ICAO

2025 ICAO TRIP SYMPOSIUM

MONTRÉAL , CANADA | NOVEMBER 4 - 6

The iMARS Project: Image Manipulation Attack Resolving Solutions: Overview

Securing Identity and Travel Documents Against Fraud

Funded by the European Union's Horizon 2020 programme

Renée Ong-de Jong
Research & Development Advisor Travel Documents
Ministry of the Interior and Kingdom Relations
The Netherlands

Introduction to iMARS

- **EU-funded project** 2020-2024 to combat identity and travel document fraud.
- **Consortium:**
  - Academic partners: NTNU, University of Bologna, University of Twente
  - Government: Bundeskriminalamt, National Police Directorate, National Office for Identity Data, Hellenic Police
  - Industry: Idemia, Cognitec, Vision-Box
- **Focus**: Morphing attacks—a major threat to European security.
- **Goal**: Develop robust solutions for detecting and preventing fraud, especially morphed face images.

iMARS
image manipulation attack resolving solutions

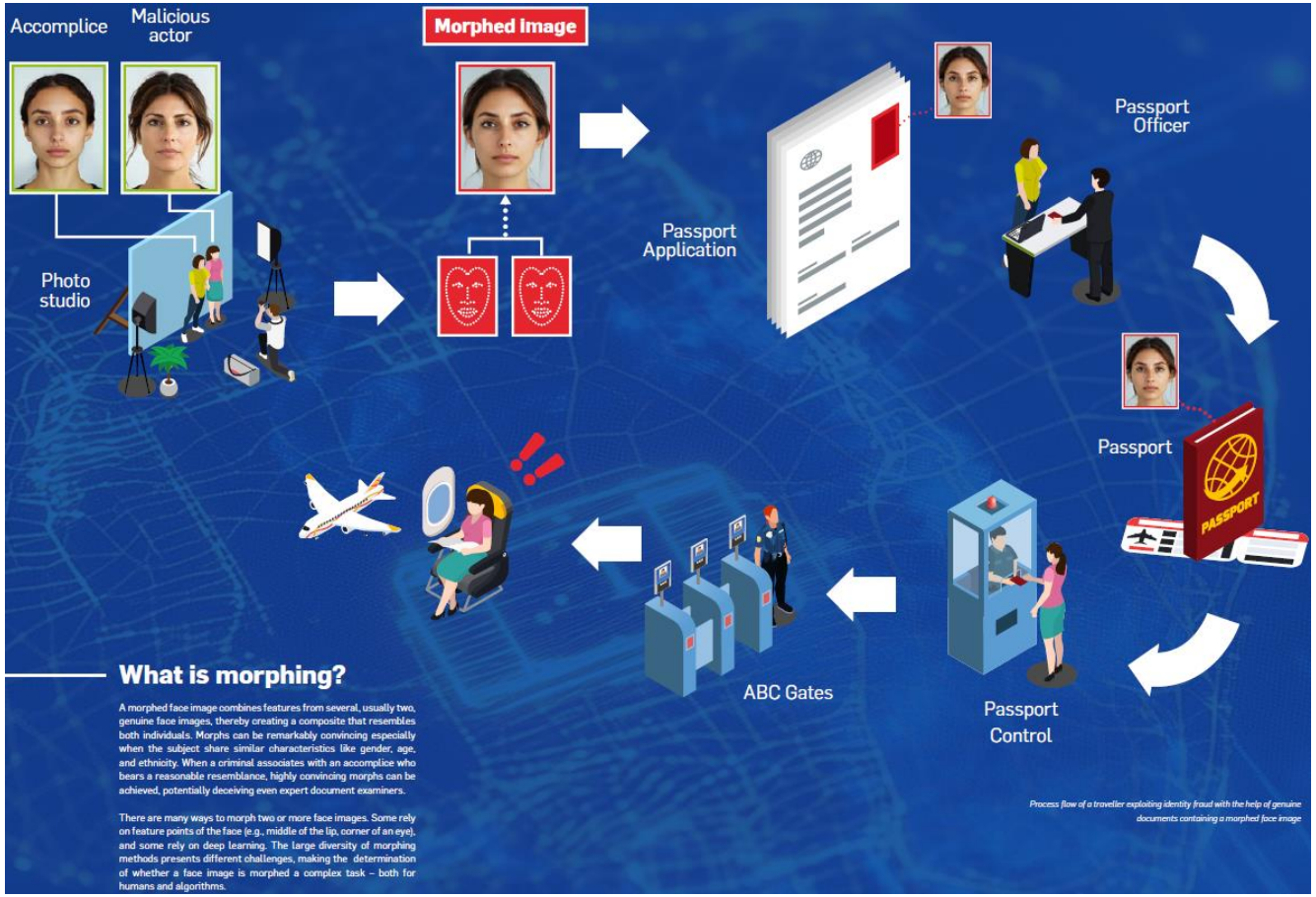
What is Morphing?

