# 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

EAB-RPC, September 16, 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 -<br>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)

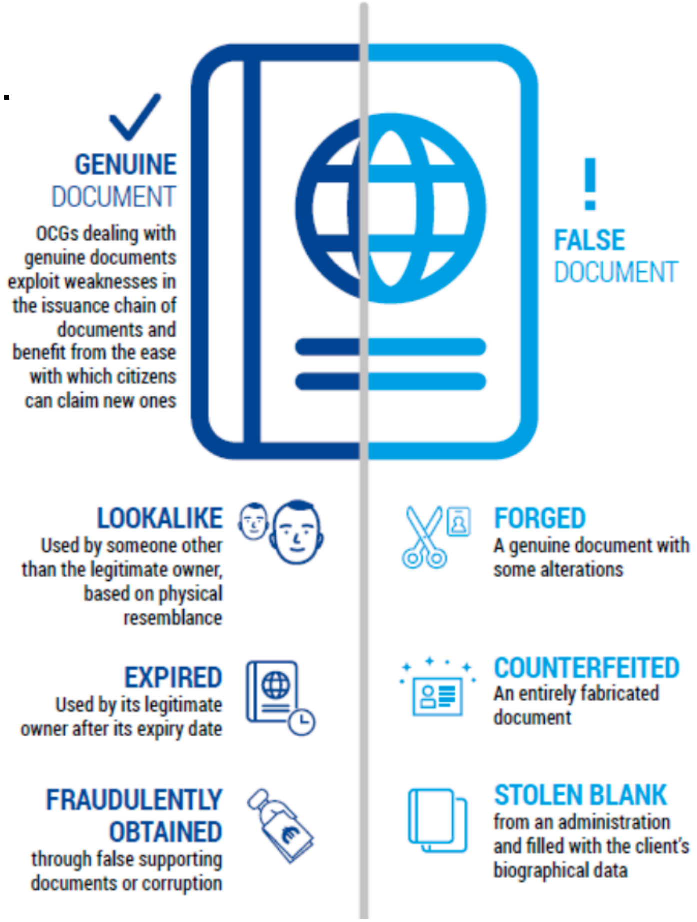
Norway
Finland
Sweden
Estonia
Latvia
Denmark
Lithuania
Ireland
United Kingdom
Belarus
Netherlands
Poland
rmany
Bel
Lu
Czechia
Ukraine
Slovakia
Fran
Liechtenstein
Austria
Hungary
Moldova
Switzerland
Slovenia
Romania
Croatia
Monaco
San Marino
Serbia
Andorra
Montenegro
Bulgaria
North Macedonia
Spain
Albania
Portugal
Greece
Turkey
Malta
Cyprus
Tunisia
Morocco
Israel
Algeria

# 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.

Understanding the different types of document fraud



GENUINE DOCUMENT
OCGs dealing with genuine documents exploit weaknesses in the issuance chain of documents and benefit from the ease with which citizens can claim new ones

FALSE DOCUMENT

LOOKALIKE
Used by someone other than the legitimate owner, based on physical resemblance

