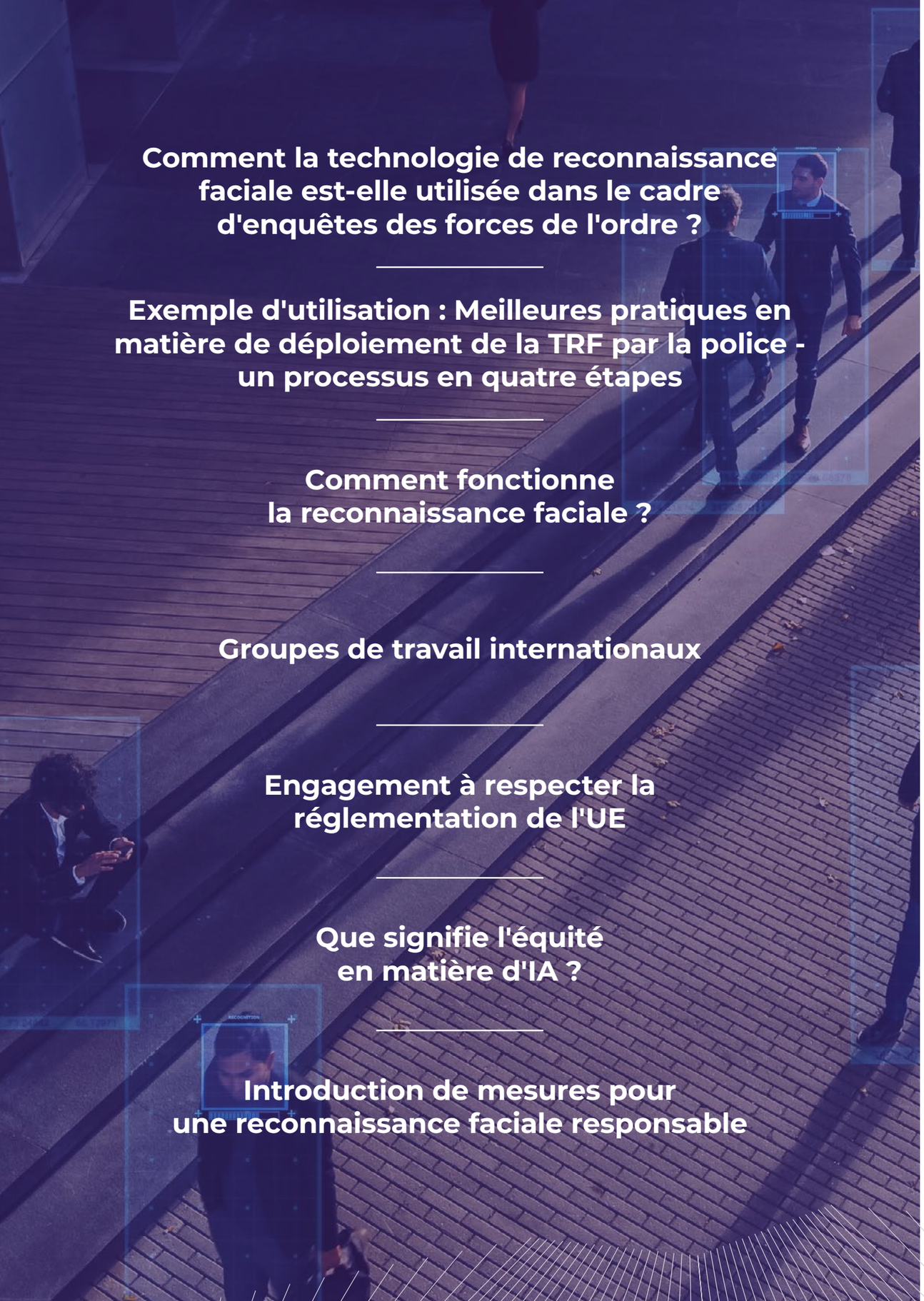
POSITION PAPER

Utilisation de la **technologie de reconnaissance faciale** pour les **enquêtes des forces de l'ordre**

IDEMIA
PUBLIC SECURITY



Comment la technologie de reconnaissance faciale est-elle utilisée dans le cadre d'enquêtes des forces de l'ordre ?

