



**THE HIGH-QUALITY WIDE MULTI-CHANNEL  
ATTACK (HQ-WMCA) DATABASE**

Zohreh Mostaani<sup>a</sup>      Anjith George<sup>b</sup>  
Guillaume Heusch      David Geissenbuhler<sup>a</sup>  
Sébastien Marcel

Idiap-RR-22-2020

SEPTEMBER 2020

---

<sup>a</sup>Idiap Research institute

<sup>b</sup>Idiap Research Institute



---

# The High-Quality Wide Multi-Channel Attack (HQ-WMCA) database

---

Zohreh Mostaani, Anjith George, Guillaume Heusch, David Geissbühler,  
and Sébastien Marcel, *Senior Member, IEEE*\*

## Abstract

The High-Quality Wide Multi-Channel Attack database (HQ-WMCA) database extends the previous Wide Multi-Channel Attack database (WMCA) [1], with more channels including color, depth, thermal, infrared (spectra), and short-wave infrared (spectra), and also a wide variety of attacks.

## 1 Introduction

Though face recognition systems are achieving near-perfect accuracies, face recognition systems remain vulnerable to presentation attacks. Several different methods have been proposed to overcome this vulnerability [2, 3]. Metrics for evaluating the methods are also standardized [4, 5]. Recent research has highlighted the importance of multi-channel information for robust face presentation attack detection [1, 6, 7, 8]. However, there is a wide range of channels available to PAD. To advance the research in multi-channel PAD, we make available the HQ-WMCA large multi-channel dataset covering a wide range of 2D, 3D, and partial attacks.

## 2 High-Quality Wide Multi-Channel Attack (HQ-WMCA) database

The High-Quality Wide Multi-Channel Attack (HQ-WMCA) database [9] consists of 2904 short multi-modal video recordings of both bona-fide and presentation attacks. There are 555 bonafide presentations from 51 participants and the remaining 2349 are presentation attacks. The data is recorded from several channels including color, depth, thermal, infrared (spectra), and short-wave infrared (spectra).

Preprocessed images for some of the channels are also provided for part of the data used in the publication.

The HQ-WMCA database is produced at Idiap within the framework of "IARPA BATL" project [10] and it is intended for research, development, and testing in biometrics and biomedical analysis.

---

\*Zohreh Mostaani, Anjith George, Guillaume Heusch, David Geissbühler, and Sébastien Marcel are with the Idiap Research Institute, Switzerland, e-mails: {zohreh.mostaani, anjith.george, guillaume.heusch, david.geissbuhler, sebastien.marcel}@idiap.ch

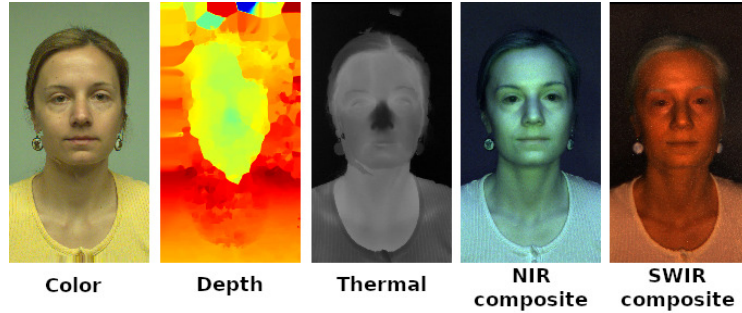


Figure 1: Sample images of bonafide from the database for different channels. From left to right the images are from color, depth, thermal, NIR, and SWIR channels. NIR composite and SWIR composite are obtained by combining a subset of the images from the corresponding spectra.

If you use this database, please cite the following publication [9].

### 3 Database Description:

The HQ-WMCA includes short video recordings from different channels including color, depth, thermal, near infra-red (NIR) and short wave infra-red (SWIR).

The sensors used for the data acquisition are:

- Basler acA1920-150uc: This sensor records the data for color channel.
- Basler acA1920-150um: This sensor records the data for NIR channel. Two identical sensors were mounted on the left and right of the system to capture data for stereo reconstruction purpose. These sensors are horizontally aligned and the distance between their centers is approximately 15 cm.
- Xenics Bobcat-640-GigE: This sensor records the data for SWIR channel.
- Xenics Gobi-640-GigE: This sensor records data from thermal channel.
- Intel Realsense D415: This sensor can records data from color, depth and infrared channels, however only the data from depth channel has been recorded.

