Iris Print Attack Detection using Eye Movement Signals

Mehedi Hasan Raju
Dillon J. Lohr
Oleg V. Komogortsev
m.raju@txstate.edu
djl70@txstate.edu
ok11@txstate.edu
Texas State University
San Marcos, Texas, USA

ABSTRACT

Iris-based biometric authentication is a wide-spread biometric modality due to its accuracy, among other benefits. Improving the resistance of iris biometrics to spoofing attacks is an important research topic. Eye tracking and iris recognition devices have similar hardware that consists of a source of infra-red light and an image sensor. This similarity potentially enables eye tracking algorithms to run on iris-driven biometrics systems. The present work advances the state-of-the-art of detecting iris print attacks, wherein an imposter presents a printout of an authentic user's iris to a biometrics system. The detection of iris print attacks is accomplished via analysis of the captured eye movement signal with a deep learning model. Results indicate better performance of the selected approach than the previous state-of-the-art.

CCS CONCEPTS

• **Human-centered computing** → **HCI theory, concepts and models**; • **Computing methodologies** → **Machine learning**.

KEYWORDS

eye movement, liveness detection, iris, print attack detection, biometrics, eye tracking

ACM Reference Format:
Mehedi Hasan Raju, Dillon J. Lohr, and Oleg V. Komogortsev. 2022. Iris Print Attack Detection using Eye Movement Signals. In *2022 Symposium on Eye Tracking Research and Applications (ETRA '22), June 8–11, 2022, Seattle, WA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3517031.3532521

1 INTRODUCTION

Biometrics aim to differentiate a human from another according to their physical, physiological and behavioral characteristics, especially as a means of verifying identity [Jain et al. 2007]. Biometrics-based recognition systems are more convenient than typical methods such as password-based authentication. Contemporary research on common biometric modalities such as iris-, fingerprint- and facial-recognition has indicated the ability of these modalities to achieve high recognition accuracy with low computational resources [Chatterjee et al. 2017; Gragnaniello et al. 2015a; Rigas and Komogortsev 2014]. Eye movement biometrics is a relatively new research direction that investigates opportunities for authenticating people based on eye movements [Friedman et al. 2017; Jäger et al. 2019; Lohr et al. 2021; Rigas and Komogortsev 2015]. Eye movement biometrics can also be paired with iris recognition in a multimodal biometrics system to help defend against spoof attacks.

The texture of the iris is highly unique and temporally persistent, making iris biometrics very accurate provided that the iris image quality is high. However, iris biometrics is still a relative static modality which presents an opportunity for circumvention via a printout of an iris with a hole for a pupil [Komogortsev et al. 2015]. An intruder can use soft, colored and textured contact lenses as presentation attack instruments (PAIs) [Kaur et al. 2019]. Despite having a few security advantages over other biometric modalities, iris-based biometrics systems show vulnerability to spoofing attacks such as presentation attacks [Czajka and Bowyer 2018; Sajjad et al. 2019; Tolosana et al. 2019].

This research paper proposes a deep learning methodology to detect iris print attack based on eye movement signal (EMS) analysis. Spoofing attacks in iris-based biometrics systems can be opposed and prevented via the presented methodology. Although contemporary iris recognition devices have built-in anti-spoofing attack systems, intruders have already developed a way to bypass these defensive measures [Czajka and Bowyer 2018]. Thus, there is clear need for anti-spoofing measures that are more robust in terms of their ability to detect spoofs quickly and efficiently.

In this work, we propose and evaluate a deep learning architecture based on a residual network (ResNet) [He et al. 2016b] for the detection of iris print attacks. We train a custom ResNet that receives as input a relatively small sample of an EMS and outputs whether that signal originates from a real eye or an iris printout. The proposed deep learning method is evaluated on the Eye Tracker Print-Attack Database (ETPAD v2) [Rigas and Komogortsev 2015] dataset. Dataset contains data from two presentation attack scenarios. The model learns to detect whether an EMS originates from real eye movements or from an iris printout. We compare our model against the state-of-the-art statistical baseline by Rigas & Komogortsev [Rigas and Komogortsev 2015].

