REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

UNIVERSITE DE YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

DEPARTEMENT DE GENIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

DEPARTMENT OF COMPUTER SCIENCE

Points sur les algorithmes de reconnaissance faciale

Membres

- **22P035 :** MBETSI DJOFANG AIME LINDSEY
- **22P105 :** NANTIA ZAGUE AXEL FRISKYL
- **22P067 :** NGUEMO VOUFO AURELLE SANDRA

Niveau : 4 CIN

Superviseur

M. MINKA MI NGUIDJOI Thierry Emmanuel

Année Scolaire : 2025–2026

Table des matières

Introduction

La reconnaissance faciale est une technologie d'intelligence artificielle permettant d'identifier ou de vérifier l'identité d'une personne à partir de ses traits du visage. Elle repose sur des algorithmes capables de détecter, d'analyser et de comparer des caractéristiques faciales uniques (par exemple la distance entre les yeux, la forme du nez, les contours de la mâchoire ou des lèvres). Ces algorithmes sont largement utilisés dans divers domaines : sécurité (vidéosurveillance, contrôle d'accès), téléphonie mobile (déverrouillage de smartphones), réseaux sociaux (étiquetage automatique de photos), etc. Toutefois, leur utilisation soulève des enjeux éthiques et juridiques importants (protection des données personnelles, respect de la vie privée).

En tant qu'investigateur numérique, la reconnaissance faciale représente un outil stratégique dans les enquêtes judiciaires et la cybersécurité. Elle permet de traiter rapidement de grands volumes d'images et de vidéos souvent collectés dans des contextes sensibles (surveillance de lieux publics, preuves numériques extraites d'appareils saisis, etc.) pour identifier ou confirmer l'identité de personnes. Ainsi, la présentation de cette technologie ne se limite pas à la description technique des algorithmes : elle intègre aussi une réflexion sur leur efficacité opérationnelle, leurs limites face aux tentatives de dissimulation ou d'usurpation, et sur leur utilisation responsable dans le respect des cadres juridique et éthique en vigueur.

1 Présentation de la reconnaissance faciale

La reconnaissance faciale (RF) est une technique biométrique qui utilise le visage d'une personne comme trait biométrique. Elle est très répandue du fait que le visage est une modalité biométrique non intrusive et facile à acquérir. Bien que la RF soit populaire, elle présente également des limites.

1.1 Mode de fonctionnement d'un système biométrique

Un système biométrique fonctionne en trois phases principales : l'enrôlement, l'identification et la vérification. Lors de l'enrôlement, l'utilisateur est inscrit pour la première fois : sa modalité biométrique (le visage) est capturée, prétraitée, et les caractéristiques pertinentes en sont extraites puis stockées dans une base de données. Des informations biographiques peuvent être associées à ce profil.

En mode identification, un individu se présente au système sans révéler explicitement son identité ; le système cherche alors parmi tous les profils enrôlés le plus proche par correspondance (recherche 1-N).

En vérification (authentification), l'utilisateur affirme une identité, et le système compare les caractéristiques extraites à son modèle enregistré (recherche 1-1). Si le score de similitude est supérieur à un seuil, l'identité est confirmée.

1.2 Architecture d'un système biométrique

Un système biométrique peut se schématiser par quatre modules :

1. **Capture / Acquisition :** module responsable de la capture des données (par exemple une caméra ou un scanner).
2. **Extraction de caractéristiques :** module qui transforme les données capturées en une représentation mathématique pertinente (vecteur de caractéristiques).
3. **Correspondance :** module qui compare le vecteur extrait aux modèles stockés en base (issus de l'enrôlement) pour évaluer la similitude.
4. **Décision :** module qui confirme ou non l'identité de l'utilisateur à partir du score obtenu.

