# IRIS SPOOF DETECTION

**MAJOR TECHNICAL PROJECT (DP 401P)**

*to be submitted by*

**DILIP KUMAR CHAUHAN**

*for the*

**FINAL-SEMESTER<br>EVALUATION**

*under the supervision of*

**DR. ADITYA NIGAM**

**SCHOOL OF COMPUTING AND ELECTRICAL ENGINEERING**

**INDIAN INSTITUTE OF TECHNOLOGY MANDI**

**KAMAND-175005, INDIA**

**JULY, 2020**

# MTP 2019-20 Project Form
# School of Computing and Electrical Engineering

Name: DILIP KUMAR CHAUHAN................................................

Roll No.: B16018........................................................................

Branch: CSE........................................................................

Project Title: IRIS SPOOF DETECTION.....................................................

Supervisor Name: DR. ADITYA NIGAM..............................................................

Objectives (mention in bullet points)

| **Original** | **Revised** |
|---|---|
| • To develop an algorithm for Iris Presentation Attack Detection(PAD)<br>• To generate high quality spoof iris images<br>• To compare our algorithm's result with state of art results | • To develop an algorithm for Iris Presentation Attack Detection(PAD)<br>• Literature review of state of art papers that can be applied to solve the iris PAD task<br>• To compare our algorithm's result with state of art results. |

Aditya nigam 14/June/2020

Signature of Supervisor

# Contents

# Abstract

With increasing demand of security and privacy in today's world, spoofing is a great concern. All the biometric traits such as fingerprint, iris, face etc which are used for authentication are susceptible to different kind of spoof attacks. Among different biometric systems, iris recognition systems are vulnerable to Presentation Attacks(PAs) by various artifacts such as textured contact lens, soft contact lens, printed iris image and plastic eyes to spoof the identify of another person. Researchers have been doing good work in this field and implemented various PAD algorithms but these algorithms are not 100% accurate and hence needs to be improved. We have approached the problem of PAD as binary classification as well as multi class classification. For the same, we have proposed an architecture Self Calibrated Feature Extactor Network(SCFENet) which utilizes SCNet based self calibrated convolution with softmax classifier on top for iris spoof detection. The self-calibrated convolution stretches the fields-of-view of every convolution layer through inner communications and therefore enhances the output features. The performance of our proposed model has been evaluated on 3 publicly available iris spoofing datasets: IIITD-CLI, IIS and ND. The KNN classifier is also utilized on feature extracted by SCFENet to check the generalization of extracted descriptive features. The proposed model exhibits an increase in CRR of 4.55% as compared to state of art results when training is done on ND-II and testing is performced on ND-I dataset. Also 100% CCR is obtained on IIS Combined dataset.

# Overall work done

## 1.1 Background and Literature Survey

In the era of internet and online verification systems even a single mistake in Spoof Detection can have very adverse effect. To enhance the security of the systems various hardware and software based approaches have been proposed in past but they are susceptible to various Presentation Attacks(PAs). Nowadays almost all the authentication systems use biometric traits such as face, finger, iris etc for person verification however all these systems are somewhat vulnerable to Presentation Attacks. These attacks include gummy fingers, printed fingerprint etc for fingerprint recognition system wheres as face recognition system is vulnerable to many different presentation attacks such as using a printed face and digital screen face etc. However like other biometric traits iris recognition system can also be susceptible to presentation attacks in the form of colored textured contact lens, soft contact lens and printed iris images etc.

Iris of a human is the part between white sclera and black pupil of the eye. Out of all the biometric traits, iris has been shown as one of the best, accurate and reliable biometrics for human authentication. Therefore, automated iris recognition systems are used in the applications such as border control, forensic and citizen authentication etc. The usefulness of iris recognition systems has motivated the researchers for past few years to develope more robust and accurate algorithm for Presentation Attack Detection(PAD) called Spoof Detection. But these systems are not so accurate to vanish the effect of presentation attacks and it is mainly because of different kind of attacks being introduced due to advancement in technology and material. So more accurate matching algorithms are required to detect spoof iris images to a great extent. Therefore, we worked on iris presentation attack detection and proposed an algorithm for the same.

**Related Works:** Doyle *et al.* [1] applied modified Local Binary Pattern(LBP) to each region(pupil, iris, sclera) of every image at multiple scales to classify the image as no lens, soft contact lens and textured contact lens. The CCR of 98% is obtained on a 2 two class problem of determining whether an iris image contains a textured contact lens or not. Kohli *et al.* [2] examined that colored cosmetic lens deteriorates the performance of iris recognition system with significant increase in false rejection rate at a fixed false acceptance rate using VeriEye. Gupta *et al.* [3] used Local Binary Pattern(LBP), Histogram of Oriented Gradients(HOG) and GIST for feature extraction and Support Vector Machine(SVM) as classifier for detection of iris spoofing over print attacks. Result shows that LBP with SVM gives the best performance while GIST gives the worst.