In this paper, our contributions include:

ETRA '22, June 8–11, 2022, Seattle, WA, USA

ACM ISBN 978-1-4503-9252-5/22/06…$15.00
https://doi.org/10.1145/3517031.3532521

- Providing a strong baseline for learning-based evaluation of iris print attack detection based on EMS.
- Using a very short time interval (1.5 s) for evaluation.
- Outperforming the previous state-of-the-art in this domain which was based on a statistical method [Rigas and Komogortsev 2015].

2 PRIOR WORK

Various iris presentation attack detection (PAD) approaches have been proposed over the last decade. Iris PAD approaches can be categorized as sensor- and feature-level approaches [Galbally and Gomez-Barrero 2016], or as software- and hardware-based approaches [Pala and Bhanu 2017]. There is no firm rule in categorizing these approaches; it varies based on different conditions. We categorize iris PAD approaches based on the format of the input given to the detection system: 1) iris/eye imaged-based or 2) EMS-based. Recent papers such as [Agarwal and Jalal 2021; Czajka and Bowyer 2018] present a comprehensive review and analysis of the state-of-the-art approaches for iris PAD. Here we will discuss approaches related to our proposed method, i.e., approaches based on machine learning and deep learning.

Among the image-based approaches, the general trend is to analyze image texture as in [Zhang et al. 2011]. Basic steps of an image-based approach include image segmentation, image normalization, feature selection/extraction and classification [Agarwal and Jalal 2021]. The procedure to execute those steps varies between research papers. For example, one study [Agarwal et al. 2020] employed Daugman's integro-differential operator for image segmentation, proposed the Local Binary Hexagonal Extrema Pattern [Agarwal et al. 2021] for the description of texture features of counterfeit irises, incorporated the extracted features into a classification scheme based on Support Vector Machines (SVMs), and used Dempster-Shafer theory for decision-level fusion. Another study [Dronky et al. 2021] proposed a liveness detection system with Binarized Statistical Image Features (BSIF) [Kannala and Rahtu 2012] and also used SVMs for classification. Three different filters were applied before BSIF computation to highlight the discriminative features of the iris. BSIF is based on Local Binary Patterns [Ojala et al. 2002] which had been used as a descriptor in many prior iris anti-spoofing studies such as [Fathy and Ali 2018; Gragnaniello et al. 2015b; Hu et al. 2016].

Deep learning approaches which take images as input are also notable to mention in iris PAD research. In [He et al. 2016a], the authors came up with a multi-patch convolutional neural network (CNN) architecture where the normalized images were first split into multiple patches. Yan et al. [Yan et al. 2018] proposed hierarchical multi-class classification for CNN-based iris liveness detection. Kimura et al. [Kimura et al. 2020] tuned the hyperparameters of the CASIA algorithm from the LivDet-Iris 2017 competition [Yambay et al. 2017], significantly reducing the attack presentation classification error rate (APCER) and the bona fide presentation classification error rate (BPCER).

In image-based techniques, the images are directly used in the system to extract distinctive iris characteristics. Any degradation of the image quality due to noise, recording procedure fault, hardware used, etc. has a high impact on the accuracy of such systems. By comparison, EMS-based approaches are relatively robust to iris image quality. Distinctive features for resisting spoof attacks have been found in eye movements [Komogortsev et al. 2015]. So, EMS-based PAD approaches are worth mentioning as a competitive alternative to iris image-based approaches.