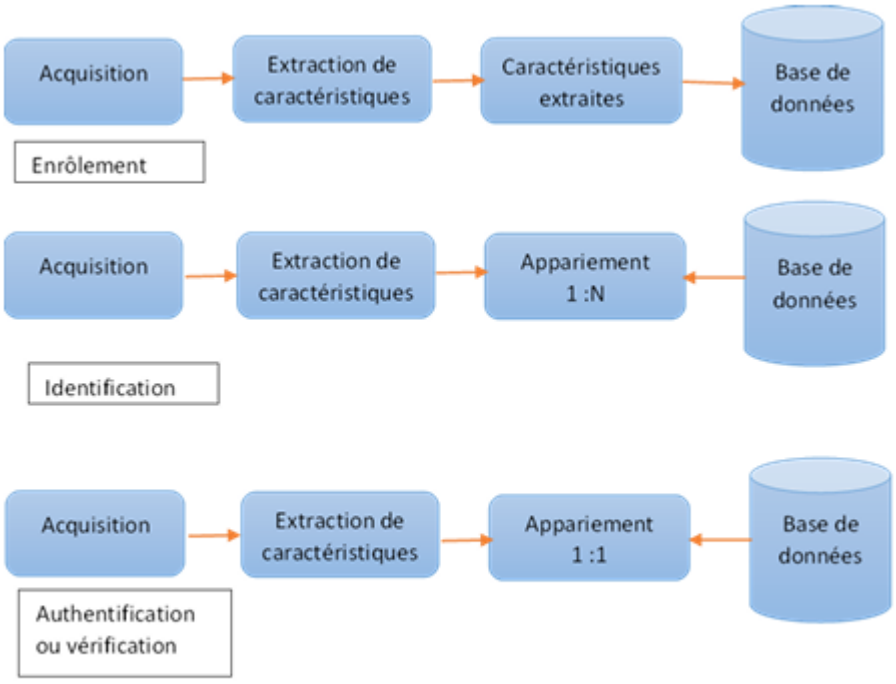

Figure 1.2- Mode de fonctionnement d'un système biométrique

2 Méthodes de reconnaissance

De nombreux algorithmes ou méthodes sophistiqués sont utilisés en reconnaissance faciale. On distingue généralement trois catégories principales : les méthodes classiques (statistiques ou analytiques), les détecteurs et descripteurs de points d'intérêt, et les méthodes d'apprentissage automatique (machine learning) et profond (deep learning).

2.1 Méthodes classiques

Les méthodes classiques interviennent lors des étapes d'extraction de caractéristiques, de correspondance et de décision. On peut classer ces méthodes en :

- **Méthodes globales :** elles utilisent l'ensemble du visage comme source d'information, sans se focaliser sur des traits particuliers. Ces méthodes sont relativement rapides mais sensibles aux variations d'illumination, de pose ou d'expression. Exemples d'approches globales : l'Analyse en Composantes Principales (PCA ou Eigenfaces), l'Analyse Discriminante Linéaire (LDA), les Machines à Vecteurs de Support (SVM), les Réseaux de Neurones, les Modèles de Mélange de Gaussiennes (GMM), les modèles 3D de surfaces faciales, etc.
- **Méthodes locales (traits géométriques) :** elles extraient des caractéristiques à partir de régions spécifiques du visage (yeux, nez, bouche) et utilisent leur géométrie ou leur apparence comme données. Elles réduisent le bruit (cheveux, lunettes, etc.), mais sont sensibles aux changements de vue. Exemples de méthodes locales : les Modèles de Markov Cachés (HMM), l'algorithme Elastic Bunch Graph Matching (EBGM), la méthode Eigen Object (EO), et l'appariement de gabarits (template matching).
- **Méthodes hybrides :** elles combinent des approches globales et locales (ou plusieurs classificateurs) afin d'unir leurs avantages. Par exemple, on peut fusionner un modèle de deep learning (reconnaissance globale) avec des descripteurs locaux robustes (SIFT, HOG, etc.) pour améliorer la résilience du système.

2.2 Détecteurs et descripteurs de points d'intérêt

Les détecteurs de points d'intérêt identifient des pixels ou régions clés dans l'image (discontinuités, motifs particuliers). Un descripteur génère ensuite un vecteur numérique décrivant la région autour de chaque point détecté. Ce vecteur doit être discriminant et le plus invariant possible (transformation, illumination). En reconnaissance faciale, plusieurs détecteurs/descripteurs sont populaires : par exemple SIFT, ASIFT, MSER, HOG, KAZE, SURF, parmi d'autres.