EXPIRED
Used by its legitimate owner after its expiry date

FRAUDULENTLY OBTAINED
through false supporting documents or corruption

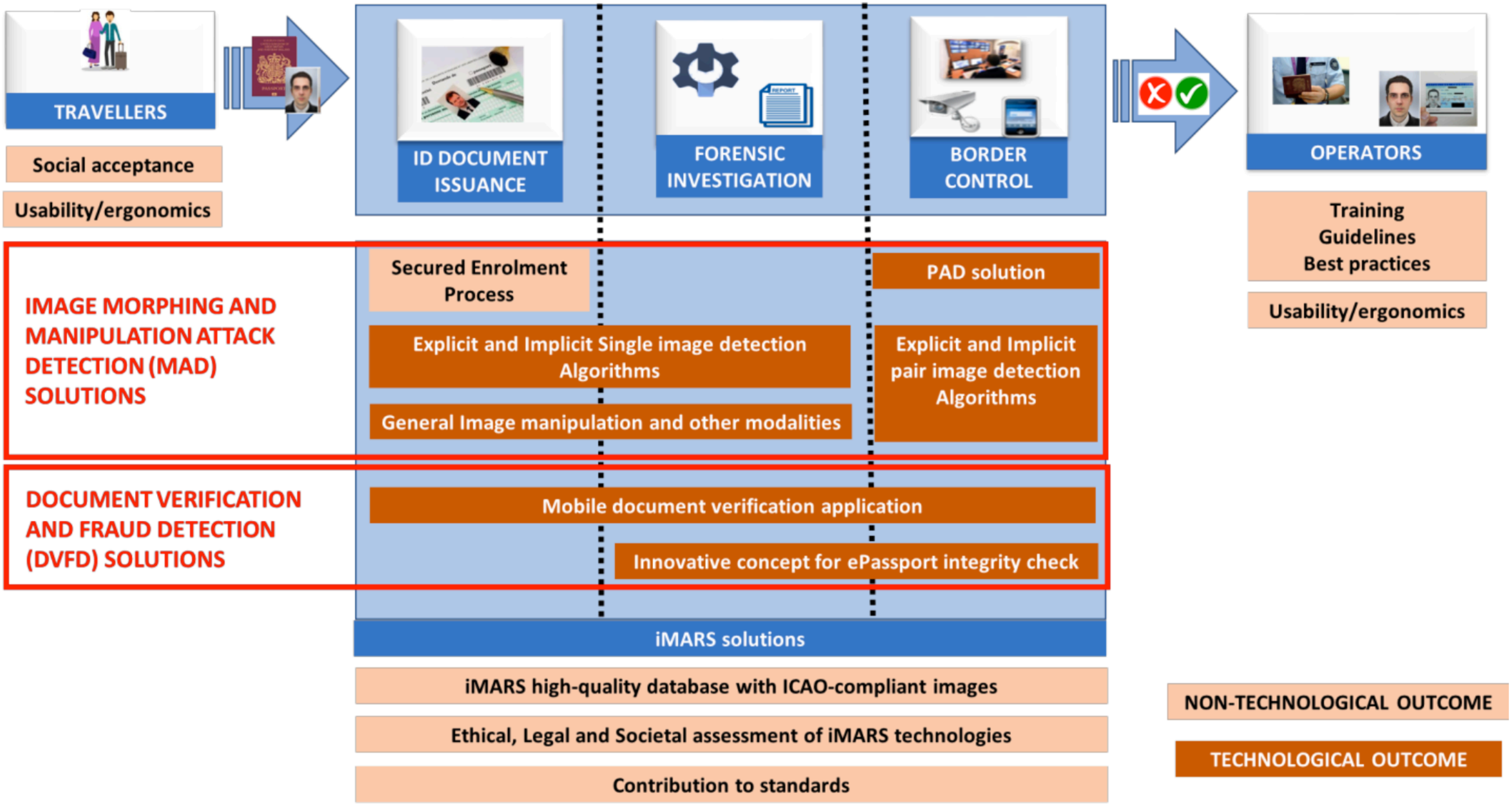
FORGED
A genuine document with some alterations

COUNTERFEITED
An entirely fabricated document

STOLEN BLANK
from an administration and filled with the client's biographical data

