IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 24, 2020, accepted May 14, 2020, date of publication May 20, 2020, date of current version June 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995829

Dynamic Fingerprint Statistics: Application in Presentation Attack Detection

ANAS HUSSEIS, JUDITH LIU-JIMENEZ, INES GOICOECHEA-TELLERIA, AND RAUL SANCHEZ-REILLO, (Senior Member, IEEE)
Electronic Technology Department, University Carlos III of Madrid, 28911 Leganés, Spain

Corresponding author: Anas Husseis (ahusseis@ing.uc3m.es)

This work was supported by the European Union's Horizon 2020 for Research and Innovation Program under Grant 675087 (AMBER).

ABSTRACT Fingerprint recognition systems have proven significant performance in many services such as forensics, border control, and mobile applications. Even though fingerprint systems have shown high accuracy and user acceptance, concerns have raised questions about the possibility of having our fingerprint pattern stolen and presented to the system by an imposter. In this paper, we propose a dynamic presentation attack detection mechanism that seeks to mitigate presentation attacks. The adopted mechanism extracts the variation of global fingerprint features in video acquisition scenario and uses it to distinguish bona fide from attack presentations. For that purpose, a dynamic dataset has been collected from 11 independent subjects, 6 fingerprints per user, using thermal and optical sensors. A total of 792 bona fide presentations and 2772 attack presentations are collected. The final PAD subsystem is evaluated based on the standard ISO/IEC 30107-3. Considering SVM classification and 3 folds cross validation, the obtained error rates at 5% APCER are 18.1% BPCER for the thermal subset and 19.5% BPCER for the optical subset.

INDEX TERMS Fingerprint, presentation attack, presentation attack detection, spoofing.

I. INTRODUCTION

Fingerprint recognition [1]–[3] is adopted in several applications due to its convenient acquisition and user acceptance, but nevertheless it had been vulnerable to direct and indirect attacks [4]. Presentation Attack (PA), also known as direct, physical or spoofing attack, is increasingly becoming a vital challenge in the security of biometric recognition. In this paper, we aim to detect attack presentations on fingerprint modality, wherein an attacker aims to claim an identity of someone other than himself (imposter attack).

PA is a challenging problem because fingerprint systems are designed to detect the pattern of ridges and valleys in a fingerprint, then prepare it to be compared with another pattern in a saved template/s. Therefore, if a fingerprint pattern was duplicated, directly from the genuine fingerprint or indirectly from a latent in a touched surface, and afterward presented to a fingerprint sensor, there would be a specific potential risk that corresponds to this imposter attack.

In this study, we propose a novel Presentation Attack Detection (PAD) mechanism that utilizes the dynamic fingerprint statistics as distinctive features. The proposed method contributes to the comprehension of fingerprint dynamic attributes and how these features can be adequately used to alleviate attack presentations.

This proposed methodology calls into question whether the formation of genuine fingerprint provides discriminative dynamic features that distinguish it from the different presentation attack species. In this context, a dataset of fingerprint videos had been collected using two sensors with different technologies and capabilities. In addition to genuine presentations, seven species of Presentation Attack Instruments (PAIs) are used to build the dataset.

Dynamic acquisition was chosen because we believe that fingerprint video provides the complete signal of the interaction between the subject and the sensor. First Order Statistics (FOSs) are used to describe the visual features of a video, considering that a video is a sequence of images. FOSs are selected because they provide a useful global description for the video frames as well as the calculation's simplicity.

Our Presentation Attack Detection (PAD) mechanism is evaluated following ISO/IEC 30107-3:2017 [5] standard's recommendations. The evaluation outlines the capability of the PAD mechanism to correctly classify bona fide and attack

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

presentations. The results are expected to provide an insight into the PAD subsystem performance in different technologies. Moreover, results should characterize the attack strength of different PA species and clearly show the mechanism's vulnerability to certain attack species.

This paper is divided into five sections. The first section has given a brief overview of this paper. Section II gives a general view of past-to-present literature on dynamic PAD mechanisms. In the third section, we discuss the proposed mechanism. The fourth section demonstrates the experimental procedure. Results are analyzed in Section V. And finally, our conclusions are drawn in section VI.

II. RELATED WORK

Several surveys, for instance [6]–[9], have been carried out to review and taxonomize the state of the art in PA and PAD on fingerprint modality. Accordingly, we can classify impersonation PAs into two distinct groups: cooperative and non-cooperative attacks. The key difference between these groups is the style of capturing a purposed fingerprint. A mold of the fingerprint is donated by the bona fide user in case of cooperative attacks [10]–[14], while non-cooperative attacks exploit bona-fide latent fingerprints in touched surfaces [10]–[12], [15], [16].

On the other hand, various approaches have been put forward to categorize PAD mechanisms: (a) Hardware/software PAD methods' categorization is proposed to distinguish if a mechanism needs a specific hardware capability, (b) static/dynamic categorization distinguishes the methods based on the acquisition method [6], [7], and (c) the basis of the PAD feature extraction are considered in [9] to classify whether the PAD features are collateral means or caused by natural phenomena. Within the framework of the proposed PAD mechanism, we initiated this section to overview the state-of-the-art studies that investigate the dynamic features of fingerprints.

Fundamentally, dynamic methods analyze the fingerprint presentation as a sequence of images regardless of the hardware capabilities of different sensors. Even though, it is certainly important to clarify the sensor's characteristics when evaluating a dynamic algorithm on a particular dataset.

In addition to the distinct pattern of ridges and valleys, a genuine fingerprint comprises natural phenomena like elasticity, perspiration, temperature, etc. These phenomena influence the dynamic signal, i.e. fingerprint image sequence, which is captured during the fingerprint presentation. Therefore, real presentations are expected to differ from attacks when an appropriate set of features is defined and extracted. Since literature studies have demonstrated that dynamic fingerprint analysis provides efficient basis to detect attacks, we propose a dynamic PAD mechanism based on the variation of image statistics in the sequence of fingerprint images.

The following subsections draw the reader's attention to the literature of dynamic PAD methods. Performance analysis is reported in Table 1 to compare the state-of-the-art dynamic mechanisms.

A. DISTORTION'S DYNAMIC ANALYSIS

Preliminary work in fingerprint plastic distortion was carried out in the early 2000s to cope with non-linear deformations of dynamic fingerprint acquisitions [24]. Then, a systematic study on skin distortion was conducted demonstrating that genuine fingerprints produce higher distortion when compared to fake fingerprints [17]. The used dataset was collected using an optical sensor (high frame rate), with user instructions on how to present the fingerprint with rotation and pressure. For each presentation the method computes the optical flow, Distortion map, and distortion code consecutively, afterward compares the distortion codes to detect attacks.

