparaison du contraste :

On évalue la variance des pixels pour chaque image afin de déterminer la différence de contraste.

3. Comparaison de la structure :

On compare la covariance des pixels entre les deux images pour identifier la similarité de structure et d'edges[57].

La métrique SSIM est calculée sur plusieurs fenêtres d'une image. La mesure entre deux fenêtres x et y de taille $N \times N$ est :

$$SSIM(x, y) = l(x, y) \cdot c(x, y) \cdot s(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)(cov_{xy} + c_3)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)(\sigma_x\sigma_y + c_3)}$$

avec

- μ_x la moyenne de x ;
- μ_y la moyenne de y ;
- σ_x^2 la variance de x ;
- σ_y^2 la variance de y ;
- cov_{xy} la covariance de x et y ;
- $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ et $c_3 = \frac{c_2}{2}$ trois variables destinées à stabiliser la division quand le dénominateur est très faible ;
- L la dynamique des valeurs des pixels, soit 255 pour des images codées sur 8 bits ;
- $k_1 = 0,01$ et $k_2 = 0,03$ par défaut.

3.3.3 Dataset

Dans notre projet, nous avons conçu et créé nous-mêmes une base de données biométrique multimédia, manuellement, conformément aux exigences du système.

Les données ont été saisies sur mesure via une interface graphique (GUI) développée en Python, permettant aux utilisateurs d'ajouter et d'associer leurs empreintes digitales à leurs images faciales. Les données sont stockées dans des dossiers et une base de données SQLite de manière organisée et cohérente.

Cette approche nous a permis de contrôler entièrement le processus de collecte, d'organisation et d'exploitation des données biométriques dans notre système.

Dataset de visage

Dossiers d'images (input_images) Contient les images faciales de chaque personne. Chaque image est associée à une seule personne dans la base de données.

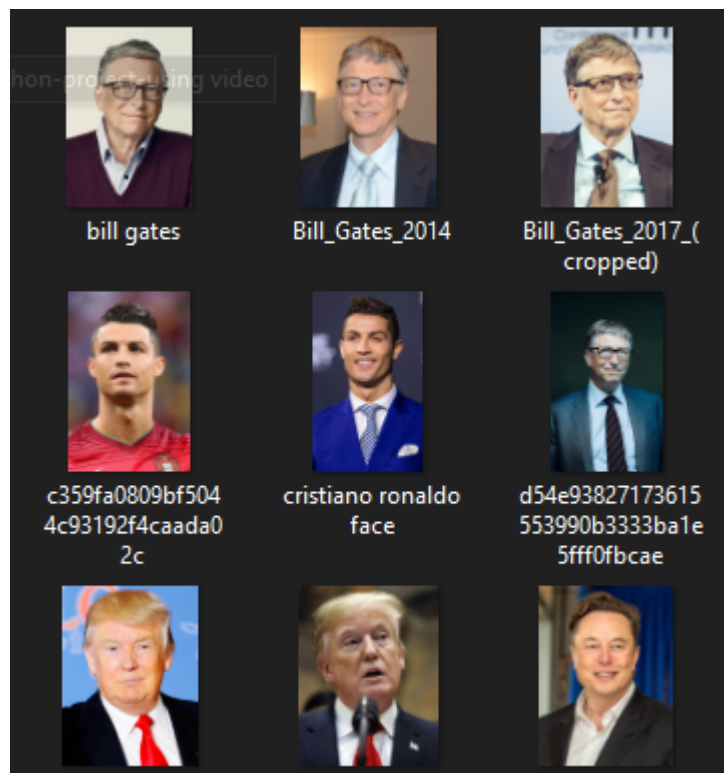


FIGURE 3.5 – Dataset de visage

Dataset d'empreinte digitale

Dossiers d'empreinte (digitaleinput_prints) Contient les images d'empreintes digitales.

Chaque image d'empreinte digitale est également associée à la même personne.



FIGURE 3.6 – Dataset d’empreinte digitale

3.3.4 langage de programmation

Python 3.8

Python est un langage de programmation le plus populaires aujourd’hui et de haut niveau. qu’il utilise une syntaxe facile à lire, traduite par l’interpréteur Python en un langage compréhensible par un ordinateur, qui fonctionne sur Microsoft Windows, Mac OS X, Linux et d’autres systèmes de type Unix [58].



FIGURE 3.7 – Python 3.8

3.4 l'implémentation

L'implémentation de notre système biométrique multimodal se base sur trois parties principales :

3.4.1 l'extraction des caractéristiques :

Chaque module suit des étapes spécifiques allant du prétraitement des données jusqu'à la comparaison des similarités.

a.l'empreinte digitale

Prétraitement des images :

Le prétraitement vise à améliorer la qualité de l'image de l'empreinte digitale pour faciliter l'extraction des caractéristiques.

- 1_ Conversion l'image d'empreintes en niveaux de gris : L'image couleur est convertie en noir et blanc pour simplifier le traitement.
- 2_Égalisation d'histogramme : Un bon contraste rend l'extraction des caractéristiques plus précise, en redistribuant les intensités des pixels que toutes les images soient comparables sur la même base .
- 3_ Filtrage Gaussien : Réduit le bruit et lisse l'image tout en préservant les détails importants.

Extraction des motifs LBP :

Local Binary Pattern (LBP) est utilisé pour capturer les motifs locaux de l'empreinte :

- 1_ Représenter la texture d'une image sous forme de motifs binaires, ce qui est particulièrement adapté à l'analyse des empreintes digitales .
- 2_ Un histogramme est créé pour représenter la distribution de ces motifs, servant de signature unique.

Calcul de similarité SSIM (Structural Similarity Index) :

Après l'extraction des caractéristiques LBP, Le SSIM mesure la similarité entre l'empreinte digitale que l'utilisateur est en train de saisir (par exemple, via un lecteur d'empreintes digitales) et l'empreinte digitale précédemment enregistrée dans la base de données lors de l'inscription initiale de l'utilisateur. ce qui permet une comparaison plus fiable :

_Score SSIM* (entre 0 et 1) :

_ Images identiques =1

_ Aucune similarité =0

_ Combinaison avec la distance d'histogramme (HISTCMP_CORREL) : 60% SSIM + 40% distance d'histogramme → Score final de similarité.

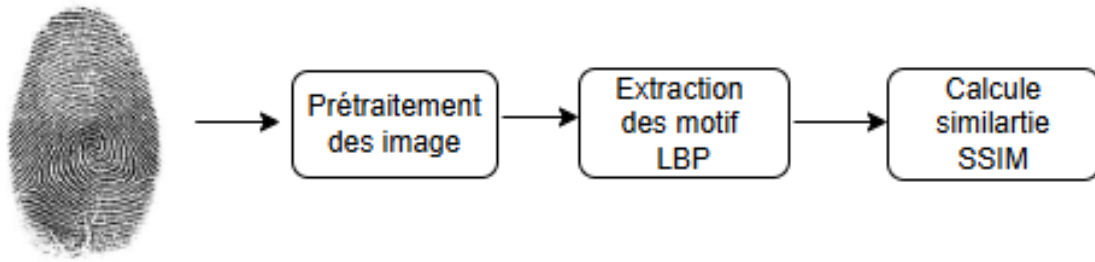


FIGURE 3.8 – Diagramme d'empreinte digitale

b.visage

Détection des Visages via HOG (Histogram of Oriented Gradients) :

- 1_Convertir l'image du visage d'entrée en niveaux de gris, en suite en Calcul des gradients pour détecter les bords et les formes de visage (Nous calculons la différence entre les pixels adjacents), après L'image est divisée en petites zones. en regroupées les cellules pour former un bloc, On normalise les histogrammes à l'intérieur du bloc, pour corriger les variations de lumière On concatène en un seul grand vecteur (le descripteur HOG).
- 2_SVM (Support Vector Machine) : classe les régions contenant des visages.