Information about each sensor is described in Table. 1

Table 1: Sensor description for HQ-WMCA data

Sensor name	Channel	Resolution	Frame rate (fps)
Basler acA1920-150uc	Color	1920×1200	30
Basler acA1920-150um	NIR	1920×1200	90
Xenics Bobcat-640-GigE	SWIR	640×512	90
Xenics Gobi-640-GigE	Thermal	640×480	30
Intel Realsense D415	Depth	720×280	30

Four LED modules are used for illumination besides the ambient illumination available in the room. Each LED module consists of LEDs operating in different wavelength mostly in NIR and SWIR. The used frequencies are 735, 850, 940, 1050, 1200, 1300, 1450, 1550, and 1650 nm. The NIR and SWIR camera captures data at the same time as a corresponding wavelength LED is illuminating. Therefore there are multiple streams of data corresponding to different illumination wavelength at the end of data acquisition for NIR and SWIR cameras. The data from cases when there is no LED illumination is captured. For stereo reconstruction from two NIR cameras separate data streams were recorded. An LED with wavelength of 735 nm is used for illumination in this case. It is showed in the cycle as stereo. The data from the other channels (color, depth, and thermal) is captured regardless of LED illumination and for whole duration of the data collection.

The data is collected during 2 seconds which is equal to 20 cycles of LED illumination. Each illumination cycle lasts for 100 ms. The trigger sequence for different cameras with respect to one LED cycle is showed in the Table. 2.

In the table where there is "T" it means that the corresponding camera is triggered and the the data is captured in that time slot. The table only shows one cycle of illumination. This cycle repeats for 20 times and at the end there are different number of frames captured for each camera and each wavelength. It should be mentioned that all the sensors capture data synchronously except for "Intel Realsense D415". It was not possible for "Intel Realsense D415" to be triggered using the controller similar to other sensors. This sensor captures data for slightly more than the duration of the data capture to make sure that there is frames available when other sensors are triggered, and therefore the number of frames captured is more than others. The total number of frames acquired is described in the Table. 3.

All the sensors are mounted and fixed on a tripod according to the TREX design from TOR labs. The cameras are placed at a distance between 50-60cm from the subject face. The distance is shown on the data capture GUI.

Each subject is given an ID number upon arriving. This ID number is used during all the data capture, including bonafide and presentation attacks if necessary. This number is referred to as "client\_id" in case of bonafide and "presenter\_id" in case the subject is presenting an attack to the system.

In order to have more variability in the dataset the data acquisition is performed during three sessions. The sessions are different based on their illumination. The background in all the sessions is simple white.

- **session 1:** Ambient office light illumination. There is no SWIR wavelength in the ambient illumination.
- **session 2:** Ambient office light illumination and a halogen lamp that is switched on far away from the cameras. This halogen lamp produces SWIR wavelength that illuminates the subject indirectly.
- **session 3:** There is no ambient office light illumination and two LED spot lights are illuminating from left and right. There is no SWIR wavelength in the spot lights.

The data includes bonafide and presentation attacks performed by the subjects participated in the data collection as well as the presentation attacks on the stand. Since the duration of the data collection was only 2 seconds, data was mostly captured twice from each presentations to include more samples. The file names for the two presentations are the same except for an 8 digit random sequence of numbers and characters at the end of the file. This part of the file name is called "trial\_id".

## 4 Presentations:

### 4.1 Bonafide:

The bonafide data was captured from subjects while they were seated in front of the cameras with a neutral facial expression. The subjects were asked to remove their medical glasses if they wore one. The data from the subjects wearing the medical glasses was also captured.

### 4.2 Presentation Attacks:

The attacks for the BATL data acquisition is including ten categories of attacks and each of those categories may include sub-categories. This makes it easy to allocate the data properly to different subsets for training and testing models.

- **Glasses (type 01):** This type of attacks includes the following sub types.
  - **00:** Retro glasses
  - **01:** Funny eyes glasses
  - **02:** Paper glasses
- **Mannequin (type 02):** This type of attacks includes the following sub types.

