iMARS - Image Manipulation Attack Resolving Solutions

Christoph Busch

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html
more information at:
https://christoph-busch.de/projects-mad.html
latest news at:
https://twitter.com/busch_christoph

ICMPD, November 24, 2020

European Association for Biometrics
eab
Human Identity in Europe

The iMARS Project Summary

The Key Figures

iMARS project

- Start date: 1 September 2020
- End date: 31 August 2024
- H2020-SU-SEC-2019
- Grant agreement ID: 883356
- Programme(s):
  - H2020-EU.3.7.3. - Strengthen security through border management
  - H2020-EU.3.7.8. - Support the Union's external security policies including through conflict prevention and peace-building
- Topic:
  - SU-BES02-2018-2019-2020 - Technologies to enhance border and external security
- Overall budget: € 6 988 521,25
- Website: https://cordis.europa.eu/project/id/883356

The Consortium

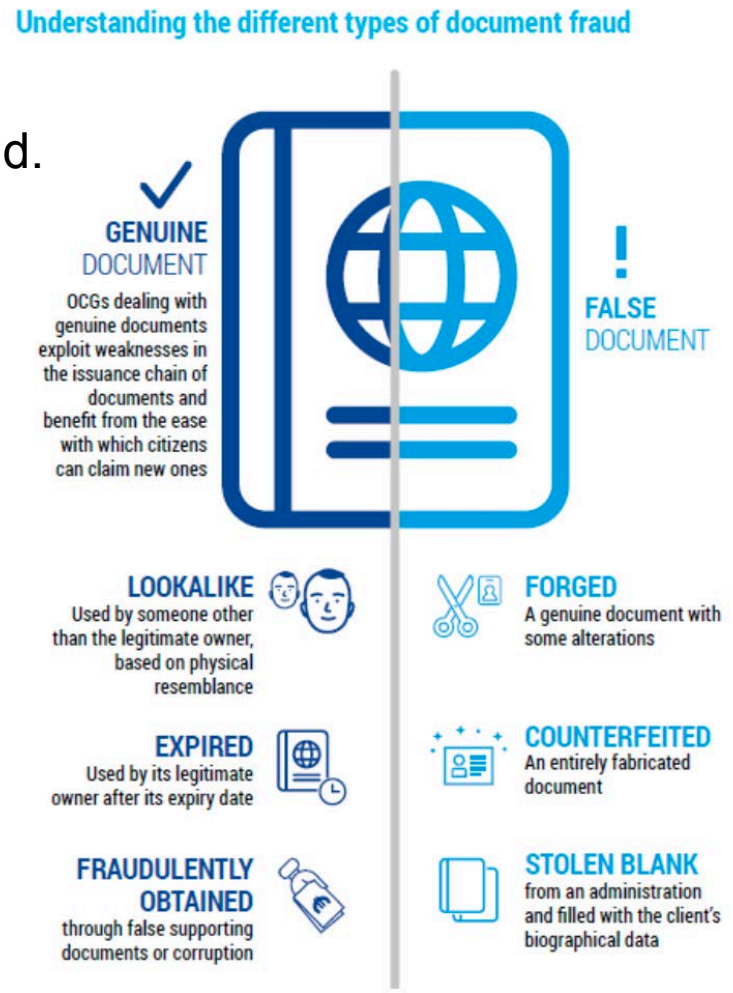
24 Partners