- **Morphing Technique**
  Morphing blends features from multiple faces to create a composite image resembling all contributors.

- **Fraudulent Use**
  Morphs can be highly convincing, especially with similar characteristics (gender, age, ethnicity) and used to fraudulently obtain identity documents.

- **Detection Challenges**
  Morphing techniques are complex, making detection difficult for humans and automated systems alike.

- **iMARS Detection Technology**
  iMARS develops advanced technologies to detect morphs across varied scenarios and image qualities.



The Challange of Identity Fraud

Threat of Identity Fraud

Identity and document fraud threaten European security by exploiting advanced face morphing techniques.

Challenges in Detection

Manipulated images are convincing and can deceive even expert document examiners.

iMARS Project Goals

iMARS develops technologies to detect morphing attacks and improve identity verification security.

Enhancing Border Security

Improved verification systems ensure secure border control and protect against morphing fraud.

iMARS Objectives

Analyzing ID Vulnerabilities

iMARS focuses on identifying weaknesses in the ID document application process to prevent morphing attacks.

Morphing Attack Detection Technologies

Developing advanced MAD technologies is central to detecting and preventing identity fraud effectively.

Enhancing Examiner Capabilities

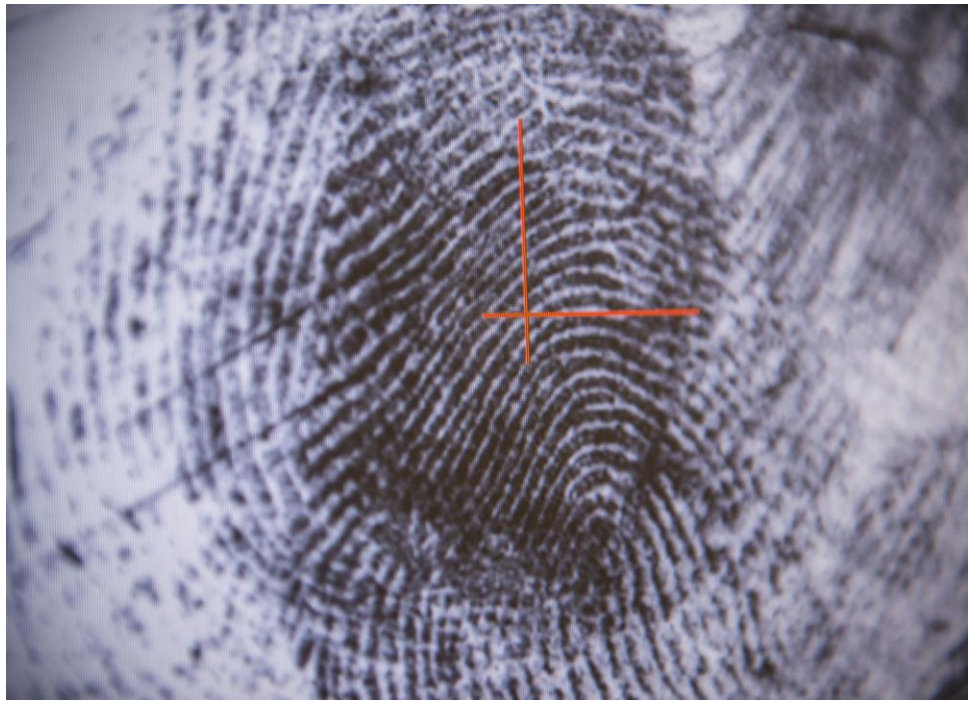
Improving both system and human examiner skills ensures more accurate identity verification processes.