In [18] the authors analyzed the fingerprint deformation and modeled the distortion of genuine fingerprints and attacks using a thin plate spline (TPS). The tested dataset was collected as following: fingerprint presentation is performed by presenting the finger to the sensor then pressure should be applied in different directions. The authors underline that attack instruments are more rigid when compared to the genuine fingerprint's elasticity, thus the deformation of attacks is lower when the same presentation conditions apply. Under those circumstances, the minutia movement represents the global distortion, and a sequence of paired minutia before and after distortion is used to calculate the parameters of the TPS model. The bending energy vector of the TPS model is utilized to distinguish bona fide and attack presentations.

Skin elasticity was analyzed under the assumption that the sequence of genuine fingerprint contains an increasing size of the fingerprint pattern and higher intensity in [19]. In this paper, the evaluation was reported using a dynamic dataset that was collected by a high frame rate capacitive sensor, while only a gelatin attack was performed. Based on those specifications, the mechanism extracts (a) the correlation coefficient of the fingerprint area and the signal intensity, and (b) the standard deviation of the fingerprint area extension in x and y axes. Finally, Fisher linear discriminant analysis is used to classify bona fide and attack presentations.

B. PERSPIRATION'S DYNAMIC ANALYSIS

Perspiration is a natural distinctive phenomenon in human skin that is affected by physical, psychological, and environmental factors. When a fingerprint contacts any surface, the finger's sweat glands start releasing moisture that diffuses along the ridges in time. Therefore, it had been suggested that a fingerprint dynamic acquisition is capable of detecting the consequence of perspiration, by analyzing the sequence of fingerprint images.

Initial work was undertaken to study the perspiration pattern in genuine fingerprints [20]. A dataset of genuine, cadaver, and artificial fingerprints was collected via a capacitive scanner to evaluate the proposed algorithm. Two successive images, five seconds apart, were used to extract: (a) four dynamic features that describe the general swing, i.e. local maximum minus local minimum, and (b) a static feature that represent the energy for the first image. It was observed that the swing is generally higher in genuine fingerprints

TABLE 1. Performance of state-of-the-art dynamic PAD mechanisms (reported in [6]).

Reference	Category	Technique	PAI species	Sensor/s	Error Rates
Antonelli 2006 [17]	Distortion	Optical flow	Gelatin, RTV silicon, white glue, latex	Optical	APCER= NA, BPCER= NA, EER = 11.24%
Zhang 2009 [18]	Distortion	Thin-Plate Spline	Silicon	Optical	APCER= NA, BPCER= NA, EER = 4.5%
Jia 2007 [19]	Distortion	Statistics	Gelatin	Capacitive	APCER= NA, BPCER= NA, EER = 4.78%
Derakhshani 2003 [20]	Perspiration	Fourier	Play-Doh, cadaver	Capacitive	APCER= NA, BPCER= NA, EER = 11.11%
Parthasaradhi 2005 [21]	Perspiration	Statistics; Fourier	Play-Doh, cadaver	Capacitive	APCER= 5% - 20%, BPCER= 6.77% - 20%
				Optical	APCER= 4.6%-14.3, BPCER= 0% - 26.9%
				Electro-Optical	APCER= 0%-19%, BPCER= 6.9% - 38.5%
Abhyankar 2009 [22]	Perspiration	Wavelet	Play-Doh, gummy, cadaver	Capacitive	APCER= NA, BPCER= NA, EER = 13.85%
				Optical	
				Electro-Optical	
Plesh 2019 [23]	Perspiration	Color	Play-Doh, ecoflex, gelatin, dragonskin, ModelMagic, SillyPutty, wood glue, latex, paper print, transparent film	Optical	APCER= 0.2%, BPCER= 13.8% - 18.35%

when compared to the attacks, furthermore, the energy of the first image is significantly high in genuine fingerprints in comparison with the attacks. Finally, classification is done using a back propagation neural network. The experiment was extended to cover electro-optical and optical sensors, furthermore, to address the extreme cases of dry and moisturized fingerprints [21].

Another proposition was to isolate the changing energy of the perspiration pattern and use the energy distribution of the changing coefficients to classify bona fide presentations from attacks [22]. A dataset of genuine, cadaver and artificial fingerprints were collected by capacitive, electro-optical and optical sensors. At each presentation two images, two seconds apart, were captured. The authors reported the contributions of this work over their previous work in [20] to be: Using a larger dataset, the algorithm requires only 2 seconds between the two successive frames instead of 5 seconds, and the algorithm is integrated with the verifinger SDK [25].

A more recent mechanism has proposed to utilize a color dynamic acquisition in order to analyze the dynamics of bona fide and attack presentations; ten different materials used for producing PAIs [23]. The algorithm analyzes two images, 0.625 second apart, by extracting five dynamic and two static features sets. The dynamic features were defined to represent intensity variation, displacement, perspiration, foreground, and background analysis. Finally, a deep neural network is used to classify the presentation.

III. FINGERPRINT DYNAMIC STATISTICS

In this section, the essential phases of the PAD scheme are explained. First, feature extractor in the proposed PAD mechanism extracts the variation of first order statistics in the images sequence of a fingerprint presentation. After that, different machine learning classifiers are used for the purpose of declaring the presentation type based on the extracted features in the previous phase.

A. FEATURE EXTRACTOR

The selected features in the PAD feature extractor are the dynamic mean, entropy, standard deviation, median, energy, skewness, kurtosis, and coefficient of variation. These measures provide statistical measures for the image visual characteristics and had confirmed a difference between bona fide and attack fingerprint images in static acquisition [26].

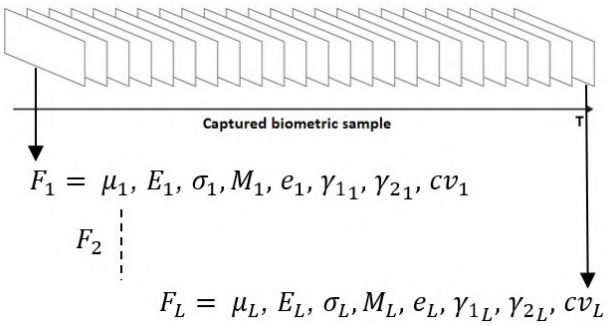


FIGURE 1. Dynamic video statistics.

Equation 1 is used to extract the features from each presentation (Figure 1):

$$(F_n)_{n=1}^{L}, \quad F_n = features(n), \ n \in [1, 2, \ldots, L] \tag{1}$$

where, $(F_n)_{n=1}^{L}$ is the features vector which describes L successive frames, n is the image number in the sequence, and L presents the last image. *features* is a vector of 8 elements, whereas each element corresponds to one of the measures in equations (2-9).

