

Received November 12, 2018, accepted December 16, 2018, date of publication January 3, 2019, date of current version January 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2888905

# Low-Cost and Efficient Hardware Solution for Presentation Attack Detection in Fingerprint Biometrics Using Special Lighting Microscopes

INES GOICOECHEA-TELLERIA<sup>1</sup>, KIYOSHI KIYOKAWA<sup>2</sup>,  
JUDITH LIU JIMENEZ<sup>1</sup>, AND RAUL SANCHEZ-REILLO<sup>1</sup>

<sup>1</sup>Electronic Technology Department, University Carlos III of Madrid, 28911 Leganés, Spain

<sup>2</sup>Nara Institute of Science and Technology, Ikoma 630-0192, Japan

Corresponding author: Ines Goicoechea-Telleria (igoicoec@ing.uc3m.es)

**ABSTRACT** Biometric recognition is already a big player in how we interact with our phones and access control systems. This is a result of its comfort of use, speed, and security. For the case of border control, it eases the task of person identification and black-list checking. Although the performance rates for verification and identification have dropped in the last decades, protection against vulnerabilities is still under heavy development. This paper will focus on the detection of presentation attacks in fingerprint biometrics, i.e., attacks that are performed at the sensor level, and from a hardware perspective. Most research on presentation attacks has been carried out on software techniques due to its lower price as, in general, hardware solutions require additional subsystems. For this paper, two low-cost handheld microscopes with special lighting conditions were used to capture real and fake fingerprints, obtaining a total of 7704 images from 17 subjects. After several analyses of wavelengths and classification, it was concluded that only one of the wavelengths is already enough to obtain a very low error rate compared with other solutions: an attack presentation classification error rate of 1.78% and a bona fide presentation classification error rate (BPCER) of 1.33%, even including non-conformant fingerprints in the database. On a specific wavelength, a BPCER of 0% was achieved (having 1926 samples). Thus, the solution can be low cost and efficient. The evaluation and reporting were done following ISO/IEC 30107-3.

**INDEX TERMS** Biometrics, fingerprint biometrics, presentation attack detection.

## I. INTRODUCTION

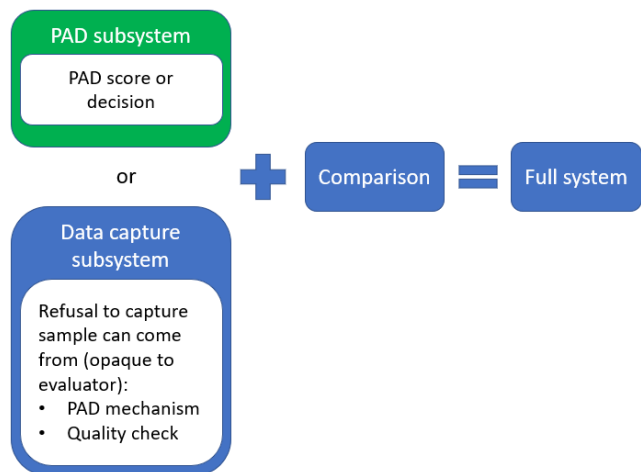
Biometrics refers to the automated recognition of individuals based on their physical or behavioral characteristics. Although its use has been widespread due to its convenience and it has been broadly tested, there are still vulnerabilities inherent to the technology. A common type of attack is the presentation attack, that is, a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [1]. These vulnerabilities need to be addressed and solved.

This work will focus on the fingerprint modality, used widely on critical infrastructures and access and border controls. Numerous approaches have been studied and implemented to overcome presentation attacks on fingerprint biometric systems [2], divided into software and hardware mechanisms. On the software side, there are static methods (sweat pore detection [3]–[5], ridge and

valley [6]–[8], perspiration [9], [10], etc.) and dynamic methods (skin distortion [11], [12], perspiration [13]). For the hardware approach, research has been made on challenge/response [14], odor [15], pulse oximetry [16], multispectral imaging [17]–[19] and OCT [20]–[22], among others.

Based on the standard ISO/IEC 30107-3 - *Biometric presentation attack detection testing and reporting*, the IUT (Item Under Test) shall be categorized into the Presentation Attack Detection (PAD) subsystem, data capture subsystem and full system (Fig. 1). For this work, the pertinent block is the PAD subsystem, that is, hardware and/or software that implements a PAD mechanism and makes an explicit declaration regarding the detection of presentation attacks.

The metrics that concern us for this work are the proportion of incorrect classifications of:



**FIGURE 1.** Diagram of categories of the IUT (Item Under Test): PAD subsystem, data capture subsystem and full system. This work falls on the first category (in green).

**TABLE 1.** Software PAD performance with independent evaluators. Results were gathered from [2].

Algorithm/author	Artefact species	APCER (%)	BPCER (%)
Dermalog [23]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	5.4	20.1
ATVS [23]		9.0	30.1
Anonymous [23]		16.0	32.8
Anonymous2 [23]		16.0	13.2
Dermalog [24]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	0.8	42.5
Greenbit [24]		39.5	38.8
Federico [24]		24.5	26.6
CASIA [24]		24.8	29.63
LBP pores detection [25]		11.13	13.30
Power spectrum [25]		24.65	41.40
Wavelet energy [25]		39.03	27.53
Ridges wavelet [25]		41.34	30.58
Valleys wavelet [25]		38.81	10.08
Curvelet energy [25]		40.70	31.08
Curvelet GLCM [25]		22.15	27.88

- Bona fide presentations: interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system, and
- Attack presentations: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

The proportion of bona fide presentations incorrectly classified as presentation attacks is called BPCER (Bona fide Presentation Classification Error Rate), and its counterpart is APCER (Attack Presentation Classification Error Rate), as stated in the standard. Two tables (Table 1 and Table 2) were done gathering the state-of-the-art results for APCER and BPCER, whenever possible, because many studies do not give results according to the standard, and others do not report numerical results at all. In Table 1, the reported results are the outcome of an evaluation performed by independent entities, using the algorithms the authors detailed. On the other hand, Table 2 gathers results that are self-declared by

**TABLE 2.** Software PAD performance with self-declared results and evaluations. Results were gathered from [2].

Algorithm/author	Artefact species	APCER (%)	BPCER (%)
Nikam and Agarwal [26]	Gelatin, Play-Doh, plastic, silicone sealant, Putty, alginate	2.08	1.62
Nikam and Agarwal [27]	Gelatin, Play-Doh	2.5	2.16
Nikam and Agarwal [28]	Gelatin, Play-Doh	2.5	2.16
Espinoza and Champod [3]	Latex	21.2	8.3
Galbally et al. [29]	Gelatin, Play-Doh, silicone	6.27	6.85
Pereira et al. [30]	White glue, silicon	3.47	10.52
Marasco and Sansone [8]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	12.3	12.63
Nikam and Agarwal [31]	Gelatin, Play-Doh	3.33	1.62
Nikam and Agarwal [32]	Gelatin, Play-Doh	3.33	1.62
Tan and Schuckers [6]	Gelatin, Play-Doh	6.0	2.28
Marasco and Sansone [33]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	12.3	12.63
Decann et al. [34]	Gelatin, Play-Doh, silicon	1.2	1.2
Tan and Schuckers [10]	Gelatin, Play-Doh, silicon	0.9	0.9
Nikam and Agarwal [35]	Gelatin, Play-Doh	0.9	2.08
Jia and Cai [36]	Gelatin	4.49	4.49
Antonelli et al. [11]	Gelatin, latex, white glue, RTV silicon	11.24	11.24
Zhang et al. [12]	Silicon	4.5	4.5
Jia et al. [37]	Gelatin	4.78	4.78

the authors, without having any outside evaluators testing the system. Also, the materials used for creating the fake fingers are detailed in both tables.

