Fingerprint Presentation Attack Detection Approaches in Open-Set and Closed-Set Scenario

Anshdha Gupta* and Akhilesh Verma
Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India-201009
Email: *anshdhgupta94@gmail.com

Abstract: In the biometric system, fingerprints are widely used to recognise an individual’s identity and are vulnerable to presentation attacks such as spoofing. Spoof fingerprints are fake fingerprints created using artificial materials like play-doh, silicone, etc., which fool the biometric identification system. Spoof handling is an urgent need nowadays, as these attacks’ success rate is more than 70%. Much work has been done on fingerprint spoof detection, but mostly involved closed-set problems, i.e., spoof materials used are the same for training and testing set, but they face poor generalisation problem. Hence to overcome closed-set problems, Open-set solution came into existence in which some novel spoof materials were introduced in the testing set, which was not seen during training. This paper will give a brief review of various closed-set and open-set solution techniques along with the tabular view of their Average Classification Error (ACE) scores.

Keyword: Fingerprints, spoofing, open-set problems, closed-set problems

1. Introduction
Biometric system is an automated system that uses the information’s generally biological traits to authenticate his identity[1]. Among all the biometrics known so far, fingerprints are widely used because of its uniqueness[2]; hence, it is important to identify the authenticity of fingerprint as they are vulnerable to presentation attack and it is important to detect these attacks in order to reduce the risks which are caused by these attacks on the biometrics recognition system[3]. One of the many types of presentation attacks known so far on fingerprints is spoofing, which involves the use of fake fingerprints created by malicious actors to fool the biometric recognition system. Hence it is important to identify these attacks as the success rate of these attacks on fingerprints are more than 70%[4].

1.1 Challenges of Fingerprint spoof detection:
Major challenges in fingerprint spoof detection are Poor Generalisation[5] and overfitting problem [6]. Many research types have been conducted, which cannot show inter-operability as their solutions were closed set and worked only for certain spoof materials, i.e., the training and testing set contains the same spoof material. It is not able to provide better results for inter-sensor experiments [7]. The spoof samples are created using two methods: Consensual and Non-Consensual. Consensual, also called Co-operative spoofing, is a type of spoofing in which live fingers create the finger's plastic mould. Artificial material like silicone, play-doh, gelatine, latex, wood glue, etc., is added to create spoof fingerprint. The spoof fingerprints formed under this category are an exact imitation of live fingerprints, e.g., Gummy fingerprints. Non- Consensual also called Non-Co-operative spoofing, is the type of spoofing method in which fake fingerprints are obtained without personal participation. They are divided into four parts- Latent fingerprint, fingerprint reactivation, Cadaver and synthesis
Although creating spoof fingerprints is not an easy task and requires more time [9]. A wide range of spoof materials are available, and learning all spoof material fingerprints is impossible [10]. Hence if a methodology is used only for training spoof samples, it will not be sustained and will not be the open-set solution.

### 1.2 Approaches to Fingerprint spoof detection:

Many fingerprint presentation attack detection [11], [12] are broadly classified as hardware-based and software-based. **The hardware-based approach** is a technique in which the fingerprint reader is attached with a fingerprint sensor to identify a person's living characteristics such as blood pressure, skin distortion, odour, etc. This approach can prevent spoof attacks to some extent but require additional hardware cost, increasing the overall expenses of fingerprint spoof detection system; hence it is expensive in terms of the cost factor. Also, this technique does not work in extreme environmental conditions [13]. **Software-based approach:** this approach works on the existing fingerprint images captured from fingerprint sensors to distinguish between fake and live fingerprints without the need of new hardware system; hence it is cheap in terms of the cost factor. It works on two types of fingerprint features: static features like sweat pores, ridge and valley features, perspiration, etc. and dynamic features like skin colour change due to pressure, skin elastic properties, etc.

![Figure 1: open set classification example](image.png)

**Table 1:** comparison between open-set and closed-set problems

| Open-Set Problems | Close-Set Problems |
|-------------------|--------------------|
| Partial knowledge or no knowledge of spoof materials is given during training phase | Full knowledge of spoof material is given during training phase |
| It can be based one class or two class problem in which spoof fingerprint data may or may not be known before testing phase | It is always two class problem where both spoof and live fingerprint data to be known before testing phase |
| It is more reliable as tested for novel spoof materials too. | It is not reliable |
| Accuracy rate is high in terms of TDR | Accuracy rate is low compared to open-set problem in terms of TDR |
| It provides better results for cross-material performance | It does not provide good results for cross-material performance. |
| Training dataset is small compared to close-set problems. | Large training dataset is required consisting of all live and fake fingerprints on which model is tested. |
| Training and testing samples come from both known and unknown class. | Training and testing samples come from known class. |

These hardware-based and software-based approaches can generate open-set or closed-set solutions [14]. The open-set solution is the recognition problem where partial knowledge of the spoof
3

materials is given at the training time. The model is tested with the novel materials that are unknown during the training set [15].