- **00**: Not specific
- **Print (type 03)**: This type of attacks includes the following sub types.
  - **00**: Printed photo on Matte paper using Typical office laser printer (CX c224e).
  - **01**: Printed photo on Glossy paper using Typical office laser printer (CX c224e).
  - **02**: Printed photo on Matte paper using Professional quality printer (Epson\_XP-860\_series instead of Canon 6010).
  - **03**: Printed photo on Glossy paper using Professional quality printer (Epson\_XP-860\_series instead of Canon 6010).
- **Replay (type 04)**: This type of attacks includes the following sub types.
  - **00**: Video while played.
  - **01**: Video while paused.
  - **02**: Digital photo presented on an electronic display.
- **Rigid mask (type 05)**: This type of attacks includes the following sub types.
  - **00**: Non-transparent plastic mask.
  - **01**: Transparent plastic mask without makeup.
  - **02**: Transparent plastic mask with makeup.
  - **03**: That’sMyFace resin mask.
- **Flexible mask (type 06)**: This type of attacks includes the following sub types.
  - **00**: Full face silicon mask
  - **01**: Half face silicon mask
- **Paper mask (type 07)**: This type of attacks includes the following sub types.
  - **00**: Not specific
- **Wigs (type 08)**: This type of attacks includes the following sub types.
  - **00**: Not specific
- **Tattoo (type 09)**: This type of attacks includes the following sub types.
  - **00**: Maori tribal face tattoo
- **Makeup (type 10)**: This type of attacks includes the following sub types.
  - **00**: Heavy contour makeup level 0.
  - **01**: Heavy contour makeup level 1.
  - **02**: Heavy contour makeup level 2.
  - **03**: Pattern makeup level 0.
  - **04**: Pattern makeup level 1.
  - **05**: Pattern makeup level 2.
  - **06**: Transformation makeup.
  - **07**: Beauty makeup level 0.
  - **08**: Beauty makeup level 1.
  - **09**: Beauty makeup level 2.

Examples of attacks from each category and for different sub-categories of makeup is shown in Fig. 2 and Fig. 3 respectively.

Each group has a “type\_id” and each sub group has a “sub\_type\_id”. The presentation attack instruments (PAI) included in each sub group has a unique “pai\_id” as well as a “client\_id” which may not be unique. More detailed information about these numbers will be presented in the following.

## 5 File Naming Convention:

The file names in the database encode some information about the type of data they contain, for example bonafide or presentation attacks. Each saved file has the following name format:

`<site_id>_<session_id>_<client_id>_<presenter_id>_<type_id>_<sub_type_id>_<pai_id>.hdf5`

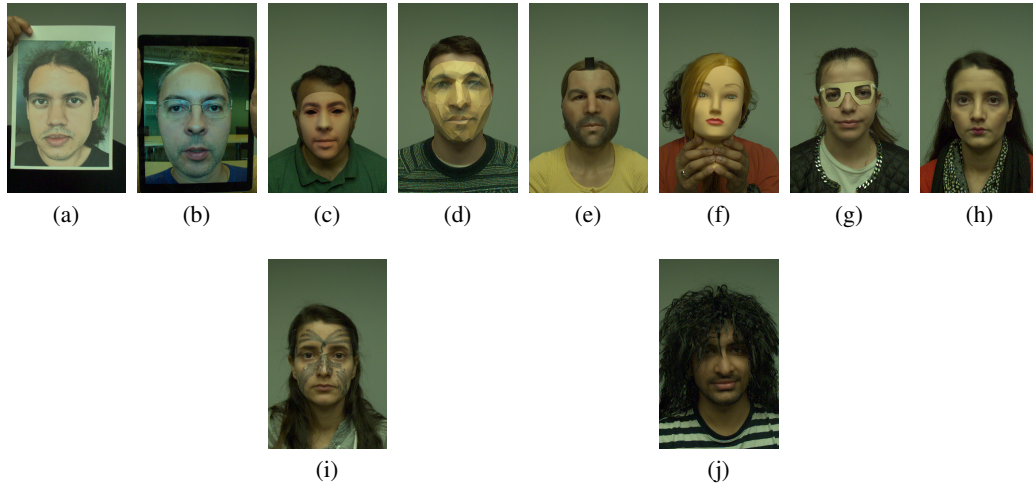


Figure 2: Example of attacks present in the database. (a) Print, (b) Replay, (c) Rigid mask, (d) Paper mask, (e) Flexible mask, (f) Mannequin, (g) Glasses, (h) Makeup, (i) Tattoo and (j) Wig. Note that only one particular example for each category is shown here, but there exists more variation across the database. For instance, print attacks have been crafted using different printers and different papers.

