

Security Sensitivity Statement

This form is related to the Security Sensitivity Assessment procedure which will assure that no sensitive information will be included in the publications and deliverables of the MobilePass project.

Security sensitive information means here all information in whatever form or mode of transmission that is classified by Council Decision on the security rules for protecting EU classified information (2011/292/EU) and all relevant national laws and regulations. The information can be already classified, or such that it should be classified.

In practice the following criteria is used:

- Information is already classified
- Information may describe shortcomings of existing safety, security or operating systems
- Information is such, that it might be misused.
- Information that can cause harm to
 - o European Union
 - o a Member State
 - o society
 - o industry and companies
 - o third country
 - o citizen or an individual person of a country.

Publication identification

Title of the Publication: Deliverable D 5.1, Report on Evaluation Dataset

Authors (Name / Affiliation):

Christof Jonietz

Fraunhofer IOSB

Contributors authors:

Kai Nickel

Videmo

Mika Fischer

Videmo

Type of the publication:

If this is a deliverable

- *To which SP/WP/deliverable this publication is related to:* WP 5
- *Dissemination level:* PU

Else

- *Which conference?*
- *Where it will be published?*

Please fill in below:

This is: *pre-assessment* ☐ *final assessment* ☒ **X**

List the input material used in the publication/deliverable:

List the results developed and presented in the publication/deliverable:

This deliverable deals with designing the reference evaluation image and video sequence dataset for the face verification process. The actual data are acquired and secured. The acquisition justification is done by MobilePass Biometric Data Collection Consent Form. Each volunteer gave his consent by signature.



The draft publication

☐ is attached to this statement

X can be found in links:

https://portal.ait.ac.at/sites/MobilePass/WP_5_Cooperative_Face_Verification_Development

<https://owncloud02.iosb.fraunhofer.de/owncloud/>

This publication does not include any data or information that could be interpreted as security sensitive.

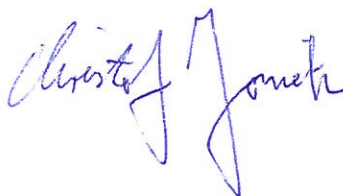
X True

☐ Not sure

If not sure, please specify what are the material / results that you are not sure if they are security sensitive? Why?

Date 28.04.2015

Signature of the Responsible Author:



Comments of the SSA Group

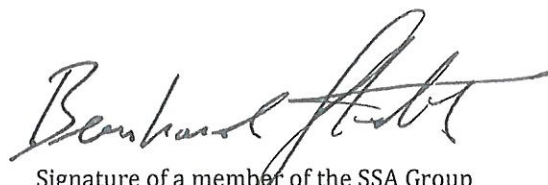
X The publication can be published as it is.

☐ Before publication the following modifications are needed:

-
-

Date: 28.04.2015

On behalf of the SSA Group: D.I. Bernhard Strobl



Signature of a member of the SSA Group



Report on Evaluation Dataset

Version 1.0, 27.04.2015

Project

Project Reference: Grant agreement no. 608016
Project Short Name: MobilePass
Call: FP7-SEC-2013-3-2-3
Funding Scheme: Capacity Project
Project web-site: www.mobilepass-project.eu



Deliverable D 5.1 Report on Evaluation Dataset

Document

Deliverable No.:	5.1	Due Date:	2015-04-30
Issued by Partner:	Fraunhofer, Videmo	Actual Date:	2015-04-27
WP/Task:	WP5/T5.1	Pages:	22
Confidentiality Status:	PU		

Authors

	Name	Organization/Unit
Main Author	Christof Jonietz	Fraunhofer IOSB
Contributing Author(s)	Kai Nickel	Videmo
	Mika Fischer	Videmo

Approval

	Name	Organization/Unit
Technical Reviewer	Bernhard Strobl	AIT
Language Reviewer	Chengchao Qu	Fraunhofer IOSB
Security Assessment		

Authorization

	Name	Organization/Unit
Project Officer	Andrei Lintu	European Commission

File MobilePass_Deliverable5.1_v1.0.doc

Document History

Document Information		Chapters affected	Description of change	Author	Document Status
Date	Version				
16.04.2015	0.1	all	Initial version	Jonietz	Open
22.04.2015	0.2	all	publicly available datasets, overall editing	Nickel, Fischer	Open
22.04.2015	0.99	all	Final changes	Jonietz	Final

Document Reviews

The following table gives an overview of all document reviews.