As it can be noticed, results that are self-reported have much lower error rates than those that went through an independent evaluation using the same methods. The average APCER for the independent evaluations of software solutions is 31.12%, while the BPCER is 25.98%. On the other hand, the APCER average for self-declared results is 5.74% and the BPCER is 5.09%.

On the hardware side, there are scarce reports on results, few databases exist and those that do are very small. In these cases, the evaluation results have been self-declared. APCER and BPCER (whenever possible to find) are shown on Table 3.

Those results that show a zero percent error rate are probably due to not having done an extensive evaluation, but only a concept proposal and trial with few users. Studies on Optical Coherence Tomography (OCT) have been more complete and, in general, adapted to ISO/IEC 30107-3. Although some reports show promising results for the said technologies, there are some drawbacks:

- OCT: expensive (thousands of euros), needs a few seconds to capture the fingerprint (0.02s for a genuine finger [45] or up to 56s for another case [41]) and the finger has to stay very still because it is easy to get

TABLE 3. Hardware PAD performance.

Hardware method	Authors	Artefact species	APCER (%)	BPCER (%)
OCT	Cheng and Larin [38], [39]	White glue, silicon, household cement	-	-
	Sousedik, Breithaupt, Busch [40]	Glycerol, graphite, window paint	11.32 (50% T) 6.17	3.52 (50% T) 25.37
	Menrath and Breithaupt [41]	?	-	-
	Nasiri-Avanaki et al. [22]	Sellotape	-	-
Challenge-response	Wei-Yun et al. [14]	Gelatin	0	0
Odor analysis	Baldiserra et al. [15]	Gelatin, latex, RTV silicon	-	-
Pulse oximetry	Reddy et al. [42]	Gelatin, Play-Doh	0	0
	Hengfoss et al. [43]	Cadaver	-	-
Multispectral	Ratha and Govindaraju [19]	Gelatin, gold latex, clay, green gummy Silicon	-	-
	Lumidigm		-	-
	Chang et al. [44]		-	-

disturbances. There are two commercial products from IDEMIA [46] and THORLABS [47], but no evaluation results are published.

- Challenge-response: in this case, the user is given a tactile pattern on the sensor surface and he/she needs to identify the pattern as a response. The problem is that the system is difficult to use, as the user cannot reliably perceive the proposed pattern. Also, it is uncomfortable for the user due to the currents sent to the finger.
- Odor analysis: although it works well with fake finger materials like silicone, others are difficult to identify because the sensor's response is similar to that obtained in the presence of human skin (for instance, with gelatin).
- Pulse oximetry: users must hold their finger for up to four seconds until the pulse sample is obtained and it does not work with thin materials, as pulse can be transmitted.
- Multispectral: although it has been claimed that this solution is very efficient, this present work shows that only one wavelength may be enough to distinguish fake from real fingerprints, simplifying the hardware needed. Also, the solutions noted on Table 3 are commercial and not academic, so the results are not public.

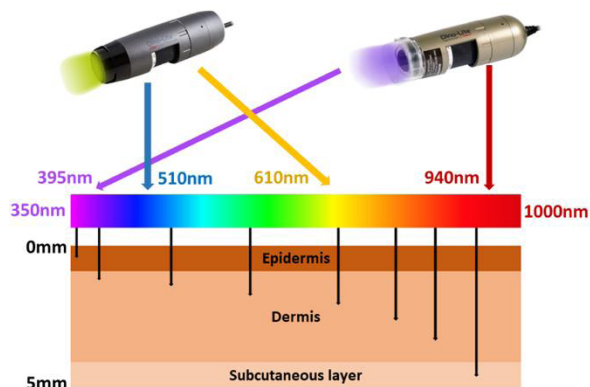
This work focuses on obtaining a low-cost and efficient hardware solution for detecting presentation attacks. For that end, 2 handheld microscopes with special lighting were used to perform a PAD (Presentation Attack Detection) evaluation by capturing 7,704 images of fake and real fingerprints of 17 subjects. These images were processed and classified using Bag of Features algorithms, **obtaining an APCER of 1.78% and a BPCER of 1.33%** at 70% training samples (3.99% and 1.11% for 50% training, respectively). It must be noted that these results were obtained even including a capture subject with non-conformant fingerprints (no ridges or valleys) in the database. Moreover, no fingerprint samples were left out, minus those that were the evaluator's fault – wrong finger, wrong LED wavelength turned on. All results are given in accordance to the standard on Presentation Attack Detection ISO/IEC 30107-3.

## II. METHODOLOGY AND IMAGE CAPTURE

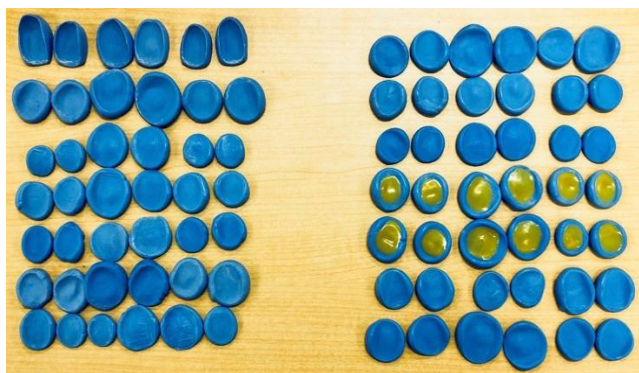
According to several works on fingerprint and skin imaging [48]–[51], different features of the skin can be observed at different wavelengths, depending on the penetration of the light, and thus, on the wavelength used. For this reason, it was decided to use two special lighting microscopes: Dino-Lite AD4113T-I2V (UV and IR lights, 395nm and 940nm respectively) and Dino-Lite Edge AM4115T-GRFBY (fluorescent lighting, excitation at 480nm and 575nm and emission at 510nm and 610nm). The cost of these microscopes was less than 500€ and less than 1000€ respectively at the time of writing, but after the study it will be concluded that a cheaper solution is possible, as only one excitation and one emission wavelength will be needed. As it is usually the case, the solutions used during research stages are more expensive than the final commercial solution. Once the study is made, a simpler, cheaper system can be developed by a manufacturer, as for the final product less microscope amplification and less wavelengths will be needed for obtaining the results. An overview of the skin penetration of each wavelength can be seen on Fig. 2.