Rigas and Komogortsev [Rigas and Komogortsev 2014] proposed an algorithm based on gaze-related features that could determine whether an EMS originated from a live eye or an iris printout. That work was later extended with a statistical approach by [Rigas and Komogortsev 2015] to incorporate a new set of features. In the latter approach, an EMS was first decomposed into elementary units, and then local features were extracted from each unit and aggregated across all units in the signal. The latter approach is the current state-of-the-art for EMS-based iris PAD. Understanding that contemporary machine learning methods may outperform statistics-based approaches on a variety of tasks, we have created and evaluated a deep learning model that performs EMS-based iris PAD.

3 METHODOLOGY

A simple block diagram showing the workflow of the proposed deep learning method is shown in Fig. 1.

3.1 Dataset

We used the ETPAD v2 [Rigas and Komogortsev 2015] dataset which is publicly available.[1] This dataset consists of 1200 eye movement recordings and 400 iris images from 200 subjects. Among the 200 subjects (female – 101; male - 99), 96 had normal vision and the rest had corrected-to-normal vision. Each subject was recorded twice to produce 400 eye movement recordings. All eye movement data was captured using an EyeLink 1000 eye tracker, which monocularly tracked the left eye at 1000 Hz. The recordings of iris images were captured using a CMITECH BMT-20 iris imager [cmi 2021], which can capture iris images at a resolution of 640×480 pixels.

Visual stimulus for the experiment was a fixation point which was placed carefully at a visual angle of 3.5° above the head straight eye point. Subjects were given instruction to look on the stimulus for 15 seconds in each session. Subject's head was 550 millimeters away from the center of the screen where the stimulus was positioned. In order to collect the data for attack scenarios printouts was adjusted in front of participants head (fastened to an eye patch). Other than placing the iris printouts in front of real eye, every other experimental conditions were kept same.

Pupil Center Corneal Reflection (PCCR) technique was used in gaze estimation in-case of both live and spoof data collection. More detailed information about the experimental setup and dataset can be found in [Rigas and Komogortsev 2015].

3.2 Data Preprocessing

We calculated the channel-wise (different for horizontal and vertical positional values) sample-to-sample differences scaled by the sampling rate (i.e., instantaneous velocity) to create velocity signals. These velocity signals were fed into the network instead of raw positional values. So, the velocity signal generated from the eyelink gaze position value is the input to our proposed network.

[1] https://userweb.cs.txstate.edu/~ok11/etpad_v2.html

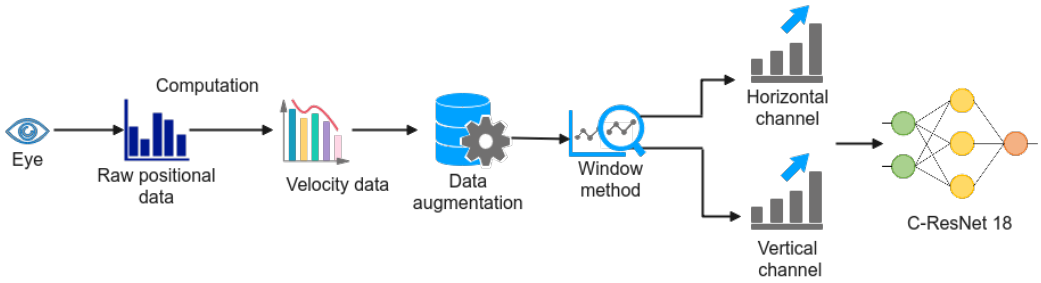

Figure 1: Block diagram of the proposed deep learning methodology.

Each eye movement recording of an individual participant is 15 seconds long. In the data augmentation step, we split each recording into overlapping windows using a strided window approach with window size = 1500 ms and stride = 125 ms. So, after this step we feed the network windows = 1500 ms length each to the network. After making windows, we replace NaN values with zeroes. Signals in the train, test and validation sets were z-score scaled using the channel-wise mean and standard deviation computed across all recordings in the train set.