Kohli *et al.* [4] applied multi-order dense Zernike moments and Local Binary Pattern with Variance(LBPV) for iris presentation attack detection over print attacks and contact lens. The spoof detection rate of 82.20% is obtained by the proposed algorithm using combined iris spoofing dataset. Hu *et al.* [5] proposed an iris liveness detection algorithm based on spatial pyramid used for constructing regional features on print attack and contact lens iris spoofing datasets. [6] implemented discrete orthogonal moments i.e Tchebichef(TM), Krawtchouk(KM) and Dual-Hahn(DM) moments for feature extraction and K-nearest neighbour(KNN) with k equal to 1 as classifier. The proposed method is evaluated on four publicly available iris spoofing datasets: IIITD-CLI, IIS, Warsaw LiveDet 2015 and Clarkson LiveDet 2015. 100% textured contact lens detection rate is obtained on IIITD-CLI dataset while detection rate of 98.93% and 98% are achieved for print+capture and print+scan attacks respectively on IIS dataset. Recently, researchers have shown more inclination towards using deep learning techniques in spoof detection task with advancement in machines and its computational capacity. Menotti *et al.* [7] presented deep representation using convolution neural network(CNN) and back propagation for weights update for iris presentation attack detection. Pala *et al.* [8] proposed a framework constructed over triplet convolution network with relative distance matching. The performance improved for both photo based and contact lens presentation attacks. Raghavendra *et al.* [9] proposed ContlensNet built using Deep Convolutional Neural Network(CNN) consisting of fifteen layers for classification of no lens, soft lens and textured contact lens on IIITD-CLI and ND cosmetic contact lens dataset. The average improvement of around 10% in CCR is obtained as compare to other state-of-art iris presentation attack detection systems. Yadav *et al.* [10] proposed DensePAD a DenseNet based convolutional neural network(CNN) model for iris presentation detection on mutiple datasets. The performance shows its superiority in detection of iris spoofing even if the images were taken in unconstrained environment. Singh *et al.* [11] proposed GHCLNet a hierarchical architecture based on ResNet-50 for three class classification of no lens, soft lens and cosmetic lens on IIITD-CLI, ND and IIT-K dataset. 100% detection of cosmetic lens is achieved on IIITD-CLI dataset. Choudhary *et al.* [12] implemented DCLNet a deep convolutional neural netwok having dense connections among layers which has been designed through a lot of customiztions over Densenet121 with SVM classifier on top. The model is evaluated on 2 publicly avaiable datasets: IIITD-CLI and ND contact lens 2013. An improvement up to 4% is achieved in Correct Classification Rate(CCR) as compared to the state of the art results. All the above works perform better on intra-sensor dataset but the performance reduces across inter-sensor dataset as well as other iris spoofing datasets. So, there is a scope of improvement and hence we have proposed a new method for iris spoof detection.

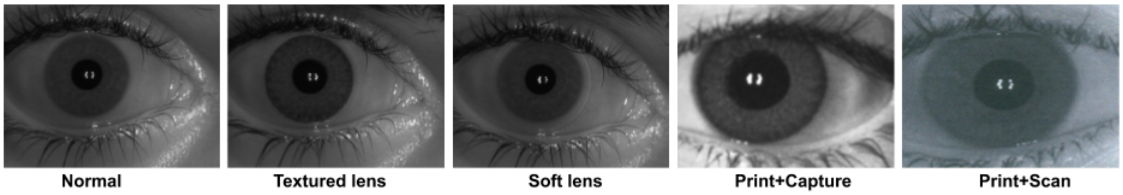

Figure 1.1: Samples of human eyes representing iris with the normal, Textured lens, Soft lens, Print+Capture and Print+Scan attacks.

## 1.2 Objective and scope of the Work

The aim is to design an algorithm for iris spoof detection and perform comparative analysis of our algorithm's performance with the state of art results.

The deep neural architecture SCFENet with softmax classifier on top, which we have proposed can be used for iris spoof detection in border control, forensics, person authentication and other places where iris is used as biometrics for authentication.

