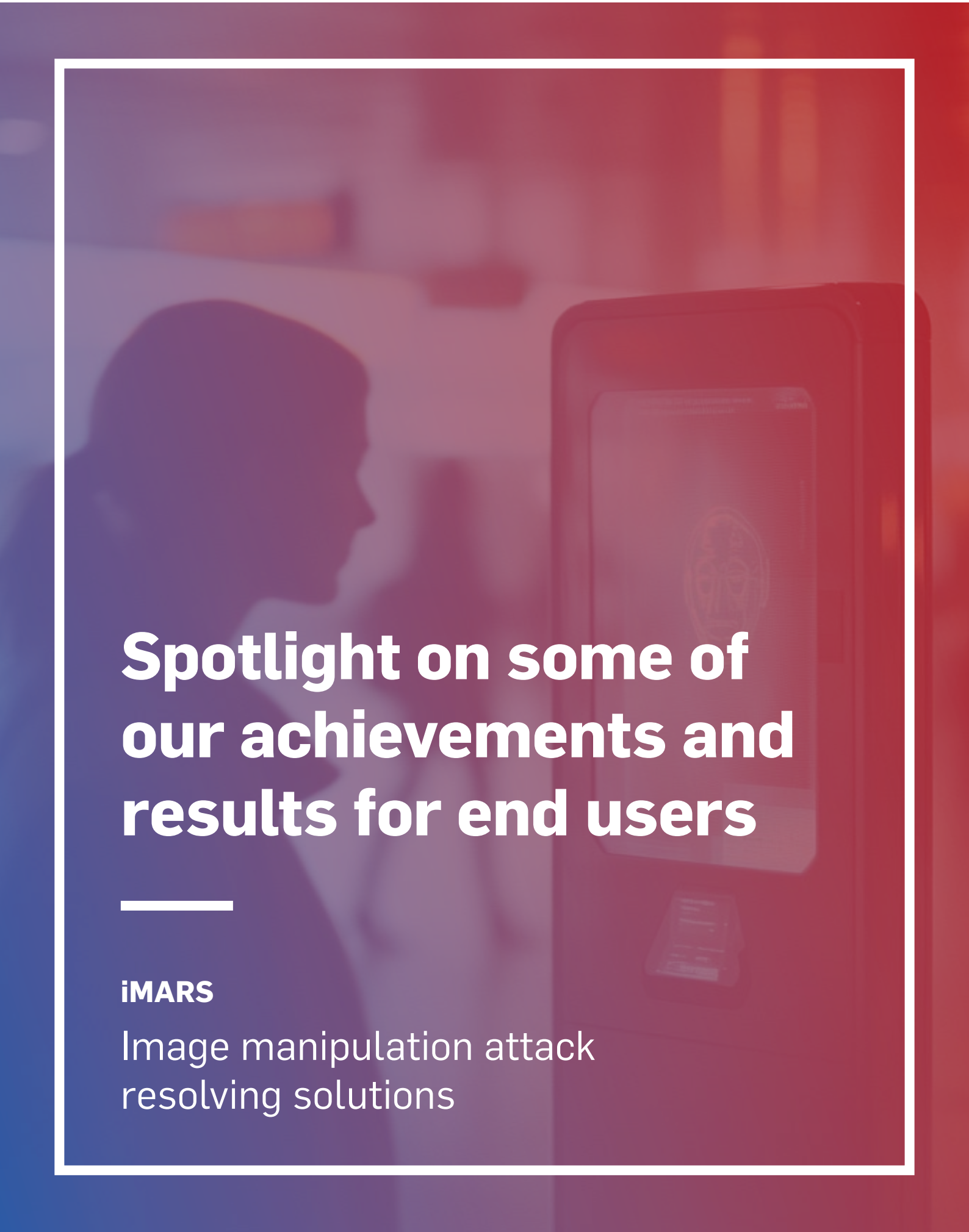
iMARS
image manipulation attack
resolving solutions

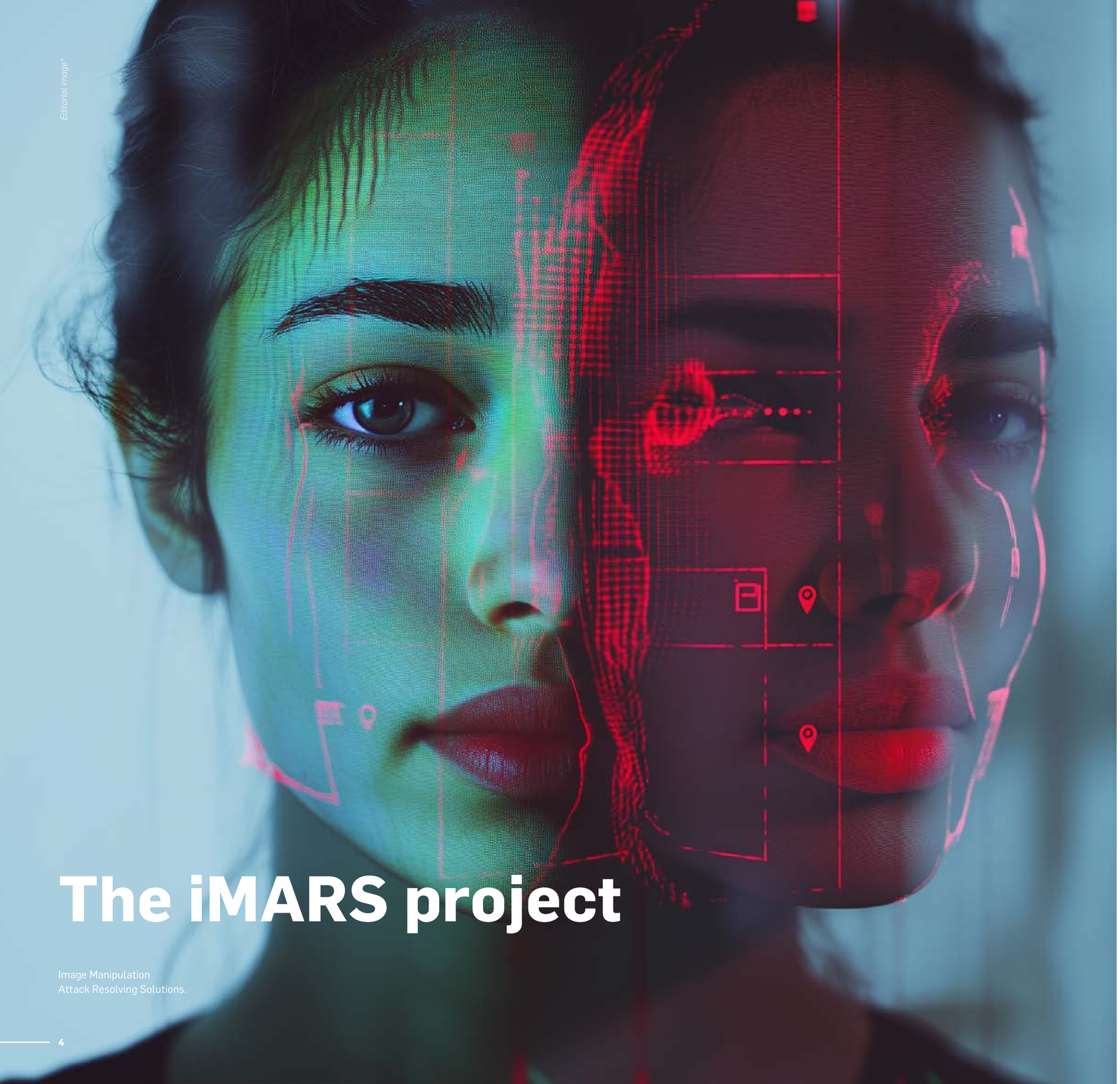


Spotlight on some of our achievements and results for end users

iMARS

Image manipulation attack resolving solutions

Table of contents



Editorial Image*

The iMARS project

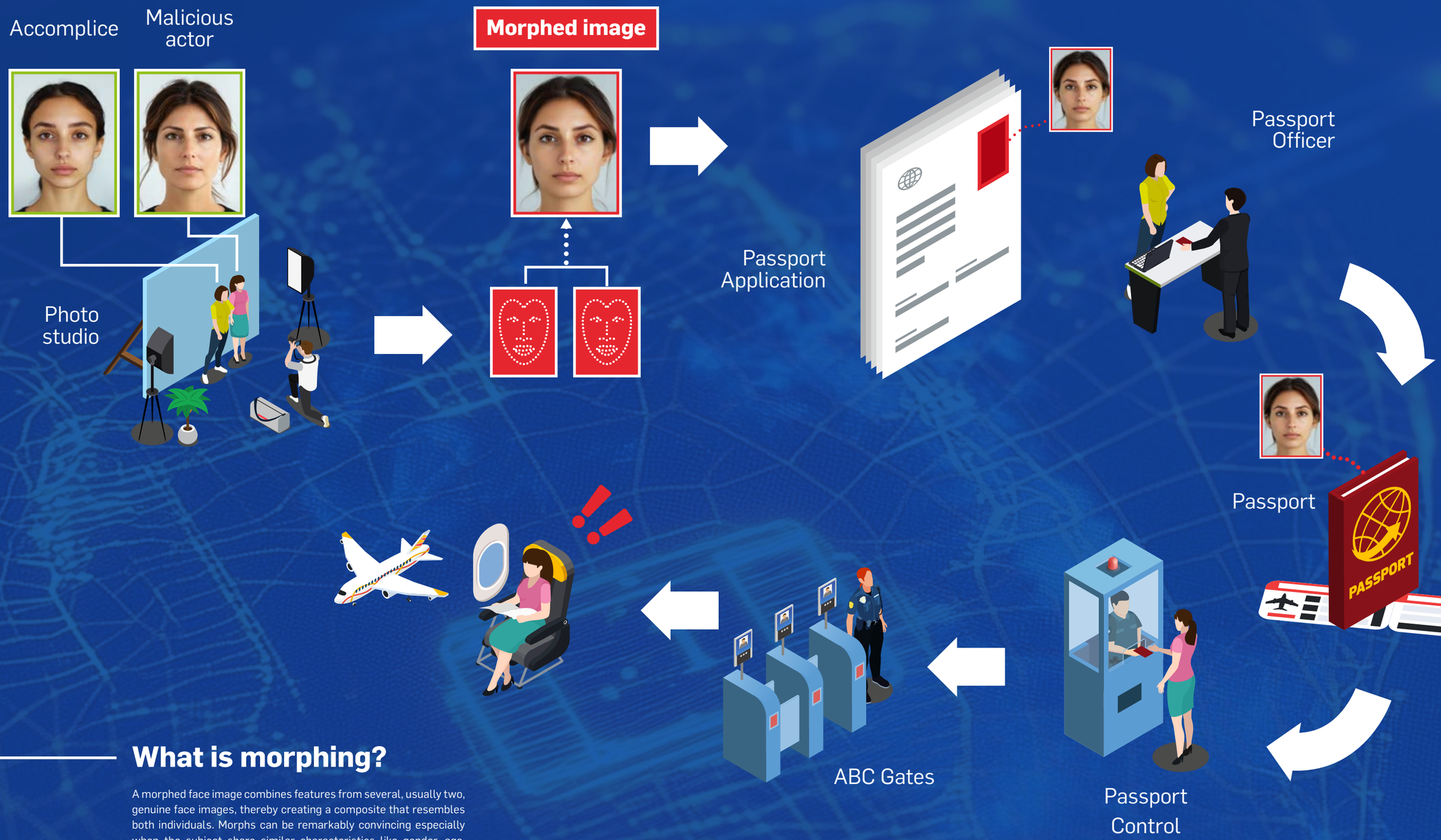
Image Manipulation
Attack Resolving Solutions.