Extraction des encodages CNN :

- 1_La bibliothèque (fac_recognition)dépend de la bibliothèque (dlib) : cette dernière utilise Convolutional Neural Network(CNN) :il est utilisé pour reconnaître des visages à partir d'images ou de vidéos.
- 2_Conversion du visage en un vecteur de 128 dimensions représentant ses caractéristiques uniques comme (la distance entre les yeux, la forme du nez, la bouche, etc.).
- 3_Stockage dans une base de données pour comparaison ultérieure.

Comparaison des Similarités :

- 1_Distance Euclidienne :en calcul la distance entre les vecteurs des visages.

$$d(V1, V2) = \sqrt{\sum_{i=1}^{128} (V1_i - V2_i)^2}.$$

- 2_Seuil de reconnaissance :

- Si $d(V1, V2) < 0.6 \rightarrow$ Visage reconnu.
- Sinon $\rightarrow$ Visage inconnu
- La distance est convertie en un pourcentage de confiance(ex : 90%).

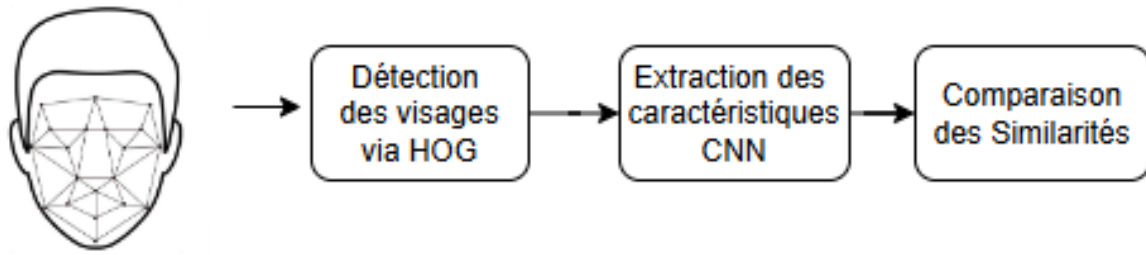


FIGURE 3.9 – Diagramme de Visage

3.4.2 la Fusion Biométrique

Cette étape consiste à combiner les caractéristiques du visage et des empreintes digitales dans un seul système biométrique.

1_ L'enregistrement des personnes : Chaque personne est enregistrée avec son visage et son empreinte digitale.

2_ Liaison via un ID unique Le visage et l'empreinte digitale sont liés par un identifiant unique (ID) pour chaque utilisateur dans la base de données.

3_ Vérification croisée : Lors du processus de reconnaissance, deux méthodes peuvent être utilisées successivement :

Étape 1 : Le visage est d'abord reconnu.

_Si une correspondance est trouvée (distance euclidienne $< 0,6$), on passe à...

Étape 2 : L'empreinte digitale est également vérifiée.

_Si l'empreinte digitale correspond à celle associée au même identifiant, l'identité est confirmée.

3.4.3 Le Filtrage par Bloom Filter

L'objectif principal d'un filtre Bloom est de réduire le nombre de comparaisons inutiles lors de la recherche d'une empreinte digitale (qu'il s'agisse d'un visage ou d'une empreinte digitale). Le système devient ainsi plus rapide et plus efficace, Réduction du temps de traitement et économie de mémoire.

- Fonctionnement :

1. Chaque empreinte est hachée (SHA-256) et stockée dans le filtre.

2. Lors d'une recherche :

- Si le filtre indique "Non présent" → L'empreinte n'existe pas (pas de fausse négative).

- Si "Peut-être présent" → Une vérification approfondie est effectuée.

```
# استدعاء مكتبة Bloom Filter
from pybloom_live import ScalableBloomFilter
import hashlib

# تهيئة مرشح بلوم داخل __init__
self.fingerprint_bloom = ScalableBloomFilter(initial_capacity=1000, error_rate=0.001)

# دالة توليد هاش للبصمة باستخدام SHA-256
def generate_fingerprint_hash(self, image_path):
    try:
        with open(image_path, 'rb') as f:
            image_data = f.read()
            return hashlib.sha256(image_data).hexdigest()
    except Exception as e:
        print(f"خطأ في توليد هاش البصمة: {str(e)}")
        return None

# أثناء إضافة بصمة شخص جديد للنظام
fingerprint_hash = self.generate_fingerprint_hash(fingerprint_path)
if fingerprint_hash:
    self.fingerprint_bloom.add(fingerprint_hash)

# أثناء التعرف على بصمة مدخلة
input_hash = self.generate_fingerprint_hash(file_path)
if input_hash in self.fingerprint_bloom:
    # يوجد احتمال أن البصمة موجودة (نمر للمقارنة الدقيقة)
    ...
else:
    # البصمة غير موجودة قطعاً (توقف المعالجة)
    self.result_label.config(text="بصمة غير معروفة", foreground='#dc3545')
```

FIGURE 3.10 – Code d'utilisation du Filter Bloom dans le système

3.5 les interfaces de L'application

3.5.1 L'enregistrement des personnes

Cette interface permet de saisir et de stocker les informations des nouveaux utilisateurs dans la base de données biométrique. Des données personnelles (telles que le nom, le numéro d'identification, etc.) sont saisies, ainsi qu'une photo faciale et une empreinte digitale.

Cette interface a pour objectif de créer une base de données précise et sécurisée contenant les informations et l'identité de chaque utilisateur.

FIGURE 3.11 – Les données personnelles

3.5.2 Galerie des utilisateurs enregistrés

Cette interface affiche la liste des utilisateurs enregistrés dans la base de données. Le visage de chaque utilisateur est affiché, ainsi que ses informations personnelles, telles que son nom, son prénom, son numéro d'identification ou toute autre information complémentaire.

Cette interface facilite la vérification visuelle des utilisateurs et permet un contrôle qualité des données saisies.

