Comment lutter contre la fraude documentaire et vérifier l'authenticité des documents d'identité ?

Le projet de recherche iMARS (image Manipulation Attack Resolving Solutions), financé par la Commission européenne (CE), vise à lutter contre la fraude documentaire.

 # VOYAGE

POSTÉ LE 05.27.24

La fraude documentaire est une réelle problématique en Europe. D'après l'initiative SOCTA (Serious and Organized Crime Threat Assessment ou Évaluation des Menaces de Criminalité Grave et Organisée) d'Europol en 2021, « La fraude documentaire facilite la plupart des activités criminelles. Sont inclus tous types de crimes transfrontaliers, tels que le trafic de migrants, la traite des êtres humains ainsi que le trafic de stupéfiants, d'armes ou de véhicules volés. La fraude documentaire facilite également la fraude financière, la corruption, les crimes contre les biens et le terrorisme ». Dans sa dernière analyse des risques, Frontex explique que « la fraude documentaire est un élément clé de l'augmentation des menaces aux frontières extérieures de l'UE ». Le projet de recherche iMARS, financé par la Commission européenne (CE) dans le cadre de la convention de subvention 883356, a pour objectif de répondre à cette menace en élaborant des solutions pour lutter contre la fraude documentaire.

Le projet iMARS a commencé en septembre 2020 pour une durée de 48 mois. L'initiative est menée par IDEMIA et repose sur un consortium de 24 partenaires (universitaires, industriels, institutions gouvernementales) de 12 pays européens. Pour IDEMIA, le but principal de ce projet est d'étudier la manipulation des images de visage, en particulier le morphing, et de trouver des solutions pour la détecter. Le morphing consiste à mélanger les images numériques de deux individus pour créer une image hybride qui ressemble aux deux visages originaux. Ce processus est particulièrement difficile car l'image synthétique incorpore des caractéristiques des deux individus. Les fraudeurs, à l'aide du morphing des visages, ont la capacité de mélanger les caractéristiques faciales de deux personnes afin de créer une photo qui pourrait passer avec succès un contrôle visuel, et même tromper des systèmes de reconnaissance faciale avancée. iMARS cherche aussi à développer des outils mobiles qui pourraient aider les gardes-frontières dans leurs missions quotidiennes dans les États-membres européens. Ces outils permettront aux gardes-frontières de contrôler l'authenticité de documents d'identité et de détecter des images de visages manipulées.

En outre, ce projet vise à encourager la CE à mettre en place des centres spécialisés chargés de prendre et de soumettre des photos en direct pour les demandes et les renouvellements de passeports. Cela garantit que la photo n'a pas été altérée ou modifiée de quelque manière que ce soit.

Quels sont les objectifs de iMARS ?

iMARS a pour ambition d'aller au-delà des limites actuelles de la détection des manipulations des images et de la fraude afin d'améliorer la sécurité et de protéger les citoyens des actes malveillants tels que l'usurpation d'identité.

Vue d'ensemble des objectifs :

- Élaborer des solutions efficaces de Détection des Attaques par Morphing (Morphing Attack Detection, MAD) adaptées à l'enregistrement, aux enquêtes médico-légales et au franchissement des frontières.
- Développer un prototype de démonstration pour les outils de Vérification des Documents et de Détection des Fraudes (Document Verification and Fraud Detection, DVFD).
- Détecter les faiblesses des systèmes biométriques, en particulier vis-à-vis des attaques par morphing.
- Fournir des outils de DVFD aux services de gardes-frontières pour les soutenir dans leurs fonctions.
- Anticiper les nouvelles attaques par morphing sur les photos d'identité et autres données biométriques pour de futurs documents de voyage.
- Former les personnes en charge de l'application des demandes, de la délivrance et des vérifications des documents d'identité afin d'augmenter leur capacité à déceler une attaque par morphing.
- Standardiser la Détection des Attaques (Presentation Attack Detection, PAD) et l'évaluation de la qualité des photos d'identité.
- Fournir des références en libre accès pour les activités de recherche sur les MAD.
- Veiller à ce que les nouvelles technologies développées pour iMARS respectent la vie privée et les autres réglementations de l'UE et soient acceptées par les citoyens.