- Mean

$$\mu = \frac{1}{N}\sum_{n=0}^{N-1} H(n) \tag{2}$$

- Entropy

$$E = -\sum_{n=0}^{N-1} H(n) log H(n) \tag{3}$$

- Variance

$$\sigma^2 = \sum_{n=0}^{N} (n-\mu)^2 H(n) \tag{4}$$

- Median

$$M = \underset{a}{\operatorname{argmin}} \sum_{n} H(n)\,|n - a| \tag{5}$$

- Energy

$$e = \sum_{n=0}^{N-1} H(n)^2 \tag{6}$$

- Skewness

$$\gamma_1 = \frac{1}{\sigma^3} \sum_{n=0}^{N-1} (n-\mu)^3 H(n) \tag{7}$$

- Kurtosis

$$\gamma_2 = \frac{1}{\sigma^4} \sum_{n=0}^{N-1} (n-\mu)^4 H(n) \tag{8}$$

- Coefficient of variation

$$cv = \frac{\sigma}{\mu} \tag{9}$$

where $H(n)$ is the frame's histogram and N is the number of histogram bins.

B. CLASSIFICATION

Choosing the machine learning algorithm for the classification model is not straight forward and depends on many factors such as type of data, accuracy, classification algorithm complexity, etc. As a result, different classification algorithms are tested to determine the method with the best generalizability. The following classifiers are investigated in this paper: (a) Linear Discriminant Analysis (LDA), (b) Support Vector Machine (second degree polynomial kernel SVM), and (c) Ensemble Learning method (RUSBoosted trees). We have tested seven classification algorithms with multiple setups, the chosen algorithms have shown the best performance and therefore reported in this paper.

IV. EXPERIMENT SETUP

To evaluate the proposed PAD mechanism, a dynamic dataset is collected whereas the interaction between a subject's fingerprint and the sensor is recorded in videos. The data were collected using commercial fingerprint sensors with different sensing technologies, which allow us to analyze the technology impact in the PAD subsystem's accuracy.

Our PAD subsystem scheme consists of three main components with the following functions: (i) fingerprint detection and segmentation, (ii) feature extraction and concatenation, and (iii) PAD classification using a pre-trained model. This scheme returns a multi-valued PAD score as reported in the results section.

A. SENSORS

The used sensors have a significant difference in their characteristics, consequently, the acquired videos have different qualities and frame rates. Table 2 lists the key characteristics of the used sensors.

TABLE 2. Sensors characteristics.

Technology	Resolution	Image size	Scanning time
Optical	500 ppi	900×900 pixels	0.05 second/frame
Thermal	385 ppi	180×256 pixels	0.7 second/frame

FIGURE 2. Preparing PAIs using silicon 3D molds.

The frame rate difference, caused by scanning time, results in two different acquisition methods. For our experiment, we captured fixed-length videos for the thermal sensor (7 frames per presentation), while in the case of the optical sensor, the subjects were asked to perform the presentation and the capture stops when the fingerprint is removed, which results in different lengths of interaction between subjects and the sensor.

B. DATA COLLECTION

The dataset is divided into two portions: (i) bona fide presentations (ii) cooperative attack presentations. Eleven independent subjects have participated in the data collection, and only one attacker has performed attacks using seven materials. Customized acquisition tools are developed using the sensors' SDKs in order to capture the sequence of frames (Video) instead of acquiring one image. The acquisition tools are developed such that no PAD mechanisms are applied to capture the presentations.

The first phase of building the dataset required capturing bona fide presentations and collecting silicon molds of the selected fingers from each subject. At least two weeks later, the subject was required to perform another session of bona fide presentations. The chosen fingers are thumb, index, and middle; left and right hands.

In the second phase, the attacker defined seven materials that can pass the detection subsystem, then using the collected molds the attacker prepared multiple types of PAIs (Figure 2) and performed 2772 attack presentations.

FIGURE 3. Optical sensor captures. For reasons of space, this figure shows partial examples of bona fide and attack presentations. The average number of frames/presentation is 25.

TABLE 3. Dataset specifications.

Sensors	2 (thermal and optical)
Participants	11 (7 males, 4 females)
Fingers per each subject	6 (thumb, index and middle) from both hands
Total fingerprints	66 fingerprints
Bona fide visits	2 (minimum 2 weeks apart)
Molds total	66 silicon molds (one per finger)
Presentation Attack Instrument species	7 (Play-Doh, white glue, spray rubber, nail polish, nail hardener, gelatin, latex)
Presentation Attack Instrument series	1 PAI per source for each material Exception (Play-Doh): 3 PAI per source
Presentation attempts per visit/Attack	3
Bona fide presentations	396 per sensor (792 total)
Attacks per species	198 per sensor (equal count for all species)
Attack presentations	1386 per sensor (2772 total)
Attacker's expertise (with respect to Specialist expertise [27])	Expert
Recording length	Thermal: 7 frames/presentation Optical: full presentation is recorded

Table 3 details the dataset considering the recommendations of ISO/IEC 30107-3.

The produced PAIs had shown a consistency such that each instrument is used for all attack attempts. An exception took place when considering attacks with Play-Doh, where for every attack a new PAI was needed, this is due to the distortion caused by the pressure during attack presentation.

The presented dataset consists of 3564 fingerprint presentations (real and attack), and it is investigated in section IV to evaluate the PAD mechanism.

C. FINGERPRINT DETECTION AND VIDEO SEGMENTATION

Fingerprint detection is carried out in the software acquisition tool using the SDKs implementations for both sensors. Therefore, empty frames before or after the fingerprint placement are taken away. Segmentation is executed differently in each sensor subset due to the different sensor sizes. (a) Thermal sensor data is segmented during the acquisition such that only the central area (90×128 pixels) is captured. Partial capture has been performed as per the sensor instructions to reduce the frame acquisition time from 1 second to 0.7 second. (b) Optical sensor data segmentation is implemented to consider the sensor's surface area where the fingerprint interaction had taken place.

Figure 3 and Figure 4 demonstrate samples from both sensors for bona fide and attack presentations.

D. ALGORITHM ADAPTATION: FEATURE EXTRACTION AND CONCATENATION

As demonstrated in section III feature extraction is performed on the segmented dataset, consequently, 8× L feature dimensions represent each fingerprint presentation. Since L is fixed to 7 frames for the thermal sensor subset, then the corresponding dimensionality is fixed to 56 for all presentations. Contrariwise, presentations in the optical sensor subset differ in length (i.e. L differ in the various presentations), resulting in 8× L feature dimension per presentation.