Document and identity fraud at large

The iMARS project, funded by the European Union, developed solutions to fight identity and travel document fraud. Document and identity fraud is recognised as a major threat to European security by Frontex and is mentioned in Europol's Serious and Organised Crime Threat Assessment (SOCTA) since 2017.

There are many types of document fraud: counterfeits, forgeries, pseudo documents, fraudulently obtained genuine documents, or genuine document misuse by an impostor[1]. Though iMARS targets multiple types of fraud, it particularly studied a specific risk: **fraudulently obtained genuine documents displaying a morphed face image.**

» 1 https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud



Process flow of a traveller exploiting identity fraud with the help of genuine documents containing a morphed face image

What is morphing?

A morphed face image combines features from several, usually two, genuine face images, thereby creating a composite that resembles both individuals. Morphs can be remarkably convincing especially when the subject share similar characteristics like gender, age, and ethnicity. When a criminal associates with an accomplice who bears a reasonable resemblance, highly convincing morphs can be achieved, potentially deceiving even expert document examiners.

There are many ways to morph two or more face images. Some rely on feature points of the face (e.g., middle of the lip, corner of an eye), and some rely on deep learning. The large diversity of morphing methods presents different challenges, making the determination of whether a face image is morphed a complex task – both for humans and algorithms.

iMARS context and objectives

iMARS started in September 2020, after it became certain that morphing had already been used by criminals to build fraudulent ID documents. iMARS followed a project called SOTAMD (State of the Art Morphing Detection), which also focused on morphing attack detection. Building on the initial understanding acquired by SOTAMD, iMARS aimed to overcome challenges by:

- Analyse vulnerabilities in the application process of id documents and formulate recommendations
- Understanding the ability of systems and people to detect morphed images in genuinely issued passports.
- Developing robust Morphing Attack Detection (MAD) technologies to detect morphing attacks automatically that are: (1) robust to a diversity of morphing attack types; (2) sustainable and able to detect the "morphing attacks of the future"; (3) suitable both for forensic experts who only have the ID document in front of them, and for border guards who simultaneously verify the ID document and its (legitimate or illegitimate) holder, whilst meeting operational needs in term of accuracy tradeoff for both.
- Developing a sustainable platform that can measure MAD algorithms' performance and evolve alongside new MAD techniques.
- Enhancing the capability of border guards and other examiners to visually identify a morphed face image.
- Developing standards to measure and evaluate MAD solutions.
- Determining the influence of face image quality on the performance of MAD solutions, and agree on a standard face-quality metric.

When iMARS started, the National Institute of Standards Technology (NIST) had already put in place a MAD evaluation benchmark, showing that performance of State of the Art MAD in 2020 were far from iMARS targets.

iMARS also considered other forms of identity document fraud and studied other types of face-image manipulation attacks such as beautification, face masks, or makeup attacks. The project explored the legal and ethical context around iMARS technologies, including the Artificial Intelligence Act[2] that entered into force while iMARS was running.

> As a citizen I would like the authorities to arrest criminals, but at the same time I would dislike to be suspected each time I cross the border. iMARS aimed at document fraud detection technologies that are efficient against criminals and at the same time traveller's friendly.

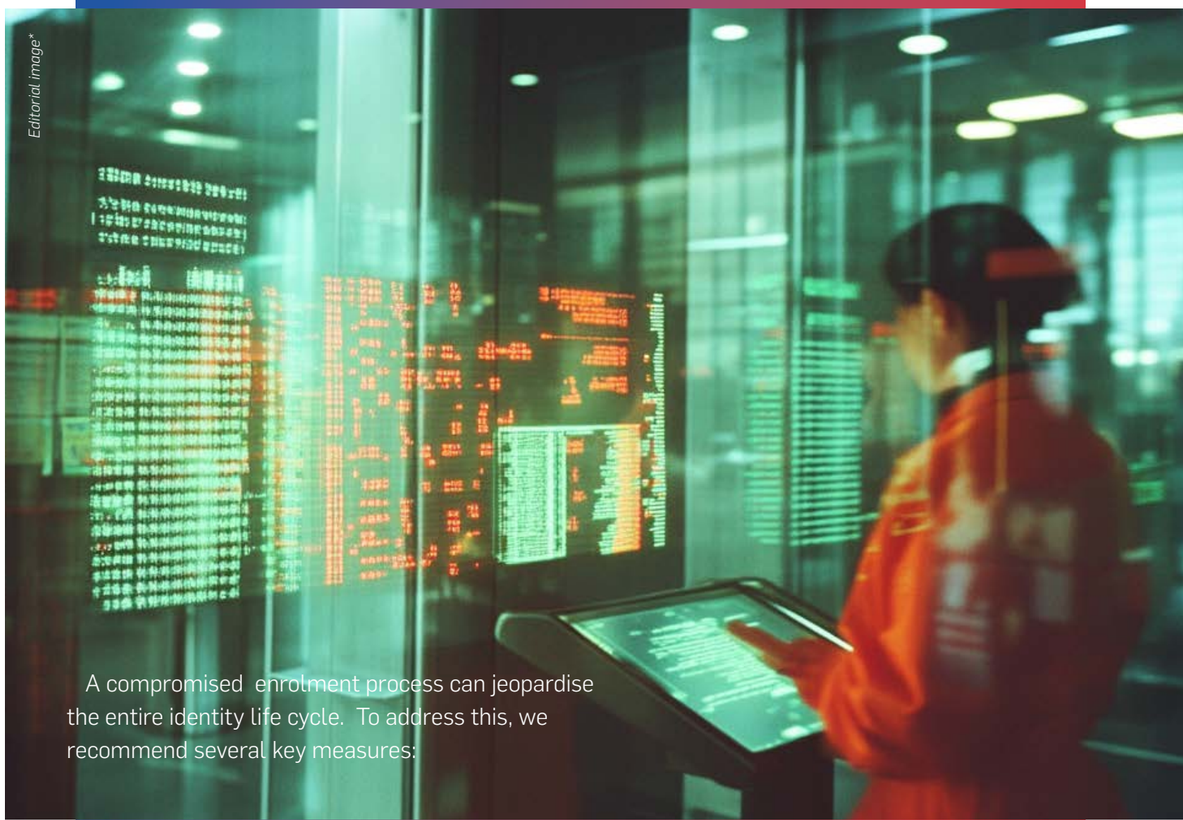
» 2 https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Findings and insights

The iMARS project achieved all its initial goals. In the field of MAD, we are now reaching an accuracy level that makes the technology suitable for detecting automatically generated morphs and average-quality morphs. We developed a training programme for ID document experts to support the verification of the diagnosis made by MAD algorithms, ensuring that humans remain in control. We have also developed a platform – BOEP - to measure the performance of MAD algorithms - offering interesting alternatives and distinctions to the NIST platform. iMARS has contributed to a standard to measure the impact of face image quality on MAD . The vulnerability of current face recognition systems has been assessed to make users aware of the risks and provide improvement targets to developers. Furthermore, we have produced guidelines to further develop and deploy iMARS technologies in a way that is compliant with regulations.

As we have reached the end of the iMARS project, both research and industry are now in a position to provide border guards and forensic experts with significant tools to detect morphing attacks.

This brochure aims to briefly introduce to end users and policy makers some of the key activities performed in iMARS, presents practical solutions that come out of our project and highlights where further research could be beneficial to continue the fight against morphing and other manipulation attacks.



*Editorial image**

iMARS Achievements

Safe enrolment systems and processes

‘Enrolment’ can be defined as the process starting with the application for an ID document and ending with the delivery of the document to the applicant. The security of its design has a potentially large impact on border security: an enrolment process that can be compromised jeopardises the entire identity life cycle, including the use of ID documents at the border control environment which requires the highest level of safety and security. **The more secure the ID enrolment is, the more secure the Border Control becomes.**

It is, therefore, of great importance to ensure that enrolment processes are designed with the latest insights on how to mitigate, remove or prevent risks of the process being compromised.

A compromised enrolment process can jeopardise the entire identity life cycle.

Strengthening ID Document Enrolment: A Comprehensive Model for Security and Resilience

We broke down the ID document enrolment process into sub-processes. For each sub-process, we identified most, if not all, possible variations. This model can be used to describe current and envisaged enrolment processes and to analyse their vulnerabilities. We provided elaborate practical and technical recommendations to improve the security of current and envisaged ID document enrolment processes, taking into account the most recent technological developments and threats, existing standards, and legal, ethical and societal requirements. Moreover, we proposed and demonstrated the use of face-image quality and manipulation detection components in the enrolment process. Last but not least, we evaluated possible criminal reactions to the proposed enrolment designs, taking our analysis one step ahead and outlining potential solutions that authorities could employ to uncover such criminal counter-forensic techniques in the digital domain.

Key measures for enhancing security through a resilient enrolment process

We began with compiling an inventory of 28 enrolment processes from eight EU countries. Our in-depth analysis revealed gaps and possible risks in current and envisaged enrolment processes. Based on these findings, we provided recommendations in terms of components and practices to mitigate each of these risks. We also anticipated how criminals might attempt to circumvent the proposed security measures. Analysis of ethical, legal and societal aspects helped ensure a balance between security risks and rights and privacy.