Quels sont les principales catégories de fraude documentaire ?

La fraude documentaire facilite la criminalité organisée au sein de l'UE. Les faux documents de voyage entraînent le risque de laisser passer des criminels, y compris des terroristes, ou des victimes de la traite des êtres humains. Il existe de nombreuses manières de modifier un document d'identité.

Voici les principaux types de fraude documentaire :

- Morphing photo : Utilisation d'une photo obtenue à travers le morphing de deux portraits dans un document authentique, permettant à deux personnes de partager le même passeport.
- Contrefaçon : Une reproduction complète d'un document authentique, réalisée avec des matériaux non authentiques ou en utilisant des parties d'un document authentique.
- Vol de documents vierges : De véritables documents vierges qui ont été volés afin de les personnaliser avec de fausses informations.
- Falsification : Une falsification des données personnelles ou des données rattachées à un document d'identité, par exemple en utilisant le morphing ou le remplacement de la photo.
- Usurpation d'identité : Utilisation d'un document authentique qui n'appartient pas au détenteur, parce que le fraudeur ressemble au porteur légitime du document.
- FOG : Un document authentique, mais obtenu frauduleusement (Fraudulently Obtained but Genuine, FOG) avec de fausses données et/ou une photo modifiée.

Quels sont les avantages à tirer d'iMARS ?

Solutions techniques

iMARS développe des solutions pour aider les professionnels impliqués dans la délivrance, l'utilisation et l'analyse médico-légale des documents d'identité, afin qu'ils puissent mieux détecter la fraude documentaire et la manipulation des photos d'identité. Ces solutions sont rapides et efficaces à la fois pour l'opérateur et le voyageur et sont compatibles avec les systèmes existants.

Le but est de renforcer la sécurité à l'échelle de l'UE. Il est également nécessaire de rétablir la confiance des citoyens dans le principe « un individu – un passeport » en renforçant la chaîne d'identité.

Formation

Les professionnels des frontières et les agents chargés des demandes de passeport doivent être davantage sensibilisés au morphing et à la manipulation des images ainsi qu'à la vulnérabilité des systèmes de reconnaissance faciale vis-à-vis des attaques par manipulation d'images.

Cependant, l'élément le plus important de la formation est de rendre les outils développés faciles d'utilisation. Tous les outils d'iMARS sont basés sur l'IA, et si elle soupçonne une tentative de fraude dans un processus de demande ou à la frontière, elle peut déclencher une alerte. Toutefois, seuls les humains, par exemple les gardes-frontières, peuvent déterminer :

- si le passeport contient une image modifiée.
- s'il s'agit d'une attaque de présentation.
- si le passeport a été falsifié.

Pendant que les contrôles sont effectués par des personnes qualifiées, la personne qui présente le document suspect doit être traitée de manière équitable et éthique, conformément aux exigences légales. Tous ces éléments sont indispensables pour exploiter les résultats du projet iMARS et peuvent être réalisés grâce à des sessions de formation, des recommandations, des bonnes pratiques, des évaluations en ligne et des ateliers.

Normalisation

iMARS assurera l'adoption par les organismes de normalisation des résultats suivants du projet :

- Procédures de délivrance des documents de voyage
- Évaluation de la vulnérabilité des sous-systèmes biométriques aux attaques par morphing
- Évaluation de la qualité des images de visages
- PAD

iMARS a également travaillé sur une plateforme d'évaluation qui met en œuvre des références claires, réalistes et reproductibles pour estimer les progrès des algorithmes.

Le rôle d'IDEMIA dans le projet iMARS

L'objectif principal d'IDEMIA dans ce projet est de détecter les documents qui ont été modifiés ou les documents qui ne correspondent pas à des types de documents authentiques connus.

IDEMIA a mis au point une méthode innovante et à l'épreuve du temps pour détecter les attaques de présentation et les attaques contradictoires.

Contrôle des documents et mécanismes de détection des fraudes

La classification des documents consiste à déterminer les principales caractéristiques d'un document présenté.