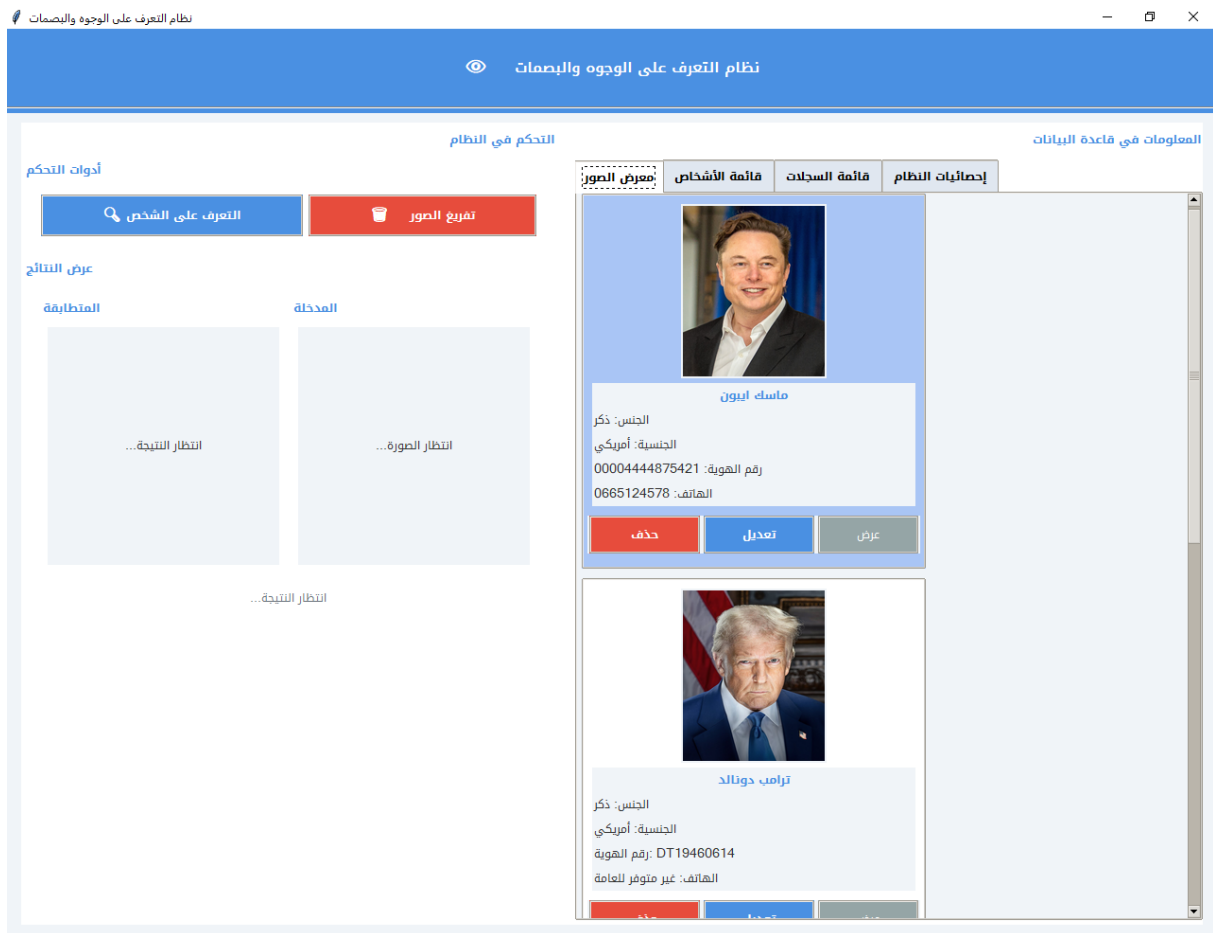


FIGURE 3.12 – Galerie

3.5.3 Affichage de la liste des utilisateurs

Cette interface affiche une liste organisée des utilisateurs enregistrés dans le système. Informations personnelles pour chaque utilisateur.

نظام التعرف على الوجوه والبصمات

المعلومات في قاعدة البيانات

التحكم في النظام

أدوات التحكم

التعرف على الشخص

تفريغ الصور

عرض النتائج

المتطابقة

المدخلة

انتظار النتيجة...

انتظار الصورة...

انتظار النتيجة...

ID	الاسم	اللقب	الجنس	الجنسية
21	ماسك	ايون	ذكر	أمريكي
17	ترامب	دونالد	ذكر	أمريكي
16	رونالدو	كريستيانو	ذكر	برازيلي
15	عيتس	بيل	ذكر	أمريكي

إضافة جديد

حذف

تعديل

بحث

FIGURE 3.13 – Affichage de la liste des utilisateurs

3.5.4 Définir L'identification des personnes.

Cette interface permet à l'utilisateur de choisir la méthode d'identification biométrique qu'il souhaite utiliser. Il peut choisir entre :

- 1_ La reconnaissance faciale.
 - 2_ La reconnaissance d'empreintes digitale.
- selon la méthode disponible.

Cette interface vise à simplifier l'utilisation et à offrir une flexibilité dans le choix de la méthode de vérification, caractéristique des systèmes biométriques multimodaux, où plusieurs méthodes peuvent être combinées pour améliorer la sécurité et la précision.

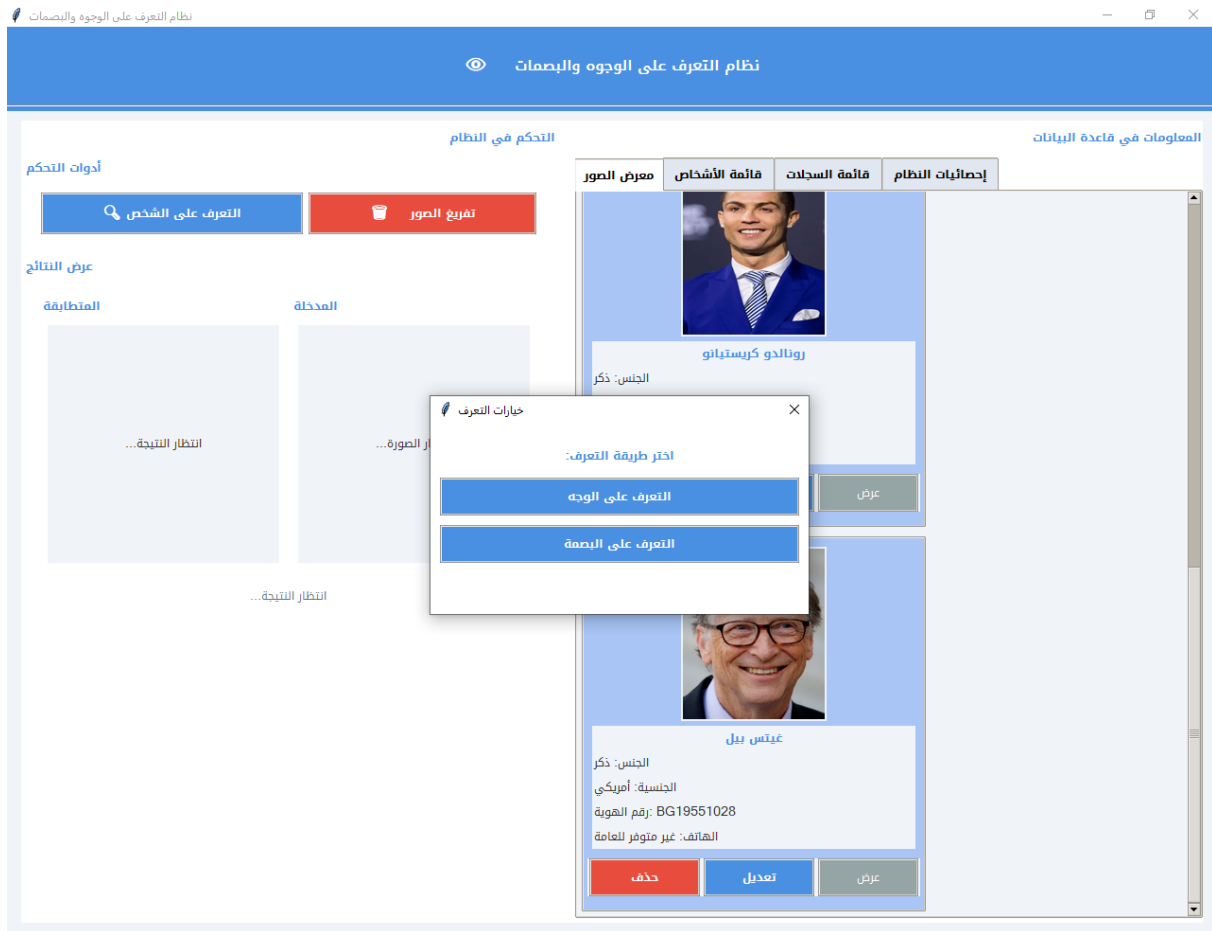


FIGURE 3.14 – L'identification des personnes

3.5.5 Reconnaissance facile

Après avoir cliqué sur “Reconnaissance faciale”, le système affiche la base de données contenant les visages enregistrés. Cette base comprend les images et les identifiants des utilisateurs. Elle sert de référence pour la comparaison avec l’image d’entrée. Cette étape assure que le système dispose d’un ensemble de données valides pour effectuer la reconnaissance.