A PAD evaluation was carried out with the microscopes, in order to test how well this technique performs in detecting artefacts, following Common Criteria [52] and ISO/IEC 30107-3 [1] standards.

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. One of its most relevant concepts to be applied to biometrics is the attack potential measurement. According to its guidelines, the attack potential can be measured as the effort to be expended in attacking a TOE (Target of Evaluation, which in this case is the fingerprint sensor) with a PAI (Presentation Attack Instrument or fake finger), expressed in terms of an attacker's expertise, resources and motivation. These parameters can be quantified by following a score system detailed in Common Criteria's CEM, which gives the final value for the Attack Potential. This value can then be mapped to be Basic, Enhanced-Basic, Moderate,



**FIGURE 2.** Different skin penetration levels depending on wavelength of digital microscopes.



**FIGURE 3.** Molds of capture subjects made of silicone.

High or Beyond high attack potentials. In sum, the attack potential is a measure of how easy it would be for an attacker to successfully spoof a system.

Moreover, also according to this standard, the evaluator is not expected to determine the exploitability for potential vulnerabilities beyond those for which a Basic attack potential is required to effect an attack. That is, once a fake finger material with a Basic attack potential has proven to be successful, no attacks that would require a higher difficulty should be made, because the system is already confirmed to be vulnerable to easier attacks.

Taking this in to account for our study, the easiest attacks were performed by using readily available and low-cost materials for building fake fingers. A test was designed following procedures from the Standard ISO/IEC 30107-3 [1] and its details can be seen on Table 4.

The fake fingers were built following very well-known techniques from the literature [24], [53]–[55]. Silicone molds created for the study are shown on Fig. 3.

A Matlab capture tool was developed to obtain images of fingerprints in an automated manner. It lets the evaluator enter bona fide and attacker IDs, number of attempts per finger, visit number, image resolution, whether they are real/artefact fingers, gender, artefact species, wavelengths and fingers.

**TABLE 4.** Details of the database following requirements of ISO/IEC 30107-3.

<b>Presentation attack instruments (PAI)</b>	438 (96 Play-Doh, 84 latex, 84 gelatin, 84 white glue, 90 nail polish)
<b>PAI species</b>	5 (Play-Doh, latex, transparent nail polish, gelatin, white glue)
<b>PAI series</b>	1 per source
<b>Capture subjects</b>	17 (13 asian, 3 caucasian, 1 african)
<b>Artefacts per capture subject</b>	6
<b>Sources</b>	96 fingers
<b>Output PAD information</b>	PAD score
<b>Attempts per presentation</b>	3
<b>Wavelengths</b>	4
<b>Attack attempts</b>	1,314 (per wavelength) <b>5,256 (total)</b>
<b>Bona fide attempts</b>	612 (per wavelength) <b>2,448 (total)</b>
<b>Images collected</b>	1,923 (per wavelength) <b>7,704 (total)</b>
<b>Attacker's expertise</b>	Expert (by the definition of CC's attack potential [52])

The app opens a window to visualize the microscope image output and captures the images in a sequence depending on the chosen parameters.

As expected, different lighting conditions gave out different features when inspecting fingerprint images. Examples of images in different wavelengths are shown on Fig. 4.

As it can be observed, the outputs can be easily distinguished in some cases. Play-Doh, the most common material used for spoofing, has very different features in every wavelength, so it can be easily detected (smoother or no edges, different color). Latex, nail polish and gelatin artefacts have sharper edges (mostly in UV and IR wavelengths). White glue has very clear bubbles on the 575/610nm wavelength, no matter how carefully the artefact is created (they cannot be seen with a naked eye).

#### A. FINGERPRINTS WITH SPECIAL CHARACTERISTICS

Commonly, in evaluations found in the literature, fingerprints with special characteristics are discarded from the test. In this work, we chose to be inclusive and execute a realistic study, so a subject with fingerprints with special characteristics was included. This user presented non-conformant fingerprints due to a skin disease, meaning that they did not have any ridges or valleys, so they would be deemed unfit for recognition. On Section IV, we calculate results both including and excluding this subject with the goal of measuring the impact of non-conformant fingerprints in realistic situations. As it can be seen on Fig. 5, ridges and valleys are barely noticeable, if not at all.

### III. PROCESSING AND CLASSIFICATION

For this work, no preprocessing or cropping was necessary before feeding the images to the chosen model, Bag of Features.

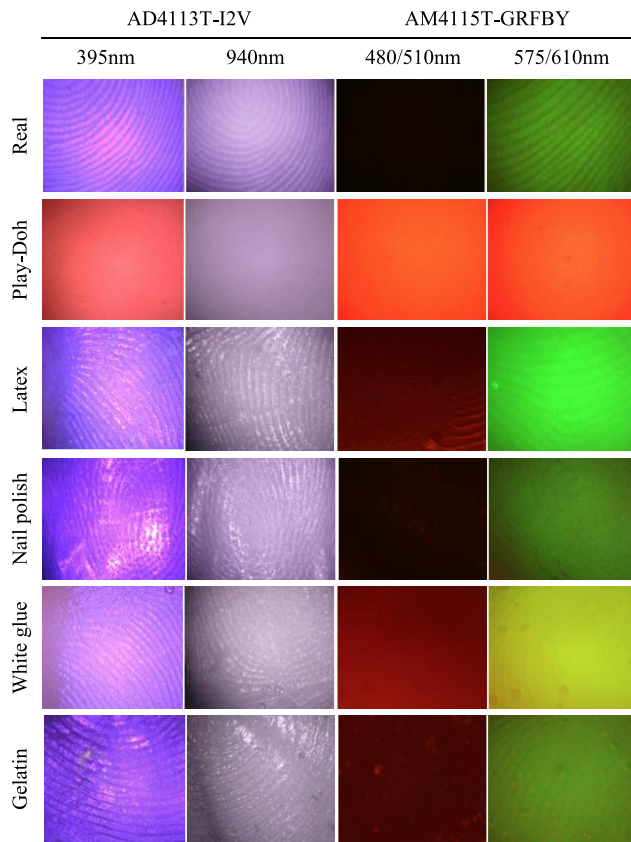


FIGURE 4. Examples of real and PAI images captured in different wavelengths.