Standard machine learning algorithms do not cope with the variation of dimensionality in different samples; thus, it is necessary to transform the dimensionality of the features for all presentations so that they fit into the learning model. The following steps are followed to transform features into a fixed dimensionality size trying to preserve the behavior of the feature using linear interpolation/decimation: First, feature extraction is executed for every presentation. Second, the number of frames per presentation is averaged across all presentations and it is found to be roughly 25 frames. Third,

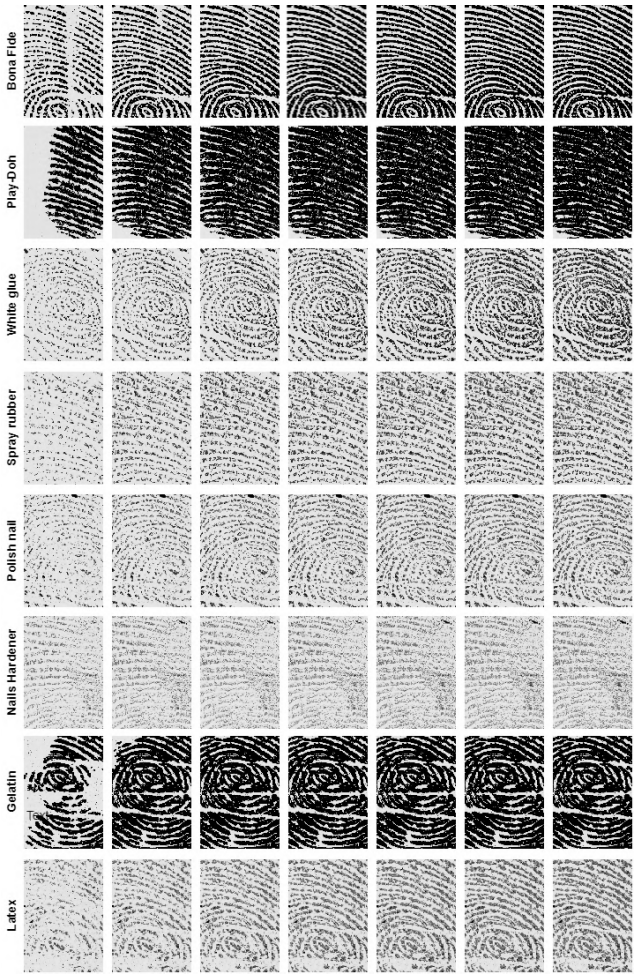


FIGURE 4. Thermal sensor captures. (Each row shows a presentation type in successive frames of a video).

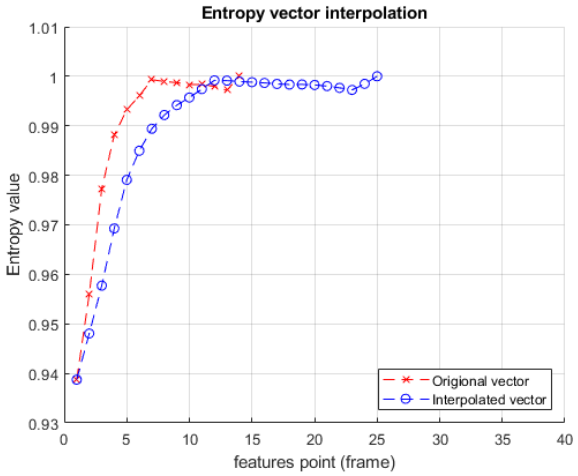


FIGURE 5. Interpolating normalized entropy of a 14 frames presentation.

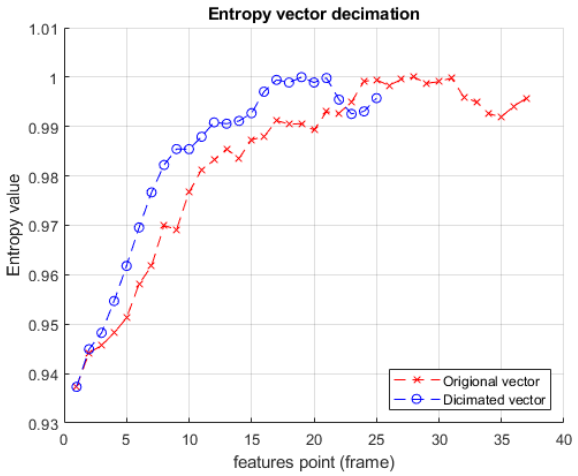


FIGURE 6. Decimating normalized entropy of a 37 frames presentation.

presentations that have less, or more than 25 frames were subject to interpolate, decimate the dimensionality of the features into 8×25points. Linear interpolation/decimation is performed as demonstrated in Figure 5 and Figure 6. Finally, all features are concatenated such as each presentation is presented by 200 dimensions.

E. PAD EVALUATION PROTOCOL

In order to evaluate the proposed mechanism on the collected dataset, each sensor's data is studied apart. We believe that for each commercial fingerprint sensor there must be an independent trained PAD model, given that each sensor captures different images' signal type, noise, and resolution. Equally important, for preserving all the details of the captured presentations, we applied the feature extraction on the raw data, i.e. no compression or pre-processing is applied to the captured data. For example, applying noise removal, contrast enhancement, and image filtering algorithms to the original image, which represents the interaction between a fingerprint/PAI and the sensor, may result in a loss in the discriminative features.