## 1.3 Methodology

**Self Calibrated Convolution:** [13] proposed the concept of self calibrated convolution instead of normal convolution. In self calibrated convolution, each portion of splitted convolutional filters is responsible for a special functionality unlike grouped convolution where every portion is treated equally. Figure 1.3 shows the workflow of self calibrated convolution. For better understanding of workflow suppose that the input channel number C is equal to output channel number and also C is divisible by 2. Given a group of K filters with shape(C, C, $K_h$, $K_w$) for a particular convolution layer where $K_h$ and $K_w$ are spatial height and width of the filters respectively, the K filters is divided into four portions where each portion is responsible for special functionality. After division of K filters, four set of filters $K_1$, $K_2$, $K_3$ and $K_4$ of shape (C/2, C/2, $K_h$, $K_w$) is obtained. The input X is uniformly splitted into two portions($X_1$, $X_2$) and each portion is passed through special pathway for learning different contextual information. $X_1$ is sent through first pathway which utilizes $K_2$, $K_3$ , $K_4$ for self calibrated operation giving output $Y_1$ whereas $X_2$ is sent through second pathway where simple convolution is performed as $Y_2=F_1(X_2)=X_2*K_1$ which retains the original spatial context. Now the output Y is obtained by concatenation of both the intermediate outputs $Y_1$ and $Y_2$.

**Image augmentation:** A deep convolution neural network needs a large number of images per class to learn the descriptive features but the iris datasets which we have used, conatin insufficient iris images per class. Hence, to generate supplementary training iris images we have used some augmentation techniques, such as horizontal flip, vertical flip, rotation, color jitter on input iris images(as shown in Fig. 1.2). Since large size input images create more parameters that can lead to overfitting, hence the input iris image is first downsam-

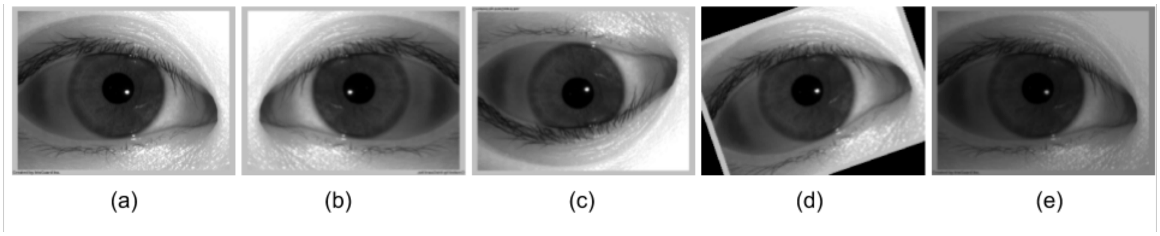

Figure 1.2: Iris image augmentation. (a) Input image (b) horizontal flip (c) vertical flip (d) rotation (e) color jitter

pled to shape 192X256 (for IIITD-CLI, IIS dataset) and 256x256 for ND dataset and then the augmentation technique is applied using the inbuilt transforms library in pytorch.

**proposed methodology:** Our proposed network is shown in Fig. 1.4 which utilizes SCNet50_v1d [13] with additional two fc layers to extract 128 dimensional descriptive features and we named this network as SCFENet(Self Calibrated Feature Extractor Network). Softmax and KNN classifiers are used on top of the feature extractor network(SCFENet) for binary as well as multi class problem of spoof detection. SCNet50_v1d is modified Resnet-50 architecture where 7x7 conv is replaced with three 3x3 convs and a 3x3 avg pool with stride 2 added before conv, whose stride is changed to 1 in the downsampling block with each convolution layer replaced with self calibrated convolution.

We utilized the weights of SCNet_v1d pretrained on imagenet dataset to start training our model. First two blocks of SCNet_v1d is fixed while rest blocks are retrained on our iris dataset for extracting the descriptive features. Our proposed model is implemented using python-3.6 and pytorch-0.3 on NVIDIA-gpu. The input iris images are first resized and augmented using the image augmentation techniques as explained above and then fed to our network SCFENet which extracts 128 dimensional descriptive feature vector. The extracted feature vector is utilized by softmax and KNN(with K=5) classifiers for the classification of input images as type of attacks they belong to, for multi class problem of spoof detection while images are classified as whether they are spoof or normal for two class problem of spoof detection. Adam optimiser with learning rate of 0.0001, β1=0.9 and β2=0.999 is used for training our network for 300 epochs for all datasets except ND-1 which is trained upto 200 epochs because of very less number of training samples in the ND-I dataset. The detailed description of parameters and their values is summarized in Table 1.1.