- IDM - IDEMIA IDENTITY & SECURITY FRANCE (FR)
- DG - IDEMIA IDENTITY & SECURITY GERMANY (DE)
- COG - COGNITEC SYSTEMS GMBH (DE)
- VIS - VISION BOX (PT)
- MOB - MOBAI AS (NO)
- ART - ARTTIC (FR)
- SUR - SURYS (FR)
- NTN - NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET (NO)
- UBO - UNIVERSITA DI BOLOGNA (IT)
- HDA - HOCHSCHULE DARMSTADT (DE)
- KUL - KATHOLIEKE UNIVERSITEIT LEUVEN (BE)
- IBS - INSTITUTE OF BALTIC STUDIES (EE)
- EAB - EUROPEAN ASSOCIATION FOR BIOMETRICS
- KEM - KENTRO MELETON ASFALEIAS (EL)
- BKA - BUNDESKRIMINALAMT (DE)
- NOI - MINISTERIE VAN BINNENLANDSE ZAKEN (NL)
- INC - IMPRENSA NACIONAL (PT)
- POD - POLITIDIREKTORATET (NO)
- PBP - PORTUGUESE IMMIGRATION AND BORDERS SERVICES (PT)
- HEP - HELLENIC POLICE (EL)
- CYP - CYPRUS POLICE (CY)
- PBM - BORDER POLICE OF THE REPUBLIC OF MOLDOVA (MD)
- BFP - POLICE FEDERALE BELGE (BE)

The Objectives

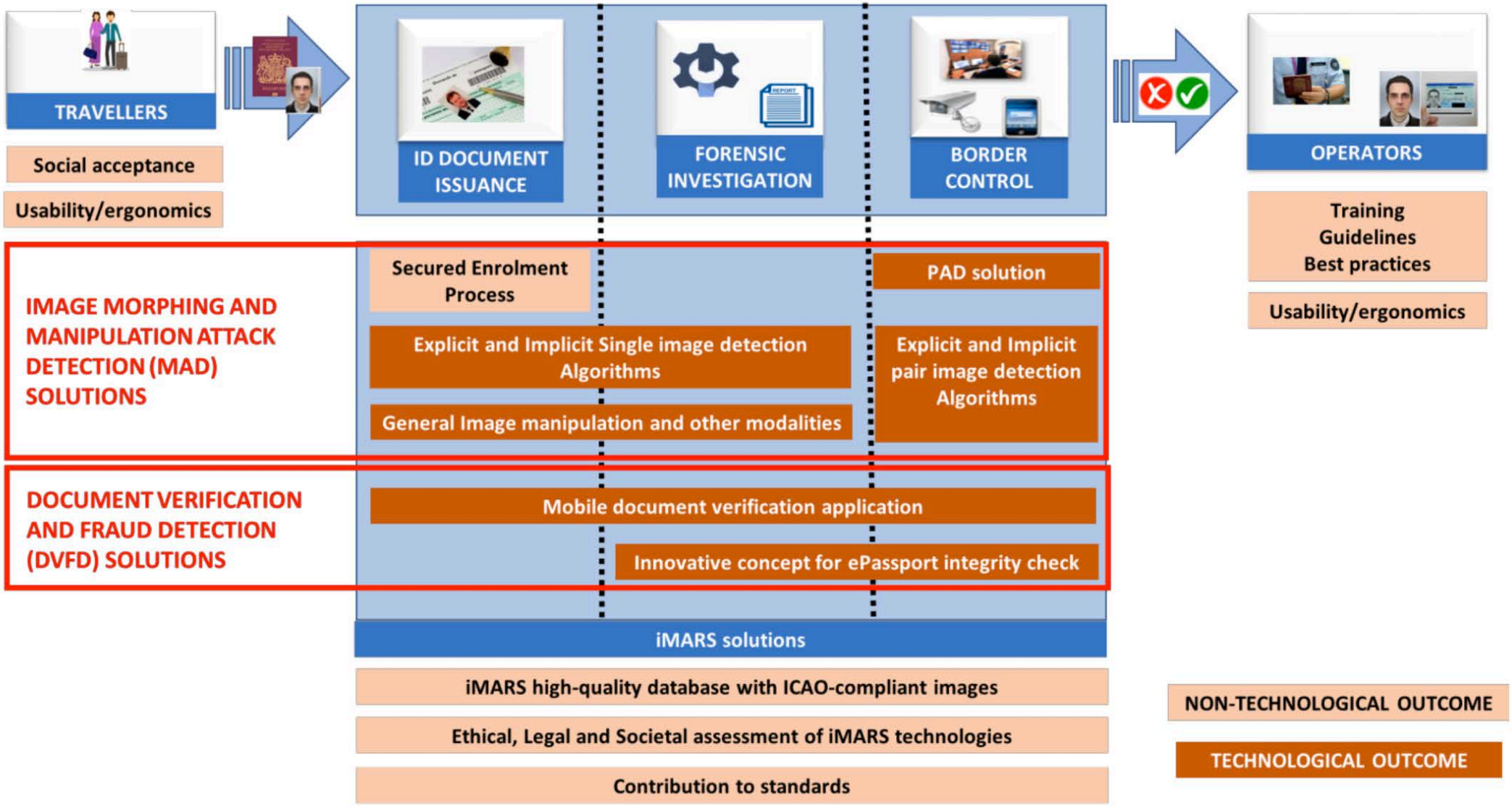
Technologies to enhance border and external security