3.3 Network architecture

We employed a customized version of the ResNet 18 [He et al. 2016b] architecture and named it C-ResNet 18. In C-ResNet 18, we made several changes compared to the basic ResNet 18. The main reasons behind the change are making it compatible to our problem statement, dataset and overall better performance in terms of evaluation metrics. We changed 2D convolutions to 1D, altered how skip connections were used, and changed the number of input and output channels in each convolutional block. In short, C-ResNet 18 has 17 convolutional blocks, followed by global average pooling, a flatten layer and a linear (fully-connected) layer. After each convolution, we apply batch normalization (BN) and the ReLU activation function. The network architecture is shown in Fig. 2.

3.4 Training & Evaluation

Performance of the proposed model was assessed in terms of binary classification accuracy, an assessment of whether a given EMS originates from a live or fake eye. The proposed deep learning model is trained on the ETPAD v2 dataset. The whole dataset is partitioned into subject-disjoint train, test and validation sets. The whole datset has been split into train, test, validation in a ratio of 60-20-20. Among the 200 subjects (2 sessions per subject), 120 subjects are used to train the model, 40 subjects are used to test the model and 40 subjects were kept untouched until the very end as the validation set to evaluate the model without any kind of information leak. The model makes liveness predictions based on 1500 ms (1.5 s) of eye movement velocity signal.

The model employs Kaiming initialization [He et al. 2015], as we employed ReLU as the activation function in C-ResNet 18. The model was optimized using the binary cross entropy (BCE) loss and AdamW [Loshchilov and Hutter 2019] optimizer, with learning rate = 3×10^{-4} and weight decay = 1×10^{-5}, with all other optimizer parameters set to default. Early stopping was used to reduce overfitting. Loss was tracked for early stopping and patience of 5 was used for it. The model has stopped training after 13 epochs with batch size of 64 because of early stopping.

We ran the experiments for two different spoofing attack scenarios: first scenario - where attack was carried both in calibration and stimulus presentation phase and second scenario - where calibration phase was skipped as some eye trackers do not require re-calibration. More detail about attack scenarios are in Section 3.6. We compare our deep learning model against a statistical baseline using the same dataset and similar subject-disjoint train, test and validation splits.

3.5 Performance evaluation metrics

We simulate each of the presentation attacks on our model and evaluate its performance using standard ISO/IEC 30107-3 assessment metrics defined in Table 1. During our simulated attacks, we treat recordings using printed iris images as "spoof" samples and recordings by live irises as "live" samples.

3.6 Attack Scenarios

Live images from 200 different subjects are used to create the printouts for presentation attacks. Two different attack scenarios have been considered in this paper, similar to those explored in [Rigas and Komogortsev 2015].

3.6.1 Attack Scenario-I (SAS-I):. The spoofing attack is carried out in the first scenario both at the calibration and stimulus presentation phases. It should be noted that during the calibration stage, the attacker must make small directional movement to carry the more peripheral points into the field of view, simulating natural eye movements. The distortions in SAS-I are caused by both the calibration stage and the inconsistency in pupil and corneal reflection positioning during the stimulus presentation stage.

3.6.2 Spoofing Attack Scenario II (SAS-II):. Spoofing attack is only carried out during the stimulus presentation stage in the second scenario. The calibration stage is carried out in this case with the attacker's own eye. This example simulates the situation where calibration is not performed. Since some eye trackers may not need re-calibration after the initial calibration, we wanted to test this scenario. Only the inconsistent orientation of the pupil and corneal

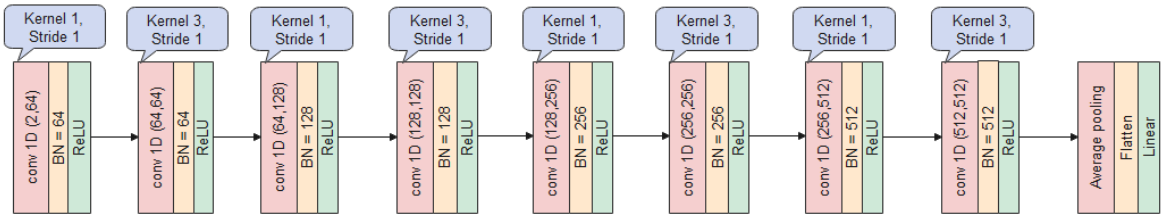

Figure 2: Network Architecture of C-ResNet 18 (Legend: ReLU-Rectified Linear Unit, BN-Batch Normalization)