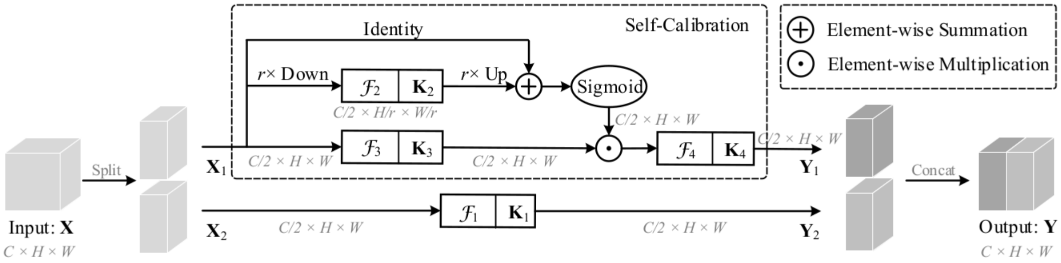

Figure 1.3: [13] schematic illustrations of self-calibrated convolutions

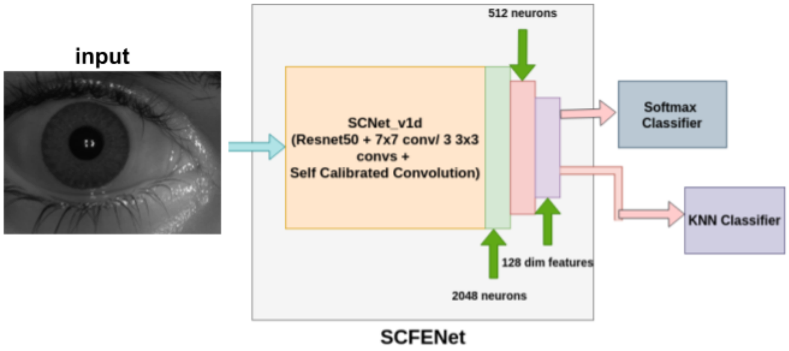

Figure 1.4: Proposed network architecture

Table 1.1: Parameters of SCFENet

| Sr No. | Parameter | Value |
|---|---|---|
| 1 | Optimizer | Adam |
| 2 | Learning Rate | 0.0001 |
| 3 | $\beta1$ | 0.9 |
| 4 | $\beta2$ | 0.999 |
| 5 | batch size | 32 |
| 6 | epochs | 300 |

## 1.4 Dataset and Testing Protocol

In this section, we discuss the details about datasets and testing protocols which have been used for experimentation. We have trained and tested our model on three publicly available datasets: IIITD-Contact lens iris(IITD-CLI), IIITD Iris Spoofing(IIS) and Notre Dame(ND) cosmetic contact lens 2013 dataset.

**IIITD-CLI:** The dataset contains a total of 6570 iris images corresponding to 101 subjects of which both right and left iris images of every subject have been captured by two sensors: Vista FA2E single iris sensor and Cogent dual iris sensor(CIS 202). The soft lenses in the dataset are manufactured by either CIBA Vision or Bausch and Lomb while four colors are used for textured lenses. This dataset provided evaluation protocol of using iris images of first 50 subjects for training and rest 51 subjects for testing.

**IIS:** This dataset comprises of 4848 iris images corresponding to 101 subjects with two print attacks scenarios: namely print+capture and print+scan attacks. The dataset has be prepared using 12 iris images per subject with varying lens types from IIITD-CLI dataset and taking high resolution printouts by HP Color LaserJet 2025 printer. The evaluation protocol of using images of first 50 subjects for training and rest 51 subjects for testing is provided.

**ND:** This dataset composed of two datasets namely: ND-I and ND-II. ND-I contains 900 iris images comprising of no lens, soft contact lens and textured contact lens which have been captured using IrisGaurd Ad-100 sensor. The dataset has already been divided into training and testing sets containing 600 and 300 images respectively. ND-II iris dataset comprises of 3000 training images and 1200 testing images from no lens, soft contact lens and textured contact lens categories which have been captured using LG-400 sensor.

## 1.5 Results and Experimentation

Our proposed network is trained and tested using the testing protocol and the results for both two class problem and multi class problem of spoof detection is presented on three different experiments: (i) intra-sensor validation, (ii) inter- senor validation and (iii) combined sensor validation.