Date	Version reviewed	Remarks, Corrections	Reviewer	New status
24.04.2015	0.99	all	Bernhard Strobl	reviewed
27.04.2015	0.992	all	Chengchao Qu	language reviewed

Table of content

Table of content.....	3
List of figures	4
1. Introduction	5
2. MobilePass Evaluation Dataset for Face Verification.....	6
2.1. Consent Form for Data Protection and Privacy Issues	6
2.2. Biometric Images	7
2.3. Test Image-Sequences	8
2.4. MobilePass Face Dataset	11
3. Publicly Available Evaluation Datasets	12
3.1. NIST Facial Recognition Technology Database (FERET) Dataset	12
3.2. NIST Face Recognition Grand Challenge (FRGC) Dataset	12
3.3. NIST Multiple Biometric Grand Challenge (MBGC) Dataset	13
3.4. NIST Face and Ocular Challenge Series (FOCS) Dataset	14
3.5. Labeled Faces in the Wild (LFW) Dataset	15
3.6. YoutubeFaces (YTF) Dataset	16
4. Conclusions	18
A MobilePass Biometric Collection Consent Form	19
B References.....	22

List of figures

Figure 1: Examples of biometric images of the MPF dataset.....	8
Figure 2: IDS UI-3013XC sensor.....	9
Figure 3: Single image from scenario 1	9
Figure 4: Sample images from scenario 2.	10
Figure 5: Single images from a sequence of scenario 3.	10
Figure 6: Folder structure of the MobilePass face dataset.	11
Figure 5: Example images from the FERET database	12
Figure 6: Example images from the controlled scenario of the FRGC database.....	13
Figure 7: Example images from the uncontrolled scenario of the FRGC database.....	13
Figure 8: Example frames from the video challenge of the FRGC database	14
Figure 9: Example images from the GBU challenge of the FOCS dataset with a “good” pair on the left, a “bad” pair in the middle and an “ugly” pair on the right	15
Figure 10: Example images from the LFW database	16
Figure 11: Example frames from the YoutubeFaces database.....	17

1. Introduction

Convenient, fast and reliable capture of faces is one of the challenges in the MobilePass project for an optimized workflow in border control systems. This deliverable deals with designing the reference evaluation image and video sequence dataset for the face verification process. The recorded reference and other publicly available evaluation datasets are described. The purpose of this deliverable is to record test and evaluation datasets in order to results from state-of-the-art methods for face verification for later benchmarking.

The organization of this deliverable is as follows. In Section 2, the requirements of the evaluation dataset suitable for applications in the MobilePass system and the different scenarios of the measurement campaign are described. Section 3 lists a number of publicly available datasets that are additionally used for the evaluation of the face recognition performance. Conclusions are presented in Section 4.

2. MobilePass Evaluation Dataset for Face Verification

In this project, a camera system optimized for the workflow in border control situations will be designed and integrated in the system. The objective is to design and to develop a fast and dedicated device for mobile face verification.

Due to the mobility of the future device, face verification has to deal with challenges like blurring (either from motion or de-focusing) and non-uniformly illuminated images. Therefore, the solution will focus on multi-frame (video) processing for selecting these images out of the video-stream that fulfil a certain quality criterion. Based on automated quality estimation of the captured face images, the images with the best quality are chosen for face verification. The image verification process is based on matching the query images to a certain reference image (one-to-one comparison for each query image).