Table 1: Performance metrics along with definition and computational formula (Legend: APCER-Attack Presentation Classification Error Rate, NPCER-Normal Presentation Classification Error Rate, ACR- Average Classification Rate, ACER-Average Classification Error Rate, TP-True Positive, TN-True Negative, FP-False Positive, FN-False Negative)

Metric	Definition	Formula
APCER	The percentage of "spoof" samples that are incorrectly classified as "live"	$\frac{FP}{TN + FP}$
NPCER	The percentage of "live" samples that are incorrectly classified as "spoof"	$\frac{FN}{FN + TP}$
ACR	The average percentage of correctly classified test feature vectors (either "live" or "spoof")	$100\% - \frac{APCER + NPCER}{2}$
ACER	The average percentage of misclassified test feature vectors (either "live" or "spoof")	$100\% - ACR$

reflection during the eye-tracking process causes signal disturbance in this case.

4 RESULT

Results are shown in Table 2 for the proposed deep learning model, C-ResNet 18. When trying to strike a balance between our model's performance and the amount of EMS required to make predictions, we found that there was a tie between 1500 ms and 2000 ms. Considering the results from all the metrics in two attack scenarios, we found that the proposed model achieved 5 of 10 best result at 1500 ms and rest at 2000 ms. To break the tie between input sizes of 1500 and 2000 ms, we chose 1500 ms in favor of the lower recording duration.

For more visual comparison, the results are also plotted in Fig. 3. In addition to the performance metrics defined in Table 1, we also calculated equal error rate (EER), which is the point on a receiver operating characteristic (ROC) curve where false acceptance rate (FAR) and false rejection rate (FRR) are equal.

5 DISCUSSION

From Table 2, we can see our proposed deep learning model correctly classified 98.06% and 87.78% of all 1.5 s windows from the SAS I and SAS II datasets, respectively. We also see that our model tends to classify "spoof" samples accurately, which is reflected by the relatively low APCER, but it has room for improvement when classifying "live" samples, which is reflected by the relatively higher NPCER. In other words, the model is quite selective when it comes to classifying a sample as "live," especially in SAS II.

5.1 Comparison against statistical approach

Our proposed deep learning model has been compared to the state-of-the-art statistical baseline [Rigas and Komogortsev 2015] across the whole recording here in Table 3.

There is no other model/approach which deals with print attacks using eye movement signal other than by [Rigas and Komogortsev 2015]. Their approach was statistical so apple-to-apple comparison is not possible. However, their approach uses the same dataset and makes classifications decision based on whole-recording we aggregated liveness classifications across all non-overlapping windows from a given recording for our model to make it fair comparison.

If more than 50% of the windows from a recording have been correctly classified then we considered that particular recording has been classified accurately. The >50% requirement employed in the proposed work was done to account for the fact that the proposed model operates on 1.5 seconds of data at a time, whereas [Rigas and Komogortsev 2015] operated on entire recordings at a time.

Our deep learning model is capable of perfectly classifying the live and fake EMS across the whole recording whereas ACR for the statistical baseline was 95.4% and 96.5% for SAS I and SAS II, respectively.

Table 2: Results for C-ResNet 18 across different recording durations for both attack scenarios. Arrows indicate whether a larger or smaller value is better. The recording duration that best balances performance and data requirements is highlighted in yellow.