Exemple d'utilisation : Meilleures pratiques en matière de déploiement de la TRF par la police - un processus en quatre étapes

Comment fonctionne la reconnaissance faciale ?

Groupes de travail internationaux

Engagement à respecter la réglementation de l'UE

Que signifie l'équité en matière d'IA ?

Introduction de mesures pour une reconnaissance faciale responsable

Introduction

La technologie de reconnaissance faciale (TRF) joue un rôle de plus en plus vital dans divers secteurs, notamment la sécurité publique, les forces de l'ordre et les entreprises commerciales. Face aux progrès de cette technologie, il est essentiel d'engager des discussions éclairées impliquant toutes les parties prenantes de la société. En privilégiant un dialogue factuel et constructif, nous pouvons garantir le développement et la mise en œuvre responsables des applications TRF.

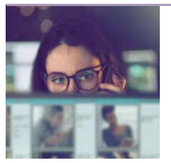
Reconnaissance faciale

La reconnaissance faciale est une application logicielle qui compare l'image d'un visage à une image ou à une base de données contenant plusieurs images de visages. Pour effectuer la comparaison, la TRF utilise l'intelligence artificielle (IA), qui a considérablement amélioré la précision et les performances des systèmes de reconnaissance faciale.

Notamment, les techniques modernes d'IA, telles que l'apprentissage profond, s'appuient sur de vastes ensembles de données lors du développement des algorithmes. Ces données sont essentielles pour former des algorithmes capables de reconnaître efficacement les visages et de minimiser les biais, garantissant ainsi des résultats justes et fiables.

La reconnaissance faciale est utilisée pour diverses applications. En fonction de la législation du pays, elle peut être utilisée dans le secteur gouvernemental ou commercial :

Contrôles d'immigration aux frontières



Assistance dans les enquêtes post-crime/ terroristes

Création et utilisation d'une identité numérique, notamment pour les services publics en ligne

Aide à l'authentification de l'utilisateur lors de l'utilisation d'applications pour smartphones

Ce document se concentre sur les exemples d'utilisation de la TRF dans le cadre d'enquêtes et sur le développement et l'application d'IDEMIA Public Security pour le marché des forces de l'ordre.