For performance testing of face verification of the future device, an appropriate data set is required. The image dataset should meet the following requirements:

1. Biometric face images must be acquired from each person. These images are considered as reference in face verification.
2. Image sequences (videos) must be recorded. In a pre-processing step, the quality of the images is determined. The images with highest quality are considered as query images for face verification.

This section describes data protection and privacy issues and the measurement campaign for capturing the biometric images and the image-sequences.

2.1. Consent Form for Data Protection and Privacy Issues

In this project scientific research on the acquisition and verification of biometric (fingerprint images, face images) and passport data is carried out. In the current project phase, MobilePass uses human volunteers to acquire datasets for developing, testing and evaluating sensor devices and algorithms for face verification. These volunteers will be recruited among employees and students of the MobilePass partners.

Compliance with EU rules on data protection and privacy issues is compulsory for FP7 research projects. In the deliverable 2.1 of MobilePass [1], data handling guidelines for research and testing activities in the research and development work packages have been formulated in order to fulfil the compliance with EU rules. When human subjects are involved as volunteers in MobilePass (e.g. as test persons providing biometrics) informed consent is required. In MobilePass, the informed consent procedure entails the recruitment of healthy adult participants who voluntarily participate in the research, and who, prior to participation, are informed about the goals, content, and procedures of the research and give their written approval.

Report on Evaluation Dataset

Version 1.0, 27.04.2015

Specific MobilePass recruitment principles (from [1]):

- Only healthy adult volunteers will be recruited among the personnel and/or students of the MobilePass project partners.
- Subjects unable or less able to give their free and informed consent will be excluded.
- Subjects will not be paid but only reimbursed for the time and expenses devoted to the participation in the research. Reimbursement will be such as to exclude any form of undue inducement.
- The researcher will explain orally the goals, content and procedures of the study, and the subject is required to read and sign an informed consent form in English and the applicable local language.

The sample informed consent form compliant with EC FP7 guidelines in [1] has been adopted for this measurement campaign, cf. Annex A. The signed informed consent form from each volunteer are archived at the Fraunhofer IOSB in Karlsruhe.

2.2. Biometric Images

The Part 5 of the ISO/IEC 19794-5 standard [3], which is mentioned in the International Civil Aviation Organization (ICAO) recommendations about the travel document, defined the standard formats for digital images of faces in order to guarantee the correct execution of operations of computer automated face verification (one-to-one matching). A summary of the specifications for capturing biometric images is given as follows:

1. Position of the subject and background: The subject shall not be too close nor too far from the camera: the distance between the eyes needs to be a little bit less than 1/4 of the width of the image. The face has to be centered both vertically and horizontally. The background has to be uniform.
2. Pose: The person shall be shown facing square to the camera, not looking over one shoulder (portrait style). The head should be upright so that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the picture.
3. Quality of the photograph: The portrait shall be in sharp focus from nose to ears, of high quality with no creases or ink marks. If in color, it should show skin tones naturally.
4. Colors and lighting: The portrait shall be color neutral showing the person with eyes open and clearly visible. The ISO standard does not allow digital alteration of the image to correct the dynamic range or the colours.

Report on Evaluation Dataset

Version 1.0, 27.04.2015

5. Hair style and expression: No hair shall obscure big areas of the face or the eyes. The person shall be looking at the camera with a neutral expression and the mouth closed. A smile with closed mouth is permitted.
6. Lighting of the applicant and background: The lighting shall be uniform with no shadows and no reflections on the face, no red eyes and the background shall not present any remarkable shadow.
7. Eye glasses: The portrait shall show the eyes with no light reflection off the glasses and no tinted lenses. If possible, avoid heavy frames. The frames shall not cover any part of the eyes.