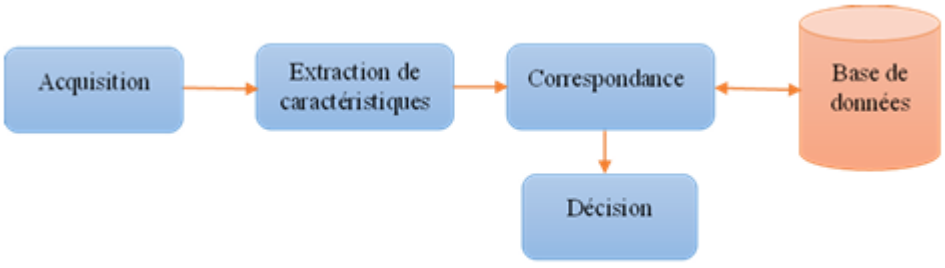

Figure 1.1- Architecture d'un système biométrique

3 Avantages et inconvénients

L'évaluation d'un système de reconnaissance faciale ne peut se limiter à sa performance technique brute. Pour un investigateur numérique, il faut considérer à la fois les atouts opérationnels et les

risques potentiels (fiabilité, biais, questions légales). Les avantages concernent surtout la rapidité, l'automatisation et la capacité à traiter de vastes volumes de données visuelles. En revanche, des faiblesses techniques, organisationnelles, sécuritaires, éthiques ou juridiques peuvent compromettre la fiabilité ou la légalité des résultats, entraînant des erreurs ou des contestations.

3.1 Fondements techniques

Fonctionnement général (Point fort) : Les algorithmes de reconnaissance faciale automatisent l'identification et la vérification en extrayant des caractéristiques faciales (points clés, embeddings) et en les comparant très rapidement à des bases de référence. Cela permet, par exemple, de rechercher des suspects ou de repérer des apparitions de personnes sur des heures de vidéo.
Limite : L'automatisation peut masquer des erreurs systématiques ; il est nécessaire de vérifier manuellement les résultats critiques.

Architecture "boîte noire" (Point faible) : De nombreux modèles (deep learning) présentent des architectures complexes et propriétaires. Pour l'investigateur, cela complique l'explication des correspondances, l'évaluation des biais et la reproductibilité des résultats.
Conséquence : Il faut exiger documentation et traçabilité (schéma d'architecture, versions de modèles, logs) et idéalement des éléments reproductibles pour valider les preuves.

Performance (vitesse et précision) (Point fort) : En conditions contrôlées, ces algorithmes peuvent atteindre une très haute précision et rapidité, ce qui est précieux pour traiter de grandes quantités de données (heures de vidéo).
Limite : En conditions réelles (faible luminosité, angles extrêmes, masques), la performance chute. L'investigateur doit tester le système sur des cas représentatifs avant de se fier aux résultats.

Interopérabilité (Point faible) : Les solutions sont souvent cloisonnées (formats propriétaires, embeddings non standard, API fermées), rendant difficile l'agrégation de preuves provenant de systèmes différents.

3.2 Sécurité et vulnérabilités

Attaques adversariales et piratage (Point faible) : Les modèles et bases de données peuvent être visés par des attaques (injections adversariales, exfiltration de données, modification des entrées). L'investigateur doit assurer l'intégrité des données : des preuves altérées compromettent toute analyse.

Protection des données biométriques (Point faible) : Les images et templates faciaux sont hautement sensibles : une fuite est irréversible (on ne change pas de visage). La chaîne de conservation des preuves (chain of custody) doit être scrupuleuse, ce qui est souvent un point faible en pratique.

Anti-usurpation (Point faible) : Des manipulations (deepfakes, photos imprimées, masques 3D, attaques de replay) peuvent tromper certains systèmes. En investigation, une correspondance seule n'est pas suffisante : elle doit être recoupée (géolocalisation, logs, témoins, etc.).

3.3 Impact éthique et sociétal

Vie privée (Point faible) : Surveiller des personnes sans consentement (caméras dans l'espace public, bases biométriques) porte atteinte à la vie privée et aux libertés civiles. L'investigateur doit évaluer la nécessité et la proportionnalité de l'usage.