### 1.5.1 Evaluation Metrics

The performance of multi class problem of iris presentation attack detection is evaluated based on Correct Classification Rate(CCR) where higher CCR corresponds to better performance of the model. The CCR is calculated as the ratio of correctly classified images of a particular class to total number of images in that class. Lets assume, there are n samples of testing images of a class out of which m images are correctly classified therefore, the CCR is mathematically calculated as

$$CCR = \frac{m}{n}$$

The performance of two class problem of iris presentation attack detection is evaluated based on the metrices like Attack Presentation Classification Error Rate(APCER), Bonafide Presentation Classification Error Rate (BPCER) and Total Error Rate(TER) where lower values of these metrices correspond to better performance of the model. APCER is defined as the ratio of incorrectly classified spoof images to total number of spoof samples, BPCER is defined as the ratio of incorrectly classified normal images to total number of normal images and TER is defined as the ratio of incorrectly classified test samples to total number of test samples. Let us consider n and m be number of test samples from normal and spoof dataset respectively. Out of n samples from normal dataset n1 samples are correctly classified as normal and n2 samples are incorrectly classified as spoof. Also out of m samples from spoof dataset m1 samples are correctly classified as spoof and m2 samples are incorrectly classified as normal. So mathematically APCER, BPCER and TER is defined as

$$APCER = \frac{m2}{m}$$

$$BPCER = \frac{n2}{n}$$

$$TER = \frac{m2 + n2}{m + n}$$

### 1.5.2 Spoof detection as multi class classification

This technique of spoof detection classifies a given sample into type of attacks it belongs to.

**Intra-sensor Validation:** In this testing approach, training and testing is performed on the data from a single sensor. Table 1.2 shows the results of our proposed model and other state of art results for intra-sensor validation. The aggregate CCR achieved through our proposed SCFENet with sotfmax classifier on top outperforms the results of GHCLNet[11] and DCLNet[12] with 0.95% and 0.50% increase in CRR for ND-I and ND-II dataset respectively whereas the performance obtained on IIITD-CLI Vista is comparable and on IIITD-CLI Cogent is little less. However 100% and 99.93% CCR for IIS Cogent and IIS Vista dataset is obtained respectively. Also applying KNN classifier instead of softmax gives CRR of 100% on IIS Vista dataset while comparable results for other dataset is obtained.

**Inter-sensor Validation:** In this testing approach, training is done on data from one sensor while testing is performed on data captured from another sensor. Table 1.3 shows the result on inter sensor validation of our proposed network along with state of art results. We have performed pairwise comparision of IIITD-CLI Cogent and IIITD-CLI Vista, IIS Cogent and IIS Vista, ND-I and ND-II. Our model outperforms the state of art result with increase in CCR of 4.55% when training is done on ND-II and testing is performed on ND-I. Also a reduced in performance is obtained on other pairwise dataset, such as IIITD-CLI Cogent and IIITD-CLI Vista and when trained on ND-I and tested on ND-II. However CRR of 99.57% and 90.25% is obtained when trained on IIS Cogent and tested on IIS Vista and vice-versa respectively. Also applying KNN as classifier performs better than softmax as classifier, in two combinations of training and testing pairs out of six combinations.

**Combined-sensor Validation:** In this testing approach, images captured from two or more sensors are combined to make a single dataset. Here, we have combined images from the same dataset as IIITD-CLI Cogent and IIITD-CLI Vista are combined to form IIIT-CLI Combined, ND-I and ND-II are combined to form ND Combined, and IIS Cogent and IIS Vista are Combined to form IIS Combined. Table 1.4 shows the result of our proposed model with other state of art results. Our proposed SCFENet with softmax classifier outperforms the state of art results with an increase in CCR of 0.42% and 0.72% for ND Combined and IIS Combined datasets respectively. The CCR obtained on IIIT-CLI Combined is little less than Fusion[6] but comparable to GHCLNet[11] and DCLNet[12]. Also applying the KNN classifier instead of softmax gives better performace on ND-Combined dataset however, overall SCFENet+softmax performs better than SCFENet+KNN.

Table 1.2: Model performance in CCR(%) for intra-sensor validation(where C-C is Cosmetic lens-Cosmetic lens, N-N is Normal-Normal, S-S is Soft lens-Soft lens, Pc-Pc is Print+Capture-Print+Capture and Ps-Ps is Print+Scan-Print+ Scan)