The reference images are captured with a Fuji X-E1 camera with a resolution of 16 Megapixel. From this, biometric images are extracted based on the requirements stated above with resolutions of 300 dpi and 1200 dpi that yield mean inter-eye-distances of 125 Pixel and 510 Pixel, respectively. In Figure 1, 4 examples of biometric images from the MPF database are depicted. These reference images are considered as the “true” data in the face verification process, whereas the test images are considered as query.



Figure 1: Examples of biometric images of the MPF dataset.

2.3. Test Image-Sequences

For capturing the image sequences, the UI-3013XC from IDS is used [2], cf. Figure 2. The UI-3013XC with 13 megapixel CMOS sensor and autofocus camera module by Sony delivers with its 13 MP resolution images of size 4192 x 3104 pixel with frame rates of 30 fps in Full HD video mode (1920 x 1080 pixel).



Figure 2: IDS UI-3013XC sensor.

The scenarios 1-3 for capturing image sequences are further described in the following. The scenarios have been chosen corresponding to possible future scenarios of the border control process.

Scenario 1:

Scenario 1 is taken inside a building with uniform background and indirect illumination to the front of the face. Figure 3 shows one sample image from the image sequence of one person.



Figure 3: Single image from scenario 1

Scenario 2:

Scenario 2 represents a more challenging scenario inside a building nearby a window with direct sunlight from outside. In order to capture the illumination from different angles, the image sequence is recorded in a 180°-scan of the frontal view of the person's face. The image sequence contains images with faces illuminated from different directions (from the left half of the face, backlight and the right half of the face). In Figure 4, the face in the left and right image is illuminated from direct sun light from the left and the right, respectively.

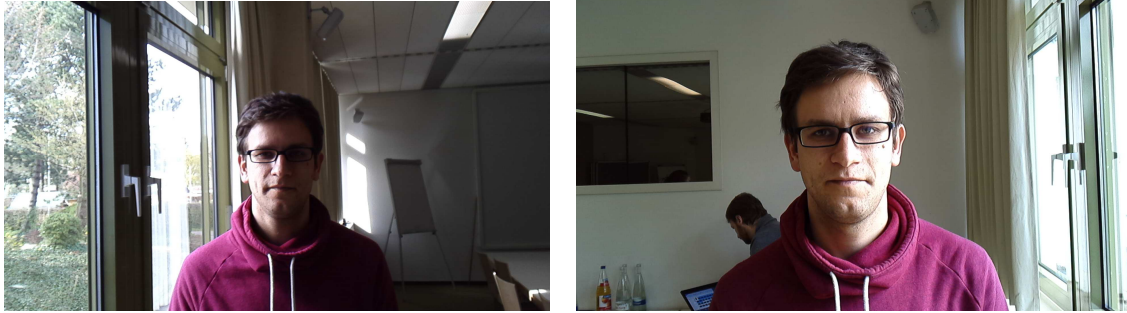


Figure 4: Sample images from scenario 2.

Scenario 3:

Scenario 3 is an outdoor scenario with relatively strong illumination from direct sunlight. In order to capture the illumination from different angles, the image sequence is captured in a 360°-scan of the frontal view of the person's face. Figure 5 shows sample images, where the face is illuminated from direct sunlight and different directions (top-left image: illumination of the left side, top-right image: illumination of the back side, bottom-left image: illumination of the right side, bottom-right image: illumination of the front side).



Figure 5: Single images from a sequence of scenario 3.

Report on Evaluation Dataset

Version 1.0, 27.04.2015

2.4. MobilePass Face Dataset

The new database MobilePass Faces (MPF) is a realistic and challenging database intended for testing face verification of the future mobile device. The MPF database includes 31 subjects. Each subject was asked to capture a single face image and record face image-sequences in 3 different scenarios.