1 Comment la technologie de reconnaissance faciale est-elle utilisée dans le cadre d'enquêtes des forces de l'ordre ?

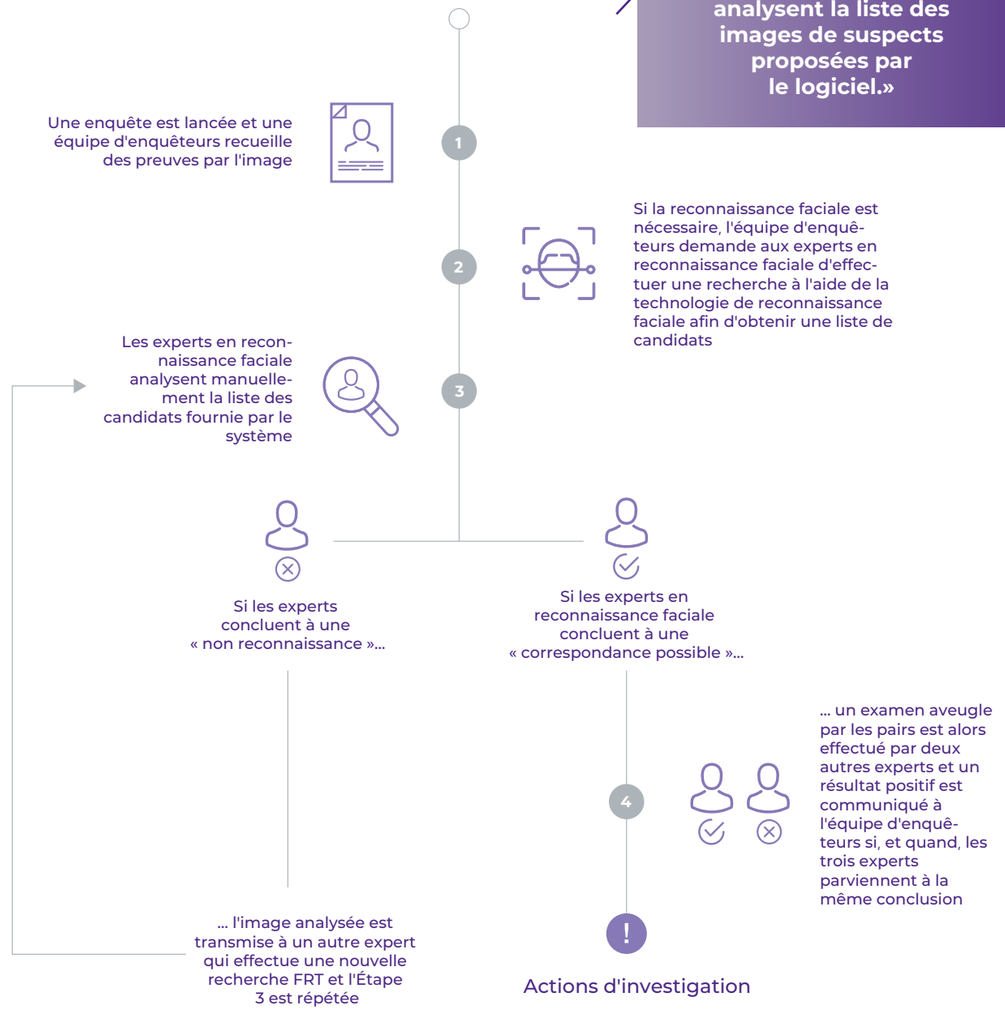
Meilleures pratiques pour améliorer l'efficacité de la police scientifique grâce à la technologie de reconnaissance faciale

La TRF est habituellement utilisée lorsque les enquêteurs disposent d'une image du visage de l'auteur potentiel de l'infraction mais n'ont pas été en mesure de déterminer l'identité de la personne. Le système TRF compare cette image à une base de données de visages de personnes connues de la police. Cette base de données est généralement composée de photo portraits prises par la police (également appelés « mugshots ») de personnes qui ont été, par exemple, précédemment arrêtées ou impliquées dans une enquête criminelle pour un délit suffisamment grave pour justifier l'acquisition de leurs caractéristiques biométriques, y compris leurs empreintes digitales et leur visage.

Le système fournit une liste de candidats potentiels, que le médecin légiste évalue pour déterminer s'il existe une correspondance. Cette évaluation est menée conformément aux procédures opérationnelles standard de l'organisation policière locale, afin de garantir la cohérence et le respect des protocoles établis.

2 Exemple d'utilisation : Meilleures pratiques en matière de déploiement de la TRF par la police - un processus en quatre étapes

« Après la recherche, les experts en reconnaissance faciale analysent la liste des images de suspects proposées par le logiciel.»



Source : Rapport du Forum économique mondial sur le cadre de gouvernance pour l'utilisation responsable de la reconnaissance faciale dans les enquêtes des forces de l'ordre[1]

3 Comment fonctionne la reconnaissance faciale ?

Développement d'algorithmes

La plupart des caractéristiques d'un système TRF sont liées aux algorithmes utilisés. Par souci de simplicité, nous nous concentrerons sur l'algorithme de comparaison biométrique. Toutefois, il faut garder à l'esprit que d'autres facteurs jouent un rôle clé, tels que les dispositifs d'acquisition (par exemple, les appareils photo) et/ou les algorithmes de détection, qui déterminent où se trouve le visage sur une photographie ou si un visage est réellement présent sur la photographie.