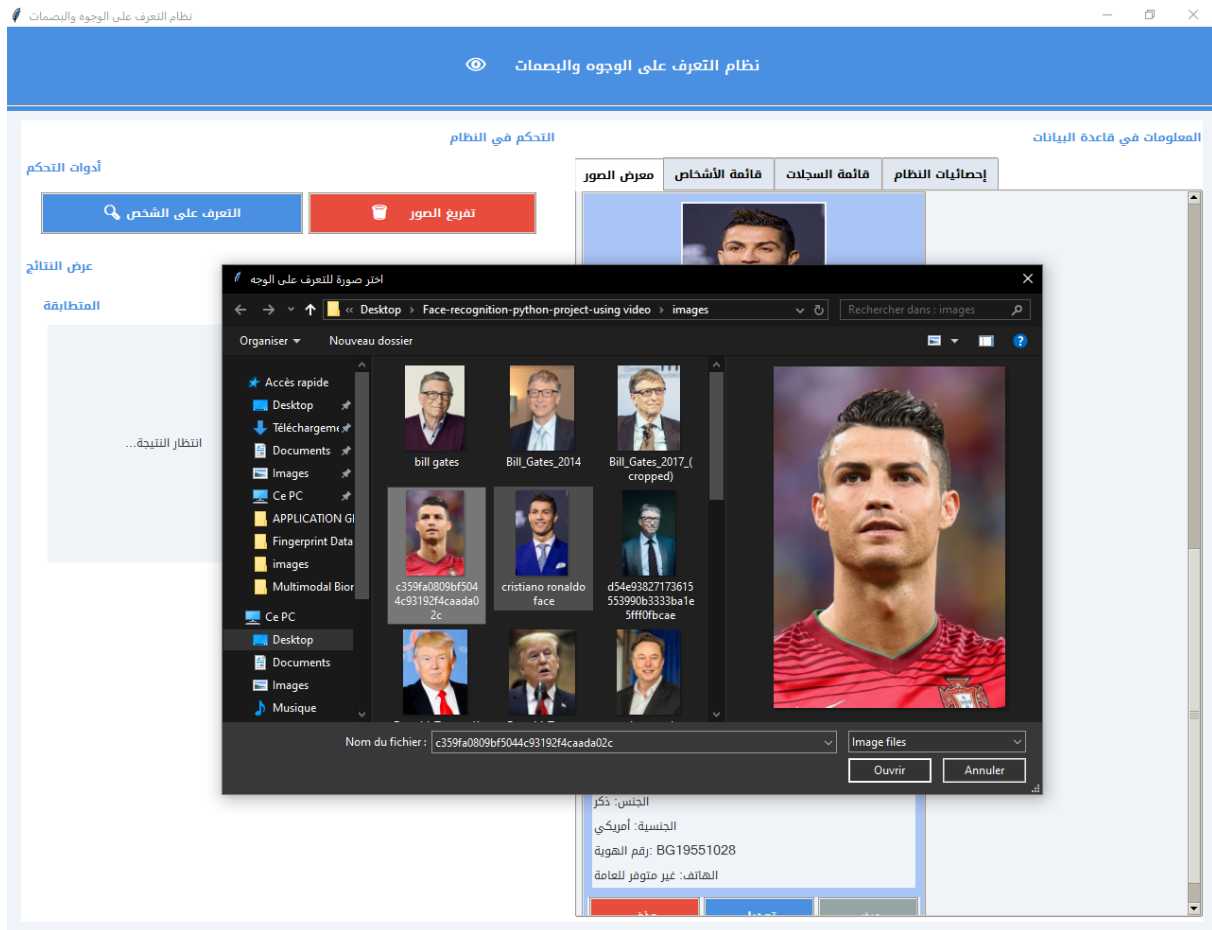


FIGURE 3.15 – Base de données contenant les visages enregistrés

3.5.6 Reconnaissance d'empreintes digitales

Lorsque vous appuyez sur le bouton "Reconnaissance d'empreintes digitales", le système affiche une base de données d'empreintes digitales précédemment enregistrées. Cette base de données contient les images d'empreintes digitales associées aux utilisateurs. Ces données sont affichées comme référence pour la comparaison avec l'empreinte digitale que l'utilisateur saisira.

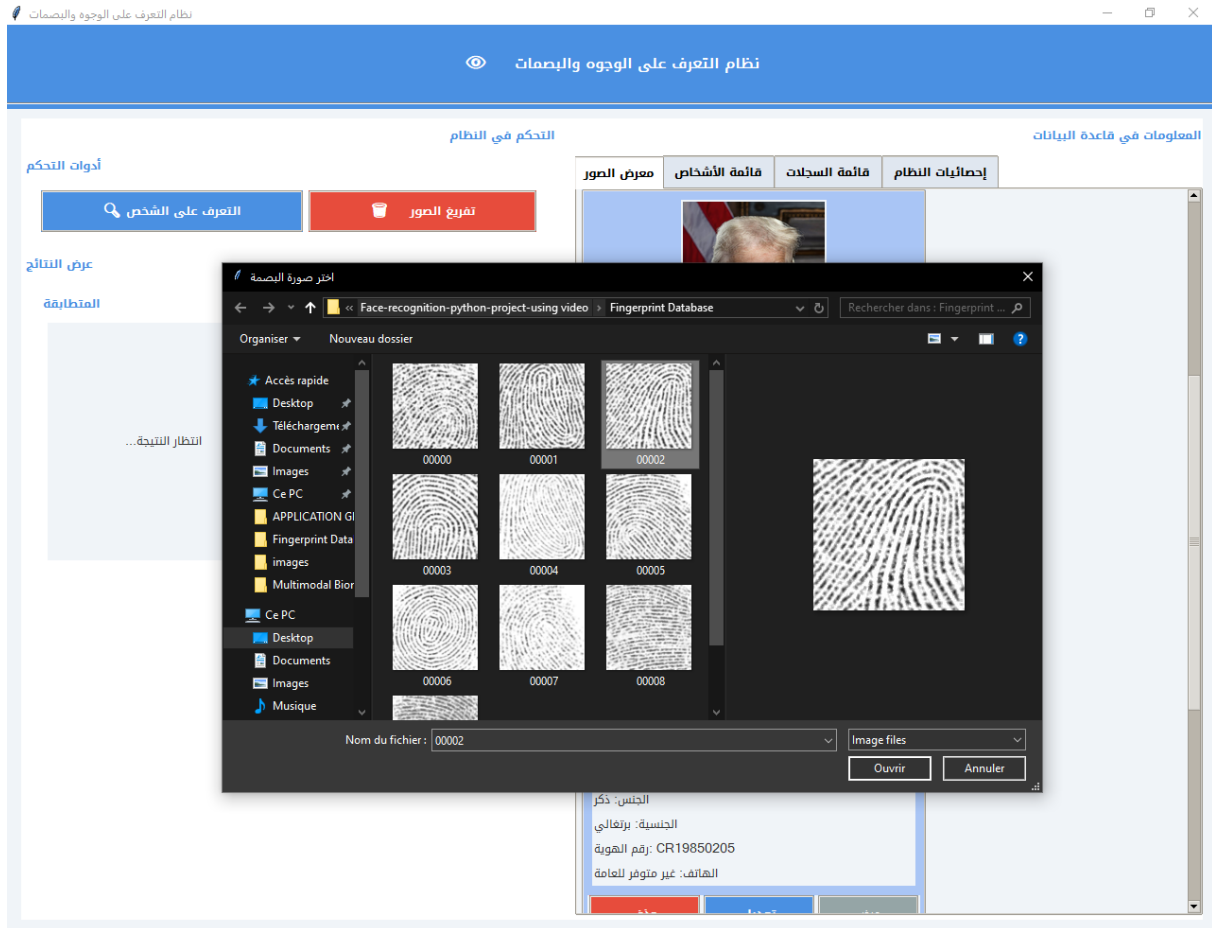


FIGURE 3.16 – Base de données d'empreintes digitales

3.5.7 Reconnaissance visage

Cette interface affiche le résultat de la comparaison entre l'image du visage fournie par l'utilisateur et celles enregistrées dans la base de données.