| Dataset | Classification Type | GHCLNet[11] | DCLNet[12] | Fusion[6] (KM+TM+HM) | SCFENet+ Softmax | SCFENet+ KNN |
|---|---|---|---|---|---|---|
| IIITD-CLI Cogent | C-C | **100** | 99.10 | **100** | **100** | 99.66 |
| | N-N | 89.86 | **94.19** | 89.20 | 77 | 86.50 |
| | S-S | 91.26 | 92.33 | **99.99** | 91.99 | 88.15 |
| | **Aggregate** | 93.71 | 95.20 | **96.32** | 89.57 | 91.99 |
| IIITD-CLI Vista | C-C | **100** | **100** | **100** | **100** | **100** |
| | N-N | 94.6 | 93.19 | 87.90 | **95** | 93 |
| | S-S | 91.88 | 92.89 | **99.98** | 89.41 | 90.39 |
| | **Aggregate** | 95.49 | 95.36 | **95.95** | 94.80 | 94.47 |
| ND-I | C-C | **100** | 98.50 | - | **100** | **100** |
| | N-N | **91.67** | 89.49 | - | 87.50 | 87.50 |
| | S-S | 87.50 | 90.86 | - | **94.23** | **94.23** |
| | **Aggregate** | 93.05 | 92.95 | - | **94.00** | **94.00** |
| ND-II | C-C | 99.75 | **99.93** | - | 99.75 | 99.5 |
| | N-N | **95.24** | 92.86 | - | 94.52 | 92.38 |
| | S-S | 89.74 | 94.45 | - | 94.47 | **96.84** |
| | **Aggregate** | 94.91 | 95.74 | - | **96.25** | 96.16 |
| IIS-Cogent | N-N | - | - | - | 100 | 100 |
| | Pc-Pc | - | - | - | 100 | 100 |
| | Ps-Ps | - | - | - | 100 | 100 |
| | **Aggregate** | - | - | - | **100** | **100** |
| IIS-Vista | N-N | - | - | - | 99.80 | 100 |
| | Pc-Pc | - | - | - | 100 | 100 |
| | Ps-Ps | - | - | - | 100 | 100 |
| | **Aggregate** | - | - | - | 99.93 | **100** |

Table 1.3: Model performance in CCR(%) for inter-sensor validation(where C-C is Cosmetic lens-Cosmetic lens, N-N is Normal-Normal, S-S is Soft lens-Soft lens, Pc-Pc is Print+Capture-Print+Capture and Ps-Ps is Print+Scan-Print+ Scan)

| Training Dataset | Testing Dataset | Classification Type | GHCLNet[11] | DCLNet[12] | Fusion[6] (KM+TM+HM) | SCFENet+ Softmax | SCFENet+ KNN |
|---|---|---|---|---|---|---|---|
| IIITD-CLI Cogent | IIITD-CLI Vista | C-C | 99.25 | 99.83 | **100** | **100** | **100** |
| | | N-N | 93.40 | 89.55 | **95.69** | 60.40 | 76 |
| | | S-S | 83.37 | 81.74 | 95.69 | **96.47** | 93.72 |
| | | **Aggregate** | 92.01 | 90.37 | **97.13** | 85.78 | 90 |
| IIITD-CLI Vista | IIITD-CLI Cogent | C-C | 85.36 | 99.82 | **100** | 89.85 | 90.18 |
| | | N-N | 96.74 | 81.43 | **98.5** | 87 | 82.33 |
| | | S-S | 65.73 | 79.26 | **95.7** | 85.54 | 89.02 |
| | | **Aggregate** | 82.61 | 86.83 | **98.09** | 87.47 | 87.13 |
| ND-I | ND-II | C-C | **100** | 97.92 | - | 93.50 | 70.25 |
| | | N-N | 81.25 | **83.00** | - | 69.76 | 70.71 |
| | | S-S | **93.27** | 92.90 | - | 82.37 | 84.21 |
| | | **Aggregate** | **91.51** | 91.27 | - | 81.67 | 74.83 |
| ND-II | ND-I | C-C | 98.00 | **100** | - | **100** | 97 |
| | | N-N | 91.90 | 92 | - | **93.75** | 83.33 |
| | | S-S | 81.84 | 84.34 | - | 96.15 | **98.07** |
| | | **Aggregate** | 90.58 | 92.11 | - | **96.66** | 93 |
| IIS-Cogent | IIS-Vista | N-N | - | - | - | 98.60 | 99.8 |
| | | Pc-Pc | - | - | - | 100 | 100 |
| | | Ps-Ps | - | - | - | 100 | 100 |
| | | **Aggregate** | - | - | - | 99.57 | **99.94** |
| IIS-Vista | IIS-Cogent | N-N | - | - | - | 74.83 | 80.16 |
| | | Pc-Pc | - | - | - | 100 | 100 |
| | | Ps-Ps | - | - | - | 98.61 | 89.86 |
| | | **Aggregate** | - | - | - | **90.55** | 90.43 |

