Face Presentation Attack Detection by Exploring Spectral Signatures

R. Raghavendra, Kiran B. Raja, Sushma Venkatesh, Christoph Busch
Norwegian Biometrics Laboratory, NTNU - Gjøvik, Norway
{raghavendra.ramachandra; kiran.raja; sushma.venkatesh; christoph.busch} @ntnu.no

Abstract

Presentation attack on the face recognition systems is well studied in the biometrics community resulting in various techniques for detecting the attacks. A low-cost presentation attack (e.g. print attacks) on face recognition systems has been demonstrated for systems operating in visible, multispectral (visible and near infrared spectrum) and extended multispectral (more than two spectral bands spanning from visible to near infrared space, commonly in 500nm-1000nm). In this paper, we propose a novel method to detect the presentation attacks on the extended multispectral face recognition systems. The proposed method is based on characterising the reflectance properties of the captured image through the spectral signature. The spectral signature is further classified using the linear Support Vector Machine (SVM) to obtain the decision on presented sample as an artefact or bona-fide. Since the reflectance property of the human skin and the artefact material differ, the proposed method can efficiently detect the presentation attacks on the extended multispectral system. Extensive experiments are carried out on a publicly available extended multispectral face database (EMSPAD) comprised of 50 subjects with two different Presentation Attack Instruments (PAI) generated using two different printers. The comparison analysis is presented by comparing the performance of the proposed scheme with the contemporary schemes based on the image fusion and score level fusion for PAD. Based on the obtained results, the proposed method has indicated the best performance in detecting both known and unknown attacks.

1. INTRODUCTION

Face recognition systems are widely used in many access control applications by considering the lower costs and non-intrusive imaging ability. However, the widespread deployment of the face recognition solutions have also resulted in newer ways of presentation attacks leveraging the vulnerability of sensors at capture level. The widespread availability of facial images of the targeted attacker can be used by any attacker to create a Presentation Attack Instrument (PAI) (or artefact) which can in-turn be used to gain access to the face recognition system posing as the legitimate user. The vulnerability of the face recognition system is well studied in the literature on different kinds of baseline face recognition systems as well as the commercial-of-the-shelf (COTS) that have indicated the vulnerability towards low-cost PAI species such as printed artefact, electronic display artefact and 3D masks [4].

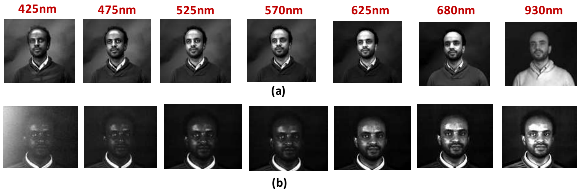


Figure 1: Example of extended multi-spectral face images from EMSPAD database (a) bona-fide (or real) samples (b) artefact samples generated using laser printer and recaptured using extended multispectral face images

Extensive studies on face Presentation Attack Detection (PAD) (or anti-spoofing or countermeasures) have resulted in various software-based techniques [4]. These developed techniques have demonstrated a reliable accuracy in detecting the presentation attacks from known artefact species, especially in the visible spectrum. However, the generalising capability of the existing PAD techniques in identifying different kinds of artefact species is still a challenge. A possible approach based on the multispectral face capture is perceived as promising alternative by the biometric community. The conventional multi-spectral face capture device will capture the face images in two different spectral bands that include visible (VIS) and near infrared (NIR) spectrum. Since the artefact species are generated from the materials with non-skin texture (e.g. plastics, electronic screen, glossy papers, silicon, rubber, latex, etc.), the use of NIR spectrum can indicate the presence of such materials as the reflective properties differ from real skin texture.