Figure 1 shows the example of open-set recognition problem in which all classes are not known during training. This figure class of interest, i.e. pentagon, is surrounded by some non-interested classes ('triangle', 'square', 'circle') and unknown classes ('?'). Closed-set problems are the recognition problem where full knowledge of spoof materials is given at the training time. The model is tested with known spoof materials only, i.e. the training and testing dataset is fixed at the beginning of the model design. Table 1 shows the comparison between open-set and closed-set problems.

1.3 Sensors for capturing fingerprint images:

Open-set solutions are also dependent on the sensors being used to capture a digital image of fingerprints. There are many types of sensors available in the market, such as optical fingerprint scanner, capacitive-based fingerprint scanner and multispectral imaging sensor. An optical scanner is a very common type of scanner that uses LED light to brighten the finger. When the person places his fingerprint on the glass plate, the sensor scans the light and dark areas created by fingerprint ridges and creates a digital image. Capacitive-based fingerprint scanner creates the fingerprint images by using electrical current instead of light. Multispectral imaging sensor was introduced to reduce fingerprint sensors’ vulnerability to spoofing attacks [16], [17].

Many methodologies are being introduced now for fingerprint spoof detection [7], [12], which uses various approaches like deep learning, Pattern-based, etc. Among all the approaches CNN (Convolution Neural Network) is widely used because it mainly applied for image recognition and object recognition, image classifications, etc. It relies on a multilayer perceptron. They are made of multiple neurons consisting of weights and biases, which can be learned [18]. Basic convolution neural network shown in Figure 2. Although CNN-based spoof detectors have shown good results in spoof detection, they require a large training dataset, which is a challenging and expensive task as there are thousands of spoof materials available. At times the size of the fingerprint image needs to be manipulated according to the network, which will in turn cause loss and distortion in the fingerprint image, so to avoid this problem, patch-wise convolution technique was introduced [19],[20]. Hence CNN is mainly used for feature extraction and SVM (Support vector machine) is used for learning purpose as it can handle large data compared to CNN. Support vector machine is a supervised machine learning algorithm used for classification and regression analysis. It uses a kernel function to obtain optimal boundary between multiple outputs [21].

1.4 Performance Evaluation of Fingerprint spoof detection techniques:

![Figure 2: Structure of basic CNN](image)
Several criteria determine the efficiency of the Bona Fide Classification Error Rates (BPCER) fingerprint spoof identification technique that recognises the incorrectly-classified live fingerprints as false fingerprints. FerrFake often refers to an error classification of fingerprints, and FerrFake also explains the incorrect classification of fingerprints as an attack classification error rate (APCER) [22].

1.5 Databases used for training and testing:
Many public databases are available for the researchers to explore in this area. The most widely used databases are from Liveness Detection Competition (LivDet) [22]–[24]. These competitions were being organised as a joint venture of the University of Cagliari and the Clarkson University in 2009. They had many variants like LivDet 2009, LivDet 2011, LivDet 2013, LivDet 2015, LivDet 2017 and LivDet 2019. These databases contain large quantities of fake and live fingerprint samples used in fingerprint spoof detection techniques. Another database used for testing fingerprint spoof detection is ATVS-FFp Database which contains around 800 real fingerprints and many fake fingerprints (with and without cooperation) [25],[26]. CASIA Fingerprint Image Database is also used and contains 20,000 fingerprint images [27],[28].

As per the survey done in this paper, the ACE score of close-set problems from 2013 to 2017 ranges from worst ‘7.87’ to best ‘1.9’. Table 2 gives a brief view of ACE scores achieved during these years. It is elaborated in section 2 of this paper.

| Year   | Technique | ACE  |
|--------|-----------|------|
| 2013   | [29] Weber local descriptor. (WLD + LPQ) | 7.87 |
| 2014   | [30] Convolution neural network (CNN) | 6.45 |
| 2014   | [31] Local Contrast phase descriptor (local contrast and LPQ) | 5.7 |
| 2015   | [32] DCNN + Voting strategy | 3.5 |
| 2015   | [33] Quality Features | 2.1 |
| 2016   | [34] Gradient-based texture features | 6.635 |
| 2016   | [19] Random Sample patches + CNN | 3.42 |
| 2017   | [35] CNN + PCA | 4.5075 |
| 2017   | [36] Worked on BISF (binarized statistical image features) | 3.03 |
| 2017   | [37] CNN Patch based voting approach | 1.9 |

Similarly, for open-set solutions known to date, the lowest ACE score was 1.02, which used a software-based approach using some spoof samples. It is further elaborated in section 3.