- **site\_id**: The number represents the place of the data collection. In this database this number is always '1'.
- **session\_id**: The number associated to a session as mentioned before.
- **client\_id**: This number presents the identity of what is presented to the system. For bonafide, it is the ID given to the participant upon arrival and for the attacks, it is a number given to a PAI in this protocol. Please note that if the identity of a subject is the same as the identity of an attack this number is the same for both cases. One example is the silicon masks. If a silicon mask is made from subject 'x' and subject 'x' also participated as bonafide in the data collection the "client\_id" for bonafide and silicon mask is the same.
- **presenter\_id**: If a subject is presenting an attack to the system, this number is the subject's "client\_id". If the attack is presented on a support, this number is '0000'. If the capture is for bonafide this number is '0000' as well since there is no presenter in this case.
- **type\_id**: The attack types mentioned in 4.2. For bonafide this number is '00'.
- **sub\_type\_id**: The sub\_types for each attack type mentioned in 4.2. For bonafide without glasses this number is '00' and if they wore medical glasses this number is '01'.
- **pai\_id**: The unique number associated with each and every PAI. This number for bonafide both with and without medical glasses is '000'.

Here are some examples for more clarification:

- 1\_01\_0035\_0000\_00\_00\_000 : This is the **bonafide** file of client number 35 in session number 1 when they did not wear medical glasses.
- 1\_01\_0005\_0000\_00\_01\_000 : This is the **bonafide** file of client number 5 in session number 1 when they did wear medical glasses.
- 1\_02\_0109\_0001\_06\_01\_016 : This is a **flexible mask** attack where the identity 109 is presented to the camera by client number 1 in session 2.
- 1\_03\_0018\_0000\_03\_02\_002 : This is a **photo** attack with sub\_type two (Printed photo on Matte paper using Professional quality printer) where the identity 18 is presented to the camera using stand in session 03.

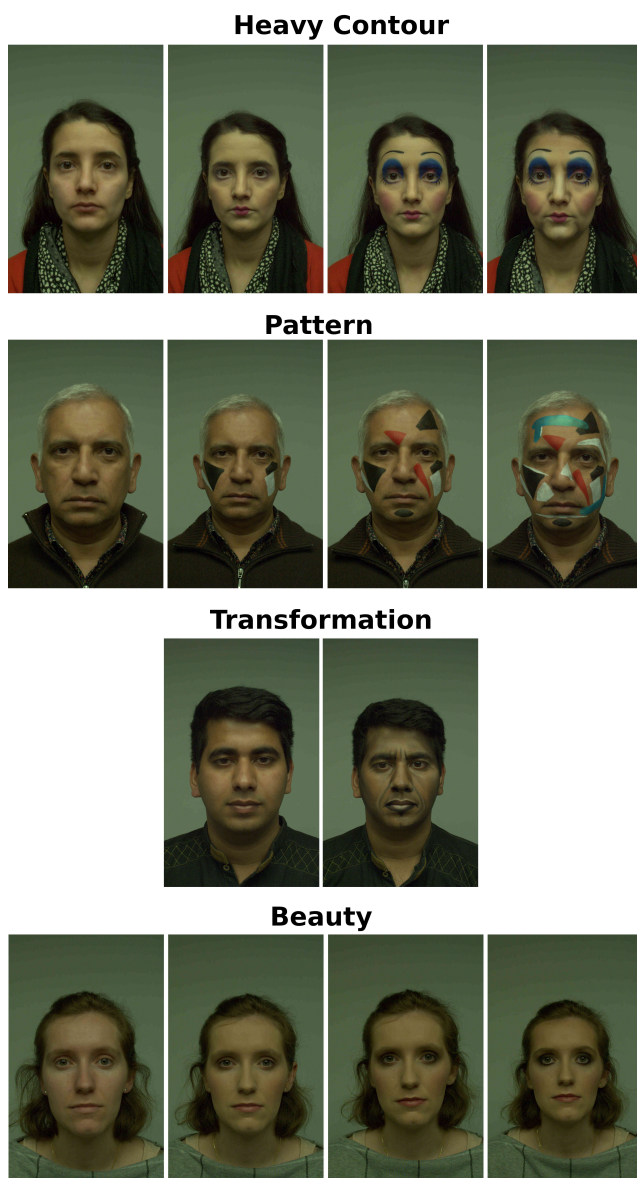


Figure 3: Sample images of makeup attacks for different sub-categories and levels. The images from top to bottom belongs to Heavy contour, Pattern, Transformation, and Beauty makeup. In each row the first image on the left is bonafide and from left to right the level of the makeup increases.