Along the lines of motivation, the applicability of multispectral face sensors for presentation attack detection has received an increasing interest in the biometric community. Early work [9] in this direction has explored the VIS and NIR spectrum to capture the face images and process them based on the color and texture features to detect the print attacks on the multispectral face recognition systems. The utility of the Short-Wave Infra-Red (SWIR) spectrum for face PAD was introduced in [8] that revealed the presence of the 3D face masks due to the reflective characteristics that are different to that of normal skin. It is interesting to note that, the 3D masks used in [8] can cover most part of the face region but parts of forehead that can be used to estimate the difference between skin and non-skin region. This may limit the applicability of the technique presented in [8] when full face mask is used without displaying any skin region. Further, the first publicly available multispectral face artefact database was presented in [1]. Experimental analysis indicated the vulnerability of the multispectral face sensor towards low-cost PAI such as the print attacks. The face PAD technique tailored to multispectral face images captured based on the $\mathrm{L}_a\mathrm{MT}_i\mathrm{F}$ descriptors was proposed in [6] that has indicated an improved performance in detecting the attacks on the publicly available multispectral face PAD database. The $\mathrm{L}_a\mathrm{MT}_i\mathrm{F}$ descriptors are used separately on VIS and NIR and decision is fused using the logical AND rule to identify the presentation attacks on multispectral face recognition sensor. Most recently, the vulnerability of the extended multispectral face sensor on print attacks was presented in [7]. Extensive experiments were further carried on extended multispectral face sensor where data was captured from seven individual spectral bands (such as 425nm, 475nm, 525nm, 570nm, 625nm, 680nm, and 930nn). Figure 1 illustrates the example of extended multispectral face images corresponding to both bona-fide (or real or normal) and artefact images from the EMSPAD database [7].

Thus, based on the available state-of-the-art techniques it can be deduced that existing algorithms have focused on exploring either colour (from VIS) or texture (from VIS and NIR) features which are limited by generalisability towards unknown attacks. To the best of our knowledge, there exists no work that explores the intrinsic characteristics of the multispectral face sensor to detect the presentation attack. Thus, in this work, we propose a framework for the multispectral face presentation attack detection by exploring the intrinsic characteristics of the sensor by analysing the spectral signature from different spectral bands. To this extent, we explore the Extended Multispectral Presentation Attack Face Database (EMSPAD) [7] to demonstrate the significance of the proposed approach. The main contributions of this work are listed as:

- Presents a novel approach of detecting the presentation attacks reliably by exploring the spectral signature of the captured face images from extended multispectral bands.
- Extensive experiments are carried out on the EMSPAD database by comparing the proposed method with the conventional texture based approaches using Binarised Statistical Image Features (BSIF) extracted individually on each band and combining the decision at score level. Further, we also present the comparison of the proposed scheme with image fusion method in which wavelet-based image fusion is explored to combine the multispectral images to form the single composite image to detect the presentation attack.
- Extensive experiments are presented to investigate the robustness of the proposed PAD scheme for the unknown attacks. To this extent, we have devised additional experiments to train the PAD methods known type of PAI (or artefact) and test them against unknown type of PAI (or artefact).

The rest of the paper is organised as follows: Section 2 describes the proposed scheme for face PAD, Section 3 presents the experimental results on the Extended Multispectral Presentation Attack Face Database (EMSPAD) and Section 4 draws the conclusion.

2. Proposed face PAD framework based on the spectral signatures

Figure 2 shows the block diagram of the proposed multispectral face PAD framework by exploring the spectral signature. The proposed framework has three main functional units, namely: (1) Extended multispectral image capture and pre-processing unit (2) Spectral signature extraction unit (3) Classification unit to separate spectral signatures using Support Vector Machine (SVM). In the following section, we discuss each of these functional components in detail.

2.1. Extended multispectral image capture and preprocessing unit

The extended multispectral images employed in this work are collected using the commercial Multispectral Camera - $SpectraCam^{\mathrm{TM}}$ [7]. The face image is captured in seven different spectral bands corresponding to wavelength of 425nm, 475nm, 525nm, 570nm, 625nm, 680nm, and 930nn. As these images are captured sequentially in

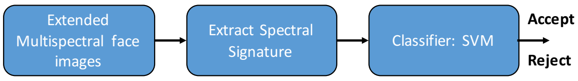

Extended Multispectral face images
Extract Spectral Signature
Classifier: SVM
Accept
Reject