2. Closed-set problems
It is a recognition problem where training and the testing dataset contains the same spoof materials. Many works are done under this category, using various approaches [12]. In this paper, some of the work done under the closed-set problem is shown below, along with their comparison table.

Work by [29] has used local weber Descriptor (WLD) for fingerprint liveness detection. Using Weber law, the researchers obtained two components (differential excitation, and orientation) for each image's pixel. A joint histogram was processed for these two components to build discriminative features that were then trained by SVM classifier using a linear kernel function. Also, they combined WLD with LPQ (local phase quantisation) to improve performance.

Work by [31] proposed an approach for fingerprint liveness detection using local contrast phase descriptor. In this method, the image under test is processed in parallel in spatial and transform domain. Two features (local contrast, LPQ) are computed for every pixel of the image for which 2D histogram is calculated combinedly. Then using feature selection, the image is classified as fake and live.
The work by [30] is broadly divided into four parts: firstly, pre-processing of the fingerprint image is done in which image is reduced to improve accuracy. In the second part, features are extracted from the reduced image using LBP (local binary pattern) and convolution network. In the third part, the dataset is normalisation to zero mean and unit variance. The normalised data is reduced dimensionally using PCA (principal component analysis). In the last part, features are fed to SVM (support vector machine). Data augmentation is also used to improve accuracy and getting rid of the overfitting problem. The researchers have used 4 different pipelines (convNet+PCA+SVM, AUG+ConvNet+PCA+SVM, LBP+PCA+SVM, AUG+LBP+PCA+SVM) and compared results for three Database LivDet 2009, LivDet 2011, LivDet 2013. For LivDet 2009 LBP+PCA+SVM showed the best result. For LivDet 2011 ConvNet+PCA+SVM showed the best result, and for LivDet 2013 AUG+ConvNet+PCA+SVM showed the best result.

[33] has performed fingerprint spoof detection by evaluating three types of fingerprints such as Ridge clarity features such as spatial coherence and clustering factor, Ridge Strength features such as ridge frequency, contrast map, Direction map and Ridge continuity features such as Gabor features, uniformity of frequency field. This technique is completely software-based and does not include any additional hardware cost.

[32] have proposed an approach for fingerprint liveness detection using DCNN (deep convolution and neural network) and voting strategy. In this work, they used DCNN for feature extraction and classification and used small patches of fingerprint images rather than using the whole image. They used a voting strategy to combine all patches result for one fingerprint image.

Work done by [38] has proposed an approach for fingerprint spoof detection in which contrast enhancement using histogram equalisation is performed for fingerprint images. Then the image is divided into many non-overlapping blocks. These both are performed in a pre-processing phase. Each block is then learned with CNN, which detect spoofness score and at last, all blocks score is combined to get final spoof decision result. In this approach, CNN is composed of 6 layers in which four layers are convolution layer, and two layers are deep. The final spoof detection is based on the majority voting system, which adds up all the block result and classifies input fingerprint image as fake or live.

Work by [19] has proposed a CNN based approach in which features were extracted from input fingerprint patches. They conducted segmentation of fingerprint image and augmentation after which a normal distribution obtains the patch location. The final decision to live and fake fingerprint is done through the voting strategy of all patches.

The identification of a lifetime in [34] fingerprints is achieved using gradient-based texture characteristics. It classifies fingerprint vitality as a two-class classification problem and generates an image gradient co-occurrence matrix to derive its functions. They have used a second-order and third-order features SVM grouping.

[36] has proposed a technique for fingerprint spoof detection using a local textural feature where binarised statistical image features (BSIF) is adopted. BSIF is used to convert texture features of fingerprint images into binary codes for every pixel based on filter responses.

The method proposed fingerprint liveness detection technique based on patch-based voting approach. Initially, they performed segmentation of images to eliminate background noise after which patches were extracted from the foreground part of the image and trained by Convolution neural network (CNN). At last final decision is taken by combining resultant spoofness scores of all patches.

A different approach by [35] has proposed fingerprint liveness detection based on feature extraction technique using CNN with PCA. In this approach, first, the ROI (Region of interest) is extracted from the original fingerprint image, which will eliminate all the useless region being obtained at the time of fingerprint being captured through the sensor. This pre-processed image will be the actual input image to convolution neural network layers. They have used five layers in CNN, which will generate deep high-level features by combining low-level features using ReLU as the activation function. The learned features are then sent to SVM classifier for classification. PCA is used along with CNN for polling operation performed after convolution operation to reduce the dimensionality of features obtained using a max-pooling function and applied only on the first three
layers. This approach has improved the training and classification performance of liveness detection. Table 3 shows the comparison of various closed-set approaches based on the methodology used, their training and testing dataset and respective ACE scores for LivDet 2009, LivDet 2011 and LivDet 2013.