# The iMARS Research

## The iMARS overall concept



TRAVELLERS

Social acceptance

Usability/ergonomics

ID DOCUMENT ISSUANCE

FORENSIC INVESTIGATION

BORDER CONTROL

OPERATORS

Training
Guidelines
Best practices

Usability/ergonomics

IMAGE MORPHING AND MANIPULATION ATTACK DETECTION (MAD) SOLUTIONS

Secured Enrolment Process

PAD solution

Explicit and Implicit Single image detection Algorithms

Explicit and Implicit pair image detection Algorithms

General Image manipulation and other modalities

DOCUMENT VERIFICATION AND FRAUD DETECTION (DVFD) SOLUTIONS

Mobile document verification application

Innovative concept for ePassport integrity check

iMARS solutions

iMARS high-quality database with ICAO-compliant images

Ethical, Legal and Societal assessment of iMARS technologies

Contribution to standards

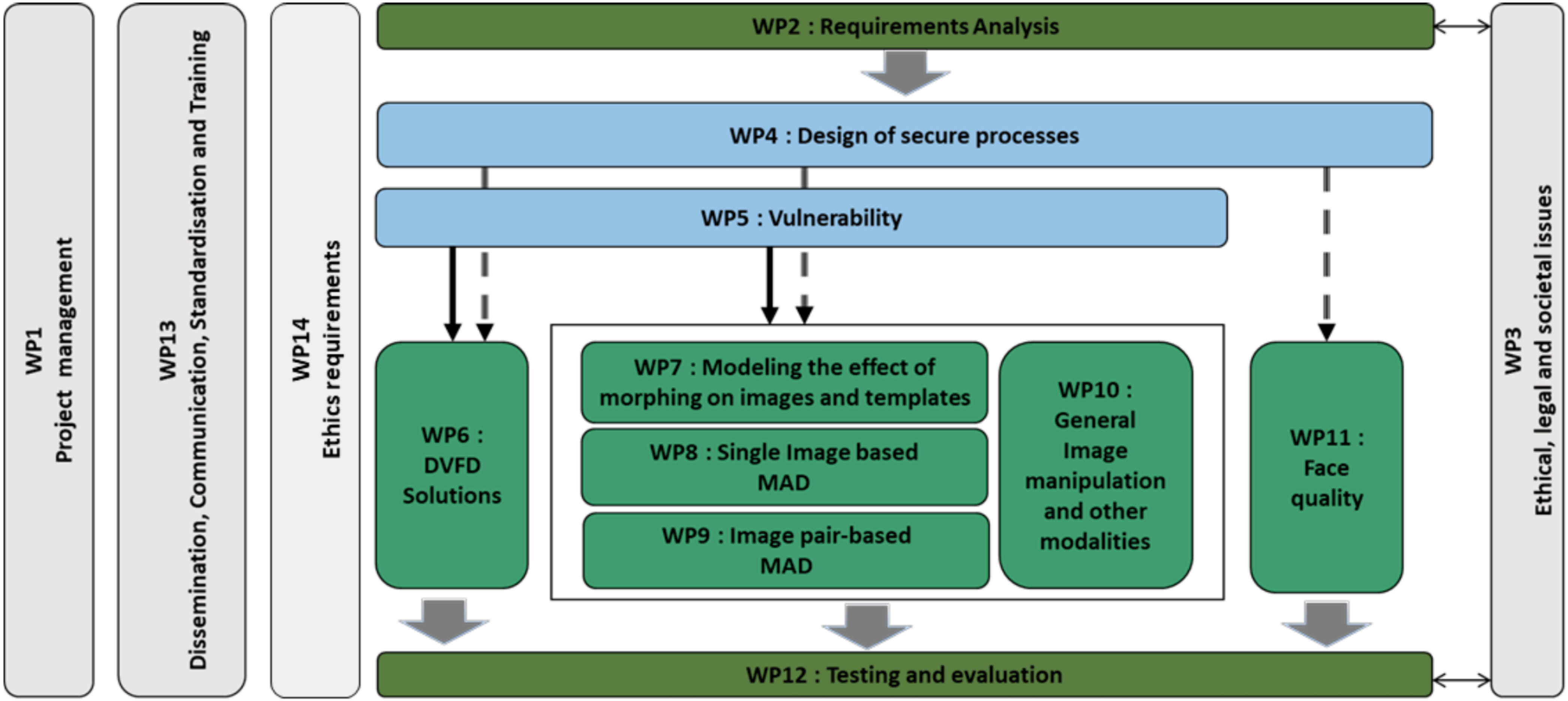
NON-TECHNOLOGICAL OUTCOME

TECHNOLOGICAL OUTCOME

# The Work Packages

## The iMARS work packages dependencies

-



WP1 Project management

WP13 Dissemination, Communication, Standardisation and Training

WP14 Ethics requirements

WP2 : Requirements Analysis

WP4 : Design of secure processes

WP5 : Vulnerability

WP6 : DVFD Solutions

WP7 : Modeling the effect of morphing on images and templates

WP8 : Single Image based MAD

WP9 : Image pair-based MAD

WP10 : General Image manipulation and other modalities

WP11 : Face quality

WP12 : Testing and evaluation

WP3 Ethical, legal and societal issues

## 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 !
    - Note: The German parliament is discussing a revision of the passport law these days
  - 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)

