Face presentation attack detection with passive imaging at 250 GHz

Marcin Ł. Kowalski[1]
[1]Institute of Optoelectronics, Military University of Technology, Gen. S. Kaliskiego 2, Warsaw, Poland

***Abstract*— Systems for detecting face presentation attacks are facing great challenges since new 3D facial masks are used. Passive terahertz imaging offer specific physical properties that may improve presentation attack detection capabilities. The aim of this paper is to present outcomes of study on using novel 3D facial masks for face presentation attack detection in passive imaging at 250 GHz. A thorough analysis of presentation attacks for facial recognition systems using custom 3D-printed and custom flexible 3D-latex masks is provided together with spectral characterization of various items. A set of experiments with various spoofing items is described and discussed. Finally, a presentation attack detection method with passive imaging at 250 GHz is presented.**

I. INTRODUCTION

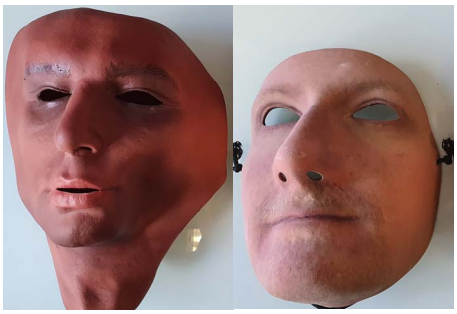
PRESENTATION attack detection (PAD) remains serious challenge for biometric recognition systems. Variety of attacks on different biometric modalities require new detection methods to be developed [1]. Presentation attack detection systems are expected to determine whether the current subject is genuine. Presentation attacks on face recognition systems are among the most popular and are presumably the easiest attacks to be done using a screen replay, a printed photo or three-dimensional models.

Terahertz radiation penetrates a variety of non-polar non-conducting materials and is inherently safe for living tissues and DNA, because it is not ionizing thanks to low photon energy. Due to high attenuation of water, penetration of living tissues is limited to a few millimeters at lower frequencies of the THz band. Imagers operating in passive mode register radiation emitted by objects do not require additional illuminators. This specific property of terahertz radiation may provide necessary material for detection of any instruments covering face.

The aim of this paper is to present the study on presentation attack detection in terahertz imaging domain. In the paper we consider various face presentation attacks, in the form of printed papers, or masks mounted on the human's face. A set of experiments with various instruments and various sets of clothing is described. In this paper an intensity analysis is shown as well as PAD method using deep learning algorithm.

II. EXPERIMENTS

For the purpose of the investigations the facial masks are considered a porous material, partly transmitting terahertz radiation. Depending on the structure, type of material, and thickness of a mask, terahertz radiation can be partly transmitted as through an optical filter. During this study, two types of masks for performing presentation attack have been considered. The main focus has been put on detecting facial 3D masks presenting realistic faces as they are the most difficult to detect by traditional face recognition systems. The presentation attack items investigated during the study contain a 3D full face flexible mask and printed 3D facial mask. Sample images of 3D facial masks are presented in Fig. 1. All the facial masks used during the study have been characterized in the range of 0.15 – 2 THz to estimate the transmissive capabilities of the materials. The characterization has been performed using TeraView TDS TPS 3000 spectrometer [2] operating in transmission mode. Mean values of transmission are provided in Table 1.



(a) **(b)**

Fig. 1. Images of sample (a) latex masks (a), and (b) 3D-printed masks.

Table 1 Mean transmission through facial masks at 250 GHz.

Masks	Transmittance value [%]
Full-face latex masks	47.88
3D-printed masks	22.87

Experiments with subjects in a stand-off position with different masks and sets of clothing have been performed. All the experiments have been made using a TS4 passive imager (Digital Barriers, ThruVision [3]) operating at 250 GHz. Sample terahertz image of subject wearing 3D facial mask is presented in Fig. 2. A database of images presenting genuine subjects and presentation attacks in variety of configurations has been acquired and characterized. The collected images have been used for numerical intensity analysis as well as for algorithm development and validation.

(a) **(b)**

Fig. 2. THz images presenting a subject wearing facial masks: (a) 3D printed – subject wearing a T-shirt, (b) full- face latex mask, subject wearing a T-shirt and a sweater.

III. PAD METHODS

The process of detection of face presentation attacks relies on the analysis of a two-dimensional distribution of the energies radiated by objects in the camera's lens field of view, as well as on the transmittance through spoofing items. Since both a human face and a mask are in a direct contact, the energy (heat) is transferred between the human face and the mask by transmission of heat between those two bodies.

