



ARTICLE DE RECHERCHE

Article Info.:

Reçu : le 04/02/2026

Accepté: le 16/02/2026

Publié : le 16/02/2026

INTEGRATION DE LA RECONNAISSANCE FACIALE 2D/3D ET DE LA GEOLOCALISATION DANS UNE ARCHITECTURE IOT POUR L'IDENTIFICATION AUTOMATIQUE DES AUTEURS D'INFRACTIONS ROUTIERES

Helene Kankolongo Malula ^{2,*}, Yannick Tshibengabu Tshimanga ¹, Rostin Mabela Matondo ¹, Eugene Mbuyi Mukendi ¹

<https://doi.org/10.70237/jafrisci.2026.v3.i2.04>

Resumé

Dans les zones urbaines des pays en développement, voir croître les infractions routières est un problème épineux pour les autorités publiques, vu la précarité des dispositifs de surveillance. Dans cet article, un système intelligent de reconnaissance faciale 2D / 3D, de géolocalisation et une architecture distribuée IoT sont proposés pour identifier automatiquement ceux qui contribuent par leur acte à la croissance des infractions. L'approche vise à augmenter la précision d'identification, la traçabilité spatio-temporelle et l'automatisation de la gestion des infractions par des solutions intelligentes. Dans l'architecture proposée, les modèles d'apprentissage automatique interviennent principalement au niveau de la reconnaissance faciale 2D/3D pour l'extraction des caractéristiques biométriques, ainsi qu'au niveau décisionnel pour la fusion intelligente des informations biométriques, géospatiales et cinématiques, tandis que des modèles légers sont déployés en périphérie pour l'optimisation du prétraitement des données. Les résultats démontrent une amélioration significative de la précision d'identification et du temps de traitement. Le système constitue une solution innovante et reproductible pour les infrastructures routières intelligentes. La méthodologie inclut une revue approfondie de la littérature, une modélisation théorique, l'implémentation d'un prototype basé sur des modules embarqués (ESP32-Cam, GPS) et un backend FastAPI, ainsi que des tests en conditions réelles dans la ville de Kananga.

Mots clés : Reconnaissance faciale, Géolocalisation GPS, Internet des Objets (IoT), Biométrie 2D/3D, Infractions routières, Systèmes intelligents

Abstract

Increase in road traffic violations in cities is a serious problem for the public authorities, especially in developing countries where systems of surveillance are deficient. This work presents an intelligent system that offers automated enforcement of road violations by integrating 2D/3D face recognition with geofence and distributed IoT. The objective of this approach is to enhance precision in identifying infringements, spatio-temporal traceability, and automation of infringement handling. According to this architecture, machine learning models are applied at two levels of work, i.e., 2D/3D facial recognition level for the purpose of biometric feature extraction and decision-making level for intelligent fusion between biometric information with geospatial and kinematic data; while lightweight models operate on edge side in order to improve data preprocessing. The results demonstrate a significant improvement in identification accuracy and processing time. The system represents an innovative and reproducible solution for intelligent road infrastructures. The methodology includes an in-depth literature review, theoretical modeling, implementation of a prototype based on embedded modules (ESP32-Cam, GPS) and a FastAPI backend, as well as real-world testing in the city of Kananga.

Key words : Facial Recognition, GPS Geolocation, Internet of Things (IoT), 2D/3D Biometrics, Road Traffic Violations, Intelligent Systems

1. Introduction

L'augmentation rapide du trafic routier et des comportements dangereux sur la voie publique rend essentiel le développement de solutions technologiques innovantes capables de renforcer les capacités des autorités en matière de

surveillance et de gestion des infractions[1, 2].

Les approches traditionnelles, souvent basées sur des interventions humaines ponctuelles, montrent leurs limites en termes de précision, de réactivité et de couverture opérationnelle. L'intégration de la biométrie faciale, de la

géolocalisation et de l'IoT ouvre de nouvelles perspectives pour les systèmes de transport intelligents[3, 4].

Cette recherche présente une solution qui combine ces trois domaines pour permettre une identification automatisée, rapide et fiable des auteurs d'infractions, contribuant ainsi à réduire l'impunité et améliorer la sécurité routière.