Compliance and Collaboration

The project adheres to legal and ethical standards while collaborating with stakeholders for sustainable solutions.

Safe Enrolment Systems

Securing ID Document Enrolment



Enrolment process: From application to document delivery.

Key recommendations:

- Phase out printed images; use supervised digital acquisition.
- Implement biometric deduplication to ensure that each person can only registrate once.
- Use multimodal biometric data (face, fingerprint, iris).
- Avoid mobile enrolment until mature and secure.

Morphing Attack Detection (MAD)

- **Differential MAD (D-MAD):** Compares passport image + live capture.
- **Single MAD (S-MAD):** Detects morphing in a single image.
- **Algorithm Development and Benchmarking**: Multiple algorithms were developed and benchmarked, significantly improving detection accuracy and robustness.
- **Biometric Security Leadership**: iMARS technologies are positioned as leading tools in biometric security with advanced MAD solutions.
- **Challenges:** Generalization, data shortage, explainability.
- **Results:** Algorithms outperform human observers.

BOEP: Bologna Online evaluation platform for MAD algorithms.
https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx

Human Detection & Training

- Studied human ability to detect morphs: **experience and training matter**.
- Developed **e-learning modules** and practical training.
- **Key finding:** Training reduces error rates significantly.

E-learning & training modules for professionals.
http://www.nidsenter.no/

Portrait Securing Technologies

- **CodeFace®**(Portuguese Mint and Official Printing Office)**:** Encodes hidden messages in printed portraits for integrity validation.
- **TrustFace®:** Uses 2D barcodes to secure portrait embeddings.

Benefits: High performance, mobile compatibility.

TrustFace

CodeFace

Document Verification & Fraud Detection

- AI algorithms classify documents by type, model, and country.
- Detects forgeries, holograms, and font inconsistencies.
- **Mobile solutions** for field testing and stakeholder feedback.