- The iMARS project will provide:
  - Image Morphing and manipulation Attack Detection (MAD) solutions to assess ID documents validity against document fraud.
    - focus on attacks during enrolment steps and at the border crossing stations
  - Document Verification and Fraud Detection (DVFD) solutions to support border guards in the verification process by providing mobile tools and training.
- The solutions developed in iMARS will:
  - focus on electronic ID documents
  - be flexible enough to enable the integration with existing solutions and serving various use cases:
    - ID Document application or renewal
    - border control
    - forensic investigation of ID Documents.



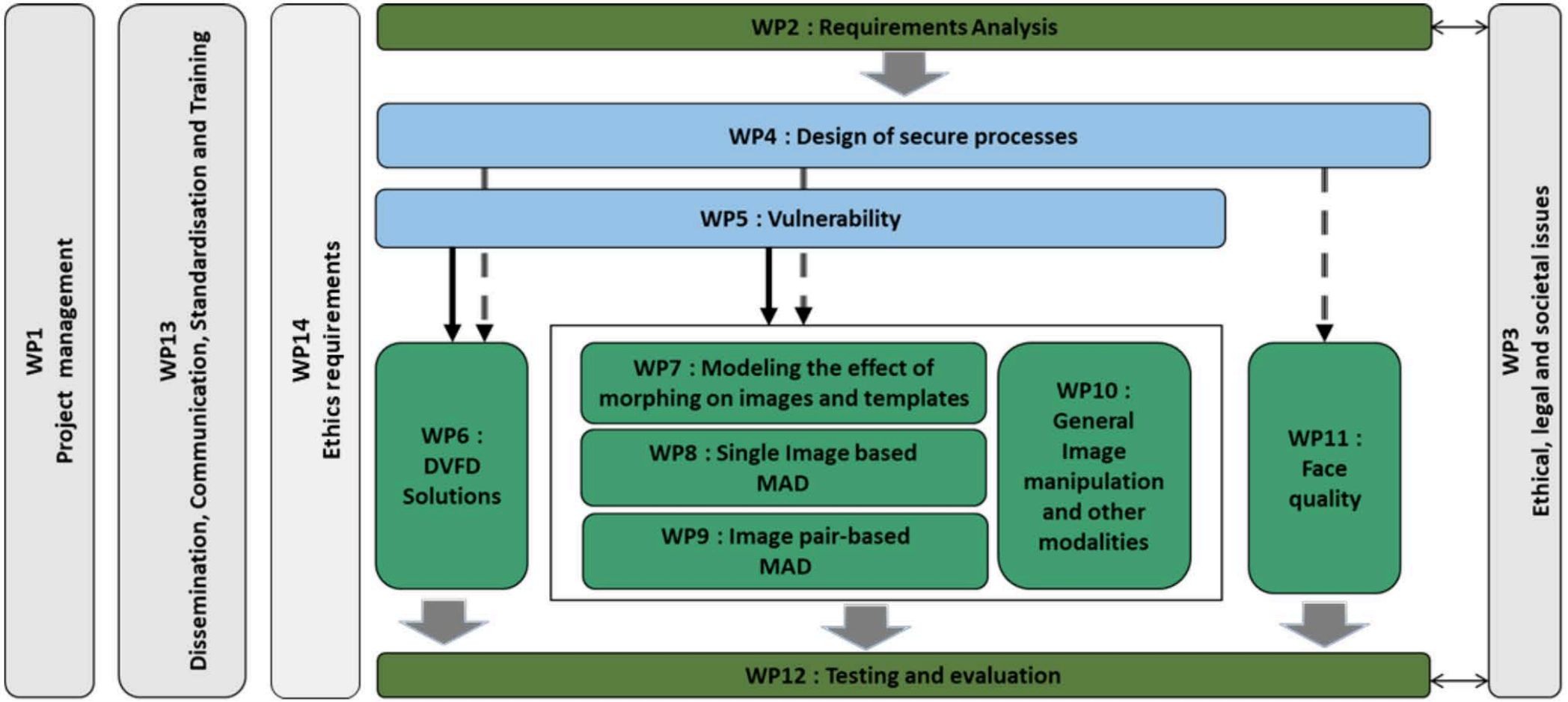
The iMARS Research

The iMARS overall concept