The image data in the MobilePass face dataset is organized as depicted in Figure 6. There, the folder structure of the dataset is given.

```

MobilePass_Face_Dataset
    +-- Id_1001
        +-- scene_1
        +-- scene_2
        +-- scene_3
    +...
    +-- Id_1031
        +-- scene_1
        +-- scene_2
        +-- scene_3
    +-- ReferenceImages_300dpi_35x45mm
    +-- ReferenceImages_1200dpi_35x45mm
  
```

Figure 6: Folder structure of the MobilePass face dataset.

The test dataset is organized as follows: For each person a unique identifier number, “Id_1001” ... “Id_1031”, is assigned in order to make the subject anonymous. The test data of scene 1-3 is stored within the respective folder, “scene_1”, “scene_2”, “scene_3”.

The reference dataset is organized as follows: The reference image from each person with 300 dpi and 1200 dpi are contained in folder “ReferenceImages_300dpi_35x45mm” and “ReferenceImages_1200dpi_35x45mm”, respectively.

3. Publicly Available Evaluation Datasets

The MobilePass Faces database described above is very important, because it attempts to replicate the conditions that can be expected in the final MobilePass system as closely as possible by using the same image sensor, recreating realistic recording environments, and providing video data instead of only still images.

In addition to the MobilePass Faces database, we will exploit a number of publicly available datasets in order to achieve a quantitatively sound assessment of the face verification performance. Benefits from using this additional data are the larger number of individuals in those datasets, as well as the larger time gap between the recording of the reference image and the recording of the query images.

Unfortunately, a dataset that covers the MobilePass use-case exactly does not exist. Therefore, we selected multiple databases, each of which covers an important aspect of the data to be expected in the MobilePass project. In the following, these databases are briefly introduced.

3.1. NIST Facial Recognition Technology Database (FERET) Dataset

Created by the National Institute of Standards and Technology (NIST), the FERET database [4] was one of the first large face databases and was used in one of the first large-scale comparative evaluations of state-of-the-art face recognition algorithms.

It contains high-resolution studio images of over 1,000 persons in different poses, with different facial expressions and with a significant time gap between recordings of up to three years. Because of the large time gap it is useful for performance evaluation in the MobilePass project.



Figure 7: Example images from the FERET database

3.2. NIST Face Recognition Grand Challenge (FRGC) Dataset

Another large evaluation corpus created at NIST, the Face Recognition Grand Challenge database [5] contains high-resolution images and 3D scans of about 500 persons. The database also features a

Report on Evaluation Dataset

Version 1.0, 27.04.2015

significant time gap between recordings and in addition contains images recorded under uncontrolled environmental conditions, such as in hallways or outdoors.



Figure 8: Example images from the controlled scenario of the FRGC database



Figure 9: Example images from the uncontrolled scenario of the FRGC database

3.3. NIST Multiple Biometric Grand Challenge (MBGC) Dataset

The Multiple Biometric Grand Challenge [6] was the first large-scale NIST evaluation on face recognition featuring video instead of only still images. In addition to a still image challenge featuring high-resolution still images, NIST introduced the portal challenge, where subjects are recorded while they pass through a portal and must be matched to a still image, as well as the video challenge, where people are walking towards the camera or performing a number of activities. While the videos are not a good match to the MobilePass scenario, the database is still one of the only ones with high resolution still image and video data.