Table 1.4: Model performance in CCR(%) for Combined sensor validation(where C-C is Cosmetic lens-Cosmetic lens, N-N is Normal-Normal, S-S is Soft lens-Soft lens, Pc-Pc is Print+Capture-Print+Capture and Ps-Ps is Print+Scan-Print+ Scan)

| Dataset | Classification Type | GHCLNet[11] | DCLNet[12] | Fusion[6] (KM+TM+HM) | SCFENet+ Softmax | SCFENet+ KNN |
|---|---|---|---|---|---|---|
| ND-Combined | C-C | **100** | 99.93 | - | 99.60 | 99.40 |
| | N-N | 91.67 | **93.89** | - | 92.83 | 93.79 |
| | S-S | 95.04 | 94.32 | - | **97.11** | 96.48 |
| | **Aggregate** | 95.57 | 96.04 | - | 96.46 | **96.53** |
| IIITD-CLI Combined | C-C | 99.73 | 99.87 | **100** | 99.91 | 99.81 |
| | N-N | 91.87 | 92.82 | **99.50** | 92.82 | 95.36 |
| | S-S | 92.85 | 92.10 | **100** | 90.04 | 85.23 |
| | **Aggregate** | 94.82 | 94.93 | **99.89** | 94.27 | 93.51 |
| IIS-Combined | N-N | - | - | 99.90 | 100 | 100 |
| | Pc-Pc | - | - | 98.93 | 100 | 100 |
| | Ps-Ps | - | - | 99.00 | 100 | 100 |
| | **Aggregate** | - | - | 99.28 | **100** | **100** |

### 1.5.3 Spoof detection as two class classification

In this approach of spoof detection a given iris image is classified whether it is spoof of normal. For applying this method, all the attacks of a dataset are combined to form spoof samples of that dataset however normal samples are left as it is. And then the binary classification is performed using SCFENet with softmax and KNN classifiers. Intra-sensor, inter sensor and combined sensor validations are performed using training and testing strategies utilized in previous subsection ”spoof detection as multi class classification ”.

**Intra-sensor Validation:** Table 1.5 shows the performance of our proposed model when experiment is performed using intra-sensor validation technique. SCFENet+softmax performs better in terms of TER on ND( ND-I and ND-II) dataset while SCFENet+KNN perfromence is better on IIIT-CLI(Cogent and Vista) dataset. However, TER of 0% is obtained on IIS(Cogent and Vista) using both softmax and KNN classifiers.

**Inter-sensor Validation:** Table 1.6 summarises the results of experimentation using inter-sensor validation technique by our proposed model. The performanece in terms of TER of SCFENet+KNN is better than SCFENet+Softmax in almost all pairwise combinations of training and testing except for the case when the training is done on ND-II and testing is performed on ND-I dataset. Also, TER of 0% is achieved in the case when training and testing is performed on IIS Cogent and IIS Vista respectively using both softmax and KNN classifiers.

**Combined-sensor validation:** The performance of our proposed model for combined sensor validation technique is shown in Table 1.7 . The TER of 5.27% and 2.93% is obtained by our model SCFENet+Softmax on ND Combined and IIITD-CLI Combined dataset respectively. Also 0% TER is achieved in case of IIS Combined dataset by using both softmax and KNN classifiers. Overall, SCFENet+Softmax performs better than SCFENet+KNN in terms of TER.

Table 1.5: Model performance in APCER(%), BPCER(%) and TER(%) for intra-sensor validation

| Dataset | Evaluation Metric | SCFENet + Softmax | SCFENet+ KNN |
|---|---|---|---|
| IIITD-CLI Cogent | APCER | 7.81 | **6.09** |
| | BPCER | **8.33** | 10.83 |
| | TER | 7.98 | **7.70** |
| IIITD-CLI Vista | APCER | 6.18 | **5.49** |
| | BPCER | **1.80** | 2.20 |
| | TER | 4.74 | **4.41** |
| ND-I | APCER | **6.86** | 7.35 |
| | BPCER | 13.54 | **12.5** |
| | TER | **9.0** | **9.0** |
| ND-II | APCER | **2.69** | 4.74 |
| | BPCER | 4.04 | **1.67** |
| | TER | **3.17** | 3.67 |
| IIS-Cogent | APCER | 0 | 0 |
| | BPCER | 0 | 0 |
| | TER | **0** | **0** |
| IIS-Vista | APCER | 0 | 0 |
| | BPCER | 0 | 0 |
| | TER | **0** | **0** |