**Table 3:** Performance Comparison of Various Closed-set approaches reported on LivDet 2009, LivDet 2011 and LivDet 2013 in terms of Average Classification Error (ACE)

| Technique | LivDet 2009 | LivDet 2011 | LivDet 2013 |
|-----------|-------------|-------------|-------------|
| Biometric / crossmatch / liveness | | | |
| Biometric / crossmatch | 0.31 | 7.20 | 3.29 |
| Identix | 1.59 | 12.65 | 7.87 |
| Average | 1.16 | 8.00 | NA |
| Weber local descriptor- (WLD + LPQ) | | | |
| Biometric / crossmatch | | | |
| Italdata | 2000-L | 2000-L | 2000-L |
| Digital persona | 3000-L | 4000-L | 4000-L |
| Sagmen | 2000-L | 2000-L | 2000-L |
| Average | 2000-L | 3000-L | 2000-L |
| Non-overlapping | | | |
| Convolutional neural network (CNN) | | | |
| Data set divided into half and half | | | |
| 18000 images of live and spoof | | | |
| Non-overlapping | | | |
| Local Contrast phase descriptor (local contrast and LPQ) | | | |
| Non-overlapping | | | |
| Quality features | | | |
| - | - | - | - |
| 520-S | 2500-L | 520-L | 2500-L |
| 1000-S | 1000-L | 1000-S | 1000-L |
| 750-S | 750-L | 750-S | 750-L |
| 6.56 | 3.5 | 3.5 | |
| DCNN + Voting strategy | | | |
| DCNN | NA | 3.5 | 0 |
| Voting strategy | NA | 0.2 | 0.2 |
| Random Sample patches + CNN | | | |
| Training set - 523 | NA | 3.42 | 3.42 |
| Validation set - 113 | NA | 3.42 | 3.42 |
| Testing set - 114 | NA | 3.42 | 3.42 |
| Gradient | 11.3 | 6.23 | 6.3 |
| 2.0 | 11.7 | 5 |
| 5.4 | 4.75 | 3.34 |
| 6.63 | 5 |
Based on Table 3, it can be depicted that the various Closed-set approaches reported for LivDet 2013 showed better results in terms of ACE as compared to other two Datasets. The minimum ACE score was 1.35 using methodology given by [32] for LivDet 2013. Figure 3 shows the line graph of ACE values from 2013 to 2017. As from 2013 to 2017, ACE is alternately increasing and decreasing, hence there is no particular pattern. This leads to a gap in the study as no fingerprint spoof detection methodology can be stated better in a particular year.

Figure 3: Comparison of ACE score from 2013 to 2017
3. Open-Set problems
It is the recognition problem where training and the testing dataset contains different spoof materials. It can be further classified into two categories: one class open-set problem and two class open-set problem.

3.1 In one class open-set problem:
only live fingerprints are used in the training set. This approach's idea is that if the system/model learns about the concept of live fingerprints, it can reject any material spoof fingerprints. Also, it will reduce the task of creating spoof fingerprints from multiple materials. Sometimes some spoof fingerprints can be used in validation phase done before testing to refine the decision boundary. The model can also be trained with only fake fingerprints to determine new spoofs materials coming across the testing phase. Some of the work done under this category is described below:

Work has proposed an approach of a novel ensemble of multiple One-Class SVM (OC-SVM) classifiers where a set of live fingerprints are used to learn them by determining the local textural features using LBP (local binary pattern), GLCM (grey level co-occurrence matrix), BSIF (Binarized Statistical Image Features), LPQ (Local Phase Quantisation), BGP (Binary Gabor Pattern). Table 4 gives a brief idea about these features. The training data set does not depend on a single feature space. Each OC-SVM uses a different set of features and some fake fingerprints to refine the decision boundary. The output of multiple OC-SVM is combined using majority voting and LSE-based weighting approach. This technique requires fewer spoof samples at the time of training and observed stable performance across different fabrication material. Obtained correct detection rate (CDR) of OC-SVM was on average of 87%, which is better compared with B-SVM (binary SVM). The database used is LivDet 2011.

| LBP | LPQ | GLCM | BSIF | BGP |
|-----|-----|------|------|-----|
| local binary pattern | Local Phase Quantization | grey level co-occurrence matrix | Binarized Statistical Image Features | Binary Gabor Pattern |
| It is visual descriptor used for texture classification. | It is powerful descriptor used for classification of texture blurriness | It is used to obtain the texture of an image which consider spatial relationship of pixels | It is used to convert texture features of fingerprint images into binary codes for every pixel based on filter responses. | It is used to encode the texture information obtained from fingerprints by entwine the image with Gabor filter and binarizing the response. |

A different approach has used only live fingerprints for training purpose. At first, the pre-processing of the live fingerprint image is conducted. The region of interest (ROI) is extracted for three images (raw FTIR image, processed FTIR image and direct-view image), reducing the noise and learning task. Now, these processed images are trained via three different Generative Adversarial Network (GAN). The generator is used for each GAN which will produce synthesises live fingerprint image. The actual live image and the synthesised image are fed to discriminator, distinguishing between the actual live fingerprint and synthesised live fingerprint images. This hypothesis is then used in a testing phase for distinguishing between live and spoof fingerprints. Training three GAN results obtained by each discriminator and it will be fused to produce final spoofness score. They have used 5.5k spoof images from 12 different materials and 11.8K live fingerprint images and has improved the cross-material spoof detection performance.