2. Travaux connexes

Les recherches en biométrie faciale ont évolué depuis les approches globales (PCA, LDA) jusqu'aux approches modernes basées sur le deep learning. Les méthodes 3D offrent une robustesse accrue face aux variations de pose et d'éclairage. Parallèlement, les systèmes de géolocalisation (GPS, GSM, RFID, Wi-Fi) ont été largement intégrés dans les smart cities. Toutefois, peu de travaux combinent biométrie, géolocalisation et IoT dans un système unifié.

Deng et al, dans leur étude sur la reconnaissance faciale basée sur les réseaux de neurones convolutifs profonds, notamment ArcFace, proposent un modèle visant à améliorer la séparabilité inter-classes et à réduire la confusion entre identités proches. La contribution clé de ce travail réside dans l'introduction d'une fonction de perte angulaire permettant d'obtenir des représentations faciales hautement discriminantes. Cependant, la principale limite de cette approche demeure sa sensibilité aux variations de pose, d'éclairage et de conditions d'acquisition non contrôlées, en particulier dans des environnements dynamiques[5].

De leur côté, Singh et al, à travers une étude combinant l'empreinte digitale et la géolocalisation GPS pour l'identification des individus, démontrent l'intérêt d'une approche multimodale pour renforcer la fiabilité de l'identification. La contribution clé de ce travail est l'intégration du contexte géographique à la biométrie, mais sa limite principale réside dans le caractère intrusif de la modalité utilisée et son inadéquation aux scénarios de trafic routier nécessitant une identification sans contact[6].

Dans le domaine des architectures IoT appliquées à la reconnaissance faciale, Mohammad et al ont présenté une étude portant sur l'intégration de modèles légers tels que MobileNetV2 et FaceNet dans des dispositifs IoT edge. La contribution clé de cette recherche est la démonstration de la faisabilité d'une reconnaissance faciale en temps quasi réel sur du matériel à faible capacité, grâce à l'optimisation des modèles. La limite principale reste l'absence de prise en compte de facteurs contextuels tels que la géolocalisation ou la mobilité des sujets[7, 8].

Abdullahu et al. ont proposé une étude basée sur une architecture décentralisée combinant CNN et SVM pour la reconnaissance multi-visages dans des environnements IoT. La contribution clé de ce travail réside dans la réduction de la charge computationnelle sur les nœuds edge, tandis que la limite principale concerne la taille restreinte du jeu de données et l'absence de validation en conditions réelles dynamiques. Par ailleurs, Aboluhom et Kandilli ont mené une étude sur l'implémentation de modèles de deep learning pour la reconnaissance faciale sur Raspberry Pi. La contribution clé est l'évaluation comparative de modèles légers adaptés aux systèmes embarqués, mais la limite principale réside dans

la faible robustesse face aux variations importantes de pose et d'éclairage[9].

Concernant l'intégration de mécanismes complémentaires pour renforcer l'identification, Chen et al ont mené une étude axée sur l'utilisation de la géolocalisation GPS dans des systèmes IoT de suivi et de surveillance [10]. La contribution clé de ce travail est la prise en compte de la dimension spatiale pour améliorer la traçabilité des événements. Néanmoins, la limite principale est l'absence d'un mécanisme biométrique d'identification fiable. Iram et al, dans une étude combinant YOLOv5Face, ArcFace et ByteTrack pour la reconnaissance faciale en temps réel, proposent une architecture performante en termes de précision et de suivi multi-individus. La contribution clé est la robustesse du système en environnement complexe, tandis que la limite principale demeure sa dépendance à des ressources matérielles élevées (GPU), rendant son déploiement difficile sur des plateformes IoT low-cost.

3. Méthodologie

La démarche méthodologique adoptée s'articule autour de cinq phases complémentaires. Elle débute par une analyse documentaire approfondie portant sur la biométrie, la géolocalisation et l'Internet des Objets, afin d'identifier les fondements théoriques et les approches existantes.

Cette phase est suivie par la modélisation théorique du système, intégrant la reconnaissance biométrique, la cohérence géographique et le contexte cinématique lié à la vitesse du véhicule. La troisième phase concerne l'implémentation d'un prototype matériel et logiciel reposant sur une architecture IoT, utilisant une ESP32-Cam pour la capture d'images, un module GPS pour la localisation, le protocole MQTT pour la transmission sécurisée des données, et un backend FastAPI pour le traitement biométrique, géospatial et décisionnel.

La quatrième phase est consacrée aux tests expérimentaux en conditions réelles afin d'évaluer le fonctionnement du système. Enfin, la dernière phase porte sur l'analyse des performances, en termes de fiabilité d'identification, de réduction des faux positifs et de cohérence entre les données biométriques, géographiques et cinématiques.