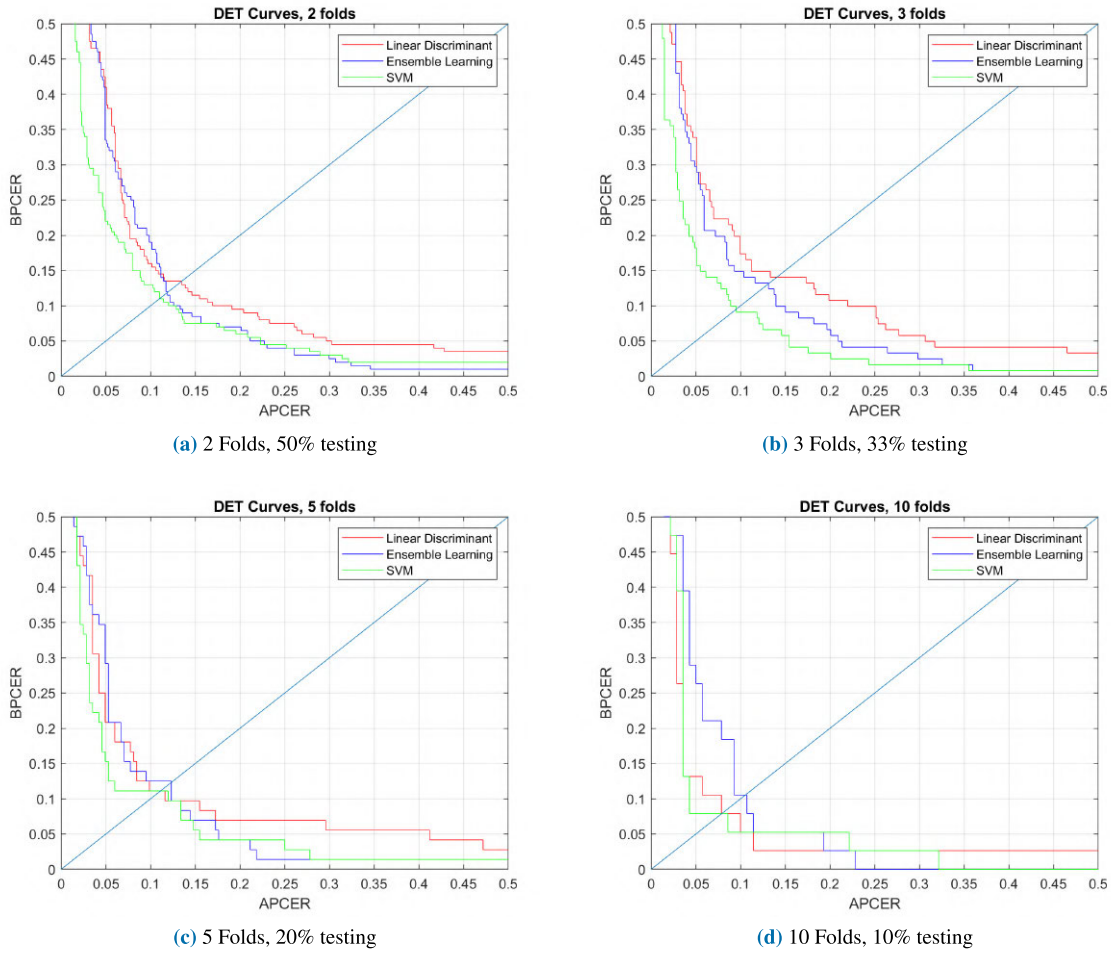
In the context of this paper, the PAD subsystem evaluation measures the ability of a PAD model to correctly determine whether a fingerprint video comes from a genuine user or an attack. The evaluation framework is defined following the international standard Biometric PAD testing and reporting ISO/IEC 30107-3. This standard states the following mandatory metrics to report a PAD subsystem performance:

1. Attack Presentation Classification Error rate (APCER): the proportion of attack presentations incorrectly classified as bona fide presentations. APCER for a specific PAI species ($\text{APCER}_{\text{PAIS}}$) is calculated using:

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right) \sum_{i=1}^{N_{PAIS}} Res_i \tag{10}$$

where N_{PAIS} is the total attacks count for a given PAI species and Res_i is 1 if the presentation is classified as an attack and 0 otherwise. The total APCER is also reported as $\text{APCER}_{\text{total}}$ to present the percentage of successful attacks considering all PAI species.

2. Bona Fide Presentation Classification Error Rate (BPCER): the proportion of bona fide presentations incorrectly classified as attack presentations. BPCER is calculated



(a) 2 Folds, 50% testing

(b) 3 Folds, 33% testing

(c) 5 Folds, 20% testing

(d) 10 Folds, 10% testing

FIGURE 7. DET Curves for PAD subsystem performance under different classification methods and partitioning. (Thermal sensor.)

using:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_{BF}} \tag{11}$$

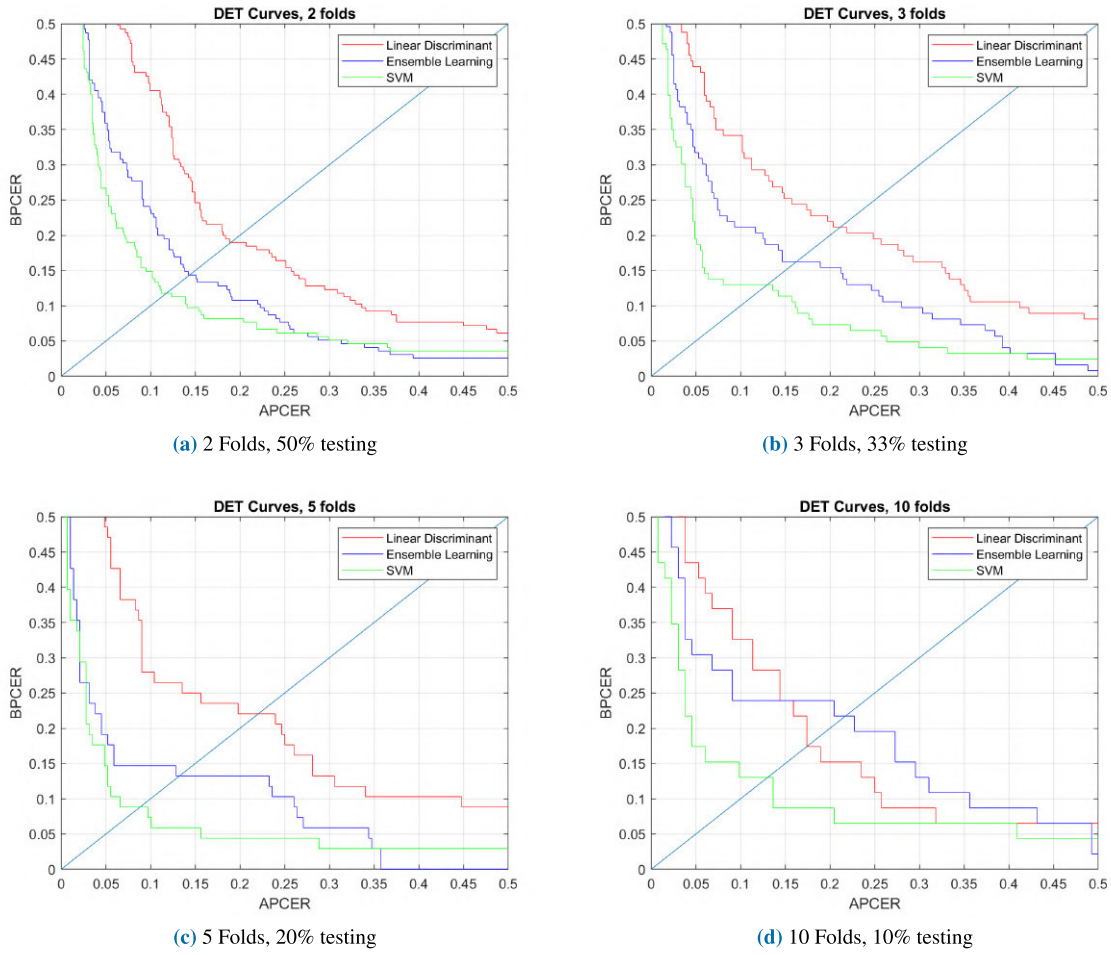
where N_{BF} is the total of bona fide presentations and Res_i is 1 if the presentation is classified as an attack and 0 otherwise. Additionally, we define $\text{BPCER}_{\text{PAIS}}$ to report the proportion of bona fide presentations incorrectly classified as specific attack species. $\text{BPCER}_{\text{PAIS}}$ can be reported, when considering a multi-class classifier, to point out the species which cause misclassification for bona fide presentations.