La plupart des approches TRF modernes font appel à la technologie de l'apprentissage profond, qui est largement utilisée depuis ces cinq à dix dernières années pour de nombreuses applications différentes et est souvent qualifiée d'intelligence artificielle. La TRF d'IDEMIA Public Security, comme la plupart des autres entreprises très performantes, s'appuie considérablement sur des techniques d'apprentissage profond.

Dans l'apprentissage profond, le développeur combine différents éléments pour produire un algorithme :

› **Développement d'un ensemble de données d'entrainement :** Les développeurs compilent un ensemble de données d'apprentissage composé de plusieurs images d'un même individu, ainsi que d'images d'autres individus. Cet ensemble de données permet à l'algorithme d'apprendre statistiquement les caractéristiques communes qui définissent la même personne sur différentes images, ainsi que de faire la distinction entre les images de différentes personnes.

› **Jeu de données de test :** Cet ensemble de données est utilisé pour évaluer les performances de l'algorithme. Il s'agit d'un ensemble de données complètement différent de l'ensemble de données d'entrainement, mais classé en fonction des images de la même personne ou de différents individus. Cela permet d'éviter une sur-adaptation de l'algorithme à l'ensemble des données d'entrainement et d'améliorer les performances dans un plus grand nombre de situations opérationnelles.

› **Fonction de coût :** La fameuse « fonction de coût » est une procédure mathématique par laquelle le développeur spécifie les paramètres que l'algorithme doit optimiser pendant l'apprentissage. Cette procédure n'est pas normalisée. Elle est basée sur l'expertise du développeur et les objectifs de l'algorithme. À bien des égards, il s'agit de « la touche secrète » de la performance d'un algorithme.

Contrôle et traçabilité des algorithmes

Une fois que l'algorithme d'IDEMIA Public Security a été entraîné, évalué et jugé conforme aux critères internes, il peut être mis en œuvre dans les systèmes opérationnels. Une fois que l'algorithme est publié par la R&D et devient opérationnel, il reste inchangé, ce qui garantit son intégrité tout au long de son cycle de vie. Les produits existants sont mis à jour avec des versions plus récentes, qui ont également été certifiées et diffusées par notre département interne de R&D. IDEMIA Public Security n'utilise pas l'apprentissage continu ou l'adaptation des algorithmes dans les systèmes de production (c'est-à-dire ceux utilisés par les clients). Ainsi, nous assurons la traçabilité et garantissons la performance de nos algorithmes diffusés, qui restent sous notre seul contrôle. Cette approche garantit aux clients et aux utilisateurs que les performances de nos algorithmes dans les applications réelles correspondent aux résultats observés lors des tests.

Un engagement sans faille en faveur de l'amélioration de la technologie

IDEMIA Public Security investit continuellement dans la R&D et améliore sa technologie de pointe, qu'il s'agisse d'algorithmes, de dispositifs ou de processus métiers. L'un des points essentiels de cet engagement est la réduction constante des taux d'erreur dans la TRF, mesurée par l'institut indépendant National Institute of Standards and Technology (NIST) sur plusieurs années.[2] Cet investissement continu dans la recherche et le développement permet à IDEMIA Public Security de rester à la pointe de l'innovation technologique.

Entre 2018 et 2023, la précision de l'algorithme d'IDEMIA Public Security a été multipliée par dix lors d'un test comparant une photo à une base de données de photos, comme illustré ci-dessous.

La précision a été décuplée au cours des trois dernières années.

Évolution de la précision des algorithmes IDEMIA sur deux ensembles de données 2018 à ce jour

Source : NIST FRVT 1:N Identification. NB : plus le taux est faible, meilleures sont les performances.

4 Groupes de travail internationaux

Afin d'améliorer la transparence et de garantir une utilisation éthique de la TRF, IDEMIA Public Security fait partie de plusieurs groupes de travail et participe à l'élaboration de normes sectorielles. Cela permet à IDEMIA Public Security de promouvoir une communication transparente sur notre technologie.