This model, initially used for document classification known as Bag of Words, can also be suitable for fingerprint image classification. It does a good job distinguishing textures by creating frequency distributions of image patches, as it is a vector of occurrence count of a vocabulary of local image features. Thus, it was thought to be adequate for this case, as differences in textures could indicate if a finger is real or fake.

The model uses SIFT feature descriptors, appropriate for this case because they handle well intensity, rotation and scale differences. Then, these vector-represented patches are sorted into “codewords”, which in turn convert into a “codebook”. For this, k-means clustering is performed automatically and the codewords are defined as the centers of these clusters. This way, each image patch is mapped to a specific codeword and any image fed to the algorithm can be represented by a histogram of codewords [56].

The results were calculated 10 times each and averaged and a cross-comparison was done with training at 10%, 30%, 50%, 70% and 90% of samples (randomized by capture subject, and never including the same subject both for training and testing). The vocabulary size of Bag of Features was 850, 80% of the strongest features were used and the grid step was of 16x16. In order to avoid adjusting parameters for only this specific database, these parameters were chosen with only the first few captured samples. Then, once the database capture

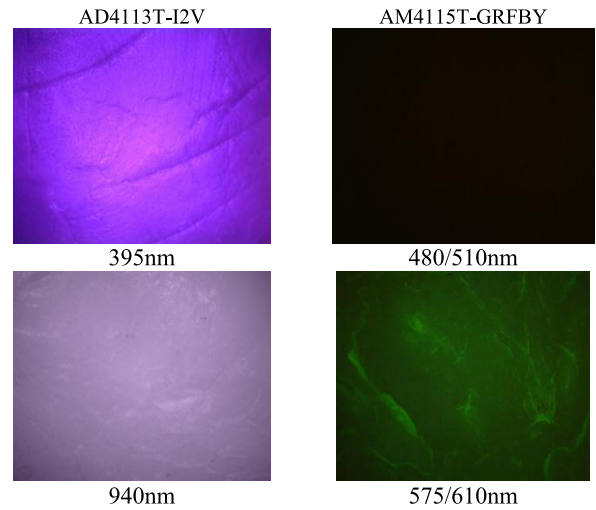


FIGURE 5. Examples of non-conformant fingerprints of one user of the database with a skin disease, in different wavelengths.

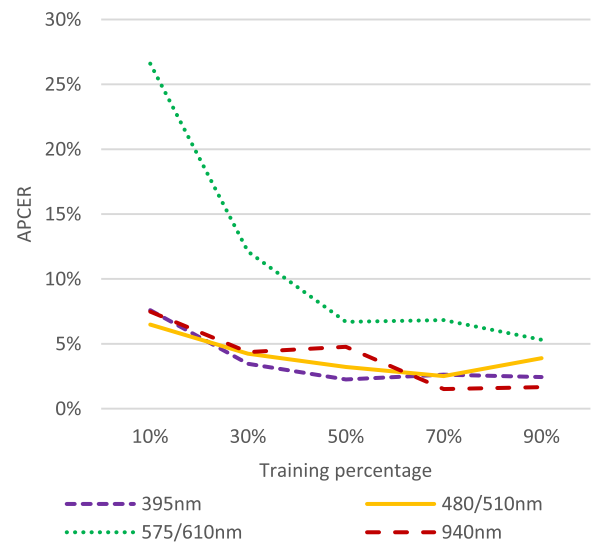


FIGURE 6. APCER cross-comparison results for each lighting mode. Every result was calculated 10 times and then averaged.

was completed, the algorithm was applied without changing the parameters and they still performed well. In all cases, the subjects used for training were not used for testing.

Two tests were made for classification: separate wavelengths and separate wavelength and channel. This way, it could be seen which wavelengths and channels behaved best for performance.

#### IV. RESULTS

This section gathers the results obtained in different tests, showing the classification error rates APCER and BPCER, as explained on the introduction. The tests performed are: classifying each wavelength separately, classifying each wavelength and RGB channel separately, using only the R channel of the 575/610nm wavelength and, lastly, leaving out the non-conformant samples of one capture subject (as it was explained in previous sections).

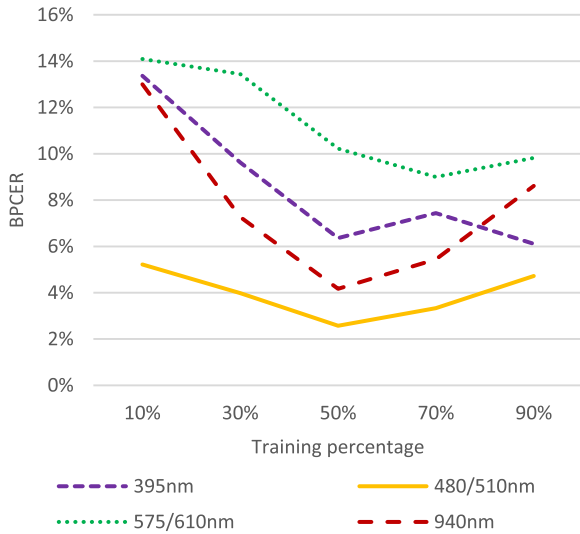


FIGURE 7. BPCER cross-comparison results for each lighting mode. Every result was calculated 10 times and then averaged.

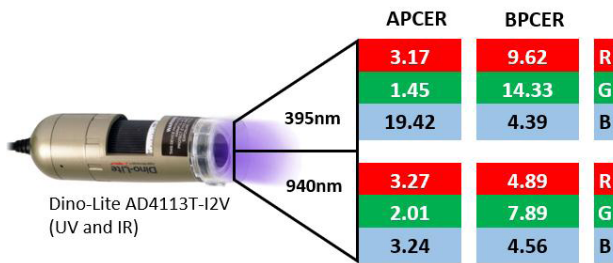
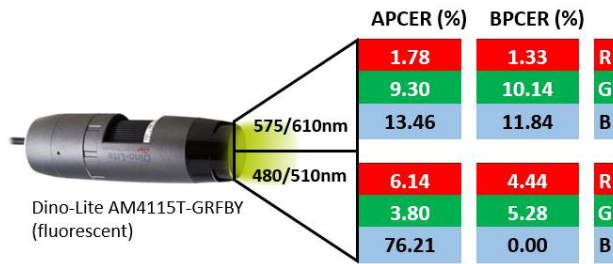


FIGURE 8. APCER and BPCER results separated by wavelength and channel. 70% training, 30% testing.

**A. CLASSIFYING EACH WAVELENGTH SEPARATELY**

Each microscope has two different lighting modes:

- Dino-Lite AD4113T-I2V:
  1. UV (395nm)
  2. IR (940nm)
- Dino-Lite AM4115T-GRFBY: fluorescent lights.
  1. Excitation at 480nm and emission at 510nm
  2. Excitation at 575nm and emission at 610nm

Thus, each mode was studied separately. The samples were fed in RGB to the algorithm, and it converts them to grayscale before classification. The database includes non-conformant samples from a subject with a skin disease. Results for APCER and BPCER cross-comparisons can be seen on Fig. 6 and Fig. 7, respectively.