The evaluator has defined the non-response as no appearance of a fingerprint in successive frames of a bona fide or attack presentation. Despite that, all presentations were successful and, consequently, non-response error rates are reported to be 0.

V. PAD EVALUATION RESULTS

The proposed PAD subsystem evaluation is characterized by positive and negative error rates, $\text{APCER}_{\text{total}}$ and BPCER, as defined in the previous section. Both metrics have been calculated for three classification algorithms, each sensor apart. For reliable results, only testing data is used to conduct the evaluation, i.e. training data is merely used to train the models. For more robust accuracy estimation, k-fold cross validation is performed using 2, 3, 5 and 10 folds by three classification algorithms as demonstrated in Figure 7 and Figure 8. Moreover, Table 4 and Table 5 report BPCER values at a fixed $\text{APCER}_{\text{total}}$=0.05 and when the equal error occurs i.e. when $\text{APCER}_{\text{total}}$=BPCER.

The figures are revealing in several ways. First, classification methods show a difference in the performances. LDA and SVM methods show high contrast between a low $\text{APCER}_{\text{total}}$ and a relatively high BPCER, while in the ensemble learning method the contrast between $\text{APCER}_{\text{total}}$ and BPCER is less notable. Secondly, the number of folds does not influence the methods' performance significantly. For instance, 2 and 10 folds (consecutively 50% and 10% of the dataset) represent different sizes of the testing set, but surprisingly, the error rates are nearly the same. This might be caused by the small size of the dataset. Thirdly, the PAD mechanism shows a resemblance between the performances when considering different sensing technologies.



(a) 2 Folds, 50% testing

(b) 3 Folds, 33% testing

(c) 5 Folds, 20% testing

(d) 10 Folds, 10% testing

FIGURE 8. DET Curves for PAD subsystem performance under different classification methods and partitioning. (Optical sensor.)

From Figures 7a and 8a, we observe that at the tradeoff equal error rate, our method achieves 89% accuracy for the thermal sensor and 88.3% for the optical sensors. These results validate our underlying supposition about the statistical differences between attacks and genuine fingerprints in the dynamic scenario.

Comparing our method with the state-of-the-art methods is not as straightforward as comparing the two sensors in our experiment. We recommend considering the following factors before comparing those results with the PAD mechanisms in Table 1: (i) experiment's protocol, (ii) database characteristics, and (iii) evaluation methodology.

The next section analyzes and interprets the obtained results where attack potential is studied for each PAI species individually. Further analysis has been performed in section B aiming to enhance the PAD subsystem performance through dimensionality reduction using sequential feature selection.

A. ATTACKS STRENGTH

Different attack types are expected to have different attack potentials, a PAD mechanism may not succeed to distinguish specific attack types, while performs more successfully with other types [27]. As an illustration, Figure 9 and Figure 10 analyzes the misclassified predictions of the three classification methods in the case of 2-folds cross-validation, considering seven PAI species and multi-class classification scheme.

Broadly speaking, we found values for $APCER_{PAIS}$ and $BPCER_{PAIS}$ of the thermal subset to be lower than 5% for all attack types excluding Play-Doh and White Glue attacks.

TABLE 4. Classification performance: BPCER at fixed $APCER_{total}$ (thermal sensor).

Classifier	Number of folds	BPCER at $APCER_{total}$=5%	$APCER_{total}$=BPCER (%)
LDA	2	41	13.4
	3	33.8	14.5
	5	20.8	11.1
	10	50	19.3
Ensemble Learning	2	33.5	11.8
	3	29.7	13.1
	5	29.1	12.3
	10	47.3	19.3
SVM	2	22	11
	3	18.1	9.5
	5	15.2	11.1
	10	23.6	10.5

TABLE 5. Classification performance: BPCER at fixed $APCER_{total}$ (optical sensor.)

Classifier	Number of folds	BPCER at $APCER_{total}$=5%	$APCER_{total}$=BPCER (%)
LDA	2	57.9	18.9
	3	43.9	21.1
	5	48.5	22
	10	43.4	17.4
Ensemble Learning	2	35.9	14.3
	3	31.7	16.2
	5	19.1	13.2
	10	30.4	21.7
SVM	2	26.6	11.7
	3	19.5	13
	5	14.7	8.8
	10	17.3	13

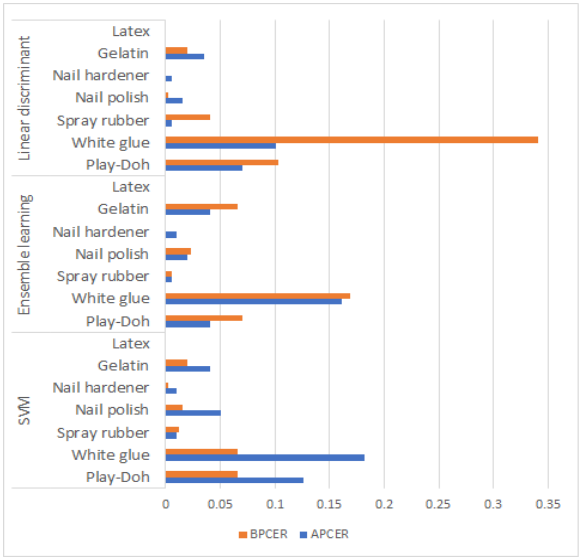


FIGURE 9. PAD subsystem performance considering $APCER_{PAIS}$, $BPCER_{PAIS}$, and 50% training and testing cross validation. (Thermal sensor.)

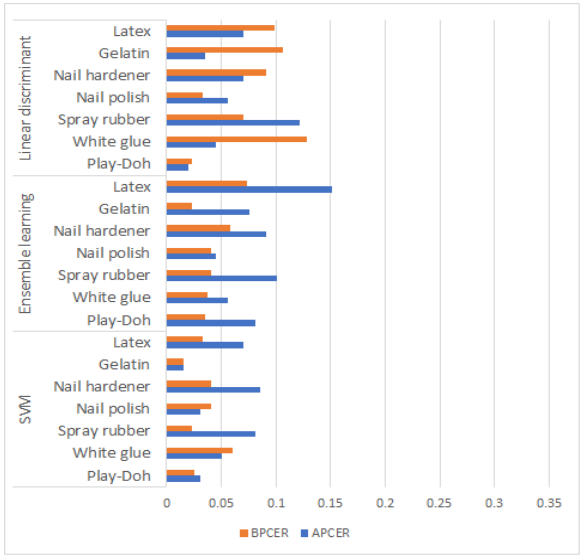


FIGURE 10. PAD subsystem performance considering $APCER_{PAIS}$, $BPCER_{PAIS}$, and 50% training and testing cross validation. (Optical sensor.)