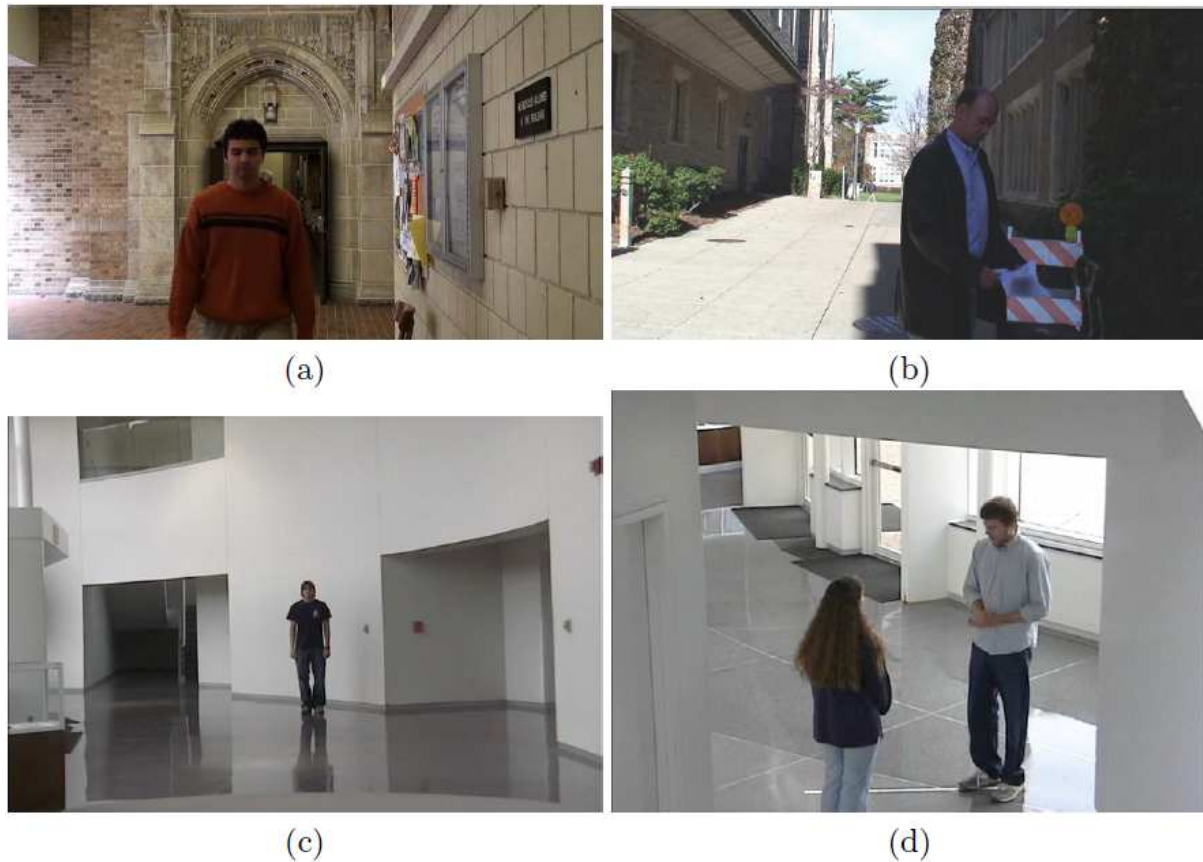


Figure 10: Example frames from the video challenge of the FRGC database

3.4. NIST Face and Ocular Challenge Series (FOCS) Dataset

In order to further drive research on face recognition algorithms to improve on challenging images, NIST created the "The Good, the bad & the ugly face recognition challenge" (GBU) [7]. There, they separated the face pairs according to the difficulty of achieving a correct face recognition result. While it contains only still images, it is very useful in order to assess algorithm performance at different levels of difficulty.



Figure 11: Example images from the GBU challenge of the FOCS dataset with a “good” pair on the left, a “bad” pair in the middle and an “ugly” pair on the right

3.5. Labeled Faces in the Wild (LFW) Dataset

The Labeled Faces in the Wild dataset [8] contains over 13,000 images of about 5,700 people taken from news photographs. The contained images are largely unconstrained and feature a very wide range of environmental conditions, making it a very challenging dataset. It is useful to assess an algorithm's robustness against uncontrolled environmental conditions.



Figure 12: Example images from the LFW database

3.6. YoutubeFaces (YTF) Dataset

The YoutubeFaces database [9] was modeled after the LFW database, just using videos downloaded from Youtube, instead of still images. It contains over 3,000 video clips of about 1,600 subjects. The conditions are again unconstrained, making it an equally challenging dataset. It is useful to assess the algorithm's ability to exploit the additional information contained in the videos as compared to still images.