Figure 2: Block diagram of the proposed face PAD approach

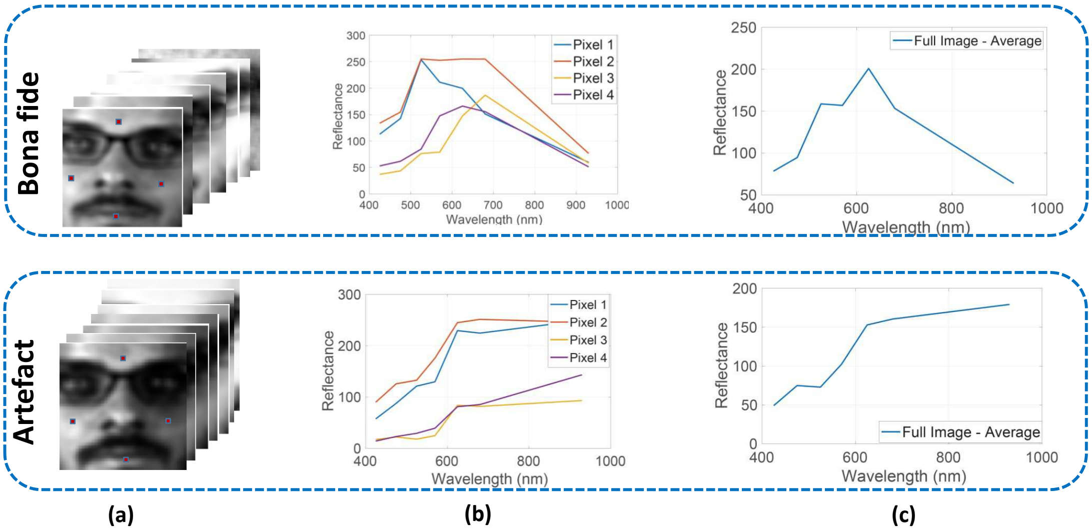


Figure 3: Illustration of the proposed face PAD approach (a) multispectral face image capture (b) illustration of the spectral signature on 4 different pixels (c) Average spectral signature obtained on multispectral images from (a)

an automatic fashion, there is no need for image registration between the spectral images captured using this sensor. Thus, for each capture, we get seven multi-spectral images that we process sequentially to extract the face region and to perform the normalisation. The face region is extracted using the Haar-based cascade detector, and normalisation is carried out to correct the minor translation and rotation effects. Thus, the detected and normalised face region is re-sized to have 120 × 120 pixels. Figure 3 (a) shows the example of the processed multispectral face images that will be treated further in next step to compute the spectral signature. Let the face detected and normalized multispectral image be $I_s = \{I_{s1}, I_{s2}, \ldots, I_{s7}\}$.

2.2. Spectral signature extraction unit

In this work, we have utilised the spectral signature of the captured and processed extended multi-spectral image I_s. It has to be noted that PAI (or artefacts) species are generated using different kinds of materials that have different spectral variability when compared to that of bona-fide face. Figure 3 illustrates the example of the spectral signatures extracted on both bona fide and artefact face samples captured using the extended multispectral sensor. Given the i^{th} interest point (x_i, y_i), the spectral signature corresponding to the multispectral image I_s can be extracted as follows:

$$S_I = [I_{s1}(x_i, y_i)||I_{s2}(x_i, y_i)|| \ldots ||I_{s7}(x_i, y_i)] \quad (1)$$

Figure 3 (b) shows the spectral signatures that are extracted from four different interest points (pixels) from the face region corresponding to bona-fide and artefact presentation. For illustration, we have considered the interest points from the fore-head, left cheek, right cheek and lip (refer Figure 3 (a)). It is interesting to note the difference in the spectral signature for both bona-fide and artefact presentation as illustrated in the Figure 3 (b). In this work, we estimate the spectral signature vector R_I by averaging over all N pixels of the extended multispectral image I_s as follows:

$$R_{\lambda_k} = \frac{1}{N \times N} \sum_{x,y} I_s(x, y, \lambda_k) \quad (2)$$

Where, N is the number of rows and columns in the image, in our case it is 120 × 120, where $k = \{1, 2, \ldots, 7\}$ indicates the number of spectral bands.

Figure 3 (c) shows the average spectral signature R_I computed on both bona fide and artefact presentation. As observed from the Figure 3 (c) there is clear distinction in profile of the spectral signature of bona-fide and artefact presentation that further justifies the applicability of the proposed method. Since, we have seven different spectral band ($K = 7$), the dimension of the $R_{\lambda_k} = 1 \times 7$.