The Work Packages

The iMARS work packages dependencies



What needs to be done -

after the SOTAMD project is completed?

MAD Action Plan

1.) Establish consensus amongst stakeholders

- Europe should immediately start an action to secure
  - the trusted link between a MRTD and the document holder meaning to switch to live enrolment !
  - and to develop and deploy technical mechanisms that can detect a morph passport at borders.
- Support the iMARS-consortium, that is ready to jointly work on the morphing challenges
  - iMARS is a pan-European approach that is supported by the European Association for Biometrics (EAB) https://eab.org/

MAD Action Plan

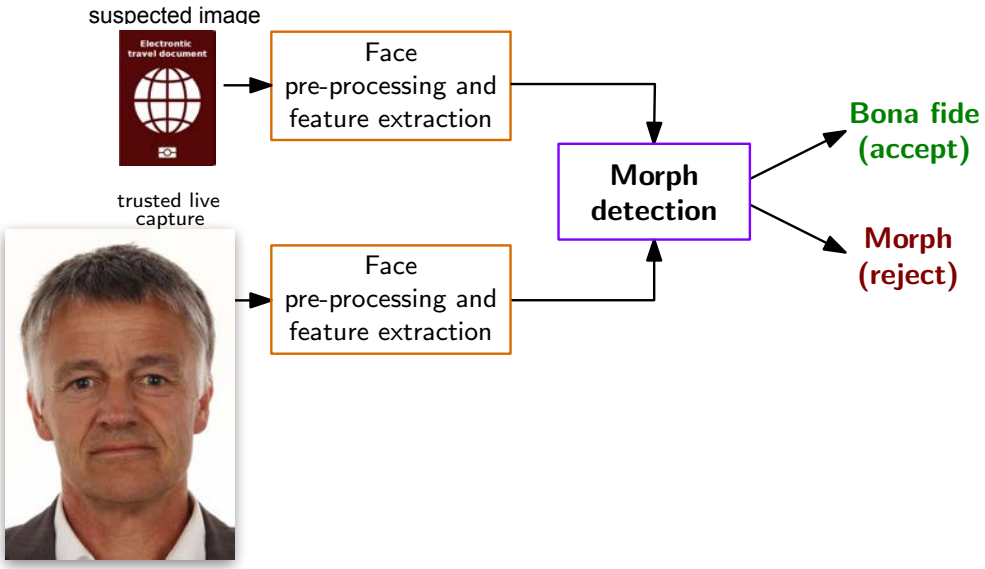
2.) Standardise the passport application process