Si une correspondance est trouvée, les deux images (celle capturée et celle de la base) sont affichées côte à côte, accompagnées des informations de l'utilisateur identifié.

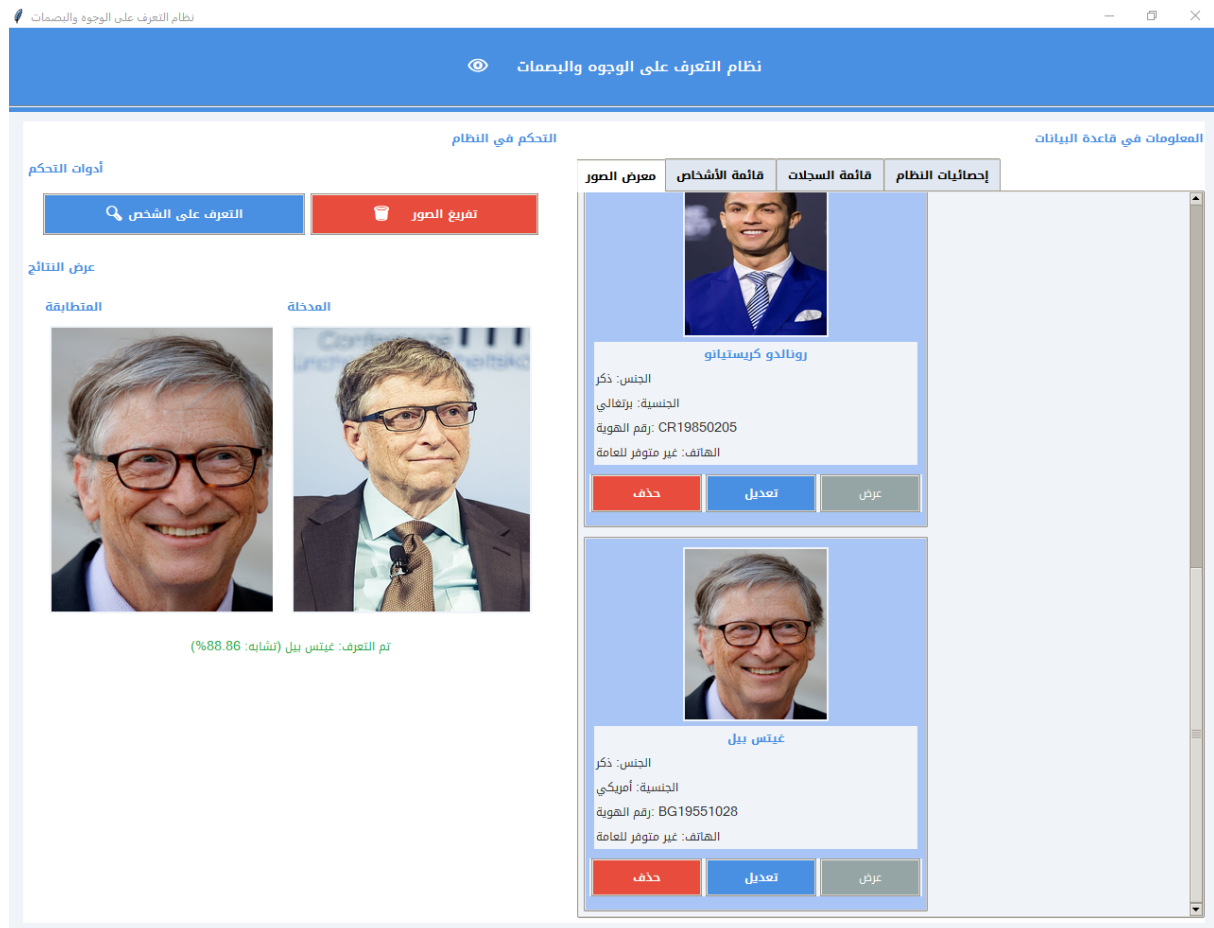


FIGURE 3.17 – Reconnaissance visage

3.5.8 Reconnaissance d'empreinte digitale

Cette interface affiche les résultats de l'identification par empreinte digitale de l'utilisateur. Après la saisie de l'empreinte, le système la compare à celles de la base de données.

Si une correspondance est trouvée, l'image de l'empreinte saisie s'affiche avec la photo (visage) et les informations personnelles de l'utilisateur.

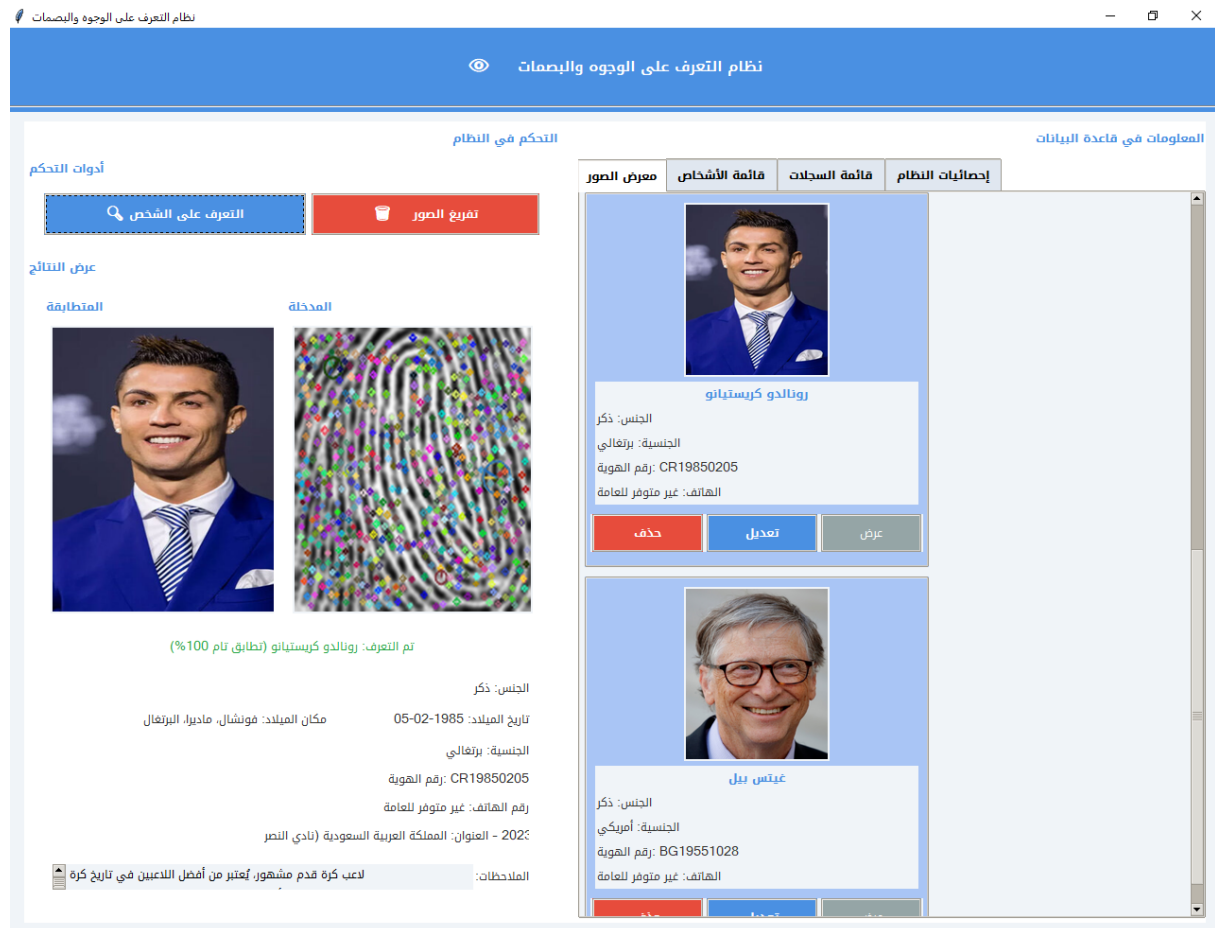


FIGURE 3.18 – Reconnaissance d'empreinte digitale

3.6 Resultat

Les résultats du système ont montré une précision acceptable dans la reconnaissance faciale et des empreintes digitales, avec un bon taux de correspondance obtenu grâce à l'utilisation du filtre Bloom [59].