Ces caractéristiques comprennent :

- Le type de document tel quel défini par l'Organisation de l'aviation civile internationale (ICAO) (ID1/ID2/ID3)
- La catégorie de document
- Le modèle et le numéro de série
- Le pays d'origine

IDEMIA a entrepris des recherches sur la détection de la fraude à l'aide d'une analyse reposant sur les capteurs disponibles sur les smartphones utilisés par les gardes-frontières pour garantir l'authenticité des documents.

Il s'agit notamment d'avoir recours au réseau neuronal à convolution pour vérifier si le document a été imprimé ou présenté sur un écran. Cet outil détecte également les différences de polices sur le document.

PAD – Détection d'attaque de présentation

On parle d'attaque de présentation lorsqu'une personne se déguise pour ressembler à quelqu'un d'autre afin de pouvoir utiliser son document d'identité, notamment son passeport. Les attaques de présentation peuvent apparaître sous plusieurs formes : maquillage, masque, cacher son visage sous une photo ou une tablette, etc. Les méthodes de détection existantes sont bien adaptées aux attaques connues, mais elles ne peuvent pas nécessairement détecter les nouvelles attaques.

Avec l'initiative iMARS, IDEMIA a mis au point une stratégie de PAD qui ne détecte que les présentations authentiques et alerte les autorités lorsqu'une présentation ne répond pas aux critères d'authenticité. Par conséquent, cette technique PAD résiste aux nouveaux types d'attaques de présentation qui pourraient être inventés à l'avenir.

Détection des attaques adverses

Bien qu'elles soient visibles à l'œil nu, les attaques adverses peuvent inciter les algorithmes de Machine Learning / Deep Learning (ML/DL) à prendre des décisions erronées. Le type d'attaque le plus courant consiste à ajouter du bruit à haute fréquence (appelé bruit adverse) pour modifier l'interprétation d'un algorithme ML/DL. Prenons l'exemple d'un fraudeurs interdit de voyage qui aurait créé un faux document d'identité en utilisant la photo d'un complice. La photo peut être modifiée à l'aide d'un bruit contradictoire spécifique, ce qui permet à l'algorithme de reconnaissance faciale de correspondre faussement à la photo manipulée, et donc au fraudeur de voyager.

IDEMIA a travaillé sur la détection des attaques adverses et a créé un processus de détection nettement plus rapide. En développant et en brevetant un cadre complet, IDEMIA a été en mesure de lutter contre les attaques adverses. Le mécanisme de détection et les réseaux biométriques fiables utilisés en cas de suspicion de fraude constituent le cœur du cadre.

Développement du démonstrateur

Un démonstrateur Android™ est déjà disponible, avec les fonctionnalités nécessaires pour évaluer si un document est authentique ou non et pour vérifier le lien entre le document et le détenteur.

Un composant de communication en champ proche lit les données de la puce du passeport, et un contrôle de qualité du visage conforme aux normes de l'ICAO, intégré au démonstrateur, évalue la qualité d'une image de selfie. L'outil PAD, également intégré au démonstrateur, capture une courte vidéo pour l'analyse des documents.

Cela permet d'effectuer les étapes suivantes :

- Classification des documents d'identité
- Détection des fraudes
- Vérification biométrique du détenteur, y compris l'évaluation de la qualité, et mécanismes de présentation et de MAD
- Mécanismes de DVFD

Exploitation

IDEMIA estime qu'il existe deux façons d'exploiter commercialement les résultats des travaux menés dans le cadre de projets de recherche collaborative.

La première consiste à améliorer en permanence les algorithmes et les méthodes utilisés dans les produits déjà disponibles, tels que les outils de détection des passeports frauduleux. Toutefois, il ne faut pas oublier que les méthodes existantes peuvent être améliorées et que de nouvelles méthodes de détection de la fraude peuvent être développées.

La deuxième consiste à évaluer la faisabilité des innovations : s'assurer que la technique fonctionne, que les utilisateurs finaux définissent ce qui, d'un point de vue opérationnel, pourrait les aider dans leurs fonctions, et que le marché est réel et abordable pour l'établissement qui déploie la solution. iMARS envisage ces deux types d'exploitation.