Approach has worked on incremental learning approach for spoof detection in which they have trained the model with some spoof fingerprints of known material. They have constructed the novel-
material detector known as an expert, determining whether the input image is from untrained spoof material. If it is new, then the spoof sample will update the existing spoof detector by integrating new spoof samples with the existing spoof-detection model using W-SVM (Weibull-calibrated SVM) technique. The expert is based on three features LPQ, LBP, BSIF. This paper has formally improved the performance of new material spoof fingerprint detection and generalisation ability.

Table 5: Average Classification Error

| Techniques                          | ACE  |
|------------------------------------|------|
| [40] ensemble of one-class SVM      | 9.25 |
| [42] One-class Classifier           | 2.4  |
| [43] Incremental learning Method    | 8.25 |

Table 5 shows a comparison between techniques based on average classification Error (ACE) and Generalizing Fingerprint Spoof Detector: Learning a One-Class Classifier [42] shows the best result, as it has the lowest ACE compared to other two techniques.

3.2 In two class open-set problem:
both live and fake fingerprints are used for training model. Some of the work done under this category is described below:

Work has developed a convolution neural network (CNN) based approach in which they have to utilise local patches extracted from fingerprint minutiae. These local patches are then trained by Inception v3- CNN model to generate global spoofness score to distinguish between fake and live fingerprints. The proposed approach has reduced up to 69% average classification error for spoof detection under both known and unknown spoof materials for LivDet 2015 dataset.

Work has shown an approach towards open-set spoof detection technique in which they proposed a method based on multi-scale local binary pattern (MSLBP). They used two types of MSLBP where each type was combined with some set of filters. They used both live and spoof images to calculate MSLBP, which are then normalised in the training phase. This normalised data is subjected to ten-fold cross-validation to obtain scale and normalisation method for testing phase. These images are then trained using SVM. They have also experimented their results for cross-device inter-operability and used database LivDet 2011.

The method proposed had developed a framework in which the features extracted from the input fingerprint were subjected to correlation mapping features of the same class, i.e., spoof or live are highly correlated. Partial least square (PLS) was used to learn correlation. These features were then sent to the discriminative-generative classification scheme, which was used for spoof detection. The SVM used here is composed of three generative classifiers GMM (Gaussian Mixture Model), QDA (Quadratic Discriminant Analysis) and GC (Gaussian Copula). Experiments were conducted on LivDet 2011 and LivDet 2013 datasets.

Approach has proposed a scheme in which the new input fingerprint sample is first detected as novel spoof material by the novel material detector and then automatically adopted by fingerprint spoof detector using W-SVM approach. The model is also trained with live fingerprints. This scheme has achieved an average correct detection rate up to 70% on the LivDet 2011 database, and for the novel material detector, it improved up to 46% compared to previously proposed techniques.

Work by has used an approach for fingerprint liveness detection by combining low-level gradient features from Speeded-Up Robust Features (SURF), pyramid extension of the Histograms of Oriented Gradient (PHOG) and texture features from Gabor wavelet using dynamic score level integration. They also formed a dynamic score level integration module for combining results of two individual classifiers.

Work done by discussed the interoperability of sensors used for capturing the fingerprint images. The fingerprint spoof detection challenges not only depend on the spoof materials but also on the
sensors used to obtain images. They have proposed an approach to overcome this interoperability issue using Least square Method (LSE). The features extracted from two different datasets being captured by different sensors are used to obtain a transformation matrix that will transform one feature space into another feature space. This method allowed considerable accuracies for sensors interoperability.

It has proposed an approach based on the sparse representation used for face recognition and can be used for fingerprint spoof detection. They have used the SRC algorithm in the training stage, which handles open set recognition problem. This algorithm uses the reconstruction error obtained by EVT (Extreme value theory).

Work done by [20] has proposed an approach in which they have used patches extracted from fingerprints rather than using the whole fingerprint. These patches are then trained by fully convolution network layer with a fewer number of parameters. As they have classified fingerprints into three categories: fake, live, and background hence pre-processing task is integrated with CNN. The learned CNN is used to find the optimal threshold value. This threshold value is used to distinguish between fake and live fingerprints in the testing phase. Using patches instead of the whole fingerprint image is advantageous, as the convolution network constructed is independent of fingerprint size and the amount of training data can be increased. They have use databases of LivDet 2011, LivDet 2013 and LivDet 2015 and average classification error (ACE) rate is 1.35%. Figure 4 describes the overall system architecture of processing method with process flow.