2.3. Classification: Support Vector Machines (SVM)

In this work, we employed the linear Support Vector Machines (SVM) classifier to the make the final decision. The SVM classifier is trained using the spectral signatures R_{λ_k} from both bona fide and artefact species from the training set of EMSPAD dataset. Given the spectral signature cor-

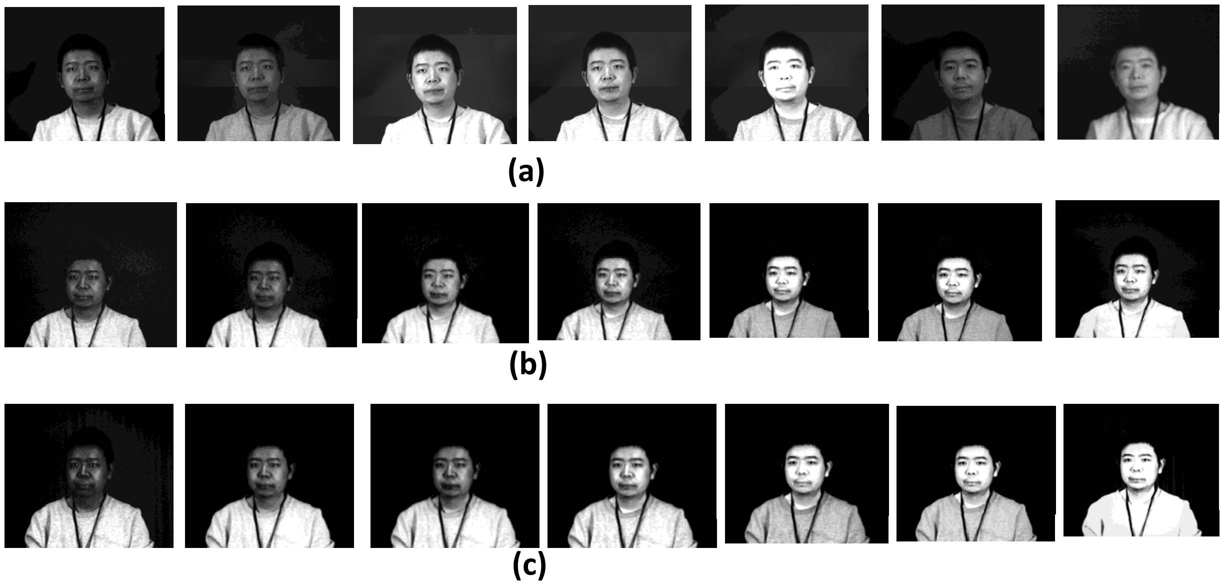


Figure 4: Example of the bona-fide and artefacts multispectral images from Extended Multispectral Presentation Attack Face Database (EMSPAD) (a) Bona fide capture (b) Laser print artefact capture (c) Inkjet print artefact capture

responding to multispectral probe face image from testing set (or probe set), the decision is made by computing the comparison score magnitude to the pre-determined threshold. The experimental protocols and the threshold selection will be discussed in the following Section 3.1.