# MAD Action Plan

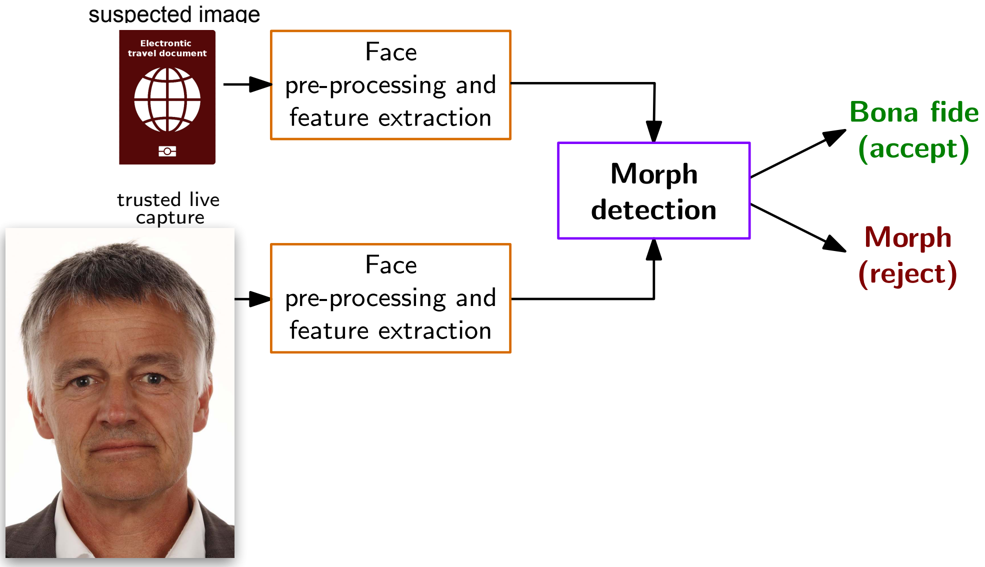
## 2.) Standardise the passport application process

- 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.
- 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

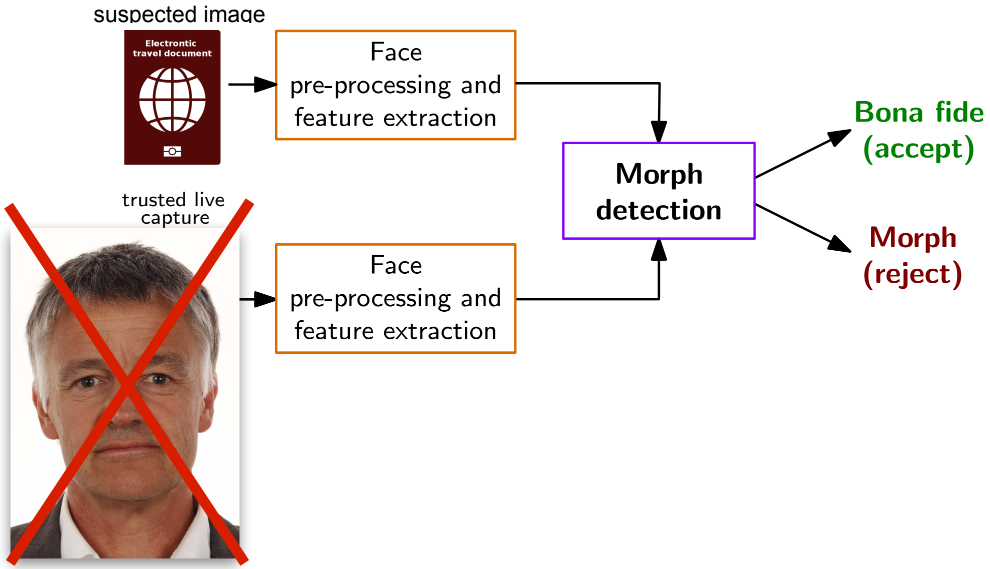
- After the completed transition to live enrolment in all MS we must anticipate that European passports
  - potentially containing a morphed image -
  are presented at least for the next 10 years.
  - Robust border control processes based on a differential morphing attack analysis, where the quality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