Lessons learnt

A compromised enrolment process can jeopardise the entire identity life cycle. To address this, we recommend several key measures:

- Printed images should not be accepted but rather phased out.
- Supervised (digital) image acquisition is recommended.
- Implementation of biometric deduplication to ensure that each person can only register once is recommended.
- Multimodal strategy for biometric data collection, i.e., acquisition of more than one modality (face, fingerprint, iris), is recommended.
- Enrolment from smart phones or other mobile devices is not yet mature enough to be used securely.
- Secure protocols for data transmission are necessary.

Morphing Attack Detection methods

Differential Morphing Attack Detection Methods

Morphing attacks pose a significant threat for border crossing and identification-control scenarios. The Differential Morphing Attack Detection (D-MAD) methods involve the examination of two images: a passport image, which may be bona fide or morphed, on one side and a live capture image on the other. The D-MAD approach aligns closely with the main goal of iMARS: to effectively detect identity fraud and image manipulation forgeries.

Advancing Image Pair-Based Detection: From Development to Rigorous Testing

iMARS developed image pair-based MAD techniques before testing and adapting them to the ID document lifecycle. We specifically focused on robustly detecting morphed face images taking into account image processing effects resulting from printing and scanning. Researchers also analysed factors such as visualization, computational effort and storage requirements, in addition to detection performance. Furthermore, to enhance the robustness and detection performance of image-pair-based morphing attack detection in a real-world automated border control scenario, we applied information fusion techniques to combine complementary approaches. Throughout the project, partners evaluated at least three different algorithms on two distinct platforms: the Bologna Online Evaluation Platform (BOEP)[3] and NIST[4].

We learnt that deep-learning approaches based on implicit algorithms outperform the explicit algorithms that are based on machine learning. However, the explainability of the results is still a challenge. The generalisation capabilities are still very dependent on train data, where bona fide images databases are still insufficient in quantity. The synthetic images show that they can be useful but not resolve the D-MAD challenge.

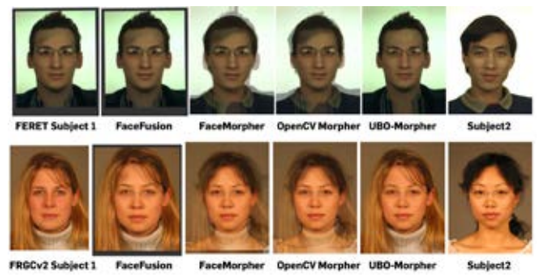
After proposing different image pair-based morph detection algorithms based on facial landmarks/features and general-purpose texture descriptors, we improved the existing face de-morphing techniques. We explored and improved the implicit and explicit approaches based on machine learning and deep-learning algorithms and we proposed new print/scan algorithms to create morph images.

The following table show the results obtained by the algorithm proposed by various partners in the project in D-MAD for a common test set dataset in BOEP platform. The evaluation for NIST platform can be found in the NIST Fate Morph report[5].

We explored and improved the implicit and explicit approaches based on machine learning and deep-learning algorithms and we proposed new print/scan algorithms to create morph images.

Benchmark	EER	$BPCER_{10}$	$BPCER_{20}$	$BPCER_{100}$
DMAD-IMARS-HQ_FULL-1.0	4.07%	0.60%	2.57%	16.97%
DMAD-IMARS-HQ_SMALL-1.0	4.10%	0.60%	2.57%	16.97%
DMAD-IMARS-HQ_HARD-1.0	2.15%	0.50%	0.70%	6.30%
DMAD-IMARS-MQ_FULL-1.0	7.54%	3.84%	15.50%	41.66%
DMAD-IMARS-MQ_SMALL-1.0	7.64%	3.84%	15.82%	41.70%
DMAD-IMARS-MQ_HARD-1.0	5.22%	2.93%	5.67%	30.13%

Best DMAD results on the iMARS BOEP benchmarks



Examples of different morphing algorithms for two subjects in the FERET and FRGCv2 databases. J. E. Tapia and C. Busch, "Single Morphing Attack Detection Using Feature Selection and Visualization Based on Mutual Information," in IEEE Access, vol. 9, pp. 167628-167641, 2021, doi: 10.1109/ACCESS.2021.3136485.

» 3 https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx
» 4 https://pages.nist.gov/frvt/html/frvt_morph.html
» 5 https://pages.nist.gov/frvt/html/frvt_morph.html

Single Morphing Attack Detection Methods

iMARS also aimed to develop automatic MAD methods when only a single image is available for processing. Here, we focused on the scenario where a morphed face image is presented during the enrolment stage. We have conducted comprehensive research activities and developed robust S-MAD algorithms including explainable methods and advanced AI techniques.

25 research works related to S-MAD were carried out, resulting in 18 peer-reviewed scientific papers, either submitted or accepted, indicating the novelty and contribution to the research community. Ten of the developed algorithms were evaluated in public platforms such as the BOEP platform and NIST FATE MORPH. We achieved considerable improvements in S-MAD methods from different perspectives such as algorithm design, training strategy, data augmentation, and explainability. In a longer term, the achievements provide both robust solution for S-MAD but also insight on the state of the S-MAD algorithms, which can be used as reference information for further policy making or practical implementation.

To achieve these robust S-MAD algorithms, different partners contributed by studying subtopics. The approaches cover explainable computer vision techniques, digital forensic techniques, AI-driven deep-learning techniques. The studies also addressed the challenges of data shortage without violating privacy legitimations by exploring new training frameworks such as continual learning or use of synthetic data.

Optimising S-MAD: Feature Extraction, Fusion Techniques, and Data Challenges

The common approach is to extract features from the image and then to apply classification using machine-learning or deep-learning techniques. Frequency analysis and residual noise are effective techniques for preparing data to enhance attack detection. It is also beneficial to extract features and classify information from different face regions, or design algorithms that fuse local and global information, as the distribution of landmark points and traces of morphing can vary in these regions. The generalisability of S-MAD algorithms on different morphing algorithms, different dataset, and different post-processing procedures remains challenging as the input does not include additional information from supportive samples. Another common challenge is the shortage of training data. When training and testing with a small size dataset, the explicit S-MAD algorithms may even achieve better results than implicit algorithms based on deep-learning modes that require more training data to avoid overfitting.

» **Further information:**
https://biolab.csr.unibo.it/fvcongoing/UI/Form/BenchmarkAreas/BenchmarkAreaSMAD.aspx

Benchmark	EER	$BPCER_{10}$	$BPCER_{20}$	$BPCER_{100}$
SMAD-IMARS-HQ_FULL-1.0	8.33%	7.33%	16.33%	46.00%
SMAD-IMARS-HQ_SMALL-1.0	8.39%	7.33%	16.67%	46.00%
SMAD-IMARS-HQ_HARD-1.0	7.68%	6.00%	12.00%	32.67%
SMAD-IMARS-MQ_FULL-1.0	5.05%	3.90%	5.37%	11.71%
SMAD-IMARS-MQ_SMALL-1.0	4.86%	3.90%	4.88%	10.73%
SMAD-IMARS-MQ_HARD-1.0	4.85%	2.44%	4.88%	6.83%

Best SMAD results on the iMARS BOEP benchmarks

We achieved considerable improvements in S-MAD methods from different perspectives such as algorithm design, training strategy, data augmentation, and explainability.

Human capability

By examining how human observers recognise morphing attacks we can establish the detection susceptibility of humans. One prevalent misconception is that an examiner or observer's ability to detect facial morphs is solely reliant on their expertise, experience, and familiarity with the issue. In reality, no studies have specifically reported the performance of professionals who regularly verify identity documents with facial images This gap is concerning, as any lapse in their competence can result in significant societal challenges.

iMARS assessed the proficiency and competence f ID issuance and verification professionals from more than 40 countries, in identifying bona fide vs altered images. . The study not only highlighted the need for dedicated training programs but also helps inform their design. The broader impact of the findings demonstrates the importance of matching professionals to suitable roles (e.g., issuance versus verification) and to provide the right training (e.g. face examination training versus fingerprint examination) to improve competencies.

Our team designed experiments to simulate realistic border-crossing scenarios like Automated Border Control (ABC) gates, considering various settings for enrolment and verification. iMARS involved experts in face comparison and fingerprint, document examiners (1st, 2nd and 3rd line), ID experts from embassies, police and other government authoritie, case handlers for ID, visa and passport, and border guards (1st line, 2nd line). We then inventoried current challenges and skill gaps, conducting a quantitative analysis on detection performance for ID issuance, verification and border crossing protocols. Dedicated settings assessed human ability to detect: (1) morph vs bona fide (2) morph vs. ABC-gate image (3) post-processed morph image vs bona fide (4) post-processed morph vs ABC-gate image (5) bona fide vs bona fide. 400 probe images were used to study the ability of human observers to detect morphed images. A new dataset of 180 morphing images was also produced to study human capacity in the S-MAD environment.

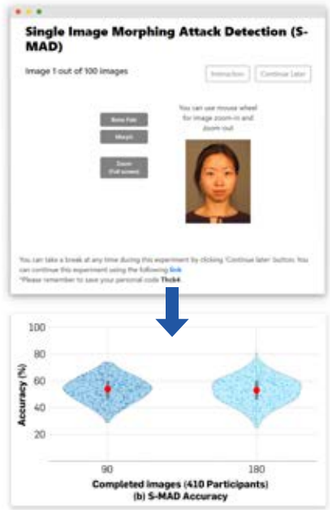
The invitation to participate in the experiment has raised the awareness of the issue of morphing. Many governmental agencies have requested dedicated training to increase their competence in manipulation detection.

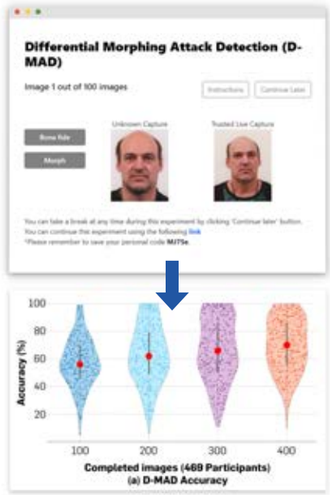
Lessons learnt

- The accuracy of various groups of observers indicate that certain types of training make observers better than others for MAD tasks.
- An indicative correlation between detection accuracy and experience in the line of work was noted. Face comparison experts perform better in identifying morphs , which may indicate a favourable influence of prior experience over observers in other fields of work.
- Our studies indicated that the average error rate of those who have received training is significantly lower than that of those who have not for document training and facial examination, indicating the effect of training.
- The algorithms perform better in both S-MAD and D- MAD settings as compared to human observers, indicating a gap in the ability to detect morphs as efficiently as algorithms.
- One key take away is that volume training makes experts better at detecting morphs, which underlines the need for dedicated training programs. Exposure to hundreds of images increased the observers' average morph detection accuracy.
- Effort and time spent on the image examination task in the experiment is not necessarily similar to that spent in a real-life scenario.