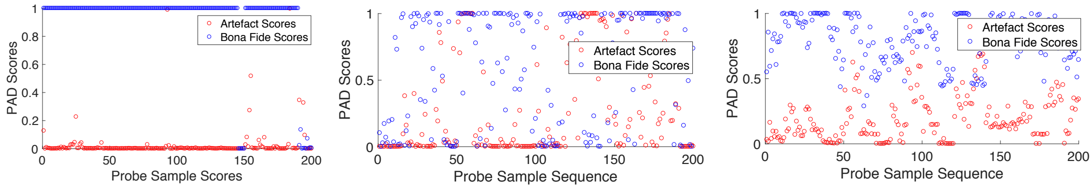
3. Experiments and Results

Extensive experiments are carried out on the Extended Multispectral Presentation Attack Face Database (EMSPAD) [7]. EMSPAD database is comprised of 50 subjects captured in two different sessions in the laboratory environment using the commercial multispectral camera - $SpectraCam^{\text{TM}}$ [7]. For each subject, five images per session are obtained in seven different spectral bands with a wavelength of 425nm, 475nm, 525nm, 570nm, 625nm, 680nm, and 930nn. Thus, the bona fide database has 50 subjects × 7 spectral bands × 2 sessions × 5 samples = 3500 image samples. EMSPAD database has two kinds of artefacts that are generated using two different printers (a) InkJet printer (HP Photosmart 5520) (b) LaserJet printer (RICOH ATICIO MP C4502) using a high-quality paper. The artefacts are generated by capturing the high-quality photo using Canon EOS 550D DSLR camera in two sessions. There are ten high-quality photos captured that correspond to five images captured in each session. These captured high-quality photos are used to generate the artefacts by printing them using a laser and inkjet printer. Finally, these artefacts are presented to the multispectral camera to perform the attacks. Thus, the artefact species corresponding to inkjet printer has a total of 50 subjects × 7 spectral bands × 10 samples = 3500 samples, and laser jet also has 3500 samples. Figure 4 shows the example of multispectral face images from bona fide and the artefact presentation from EMSPAD database.

3.1. Performance evaluation protocol

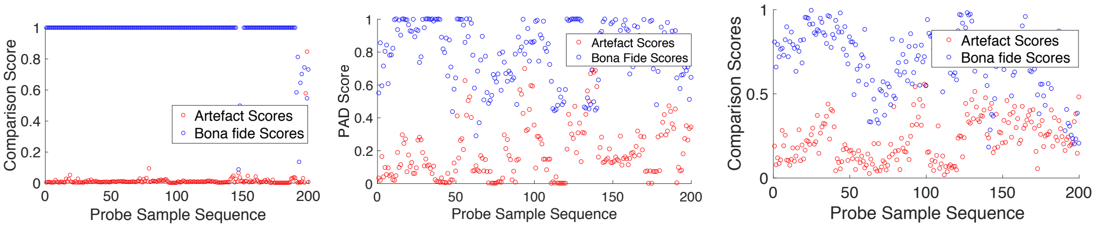
In this work, we follow the experimental protocol as described in [7] for the PAD evaluation to demonstrate the superiority of the proposed method under the same protocol. The database is divided in two independent partitions, namely: Partition-I with 10 subjects and Partition-II with 40 subjects. The Partition-I is used as the development database to determine the threshold value for bona fide and artefact species for the final classification. The Partition-II is solely utilized for the testing and reporting the results. Among 40 subjects from partition-II, we divide in two independent partitions with 20 subjects each to get Set-I and Set-II. The Set-I is used as the training set and Set-II is used as the testing set in all the experiments reported in this paper.

The performance of the PAD algorithms is presented using the following metrics [2]: Attack Presentation Classification Error Rate (APCER %): The error in classifying the attack samples as bona-fide (or normal) samples. Bona-fide Presentation Attack Classification Error Rate (BPCER %): The error in classifying the bona fide samples as artefact samples. In this work, we report the performance at



(a) Proposed scheme: Spectral Signature (b) Image fusion scheme: Wavelet based (c) Score level fusion : Sum rule

Figure 5: Distribution of the comparison scores obtained on the probe multispectral face samples and the PAI species correspond to the Laser print artefacts (Laser-Laser)



(a) Proposed scheme: Spectral Signature (b) Image fusion scheme: Wavelet based (c) Score level fusion : Sum rule

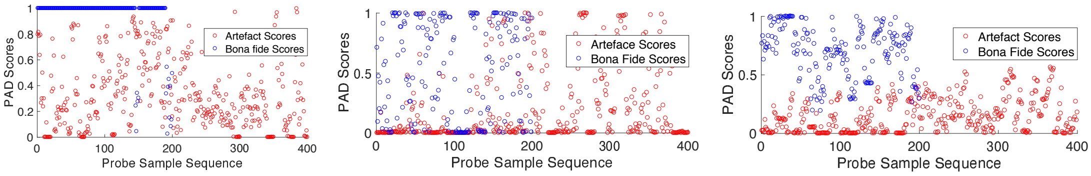
Figure 6: Distribution of the comparison scores obtained on the probe multispectral face samples and the PAI species correspond to the Inkjet print artefacts (Inkjet-Inkjet)

the operating point with APCER = 5% and 10% and also the Equal Error Rate (EER%) computed when APCER is equal to BPCER. The operating point or threshold is set corresponding to the value of APCER = 5% and 10% to report the performance of the proposed method along with the state-of-the-art PAD methods.