Recording duration (ms)	ACR (%) ↑		APCER (%) ↓		NPCER (%) ↓		ACER (%) ↓		EER (%) ↓	
	SAS I	SAS II	SAS I	SAS II	SAS I	SAS II	SAS I	SAS II	SAS I	SAS II
250	96.55	85.17	1.86	4.26	5.04	25.40	3.45	14.83	4.89	20.96
500	97.24	86.55	0.69	3.06	4.83	23.84	2.76	13.45	4.64	19.74
750	97.47	87.40	0.46	2.24	4.61	22.96	2.53	12.60	4.42	19.02
1000	97.86	87.68	0.18	1.43	4.11	23.21	2.14	12.32	3.95	19.06
1500	98.06	87.78	0.14	1.25	3.75	23.19	1.94	12.22	3.62	19.02
2000	98.04	87.95	0.00	1.61	3.93	22.50	1.96	12.05	3.78	18.61
3000	97.66	87.03	0.00	1.88	4.69	24.06	2.34	12.97	4.48	19.69
4000	97.71	87.08	0.00	1.25	4.58	24.58	2.29	12.92	4.38	19.93

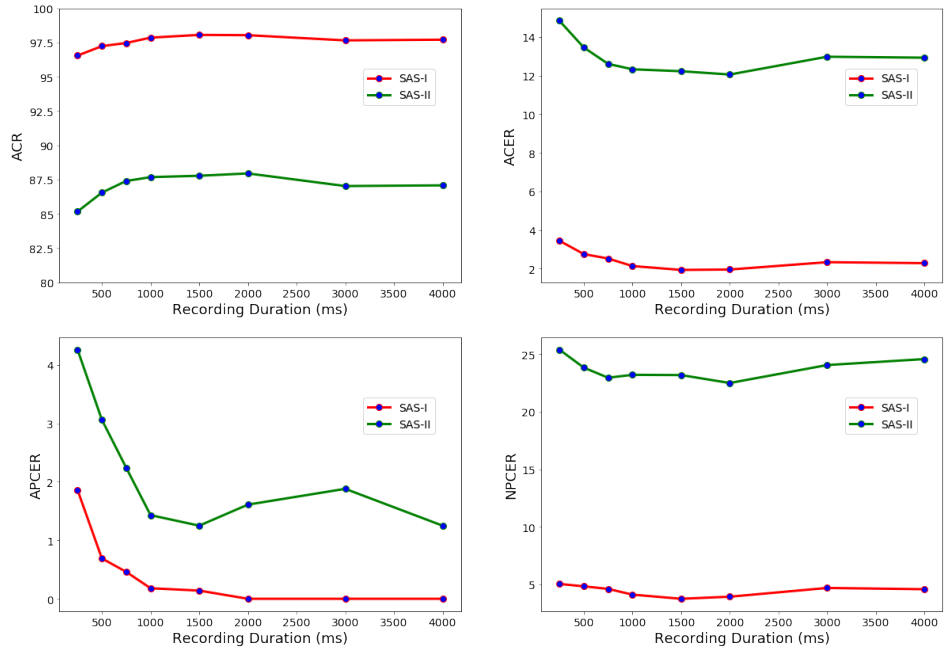

Figure 3: Performance metrics distribution across all tested recording durations.

Table 3: Comparison of C-ResNet 18 against the statistical baseline when making recording-level predictions.

Performance metrics	C-ResNet 18		[Rigas and Komogortsev 2015]	
	SAS I (%)	SAS II (%)	SAS I (%)	SAS II (%)
ACR	100	100	95.4	96.5
APCER	0	0	5.9	3.4
NPCER	0	0	3.4	3.5
EER	0	0	4.7	3.4

5.2 Limitations

We only consider print-attacks with two different attack scenarios in our proposed method. Other spoofing attacks, such as replay attacks, use of contact lenses, are not in our research scope, thus it is unknown how our deep learning architecture performs on any other form of iris spoofing attack. The effect of head movement

during attack scenarios is not investigated in the paper, so we are unsure how the deep learning approach is affected with participants head movement. What security issues may arise in the system while using the deep learning approach is still an open research question to work on. Possibility of being attacked in the layers of proposed deep learning model is worth exploring in the future.