Table 1.6: Model performance in APCER(%), BPCER(%) and TER(%) for inter-sensor validation

| Training Dataset | Testing Dataset | Evaluation Metric | SCFENet + Softmax | SCFENet+ KNN |
|---|---|---|---|---|
| IIITD-CLI Cogent | IIITD-CLI Vista | APCER | 6.96 | **4.90** |
| | | BPCER | **7.8** | 10.0 |
| | | TER | 7.24 | **6.58** |
| IIITD-CLI Vista | IIITD-CLI Cogent | APCER | 22.92 | **22.15** |
| | | BPCER | **1.33** | 1.83 |
| | | TER | 15.58 | **15.24** |
| ND-I | ND-II | APCER | **12.44** | 13.97 |
| | | BPCER | 17.38 | **14.29** |
| | | TER | 14.17 | **14.08** |
| ND-II | ND-I | APCER | **6.37** | 8.82 |
| | | BPCER | 10.42 | **6.25** |
| | | TER | **7.67** | 8.0 |
| IIS-Cogent | IIS-Vista | APCER | 0 | 0 |
| | | BPCER | 0 | 0 |
| | | TER | **0** | **0** |
| IIS-Vista | IIS-Cogent | APCER | **3.45** | 5.69 |
| | | BPCER | 16.26 | **7.0** |
| | | TER | 8.09 | **6.16** |

Table 1.7: Model performance in APCER(%), BPCER(%) and TER(%) for combined-sensor validation

| Dataset | Evaluation Metric | SCFENet + Softmax | SCFENet+ KNN |
|---|---|---|---|
| ND-Combined | APCER | 4.39 | **3.30** |
| | BPCER | **7.0** | 11.55 |
| | TER | **5.27** | 6.05 |
| IIITD-CLI | APCER | **0.61** | 1.32 |
| Combined | BPCER | 7.36 | **6.40** |
| | TER | **2.93** | 3.07 |
| IIS-Combined | APCER | 0 | 0 |
| | BPCER | 0 | 0 |
| | TER | **0** | **0** |

## 1.6 Conclusion and Future Work

The proposed network outperforms the state of art results in some cases while reduction in spoof detection rate is observed in other cases. This reduction in detection rate arises either due to the less number of samples in the dataset or low quality of images. Our proposed network SCFENet is able to extracts more descriptive features, so that any classifier can be trained on top of that, in this regard KNN classifier performance is found to be comparable with softmax clssifier. The proposed algorithm can be applied for spoof detection in other biometric traits, such as fingerprint, face etc.

# Bibliography

[1] J. S. Doyle, P. J. Flynn, and K. W. Bowyer, "Automated classification of contact lens type in iris images," in *2013 International Conference on Biometrics (ICB)*, pp. 1–6, 2013.

[2] N. Kohli, D. Yadav, M. Vatsa, and R. Singh, "Revisiting iris recognition with color cosmetic contact lenses," in *2013 International Conference on Biometrics (ICB)*, pp. 1–7, 2013.

[3] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On iris spoofing using print attack," in *2014 22nd International Conference on Pattern Recognition*, pp. 1681–1686, 2014.

[4] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Detecting medley of iris spoofing attacks using desist," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6, 2016.

[5] Y. Hu, K. Sirlantzis, and G. Howells, "Iris liveness detection using regional features," *Pattern Recognition Letters*, vol. 82, pp. 242 – 250, 2016. An insight on eye biometrics.

[6] K. Bineet, "Iris spoofing detection using discrete orthogonal moments," *Multimedia Tools and Applications*, vol. 79, 2020.

[7] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. Falcão, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 864–879, 2015.

[8] F. Pala and B. Bhanu, "Iris liveness detection by relative distance comparisons," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, July 2017.

[9] R. Raghavendra, K. B. Raja, and C. Busch, "Contlensnet: Robust iris contact lens detection using deep convolutional neural networks," in *2017 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1160–1167, 2017.

[10] D. Yadav, N. Kohli, M. Vatsa, R. Singh, and A. Noore, "Detecting textured contact lens in uncontrolled environment using densepad," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2019.

[11] A. Singh, V. Mistry, D. Yadav, and A. Nigam, “Ghclnet: A generalized hierarchically tuned contact lens detection network,” in *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pp. 1–8, 2018.

[12] M. Choudhary, V. Tiwari, and V. U., “An approach for iris contact lens detection and classification using ensemble of customized densenet and svm,” *Future Generation Computer Systems*, vol. 101, pp. 1259 – 1270, 2019.

[13] J.-J. Liu, Q. Hou, M.-M. Cheng, C. Wang, and J. Feng, “Improving convolutional networks with self-calibrated convolutions,” in *The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.