## 6 Evaluation:

The SWIR spectra is mainly used in the reference publication. Since the consecutive frames are correlated, only 10 frames from each video were selected. The frames are uniformly sampled in the temporal domain. The total number of 2904 presentations including bonafide and presentation attacks were grouped into three subsets, train, dev, and eval. The data split is done ensuring almost equal distribution of PA categories and disjoint set of client identifiers in each set. Each of the PAIs had different client id. The split is done in such a way that a specific PA instrument will appear in only one set. A low level database interface is implemented that handles loading and spatial and temporal alignment of the data <sup>2</sup>. The preprocessed method is described in details in the reference publication

<sup>2</sup><https://gitlab.idiap.ch/bob/bob.db.hqwmca>



[9] and the implementation is available publicly <sup>3</sup>. The number of presentations in train, dev, and eval subset for the protocols in the reference publication is mentioned in Table 5. Note that these are the numbers of the original videos fed to the pipeline, however the actual number of preprocessed images provided here are less than the numbers in the Table 5 due to failure of the face detection stage.

Examples of different channels present in the database are shown in Fig. 4. Please refer to the reference publication for more information.

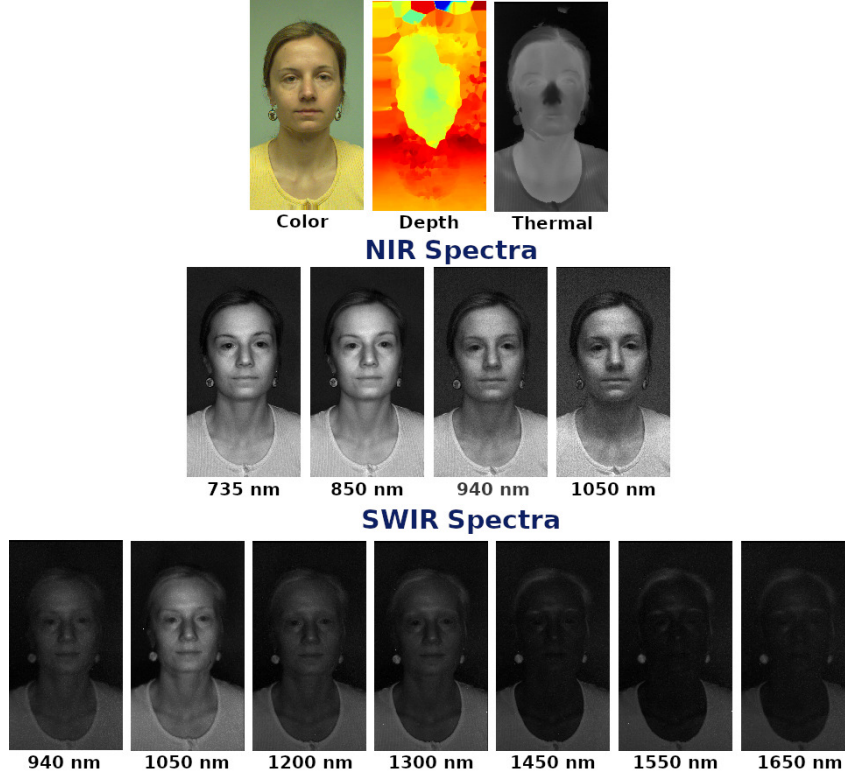


Figure 4: Different channels from the face images, first row shows the color, depth and thermal channels; second row shows the channel-wise normalized images from four NIR wavelengths, and the third row shows the channel-wise normalized images from different SWIR wavelengths.

## 7 Preprocessed files

Since the original database is large and cannot be downloaded directly, we provide preprocessed files to reproduce the paper. Specifically, we provide two sets of preprocessed files for the two CNN models used in the reference publication. The processed files are in folders *MCCNN-128* and *MC-PixBiS-224*. The difference between the two sets is in the size of image crop and the type of alignment. All the other steps are similar.

- *MCCNN-128*: This is the set of preprocessed files to use with the *MCCNN* models presented in the reference paper. The images are of size  $(128 \times 128)$  and the face crop is loose made suitable for the LightCNN model.
- *MC-PixBiS-224*: This is the set of preprocessed files to use with the *MC-PixBiS* models presented in the reference paper. The images are of size  $(224 \times 224)$  and the face crop is tight as shown in images below.