3.1 La biométrie

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques (humaine) préalablement enregistrer : physiologique, comportementale, biologique[11, 12].

On considère qu'une identité biométrique est définie par un ensemble de caractéristiques mesurables dont les paramètres sont : l'ensemble des individus I , l'espace biométrique B , l'individu x , tel que $x \in I$, le vecteur biométrique $b(x)$ appartenant à B est inclus dans $\mathbb{R}^n$ extrait (visage, empreinte, comportement, etc.), la fonction biométrique est définie par [13]:

$$f: I \rightarrow B, f(x) = b(x) \quad (1)$$

Cette fonction représente la mesure numérique d'une caractéristique humaine unique[14]. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu[14]. Comme indiqué dans la théorie, les caractéristiques biométriques ne sont ni parfaitement uniques ni infalsifiables.

Une variation intra-individuelle tel que le bruit $\varepsilon^{(k)}$ déterminé par : la pose, l'éclairage, le capteur et le comportement et k : le numéro de la capture, cette variation peut être modélisée de la manière suivante :

$$b_x^{(k)} = f(x) + \varepsilon^{(k)} \quad (2)$$

3.1.1. Modalités biométriques

Les modalités biométriques sont les caractéristiques humaines physiologiques, comportementales ou biologiques[15].

▪ Modalités biométriques physiques

Il y a différents traits physiques qui sont spécifiques à chaque personne et pour chaque trait, il existe plusieurs méthodes pour les évaluer : Empreintes digitales, Géométrie de la main, Iris, Rétine, Visage, Système et configuration des veines.

▪ Modalités de comportement

En plus des caractéristiques physiques, une personne a aussi plusieurs éléments liés à son comportement qui la rendent unique : Dynamique des frappes au clavier, Reconnaissance vocale, Dynamique des signatures

▪ Modalités liées à la biologie.

Ce sont des méthodes d'identification basées sur les caractéristiques naturelles de chaque personne, comme l'odeur, le sang, la salive, l'urine et l'Acide Désoxyribose Nucléique. Dans notre recherche, nous pensons, qu'il soit préférable que plusieurs caractéristiques soient utilisées en définissant la modalité biométrique m $b^{(m)}$, le poids de fiabilité ω_m dont $\sum \omega_m = 1$, cela permet de modéliser le fait que : certaines caractéristiques sont plus faibles que d'autres :

$$b(x) = \sum_{m=1}^M \omega_m \cdot b^{(m)}(x) \quad (3)$$

3.2 La géolocalisation

La géolocalisation, qui se dit aussi géopositionnement ou géoréférencement, est une méthode technique qui permet de situer un objet, une personne, etc., sur une carte ou un plan en utilisant des coordonnées géographiques[16].

Aujourd'hui, il existe plusieurs méthodes pour déterminer la position géographique d'un objet ou d'une personne. Il est essentiel de bien comprendre et maîtriser ces différentes méthodes pour évaluer correctement la solution de localisation adaptée à ses besoins[17]. Ci-dessous, nous décrivons les différentes méthodes employées à l'extérieur comme à l'intérieur d'un espace spécifique :

3.2.1. La géolocalisation à l'extérieur[18] :

Localisation par satellite : On détermine ces distances en évaluant la durée nécessaire à l'arrivée des signaux provenant des satellites, et cette estimation repose sur le

concept de triangulation.

- **Géolocalisation par le GSM:** Le GSM est un système utilisé pour les appels téléphoniques sur mobile. Dans un réseau GSM, le territoire est divisé en petites zones appelées cellules, d'où vient le terme localisation cellulaire.
- **Les équipements du réseau GSM:** Le réseau GSM est composé de plusieurs entités qui se distinguent par leur fonctionnement.
- **Géolocalisation par Géocodeur:** Le géocodage permet d'affecter des coordonnées géographiques (la longitude et la latitude) à une adresse. Ce principe de géocodage est automatisé à l'aide d'un géocodeur qui peut être sous forme de logiciel ou de service en ligne.
- **Localisation à l'aide d'une adresse IP :** Ce procédé permet de trouver l'emplacement géographique d'un ordinateur ou de n'importe quel appareil branché sur Internet, en utilisant l'adresse IP de cet appareil.