» **Further information:**
https://ieeexplore.ieee.org/document/9997091

https://dl.acm.org/doi/abs/10.1145/3658664.3659649





Document verification and fraud detection

To counter security threats, counterfeited and forged travel documents detection tools were developed, for use by both security professionals and citizen in self-assessment frameworks. The wide variety of travel documents coming from various countries, each with their own specific security features, represents a significant challenge for border guards and others professionals in their assessment and determination of whether a documents is genuine, counterfeit or a forgery.

Algorithms based on artificial intelligence were developed to automatically classify a document by determining its category (i.e. passport, ID card, resident permit), model and country of origin by comparing the document against a reference dataset of document templates. To detect forgeries or counterfeits, the algorithm then checks whether all expected security features (i.e., holograms using fakeogram detection technology) are present and conformant. Security checks also include identifying with the use of convolutional neural networks whether the document was printed or presented on a screen, and algorithms detect inconsistent fonts used in the document.

Demonstrating and Refining Mobile Detection Algorithms – from field testing to stakeholder feedback

The developed algorithms were integrated in a demonstrator deployed on Android devices and shown to relevant stakeholders in security related events (SRE 2023 and Milipol 2023). Laboratory evaluation, which involved a significant variety of travel documents, returned promising results.

Helpful feedback from stakeholders suggest that ergonomics of the demonstrator can be improved showing that the involvement of relevant professionals during the development is integral

Results for some algorithms on field tests were not as satisfactory as one could have expected during development on previously unseen attacks, suggesting more work is necessary to create realistic and varied false documents for algorithm training.

> The wide variety of travel documents coming from various countries, each with their own specific security features, represents a significant challenge for border guards and others professionals

Other manipulation detection capabilities

Morphed iris

Face morphing has been shown to be a complex challenge for facial recognition systems (FRS). To enhance biometric systems, it is critical to explore and evaluate other biometric modalities such as fingerprint and iris. iMARS studied new techniques to create morphed iris images and textures by employing image-level attacks based on landmark and pupil sizes selection.

In this work, we introduced a new dataset and an iris recognition system based on Siameses network using periocular images. We also developed an image-level periocular iris morphing algorithm that demonstrated both its feasibility and limitations. This showed that iris recognition systems are very sensitive to periocular iris morphed images, and these systems can be attacked with a high success rate.

Assessing Vulnerability in Iris Recognition: Creating Realistic Morphs for Periocular Analysis

To evaluate the impact of these morph attacks, we generated a new dataset specifically for analysing the quality and realism of the morphed iris images. Selecting appropriate iris pairs to create a realistic morph is one of the most challenging processes as the state-of-the-art pre-trained extraction network used for morphing face images, are not usable for iris. Our evaluation of iris periocular images showed that recognition system are vulnerable to iris manipulations. It is essential to highlight that creating morph periocular images allows us to obtain the three traditional representations of the iris biometric sample. Then, iris and texture images can be made based exclusively on the morphed periocular iris images.

The research shows that creating morph images from periocular iris images is feasible and challenging for iris recognition systems. In the state-of-the-art methods, more than 90% of morph images can vulnerate the iris recognition systems for both datasets analysed. Creating morph images from periocular images has several advantages because we can obtain the periocular, normalised and iris-code images from the same morph images. As of today, the detection of the morph attack does not seem to exist or be reported as a real attack. We believe that this kind of attack would occur as any other presentation attack and be detected as such.

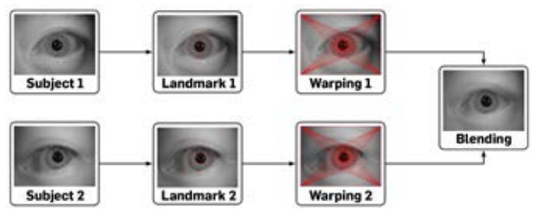


Image representation of periocular morph iris at image level

3D face morphing

3D face recognition is a biometric characteristic that can be used in electronic Machine Readable Travel Documents (eMRTDs). Although it has yet to be fully adopted, it is crucial to investigate whether the threat posed by face morphing in 2D face recognition systems can also affect 3D systems. Understanding this potential risk is essential for evaluating the security of 3D face recognition and ensuring its safe implementation in eMRTDs.

Our research has focused on generating 3D face morphs using various approaches. State-of-the-art technologies and algorithms have been employed to create morphed 3D face models, followed by a thorough vulnerability assessment to evaluate the resilience of 3D FRSs against this type of attack.

Advancing 3D Morphing Techniques: Vulnerability Assessment of Face Recognition Systems

We developed a 3D face morphing algorithm based on the alignment of the two contributing 3D models to a reference shape. A 3D depth maps morphing algorithm was developed based on Convolutional Autoencoders. Finally, an extensive vulnerability assessment of state-of-the-art 3D face recognition systems was conducted.

This research demonstrated that 3D face morphing is indeed feasible, and effective methods for generating morphed 3D models were successfully developed during the project. However, an extensive vulnerability analysis revealed that 3D FRSs are generally robust against this form of attack. As a result, 3D face morphing does not currently pose a significant security threat to these systems. Nevertheless, continuous monitoring and further research are recommended to ensure the ongoing security of 3D face recognition as technology evolves.

An example of 3D face morphing

MAD approaches developed within the project are effective in identifying morphed fingerprints, significantly reducing the vulnerability of biometric systems.

Fingerprints

Fingerprints are a viable alternative biometric characteristic for identity verification in eMRTDs. Given their importance, it is crucial to analyse the feasibility of fingerprint morphing, which could pose a significant threat to the security of automatic fingerprint recognition systems. Exploring this risk will help determine potential vulnerabilities and guide the development of effective countermeasures to ensure the integrity of fingerprint-based identity verification in eMRTDs.

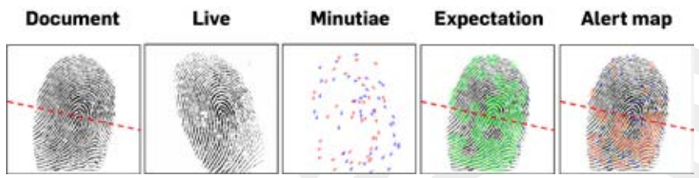
Through our research efforts, we have made significant progress in understanding the attack potential of fingerprint morphing. Our work has provided deeper insights into how morphing techniques can be used to manipulate fingerprint images, posing a threat to fingerprint-based recognition systems. At the same time, we have successfully developed effective countermeasures that mitigate these risks. These countermeasures are designed to detect and prevent morphing attacks, thereby enhancing the security and reliability of fingerprint-based biometric systems.

Enhancing Fingerprint Security: Advanced Morph Detection and Real-World Risk Assessment

Our work provided an improved fingerprint morphing algorithm that produces high-quality fingerprint morphs. An effective D-MAD solution was developed, designed to detect fingerprint morphing based on a comparison between the enrolment image and a probe sample acquired live. Our novel S-MAD approach based on CNNs to detect double-identity fingerprints was studied and tested in a complex cross-database and cross-morphing algorithm scenario.

One of the key lessons learned from our research is that fingerprint morphing indeed possesses an attack potential in the digital domain, capable of undermining the reliability of fingerprint-based recognition systems. However, the risk posed by such attacks can be considered limited in real operational scenarios, thanks to the MAD approaches developed within the project which are effective in identifying morphed fingerprints, thereby significantly reducing the vulnerability of biometric systems.

The practical complexity of executing a successful physical fingerprint morphing attack further limits the likelihood of its occurrence in real-world applications, since fingerprints are subject to live enrolment.



An example of fingerprint morphing detection

Portrait securing printing technologies

iMARS aimed to secure the personalised (printed) portrait in ID documents, which is one of their most attacked security elements and protection against traditional face image attacks, such as image substitution or image alteration is of utmost importance for border and ID documents security. Two solutions developed to address these challenges are CodeFace® TrustFace® technologies.

The CodeFace® technology is based on a deep learning algorithm resorting to robust steganography. The deep architecture built to support CodeFace® is able to learn and reproduce the noise and distortion effects of the physical personalising process (printing) of the portrait on the ID document and then scanning it back to the digital format. This technology is able to secure the personalised (printed) portrait by encoding within it a hidden message which can be used for validation of the portrait's integrity. The technology was proven to work in real (unconstrained) scenarios and was designed to be compatible for use in mobile devices. Deep architecture is able to automatically decode very slight, almost imperceptible, changes in face portraits. The main challenges of CodeFace® technologies were to reduce the impact of the slight visual changes in the portrait and to make it unbiased towards demographic variables.

TrustFace

CodeFace

Innovative Portrait Security for Enhanced Document Integrity

The TrustFace® technology, based on a deep learning algorithm resorting to an advanced face embedding extractor, is able to secure the portrait by computing a deep embedding of the portrait photo and encoding it on a machine readable 2D barcode which can be personalised (printed) in the ID document surface itself. The matching between a live acquisition of the portrait and the decoded information from the immutable 2D barcode can be used for validation of the portrait's integrity thanks to a purposely built deep architecture. The technology was proven to work in real (unconstrained) scenarios and was designed to be available in mobile devices. The 2D barcode selected to secure the protected portrait embedding was the UniQode®, a proprietary barcode by INCM, though a secured 2D barcode can also be used for this purpose. The main challenge of TrustFace® was to achieve a perfect match between an immutable barcode message and the varying (illumination, camera and pose) embedding extracted from the portrait's image.

Exhaustive experiments showed a very high performance of both CodeFace® and TrustFace®, making ID documents more secure with than without them.

The decoding process and the subsequent validation of the integrity of the portrait are very easy and can be performed using an authorised mobile app with a smartphone.

Exhaustive experiments showed a very high performance of both CodeFace® and TrustFace®, making ID documents more secure with than without them.