Conformité aux normes internationales relatives à la technologie biométrique

Norme ISO/IEC 19795-1-Technologies de l'information-Essais de performance biométrique et établissement de rapports

Cette norme définit des méthodes et des paramètres permettant de tester les performances des systèmes et algorithmes biométriques par l'analyse des scores de comparaison et des décisions prises par le système, sans qu'il soit nécessaire d'avoir une connaissance détaillée des algorithmes du système ou de la distribution sous-jacente des caractéristiques biométriques dans la population concernée.

Associations professionnelles

IDEMIA est un membre actif de plusieurs associations professionnelles, telles que le **Biometrics Institute** et l'**European Association for Biometrics.** IDEMIA Public Security présente fréquemment les avancées des technologies biométriques afin de sensibiliser aux meilleures pratiques et aux technologies émergentes qui contribuent à protéger les données personnelles dans les applications biométriques.[3] Nous facilitons également les discussions sur l'équité dans les systèmes biométriques avec les principaux acteurs, y compris le NIST et le Bureau des Nations Unies pour la lutte contre le terrorisme.[4]

5 Engagement à respecter la réglementation de l'UE

Les équipes de recherche d'IDEMIA Public Security, spécialisées dans les algorithmes de la technologie de reconnaissance faciale, sont basées dans l'UE (France et Allemagne). Ce positionnement stratégique garantit le respect total du Règlement général sur la protection des données (RGPD) et nous permet de nous conformer rigoureusement à la future Loi européenne sur l'IA. En tant que contributeurs actifs à l'élaboration de ces cadres réglementaires, y compris notre participation au Pacte européen sur l'IA, nous nous engageons à façonner et à nous aligner sur les réglementations en évolution qui mettent l'accent sur l'équité algorithmique et la responsabilité des développeurs. IDEMIA Public Security s'engage à respecter ces normes et à établir une référence en matière de conformité et de responsabilité éthique.

Conformité au RGPD et collaboration

Notre collaboration de longue date avec les autorités administratives françaises, notamment par le biais de consultations régulières avec la Commission nationale de l'informatique et des libertés (CNIL), souligne notre approche proactive en matière de conformité réglementaire. Cet engagement comprend des consultations préalables au lancement de programmes de recherche internes, garantissant la transparence et le respect des exigences du RGPD.

Contrôle éthique et sécurité des données

IDEMIA Public Security adhère à des directives éthiques strictes concernant la collecte et l'utilisation des données :

- Les données sont collectées exclusivement à des fins de recherche, en garantissant une participation volontaire, en fournissant des droits d'accès et de rectification des données, et en limitant les périodes de conservation des données, le tout en conformité avec le RGPD.
- L'accès aux données est limité au personnel de recherche autorisé, régi par des processus certifiés ISO 27001 et soumis à des audits réguliers afin de maintenir la sécurité et l'intégrité.
- Notre propriété intellectuelle est protégée par les réglementations française et allemande, renforçant ainsi notre engagement en matière de conformité juridique et d'innovation au sein de l'Europe.

Des approches innovantes pour relever les défis liés aux données

Pour relever les défis posés par la disponibilité limitée des données, nous sommes les premiers à utiliser des données synthétiques à des fins d'entrainement. Si les données synthétiques actuelles sont très performantes dans certains domaines, tels que les objets inanimés ou la reconnaissance optique de documents, elles ne présentent pas la diversité requise pour un entrainement efficace à la reconnaissance faciale. IDEMIA Public Security affine activement cette approche, afin de surmonter les contraintes liées au volume de données et d'améliorer les performances algorithmiques.

Nos efforts continus en matière de recherche et de développement, ainsi que notre engagement proactif dans l'élaboration des normes réglementaires, reflètent notre engagement en faveur de l'innovation éthique et de l'excellence réglementaire.

6 Que signifie l'équité en matière d'IA ?

En raison de la nature sensible d'applications telles que l'identification criminelle, il est impératif de veiller à ce que les algorithmes de reconnaissance faciale ne présentent pas de disparités significatives en termes de performances entre les différents groupes de population. Bien que la décision finale en matière d'identification criminelle revienne à un expert de la police scientifique humain, l'algorithme ne doit pas introduire de biais susceptibles d'entraîner des taux d'erreur inégaux.