3.6.1 Équations Utilisées

Pour évaluer le système biométrique, nous avons utilisé les équations suivantes :

a.Précision de reconnaissance faciale

$$\text{Précision_Visage} = \frac{1}{N_{\text{visage}}} \sum_{i=1}^{N_{\text{visage}}} C_{\text{visage},i}$$

où :

- N_{visage} : nombre total de tentatives de reconnaissance faciale effectuées.
- $C_{\text{visage},i}$: le niveau de confiance obtenu pour la $i^{\text{ème}}$ tentative de reconnaissance faciale.

b.Précision de reconnaissance d'empreintes digitales

$$\text{Précision_Empreinte} = \frac{1}{N_{\text{empreinte}}} \sum_{i=1}^{N_{\text{empreinte}}} C_{\text{empreinte},i}$$

où :

- $N_{\text{empreinte}}$: nombre total de tentatives de reconnaissance par empreinte digitale.
- $C_{\text{empreinte},i}$: le niveau de confiance obtenu pour la $i^{\text{ème}}$ tentative de reconnaissance par empreinte.

c.Précision globale du système

$$\text{Précision_Totale} = \frac{\text{Précision_Visage} + \text{Précision_Empreinte}}{2}$$

Cette équation représente la moyenne des précisions obtenues à travers les deux modalités biométriques (visage et empreinte digitale).

3.6.2 Résultats Totales

Malgré le nombre limité d'utilisateurs et notre dépendance totale aux données générées par nos sions dans des conditions réelles, le système a un taux de précision de 64.80%.

	Précision
Précision moyenne de la reconnaissance faciale	66.56%
Précision moyenne de la reconnaissance d'empreintes digitale	63.04%
Précision totale du système	64.80%

3.6.3 Les statistiques du système

Le système comprend une interface permettant d'afficher des statistiques graphiques sur les processus de reconnaissance, calculant l'évolution de la précision de la reconnaissance faciale et d'empreintes digitales sur une période donnée.

Ces valeurs sont affichées sous forme de graphique, ce qui permet de comprendre l'efficacité du système au fil du temps.

L'image ci-dessous présente un exemple de courbe illustrant l'évolution de la précision de la reconnaissance sur plusieurs mois.

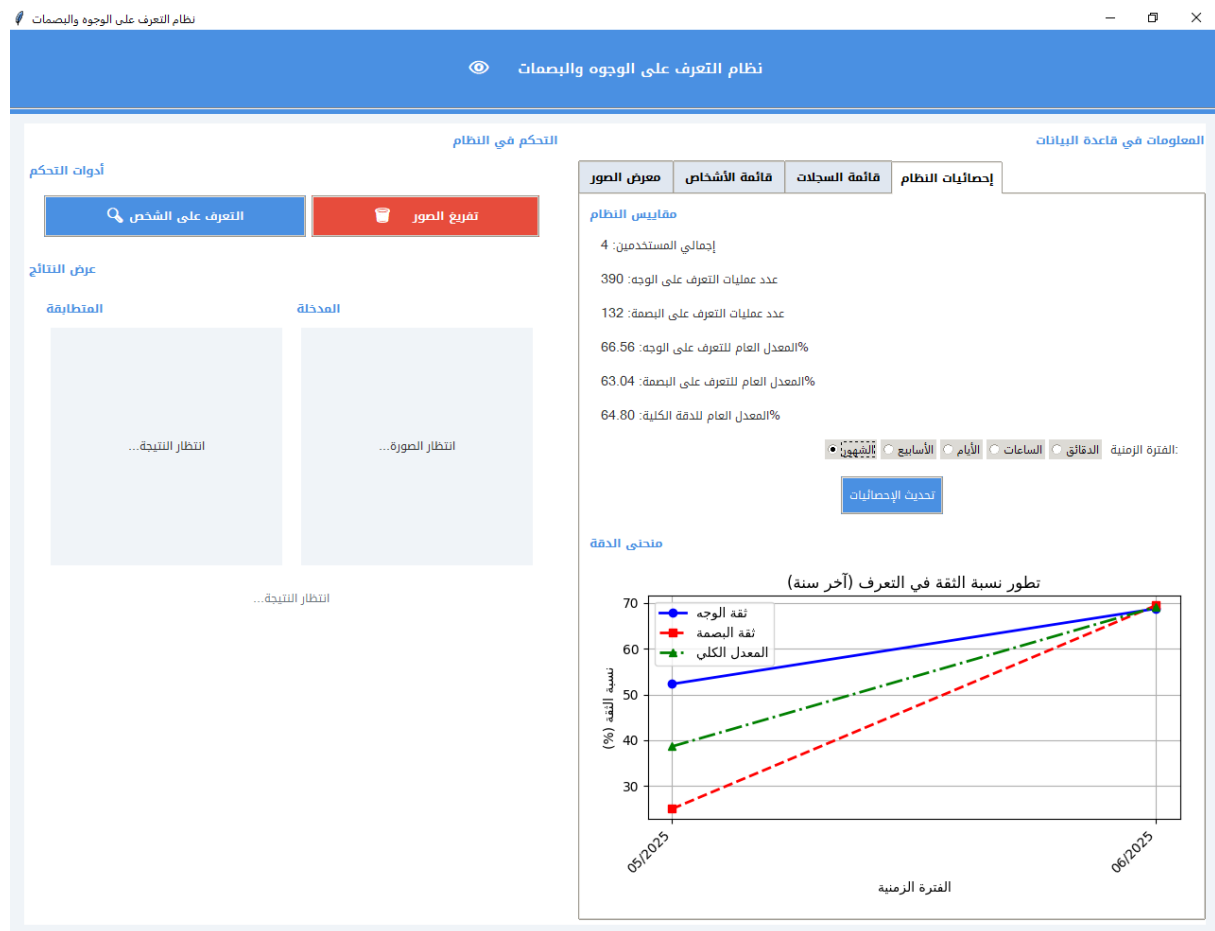


FIGURE 3.19 – la précision de la reconnaissance sur plusieurs mois

3.6.4 Résultats d'interface

Un test a été réalisé à partir d'une image d'empreinte digitale originale extraite de la base de données. Le système l'a reconnue dans 100% des cas, démontrant une correspondance parfaite.

Lorsqu'une image du visage de la même personne était saisie, mais sous un angle d'éclairage différent, le système l'a reconnue dans 88% des cas, démontrant la flexibilité de l'algorithme de reconnaissance faciale malgré les modifications.