Standards

Since 2021, the work of International Organization for Standards (ISO) on ISO/IEC JTC 1/SC 37, which develops and facilitates standards with the aim to support interoperability and data interchange among biometric applications and systems pertaining to human beings, has received contributions from iMARS. Our partners' involvement and contributions were particularly significant for the international standards ISO/IEC 29794-1 Biometric sample quality – Part 1: Framework and ISO/IEC 29794-5 Biometric sample quality – Part 5: Face image data. The technical contributions and insights from the research conducted in iMARS not only improved and strengthened international standards directly relevant to sample quality assessment, but also established a new standard related to morphing attack detection

iMARS' research was instrumental for the conception of ISO/IEC 29794-5 Biometric sample quality – Part 5: Face image data. which was promoted to Final Draft International Standard in July 2024. It will relate to quality requirements from both ISO/IEC 19794-5:2011 and ISO/IEC 39794-5:2019, and it will also be applicable to scenarios with relaxed quality requirements such as surveillance applications. Thanks to the work of iMARS, good progress was achieved on the definition of numerous quality components specifically regarding neutral expression and radial distortion prevention.

Similarly, Standard ISO/IEC DIS 20059, which has reached the level of Draft International Standard, includes the iMARS methodology to quantise the power of a morphing method, now termed as morphing attack potential (MAP). The DIS document now awaits a final round of comments, which are to be discussed in January 2025.

Other contributions of the iMARS project are present in the harmonised vocabulary of ISO/IEC 2382-37 and the testing methodologies for a Relative Impostor Attack Presentation Accept Rate to ISO/IEC 30107-3 Biometric presentation attack detection – Part 3: Testing and reporting.

Moreover, continuous efforts were made to contribute to the Biometric Harmonised Vocabulary (HBV), which for instance now contains a clear definition of morphing attacks versus manipulation attacks.

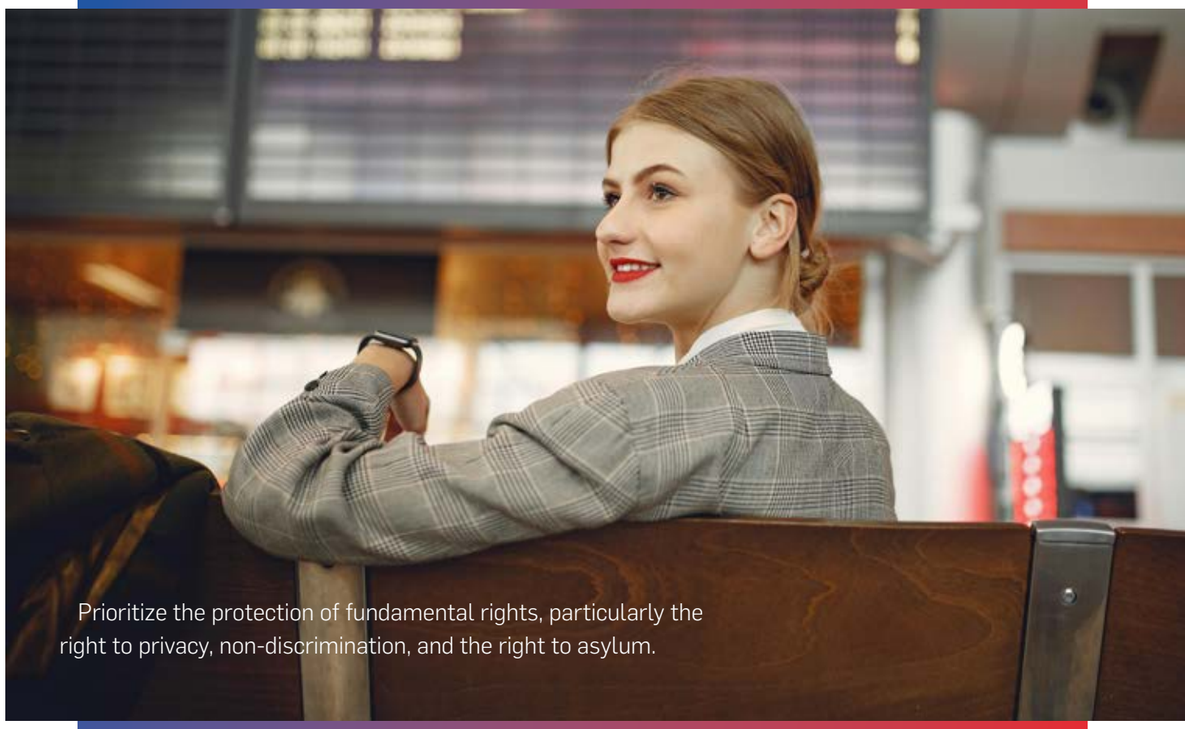
Providing concepts (e.g. for EDC and MAP) with OpenSource code software in GitHub increased the adoption of such project results not only in the research community but also in standards. This approach also reduces the risk of wrong interpretation of technical standards.

» **Further information:**
https://www.iso.org/standard/79519.html

https://www.iso.org/standard/81005.html

https://www.iso.org/standard/86084.html

Expression Neutrality Measure with cumulative 2-norm distances.



Prioritize the protection of fundamental rights, particularly the right to privacy, non-discrimination, and the right to asylum.

Legal, ethics and society acceptance

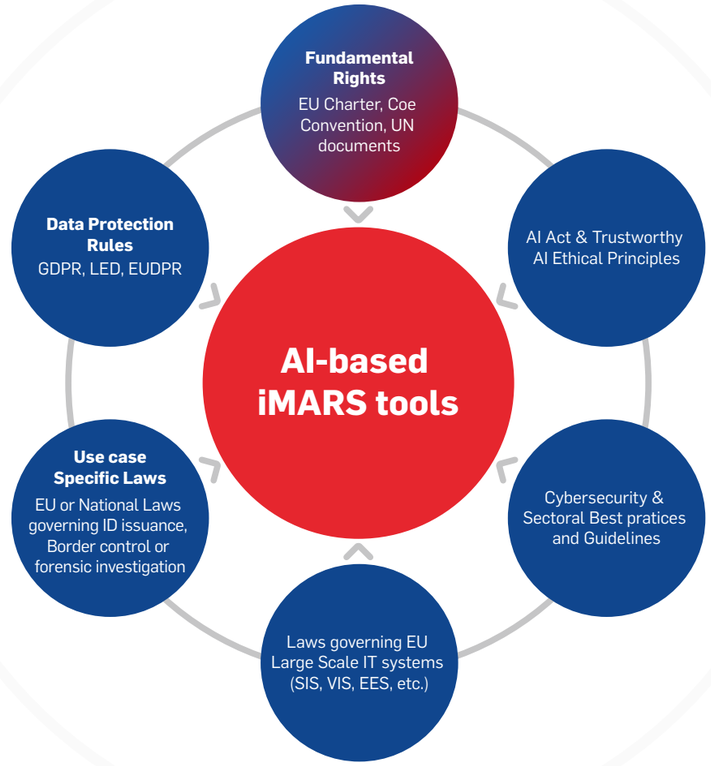
Meeting legal, ethical, and societal standards is crucial for leveraging the full benefits of iMARS technologies and ensuring trust in their responsible development and future use. We monitored and analysed iMARS technologies to guarantee that their design, development, and testing are fully compliant with EU regulations, best practices, and ethical standards, all of which are adhered to by iMARS partners.

The questions addressed included:

- Which legal frameworks should be applied to ensure trust in iMARS technologies, covering both the development and deployment phases?
- What are the potential benefits and risks associated with iMARS tools, and how can we effectively mitigate these risks and respect fundamental rights as well as EU values?
- What are the key guidelines and best practices relevant to the development and deployment of the iMARS technologies?

To answer these questions, we mapped ethical and societal requirements and developed guidelines and best practices for iMARS in two public deliverables. We analysed the societal acceptability of iMARS technologies and similar tools and also took into account feedback and perspectives from an independent ethics advisor. A final public report aims to assess ethical, legal and societal aspects of the technologies effectively developed in iMARS. Within the research activities themselves, we ensured data protection compliance, via, for example, the development of joint controller agreements, data processing agreements, consent forms, etc. We also designed a dedicated module in the human expert training. The outcomes of this work has the potential to guide the R&D and deployment of similar technologies in the future.

» **Further information:**
https://cordis.europa.eu/project/id/883356/results



*Various applicable legal rules, either international, EU, or national level, influence the use of iMARS tools. Depending on the deployment area or use case of iMARS technologies, different **domain-specific laws** apply **in combination** or **separately**.*

Security and fundamental rights go hand in hand; ensuring security is itself a fundamental duty. Both must be supported simultaneously, each strengthening the other. Public authorities also have a duty of good administration, meaning they must incorporate new technologies while respecting EU values and adhering to legal frameworks.

Our key legal and ethical takeaway are:

Tailored legal and ethical analysis: Biometric recognition technologies, including facial recognition, are composed of multiple algorithms with distinct functions, limitations, and risks, working together to provide reliable identity verification or identification. iMARS technologies will either function standalone or as a component of existing biometric recognition systems. Therefore, legal and ethical analyses of iMARS tools and similar technologies must be tailored to their specific purpose and deployment context.

Upholding fundamental rights: iMARS and similar technologies must prioritize the protection of fundamental rights, particularly the right to privacy, non-discrimination, and the right to asylum depending on the context of operational use. It is essential to contribute positively to EU society, ensuring that these rights, guaranteed to all within the EU, are fully respected.

Ensuring data protection compliance: Compliance with data protection regulations, including GDPR, must be maintained throughout the entire R&D phase of iMARS technologies, with ongoing efforts during further development and deployment stages after the project to safeguard data protection rights of individuals. Conducting thorough assessments, such as Data Protection Impact Assessments (DPIAs) and Fundamental Rights Impact Assessments (FRIAs), to ensure compliance should be emphasized as a best practice.

Ensuring trust in iMARS by complying with trustworthy iMARS tools AI principles: iMARS must adhere to the Trustworthy AI ethics principles, in particular transparency, accountability, accuracy and fairness in AI. Transparent algorithms should be favoured over opaque “black box“ models. Clear accountability must be established for all stakeholders, including public and private actors. Additionally, it is necessary to ensure that the technology avoids bias, operates fairly, and remains robust against digital vulnerabilities.

Clear information for individuals who are subject to the iMARS tools: Individuals subject to iMARS technologies must be provided with clear, accessible information about how their data is collected, processed, and used, ensuring informed consent, to build trust in the system.