Les catégories de population clés, telles que les groupes ethniques, l'âge, le sexe et les attributs physiques tels que les lunettes ou la pilosité faciale, doivent être prises en compte pour garantir des performances équitables. La définition largement acceptée de l'équité dans le cadre de la TRF consiste à obtenir des performances statistiques cohérentes entre ces groupes, en minimisant la probabilité de disparités d'erreurs.

Une identification faussement positive (IFP) se produit lorsqu'un système TRF présente par erreur, à l'expert de la police scientifique, un visage extrêmement similaire au visage recherché. Cela peut conduire à l'ouverture d'une enquête sur une personne qui n'a pourtant rien à voir avec le crime ou l'incident. Bien que cette situation puisse être corrigée en premier lieu par la décision experte de l'expert en reconnaissance faciale et, plus tard, par le processus d'enquête, il s'agit toujours d'un résultat indésirable qui ne devrait pas porter la marque de l'iniquité statistique. Dans le cas de l'identification criminelle, l'IFP est le type d'erreur qu'il convient de limiter, et la stabilité entre les différents groupes est nécessaire.

Comment IDEMIA Public Security garantit-elle l'équité en matière d'IA ?

IDEMIA Public Security applique des techniques de pointe au processus de développement des algorithmes. Le discours public actuel sur la reconnaissance faciale et l'IA en général est que toute disproportion dans l'ensemble de données d'entraînement (avec des catégories de population sous-représentées) empêchera l'équité. La distribution de l'ensemble de données d'entrainement n'est pas le seul facteur influençant l'équité. La fonction de coût et, par conséquent, l'expertise du développeur, auront également un impact significatif sur les performances. En construisant avec soin l'ensemble de données d'apprentissage et la fonction de coût simultanément, un développeur peut grandement influencer les performances de l'algorithme résultant.

L'ensemble de données de test doit être :

- représentatif du type de données auxquelles l'algorithme sera confronté sur le terrain.
- représentatif de tous les groupes de population auxquels l'algorithme peut être confronté sur le terrain.

Cette approche globale garantit que les évaluations internes des performances reflètent fidèlement le comportement réel de l'algorithme. IDEMIA Public Security sélectionne les algorithmes à diffuser en fonction non seulement de la précision de l'identification, mais aussi de leur équité entre les différents groupes démographiques.

Il est important de noter que l'engagement d'IDEMIA Public Security en matière d'équité va au-delà des évaluations internes et des réclamations des fournisseurs, renforçant ainsi la confiance grâce à la transparence et à une validation externe rigoureuse.

Tests effectués par des tiers pour plus de transparence

IDEMIA Public Security soumet systématiquement ses algorithmes de reconnaissance faciale, d'empreintes digitales et d'iris à des organismes de test tiers indépendants, renforçant ainsi son engagement en matière de transparence et de fiabilité. Parmi ces évaluations, la plus complète est menée par le NIST. Récemment, le NIST a divisé son Face Recognition Vendor Test (FRVT) en deux programmes distincts : le Face Recognition Technology Evaluation (FRTE) et le Face Analysis Technology Evaluation (FATE).[5] Le FRTE se concentre sur les performances et la précision des technologies de reconnaissance faciale, tandis que le FATE évalue des aspects tels que la qualité de l'image et la détection de morphing.

Les algorithmes d'IDEMIA Public Security ont toujours obtenu des résultats parmi les meilleurs, malgré le grand nombre de soumissions. Jusqu'à présent, le NIST a évalué plus de 570 algorithmes de 172 développeurs uniques dans le cadre du programme FRVT/FRTE 1:N, et 1 260 algorithmes de 395 développeurs uniques dans le cadre du programme 1:1.