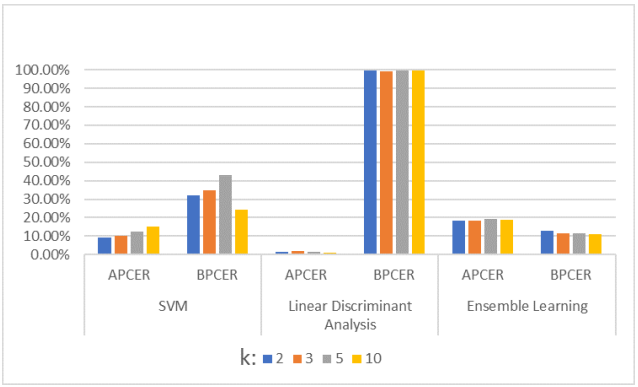


FIGURE 11. PAD subsystem performance after applying sequential feature selection. (Thermal sensor.)

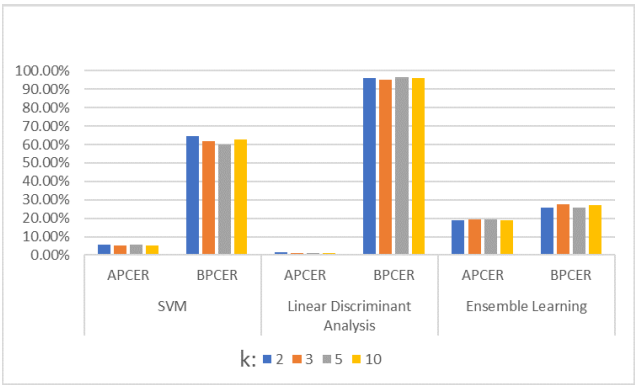


FIGURE 12. PAD subsystem performance after applying sequential feature selection. (Optical sensor.)

This lends support to the fact that different attack types have different potentials. On the contrary, the PAD mechanism shows a form of consistency for the different attacks when considering the optical sensor subset, $APCER_{PAIS}$ and $BPCER_{PAIS}$ are $5\% \pm 3\%$ for all attack species in the SVM model.

Since all attacks are performed by the same attacker, fingerprint sources (i.e. 3D molds), and attack methodology, we suggest that the attack potential of the different species varies due to the characteristics of each PAI species; nonetheless, introducing another attacker might produce different results.

B. SEQUENTIAL FEATURE SELECTION

Sequential feature selection method is used to eliminate the features that increase the prediction error. The algorithm starts by choosing one feature and calculate the corresponding prediction error. Then the rest of the features are tested one by one, and only those features which reduce the error are added to the model.

Contrary to expectations, the overall performance of the tested models is decreased compared to classification results without dimensionality reduction. Figure 11 and Figure 12

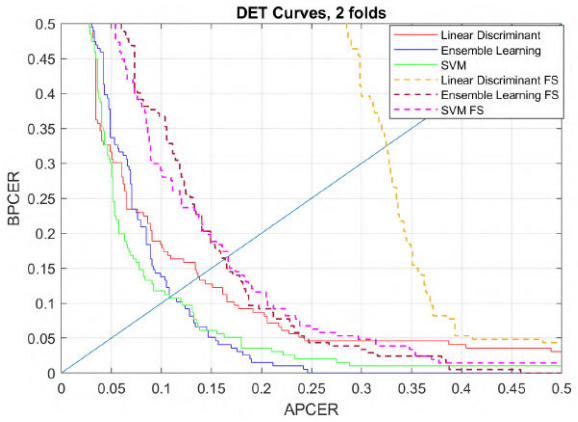


FIGURE 13. PAD subsystem performance with and without Feature Selection (FS). (Thermal sensor.)

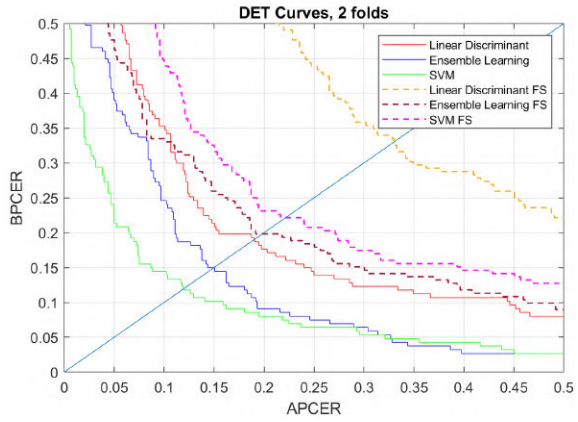


FIGURE 14. PAD subsystem performance with and without Feature Selection (FS). (Optical sensor.)

TABLE 6. Classification performance using feature selection: BPCER at fixed $APCER_{total}$. (Thermal sensor).

Classifier	BPCER at $APCER_{total}$=5%	$APCER_{total}$=BPCER (%)
LDA	95.6	32.4
Ensemble Learning	57.9	16.3
SVM	52.1	16.6

TABLE 7. Classification performance using feature selection: BPCER at fixed $APCER_{total}$. (Optical sensor).

Classifier	BPCER at $APCER_{total}$=5%	$APCER_{total}$=BPCER (%)
LDA	73.1	32.9
Ensemble Learning	47.6	19.8
SVM	65.5	22.17

demonstrate the PAD subsystem performance using 2, 3, 5, 10 folds cross validation, while Figure 13 and Figure 14 compare DET curves of feature selection for each classifier considering 2 folds cross validation.

Table 6 and Table 7 report the PAD performance after feature selection by showing BPCER at fixed APCER and the equal error rate.

Even though feature selection reduces the computational cost of the overall PAD system, it decreases the PAD performance, thus feature selection is not considered in our method.

VI. CONCLUSION

Our work has led us to the conclusion that genuine fingerprint is a rich source of information, rather than only a graphical static pattern. Having an accurate and deep understanding of fingerprint phenomena, e.g. skin elasticity, temperature, perspiration, etc. is a key for PAD solutions' development. The findings of the studies on dynamic fingerprint features support the fact that genuine fingerprints produce unique dynamic patterns.

The proposed PAD method explores the variation of eight global measures e.g. intensity (mean), contrast (std), randomness (entropy), during fingerprint presentations. Those features are concatenated to form a description of the fingerprint pattern's formation. To verify whether the description is sufficiently discriminative, different classification algorithms are tested; SVM, LDA, and ensemble learning. The evaluation is conducted using a dynamic dataset that was collected using thermal and optical sensors, 66 genuine fingerprints, and 7 PAI species.