This approach consists of following steps: 1) Image Normalisation and database Augmentation: under this region of interest is obtained from the fingerprint image, and then ROI is resized, and patches are obtained from it. These patches will be the input from DBM 2) DBM training. In this part, the grayscale patches obtained are initially trained via GB-RBM (Gaussian-Bernoulli RBM) which convert real-valued patches to posterior probabilities of activation are then fed to DBM. 3) Feature Extraction and SVM training: after training fingerprint patches with DBM, high-level features are obtained, and these features vectors are dimensionally reduced through PCA and fed to SVM for classification. They have obtained the accuracy of around 85.82% and is robust due to its deep architecture. Figure 5. describes the architecture of how Deep Boltzmann Machine (DBM) works.
Figure 5: The basic architecture of Deep Boltzmann Machine (DBM)

Table 6 shows the comparison of various open-set approaches based on Average Classification Error (ACE) score (cross-sensor, cross-material and cross-dataset), Equal Error Rate (ERR) and training - testing dataset comprising of many fake fingerprints and live fingerprints used for LivDet 2011, 2013 and 2015. According to Table 6, the minimum ACE score for cross-sensor was 3.9, for cross-dataset was 4.825 and for cross-material 0.95. Hence, the experiments when conducted for cross-material showed better results as compared to the other two. Also, the techniques [20] using patches instead of whole fingerprints for training purpose showed ACE of 0.275, which is the minimum among all the ACE scores of various techniques. The minimum EER is 3.9.

Table 6: Performance Comparison of Various open-set approaches reported on LivDet 2011, LivDet 2013 and LivDet 2015 in terms of Average Classification Error (ACE) for Cross-sensor, ACE for Cross-material, ACE for Cross-dataset and Equal Error Rate (EER) along with training and testing dataset

| Technique                          | Dataset          | Live/fake fingerprints Training set | Live/fake fingerprints Testing set | ACE (Cross-sensor) | ACE (Cross-material) | ACE (Cross-dataset) | EER               |
|------------------------------------|------------------|------------------------------------|-----------------------------------|--------------------|----------------------|----------------------|---------------------|
| Minutiae-centred patches           | LivDet 2011      | 4000/4000                          | 4000/4000                         | 1.67               | 25.28                | 7.2                  | 7.15                |
|                                    | LivDet 2013      | 2000/2000                          | 2000/2000                         | 0.25               | 3.9                  | 0.95                 | 28.66               |
|                                    | LivDet 2015      | 4510/4473                          | 4500/5948                         | 0.97               | NA                   | 1.25                 | NA                  |
| Multi-scale Local binary pattern (MSLBP) | LivDet 2011 | 4000/4000                          | 4000/4000                         | 7.475              | 48.38                | NA                   | 7.525               |
|                                    |                  |                                    |                                   |                    |                      |                      | 9.075               |
| used correlation mapping along with discriminative-generative classification scheme | LivDet 2011      | 1000/1000                          | 1000/1000                         | NA                 | NA                   | NA                   | 6.077 (Average of 9 various proposed schemes) |
|                                    |                  |                                    |                                   |                    |                      |                      |                     |
|                                    | LivDet 2013      | 1250/1250                          | 1250/1250                         | NA                 | NA                   | NA                   | 8.34 (Average of 9 various proposed schemes) |

Legend:
- **ERR<sub>unknown</sub> (TS1)**: GMM 8.4, GC 7.2, QDA 7.2
- **ERR<sub>unknown</sub> (TS2)**: GMM 7.1, GC 6.5, QDA 6.7
used low-level features SURF, PHOG.

LivDet 2011

\[
\begin{array}{c|c|c|c|c}
 & \text{T1-500/500} & \text{T2-500/500} & \text{NA} & \text{NA} \\
\hline
\text{LivDet 2011} & 1000/800 & 1200/1000 & 6.9 & 18.1 \\
\end{array}
\]

LivDet 2013

\[
\begin{array}{c|c|c|c|c}
 & \text{T1-500/500} & \text{T2-500/500} & \text{NA} & \text{NA} \\
\hline
\text{LivDet 2013} & 1000/1000 & 1200/1000 & 2.61 & 15.95 \\
\end{array}
\]

Fully CNN using minimal number of parameters and optimal threshold for fingerprint patches

LivDet 2011

\[
\begin{array}{c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} \\
\hline
\text{LivDet 2011} & 278463/2751 & 137758/1358 & 82068/80146 \\
\end{array}
\]

LivDet 2013

\[
\begin{array}{c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} \\
\hline
\text{LivDet 2013} & 124407/1225 & 61686/60397 & 149300/12906 \\
\end{array}
\]