3.2.2. Géolocalisation en intérieur

Pour avoir des précisions de l'ordre du mètre, voire encore meilleures, différentes technologies de proximité ont été étudiées.

La proximité de tous les éléments du système (mobile, stations de base du réseau) permet d'obtenir une précision au mètre. L'apparition des nouveaux réseaux sans fil représente une solution à considérer pour déterminer sa position à l'intérieur des bâtiments.

- **Géolocalisation par RFID:** La RFID, acronyme d'identification par radiofréquence, représente une mécanisme de communication sans fil entre une étiquette ou une puce RFID et un terminal ou une porte, souvent désignée par le terme « tag ». Ces étiquettes renferment des données stockées électroniquement, telles que des identifiants uniques, des numéros de série ou d'autres formes d'informations. Ils peuvent être liés à des objets, des animaux ou être insérés directement dans des insignes, des cartes d'identité ou des dispositifs portables. L'échange entre le tag et le lecteur se réalise par le biais d'ondes radioélectriques. Lorsque le lecteur émet un signal radio, l'étiquette le détecte et lui retourne ses données.
- **Localisation par infrarouge :** Le système Active Badge est l'un des premiers systèmes de localisation à l'intérieur.
- **La localisation par vidéo :** La vidéo est un moyen qui permet de repérer la présence d'un objet et de savoir où il se trouve dans une scène. La localisation se fait en transformant l'image de la scène vers les différents angles de vue de la caméra. La technologie permet de détecter une entrée illégale en utilisant des méthodes de reconnaissance des formes, ce qui permet d'identifier un objet sur une photo. On peut suivre le déplacement de ce contour tant qu'il reste visible sur l'écran de la caméra.
- **Localisation par Wi-Fi :** C'est un standard de réseau sans fil local qui suit la norme 802.11b, et aujourd'hui aussi la norme 802.11g, qui fonctionne bien avec la première. Il s'agit d'un réseau à haut

débit dont la couverture est censée être "étendue", comme la téléphonie mobile, et il est conçu pour permettre une connexion à Internet.

3.2.3. La Biométrie et la Géolocalisation

Partant du Principe qui dit : « Deux signatures biométriques similaires sont plus crédibles si elles sont cohérentes spatialement et temporellement où la décision biométrique est contextualisée par la géolocalisation »[19]. On passe donc d'une décision pure biométrie à une décision biométrie liée à contexte géographique[20]. Cette décision est motivée par les variables suivantes : **le vecteur biométrique observé (test)** b_t , **le vecteur biométrique enregistré par l'individu j** b_j , **la distance biométrique** $d_b(.)$, **le seuil biométrique** θ_b , **la position observée** P_t , **la position de référence associée à l'identité j** p_j , **la distance géographique** $d_g(.)$ et **le seuil géographique** θ_g . On peut utiliser la distance géographique GPS de Haversine :

$$d_g(p_t, p_t) = 2R \arcsin \left(\sqrt{\sin^2 \left(\frac{\Delta \varphi}{2} \right) + \cos(\varphi_t) \cos(\varphi_t) \sin^2 \left(\frac{\Delta \lambda}{2} \right)} \right) \quad (4)$$

Où R est le rayon de la Terre.

Ainsi la fonction décision biométrique associée à la géolocalisation sera :

$$\hat{x} = \begin{cases} x_j & \text{si } \begin{cases} d_b(b_t, b_j) \leq \theta_b \\ d_g(p_t, p_t) \leq \theta_g \end{cases} \\ \text{inconnu} & \text{sinon} \end{cases} \quad (5)$$

Afin de renforcer la fiabilité de l'identification, la décision biométrique est contextualisée par la géolocalisation.

La similarité faciale est ainsi validée uniquement lorsqu'elle est spatialement cohérente avec la position GPS associée à l'événement. Cette approche permet de réduire les faux positifs, en particulier dans les environnements urbains dynamiques où plusieurs individus peuvent présenter des similarités biométriques.

3.3 Internet des Objets

L'Internet des Objets est un réseau qui relie différents réseaux entre eux. Grâce à des systèmes d'identification électronique standardisés et unifiés, ainsi qu'à des appareils mobiles sans fil, il permet d'identifier clairement et sans confusion des objets physiques et des entités numériques.

Cela permet ensuite de récupérer, stocker, transmettre et traiter les données associées à ces objets, sans interruption entre le monde physique et le monde virtuel[21].