Considering SVM classification and 50% partitioning for training and testing, we note comparable PAD performance for both sensors. Error rates are $APCER_{total}$ = BPCER= 11% for the thermal subset and $APCER_{total}$ = BPCER = 11.7% for the optical subset. Even though error rates show a resemblance for both sensors, we have shown that each PAI species has a certain attack potential. To put it differently, dominant attacks that increase error rates in the thermal subset are Play-Doh and white glue attacks, while different attack species have roughly homogeneous error rates in the optical subset.

Dimensionality reduction method has been tested seeking to enhance the PAD subsystem performance, but results were unsatisfactory compared to the original results.

The most important limitation of this investigation is the small size of the dataset, which consists of 11 independent subjects 6 fingers each. Moreover, the proposed mechanism has a limitation in distinguishing specific materials for the thermal sensor. Nevertheless, we believe our methodology could be a starting point for developing more sophisticated mechanisms.

To further our research, we intend to acquire data from new subjects, as well as investigating more sophisticated features in order to enhance the performance of the PAD subsystem.

REFERENCES

[1] A. A. Moenssens, *Fingerprint Techniques*. Philadelphia, PA, USA: Chilton Book Co, 1971.
[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.
[3] R. Ramotowski, *Lee and Gaensslen's Advances in Fingerprint Technology*. Boca Raton, FL, USA: CRC Press, 2013.
[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[5] *Information Technology—Biometric Presentation Attack Detection—Part 3: Testing and Reporting*, Standard ISO/IEC 30107-3, 2017.
[6] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surveys*, vol. 47, no. 2, pp. 1–36, Jan. 2015.
[7] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, Dec. 2014.
[8] M. S. Nixon, *Handbook of Biometric Anti-Spoofing*. Cham, Switzerland: Springer, 2019, pp. 207–228.
[9] A. Husseis, J. Liu-Jimenez, I. Goicoechea-Telleria, and R. Sanchez-Reillo, "A survey in presentation attack and presentation attack detection," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–13.
[10] T. Matsumoto, "Gummy and conductive silicone rubber fingers importance of vulnerability analysis," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2002, pp. 574–575.
[11] T. Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," in *Smart Card Research and Advanced Applications*. Boston, MA, USA: Springer, 2000, pp. 289–303.
[12] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, "Analysis of the attack potential in low cost spoofing of fingerprints," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2017, pp. 1–6.
[13] J. Spurny, M. Doleel, O. Kanich, M. Drahansky, and K. Shinoda, "New materials for spoofing touch-based fingerprint scanners," in *Proc. Int. Conf. Comput. Appl. Technol.*, Aug. 2015, pp. 207–211.
[14] S. J. Elliott, S. K. Modi, L. Maccarone, M. R. Young, C. Jin, and H. Kim, "Image quality and minutiae count comparison for genuine and artificial fingerprints," in *Proc. 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2007, pp. 30–36.
[15] M. Sandström, "Liveness detection in fingerprint recognition systems," Ph.D. dissertation, Dept. Elect. Eng., Linköping Univ., Linköping, Sweden, 2004.
[16] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body check: Biometric access protection devices and their programs put to the test," *C'T Mag.*, vol. 11, p. 114, 2002.
[17] 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.
[18] Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake finger detection based on thin-plate spline distortion model," in *Advances in Biometrics*. Berlin, Germany: Springer, 2007, pp. 742–749.
[19] J. Jia, L. Cai, K. Zhang, and D. Chen, "A new approach to fake finger detection based on skin elasticity analysis," in *Advances in Biometrics*. Berlin, Germany: Springer, 2007, pp. 309–318.
[20] 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, Feb. 2003.
[21] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 35, no. 3, pp. 335–343, Aug. 2005.
[22] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recognit.*, vol. 42, no. 3, pp. 452–464, Mar. 2009.
[23] R. Plesh, K. Bahmani, G. Jang, D. Yambay, K. Brownlee, T. Swyka, P. Johnson, A. Ross, and S. Schuckers, "Fingerprint presentation attack detection utilizing time-series, color fingerprint captures," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2019, pp. 1–8.
[24] R. Cappelli, D. Maio, and D. Maltoni, "Modelling plastic distortion in fingerprint images," in *Advances in Pattern Recognition—ICAPR*. Berlin, Germany: Springer, 2001, pp. 371–378. [Online]. Available: http://link.springer.com/10.1007/3-540-44732-6_38
[25] *VeriFinger Fingerprint Recognition Technology, Algorithm and SDK for PC, Smartphones and Web*. Accessed: Mar. 25, 2020. [Online]. Available: http://www.neurotechnology.com/verifinger.html
[26] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques," in *Proc. Int. Conf. Image Process.*, Oct. 2006, pp. 321–324.
[27] *Common Methodology for Information Technology Security Evaluation*, Standard, Common Criteria, Sep. 2012, p. 433.

ANAS HUSSEIS received the B.S. degree in communication engineering from Yarmouk University, Irbid, Jordan, in 2012, and the M.S. degree in multimedia networking from the Telecom-ParisTech, Paris-Saclay University, Paris, France, in 2017. He is currently pursuing the Ph.D. degree in electrical engineering, electronics and automation with the University Carlos III of Madrid (UC3M), Madrid, Spain. From 2012 to 2016, he was a Communication Engineer with STC. He was a Visiting Researcher with the Warsaw University of Technology, Warsaw, Poland. He was also a Researcher with Next Biometrics Research and Development, Prague, Czech Republic, in 2018, in the framework of the European Project AMBER. He is a Marie Sklodowska-Curie Research Fellow with AMBER project. His research interests include biometric recognition with a focus on presentation attack detection, biometric systems evaluation, and computer vision. He is a member of the European Association for Biometrics (EAB).

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 (UC3M), in 2010. Since 2004, she has been with UC3M. She has participated in several national and European funded projects, besides working on ID management, evaluation, and anti-spoofing mechanisms. Her research interests include biometrics and hardware/software codesign, specifically for iris biometrics.

INES GOICOECHEA-TELLERIA received the bachelor's degree in industrial electronics and automation, the master's degree in electronic systems and applications engineering, and the Ph.D. degree in electronics from the University Carlos III of Madrid (UC3M), in 2014, 2015, and 2019, respectively. She is a member of ISO/IEC JTC1 SC27, SC37, and CEN/TC 224 WG18.

RAUL SANCHEZ-REILLO (Senior Member, IEEE) received the Ph.D. degree. He is currently a Full Professor with the University Carlos III of Madrid. He is also the Head of the University Group for Identification Technologies (GUTI), 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 is an Expert in security and biometrics. He has participated in several European projects, such as eEpoch and BioSec, by virtue of being the WP Leader. He served as a member for the SC17, SC27, and SC37 Standardization Committees. He is also the Spanish Chair of SC17 and the Secretariat of SC37.