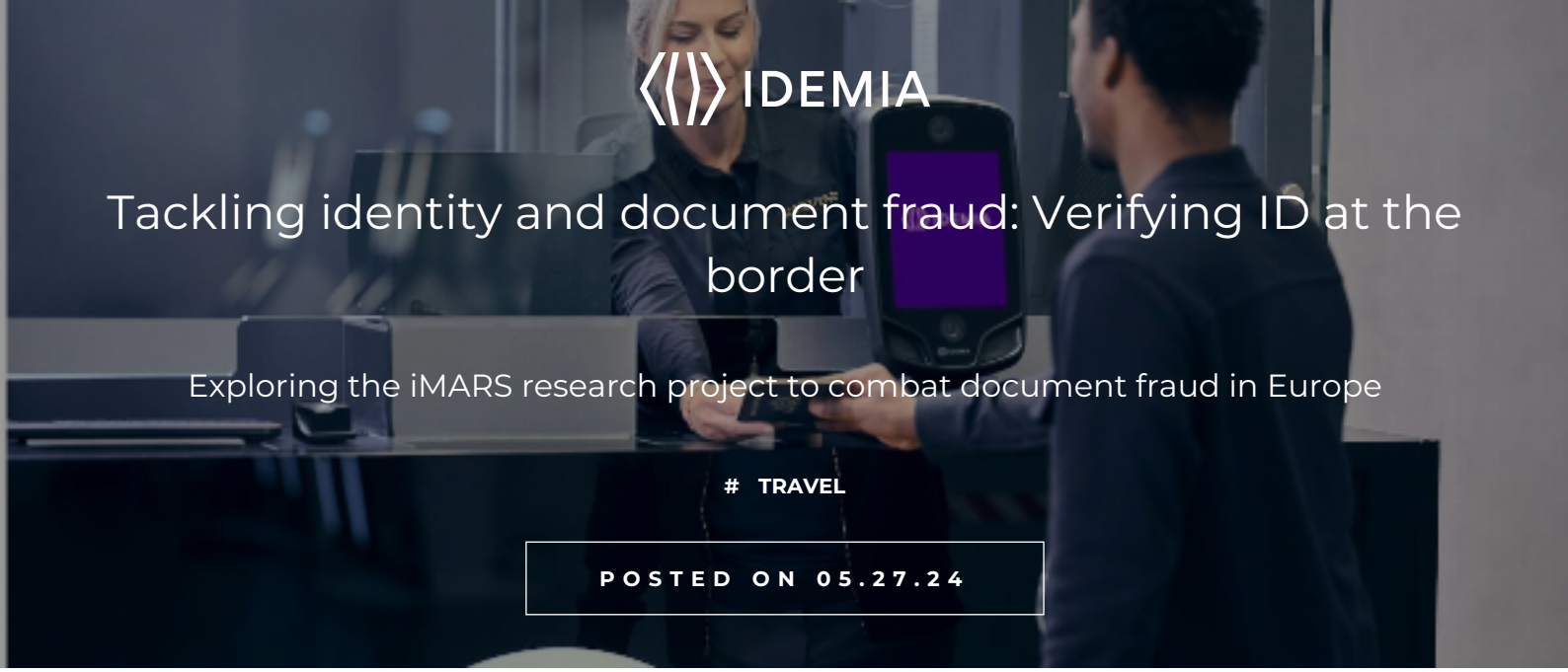

Tackling identity and document fraud: Verifying ID at the border

Exploring the iMARS research project to combat document fraud in Europe

 # TRAVEL

POSTED ON 05.27.24

Document fraud is a concern for Europe. Europol's Serious and Organized Crime Threat Assessment (SOCTA) of 2021 reported, "Document fraud is an enabler for most criminal activities. This includes all types of cross-border crime, such as migrant smuggling, trafficking in human beings as well as the trafficking of drugs, weapons, or stolen vehicles. Document fraud can also facilitate general financial fraud, corruption, property crime, and terrorism." Frontex reports, in its latest risk analysis, "Document fraud continues to be a key enabler of threats at the EU's external borders." The iMARS (image manipulation attack resolving solutions) research project, funded by the European Commission (EC) under grant agreement 883356, intends to address this threat, by developing solutions against document fraud.

iMARS started in September 2020 and is running for 48 months. It is led by IDEMIA and has a consortium of 24 partners (academics, industrials, and government agencies) from 12 European countries. For IDEMIA, the primary goal of this project is to study face image manipulation, especially morphing, and find solutions to detect it. Morphing involves blending the digital images of two individuals to create a hybrid image that resembles both original faces. This process is particularly challenging because the synthetic image incorporates features from both individuals. Fraudsters exploit facial morphing to generate photos that can potentially pass visual inspections and even deceive advanced facial recognition systems. iMARS also includes the development of mobile tools to support border guards in European member states with their daily missions. These tools will allow border guards to verify the authenticity of identity documents and detect manipulated face images.

Furthermore, this project sets out to encourage the EC to allocate dedicated centers that are responsible for taking and submitting live photos for passport requests and renewals. This would guarantee that the photo has not been tampered with or altered in any way.

What are iMARS' objectives?

iMARS aims to overcome current limitations on image manipulation detection, and document and fraud detection, to increase security and protect citizens from malicious acts such as identity theft.

Overview of the objectives:

- Develop efficient Morphing Attack Detection (MAD) solutions that are suitable for enrollment, forensic investigation, and border crossing.