6 CONCLUSION

We presented a deep learning approach for detecting iris print attacks using eye movement analysis. Our proposed deep learning model has outperformed the previous state-of-the-art in this domain by [Rigas and Komogortsev 2015]. Our results were validated on the ETPAD v2 dataset, containing 400 real eye movements from 200 subjects. The print attacks executed and recorded in this dataset presented a case where relatively high-quality eye tracking signal was captured during different forms of attack. This study investigates the feasibility of distinguishing a genuine eye from a spoofed one using EMS-based features. The proposed technique results in an ACR of 98.06% and 87.78% in two different attack scenarios, requiring just 1.5 seconds of eye movement data to make a decision for spoof detection. The proposed model perfectly classifies the live and fake EMS across the whole recording duration whereas the ACR for the statistical baseline was 95.4% and 96.5% for SAS I and SAS II, respectively. The proposed methodology indicates that deep learning models can effectively use EMS and its derivatives for iris PAD—something that was not demonstrated before.

ACKNOWLEDGMENTS

This material is supported by the National Science Foundation under Grant No. CNS-1714623 bestowed on Dr. Oleg V Komogortsev and by the National Science Foundation Graduate Research Fellowship under Grant No. DGE-1144466 bestowed on Mr. Dillon J Lohr. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

2021. CMITech. BMT-20 Iris Recognition System. www.cmi-tech.com

Rohit Agarwal and Anand Singh Jalal. 2021. Presentation attack detection system for fake Iris: a review. *Multimedia Tools and Applications* (2021), 1–22.

Rohit Agarwal, Anand Singh Jalal, and KV Arya. 2020. A multimodal liveness detection using statistical texture features and spatial analysis. *Multimedia Tools and Applications* 79, 19 (2020), 13621–13645.

Rohit Agarwal, Anand Singh Jalal, and KV Arya. 2021. Local binary hexagonal extrema pattern (LBH X EP): a new feature descriptor for fake iris detection. *The Visual Computer* 37 (2021), 1357–1368.

Kakali Chatterjee et al. 2017. An efficient biometric based remote user authentication technique for multi-server environment. *Wireless Personal Communications* 97, 3 (2017), 4729–4745.

Adam Czajka and Kevin W Bowyer. 2018. Presentation attack detection for iris recognition: An assessment of the state-of-the-art. *ACM Computing Surveys (CSUR)* 51, 4 (2018), 1–35.

Manar Ramzy Dronky, Wael Khalifa, and Mohamed Roushdy. 2021. Using residual images with BSIF for iris liveness detection. *Expert Systems with Applications* (2021), 115266.

Waleed S-A Fathy and Hanaa S Ali. 2018. Entropy with local binary patterns for efficient iris liveness detection. *Wireless Personal Communications* 102, 3 (2018), 2331–2344.

Lee Friedman, Mark S Nixon, and Oleg V Komogortsev. 2017. Method to assess the temporal persistence of potential biometric features: Application to oculomotor, gait, face and brain structure databases. *PloS one* 12, 6 (2017), e0178501.

Javier Galbally and Marta Gomez-Barrero. 2016. A review of iris anti-spoofing. In *2016 4th international conference on biometrics and forensics (IWBF)*. IEEE, 1–6.

Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. 2015a. An investigation of local descriptors for biometric spoofing detection. *IEEE transactions on information forensics and security* 10, 4 (2015), 849–863.

Diego Gragnaniello, Carlo Sansone, and Luisa Verdoliva. 2015b. Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters* 57 (2015), 81–87.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2015. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification. In *Proceedings of the IEEE international conference on computer vision*. 1026–1034.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016b. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 770–778.