The preprocessing for the color channel is done in several steps. First a face detection is performed. Once the face bounding box is obtained, face landmark detection is performed in the detected face

<sup>3</sup>[https://gitlab.idiap.ch/bob/bob.paper.pad\\_mccnns\\_swirdiff](https://gitlab.idiap.ch/bob/bob.paper.pad_mccnns_swirdiff)

bounding box. Then the images are aligned by transforming them such that the eye centers and mouth center are aligned to predefined coordinates. The aligned face images are converted to grayscale, and resized, to the resolution of  $128 \times 128$  pixels. The preprocessing stage for non-RGB channels is done by reusing the facial landmarks detected in the color channel and then a similar alignment procedure is performed. The images are then normalized to convert the range of the non-RGB images to 8-bit format.

Instead of directly using images at different SWIR wavelengths, a normalized difference between these images has been considered. This normalization is independent of the absolute brightness and exhibits differences between skin and non-skin pixels. Consider two SWIR images of the same individual,  $I_{s_1}$  and  $I_{s_2}$ , recorded at (almost) the same time<sup>4</sup> but at different wavelengths, the normalized difference is given by:

$$d(I_{s_1}, I_{s_2}) = \frac{I_{s_1} - I_{s_2}}{I_{s_1} + I_{s_2} + \epsilon} \quad (1)$$

$\epsilon$  was set to  $1e^{-4}$ . Since our recording setup allows to capture SWIR data at no less than  $n = 7$  different wavelength in each recordings, the number of possible SWIR image differences is hence given by:

$$\frac{n!}{(n-2)!} = \frac{7!}{5!} = 6 \cdot 7 = 42 \quad (2)$$

The preprocessed files provided contains a total of 43 channels, i.e., one grayscale image and the 42 combinations of SWIR wavelengths. The details can be found from the paper package.

The preprocessed method is described in details in the reference publication and the implementation is available publicly<sup>5</sup>. The distribution of samples in each set and the details of the protocols can be found from the reference publication and the database package<sup>6</sup>.

---

<sup>4</sup>There is a lag of 11ms between frames recorded at different wavelength, resulting in a total lag of 77ms within the considered SWIR range.

<sup>5</sup>[https://gitlab.idiap.ch/bob/bob.paper.pad\\_mccnns\\_swirdiff](https://gitlab.idiap.ch/bob/bob.paper.pad_mccnns_swirdiff)

<sup>6</sup><https://gitlab.idiap.ch/bob/bob.db.hqwmca>

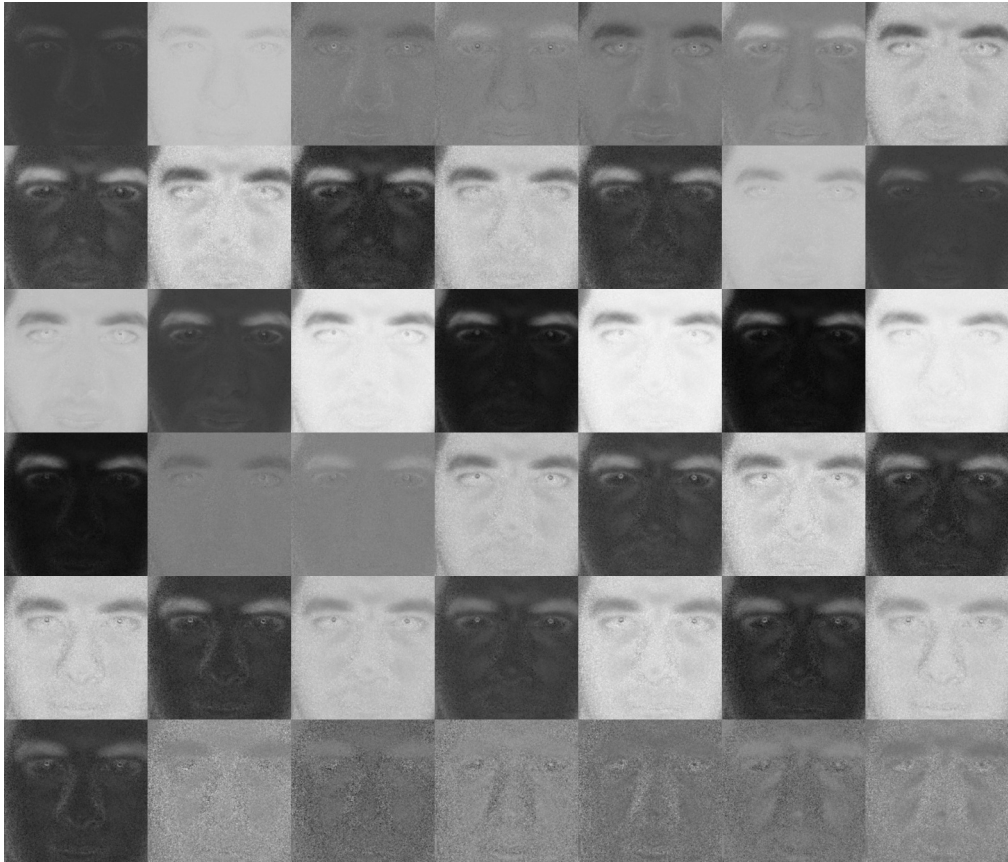


Figure 5: All 42 SWIR difference images at resolution  $224 \times 224$ , for the MC-PixBiS Model