- A European regulation should enforce that all Member States switch to live enrolment, as it is already operational e.g. in Norway and Sweden.
  - Only then, with full control of the biometric capture process by a civil servant in the passport application office, trust in the link of passport holder to reference data can be assured.
    - Note: The German parliament has only recently (November 4) revised the passport law, to avoid printed passport photos
- The iMARS consortium has proposed to define a secure ID Document application process:
  - Make it difficult to apply for an ID document with a photograph that has been morphed or manipulated otherwise (e.g. data subjects want to look younger)
  - Take precautions to detect a case that someone tries to enrol with a well-crafted facemask (avoid a presentation attack with a morphed face image on the mask)
  - The capture device certification scheme will be recorded in the data record, as defined in the new extensible interchange format ISO/IEC 39794-5

MAD Action Plan - iMARS Project

3.) Detect automatically Morph Passports at Borders

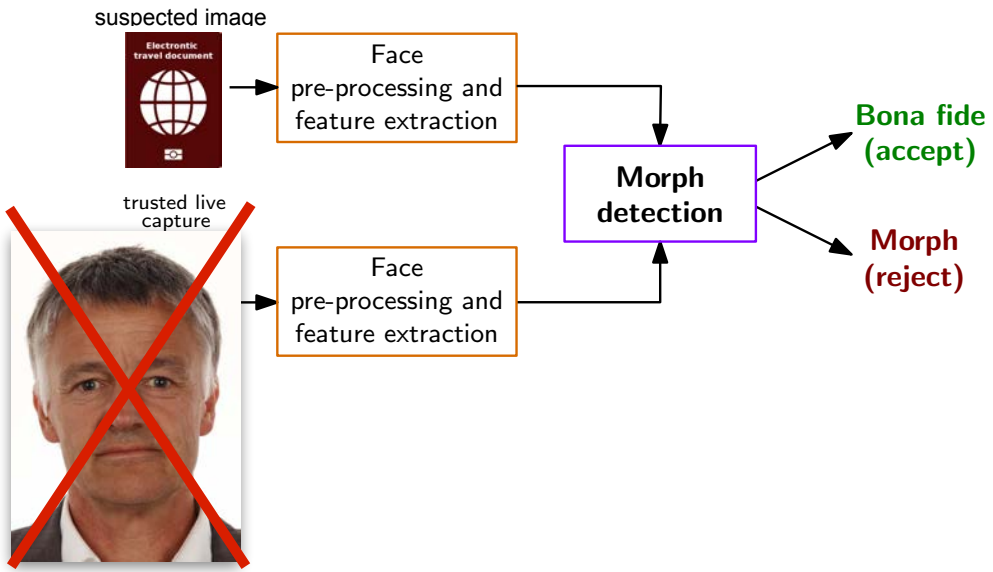
- After the completed transition to live enrolment in all MS we must anticipate that European passports - potentially containing a morphed image - are presented at least for the next 10 years.
  - Robust border control processes based on a differential morphing attack analysis, where the quality of probe image varies.
  - Trusted live capture images must be in realistic degraded quality!