Type de données	Résultat
Empreinte digitale	100%
Visage	88.86%

TABLE 3.1 – Résultat

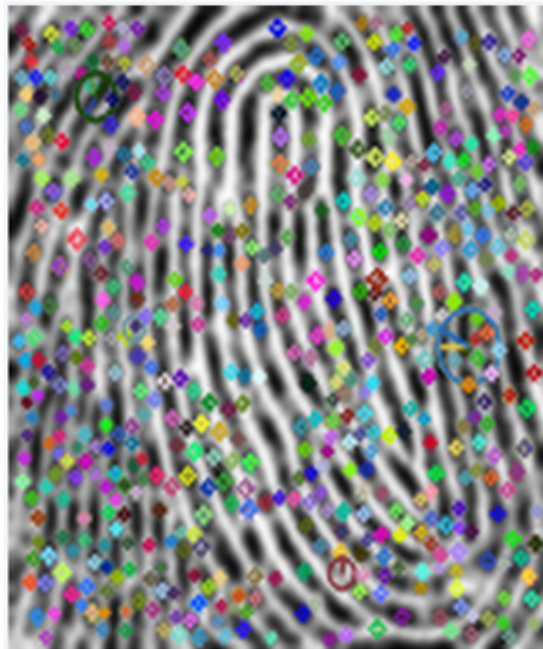
La reconnaissance d'empreinte digitale montre l'empreinte digitale et le visage el le pourcentage est de 100%.

عرض النتائج

المتطابقة



المُدخلة



تم التعرف: رونالدو كريستيانو (تطابق تام 100%)

FIGURE 3.20 – La reconnaissance d'empreinte digitale

La reconnaissance faciale affiche les deux visage avec taux de reconnaissance de 88%.

عرض النتائج

المتطابقة



المدخلة



تم التعرف: غيتس بيل (تشابه: 88.86%)

FIGURE 3.21 – La reconnaissance de visage

3.7 conclusion

Nous avons présenté, tout au long de ce chapitre, les détails concernant la réalisation de notre travail . Dans la première section, nous avons citter l'environnement de travail (les bibliothèque, les methodes,dataset,longage de programmation) .en suite l'implementation qui visier (l'extraction des caractéristique,la fusion,filtrage par bloom filer),et a la fin le resultat ,pour la reconnaissance d'un individu par leur visage et leur empreinte digitale qui utilise bloom filter pour Accélérer le processus.

Conclusion Générale

les systèmes biométriques représentent une réponse technologique innovante et efficace. Le système biométrique multimodal que nous avons développé, combinant la reconnaissance faciale et la reconnaissance d'empreintes digitales, s'inscrit dans cette dynamique d'innovation. En associant ces deux modalités, notre système vise à surmonter les limites des approches unimodales, notamment en termes de précision, de fiabilité et de résistance aux tentatives de fraude.

L'importance de notre travail réside dans sa capacité à offrir une identification unique, robuste et efficace des individus. En exploitant simultanément les caractéristiques biométriques du visage et des empreintes digitales, nous augmentons la fiabilité du processus d'authentification. Cette combinaison permet de compenser les faiblesses éventuelles d'une modalité par la force de l'autre, assurant ainsi un niveau de sécurité bien plus élevé. De telles avancées sont particulièrement pertinentes dans les domaines de la sécurité des accès, de la surveillance intelligente, ou encore dans des secteurs sensibles comme les aéroports, les institutions gouvernementales, et les systèmes bancaires.

Par ailleurs, l'intégration d'un filtre de Bloom dans notre approche représente une amélioration significative sur le plan de la gestion de données biométriques. Ce mécanisme permet un stockage optimisé et une vérification rapide des données, tout en préservant un bon compromis entre performance, sécurité et consommation de ressources. Ce choix technique ouvre la voie à des implémentations à grande échelle, dans des environnements nécessitant une réactivité accrue.

Néanmoins, malgré les résultats prometteurs obtenus, plusieurs défis subsistent. Il s'agit notamment de la gestion des données sensibles, du respect de la vie privée, des risques de falsification biométrique, et de l'adaptation à des environnements variés et dynamiques. Ces défis représentent autant d'opportunités pour de futures recherches et développements.

Nous espérons que cette étude contribuera à enrichir les travaux existants dans le domaine de la biométrie multimodale et qu'elle servira de base pour des recherches futures. Ces recherches pourraient porter, par exemple, sur l'intégration de nouvelles modalités biométriques (iris, voix, comportement), l'amélioration des algorithmes de fusion, ou encore la mise en œuvre de techniques avancées de protection des données.

En conclusion, notre système biométrique multimodal représente un pas important vers une sécurité renforcée, aussi bien dans le monde réel que dans le cyberspace. Les implications futures sont nombreuses et prometteuses, notamment en ce qui concerne l'amélioration de la cybersécurité, la protection des données personnelles et la fiabilisation des systèmes d'identification et de vérification.

Bibliographie

- [1] FaceOnLive, “Faceonlive - face recognition technology solutions.” <https://www.faceonlive.com>, 2025. Accessed : 2025-04-21.
- [2] SecurityForceNow, “Securityforcenow - cybersecurity news and updates.” <https://www.securityforcenow.com>, 2025. Accessed : 2025-04-21.
- [3] Innovatrics, “Biometric system - definition, faqs,” 2025. Accessed : May 2, 2025.
- [4] C. Medjahed, A. Rahmoun, C. Charrier, and F. Mezzoudj, “A deep learning-based multimodal biometric system using score fusion,” *IAES Int. J. Artif. Intell.*, vol. 11, no. 1, p. 65, 2022.
- [5] A. Khider, *Un système biométrique multimodal basé sur la fusion visage-iris*. PhD thesis, 2023.
- [6] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, “Face recognition systems : A survey,” *Sensors*, vol. 20, no. 2, p. 342, 2020.
- [7] D. Mahjabeen and M. R. Tarafder, “Unique authentication for door lock system through bio scanning-finger print security system,” *GSJ*, vol. 9, no. 10, 2021.
- [8] Innovatrics, “Fingerprint biometrics - definition, faqs,” 2025. Accessed : 2025-05-02.
- [9] Wikipedia contributors, “Speech recognition.” https://en.wikipedia.org/wiki/Speech_recognition, 2024. Accessed : 2025-05-06.
- [10] S. Rechache, “Face attributes classification based on deep neural network,” mémoire de master professionnel, Université Kasdi Merbah Ouargla, Ouargla, Algérie, 2022. Spécialité : Administration et Sécurité des Réseaux.
- [11] R. V. Yampolskiy and V. Govindaraju, “Behavioural biometrics : a survey and classification,” *International Journal of Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.
- [12] GeeksforGeeks, “Biometric system architecture,” 2022. Accessed : 2025-04-14.
- [13] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, “Comprehensive survey : Biometric user authentication application, evaluation, and discussion,” *arXiv preprint arXiv :2311.13416*, 2024.
- [14] RecFaces, “Two main types of biometrics : Physical vs. behavioral biometrics,” 2024. Consulté en avril 2025.
- [15] R. A. Hamaamin, O. M. A. Ali, and S. W. Kareem, “Biometric systems : A comprehensive review,” *Basrah Journal of Sciences*, vol. 42, no. 1, pp. 146–167, 2024.
- [16] A. Siagh and S. Bennouna, *Convolutional Autoencoder for distorted facial images recognition*. PhD thesis, UNIVERSITE KASDI MERBAH OUARGLA.
- [17] K. Nguyen, H. Proença, and F. Alonso-Fernandez, “Deep learning for iris recognition : A survey,” *ACM Computing Surveys*, vol. 56, no. 9, pp. 1–35, 2024.