Figure N°1 : outils IoT

En se basant sur le Principe qui dit : « Une identité est valide si la biométrie est cohérente avec la position ET avec la dynamique du véhicule (vitesse) »[22].

La vitesse devient donc un contexte cinématique qui renforce ou invalide l'identification, cette fonction est déterminée par les variables supplémentaires : vitesse mesurée du véhicule au moment de l'infraction v_t , la vitesse maximale autorisée sur le point d'intérêt v_{max} , la vitesse de référence associée à l'identité j v_j , la distance cinématique $d_v(.)$, le seuil de cohérence de vitesse θ_v . Ainsi la fonction de cohérence de vitesse qui mesure la gravité de l'infraction est:

$$d_v(v_t) = \max(0, v_t - v_{max}) \quad (6)$$

3.4 Modèle proposé

Notre solution fonctionne selon cet algorithme:

ALGORITHME Système_Infractions_Biométrie

ENTRÉES :

image, latitude, longitude, vitesse, base_biométrique, θ , vitesse_max

SORTIES :

identité_conducteur, position_infraction, statut_enregistrement

DEBUT

1. Initialiser les capteurs IoT et le backend

2. Charger la base biométrique

3. Définir le seuil de similarité θ

TANT QUE le système est actif FAIRE

// --- DÉTECTION D'INFRACTION ---

4. SI vitesse > vitesse_max ALORS

infraction_détectée ← VRAI

SINON

infraction_détectée ← FAUX

FIN SI

5. SI infraction_détectée = VRAI ALORS

// --- BIOMÉTRIE ---

6. visages ← détecter_visages(image)

7. SI visages est vide ALORS

identité_conducteur ← "Inconnu"

score ← 0

SINON

POUR chaque visage dans visages FAIRE

vecteur ← extraire_caractéristiques(visage)

score_min ← ∞

POUR chaque profil dans base_biométrique

FAIRE

score_temp ← distance(vecteur, profil.vecteur)

SI score_temp < score_min ALORS

score_min ← score_temp

identité_temp ← profil.identité

FIN SI

FIN POUR

SI score_min ≤ θ ALORS

identité_conducteur ← identité_temp

SINON

```

    identité_conducteur ← "Inconnu"
  FIN SI
  FIN POUR
  FIN SI
  // --- GÉOLOCALISATION ---
  8. position_infraction ← créer_point(latitude,
longitude)
  // --- ENREGISTREMENT ---
  9. Insérer (identité_conducteur, position_infraction,
vitesse, date_heure) dans BASE_INFRACTIONS
  10. Journaliser l'événement dans LOGS
  11. statut_enregistrement ← "Succès"

  // --- NOTIFICATION & INTERFACE ---
  12. Mettre à jour le tableau de bord
  13. Notifier les agents compétents
  // --- SÉCURITÉ ---
  14. Chiffrer les données biométriques
  15. Contrôler les accès utilisateurs
  16. Auditer les modifications
  FIN SI
  FIN TANT QUE
  FIN

```

4. Architecture propose

Le schéma ci-dessous présente le fonctionnement détaillé de l'algorithme du Système d'Infractions Biométrique, depuis la détection d'une infraction jusqu'à l'identification et l'enregistrement sécurisé de l'évènement.

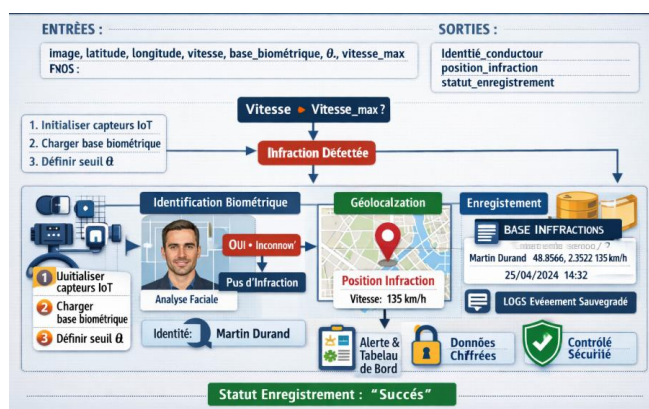


Figure N°2 : Fonctionnement de la solution

5. Résultats expérimentaux

Le tableau ci-dessous présente une synthèse structurée de l'ensemble des résultats expérimentaux obtenus lors de l'évaluation du système d'infractions biométriques, couvrant à la fois l'environnement matériel, les outils logiciels, les performances biométriques, la précision géospatiale et le potentiel de déploiement.