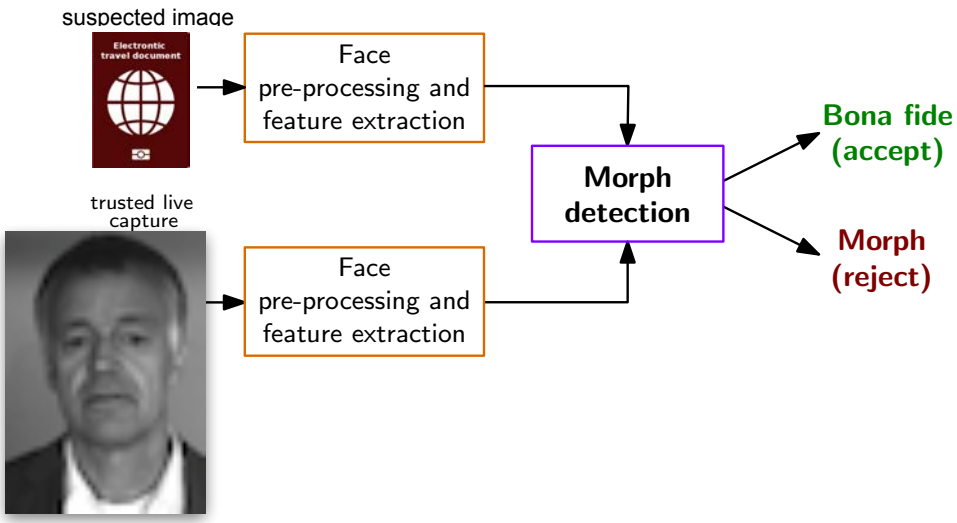


MAD Action Plan - iMARS Project

3.) Detect automatically Morph Passports at Borders

- After the completed transition to live enrolment in all MS we must anticipate that European passports - potentially containing a morphed image - are presented at least for the next 10 years.
  - Robust border control processes based on a differential morphing attack analysis, where the quality of probe image varies.
  - Trusted live capture images must be in realistic degraded quality!





- Explicit and implicit D-MAD algorithms

MAD Action Plan

4.) Detect Morph Passports in Forensic Investigations

- A forensic investigator has a single image only
- In support of forensic investigations, we need single image MAD
  - also known as no-reference MAD or forensic MAD
  - explicit MAD and implicit MAD with transfer learning
  - trained with large-scale face morph databases.
  - based on the relatively low-resolution digital image stored in the passport,
  - print and scan MAD robustness
  - fusion of multiple MAD subsystems.

MAD Action Plan

5.) Compose Test Data and Online Evaluation Platform

- Testing of MAD solution can't be done without appropriate data.
- Need for an iMARS mixed quality dataset and diversification
  - more subjects
  - more enrolment processes / print and scan equipment
  - more morphing tools
  - high AND controlled degrading quality
- Augment the Bologna-Online-Evaluation-Platform (BOEP)
  - Provide open access benchmark tests.
  - Include S-MAD evaluation:
    https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaSMAD.aspx
  - Thus national border control agencies will be able to evaluate
    if the MAD State-of-the Art meets the operational requirements.

MAD Action Plan

6.) Standardise Testing of MAD Solutions

- Find consensus, how we test
  - Measures for vulnerability and detection accuracy
- Morphing vulnerability metric based on the Mated-Morph-Presentation-Match-Rate (MMPMR)
  - anchor the MAD evaluation methodology in the ISO/IEC 30107 multipart standard
  - Find consensus in the MAD research community
- Standardise metrics to evaluate the performance of MAD methods
  - APCER - Attack Presentation Classification Error Rate
  - BPCER - Bona Fide Presentation Classification Error Rate
  - corresponding DET-Plots
- Border control agencies of EU Member State shall be motivated to participate in this standardisation process