LivDet 2015

\[
\begin{array}{c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} \\
\hline
\text{LivDet 2015} & 519174/4307 & 251159/2136 & 149300/12906 \\
\end{array}
\]

utilises gram module for detecting fake fingerprints

LivDet 2011

\[
\begin{array}{c|c|c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} & \text{NA} & \text{NA} \\
\hline
\text{LivDet 2011} & 4000/4000 & 35991/34964 & 4500/3851 & 4500/3851 & 4500/3851 \\
\end{array}
\]

LivDet 2013

\[
\begin{array}{c|c|c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} & \text{NA} & \text{NA} \\
\hline
\text{LivDet 2013} & 124407/1225 & 61686/60397 & 149300/12906 & 149300/12906 & 149300/12906 \\
\end{array}
\]

LivDet 2015

\[
\begin{array}{c|c|c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} & \text{NA} & \text{NA} \\
\hline
\text{LivDet 2015} & 4000/4000 & 35991/34964 & 4500/3851 & 4500/3851 & 4500/3851 \\
\end{array}
\]

Style transfer-based augmentation wrapper i.e. universal material transfer (UMT)

LivDet 2015

\[
\begin{array}{c|c|c|c|c}
 & \text{Patch-32*32} & \text{Patch-48*48} & \text{Patch-64*64} & \text{NA} \\
\hline
\text{LivDet 2015} & 519174/4307 & 251159/2136 & 61686/60397 \\
\end{array}
\]

Deep Boltzmann Machine (DBM) for extraction of high-level features.
Figure 6 shows a brief view of ACE values for cross-sensory, cross-material, and cross-dataset 2013, 2016, 2018, and 2019. It can be depicted that there is no particular pattern for ACE scores. ACE for cross-sensor from 2013 to 2018 showed a decreasing trend. In 2018, ACE for all three (cross-sensor, cross-material, cross-dataset) resulted in a minimum score. Hence, it can be said that the methodology[20] used in this year is better than in other years.

**Figure 6. Brief Comparison of various ACE for 2013, 2016, 2018 and 2019**

### 4. Conclusion

Fingerprint spoof detection is a challenging task in the biometric recognition system and should be done with utmost care to prevent threats. Many researchers give many closed-set solutions for spoof detection, but they face certain challenges like poor generalisation performance, high memory and computational requirement, which need to be addressed. Open-set recognition techniques somewhat overcome these issues. The idea behind open-set fingerprint spoof detection techniques is to handle unseen conditions with robustness. Although there is still a need to improve Fingerprint Spoof detection approaches as they are difficult to generalise, efforts are evident in the above-cited work that researchers find new ways for open-set scenarios. Much work on open-set problems are being carried out based on deep-learning approaches and showed good results for the same, but no solution showed 100% accuracy but minimum ACE. There is a need for universal guidelines in handling spoof samples using uniform open-set architecture.

### 5. Future Scope

Due to universal users, multiple hardware and localised software-based approaches for fingerprint spoof detection, there is a need to have more case study-based open-set solutions to be elaborated. Hence, the author believes that our work will provide direction for finding out areas of failure in fingerprint spoof detection and address those areas with the most robust approach. Author’s future work will be providing of such solution which will give a more generalised result.
References

[1]. A. Othman, “Biometric system,” 2018. [Online]. Available: https://www.veridiumid.com/blog/biometric-system-secure/

[2]. J. E. Hoover, “Fingerprint Anatomy,” 2016. [Online]. Available: https://www.britannica.com/topic/fingerprint

[3]. A. A. A. Goshtasby, Advances in Computer Vision and Pattern Recognition. 2012.

[4]. R. Blanco Gonzalo et al., “Attacking a Smartphone Biometric Fingerprint System: A Novice’s Approach,” Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2018-Octob, no. 675087, pp. 0–4, 2018.

[5]. B. Mele and G. Altarelli, "Lepton spectra as a measure of b quark polarisation at LEP," Phys. Lett. B, vol. 299, no. 3–4, pp. 345–350, 1993.

[6]. E. Marasco and A. Ross, “A survey on antispooﬁng schemes for fingerprint recognition systems,” ACM Comput. Surv., vol. 47, no. 2, 2014.

[7]. S. S. Kulkarni, “Survey on Fingerprint Spoofing, Detection Techniques and Databases,” no. Ncac, pp. 30–33, 2015.

[8]. D. Singh, Fake Fingerprint. 2013.

[9]. ITL, “biometric devices and fingerprint spoofing,” 2006. [Online]. Available: http://www2.washjeff.edu/users/ahollandminkley/Biometric/.