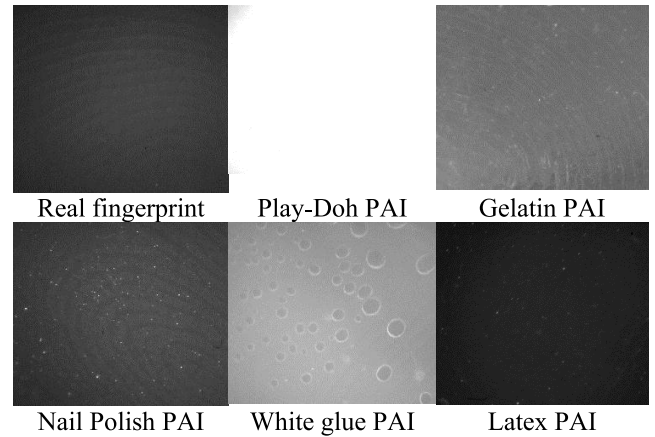


FIGURE 9. Noticeable variation in R channel.

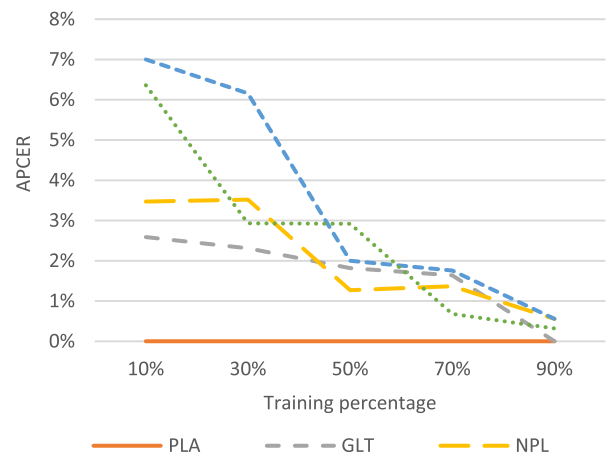


FIGURE 10. APCER cross-comparison with different artefact species. PLA = Play-Doh, GLT = gelatin, NPL = nail polish, WGL = white glue, LTX = latex.

It can be observed that some wavelengths perform better than others. 395nm and 480/510nm seem to work better for APCER results but, for the BPCER case, 480/510nm and 940nm yield a lower error rate.

**B. SEPARATED BY WAVELENGTH AND CHANNEL**

It was decided to break down the tests also by RGB channels, to check if some perform better than others. Results of this are detailed on Fig. 8.

This study shows that the best performing conditions are using the red channel of the 575/610nm mode, one of the available lightings of the fluorescent microscope. With a naked eye, it can be observed that there are indeed perceivable differences (Fig. 9).

Interestingly, using the 480/510nm in the blue channel, the BPCER is always 0% on this database. It was calculated 30 times. Thus, if wanted, only this channel could be used for eradicating the BPCER error of classifying real fingers as attacks. Nevertheless, this channel is the least suitable for APCER, as the error is very high (76%).

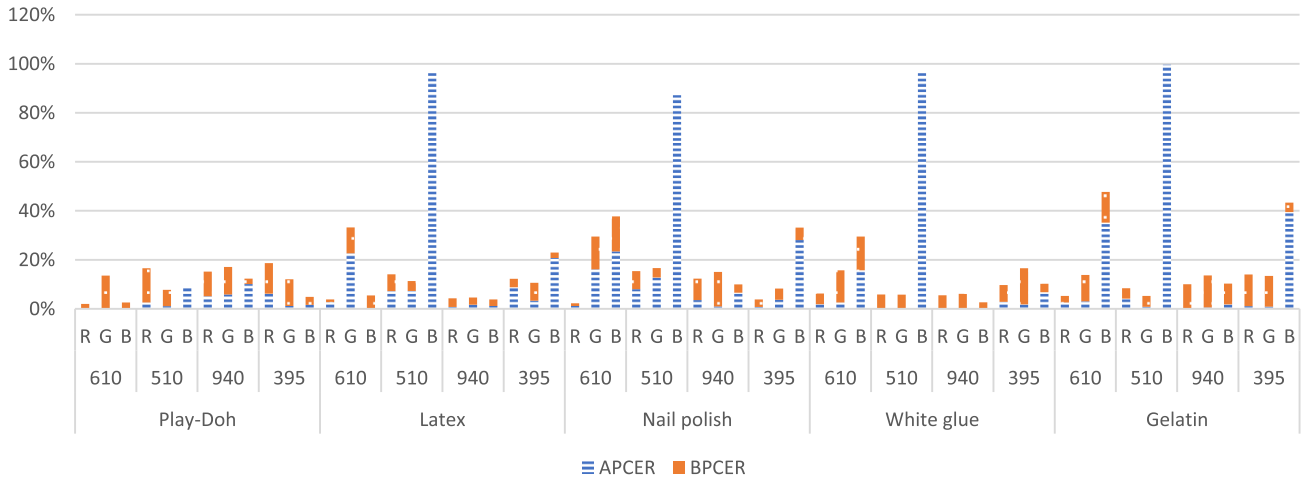


FIGURE 11. APCER and BPCER calculated by artefact species, wavelength and RGB channel.

TABLE 5. APCER and BPCER cross-comparison of 575/610nm wavelength samples in the red channel. Results were calculated 10 times and averaged.

	Training percentage				
	10%	30%	50%	70%	90%
APCER	9.36	4.07	3.99	1.78	0.89
BPCER	7.04	2.92	1.11	1.33	2.79

As the 575/610nm wavelength in the red channel seems to achieve lower error rates, a full cross-comparison was performed with it and it can be seen on Table 5.

According to ISO/IEC 30107-3, APCER and BPCER shall be calculated separately by artefact species. Thus, this subsection gathers the different results achieved per fake finger material, using the 575/610nm lighting mode and taking the red channel. The cross-comparisons for APCER and BPCER can be seen on Fig. 10 and Fig. 12.

According to the graphs, the lowest APCER is clearly for the Play-Doh case (0%), followed by gelatin (1.64% at 70% training). For BPCER, latex gives the lowest error rate, 1.36% at 70% training, and Play-Doh, gelatin and white glue follow it with very similar rates: 2.41%, 2.35% and 2.34%, respectively.

C. BY ARTEFACT SPECIES, WAVELENGTH AND RGB CHANNEL

With the goal of having a more thorough study on wavelength and channel influence on the different materials, errors were calculated for each category classification. Similarly to subsection B, channels R, G and B and wavelengths 575/610nm, 480/510nm, 940nm and 395nm were separated to calculate the different APCER and BPCER depending on the material put to the test. Results can be seen on Fig. 11. As it can be observed, some wavelengths and channels yield better error rates than others for different materials. For instance, the blue channel is the most problematic one when detecting

TABLE 6. Lowest error rates for each artefact species. Lower error rate considers the lowest APCER and BPCER combination.