Training for meaningful oversight: Agents using iMARS as decision-support systems in one of the identified iMARS use cases must be thoroughly trained to provide meaningful oversight, helping to prevent automation bias against the outcome of iMARS tools and ensure accountability in the decision-making process.

Sector-specific compliance: When developing or deploying iMARS and similar technologies, it is crucial to follow sector-specific regulations, best practices, and guidelines (such as ICAO and ISO standards) to ensure ethical and legal compliance across iMARS use cases.

Seek guidance from regulators: Engaging with supervisory authorities and policymakers to advocate for more tailored guidelines specific to iMARS and similar technologies is crucial, ensuring that operational use of iMARs technologies is properly aligned with the applicable legal and ethical frameworks.

Editorial image

Tools & solutions spotlight

Results and dissemination

With over 50 publications and 20 developed algorithms, iMARS demonstrates the scale of results achieved—more than this brochure could fully capture. Here, we spotlight the tools and solutions most relevant and accessible to government practitioners. While further research is underway, fully exploiting these results will also require essential next steps: further testing, integration, and deployment in partnership with end-users. In many ways, the end of iMARS marks the beginning of practical applications to strengthen biometric security.

BOEP

The BOEP (Bologna Online Evaluation Platform) is a web-based, fully automated evaluation platform designed to objectively assess and compare the performance of MAD algorithms. Its primary purpose is to provide a comprehensive and independent evaluation environment for researchers and developers in the field of biometric security, particularly those working on face recognition systems.

Benefits

- Objective evaluation: Provides an automated, independent and unbiased testing and assessment of MAD algorithms through evaluation on sequestered datasets, ensuring fair comparison and reliable results.
- Enhanced efficiency: Utilises Graphics Processing Units (GPUs) and parallel computation to speed up the evaluation process.
- Interoperability with NIST FATE MORPH: Allows the submission of Dynamic-linked libraries compliant with NIST FATE MORPH specifications, enhancing compatibility and integration with existing evaluation frameworks.
- Ease of use: Supports Python script submissions, reducing the implementation efforts required from participants and making it more accessible for a wider range of users on both Linux and Windows.
- Comprehensive benchmarks: Offers several high-quality and new benchmarks for S-MAD and D-MAD, allowing for thorough testing and evaluation of algorithms.
- Data security: Ensures the testing of algorithms without the need for access to the data, maintaining the confidentiality and integrity of the datasets, the algorithms and the results. The platform is composed of two separate servers (Front End and Test Engine) to protect sensitive information and prevent external attacks.
- Performance indicators: The platform reports results using standard performance indicators and metrics, such as Bona fide Presentation Classification Error Rate (BPCER) and Morphing Attack Classification Error Rate (MACER).
- Continuous updates: The platform is designed to track advances in MAD through continuously updated with new benchmarks to ensure it remains current and relevant.

» **Further information:**
https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx

E-learning

The iMARS e-learning seeks to improve human ability to detect face image morphing. It consists of theory modules and examination-based modules, as well as testing.

Just like the training below, the e-learning aims to equip professionals with a better understanding of morphing and better knowledge on how to detect artifacts, so that human examiners remain in control of the decision-making even when they use image manipulation detection technology.

Benefits

The ultimate goals and benefits of the e-learning are to improve detection competence, so that the risk of morphed face images in travel documents is reduced and border control is reinforced.

The e-learning is inclusive and flexible: professionals involved in ID verification can learn at their own pace, online within the NID (Nasjonalt ID-senter) platform and self-assess their progress. It is free, and available to eligible government agencies.

Apply for access at www.nidsenter.no

Training modules

Theoretical and practical modules that can be easily integrated in institutions' own wider training programs on fraud detection were developed in iMARS. They aim to equip professionals who inspect face images on/for ID documents with a better understanding of how morphing occurs in a real world scenario, what artifacts morphing leaves behind and how to detect them in printed documents.

Training modules

- **Module 1:** Identification Documents (types, frauds and checks) – KEMEA
- **Module 2:** Manual facial comparison and identification – KEMEA
- **Module 3:** Introduction to face image morphing (concept and techniques used for image morphing creation and attack detection) - KEMEA
- **Module 4:** Responsible Use of IMARS tools and Fundamental Rights - KUL
- **Module 5:** Codeface & Trustface Technologies developed in IMARS – INCM

CodeFace® application

CodeFace® application (Portuguese Mint and Official Printing Office) The CodeFace® app was built to validate the integrity of the portrait of ID documents. This app can be used by authority agents, border police or fraud examiners willing to check the integrity of the portrait of ID documents that use CodeFace® technology. The app reads the portrait of the ID document, decodes a hidden secret message encoded within it and matches this secret information against an expected code for this portrait. If matching occurs, the ID document is validated.

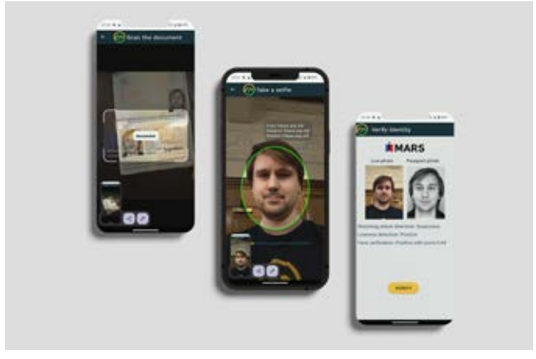
A deep-learning architecture based on a robust steganography algorithm is able to encode and decode hidden secret messages to add to photos in printed format. The technology was extensively optimised to be used in real ID documents.

Benefits

Since the portrait is one of the most attacked security elements of ID documents, particularly the personalised (printed) portrait, this app can create a highly secure and practical tool to check for its integrity.

Mobile solution

An advanced remote identity proofing solution was developed with differential morphing attack detection for mobile devices, designed to streamline identity verification processes at land and maritime borders. This solution is built on a client-backend architecture that includes several key modules: passport authenticity, face verification, face presentation attack detection, and differential morphing attack detection, all housed within the backend system. Thanks to this modular design, these backend components can be seamlessly integrated into an automated border control system, enhancing security and efficiency.



Its use is very simple: the app captures the ID document page to extract MRZ (Machine Readable Zone) information, and reads the data from chip. A live photo of the document holder is taken, to allow the app to perform a face comparison, verifying that the individual is the leg imitate hold of the document. The authenticity ID document and the ID Photo from the chip are validated by the app, verifying that the ID photo from the chip, and the app also validates that the live photo was captured from a real person in real time.

Benefits

This app offers a user-friendly solution with high flexibility for border officers, that secures ID document validation and biometric-based identity verification.

Morphing traces detection tool

The morphing traces visualization tool provides a way of isolating and visualizing face image morphing-related traces left on digital images. The tool can be used by institutions (e.g., ID document issuing authorities, banks, biometrics companies) to examine digital face images for manipulation traces. It can be used as a standalone tool or to support an automated algorithmic decision.

An example of a morphed image (left) and two filtered versions produced with the tool (middle and right)

The tool makes use of classic image forensics methods such as JPEG compression error, discrete Fourier transform and colour gradients to filter questioned images and uncover traces of image manipulation that is related with the process of morphing.

Benefits

Written in Python, this tool is easy to explain, easy to use and efficient, taking just a few seconds per image.

» **Further information:**
https://doi.org/10.3389/fcomp.2023.981933

Morph generation tools

Generating better quality morphs is important to develop morphing attack detection. The previous tools for generating morphing attacks required a high degree of manual intervention for eliminating the misalignments in morphed images. The partners of iMARS have developed more than 10 tools to generate better morphed images. These tools can be landmark based (i.e. relying on the detection of specific points in the face), or Depp-learning based (i.e. based on the ability to generate faces using AI tools).

The goal was to develop realistic morphs in a fully automatic way, difficult to detect, and enabling for the production of large sets of morphs for algorithm developers and operators.

Furthermore iMARS partners also considered the possibility of generating "blends" of iris and fingerprints, enabling two different subjects to be identified with the same "synthetic biometrics".

Benefits

- The new morphs generators are relying on new technologies, therefore figuring what future morphs will be.
- In order to make MAD methods more robust to a variety of morphing methods, it is required to train them and test them on datasets built with a variety on morphing techniques (and also cross checking the algorithms trained on a set of morph generated with a given set of morphing techniques and then tested on a test set generated with other morphing techniques
- The large variety of morphing methods "fuels" the detailed study of the impact of morphing on generated images, so that training adapted to a variety of morphing methods can be developped
- iMARS also delivers Print-Scan simulation techniques, able to mimic a variety of scanners and printers, to simulate real-world diversity in enrolment photos.

Landmark based iMARS morph techniques are based on DLib landmarks plus additional feature points, plus techniques to reduce the "merging" effect of aligned faces

Deep learning based morphing techniques of iMARS include the use of MIPGAN and StyleGAN, and also include methods using diffusion autoencoder models.

Policy brief

The policy brief emphasises the importance of enhancing facial image acquisition processes during identity document enrolment to prevent fraud. It outlines two common attack methods: morphing, where multiple faces are blended to create a realistic, fraudulent image, and presentation attacks, where physical alterations or substitutions are used. To counter these, the brief recommends "live enrolment under supervision", where government agents directly capture images. This method restricts opportunities for tampering and ensures higher image quality, making identity documents more secure against fraudulent use.

The full brief is available for free to eligible government and agencies. Contact secretariat@eab.org for access.

Publications

The iMARS project has produced a wealth of scientific publications covering innovations in morphing attack detection, image quality assessment, and biometric security. These works represent collaborations across multiple disciplines, providing foundational knowledge and advanced techniques for biometric researchers and security professionals. Over 50 publications are openly available and serve as resources for anyone interested in biometric and forensic advancements, underscoring iMARS's commitment to supporting the broader research community.