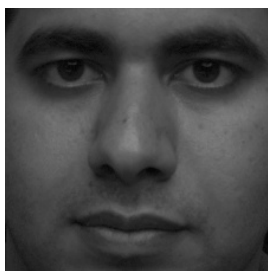


Figure 6: The grayscale image at resolution  $224 \times 224$ , for the MC-PixBiS Model

Table 2: LED cycle description for synchronized sensors

Sensor name	Slot-01	slot-02	slot-03	slot-04	slot-05	slot-06	slot-07	slot-08	slot-09	slot-10	slot-11	slot-12	slot-13	slot-14	slot-15	slot-16	slot-17	slot-18	slot-19	
Basler acA1920-150uc																				
Basler acA1920-150um																				
Xenics Bobcat-640-GigE																				
Xenics Gobi-640-GigE																				
LEDs SWIR	dark	940	1050	1050	1200	1300	1450	1550	1650	dark	dark	dark	dark	dark	dark	dark	dark	dark	dark	dark
LEDs NIR	ster	940	1050	1050	1200	1300	1450	1550	1650	ster	ster	ster	ster	ster	ster	ster	ster	ster	ster	ster
time [ms]	0	11	22	22	33	44	55	66	77	88	88	88	88	88	88	88	88	88	88	100

Table 3: Frame description for each data collection sample

Sensor	Channel	Wavelength (nm)	number of frames
Basler acA1920-150uc	Color	NA	60
Basler acA1920-150um	NIR	735	20
Basler acA1920-150um	NIR	850	20
Basler acA1920-150um	NIR	940	20
Basler acA1920-150um	NIR	1050	20
Basler acA1920-150um	NIR	dark	40
Basler acA1920-150um	NIR	stereo	60
Xenics Bobcat-640-GigE	SWIR	940	20
Xenics Bobcat-640-GigE	SWIR	1050	20
Xenics Bobcat-640-GigE	SWIR	1200	20
Xenics Bobcat-640-GigE	SWIR	1300	20
Xenics Bobcat-640-GigE	SWIR	1450	20
Xenics Bobcat-640-GigE	SWIR	1550	20
Xenics Bobcat-640-GigE	SWIR	1650	20
Xenics Bobcat-640-GigE	SWIR	dark	40
Xenics Gobi-640-GigE	Thermal	NA	60
Intel Realsense D415	Depth	NA	70

Table 4: Number of examples for bonafide and attack examples in each set. The number of different identities is given in parenthesis. Note that having different identities provides variability for bonafide examples.

	Train	Validation	Test
<i>Bonafide</i>	228 (21)	145 (14)	182 (16)
Attacks	742	823	784

Table 5: Distribution of attacks in the different sets, grandtest protocol is the superset of these two protocols

	Attack type	Train	Validation	Test
<b>Impersonation</b>	Print	48	98	0
	Replay	36	100	126
	Rigid Mask	162	118	140
	Paper Mask	28	24	49
	Flexible Mask	90	86	48
	Mannequin	20	38	77
	<i>Total</i>	<i>384</i>	<i>464</i>	<i>440</i>
<b>Obfuscation</b>	Glasses	56	38	36
	Makeup	264	271	258
	Tattoo	24	24	24
	Wig	14	26	26
	<i>Total</i>	<i>358</i>	<i>359</i>	<i>344</i>