	PLA	LTX	NPL	WGL	GLT
APCER (%)	0.00%	1.20	1.19	0.00	2.59
BPCER (%)	2.03%	2.67	1.12	2.67	2.67
Wavelength	610	940	610	940	610
Color channel	R	B	R	B	R

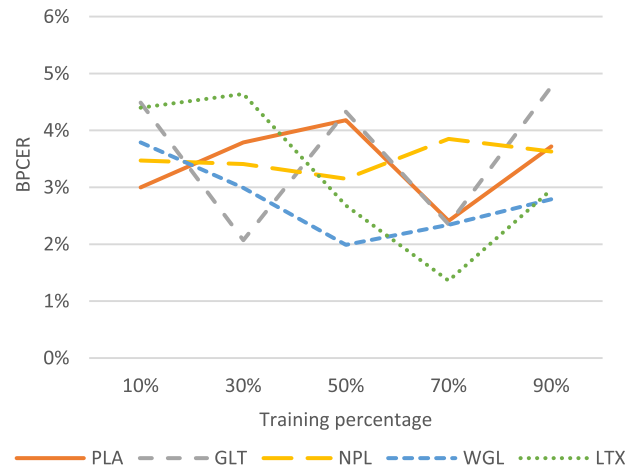
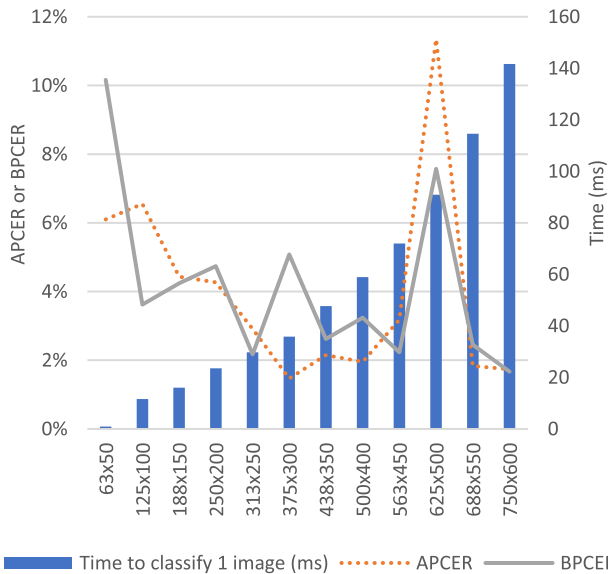


FIGURE 12. BPCER cross-comparison with different artefact species. PLA = Play-Doh, GLT = gelatin, NPL = nail polish, WGL = white glue, LTX = latex.

fake fingers, with error rates as high as 96.54% for white glue in the 475/510nm wavelength. On the other hand, some channels and wavelengths produce very promising error rates. The lowest ones for each material are shown on Table 6 (70% of the samples were used for training)

D. TIME PERFORMANCE AND IMAGE SIZE

The duration of a PAD subsystem classification is important for time-bound situations. A system that is meant for access control requires that the process for verification is fast, for



**FIGURE 13.** APCER and BPCER results for different image sizes, as well as time elapsed for classifying 1 image. 70% of the samples were used for training and the results were calculated 10 times and averaged.

**TABLE 7.** APCER and BPCER cross-comparison of 575/610nm wavelength samples in the red channel, leaving out one capture subject's non-conformant fingerprints due to a skin disease. Results were averaged 10 times.

	Training percentage				
	10%	30%	50%	70%	90%
APCER	9.05	6.90	3.51	1.70	2.46
BPCER	3.25	2.02	1.49	1.17	1.25

convenience purposes. For other cases, like critical infrastructures where a high security level is required, taking more time might be acceptable in exchange for lower error rates.

To study this matter, images from the 575/610nm wavelength in the red channel were cropped to different sizes, from 50px to 600px, and then the algorithm was used again to check if the performance held at smaller sizes. Then, the time performance was calculated for each case, for classifying one image as real or fake. The PC used for the calculations is an Intel Core x64 i7-6700 CPU at 3.40GHz with 16GB RAM, using MATLAB. The results can be seen on Fig. 13.

The graph shows an overview of the different trade-offs between size, error rates and time performance. For instance, at the 313x250px size, the error rates are quite low (2.91% APCER and 2.17% BPCER) while the time to classify one sample as real or fake is also low, 59.8ms, which could be a balanced trade-off. Both APCER and BPCER are best performing at the initial size, 750x600px (duration being 141.7ms); nevertheless, the size of 438x350 leads also to a low error rate, with an increase of 0.41% for APCER and 0,95% for BPCER (duration being 47.7ms).

### E. LEAVING OUT NON-CONFORMANT FINGERPRINTS

As there is a user in the database with non-conformant fingerprints due to a skin disease, another classification was

**TABLE 8.** Decrease of APCER and BPCER leaving out the capture subject with a skin disease.

	Training percentage				
	10%	30%	50%	70%	90%
$\Delta$ APCER	-0,31	2,83	-0,48	-0,08	1,57
$\Delta$ BPCER	-3,79	-0,90	0,38	-0,16	-1,54

done leaving these samples out (90 fake and 36 real). As it can be seen on Table 7, APCER and BPCER are still similar to the values obtained including the user, meaning that the system can work even with non-conformant fingerprints, as it is represented on Table 8.

### V. LESSONS LEARNED

This paper gathers a thorough evaluation on a presentation attack detection technique and proposes a novel method to acquire fingerprints, having carried out the capture (including selection of hardware and the design of capture tools) and processing, classification and results analysis. As an outcome, a low-cost and good performing PAD subsystem was obtained. This is meaningful because hardware solutions have barely been researched and there are scarce reports, and usually these methods yield a high cost.

It was seen that it is possible to achieve a low APCER and BPCER values using only one wavelength (575nm) with a filter (610nm) and taking only the red channel, which makes it inexpensive and accurate (APCER of 1.78% and BPCER of 1.33% at 70% training). Moreover, although it has to be more thoroughly tested and with a bigger database, all iterations of classifying the 480/510nm wavelength of the blue channel have shown a BPCER of 0,00%. Furthermore, it was discovered that Play-Doh artefacts are very easy to detect with this approach, which is a very commonly used material.

In addition, the database included one subject whose fingerprints did not have any noticeable ridges and valleys due to a skin disease, and it was seen that the attack detection error only improved very slightly when removing these samples. That means that this approach is also appropriate for these cases.

As future work, a bigger database will be gathered, and more approaches will be tried for the processing part, as well as fusion methods for different wavelengths.