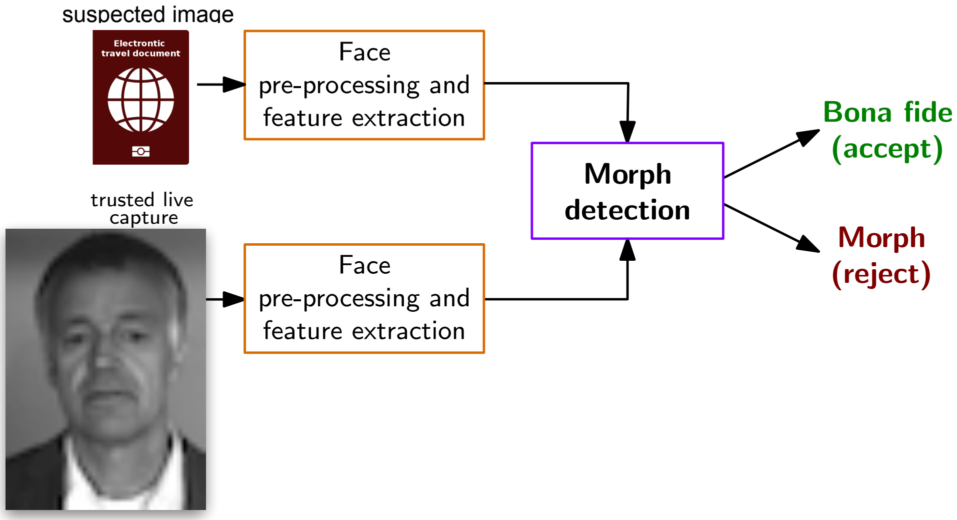

suspected image
Electrontic travel document
trusted live capture
Face pre-processing and feature extraction
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

# 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!


suspected image
Electronic travel document
Face pre-processing and feature extraction
trusted live capture
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)


suspected image
Electronic travel document
Face pre-processing and feature extraction
trusted live capture
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

- 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.
  - Thus Frontex and the national border control agencies will be able to evaluate if the MAD State-of-the Art meets the operational requirements.
  - The technical interfaces are by design equivalent to the benchmark portal of the NIST Face Recognition Vendor Test (FRVT) MORPH Competition
  - https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

# 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

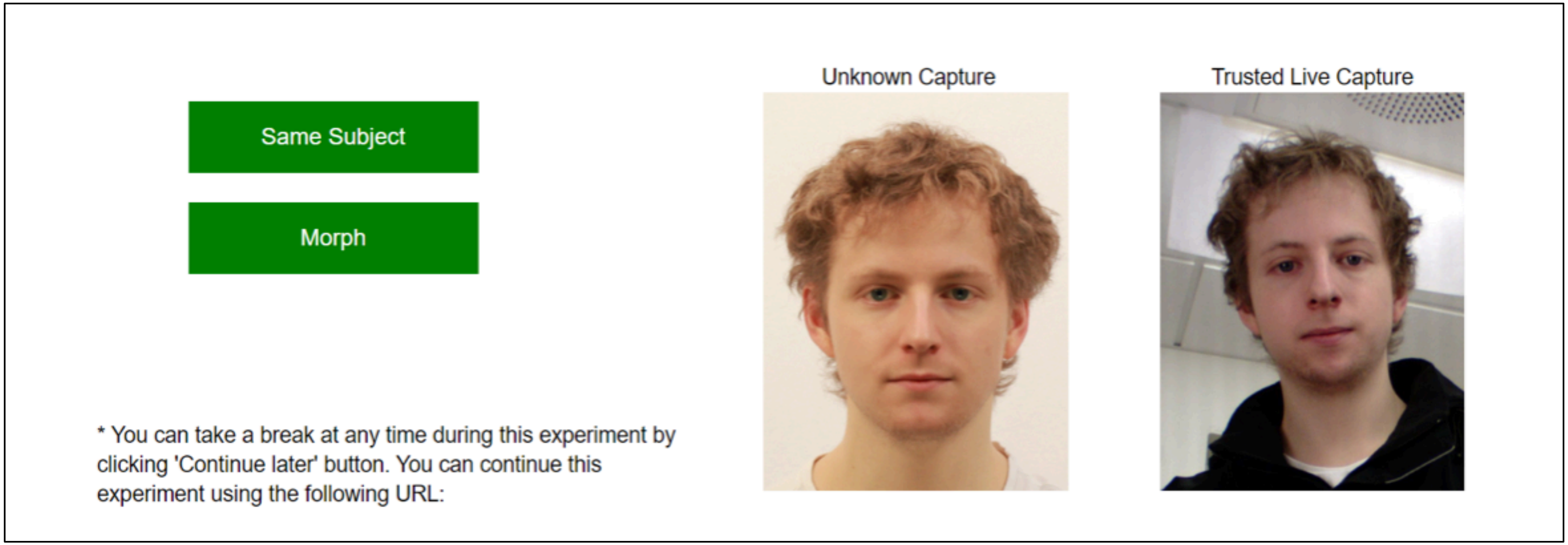
## 7.) Develop Face Image Quality Metrics

- 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
- 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.