Table 2
Détails des résultats

Section	Éléments clés
Environnement expérimental	<ul style="list-style-type: none"> Tests réalisés à Kananga en conditions réelles Prototype : ESP32-Cam, GPS NEO-6M, routeur Wi-Fi Backend exécuté sur FastAPI (serveur local CPU/GPU) Caméra HD pour captures

	faciales • Microcontrôleur IoT pour prétraitement et transmission • Stockage SSD pour images, vecteurs biométriques et données GPS
Outils logiciels et technologies	• Python pour le traitement principal • OpenCV & TensorFlow : détection et reconnaissance faciale • FastAPI : backend applicatif • PostgreSQL/PostGIS : stockage + données géospatiales • MQTT : communication IoT ↔ serveur • Leaflet.js : visualisation cartographique en temps quasi réel
Protocole expérimental & Dataset	• 300 captures réalisées • Variations : luminosité, orientation du visage, contexte urbain • Collecte effectuée sur plusieurs points de la ville de Kananga • Objectif : tester la robustesse du système en conditions réelles
Résultats de reconnaissance biométrique	• Modèle 2D : précision entre 78 % et 85 % • Modèle hybride 2D/3D : précision moyenne 87 %, maximum 92 % • Amélioration notable grâce à la fusion 2D+3D • Meilleure stabilité en environnement non contrôlé
Précision GPS & Temps de traitement	• Précision GPS : 1–3 m (zones dégagées), 3–5 m (centre-ville) • Temps global de traitement : 2,1 à 3,4 s • Fonctionnement en temps quasi réel : capture → biométrie → enregistrement → transmission
Analyse globale & Déploiement	• Système robuste malgré l'utilisation de matériel low-cost • Bonne précision biométrique et GPS • Temps de traitement compatible avec l'usage routier • Fort potentiel de déploiement urbain à large échelle

Le modèle proposé a été comparé à une approche de référence basée uniquement sur la reconnaissance faciale 2D, sans intégration de la dimension 3D ni du contexte géographique. Cette comparaison permet d'évaluer objectivement l'apport de la fusion 2D/3D et de la géolocalisation dans le processus d'identification.

L'évaluation des performances biométriques repose sur des métriques standards largement utilisées dans la littérature, à savoir l'Accuracy, la Precision, le Recall, ainsi que les taux de fausse acceptation (FAR) et de faux rejet (FRR). Les performances système sont évaluées à travers le temps moyen de traitement et la précision de géolocalisation. Les résultats expérimentaux montrent une amélioration significative des performances lorsque la reconnaissance faciale combine les modalités 2D et 3D.

En effet, le modèle basé uniquement sur la reconnaissance 2D obtient une Accuracy de 81,4 %, une précision de 80,2 % et un recall de 79,6 %. Son taux de fausses acceptations (FAR) est de 7,8 %, tandis que le taux de faux rejets (FRR) atteint 12,6 %.

En revanche, l'approche proposée combinant la reconnaissance 2D et 3D améliore nettement les performances, avec une Accuracy de 87,0 %, une précision de 86,3 % et un recall de 85,9 %. De plus, le FAR diminue à 4,2 % et le FRR à 8,1 %, ce

qui confirme la robustesse et la fiabilité accrues du modèle multimodal par rapport à l'approche unimodale. Les résultats montrent que l'intégration de la reconnaissance faciale 3D permet une amélioration significative des performances par rapport à la reconnaissance 2D seule, avec un gain moyen de 5 à 7 % en termes d'accuracy. La réduction du FAR et du FRR confirme l'apport de la fusion biométrique et du contexte géographique, en particulier dans des environnements urbains non contrôlés.

6. Discussion

La discussion met en évidence les apports du système : automatisation du processus de contrôle routier, réduction du temps d'identification, fiabilité accrue grâce à la fusion biométrique et géolocalisation.

Les limites concernent la dépendance à la qualité des images, la variabilité de la connectivité Internet et la nécessité d'un matériel plus performant pour la reconnaissance 3D avancée. Des perspectives innovantes incluent l'intégration de modèles deep learning (FaceNet, ArcFace) et l'utilisation de caméras HD.