Accent mis sur les « effets démographiques »

Le NIST a étudié de manière approfondie les effets démographiques de la TRF et est allé jusqu'à publier un rapport spécifique à ce sujet.[6] Dans ce rapport, le NIST étudie les taux d'erreur pour une variété d'algorithmes soumis par les fournisseurs et fait état des performances en termes d'équité. L'exemple d'utilisation qui nous intéresse est celui de l'identification criminelle, où la cohérence du taux d'IFP dans différents groupes de population est la situation souhaitée. À la page 8 du rapport, dans le résumé technique, dans une section consacrée aux taux d'erreur des faux positifs des algorithmes d'identification, l'auteur écrit qu'il est noté :

« La présence d'une base de données d'inscription permet aux algorithmes « un-à-plusieurs » d'atténuer les effets démographiques, ce que les systèmes de vérification « un-à-un » n'ont pas. Nous notons que les différences démographiques présentes dans les algorithmes de vérification « un-à-un » sont généralement, mais pas toujours, présentes dans les algorithmes de recherche « un-à-plusieurs »... **Toutefois, certains développeurs ont fourni des algorithmes d'identification pour lesquels les faux positifs ne sont pas détectables. Parmi eux, IDEMIA a décrit publiquement comment elle y est parvenue. »**[7]

Les bons résultats d'IDEMIA Public Security en matière d'atténuation des différences démographiques reflètent son expertise de longue date dans le domaine de la technologie biométrique. Dans le benchmark NIST FRTE 1:1 d'août 2024, l'algorithme d'IDEMIA Public Security a été reconnu pour avoir atteint le meilleur équilibre entre l'équité et la précision.

7 Introduction de mesures pour une reconnaissance faciale responsable

Le Forum économique mondial, l'Organisation internationale de police criminelle (INTERPOL), l'Institut interrégional de recherche des Nations unies sur la criminalité et la justice (UNICRI) et la police néerlandaise ont convoqué une communauté multipartite centrée sur la co-conception d'un ensemble de principes qui décrivent ce qui constitue une utilisation responsable des TRF dans le cadre des enquêtes des forces de l'ordre. Parmi ces principes figurent le respect des droits de l'homme et des droits fondamentaux, la surveillance humaine et la responsabilité, l'optimisation des performances du système et l'atténuation des erreurs et des biais.

Évaluation de votre fournisseur de technologie pour une reconnaissance faciale responsable

Ces principes sont accompagnés d'un questionnaire d'auto-évaluation destiné à aider les forces de l'ordre à concevoir des politiques relatives à l'utilisation des TRF et à s'assurer que le fournisseur de technologie respecte les principes proposés.

- Quelles sont les normes existantes ou à venir que vous demandez à votre fournisseur de respecter pour évaluer les performances de votre système TRF ?
- Avez-vous établi des règles de passation de marchés pour sélectionner les fournisseurs qui respectent ces normes de performance ?
- Avez-vous établi des règles de passation de marchés pour sélectionner les fournisseurs qui ont soumis leur système TRF à une évaluation indépendante telle que celle organisée par le NIST ?
- Avez-vous choisi le fournisseur de technologie qui a présenté les meilleurs résultats ?
- Les tests indépendants de performance en laboratoire sont-ils conçus pour reproduire, aussi fidèlement que possible, les objectifs et les conditions réelles dans lesquelles la TRF est appliquée ?
- Informez-vous le fournisseur de technologie lorsque vous identifiez des erreurs pertinentes dans l'utilisation du système TRF ?
- Quelles règles de passation des marchés avez-vous établies pour garantir la mise à niveau ou le remplacement régulier de la TRF ?

Points importants à retenir

IDEMIA Public Security encourage l'amélioration technologique en participant à des évaluations publiques par des tiers, qui démontrent la transparence des capacités technologiques par le biais de normes internationales.

La TRF d'IDEMIA Public Security est exclusivement développée en Europe et respecte toutes les normes et réglementations en matière de protection de la vie privée, y compris le RGPD. Le Contrôle des exportations s'applique à toutes nos activités commerciales à l'intérieur et à l'extérieur de l'Europe.

La TRF est utilisée comme un outil pour les enquêteurs - les décisions susceptibles d'avoir une incidence sur la vie privée et les droits fondamentaux des citoyens sont toujours prises par un expert humain.