3.2. Results and discussion

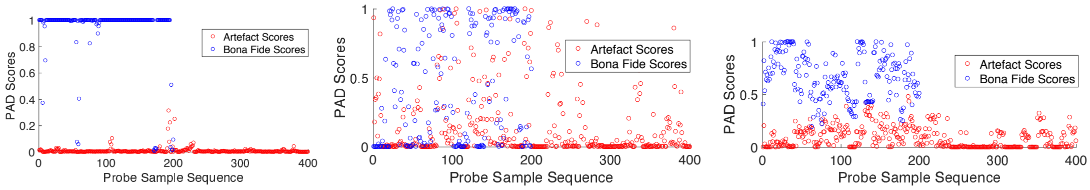
In this section, we present the quantitative results of the proposed multispectral PAD scheme together with the comparative performance of the contemporary systems based on the image fusion and comparison score fusion. As the conventional multispectral face recognition systems work by combining the images capturing with different spectral wavelength either at image level or the comparison score level [5], we also compare these two approaches with the proposed approach. The image fusion approach is based on combining the multispectral images using wavelet coefficients by taking the average of all pixels across different spectral bands [3]. Further, we have used the Binarised Statistical Image Features (BSIF) and Support Vector Machines (SVM) as the PAD scheme to detect the attacks on the multispectral face recognition system. The second comparison system is based on the comparison score (a.k.a, PAD score) level fusion such that, BSIF-SVM scheme is evaluated independently on each spectral band and the corresponding PAD scores are combined using the sum rule to make the final decision on either bona fide or attack presentation. In this work, we have selected BSIF-SVM by considering it's robustness and accuracy on the detecting the artefact species, especially from the print attack on the extended multispectral face database [7].

To effectively quantify the performance of the proposed scheme, we carried out two different experiments namely: *Experiment 1:* This experiment aims at evaluating the performance of the PAD techniques on the known attack. Thus, the PAD methods are trained and tested on the same artefact species. Thus, this experiment has two protocols such as: training and testing with Laser print artefact (Laser-Laser) and training and testing with Inkjet print artefact (Inkjet-Inkjet) independently. In this experiment, we employ images from 20 Subjects × 10 samples = 200 bona fide and artefact scores from the PAD module that corresponds to the testing set. *Experiment 2:* This experiment is designed to evaluate the performance of the PAD methods to unknown attacks. Thus, this experiment has two protocols in which the first protocol is based on training the PAD modules with Laser print artefact and testing with Inkjet print artefact (indicated as Laser-Inkjet) and the second protocol is based on training the PAD module with Inkjet print artefact and testing with Laser print artefacts (indicated as Inkjet-Laser). In this experiment, we have employed 20 subjects × 10 sam-



(a) Proposed scheme: Spectral Signature (b) Image fusion scheme: Wavelet based (c) Score level fusion : Sum rule

Figure 7: Distribution of the comparison scores obtained on the probe multispectral face samples and the PAI species when training data corresponds to Inkjet print artefacts and testing data corresponds to Laser print artefacts (Inkjet-Laser)



(a) Proposed scheme: Spectral Signature (b) Image fusion scheme: Wavelet based (c) Score level fusion : Sum rule

Figure 8: Distribution of the comparison scores obtained on the probe multispectral face samples and the PAI species when training data corresponds to Laser print artefacts and testing data corresponds to Inkjet print artefacts (Laser-Inkjet)

ples = 200 bona-fide scores that corresponds to the testing set and 20 subjects × 10 samples = 200 artefact species scores that corresponds to both training and testing set of the artefact species (independent on Laser and inkjet print artefact).

Figure 5 illustrates the PAD score distribution of the proposed scheme and the scores obtained from image fusion and score level fusion obtained on the artefact species corresponding to the Laser print (Laser-Laser). It can be observed that, the proposed PAD scheme shows better separation of artefact and bona fide scores indicating better performance as compared to combining the information of spectral bands of both image and comparison score level fusion. Table 1 indicates the quantitative performance of the proposed scheme on Laser-Laser protocol when compared to the performance of both image fusion and comparison score level fusion methods. The proposed scheme has indicated the best result with an EER of 3.50% (see Figure 9 (a)) and a BPCER of 1 % at APCER = 5% and BPCER = 0% at APCER = 10%.