* You can take a break at any time during this experiment by clicking 'Continue later' button. You can continue this experiment using the following URL:

# Conclusion

We are facing a situation, where

- Passports with morphs are already in circulation
  - 1000+ reported cases
  - Switch to live enrolment is a good decision, but does not solve the problem
- Passports with morphed face images will have a major impact on border security (introduction of EU's entry/exit system, global migration flows)
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous such opportunities …

***This project has received funding from the European Union's H2020 research and innovation programme under grant agreement No 883356***

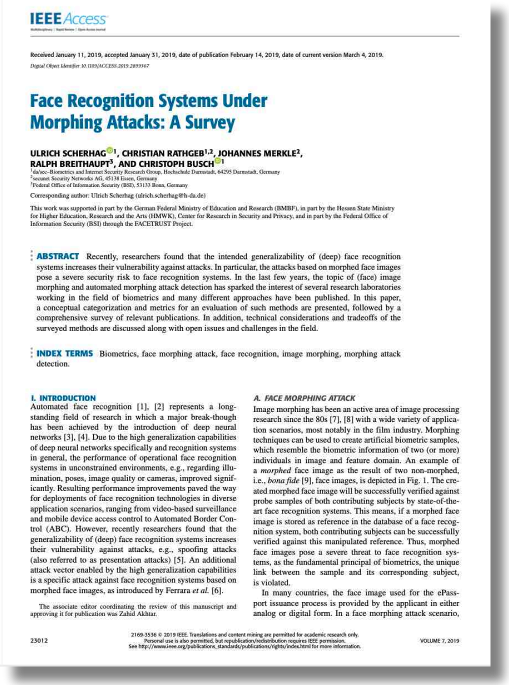
# More information

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

Received January 11, 2019, accepted January 31, 2019, date of publication February 14, 2019, date of current version March 4, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2899367*

## Face Recognition Systems Under Morphing Attacks: A Survey

ULRICH SCHERHAG[1], CHRISTIAN RATHGEB[1,2], JOHANNES MERKLE[2], RALPH BREITHAUPT[3], AND CHRISTOPH BUSCH[1]

[1] da/sec–Biometrics and Internet Security Research Group, Hochschule Darmstadt, 64295 Darmstadt, Germany
[2] secunet Security Networks AG, 45138 Essen, Germany
[3] Federal Office of Information Security (BSI), 53133 Bonn, Germany

Corresponding author: Ulrich Scherhag (ulrich.scherhag@h-da.de)

This work was supported in part by the German Federal Ministry of Education and Research (BMBF), in part by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK), Center for Research in Security and Privacy, and in part by the Federal Office of Information Security (BSI) through the FACETRUST Project.

**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

Automated face recognition [1], [2] represents a long-standing field of research in which a major break-though has been achieved by the introduction of deep neural networks [3], [4]. Due to the high generalization capabilities of deep neural networks specifically and recognition systems in general, the performance of operational face recognition systems in unconstrained environments, e.g., regarding illumination, poses, image quality or cameras, improved significantly. Resulting performance improvements paved the way for deployments of face recognition technologies in diverse application scenarios, ranging from video-based surveillance and mobile device access control to Automated Border Control (ABC). However, recently researchers found that the generalizability of (deep) face recognition systems increases their vulnerability against attacks, e.g., spoofing attacks (also referred to as presentation attacks) [5]. An additional attack vector enabled by the high generalization capabilities is a specific attack against face recognition systems based on morphed face images, as introduced by Ferrara *et al.* [6].

#### A. FACE MORPHING ATTACK

Image morphing has been an active area of image processing research since the 80s [7], [8] with a wide variety of application scenarios, most notably in the film industry. Morphing techniques can be used to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and feature domain. An example of a *morphed* face image as the result of two non-morphed, i.e., *bona fide* [9], face images, is depicted in Fig. 1. The created morphed face image will be successfully verified against probe samples of both contributing subjects by state-of-the-art face recognition systems. This means, if a morphed face image is stored as reference in the database of a face recognition system, both contributing subjects can be successfully verified against this manipulated reference. Thus, morphed face images pose a severe threat to face recognition systems, as the fundamental principal of biometrics, the unique link between the sample and its corresponding subject, is violated.

In many countries, the face image used for the ePassport issuance process is provided by the applicant in either analog or digital form. In a face morphing attack scenario,

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

23012

2169-3536 © 2019 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

VOLUME 7, 2019

# 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