- [18] S. Trabelsi, D. Samai, F. Dornaika, A. Benlamoudi, K. Bensid, and A. Taleb-Ahmed, "Efficient palmprint biometric identification systems using deep learning and feature selection methods," *Neural Computing and Applications*, vol. 34, no. 14, pp. 12119–12141, 2022.
- [19] K. Chachadi and S. Nirmala, "Voice-based gender recognition using neural network," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020) ICT : Applications and Social Interfaces*, pp. 741–749, Springer, 2021.
- [20] F. Boussad and R. R. Boussa, *Développement d'un système biométrique multimodal basé sur la fusion des scores de matching*. PhD thesis, Université Mouloud Mammeri, 2020.
- [21] A. BENZAOUI, *Identification Biométrique par Descripteurs de Texture Locaux : Application au Visage & Oreille*. PhD thesis, 2015.
- [22] C. CHARRIER, "Evaluation de la confiance des minuties d'une empreinte digitale,"
- [23] J. K. P. S. Yadav, L. Singh, and Z. A. Jaffrey, "A robust automatic fingerprint recognition system using multi-connection hopfield neural network," *Traitement du Signal*, vol. 39, no. 2, p. 683, 2022.
- [24] N. Ali *et al.*, "Fingerprint recognition," in *IOP Conference Series : Materials Science and Engineering*, vol. 928, p. 032078, IOP Publishing, 2020.
- [25] Y. Qian, W. Deng, and J. Hu, "Unsupervised face normalization with extreme pose and expression in the wild," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 9851–9858, 2019.
- [26] C. Li, M. Liang, W. Song, and K. Xiao, "A multi-scale parallel convolutional neural network based intelligent human identification using face information," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1494–1507, 2018.
- [27] D. Salama AbdELminaam, A. M. Almansori, M. Taha, and E. Badr, "A deep facial recognition system using computational intelligent algorithms," *Plos one*, vol. 15, no. 12, p. e0242269, 2020.
- [28] S. Kadhim, J. K. S. Paw, Y. C. Tak, S. Ameen, and A. Alkhayyat, "Deep learning for robust iris recognition : Introducing synchronized spatiotemporal linear discriminant model-iris," 2025.
- [29] H. Hafeez, M. N. Zafar, C. A. Abbas, H. Elahi, and M. O. Ali, "Real-time human authentication system based on iris recognition," *Eng*, vol. 3, no. 4, pp. 693–708, 2022.
- [30] Y. Zhuang, J. H. Chuah, C. O. Chow, and M. G. Lim, "Iris recognition using convolutional neural network," in *2020 IEEE 10th International Conference on System Engineering and Technology (ICSET)*, pp. 134–138, IEEE, 2020.
- [31] C. Dewi, A. P. S. Chen, and H. J. Christanto, "Deep learning for highly accurate hand recognition based on yolov7 model," *Big Data and Cognitive Computing*, vol. 7, no. 1, p. 53, 2023.
- [32] F. Al Farid, N. Hashim, J. Abdullah, M. R. Bhuiyan, W. N. Shahida Mohd Isa, J. Uddin, M. A. Haque, and M. N. Husen, "A structured and methodological review on vision-based hand gesture recognition system," *Journal of Imaging*, vol. 8, no. 6, p. 153, 2022.
- [33] H. H. Mohammed, S. A. Baker, and A. S. Nori, "Biometric identity authentication system using hand geometry measurements," in *Journal of Physics : Conference Series*, vol. 1804, p. 012144, IOP Publishing, 2021.

- [34] A. S. Mustafa, A. J. Abdulelah, and A. K. Ahmed, "Multimodal biometric system iris and fingerprint recognition based on fusion technique," *International Journal of Advanced Science and Technology*, vol. 29, no. 03, pp. 7423–7432, 2020.
- [35] C. Kamlaskar and A. Abhyankar, "Iris-fingerprint multimodal biometric system based on optimal feature level fusion model," *AIMS Electronics and Electrical Engineering*, vol. 5, no. 4, pp. 229–250, 2021.
- [36] A. K. Yadav, "Deep learning approach for multimodal biometric recognition system based on fusion of iris, fingerprint and hand written signature traits," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 1627–1640, 2021.
- [37] B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face-iris multimodal biometric identification system," *Electronics*, vol. 9, no. 1, p. 85, 2020.
- [38] O. N. Kadhim, M. H. Abdulameer, and Y. M. H. Al-Mayali, "A multimodal biometric system for iris and face traits based on hybrid approaches and score level fusion," in *BIO Web of Conferences*, vol. 97, p. 00016, EDP Sciences, 2024.
- [39] Z. Youbi, *Reconnaissance biométriques de personnes par le visage et l'oreille*. PhD thesis, 2020.
- [40] D. Le JURY, *Intitulé : Identification biométrique par le visage et l'oreille*. PhD thesis, UNIVERSITE BADJI MOKHTAR ANNABA, 2020.
- [41] Q. Charatan and A. Kans, "Python graphics with tkinter," in *Programming in Two Semesters : Using Python and Java*, pp. 211–254, Springer, 2022.
- [42] GeeksforGeeks, "Python pillow tutorial," 2024. Accessed : 2025-05-27.
- [43] Y. Patil, M. Paun, D. Paun, K. Singh, and V. K. Borate, "Virtual painting with opencv using python," *International Journal of Scientific Research in Science and Technology*, vol. 5, no. 8, pp. 189–194, 2020.
- [44] B. Amos, B. Ludwiczuk, M. Satyanarayanan, *et al.*, "Openface : A general-purpose face recognition library with mobile applications," *CMU School of Computer Science*, vol. 6, no. 2, p. 20, 2016.
- [45] A. Verma and B. Sharma, "Dynamic e-certificate designing with automatic mailing system using python and sqlite3," *Journal of Applied Information Science*, vol. 10, no. 2, 2022.
- [46] D. G. Dommeti, "Network traffic analysis and alerting system,"
- [47] D. Kartinah, "Konsep blockchain python dengan penggunaan flask hashlib," *Jurnal Teknik dan Science*, vol. 3, no. 2, pp. 107–111, 2024.
- [48] P. Gupta and A. Bagchi, *Essentials of Python for Artificial Intelligence and Machine Learning*. Springer, 2024.
- [49] E. Gouillart, J. Nunez-Iglesias, F. Boulogne, and S. van der Walt, "Analyzing tomography data with python and the scikit-image library," 2017.
- [50] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern recognition*, vol. 29, no. 1, pp. 51–59, 1996.
- [51] M. A. Rahim, M. N. Hossain, T. Wahid, and M. S. Azam, "Face recognition using local binary patterns (lbp)," *Global Journal of Computer Science and Technology*, vol. 13, no. 4, pp. 1–8, 2013.

- [52] M. M. Bouchene, “Bayesian optimization of histogram of oriented gradients (hog) parameters for facial recognition,” *The Journal of Supercomputing*, vol. 80, no. 14, pp. 20118–20149, 2024.
- [53] S. Huang, N. Cai, P. P. Pacheco, S. Narrandes, Y. Wang, and W. Xu, “Applications of support vector machine (svm) learning in cancer genomics,” *Cancer genomics & proteomics*, vol. 15, no. 1, pp. 41–51, 2018.
- [54] S. BEGGARI and K. KHAMRA, “Système de reconnaissance de visage par un réseau de neurone convolutionnel (cnn),” 2017.
- [55] S. NECIB, “Fusion de face 3d couleur, profondeur et profil pour srv3d,” Master’s thesis, 2013.
- [56] M. Zeghlache, “facial recognition using convolutional neural networks,” 2019.
- [57] Wikipédia contributors, “Indice de similarité structurelle – wikipédia.” https://fr.wikipedia.org/wiki/Structural_Similarity, 2024. Page consultée le 29 mai 2025.
- [58] Webucator, *Introduction to Python 3.8*. Webucator, 2020. Version : PYT138.1.1.2.
- [59] A. K. Jain, K. Nandakumar, and A. Ross, “Score normalization in multimodal biometric systems,” *Proceedings of the 3rd International Conference on Audio-and Video-based Biometric Person Authentication (AVBPA)*, 2005.