[10]. A. S. Ahmad, R. Hassan, and M. N. Ahmad, "Fake Fingerprint Detection Approaches: A Systematic Review 2 Fig. 2 Example of fake ﬁngerprints. (a) reverse-engineered ﬁngerprint image; (b) 2-D fake ﬁngerprint using silicone; (c) cadaver ﬁngerprint; (d) synthesised 3-D fake ﬁngerprint [3]," no. 5, pp. 1–8, 2019.

[11]. A. S. Ahmad, R. Hassan, and R. M. Othman, “An investigation of fake fingerprint detection approaches,” AIP Conf. Proc., vol. 1891, no. October, 2017.

[12]. C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: A survey,” IET Biometrics, vol. 3, no. 4, pp. 219–233, 2014.

[13]. Michael eckmann, “open set source camera attribution,” Costa, Filipe & Eckmann, Michael & Scheirer, Walter & Rocha, Anderson. (2012). Open Set Source Camera Attribution. Brazilian Symposium of Computer Graphic and Image Processing. 71-78. 10.1109/SIBGRAPI.2012.19., 2012.

[14]. D. Thakkar, “BAYOMETRIC.” [Online]. Available: https://www.bayometric.com/fingerprint-reader-technology-comparison/.

[15]. R. Triggs, “Fingerprint scanner,” 2019. [Online]. Available: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/.

[16]. K. O’Shea and R. Nash, “An Introduction to Convolutional Neural Networks,” no. November, 2015.

[17]. E. Park, “Fingerprint Liveness Detection using CNN Features of Random Sample Patches.” 2016.

[18]. E. Park, X. Cui, W. Kim, J. Liu, and H. Kim, “Patch-based Fake Fingerprint Detection Using a Fully Convolutional Neural Network with a Small Number of Parameters and an Optimal Threshold,” pp. 1–12, 2018.

[19]. T. Evgeniou and M. Pontil, “Workshop on Support Vector Machines: Theory and Applications,” Mach. Learn. Its Appl. Adv. Lect., no. January 2001, pp. 249–257, 2001.

[20]. M. S. Nixon, Handbook of Biometric Anti-Spoofing. Springer International Publishing, 2019.

[21]. V. Mura et al., “LivDet 2017 fingerprint liveness detection competition 2017,” Proc. - 2018 Int. Conf. Biometrics, ICB 2018, pp. 297–302, 2018.

[22]. G. Orrù et al., “LivDet in Action - Fingerprint Liveness Detection Competition 2019,” 2019.

[23]. N. Evans, T. Kinnunen, J. Yamagishi, Z. Wu, F. Alegre, and P. De Leon, Handbook of Biometric Anti-Spoofing. 2014.
[24]. “Biometrics and Data Pattern Analytics,” BiDA labs. [Online]. Available: http://atvs.ii.uam.es/atvs/ffp_db.html.

[25]. C. Fingerprint and I. Database, “Note on CASIA-FingerprintV5,” vol. 0.

[26]. “Biometrics Ideal Test,” BIT. [Online]. Available: http://biometrics.idealtest.org/findDownloadDbByMode.do?mode=Fingerprint.

[27]. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Fingerprint liveness detection based on Weber Local image Descriptor,” 2013 IEEE Work. Biometric Meas. Syst. Secur. Med. Appl. BioMS 2013 - Proc., no. September, 2013.

[28]. A. Ijcb, “Fingerprint Liveness Detection using Convolutional Networks,” pp. 1–8, 2014.

[29]. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Local contrast phase descriptor for fingerprint liveness detection,” Pattern Recognit., vol. 48, no. 4, pp. 1050–1058, 2014.

[30]. J. Yang, J. Yang, Z. Sun, S. Shan, W. Zheng, and J. Feng, “Biometric recognition: 10th Chinese conference, CCBR 2015 Tianjin, China, November 13-15, 2015 proceedings,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9428, pp. 241–249, 2015.

[31]. G. Arunalatha and M. Ezhilarasan, “Fingerprint spoof detection using quality features,” Int. J. Secur. its Appl., vol. 9, no. 10, pp. 83–94, 2015.

[32]. Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, and Y. Q. Shi, “Fingerprint liveness detection using gradient-based texture features,” Signal, Image Video Process., vol. 11, no. 2, pp. 381–388, 2016.

[33]. C. Yuan, X. Li, Q. M. J. Wu, J. Li, and X. Sun, “Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis,” vol. 53, no. 4, pp. 357–372, 2017.

[34]. L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, “Fingerprint liveness detection using local texture features,” IET Biometrics, vol. 6, no. 3, pp. 224–231, 2017.

[35]. A. Toosi, S. Cumani, and A. Bottino, “CNN patch-based voting for fingerprint liveness detection,” IJCCI 2017 - Proc. 9th Int. Jt. Conf. Comput. Intell., no. Ijcci, pp. 158–165, 2017.

[36]. S. Saadah and G. S. Wulandari, “Information Science and Applications,” Lect. Notes Electr. Eng., vol. 339, pp. 777–784, 2015.