Les résultats expérimentaux obtenus mettent clairement en évidence l'apport de la fusion biométrique et contextuelle proposée dans cette étude. La comparaison entre la reconnaissance faciale 2D seule et l'approche hybride 2D/3D intégrant la géolocalisation montre une amélioration significative des performances d'identification. En termes de métriques biométriques standards, le modèle proposé affiche une augmentation notable de l'Accuracy, accompagnée d'une amélioration de la précision et du recall, ainsi qu'une réduction des taux de fausse acceptation (FAR) et de faux rejet (FRR). Ces gains s'expliquent par la capacité de la composante 3D à atténuer les effets des variations de pose et d'éclairage, tandis que la géolocalisation agit comme un filtre contextuel permettant de valider la cohérence spatiale de l'identité détectée. Cette approche comparative met ainsi en évidence que la performance globale ne repose pas uniquement sur la qualité du modèle biométrique, mais également sur l'exploitation intelligente du contexte géographique et cinématique, ce qui rejoint les observations rapportées dans la littérature récente sur les systèmes biométriques contextualisés.

Au-delà des performances biométriques, l'analyse des résultats système confirme la pertinence du choix architectural basé sur une infrastructure IoT distribuée. Le temps moyen de traitement, compris entre quelques secondes, demeure compatible avec une utilisation en quasi temps réel dans un contexte de surveillance routière, malgré l'utilisation de matériel embarqué à faible coût. La précision de géolocalisation obtenue, de l'ordre de quelques mètres, s'avère suffisante pour assurer la traçabilité spatio-temporelle des infractions et renforcer la crédibilité de l'identification. Néanmoins, certaines limites subsistent, notamment la dépendance à la qualité des images acquises par les capteurs, les fluctuations de connectivité réseau et les contraintes matérielles liées à la reconnaissance 3D avancée. Ces limites ouvrent des perspectives d'amélioration, notamment par l'intégration de modèles deep learning plus robustes tels que FaceNet ou ArcFace, l'utilisation de caméras de meilleure résolution et le déploiement de plateformes embarquées plus performantes. Ainsi, les résultats obtenus confirment que l'approche proposée

constitue une solution équilibrée entre précision, coût et déployabilité, tout en offrant une base solide pour l'évolution vers des systèmes de surveillance routière intelligents à grande échelle.

7. Conclusion et Perspectives

Cette étude met en évidence la pertinence et la faisabilité d'un système intelligent combinant la reconnaissance faciale 2D/3D [3], la géolocalisation GPS et une architecture IoT distribuée pour l'identification automatisée des auteurs d'infractions routières[23].

Les expérimentations menées dans la ville de Kananga ont démontré que même avec un matériel IoT à faible coût, tel que l'ESP32-Cam et le module GPS NEO-6M, il est possible d'obtenir des performances satisfaisantes en termes de précision biométrique, de localisation géographique et de rapidité de traitement. L'approche hybride 2D+3D a permis d'améliorer la robustesse de la reconnaissance faciale dans des conditions variées de luminosité, d'orientation et d'environnement, atteignant une précision moyenne de 87 %, tandis que la géolocalisation a fourni une précision de 1 à 5 mètres, conforme aux exigences des systèmes de surveillance routière.

De plus, le temps global de traitement compris entre 2,1 et 3,4 secondes confirme l'aptitude du système à opérer en quasi temps réel, élément essentiel pour les infrastructures de contrôle intelligent.

L'ensemble de ces résultats montre que le système proposé constitue non seulement une solution innovante pour la gestion automatisée des infractions routières, mais également un outil technologique viable pour les villes en quête de modernisation de leurs dispositifs de sécurité publique. Son architecture modulaire et distribuée favorise un déploiement progressif, adaptable à divers environnements urbains, tout en offrant la possibilité d'intégrer de nouvelles fonctionnalités ou de monter en échelle selon les besoins institutionnels.

Les perspectives futures consistent principalement à renforcer les capacités d'analyse et de reconnaissance grâce à l'intégration d'algorithmes d'apprentissage profond (CNN, FaceNet, ArcFace), qui permettraient d'améliorer la précision et la résilience du système face à des conditions plus extrêmes, telles que les occlusions partielles ou les variations rapides d'angle. L'utilisation de caméras HD ou thermiques, associée à des microcontrôleurs plus puissants (Jetson Nano, Raspberry Pi 5), pourrait également accroître la qualité des images et réduire davantage les erreurs d'identification. À plus long terme, le déploiement à grande échelle devrait s'accompagner de la mise en place de centres de contrôle intelligents intégrant tableaux de bord avancés, systèmes d'alerte automatisés, analyses statistiques et interfaces géospatiales dynamiques[23, 24].