Discrimination et biais (Point faible) : Les modèles entraînés sur des données déséquilibrées peuvent avoir des taux d'erreur plus élevés pour certaines catégories (ethnie, genre, âge). Cela peut conduire à de fausses accusations ciblant des groupes vulnérables.

Effet dissuasif (Point faible potentiel) : Savoir qu'on est filmé ou analysé modifie les comportements (« chilling effect »). L'utilisation généralisée peut affecter la liberté d'expression et de manifestation. Ces impacts sociaux doivent être mesurés, en particulier dans les contextes publics.

3.4 Enjeux juridiques

Conformité légale (Point faible) : Dans la plupart des pays, la collecte et le traitement des données biométriques requièrent une base légale (consentement éclairé, mandat judiciaire, intérêt public). Sans base légale, toute preuve peut être contestée en justice.

Responsabilité (Point faible) : En cas d'erreur (fausse identification, biais), déterminer la responsabilité (fournisseur du système, opérateur, État) est complexe. L'investigateur doit documenter précisément les décisions et paramètres utilisés.

Supervision et traçabilité (Point faible/fort) : Un système bien encadré (autorisations claires, registre d'accès, historique des traitements) est défendable en justice ; en l'absence de ces garde-fous, le système devient vulnérable juridiquement.

3.5 Impacts organisationnels et opérationnels

Coûts et maintenance (Point faible) : Installer et maintenir un système de reconnaissance faciale demande du matériel adapté (caméras, serveurs, GPU), des licences logicielles et une formation adéquate. Ces coûts peuvent être sous-estimés et menacer la pérennité du projet.

Infrastructure (Point faible) : Un système performant nécessite un stockage massif, des GPU pour l'inférence, et un réseau rapide. Sans cela, la latence et la perte de qualité nuisent à l'efficacité en investigation.

Acceptabilité (Point faible) : Le public et le personnel peuvent résister (méfiance, peur des erreurs). L'acceptabilité sociale et institutionnelle est cruciale : un opérateur mal formé ou un public hostile peuvent compromettre l'efficacité du système.

3.6 Finalité et contexte d'usage

Objectif légitime (Point fort/faible) : L'objectif du système doit être proportionné. Par exemple, identifier un suspect dangereux sous mandat est légitime (atout), tandis que la surveillance généralisée d'une population pour le contrôle social est abusif (risque).

Proportionnalité (Point faible si ignorée) : Les bénéfices doivent compenser les risques. En pratique, cette analyse est souvent inexistante : les erreurs et atteintes potentielles ne sont pas toujours justifiées par un gain concret.

Légitimité de l'usage (Point faible si contestée) : La légitimité sociale dépend du cadre légal, de la transparence et de la supervision démocratique. Sans cela, l'utilisation est vulnérable aux contestations publiques et judiciaires.

4 Recommandations

Face aux atouts et aux risques identifiés, plusieurs mesures d'encadrement sont proposées pour le contexte camerounais. Ces recommandations visent à renforcer les performances techniques, assurer la conformité juridique, la fiabilité opérationnelle, réduire les biais et protéger les données. Elles s'adressent aux autorités, aux forces de l'ordre et aux acteurs techniques ou judiciaires concernés, afin de favoriser un déploiement maîtrisé et responsable de la reconnaissance faciale.

4.1 Fondements techniques (pipeline, architectures, données)

- **Documenter le pipeline :** Garder à jour un schéma d'architecture, les versions des modèles, le format des embeddings et les étapes de prétraitement. Cela facilite la reproductibilité et l'expertise judiciaire.
- **Tests locaux (benchmarks) :** Réaliser des tests de précision et de latence sur des jeux de données locaux (diverses carnations, éclairages, accessoires) avant une utilisation opérationnelle.

— **Pipelines hybrides :** Combiner modèles profonds et descripteurs classiques (SIFT, HOG) ainsi que des règles pré-traitement pour améliorer la robustesse aux conditions locales.