- I. Batskos, F. F. de Wit, L. Spreeuwers, R. N. J. Veldhuis „Preventing face morphing attacks by using legacy face images" in IET biometrics, (2021)
- G. Borghi, E. Pancisi, M. Ferrara, D. Maltoni: "A Double Siamese Framework for Differential Morphing Attack Detection", in MDPI, (2021)
- G. Borghi, E. Pancisi, M. Ferrara, D. Maltoni: "Automated Artifact Retouching in Morphed Images with Attention Maps", in IEEE Access, (2021)
- S. Lorenz, U. Scherhag, C. Rathgeb, C. Busch: "Morphing Attack Detection: A Fusion Approach", IEEE FUSION, (2021)
- J. Tapia, C. Busch: "Single Morphing Attack Detection using Feature Selection and Visualisation based on Mutual Information", in IEEE Access, (2021)
- S. Venkatesh, R. Ramachandra, K. Raja, C. Busch: "Face Morphing Attack Generation and Detection: A Comprehensive Study", in IEEE Transactions on Technology and Society, (2021)
- H. Zhang, S. Venkatesh, R. Ramachandra, K. Raja, N. Damer, C. Busch: "MIPGAN—Generating Strong and High Quality Morphing Attacks Using Identity Prior Driven GAN", in IEEE Transactions on Biometrics, Behavior, and Identity Science, (2021)
- G. Borghi, A. Franco, G. Graffieti, D. Maltoni: "Automated Artifact Retouching in Morphed Images With Attention Maps", in IEEE Access, (2021)
- T. Schlett, C. Rathgeb, J. Tapia, C. Busch: "Evaluating Face Image Quality Score Fusion for Modern Deep Learning Models", in IEEE BIOSIG, (2022)
- A. Franco, A. Magnani, D. Maltoni, D. Maio, L. Odorisio, A. De Maria: "Face Image Quality Assessment in Electronic ID Documents", in IEEE Access, (2022)
- T. Schlett, C. Rathgeb, O. Henniger, J. Galbally, J. Fierrez, C. Busch: "Face Image Quality Assessment: A Literature Survey", in ACM, (2022)
- D. Schulz, J. Maureira, J. Tapia, C. Busch: "Identity Documents Image Quality Assessment", in EUSIPCO, (2022)
- G. Borghi, G. Graffieti, A. Franco, D. Maltoni: "Incremental Training of Face Morphing Detectors", in ICPR, (2022)
- S. Rancha Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Ramachandra, C. Busch: "Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?", in IEEE Transactions on Technology and Society, (2022)
- M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in IEEE IWBF, (2022)
- R. Ramachandra, G. Li: "Multimodality for Reliable Single Image based Face Morphing Attack Detection", in IEEE Access, (2022)
- K. Laas-Mikko, T. Kalvet, R. Derevski, M. Tiits: "Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding", in Springer, (2022)
- G. Li, R. Ramachandra: "Residual Colour Scale-Space Gradients for Reference-based Face Morphing Attack Detection", in IEEE FUSION, (2022)
- J. Tapia, A. Valenzuela, R. Lara, M. Gomez-Barrero, C. Busch: "Selfie Periocular Verification using an Efficient Super-Resolution Approach", in IEEE Access, (2022)
- J. Tapia, D. Schulz, C. Busch: "Single Morphing Attack Detection using Siamese Network and Few-shot Learning", in arXiv, (2022)
- K. Raja, G. Gupta, S. Venkatesh, R. Ramachandra, C. Busch: "Towards Generalized Morphing Attack Detection by Learning Residuals", in Elsevier Image and Vision Computing, (2022)
- S. Gonzalez, J. Tapia: "Towards Refining ID Cards Presentation Attack Detection Systems using Face Quality Index", in IEEE EUSIPCO, (2022)
- H. Chabanne, V. Despiegel, L. Guiga: "One Picture is Worth a Thousand Words: A New Wallet Recovery Process", in IEEE GLOBECOM, (2022)
- L. Dargaud, M. Ibsen, J. Tapia, C. Busch: "A Principal Component Analysis-Based Approach for Single Morphing Attack Detection", in IEEE WACVW, (2023)
- E. Kindt, C. Fontanillo López: "Legal Aspects of Image Morphing and Manipulation Detection Technology", in Springer, Handbook of Biometric Anti-Spoofing, (2023)
- I. Batskos, L. Spreeuwers, R. Veldhuis: "Visualizing Landmark-Based Face Morphing Traces on Digital Images", in Frontiers in Computer Science, (2023)
- M. Ferrara, R. Cappelli, D. Maltoni: "Detecting Double-Identity Fingerprint Attacks", in IEEE Transactions on Biometrics, Behavior, and Identity Science, (2023)
- G. Borghi, N. Di Domenico, A. Franco, M. Ferrara, D. Maltoni: "Revelio: A Modular and Effective Framework for Reproducible Training and Evaluation of Morphing Attack Detectors", in IEEE Access, (2023)
- T. Schlett, S. Schachner, C. Rathgeb, J. Tapia, C. Busch: "Effect of Lossy Compression Algorithms on Face Image Quality and Recognition", in IEEE ICASSP, (2023)
- J. Tapia, C. Busch: "Face Feature Visualisation of Single Morphing Attack Detection", in IWBF, (2023)
- D. Benalcazar, J. Tapia, S. Gonzalez, C. Busch: "Synthetic ID Card Image Generation for Improving Presentation Attack Detection", in IEEE Transactions on Information Forensics and Security, (2023)
- T. Schlett, C. Rathgeb, J. Tapia, C. Busch: "Considerations on the Evaluation of Biometric Quality Assessment Algorithms", in IEEE Transactions on Biometrics, Behavior, and Identity Science, (2023)
- D. Pasmino, C. Aravena, J. Tapia, C. Busch: "Flickr-PAD: New Face High-Resolution Presentation Attack Detection Database", in IEEE IWBF, (2023)
- J. Tapia, C. Busch, H. Zhang, R. Ramachandra, K. Raja: "Simulating Print/Scan Textures for Morphing Attack Detection", in IEEE EUSIPCO, (2023)
- N. Di Domenico, G. Borghi, A. Franco, D. Maltoni: „Combining Identity Features and Artifact Analysis for Differential Morphing Attack Detection", in Springer, Image Analysis and Processing, (2023)
- N. Di Domenico, G. Borghi, A. Franco, M. Ferrara, D. Maltoni: „A Framework to Improve the Comparability and Reproducibility of Morphing Attack Detectors", in IEEE MetroXRAINE, (2023)
- A. Franco, F. Løvåsdal, D. Maltoni: „On the Human Ability in Detecting Digitally Manipulated Face Images", in IEEE MetroXRAINE, (2023)
- L. Pellegrini, G. Borghi, A. Franco, D. Maltoni: „Detecting Morphing Attacks via Continual Incremental Training", in IEEE IJCB, (2023)
- J. Tapia, C. Busch: „Impact of Synthetic Images on Morphing Attack Detection Using a Siamese Network" in Springer CIARP, (2023)
- W. Kabbani, C. Busch, K. Raja: „Robust Sclera Segmentation for Skin-tone Agnostic Face Image Quality Assessment", in IEEE BIOSIG, (2023)
- R. Kessler, K. Raja, J. Tapia, C. Busch: "Towards Minimizing Efforts for Morphing Attacks—Deep Embeddings for Morphing Pair Selection and Improved Morphing Attack Detection", in PLOS ONE, (2024)
- N. Di Domenico, G. Borghi, A. Franco, D. Maltoni: "Dealing with Subject Similarity in Differential Morphing Attack Detection", in arXiv, (2024)
- M. Ibsen, L. J. Gonzalez-Soler, C. Rathgeb, C. Busch: "TetraLoss: Improving the Robustness of Face Recognition Against Morphing Attacks", in IEEE FG, (2024)
- T. Schlett, C. Rathgeb, J. Tapia, C. Busch: "Double Trouble? Impact and Detection of Duplicates in Face Image Datasets", in ICIS, (2024)
- N. Di Domenico, G. Borghi, A. Franco, D. Maltoni: "ONOT: a High-Quality ICAO-compliant Synthetic Mugshot Dataset", in arXiv, (2024)
- N. Di Domenico, G. Borghi, A. Franco, D. Maltoni: "Face Restoration for Morphed Images Retouching", in IEEE IWBF, (2024)
- I. Batskos, L. Spreeuwers: "Improving Fully Automated Landmark-based Face Morphing", in IEEE IWBF, (2024)
- G. Borghi, A. Franco, N. Di Domenico, M. Ferrara, D. Maltoni: "V-MAD: Video-based Morphing Attack Detection in Operational Scenarios", in arXiv, (2024)
- P. Kumar Chandaliya, K. Raja, R. Ramachandra, Z. Akhtar, C. Busch: "Towards Inclusive Face Recognition Through Synthetic Ethnicity Alteration", in arXiv, (2024)
- W. Kabbani, K. Raja, R. Ramachandra, C. Busch: "Eye Sclera for Fair Face Image Quality Assessment", in IEEE IWBF, (2024)
- J. Tapia, S. Gonzalez, D. Benalcazar, C. Busch: "On the Feasibility of Creating Iris Periocular Morphed Images", in arXiv, (2024)
- J. Tapia, M. Russo, C. Busch: "Generating Automatically Print/Scan Textures for Morphing Attack Detection Applications", in arXiv, (2024)

Algorithms

Numerous algorithms have been developed in iMARS at various maturity levels. Some are ready for further development, for testing, licensing or deployment. If you want to get access to such solutions, you can approach the individual contact given in the table rows below.