Lingxiao He, Haiqing Li, Fei Liu, Nianfeng Liu, Zhenan Sun, and Zhaofeng He. 2016a. Multi-patch convolution neural network for iris liveness detection. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 1–7.

Yang Hu, Konstantinos Sirlantzis, and Gareth Howells. 2016. Iris liveness detection using regional features. *Pattern Recognition Letters* 82 (2016), 242–250.

Lena A Jäger, Silvia Makowski, Paul Prasse, Sascha Liehr, Maximilian Seidler, and Tobias Scheffer. 2019. Deep eyedentification: Biometric identification using micro-movements of the eye. *arXiv preprint arXiv:1906.11889* (2019).

Anil K Jain, Patrick Flynn, and Arun A Ross. 2007. *Handbook of biometrics*. Springer Science & Business Media.

Juho Kannala and Esa Rahtu. 2012. Bsif: Binarized statistical image features. In *Proceedings of the 21st international conference on pattern recognition (ICPR2012)*. IEEE, 1363–1366.

Bineet Kaur, Sukhwinder Singh, and Jagdish Kumar. 2019. Cross-sensor iris spoofing detection using orthogonal features. *Computers & Electrical Engineering* 73 (2019), 279–288.

Gabriela Y Kimura, Diego R Lucio, Alceu S Britto Jr, and David Menotti. 2020. CNN hyperparameter tuning applied to iris liveness detection. *arXiv preprint arXiv:2003.00833* (2020).

Oleg V Komogortsev, Alexey Karpov, and Corey D Holland. 2015. Attack of mechanical replicas: Liveness detection with eye movements. *IEEE Transactions on Information Forensics and Security* 10, 4 (2015), 716–725.

Dillon Lohr, Henry Griffith, and Oleg V Komogortsev. 2021. Eye Know You: Metric Learning for End-to-end Biometric Authentication Using Eye Movements from a Longitudinal Dataset. *arXiv preprint arXiv:2104.10489* (2021).

Ilya Loshchilov and Frank Hutter. 2019. Decoupled Weight Decay Regularization. In *International Conference on Learning Representations*.

Timo Ojala, Matti Pietikainen, and Topi Maenpaa. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on pattern analysis and machine intelligence* 24, 7 (2002), 971–987.

Federico Pala and Bir Bhanu. 2017. Iris liveness detection by relative distance comparisons. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 162–169.

Ioannis Rigas and Oleg V Komogortsev. 2014. Gaze estimation as a framework for iris liveness detection. In *IEEE International Joint Conference on Biometrics*. IEEE, 1–8.

Ioannis Rigas and Oleg V Komogortsev. 2015. Eye movement-driven defense against iris print-attacks. *Pattern Recognition Letters* 68 (2015), 316–326.

Muhammad Sajjad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, and Sung Wook Baik. 2019. CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters* 126 (2019), 123–131.

Ruben Tolosana, Marta Gomez-Barrero, Christoph Busch, and Javier Ortega-Garcia. 2019. Biometric presentation attack detection: Beyond the visible spectrum. *IEEE Transactions on Information Forensics and Security* 15 (2019), 1261–1275.

David Yambay, Benedict Becker, Naman Kohli, Daksha Yadav, Adam Czajka, Kevin W Bowyer, Stephanie Schuckers, Richa Singh, Mayank Vatsa, Afzel Noore, et al. 2017. LivDet iris 2017—Iris liveness detection competition 2017. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 733–741.

Zihui Yan, Lingxiao He, Man Zhang, Zhenan Sun, and Tieniu Tan. 2018. Hierarchical multi-class iris classification for liveness detection. In *2018 International Conference on Biometrics (ICB)*. IEEE, 47–53.

Hui Zhang, Zhenan Sun, Tieniu Tan, and Jianyu Wang. 2011. Learning hierarchical visual codebook for iris liveness detection. In *International Joint Conference on Biometrics*, Vol. 1.