As a results of image intensity analysis, intensity patterns have been recognized. Each mask, depending on material, thickness and transmission introduces some loss of energy radiated by subject's face. Moreover, the amount of energy radiated by masks changes during the experiment. It has been noticed that a full-face latex mask introduces a small change of intensity since the transmission through this type of presentation attack instruments (PAIs) is very high at 250 GHz. However, the mean normalized intensities are still higher than the pixel intensities of the bare face and the reference area. The difference between mean pixel intensities for 3D-printed masks and a reference is large. The 3D-printed masks are of a very low transmission, thus they block the radiation coming from a human's face.

a) Threshold-based method

For the numerical analysis, mean values of pixels from two regions of interests (ROIs) are compared. The first ROI is located in a head area and covers a square of 6 x 6 pixels while the second ROI covers an area of 40 x 60 pixels and corresponds with the torso.

The intensity analysis resulted with a threshold-based PAD method. The intensity threshold is calculated for distinguishing genuine subjects and imposters based on a difference between mean normalized intensities of two RoIs and a bare face. During validation, mean intensities for two RoIs have been calculated for each sample (image) and compared with the threshold.

Results are presented using two validation metrics, namely attack presentation classification error rate (APCER) and bona fide presentation classification error rate (BPCER). APCER corresponds to an attack presentations proportion using the same PAI species incorrectly classified as bona fide presentations in a specific scenario, while BPCER corresponds to a proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario. For the purpose of validation, thresholds have been calculated to achieve APCER of 1% based on 70% randomly selected samples of the whole dataset. The intensity based algorithm achieved BPCER of 14.22 % calculated for the given APCER = 1%. Results of unknown attack validation are provided in Table 2.

Table 2. Results of unknown attack validation for threshold-based PAD method.

PAI	All	
	APCER[1]	BPCER[1]
Latex mask	19.34±2.00	14.21±2.00
3D-printed mask	1.11±0.00	1.21±0.00

[1] All the numbers are given in [%].

As a second validation method, an unknown attack method have been used. During the unknown attack validation, the dataset has been divided based on known and unknown PAIs. In all the cross-material scenarios, thresholds have been calculated based on groups of PAIs not used for validation.

b) Deep learning method

The second PAD method proposed in this study is based on deep learning classification algorithm. Terahertz images extracted from original images were transferred to a deep neural network for presentation attack detection. For the automatic presentation attack detection ResNet-18 [4] has been selected. The algorithm has been trained with images presented genuine subjects and imposters. Two validation approaches have been applied. First, the classifier has been validated in a ten-fold cross-validation scheme and achieved APCER of 23.22 % with 11.83% of BPCER. Results of unknown attack validation for ResNet-18 are provided in Table 3.

Table 3. Results of unknown attack validation for deep learning PAD method.

PAI	All	
	APCER[1]	BPCER[1]
Latex mask	17.04	17.74
3D-printed mask	0.39	0.30

[1] All the numbers are given in [%].

It seems that attacks performed using latex masks are the most difficult to detect due to relatively high transmission of radiation at 250 GHz.

IV. SUMMARY

The study revealed that detection of face presentation attacks in passive terahertz imaging domain is possible. However, the presented methods do not achieve the state-of-the-art performance presented by some of the works in visible range and thermal infrared.

The validation with unknown attacks on deep learning models revealed that PAD performance is not uniform across all presentation attack instruments. Intensity analysis revealed that thermalization influences 3D printed and latex masks. Heating impact on PAD performance for attacks using 3D-printed and latex masks is low. Both classification errors for 3D printed masks and latex masks are constant at the beginning and end of the experiment, independent from the acquisition moment.

This paper presents initial study on PAD with passive terahertz imaging. Further works are needed to better understand how different PAIs change the terahertz image.

Funding: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833704 and from Military University of Technology, grant no. UGB/22-783/2020.

REFERENCES

[1]. R. Ramachandra; S. Venkatesh; K. B. Raja; S. Bhattacharjee; P. Wasnik; S. Marcel, C. Busch "Custom silicone Face Masks: Vulnerability of Commercial Face Recognition Systems & Presentation Attack Detection," 2019 7th International Workshop on Biometrics and Forensics (IWBF).
[2]. Teraview website, https://teraview.com/, accessed 10/08/2020.
[3]. ThruVision wersite: https://www.digitalbarriers.com/ accessed 10/08/2020.
[4]. 45. He, K., Zhang, X., Ren, S., Sun, J.: 'Deep residual learning for image recognition.', Proc. CVPR, Las Vegas, USA, June 2016.