Enfin, l'interopérabilité avec les systèmes nationaux de transport, les bases de données administratives ou les applications mobiles pourrait renforcer l'efficacité globale de la chaîne de surveillance et contribuer durablement à l'amélioration de la sécurité routière dans des villes comme Kananga et au-delà.

Références

- [1] AISSAOUI, M., F. BOUCHENAF, and O. ANNAD, *Amélioration de la sécurité routière pilotée par l'IA pour les véhicules de transport public: Une approche par le management des risques*. 2024, ENSTA.
- [2] Bouassida, S., *Optimisation multi-objectif des flux de circulation routière en abord d'intersection*. 2024, Université Paris-Saclay; Université de Tunis El Manar.
- [3] ADEL, S., *Reconnaissance Biométrique par Fusion Multimodale de Visages*. 2022, Faculté des Sciences et de la technologie.
- [4] BEN_HAMZA, N., *Fusion 2D et 3D pour la reconnaissance de visage*.
- [5] Deng, Y., et al. *Accurate 3d face reconstruction with weakly-supervised learning: From single image to image set*. in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*. 2019.
- [6] Rana, V., M. Singh, and A. Rana, *Variability and Diversity Studies Using Morpho-physiological Traits in Wheat (Triticum aestivum L.) under Irrigated and Rainfed Conditions*. *International Journal of Bioresource and Stress Management*, 2024. **15**(8): p. 01-15.
- [7] Datoo, M.S., et al., *Safety and efficacy of malaria vaccine candidate R21/Matrix-M in African children: a multicentre, double-blind, randomised, phase 3 trial*. *The Lancet*, 2024. **403**(10426): p. 533-544.
- [8] Subrahmanyam, V., et al. *An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT)*. in *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)*. 2024. IEEE.
- [9] Abdullahu, E., H. Wache, and M. Piangerelli, *Secure and decentralized hybrid multi-face recognition for IoT applications*. *Sensors*, 2025. **25**(18): p. 5880.
- [10] Li, Y., et al. *NTIRE 2023 challenge on efficient super-resolution: Methods and results*. in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2023.
- [11] MAISL, M.H., *Identification biométrique, protection des données et droits de l'homme*.
- [12] LAZOUL, A.O., et al., *Identification Des Personnes Par Utilisant Un Descripteur De Texture*. 2017.
- [13] Le JURY, D., *Intitulé: Identification biométrique par le visage et l'oreille*. 2020, UNIVERSITE BADJI MOKHTAR ANNABA.
- [14] MELITI, Z., Y. FETHALLAH, and M. Encadré par Abdallah, *Tatouage Biométrique: Une Approche Innovante pour la Sécurité et l'Authentification*. 2024, UNIVERSITE DE ECHAHID CHEIKH LARBI TEBESSI.
- [15] Fatima, I., *Reconnaissance humaine multimodale (ECG-EMG)*. 2023, UNIVERSITY BBA.
- [16] Guinard, P. and F. Troin, *Tous immobiles, tous cartographes? Approches cartographiques des mobilités, des circulations, des flux et des déplacements. Méthodes, outils, représentations, pratiques et usages*. 2021.
- [17] Cliquet, G. and J. Baray, *Géomarketing et géolocalisation: Un marketing spatial dynamique*. 2019: ISTE Group.
- [18] Le Floch, A., *Méthodes de localisation en intérieur en 5G*. 2025, Université de Toulouse.
- [19] Hedjaz, H., *Identification de personnes par signature manuscrite*. 2022.
- [20] Louis, V., *La reconnaissance biométrique dans l'espace public*. *La privatisation de l'espace public*, 2025.
- [21] Abbassi, Y. and H. Benlahmer. *Un aperçu sur la sécurité de l'internet des objets (IOT)*. in *Colloque sur les Objets et systèmes Connectés-COC'2021*. 2021.
- [22] Boualleg, A., *Reconnaissance Automatique des Personnes*. 2020.
- [23] SMAALI, B., *La géolocalisation en environnement intérieur basée sur le signal Wi-Fi*. 2025.
- [24] Liouane, O., *Amélioration des techniques de la géolocalisation dans les réseaux de capteurs sans fil: Application et implémentation temps réel*. 2022, Université Bourgogne Franche-Comté; Faculté des Sciences de l'Université de