### REFERENCES

- [1] *Information Technology—Biometric Presentation Attack Detection—Part 3: Testing and Reporting*, Standard ISO/IEC 30107-3:2017, 2017.
- [2] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.
- [3] M. Espinoza and C. Champod, "Using the number of pores on fingerprint images to detect spoofing attacks," in *Proc. Int. Conf. Hand-Based Biometrics*, Nov. 2011, pp. 1–5.
- [4] N. Manivanan, S. Memon, and W. Balachandran, "Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering," *Electron. Lett.*, vol. 46, no. 18, pp. 1268–1269, Sep. 2010.
- [5] H. Choi, R. Kang, K. Choi, and J. Kim, "Aliveness detection of fingerprints using multiple static features," *Int. J. Biol. Med. Sci.*, vol. 2, pp. 200–205, Jan. 2007.



- [6] B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis," *J. Electron. Imag.*, vol. 17, no. 1, pp. 011009-1–011009-9, 2008.
- [7] C. Jin and L. Shengzhe. (2011). *Fingerprint Liveness Detection Based on Multiple Image Quality Features*. [Online]. Available: [http://atibook.ir/dl/en/Engineering/ComputerScience/9783642179549\\_information\\_security\\_applications.pdf#page=296](http://atibook.ir/dl/en/Engineering/ComputerScience/9783642179549_information_security_applications.pdf#page=296)
- [8] E. Marasco and C. Sansone, "An anti-spoofing technique using multiple textural features in fingerprint scanners," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl.*, Sep. 2010, pp. 8–14.
- [9] B. Tan and S. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2006, p. 26.
- [10] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise," *Pattern Recognit.*, vol. 43, no. 8, pp. 2845–2857, 2010.
- [11] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 360–373, Sep. 2006.
- [12] Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake finger detection based on thin-plate spline distortion model," *Adv. Biometrics*, vol. 4642, pp. 742–749, 2007.
- [13] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, 2003.
- [14] Y. Wei-Yun, T. Hai-Linh, and T. Eam-Khwang, "Fake finger detection using an electrotactile display system," in *Proc. 10th Int. Conf. Control. Autom. Robot. Vis. (ICARCV)*, Dec. 2008, pp. 962–966.
- [15] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," *Adv. Biometrics*, vol. 3832, pp. 265–272, 2006.
- [16] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, "A new method for fingerprint anti-spoofing using pulse oximetry," in *Proc. 1st IEEE Int. Conf. Biometrics, Theory, Appl., Syst.*, Sep. 2007, pp. 1–6.
- [17] R. K. Rowe, K. A. Nixon, and S. P. Corcoran, "Multispectral fingerprint biometrics," in *Proc. 6th Annu. IEEE Syst., Man Cybern. Inf. Assurance Workshop (SMC)*, Jun. 2005, pp. 14–20.
- [18] D. Zhang, Z. Guo, and Y. Gong, *Multispectral Biometrics: Systems and Applications*. Cham, Switzerland: Springer, 2015, pp. 1–229.
- [19] N. K. Ratha and V. Govindaraju, "Multispectral fingerprint image acquisition," *Adv. Biometrics*, pp. 3–23, 2008.
- [20] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric fingerprint data analysis using optical coherence tomography," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–6.
- [21] E. Auksoorius and A. C. Boccara, "Fingerprint imaging from the inside of a finger with full-field optical coherence tomography," *Biomed. Opt. Express*, vol. 6, no. 11, pp. 4465–4471, 2015.
- [22] M.-R. Nasiri-Avanaki, A. Meadway, A. Bradu, R. M. Khoshki, A. Hojjatoleslami, and A. G. Podoleanu, "Anti-spoof reliable biometry of fingerprints using en-face optical coherence tomography," *Opt. Photon. J.*, vol. 1, no. 3, pp. 91–96, 2011.
- [23] G. L. Marcialis, "LivDet 2009—fingerprint liveness detection competition 2009," Dept. Elect. Electron. Eng., Univ. Cagliari, Cagliari, Italy, Tech. Rep., 2009.
- [24] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011—Fingerprint liveness detection competition 2011," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 208–215.
- [25] L. Ghiani, P. Denti, and G. L. Marcialis, "Experimental results on fingerprint liveness detection," in *Articulated Motion and Deformable Objects* (Lecture Notes in Computer Science), vol. 7378. Berlin, Germany: Springer-Verlag, 2012, pp. 210–218.
- [26] S. B. Nikam and S. Agarwal, "Fingerprint liveness detection using curvelet energy and co-occurrence signatures," in *Proc. 5th Int. Conf. Comput. Graph., Imag. Visualisation, Mod. Techn. Appl. (CGIV)*, 2008, pp. 217–222.
- [27] S. B. Nikam and S. Agarwal, "Wavelet energy signature and GLCM features-based fingerprint anti-spoofing," in *Proc. Int. Conf. Wavelet Anal. Pattern Recognit. (ICWAPR)*, vol. 2, Aug. 2008, pp. 717–723.
- [28] S. B. Nikam and S. Agarwal, "Gabor filter-based fingerprint anti-spoofing," in *Proc. Int. Conf. Adv. Concepts Intell. Vis. Syst.*, 2008, pp. 1103–1114.
- [29] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.
- [30] L. F. A. Pereira et al., "A fingerprint spoof detection based on MLP and SVM," in *Proc. Int. Joint Conf. Neural Netw.*, Jun. 2012, pp. 1–7.
- [31] S. B. Nikam and S. Agarwal, "Ridgelet-based fake fingerprint detection," *Neurocomputing*, vol. 72, nos. 10–12, pp. 2491–2506, Jun. 2009.
- [32] S. B. Nikam and S. Agarwal, "Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems," in *Proc. 1st Int. Conf. Emerg. Trends Eng. Technol. (ICETET)*, Jul. 2008, pp. 675–680.
- [33] E. Marasco and C. Sansone, "Combining perspiration- and morphology-based static features for fingerprint liveness detection," *Pattern Recognit. Lett.*, vol. 33, no. 9, pp. 1148–1156, 2012.
- [34] B. DeCann, B. Tan, and S. Schuckers, "A novel region based liveness detection approach for fingerprint scanners," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 5558. Cham, Switzerland: Springer, 2009, pp. 627–636.
- [35] S. B. Nikam and S. Agarwal, "Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection," *Int. J. Inf. Comput. Secur.*, vol. 3, no. 1, pp. 1–46, 2009.
- [36] J. Jia and L. Cai, "Fake finger detection based on time-series fingerprint image analysis," in *Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues*. Cham, Switzerland: Springer, 2007, pp. 1140–1150.
- [37] J. Jia, L. Cai, K. Zhang, and D. Chen, "A new approach to fake finger detection based on skin elasticity analysis," *Adv. Biometrics*, vol. 4642, pp. 309–318, 2007.
- [38] Y. Cheng and K. V. Larin, "Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis," *Appl. Opt.*, vol. 45, no. 36, pp. 9238–9245, 2006.
- [39] Y. Cheng and K. V. Larin, "In vivo two- and three-dimensional imaging of artificial and real fingerprints with optical coherence tomography," *IEEE Photon. Technol. Lett.*, vol. 19, no. 20, pp. 1634–1636, Oct. 15, 2007.
- [40] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric fingerprint data analysis using optical coherence tomography," in *Proc. Int. Conf. BIOSIG Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–6.
- [41] M. Menrath, "Fingerprint with OCT," M.S. thesis, Fern-Univ. Hagen Cooperat. Bundesamt Sicherheit Inf., 2011.
- [42] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, "A new anti-spoofing approach for biometric devices," *IEEE Trans. Biomed. Circuits Syst.*, vol. 2, no. 4, pp. 328–337, Dec. 2008.
- [43] C. Hengfoss, A. Kulcke, G. Mull, C. Edler, K. Püschel, and E. Jopp, "Dynamic liveness and forgeries detection of the finger surface on the basis of spectroscopy in the 400–1650 nm region," *Forensic Sci. Int.*, vol. 212, nos. 1–3, pp. 61–68, 2011.
- [44] S. Chang, K. Larin, Y. Mao, C. Flueraru, and W. Almuhtadi, "Fingerprint spoof detection by NIR optical analysis," in *State of the Art in Biometrics*. Rijeka, Croatia: InTech, May 2017, pp. 57–84, ch. 3.
- [45] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric fingerprint data analysis using optical coherence tomography," in *Proc. Int. Conf. BIOSIG Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–6.
- [46] IDEMIA. (2018). *Télécom SudParis and IDEMIA Present BioDigital, A New Biometric Technology to Combat Identity Spoofing*. [Online]. Available: <https://www.idemia.com/press-release/telecom-sudparis-and-idemia-present-biodigital-new-biometric-technology-combat-identity-spoofing-2018-09-06>
- [47] Thorlabs. *OCT Imaging Systems & Components*. Accessed: Nov. 1, 2018. [Online]. Available: [https://www.thorlabs.com/navigation.cfm?guide\\_id=2039](https://www.thorlabs.com/navigation.cfm?guide_id=2039)
- [48] Y. Tamura, T. Mashita, Y. Kuroda, K. Kiyokawa, and H. Takemura, "Feature detection in biological tissues using multi-band and narrow-band imaging," *Int. J. Comput. Assist. Radiol. Surg.*, vol. 11, no. 12, pp. 2173–2183, 2016.
- [49] K. Tanaka, Y. Mukaigawa, H. Kubo, Y. Matsushita, and Y. Yagi, "Recovering inner slices of layered translucent objects by multi-frequency illumination," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 4, pp. 746–757, Apr. 2017.
- [50] A. Krishnaswamy and G. V. G. Baranoski, "A study on skin optics," Center Biometrics Secur. Res., Key Lab., Complex Syst. Intell. Sci., Inst. Automat., Chin. Acad. Sci., Graduate School Chin. Acad. Sci., Beijing, China, Tech. Rep. 200401, 2004.
- [51] I. V. Meglinski and S. J. Matcher, "Quantitative assessment of skin layers absorption and skin reflectance spectra simulation in the visible and near-infrared spectral regions," *Physiol. Meas.*, vol. 23, no. 4, pp. 741–753, 2002.
- [52] *Common Methodology for Information Technology Security Evaluation Evaluation methodology September 2012 Revision 4 Foreword*, Standard, Common Criteria, Sep. 2012, p. 433.