Figure 6 illustrates the PAD score distribution of the proposed scheme and the contemporary schemes based on image fusion and comparison score level fusion on the inkjet print artefacts (Inkjet-Inkjet). It can also be observed that the proposed PAD scheme shows good separation between artefact and bona fide scores when compared with both image and comparison score level fusion. Table 1 indicates the quantitative performance of the proposed scheme that indicates the best performance with EER of 1% (see Figure 9 (a)) and a BPCER of 0 % at APCER = 5% and BPCER = 0% at APCER = 10%.

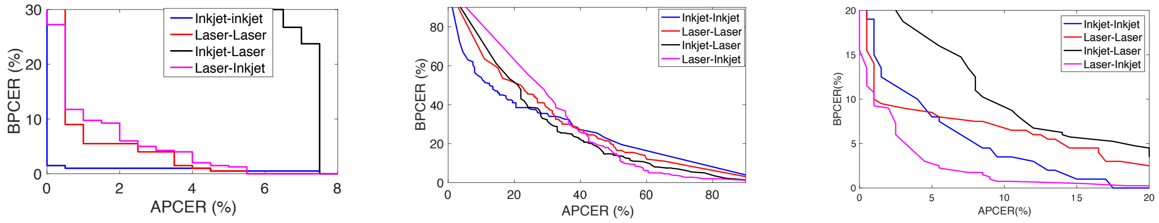
Thus, based on the experimental results obtained on both Laser-Laser and Inkjet-Inkjet in which the PAD systems are trained and tested on the same artefacts, it can be noted that performance of the proposed method has indicated best results with the lowest error rates.

Figure 7 illustrates the PAD score distribution of the proposed scheme and the contemporary schemes based on image fusion and comparison score level fusion when Inkjet print artefact is used to train the systems and Laser print artefact is used test the systems (Inkjet-Laser). In this experiment, 400 Inkjet print artefacts are used for training and 400 Laser print artefact is used for the testing. It can observed here that, the artefact score distribution is spread close to the bona fide score presentation that has resulted in the reduced performance of the proposed method. However, similar observation is also valid for the image fusion and comparison score level fusion schemes. In spite of this, the proposed scheme has indicated the best performance with the EER of 7.62 % (see Figure 9 (a)) and a BPCER of 3.75 % at APCER = 5% and BPCER = 0% at APCER = 10%.

Figure 8 illustrates the PAD score distribution of the proposed scheme and the contemporary schemes based on image fusion and comparison score level fusion when Laser print artefact is used to train the systems and Inkjet print artefact is used test the systems (Laser-Inkjet). It is inter-

Table 1: Quantitative performance of the proposed method

Method	Training-Testing	EER (%)	BPCER @	
			APCER = 5%	APCER = 10%
Score fusion Approach	Inkjet-Inkjet	9.20	23.50	15.00
	Laser-Laser	7.75	14.50	1.00
	Inkjet-Laser	9.20	23.50	15.00
	Laser-Inkjet	4.00	5.00	3.50
Image Fusion Approach	Inkjet-Inkjet	33.25	66.50	63.00
	Laser-Laser	32.50	83.50	69.00
	Inkjet-Laser	30.75	86.00	75.70
	Laser-Inkjet	32.50	81.50	67.00
Proposed Approach	Inkjet-Inkjet	**1.00**	**0.00**	**0.00**
	Laser-Laser	**3.50**	**1.00**	**0.00**
	Inkjet-Laser	**7.62**	**3.75**	**0.00**
	Laser-Inkjet	**3.00**	**0.50**	**0.00**



(a) Proposed scheme: Spectral Signature (b) Image fusion scheme: Wavelet based (c) Score level fusion : Sum rule

Figure 9: EER performance of the proposed scheme and the state-of-the-art schemes on four different protocols corresponding to two different experiments on EMSPAD database

esting to observe for the separation of bona fide and artefact samples with the proposed scheme when compared with the contemporary methods. The proposed method has demonstrated the best performance with the EER of 3.00 % (see Figure 9 (a)) and a BPCER of 0.50 % at APCER = 5% and BPCER = 0% at APCER = 10%.