4.2 Sécurité et vulnérabilités

— **Pentests réguliers :** Programmer des tests d'intrusion incluant des attaques adversariales et corriger les vulnérabilités critiques ; conserver les rapports signés.
— **Anti-spoofing multi-sensoriel :** Intégrer des contrôles de « liveness » (capteurs IR/3D, angles multiples) et enregistrer les sessions vidéo pour valider les captures contestées.
— **Protection des templates :** Chiffrer les modèles biométriques au repos et en transit, séparer les clés et appliquer des accès restreints avec journalisation immuable.

4.3 Impact éthique et sociétal

— **Étude d'impact (DPIA) :** Réaliser et publier une étude d'impact sur la vie privée avant tout déploiement public ; définir clairement les finalités et durées de conservation des données.
— **Audits de biais :** Mesurer la performance par sous-groupes (ethnie, âge, genre) ; corriger ou suspendre les usages si des biais significatifs sont détectés.
— **Communication et recours :** Informer le public concerné (affichage de panneaux, procédures d'information) et mettre en place un mécanisme clair de plainte et de recours.

4.4 Enjeux juridiques et conformité

— **Base légale :** Vérifier la légalité du traitement (consentement explicite, mandat judiciaire, intérêt public restreint) ainsi que les obligations de conservation des données sous contrôle de l'autorité nationale.
— **Cadre réglementaire :** Aligner la pratique sur la loi n°2024/017 (Données personnelles) et tenir un registre des activités. Effectuer une DPIA et préparer les dossiers d'enregistrement auprès de l'ANPD ou équivalent.
— **Usages sensibles :** N'utiliser la reconnaissance faciale pour identification ciblée qu'avec mandat judiciaire ou justification écrite (documentée par la sécurité publique).
— **Clauses contractuelles :** Inclure dans les contrats avec les fournisseurs des SLA, la traçabilité des versions de modèles et des clauses de responsabilité/indemnisation.

4.5 Impacts organisationnels et opérationnels

— **Plan budgétaire (TCO) :** Budgéter le matériel adapté (GPU, stockage sécurisé), les licences logicielles et assurer des formations régulières certifiées pour opérateurs et experts judiciaires.
— **Procédures opérationnelles (SOP) :** Définir les procédures (lancement d'une recherche, seuils de confiance, validation de mise en production) et mettre en place des preuves d'intégrité (hash, horodatage).
— **Pilote restreint :** Déployer d'abord sur un périmètre limité (aéroport, poste de police) avec des indicateurs de performance (KPI) et des revues avant extension.

4.6 Finalité et proportionnalité (contexte d'usage)

— **Nécessité :** S'assurer que l'usage est strictement nécessaire et proportionné (par exemple, viser un suspect dangereux sous mandat est justifié).
— **Documenter la finalité :** Exiger pour chaque projet une finalité précise, une durée maximale et des métriques démontrant l'utilité réelle.

— **Validation humaine :** Imposer qu'aucune décision critique (arrestation, poursuite) ne soit fondée sur la seule sortie automatique ; exiger une validation humaine et des recoupements.
— **Arrêt ou suspension :** Définir les conditions et procédures pour suspendre ou retirer le système en cas de dérive, de plaintes massives ou de biais irréparables.

Conclusion

La reconnaissance faciale est aujourd'hui un outil technologique puissant pour l'investigation numérique, permettant d'exploiter rapidement de vastes volumes d'images et de vidéos dans des contextes sécuritaires, judiciaires ou de prévention. Toutefois, son efficacité réelle dépend de nombreux facteurs : la fiabilité des algorithmes, l'intégrité des données, les infrastructures disponibles, le cadre juridique en vigueur, la proportionnalité des usages et le respect des droits humains.

Sans encadrement clair, audits techniques, transparence et gouvernance adaptée, cette technologie peut générer des dérives graves : faux positifs judiciaires, atteintes à la vie privée, discriminations, contestations légales ou défiance sociale. En revanche, lorsqu'elle est contrôlée, contextualisée et accompagnée de procédures rigoureuses, la reconnaissance faciale peut devenir un atout majeur pour les enquêtes judiciaires et la cybersécurité.

Ainsi, la mise en œuvre d'un cadre juridique actualisé, d'une supervision technique continue et d'une utilisation proportionnée est la condition essentielle pour concilier sécurité, innovation et respect des droits fondamentaux au Cameroun.