- [53] T. Matsumoto, S. Hoshino, H. Matsumoto, and K. Yamada, "Impact of artificial 'gummy' fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, Apr. 2002.
- [54] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," in *Proc. 4th Workshop Conf. Smart Card Res. Adv. Appl.*, Bristol, U.K., vol. 31, 2000, p. 16.
- [55] S. A. C. Schuckers, "Spoofing and anti-spoofing measures," *Inf. Secur. Tech. Rep.*, vol. 7, no. 4, pp. 56–62, 2002.
- [56] C. Schmid, "Bag-of-features for category classification," in *Proc. ENSI/NRIA Vis. Recognit. Mach. Learn.*, 2011.



**INES GOICOECHEA-TELLERIA** received the bachelor's degree in industrial electronics and automation from the University Carlos III of Madrid (UC3M), in 2014, and the master's degree in electronic systems and applications engineering, in 2015. She is currently pursuing the Ph.D. degree, with a focus on the evaluation of presentation attack detection in the context of common criteria. She is currently with the Electronics Technology Department, UC3M, as a part of the

University Group for Identification Technologies (GUTI). In 2014, she joined GUTI, where she has been involved in presentation attack detection, since 2014. She is a member of ISO/IEC JTC1 SC27 and SC37, and CEN/TC 224 WG18.



**KIYOSHI KIYOKAWA** was a Researcher with the Communications Research Laboratory from 1999 to 2002, a Visiting Researcher with the Human Interface Technology Laboratory, University of Washington, from 2001 to 2002, and an Associate Professor with the Cybermedia Center, Osaka University, from 2002 to 2017. He is currently a Full Professor with the Nara Institute of Science and Technology, where he leads the Cybernetics and Reality Engineering Laboratory.

He has been involved in organizing various IEEE and ACM conferences, such as the IEEE International Symposium on Mixed and Augmented Reality, the IEEE Virtual Reality, the IEEE International Symposium on Wearable Computers, the IEEE Symposium on 3D User Interfaces, and the ACM Symposium on Virtual Reality Software and Technology. He was a Research Fellow of the Japan Society for the Promotion of Science, in 1998.



**JUDITH LIU-JIMENEZ** received the degree in telecommunication engineering from the Polytechnic University of Madrid, in 2004, and the Ph.D. degree in electronics from the University Carlos III of Madrid, in 2010. Since 2004, she has been with the University Carlos III of Madrid. The focus of her work is on biometrics and hardware/software codesign, specifically for iris biometrics. She has participated in several national and European funded projects, besides working on

ID management, evaluation, and anti-spoofing mechanisms.



**RAUL SANCHEZ-REILLO** received the Ph.D. degree. He is currently an Associate Professor with the University Carlos III of Madrid. He is also the Head of the University Group for Identification Technologies, where he is involved in project development and management concerning a broad spectrum of applications, ranging from social security services to financial payment methods. He has participated in European projects, such as eEpoch and BioSec, by virtue of being the

WP Leader. He is expert in security and biometrics. He served as a member of the SC17, SC27, and SC37 Standardization Committees. He has been the Spanish Chair of SC17 and the Secretariat of SC37.

...