Figure 13: Example frames from the YoutubeFaces database

4. Conclusions

This report describes the image and video dataset for face verification of the future device. The new MobilePass faces (MPF) dataset comprises biometric images as a reference and image sequences (videos) as a query for the face verification process. Images from 31 persons have been acquired in 3 different challenging scenarios. The scenarios have been chosen corresponding to possible future scenarios of the border control process. The first scenario takes into account only a uniform background and more or less uniformly illuminated faces inside a building. In the second scenario, direct sunlight from different directions within a building next to a window has been taken into account. In the third scenario, direct sunlight from different directions outside a building is considered.

A number of publicly available datasets from the face-recognition community were selected as additional evaluation material. In this way we are able to conduct a face-recognition evaluation that is on the one hand precisely targeted to the scenario definition of MobilePass, and on the other hand provides a quantitatively sound assessment of face verification performance.

A MobilePass Biometric Collection Consent Form

Purpose

The Fraunhofer IOSB is carrying out scientific research on the acquisition and verification of biometric (fingerprint images, face images) and passport data. The overall goal of the study is to develop a handheld biometric device that allows European border control authorities to check travellers in a comfortable, fast, and secure way. The study is part of a larger European research project called MobilePass (full title: A secure, modular and distributed mobile border control solution for European land border crossing points), funded by the European Commission within the scope of the 7th Framework Programme (GA no: 608016). In the current project phase, MobilePass uses human volunteers to acquire datasets for developing, testing and evaluating sensor devices and algorithms for fingerprint and face recognition. In addition, real passports may be used for developing and testing the passport reader and for testing biometric verification.

Procedure

In order to provide training and experimental data necessary to the theoretical and practical research and development activities required by the MobilePass project, a number of physical features will be recorded under different ambient conditions.

In these sessions we are going to collect the following personal characteristics:

1. single photo of the face
2. video sequences in three different scenarios of the face

Additional personal data (name, age, gender, etc.) is not recorded.

Each session will last approximately 15 minutes and individuals may discontinue their participation at any time for any reason without any need to give an explanation for their wish to stop their participation.

Data protection, confidentiality and privacy

All personal data stored during the study will be completely and irreversibly anonymised (unless this refutes the purpose of the study), or be erased on completion of the MobilePass Project. No personal data will ever be used for any purposes other than those stated in this form. Your personal data will not be transferred to any third party or be commercialised. When your data is stored it will be encrypted and access to the data storage is restricted by password protection. Your personal data may be used by MobilePass project partners located in different European countries. Only staff who are assigned to the relevant WPs in MobilePass have access to the data and transfer of personal data between MobilePass partners will be secured.

Report on Evaluation Dataset

Version 1.0, 27.04.2015

The investigator will record the data collected in a file. This file will be identified only by a random user identifier. Your biometric data will be stored separately from other identifying information (such as your name or ID number). The link associating the random user identifier with you is stored separately and securely.

The results of the study may be published in scientific books or journals or may be used for didactic purposes. However, no identifying information about you (name, facial photograph) will ever be revealed in any document, publication or teaching materials.

You may exercise your rights of access, rectification and deletion of data at any time. In order to do so, you will need to communicate your wish to do so to Eduardo Monari by email to the following address eduardo.monari@iosb.fraunhofer.de

Right to get more information about the study

You can ask any questions about the study at any time throughout the recording period. The investigator will be available to answer to your questions or concerns about the study. You will be informed of any new discovery that could occur throughout the study and that may affect your participation in future studies. If during the study and thereafter you wish to discuss your rights as a person who participates in an investigation, your participation in the study or your concerns about it, or if you do not want to continue in that investigation or future research, please contact Eduardo Monari any time you wish.