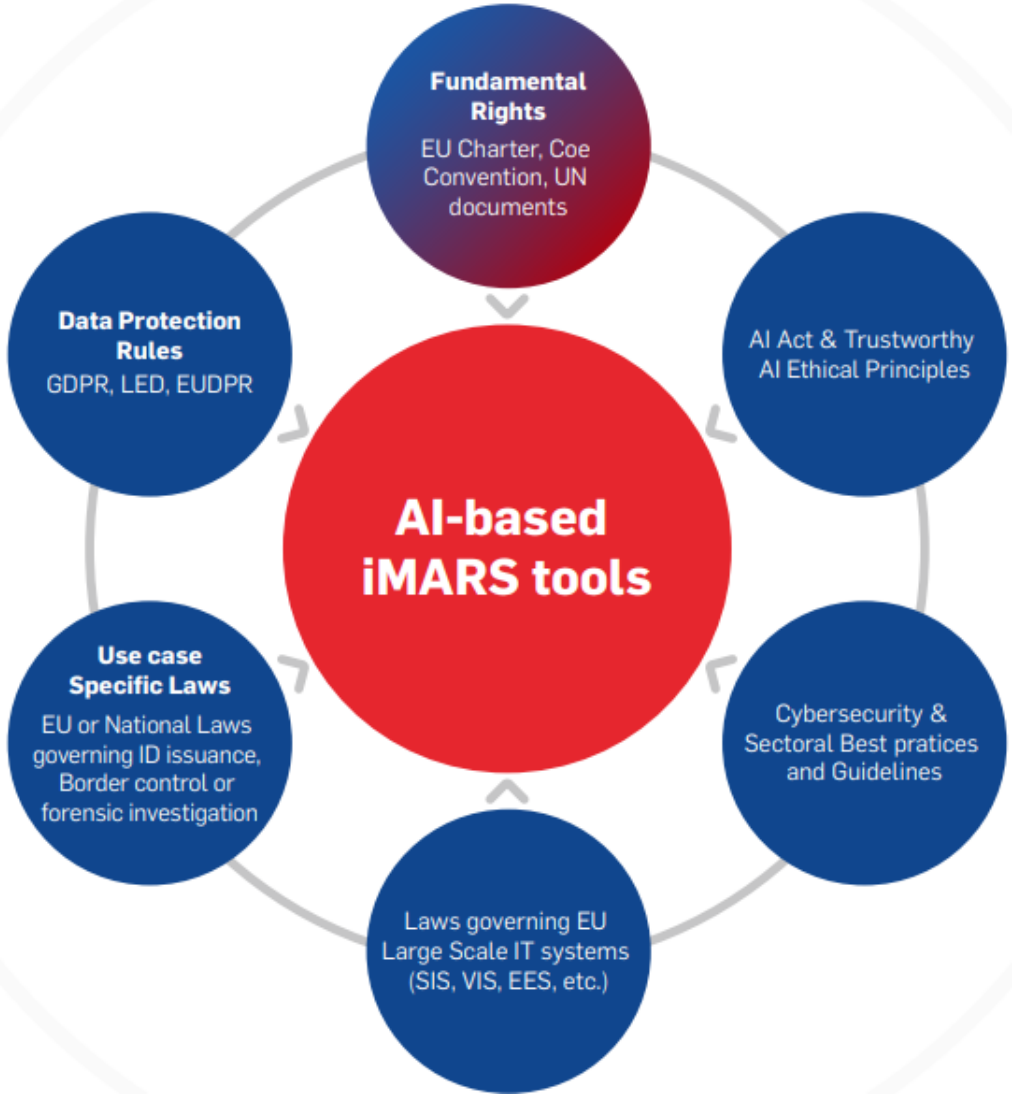
Morphing traces detection tool

- **Morphing traces detection tool for digital image analysis.** https://doi.org/10.3389/fcomp.2023.981933
- 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.
- **Benefits**: Written in Python, this tool is easy to explain, easy to use and efficient, taking just a few seconds per image.

Legal, Ethical & Societal Compliance

Ethical & Legal Considerations

- Ensured compliance with **GDPR** and EU values.
- Addressed fundamental rights: privacy, non-discrimination.
- Developed **guidelines** for responsible use of MAD technologies.



*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**.*

Key Achievements

- Developed **automated MAD algorithms** for single and differential image detection.
- Created **BOEP** (Bologna Online Evaluation Platform) for benchmarking MAD algorithms.
- Established **training programs** for ID document experts.
- Contributed to **ISO/IEC standards** for biometric sample quality.
- Produced **50+ scientific publications** and **20+ algorithms**.

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 *Julie Petit* julie.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 Guoqiong 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

[Publications — iMARS](www.imars-project.eu)
www.imars-project.eu

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)
- 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)

Future Steps & Related Projects

Recommendations:

- Use live capture processes in passport applications.
- Train practitioners and measure the importance of morphing attacks.
- Continuous improvement of MAD technologies.

Related EU projects:

- **CarMen:** Continuous border control for pedestrians/vehicles.
- **EINSTEIN:** Digital identity and fraud detection.
- **PopEye:** Biometric technologies for EU borders.
- **SafeTravellers**: Secure and Frictionless Identity for EU and Third Country National citizens

Thank You

ICAO