Algo name/title	Algo owner	Description	Maturity - For testing / For licensing	Contact
HDA-DFR	Hochschule Darmstadt	This is a differential morphing attack detection algorithm based on the implementation of [1]. During iMARS was generated a second version between HDA/ NTNU called HDA-MAG based in [1] and [2] [1] U. Scherhag, C. Rathgeb, J. Merkle and C. Busch, "Deep Face Representations for Differential Morphing Attack Detection," in IEEE Transactions on Information Forensics and Security. [2] Roman Kessler, Kiran Raja, Juan Tapia, Christoph Busch. Towards minimizing efforts for Morphing Attacks—Deep embeddings for morphing pair selection and improved Morphing Attack Detection.	TRL-7 Algorithm Patented[1]. The patent is pre-dating the iMARS project, but it is part of the licensing contract. Ready to be licensed	*Christoph Busch* christoph.busch@h-da.de
GMORPH	IN Groupe	Face Morpher tool	TRL-6	*Michael Scherer* michael.scherer@ingroupe.com *Julia Petit* julia.petit@ingroupe.com
Feature difference-based D-MAD	Mobai	This D-MAD approach is built using MOB's in-house feature template, extracted from the input image. By subtracting the feature template from both the reference and probe images, a vector is generated, which is then used to train a classification model. The effectiveness of this method has been demonstrated through evaluations on several datasets.	Ready for testing	*Erik Guoqiang Li* erik@mobai.bio
A double Siamese framework for differential morphing attack detection	Universita di Bologna	A double Siamese architecture for D-MAD, merging the contribution of an identity and an artifact module.	Ready for testing	*Guido Borghi* guido.borghi@unibo.it
Combining identity features and artifact analysis for Differential Morphing Attack Detection	Universita di Bologna	A D-MAD system that combines the features of a state-of-the-art S-MAD method, alongside the difference of identity embeddings.	Ready for testing	*Nicolò Di Domenico* nicolo.didomenico@unibo.it
Dealing with Subject Similarity in Differential Morphing Attack Detection	Universita di Bologna	A D-MAD system that adds a pair classification module that weighs scores coming from state-of-the-art D-MAD and S-MAD modules.	Ready for testing	*Nicolò Di Domenico* nicolo.didomenico@unibo.it
UBO-SMAD-R3: an Inception-ResNet-based model for Single-image Morphing Attack Detection	Universita di Bologna	A state-of-the-art deep learning-based S-MAD system, robust to several morphing algorithms and postprocessing techniques such as lossy compression and printing and scanning.	Ready for testing	*Nicolò Di Domenico* nicolo.didomenico@unibo.it
Revelio: A modular and effective framework for reproducible training and evaluation of morphing attack detectors	Universita di Bologna	A comprehensive framework to train and evaluate both S-MAD and D-MAD systems in a standardized way, providing several specialized data preprocessing and augmentation modules tailored to the MAD task.	Ready for testing	*Nicolò Di Domenico* nicolo.didomenico@unibo.it
Software tool to support human examiners in face image manipulation detection	Universita di Bologna	A software tool that allows human examiners to easily compare a live image with an ID photo to identify in the latter the possible presence of image manipulations.	Ready for testing	*Annalisa Franco* annalisa.franco@unibo.it

Algo name/title	Algo owner	Description	Maturity - For testing / For licensing	Contact
Landmark-based morphing with ghost artefact removal	University of Twente	This algorithm consists of a pre-processing module, a morphing module and a post-processing module that removes ghost artefacts from complex facial regions. It is quite efficient and can be used for mass morphing production	Ready for testing	*Ilias Batskos* i.batskos@utwente.nl *Luuk Spreeuwers* l.j.spreeuwers@utwente.nl
Compression Error Single Image Morphing Attack Detection	University of Twente	This algorithm is an automated single image morphing attack detection solution. It is based on extracting statistical image features from a questioned image and JPEG compressed versions therefof and classify the questioned image as either bona fide or morphed using a trained support vector machine.	Ready for testing	*Ilias Batskos* i.batskos@utwente.nl *Luuk Spreeuwers* l.j.spreeuwers@utwente.nl
Morph-PIPE	Norwegian University of Science and Technology	Morph-PIPE tool from NTNU retains high level of identity information of two contributing subjects making the morphed images look realistic with high quality.	TRL 3	*Haoyu Zhang* haoyu.zhang@ntnu.no
SynMorph	Norwegian University of Science and Technology	SynMorph tool can be used to create massive number of morphed images using generative approaches (Generative Adversarial Networks and Diffusion models). Synthetic images can further be used for training algorithms and human observers.	TRL 3	*Haoyu Zhang* haoyu.zhang@ntnu.no
IN CMF Detection	IN Groupe	Copy and Move forgery counter-measure for ID documents	TRL-3	*Michael Scherer* michael.scherer@ingroupe.com *Julia Petit* julia.petit@ingroupe.com
IN SMAD	IN Groupe	Single image morph attack detection	TRL-3	*Axel Veillas* axel.veillas@ingroupe.com
IN DMAD	IN Groupe	Differential morph attack detection	TRL-3	*Axel Veillas* axel.veillas@ingroupe.com
Vision-Box MorphingAttackDetection SDK v1.0.0	Vision-Box, an Amadeus Company	Contains both S-MAD and D-MAD versions developed by VIS in the scope of the iMARS project. S-MAD is based on jpeg compression error and D-MAD is based on Vision-Box proprietary matcher and embedding differences between the reference and probe images.	Testing on both FVC-Ongoing (BOEP) and NIST FRTE Morph have shown promising results, which were inline with the observed performance in internal benchmarking. Preliminary tests with passport and live e-Gate images have achieved interesting performance (5% EER). Further improvements and proof-of-concepts will be required before this technology is mature enough for licensing.	*Joao Monteiro* joao.monteiro@amadeus.com *Joao Ferreira* joao.ferreira@amadeus.com

Editorial image

The next steps of iMARS

Future avenues and applications

Twenty years ago, automatic face recognition was still a challenge. There were obvious applications – among other for border management – and the technology was slowly crossing the boundaries of usability. Morphing Attack Detection technologies have reached a point where they can start to be used and they can now be required in different applications where documents showing face images are used: at the border, at the bank, on drivers' licenses, on social security cards, etc. Like with Presentation Attack Detection, this will be a permanent fight between the attackers and the defenders – each of them becoming smarter with time. Thanks to iMARS, we now have on the defender side a reliable base.

However, the morphing attack problem is quite specific: we know morphing attacks exist, but what we have seen so far is the tip of an iceberg made of a substance of unknown density. We are not able to evaluate the size of the problem and the dimension in terms of a security flaw that endangers European security. Therefore, the most important action that we can now undertake with confidence and with no delay is to use live capture processes in all passport application processes. As complementary measures we recommend to start training the practitioners, and put in place pilot efforts to measure the importance of morphing attacks using for instance iMARS algorithms.

Related EU-funded research projects

CarMen

The EU-funded CarMen project aims to develop biometric solutions for the continuous border control of both pedestrians and vehicles, with a focus on fraud detection, compliance with legal and ethical standards, and privacy protection. At present, the main challenges related to 'on the move' biometrics are lower quality live biometric data and the impossibility to read ePassports. In uncontrolled environmental conditions, CarMen innovates biometric solutions for non-stop border control that are suitable for pedestrians and vehicles.

CarMen will introduce a multimodal approach to the face, iris, and periocular regions to generate more robust biometrics, aiming to: detect presentation attacks and anomalous traveller behaviour on the move with efficiency, demonstrate the usage and benefits of Digital Travel Credentials at the border, and ensure resilient on-the-move face recognition in different lighting conditions.

EINSTEIN

EINSTEIN (Interoperable Applications Suite to Enhance European Identity and Document Security and Fraud Detection) is an innovation project focused on enhancing the security of, and combating the frauds on, identity management and identity and travel documents.

In the context of future increasingly digitalised borders, EINSTEIN's vision is to expand existing physical and digital identity checks, privacy-preserving identity management, and fraud detection capabilities of border and police authorities. Its overarching goal is to increase these capabilities across a wide range of operational environments by developing, deploying and validating a set of interoperable applications addressing the entire identity lifecycle and applicable to a wide range of use cases and environments.

The applications will be six in total: 1) online document issuance, 2) mobile document and identity checks, 3) documents authentication, 4) pre-registration for border crossings, 5) EES kiosks with advanced fraud detection, and 6) fast-track biometric corridors.

PopEye

PopEye (Robust Privacy-preserving Biometric Technologies for Passengers' Identification and Verification at EU External Borders Maximising the Accuracy, Reliability and Throughput of the Recognition) aims to improve the identification and verification process at the EU's external borders, which currently ace long waiting times and inefficiencies, partly due to the limitations of existing biometric technologies.

PopEye intends to develop a new biometric framework that overcomes the current, thus enhancing the reliability of identification for both EU citizens and third country nationals. Its value proposition focuses on strengthening the security at the external EU borders through fusing robust biometric technologies, maximising the travellers' experience through unobtrusive on-the-move biometric technologies, and improving the productivity of border authorities and law enforcement agencies in a variety of settings.

The proposed modalities include infrared face recognition, 3D face recognition, contactless friction ridge recognition, iris recognition in the near-infrared spectrum, and iris recognition in the visible spectrum combined with gait recognition and behavioural biometrics.

SafeTravellers

The value proposition of the SafeTravellers project (Secure and Frictionless Identity for EU and Third Country National Citizens) is threefold. First, it aims at strengthening the security at the EU external borders. Second, it seeks to improve the productivity of the border authorities and law enforcement agencies by providing them with the appropriate tools to combat identity fraud based on multi-modal biometrics as well as improved identity verification mechanisms. Third, it hopes to offer a frictionless border crossing experience for EU citizens and third-country nationals as they will not have to stop at border checkpoint. As such, SafeTravellers is both proposing a new way of citizen identification as well as an enhancement of the current method of identity verification through a new set of tools.

Contact us

Academics

- **Norwegian University of Science and Technology**
  kiran.raja@ntnu.no
- **Universita di Bologna**
  annalisa.franco@unibo.it
- **University of Twente**
  l.j.spreeuwers@utwente.nl
- **Hochschule Darmstadt**
  christoph.busch@h-da.de
- **Katholieke Universiteit Leuven**
  abdullah.elbi@kuleuven.be

Government Agencies, Practitioners

- **Bundeskriminalamt**
  uwe.seidel04@bka.bund.de
- **National Office for Identity Data - NL**
  renee.ong@rvig.nl
- **National Police Directorate - NO**
  froy.lovasdal@politiet.no
- **Hellenic Police**
  v.bakali@passport.gov.gr
- **Belgian Federal Police**
  jurgen.desmedt@police.belgium.eu
- **Border Police Republic of Moldova**
  dorina.rusu@border.gov.md
- **Cyprus Police**
  horizon@police.gov.cy
- **UCFE (ex SEF)**
  erica.santos@ssi.gov.pt

Industry & SMEs

- **Idemia Identity & Security France**
  claude.bauzou@idemia.com
- **Cognitec**
  weber@cognitec.com
- **Vision Box**
  joao.ferreira@vision-box.com
- **Imprensa Nacional Casa da Moeda**
  nuno.miguelgoncalves@incm.pt
- **SURYS / Ingroup**
  julia.petit@ingroupe.com
- **Mobai**
  brage@mobai.bio
- **Identity & Security Germany**
  michael.brauckmann@idemia.com

Research Centers, Association, & Consultancy

- **European Association for Biometrics**
  dinusha.frings@eab.org
- **KEMEA**
  m.kermitsis@kemea-research.gr
- **ARTTIC**
  sylvia.cucinelli@arttic.eu
- **Institute of Baltic Studies**
  marek@ibs.ee

***Editorial images:** *These images were used for editorial purposes only and do not reflect iMARS technologies.*

iMARS

image manipulation attack
resolving solutions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356.