Refusal or cessation of participation

Your participation in this study is voluntary. You do not have to participate in the study if you do not want to do so. If you choose to participate, you can change your mind or leave the study at any time without having to give explanations and without being affected in any way by this decision. Similarly, at the discretion of the investigator, you may be withdrawn from the study for any of the following reasons: (a) if the minimum requirements of the study are not met (b) if for any reason the study is interrupted.

Risks and discomforts

The personal risk by participating in this study does not exceed the risks of daily and normal life. None of the procedures represent a danger to your health or to physical and mental integrity.

Financial Compensation

You understand that there is no financial compensation for participating in this study, but you may be reimbursed for the working hours lost due to participation, or other costs incurred because of your participation (e.g. travel costs).

Report on Evaluation Dataset

Version 1.0, 27.04.2015

Consent

By signing the present form, I, the undersigned, understand and consent freely that my personal data, including biometric data, my name and contact details, will be collected and processed by Fraunhofer IOSB, the data controller, and by appointed processors on behalf of the data controller, in accordance with applicable laws and with what is stated in the present clause. I have been informed about the study carried out within the scope of the MobilePass project and its purposes have been explained to me.

I understand that my personal data will be encoded in order to safeguard confidentiality, and that if results of the study are published, my identity will not be revealed. I also understand that I have the right to request access to my personal data, to correct, if applicable, and delete my personal data in conformity with the applicable legislation. For these purposes, I can contact Eduardo Monari.

I have read the above and I understand that I can refuse to participate in this study without any direct or indirect negative consequence on my life.

By signing the present form, I agree with the above.

[the volunteer]

Date: _____ Place:

Name:

Signature:

Email:

Telephone:

The undersigned responsible declares to have explained the purpose of the investigation, the procedures used in the study, and any potential risks and inconvenience that are likely to arise from participation. They have responded to the best of their abilities to the questions asked with respect to the study.

[the investigator]

Date: _____ Place:

Name:

Signature:

B References

- [1] Sanneke Kloppenburg, Irma van der Ploeg, „Data handling guidelines”, MobilePass Deliverable 1.2, Grant agreement no. 608016
- [2] Datasheet IDS UI-3013XC, https://en.ids-imaging.com/IDS/datasheet_pdf.php?sku=AB00582
- [3] ISO/IEC 19794-5 standard
- [4] Phillips, P. J., Wechsler, H., Huang, J., & Raussa, P. J. (1998). The FERET database and evaluation procedure for face-recognition algorithms. *Image and Vision Computing*, 16(5), 295–306. doi:10.1016/S0262-8856(97)00070-X
- [5] Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., ... Worek, W. (2005). Overview of the Face Recognition Grand Challenge. In *Proc. IEEE Conf. on Computer Vision and Pattern Recognition* (pp. 947–954). San Diego, USA: IEEE. doi:10.1109/CVPR.2005.268
- [6] Phillips, P. J., Flynn, P. J., Beveridge, J. R., Scruggs, W. T., O’Toole, A. J., Bolme, D., ... Weimer, S. (2009). Overview of the Multiple Biometrics Grand Challenge. In *Proc. Intl. Joint Conf. on Biometrics* (pp. 705–714). Alghero, Italy. doi:10.1007/978-3-642-01793-3_72
- [7] Phillips, P. J., Beveridge, J. R., Draper, B. A., Givens, G., O’Toole, A. J., Bolme, D. S., ... Weimer, S. (2011). An Introduction to the Good, the Bad, & the Ugly Face Recognition Challenge Problem. In *Proc. IEEE Intl. Conf. on Automatic Face and Gesture Recognition*. Santa Barbara, USA.
- [8] Huang, G. B., Ramesh, M., Berg, T., & Learned-miller, E. (2007). Labeled Faces in the Wild : A Database for Studying Face Recognition in Unconstrained Environments. Amherst.
- [9] Wolf, L., Hassner, T., & Maoz, I. (2011). Face Recognition in Unconstrained Videos with Matched Background Similarity. In *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*.