MAD Action Plan - iMARS Project

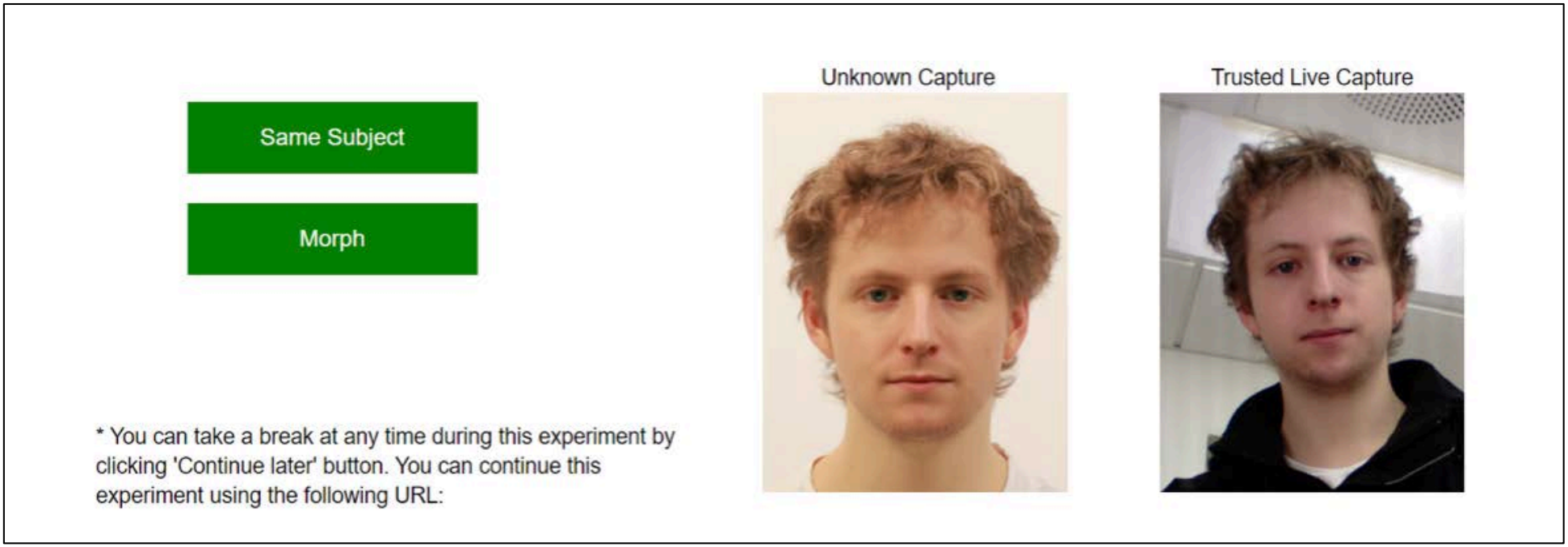
7.) Develop Face Image Quality Metrics

- We need the equivalent to NFIQ2.0 for facial images
- Ensure that captured samples that are sufficiently good in terms of illumination, sharpness, or pose
- Align with the framework for biometric sample quality described in ISO/IEC 29794-1:2016
  - align with ISO/IEC NP 29794-5
    https://www.iso.org/standard/81005.html
    http://www.paddymondo.net/ISO_IEC_29794_5.pdf
- Develop an automatic face image quality assessment software,
  - which can predict recognition accuracy
- Once predictive face quality metrics are available,
  - MAD evaluation can be adapted to the three relevant scenarios (ID Document issuance, border control, and forensic investigation)
  - we can report the impact of face image quality on morphing attack detection

MAD Action Plan

8.) Train Communication Personnel and Border Officers

- Train the agencies staff, how to react
  - to mitigate public excitement and explain attack resolving solutions against morphing attacks,
- Develop best practices for improving the officers' skills on manipulated/morphed image and document fraud detection
  - show to border guards that the MAD tools will not replace, but complement, their expertise.



Thanks

I would like to thank the sponsors of this work:

- iMARS-Project has received funding from the European Union's H2020 research and innovation programme under grant agreement No 883356
  - The content of this presentation represents the views of the author only and is his sole responsibility.
    The European Commission does not accept any responsibility for use that may be made of the information it contains.

More information

The MAD website

https://www.christoph-busch.de/projects-mad.html

The MAD survey paper

- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019)

IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

ULRICH SCHERHAG, CHRISTIAN RATHGEB, JOHANNES MERKLE, RALPH BREITHAUPT, AND CHRISTOPH BUSCH

ABSTRACT Recently, researchers found that the intended generalizability of (deep) face recognition systems increases their vulnerability against attacks. In particular, the attacks based on morphed face images pose a severe security risk to face recognition systems. In the last few years, the topic of (face) image morphing and automated morphing attack detection has sparked the interest of several research laboratories working in the field of biometrics and many different approaches have been published. In this paper, a conceptual categorization and metrics for an evaluation of such methods are presented, followed by a comprehensive survey of relevant publications. In addition, technical considerations and tradeoffs of the surveyed methods are discussed along with open issues and challenges in the field.

INDEX TERMS Biometrics, face morphing attack, face recognition, image morphing, morphing attack detection.

I. INTRODUCTION

A. FACE MORPHING ATTACK

Contact

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194