Based on the extensive experiments carried out on four different protocols, the best performance of the proposed scheme has been revealed on both known and unknown attacks. Since the proposed method is based on the spectral signature that are characterized based on the reflective properties of the captured image, it can reliably detect and differentiate the skin reflectance when compared to that of the artefact (or material used to generate the artefact).

4. Conclusion

Presentation attack detection techniques are widely studied, especially, for the visible spectrum face recognition. However, the use of extended multispectral face sensor for face PAD detection is gaining momentum as they can be used to detect low cost attacks based on artefacts such as printed photo attack. This work has explored the intrinsic characteristics of the extended multispectral sensor by characterising the spectral signatures to quantify the captured images as bona fide or artefact. The spectral signature is a unique feature that can quantify the reflective properties of the captured images and the applicability of the spectral signatures can robustly detect the presentation attacks on extended face recognition sensors. Furthermore, as the spectral characteristics of the normal skin is very different than the materials used for the presentation attacks when imaged from extended spectral camera, the proposed scheme can also be used to detect the unknown attacks. Extensive experiments are carried out on the publicly available Extended Multispectral Presentation Attack Face Database (EMSPAD) comprising of 50 subjects with two different

Presentation Attack Instruments (PAI) generated using two different printers. Experiments are designed in four different protocols in which first two protocols are based on detecting the known attacks and thus, the proposed method is trained and tested on the same PAI (or artefact). The next two protocols are based on the evaluating the proposed method for the unknown attacks and thus, the proposed scheme is trained and tested using different PAIs. Based on the obtained results, the proposed method has illustrated an improved performance when compared with the contemporary methods based on the image fusion and the PAD score fusion using SUM rule. The proposed method has also indicated the best performance for known and unknown attacks with the performance of BPCER = 0% at APCER = 10%. The future work will focus on extracting the spectral signature from the prominent region of the face (e.g. cheeks, eye region) and establish a weighting strategy to characterise the spectral signature with higher degree of accuracy.

Acknowledgment

This work is carried out under the funding of the Research Council of Norway (Grant No. IKTPLUSS 248030/O70).

References

[1] I. Chingovska, N. Erdogmus, A. Anjos, and S. Marcel. Face recognition systems under spoofing attacks. In *Face Recognition Across the Imaging Spectrum*, pages 165–194. Springer, 2016.

[2] International Organization for Standardization. *ISO/IEC WD 30107-3. Information Technology - Biometric presentation attack detection - Part 3: Testing and Reporting*, 2015.

[3] H. Li, B. Manjunath, and S. K. Mitra. Multi-sensor image fusion using the wavelet transform. In *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, volume 1, pages 51–55, 1994.

[4] R. Raghavendra and C. Busch. Presentation attack detection methods for face recognition system - A comprehensive survey. *ACM Computing Surveys*, 50(1(8)):1–45, 2017.

[5] R. Raghavendra, B. Dorizzi, A. Rao, and K. Hemantha. Particle swarm optimization based fusion of near infrared and visible images for improved face verification. *Pattern Recognition*, 44(2):401 – 411, 2011.

[6] R. Raghavendra, Kiran Raja, S. Marcel, and C. Busch. Face presentation attack detection across spectrum using time-frequency descriptors of maximal response in laplacian scale-space. In *Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pages 1–8. IEEE, 2017.

[7] R. Raghavendra, Kiran Raja, V. Sushma, C. Faouzi, and C. Busch. On the vulnerability of extended multispectral face recognition systems towards presentation attacks. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pages 1–8. IEEE, 2017.

[8] H. Steiner, A. Kolb, and N. Jung. Reliable face anti-spoofing using multispectral swir imaging. In *2016 International Conference on Biometrics (ICB)*, pages 1–8, June 2016.

[9] D. Yi, Z. Lei, Z. Zhang, and S. Z. Li. Face anti-spoofing: Multi-spectral approach. In *Handbook of Biometric Anti-Spoofing*, pages 83–102. Springer, 2014.