- Develop a prototype demonstrator for Document Verification and Fraud Detection (DVFD) tools.
- Assess vulnerabilities in biometric systems, notably against morphing attacks.
- Provide DVFD tools to support border guards with their missions.
- Anticipate new morphing attacks against face images and other biometric modalities for future travel documents.
- Train people involved in ID document application, delivery, and checks to increase their ability to detect morphing attacks.
- Standardize Presentation Attack Detection (PAD) and face image quality assessment.
- Provide open access benchmarks to research activities on MAD.
- Ensure that new technologies developed for iMARS respect privacy and other EU regulations and are accepted by citizens.

What are the main types of document fraud?

Document fraud facilitates organized crime in the EU. Counterfeit travel documents generate the risk of letting through criminals, including terrorists, or victims of human trafficking. There are many ways to alter an identity document.

Here are the main types of document fraud:

- Morphed photo: Use of a morphed image in a genuine document, allowing two individuals to share the same passport.
- Counterfeit: The complete fake reproduction of a genuine document made with non-genuine materials or using parts of genuine documents.
- Stolen blank documents: Genuine blank documents that have been stolen in order to personalize them with false information.
- Forgery: Falsification of personalized or affixed data on an ID document—for example, using a replacement photo.
- Impostor: Use of a genuine document that does not belong to the holder, because the fraudster resembles the legitimate document bearer.
- FOG: Fraudulently Obtained but Genuine document with false data and/or manipulated portrait.

What are the benefits of iMARS?

Technical solutions

iMARS is developing solutions to help professionals involved in ID document delivery, usage, and forensic analysis, so that they can better detect document fraud and face image manipulation. These solutions are fast and efficient for both operators and travelers and are compatible with existing systems.

The target is to increase security at an EU level. There is also a need to reestablish citizens' trust in the principle 'one individual—one passport' by strengthening the chain of identity.

Training

Awareness needs to be increased, among border professionals and passport application officers, of image morphing and manipulation and the vulnerability of facial recognition systems to image manipulation attacks.

However, the most important element of training is to make the developed tools usable. All of iMARS' tools are based on AI and if it suspects a fraud attempt in an application process, or at the border, it can raise an alert. But only humans, for example border guards, can decide if:

- the passport contains a manipulated image.
- there is a presentation attack.
- the passport is forged.

While checks are being conducted by qualified people, the person presenting the suspected document must be treated fairly and ethically, in compliance with legal requirements. All of this is mandatory to exploit iMARS' results, and can be achieved with training sessions, guidelines, best practices, online evaluations, and workshops.

Standardization

iMARS will ensure adoption by the standardization bodies for the following project results:

- Travel document issuance procedures
- Vulnerability assessment of biometric subsystems for morphing attacks
- Face image quality assessment
- PAD

iMARS has also worked on an evaluation platform which implements clear, realistic, and reproducible benchmarks to assess the progress of algorithms.

IDEMIA's role in the iMARS project

IDEMIA's main aim in this project is to detect documents that have been altered or documents that do not correspond to known, genuine document types.

IDEMIA has developed an innovative and future-proof method to detect presentation and adversarial attacks.

Document Verification and Fraud Detection mechanisms

Document classification is determining the key characteristics of a presented document.

The characteristics include:

- Type of document as defined by ICAO (ID1/ID2/ID3)
- Category of document
- Model and serial number
- Country of origin

IDEMIA has worked on the detection of fraud based on an analysis using common sensors available in smartphones used by border guards to ensure document authentication.

This includes the use of the convolutional neural network to check if the document was printed or presented on a screen. It also detects inconsistent fonts used in the document.

PAD—Presentation Attack Detection

A presentation attack is when a person disguises themself to look like someone else so that they can use their identity document, notably their passport. Presentation attacks can take many forms: makeup, masks, covering your face with a photo or tablet, etc. Existing detection methods are well suited to known attacks, but they cannot necessarily detect new attacks.

In iMARS, IDEMIA developed a PAD strategy that detects bona fide presentations only and alerts authorities when a certain presentation does not seem genuine. Consequently, this PAD technique is resistant to new types of presentation attacks that may be invented in the future.

Adversarial attack detection

Despite being visible to the human eye, adversarial attacks can trick Machine Learning / Deep Learning (ML/DL) algorithms into making incorrect decisions. The most common type of adversarial attack is adding high-frequency noise (aka adversarial noise) to change the interpretation of an ML/DL algorithm. Imagine a fraudster, who is banned from traveling, creating a fake identity document using a photo of an accomplice. The photo can be modified using specific adversarial noise, allowing the facial recognition algorithm to falsely match the manipulated photo, and thus enabling the fraudster to travel.

IDEMIA has worked on the detection of adversarial attacks and created a significantly faster detection process. By developing and patenting a complete framework, IDEMIA was able to defend against face adversarial attacks. The framework's core is the detection mechanism and the robust biometric networks used when fraud is suspected.

Demonstrator development

An Android™ demonstrator is already available, with functionalities required to assess if a document is genuine or not and to verify the link between the document and the holder.

A near-field communication component reads the data of the passport chip, and an ICAO compliance face quality check, integrated into the demonstrator, assesses the quality of a selfie image. PAD, also integrated into the demonstrator, captures a short video for document analysis.

This allows the following steps to be performed:

- Classification of the ID document
- Detection of fraud
- Biometric verification of the holder, including quality assessment, and presentation and MAD mechanisms
- DVFD mechanisms

Exploitation

IDEMIA believes there are two ways to commercially exploit the results of the work being carried out in cooperative research projects.

The first is to continuously improve the algorithms and methods used in products already available, such as tools that detect fraudulent passports. However, we must remember that existing methods can be improved, and new fraud detection methods can be developed.

The second is assessing the feasibility of innovations: ensuring that the technique works, that end users define what, operationally, could help them with their missions, and that the market is real and affordable for the establishment deploying the solution. iMARS is considering both types of exploitation.