La précision de la TRF s'est rapidement améliorée, les taux d'erreur ayant été divisés par cinq entre 2018 et 2023.

L'équité est assurée par conception dans les algorithmes d'identification d'IDEMIA Public Security, comme l'a démontré l'évaluation publique indépendante de leurs performances par le NIST.

Notes de fin d'ouvrage

1 **Le Forum économique mondial :** A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations (révisé en 2022).

WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (weforum.org)

2 Le National Institute of Standards and Technology (NIST) a été fondé en 1901 et fait aujourd'hui partie du Ministère américain du commerce. Le NIST est l'un des plus anciens laboratoires de sciences physiques des États-Unis.

3 **Biometrics Institute** Congrès 2021 - 13 octobre 2021, IDEMIA a fait une présentation intitulée *How to enhance biometric applications to protect privacy.*

https://www.biometricsinstitute.org/event/biometrics-institute-congress-2021/

4 **Série d'événements virtuels de l'EAB (European Association for Biometrics)** Equité démographique dans les systèmes biométriques-Mars 2021, IDEMIA a présenté une conférence sur *l'équité dans la reconnaissance des visages* et a participé à une table ronde avec des acteurs majeurs tels que le NIST et le Bureau de l'ONU pour la lutte contre le terrorisme.

https://eab.org/events/program/237

5 NIST Face Recognition Vendor Test.

https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

6 NIST Face Recognition Vendor Test, Part 3: Demographic Effects.

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

7 Stéphane Gentric, Responsable de la recherche en intelligence artificielle chez IDEMIA. Évaluation de la reconnaissance faciale @IDEMIA. In Proc. International Face Performance Conference, National Institute of Standards and Technology NIST, Gaithersburg, MD, novembre 2018. Page 8,

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

8 Ongoing Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Annexe 17 : Ampleur des scores des listes de candidats par sexe et par race. Page 24, figure 21.

https://pages.nist.gov/frvt/reports/demographics/annexes/annex_17.pdf

À propos d'IDEMIA Public Security

Justice and Public Safety est le nom du département d'IDEMIA Public Security qui travaille à mettre l'excellence de nos technologies biométriques au service des agences de forces de l'ordre. Elles leur permettent de prévenir plus d'infractions, de résoudre plus de crimes et de protéger une plus grande partie de la population.

Avec plus de 50 ans d'expérience et une équipe de près de 600 experts à travers le monde, nous nous consacrons au développement de technologies fondées sur la biométrie et de solutions qui améliorent l'efficacité et la fiabilité des initiatives de justice et de sécurité publique. Nos solutions, qui vont de la comparaison d'empreintes digitales à la reconnaissance faciale en passant par l'analyse des données d'enquête, sont conçues pour répondre aux besoins spécifiques des forces de l'ordre du monde entier.

Plus de 85 gouvernements dans 55 pays nous font confiance pour traiter et faire correspondre des millions d'empreintes digitales, de photos portraits et d'enregistrements d'empreintes latentes, ainsi que des données structurées et non structurées. Nous développons également des outils propriétaires de pointe tels que LiveScan et les dispositifs mobiles de prise d'empreintes digitales, afin de rendre le processus de maintien de l'ordre plus efficace. Notre objectif est de venir en soutien aux forces de l'ordre avec des ressources de pointe qui évoluent pour répondre à leurs besoins changeants tout en veillant à ce qu'ils disposent des outils dont ils ont besoin pour protéger et servir leurs communautés.

Chez IDEMIA Public Security, nous privilégions l'équité, la précision et la fiabilité dans toutes nos solutions. Nous travaillons main dans la main avec nos clients pour répondre aux besoins et aux défis qui leur sont propres, créant ainsi un monde plus sûr et plus sécurisé pour tout le monde.

Pour plus d'informations, visitez le site **www.idemia.com**

Suivre **@IdemiaGroup** sur LinkedIn

Ouvrir le monde,
Le rendre plus sûr.

IDEMIA GROUP

www.idemia.com