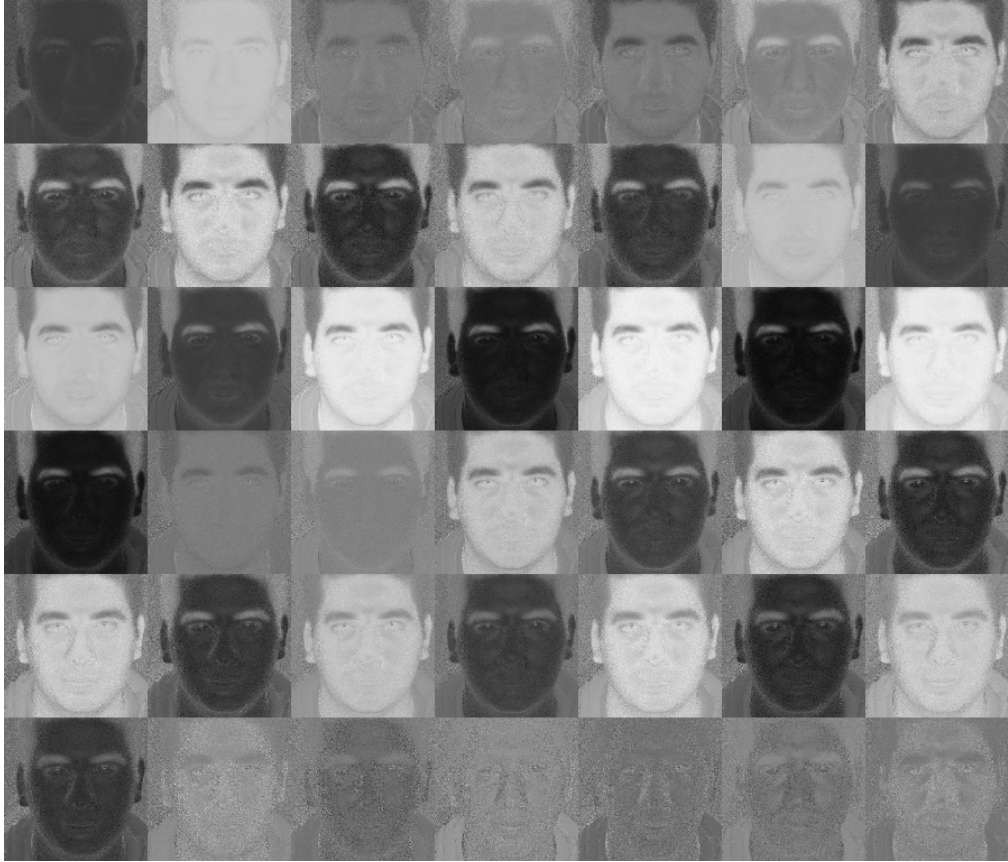


Figure 7: All 42 SWIR difference images at resolution  $128 \times 128$ , for the MC-CNN Model



Figure 8: The grayscale image at resolution  $128 \times 128$ , for the MC-CNN Model

## Acknowledgment

Part of this research is based upon work supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via IARPA R&D Contract No. 2017-17020200005. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.

## References

- [1] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, and S. Marcel, "Biometric face presentation attack detection with multi-channel convolutional neural network," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2019.
- [2] A. George and S. Marcel, "Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection," in *International Conference on Biometrics (ICB)*, 2019.
- [3] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of biometric anti-spoofing : Presentation attack detection*. Editors: Marcel, S., Nixon, M.S., Fierrez, J., Evans, N. (Eds.); Springer International Publishing, 2018, 2nd ed.; ISBN: 978-3319926261, 09 2018. [Online]. Available: <http://www.eurecom.fr/publication/5667>
- [4] ISO/IEC JTC 1/SC 37 Biometrics, "Information technology –International Organization for Standardization," International Organization for Standardization, ISO Standard, Feb. 2016.
- [5] "Information technology – Biometric presentation attack detection – Part 1: Framework." International Organization for Standardization, Standard, Jan. 2016.
- [6] A. George and S. Marcel, "Learning One Class Representations for Face Presentation Attack Detection using Multi-channel Convolutional Neural Networks," *IEEE Trans. on Information Forensics and Security*, 2020.
- [7] O. Nikisins, A. George, and S. Marcel, "Domain adaptation in multi-channel autoencoder based features for robust face anti-spoofing," in *International Conference on Biometrics (ICB)*, 2019.
- [8] A. George and S. Marcel, "Can your face detector do anti-spoofing? face presentation attack detection with a multi-channel face detector," *Idiap Research Report, Idiap-RR-12-2020*, 2020.
- [9] G. Heusch, A. George, D. Geissbühler, Z. Mostaani, and S. Marcel, "Deep models and shortwave infrared information to detect face presentation attacks," *IEEE Transactions on Biometrics, Behavior, and Identity Science (T-BIOM)*, 2020.
- [10] "IARPA ODIN," <https://www.iarpa.gov/index.php/research-programs/odin>, accessed: 2018-10-20.