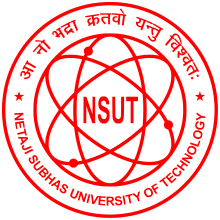
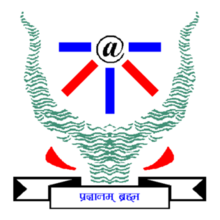
**FINGERPRINT LIVELINESS DETECTION TO MITIGATE SPOOFING ATTACKS USING GENERATIVE NETWORKS IN BIOMETRIC SYSTEM**

**Sahil Bhola**  
**Netaji Subhas University of Technology**, New Delhi , nsitsahilbhola@gmail.com



Under the guidance of  
**Dr Satish Kumar Singh**  
Associate Professor, Department of Information Technology (Head Computer Vision and Biometrics Lab) , Centre for Cognitive Computing, **Indian Institute of Information Technology (IIIT-Allahabad)**



(A university established under Sec.3 of UGC Act, 1956 Vide Notification No. F.9-4/99- U.3 dated 04.08.2000 of the Govt. of India)

**INDEX**

|  |  |
| --- | --- |
| **Sr.No** | **Name** |
|  | Declaration |
|  | Acknowledgement |
|  | Certificate |
|  | Abstract |
| 1. | Introduction |
| 2. | Approaches |
| 3. | Implementation Details |
| 4. | Experimental Results and Inference |
| 5. | Conclusion |
| 6. | References |

**Declaration**

I declare that I have used LivDet Dataset in collaboration with Mr. Kapil Mishra (Research Scholar, CVB lab, IIIT-Allahabad) for the purpose of my internship assignment titled **FINGERPRINT LIVELINESS DETECTION TO MITIGATE SPOOFING ATTACKS USING GENERATIVE NETWORKS IN BIOMETRIC SYSTEM**. I have submitted all the work done in the form of codes, dataset, presentation and report. I hereby agree that I am not eligible to use it for either personal or commercial purposes without obtaining explicit license access from the original dataset owners.

(Sahil Bhola)

NSIT Delhi

**ACKNOWLEDGEMENT**

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I am highly indebted to **Dr Satish Kumar Singh** for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my special gratitude and thanks to **Research Scholar , Mr Kapil Mishra** for giving me such his resourceful time and without his help results and outcome of the work would not have been achieved

I would like to express my gratitude towards my parents & member of **(Computer Vision and Biometrics Lab , IIIT Allahabad )** for their kind co-operation and encouragement which help me in completion of this project.

I would also like to express my special gratitude and thanks to other researcher scholars for giving me such attention and time.

My thanks and appreciations also go to my colleagues in developing the project and people who have willingly helped me out with their abilities.

**BONAFIDE CERTIFICATE**

Certified that this project report titled **FINGERPRINT LIVELINESS DETECTION TO MITIGATE SPOOFING ATTACKS USING GENERATIVE NETWORKS IN BIOMETRIC SYSTEM**

is the bonafide work of **Sahil Bhola** (Reg No: R25) who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Signature

**Dr.Satish Kumar Singh**

(SUPERVISOR)

Associate Professor

Head Computer Vision and Biometrics Lab

Indian Institute of Information Technology Allahabad , India

**ABSTRACT**

#### Today fingerprint detection system are being used widely , from a corporate office to military camps . They are secure , have speed and accurate but they are vulnerable to spoof attacks. And the primary purpose of the fingerprint reader is to provide reliable and accurate user authentication but also to be secure and ensure user confidence.

#### The most prominent vulnerability in fingerprint spoof detection system were poor generalization of spoof classes that means whenever a unknown spoof material was given to detection system the error rate increases upto 3 folds .

To Improve the accuracy and performance of the fingerprint detection systems when fabricated to a unknown number of spoof materials thus decreasing the cross performance error rate. Hence improving the poor generalizing problem of a fingerprint spoof detector using generative and other convolution networks.

We are using one class classification and Minutiae extraction approaches using DCGANs and MobileNets Respectively and using these networks giving a spoof score to given fingerprint and found out that our results had an accuracy of 5-10% more than the previous binary spoof classifiers.

1. **INTRODUCTION**

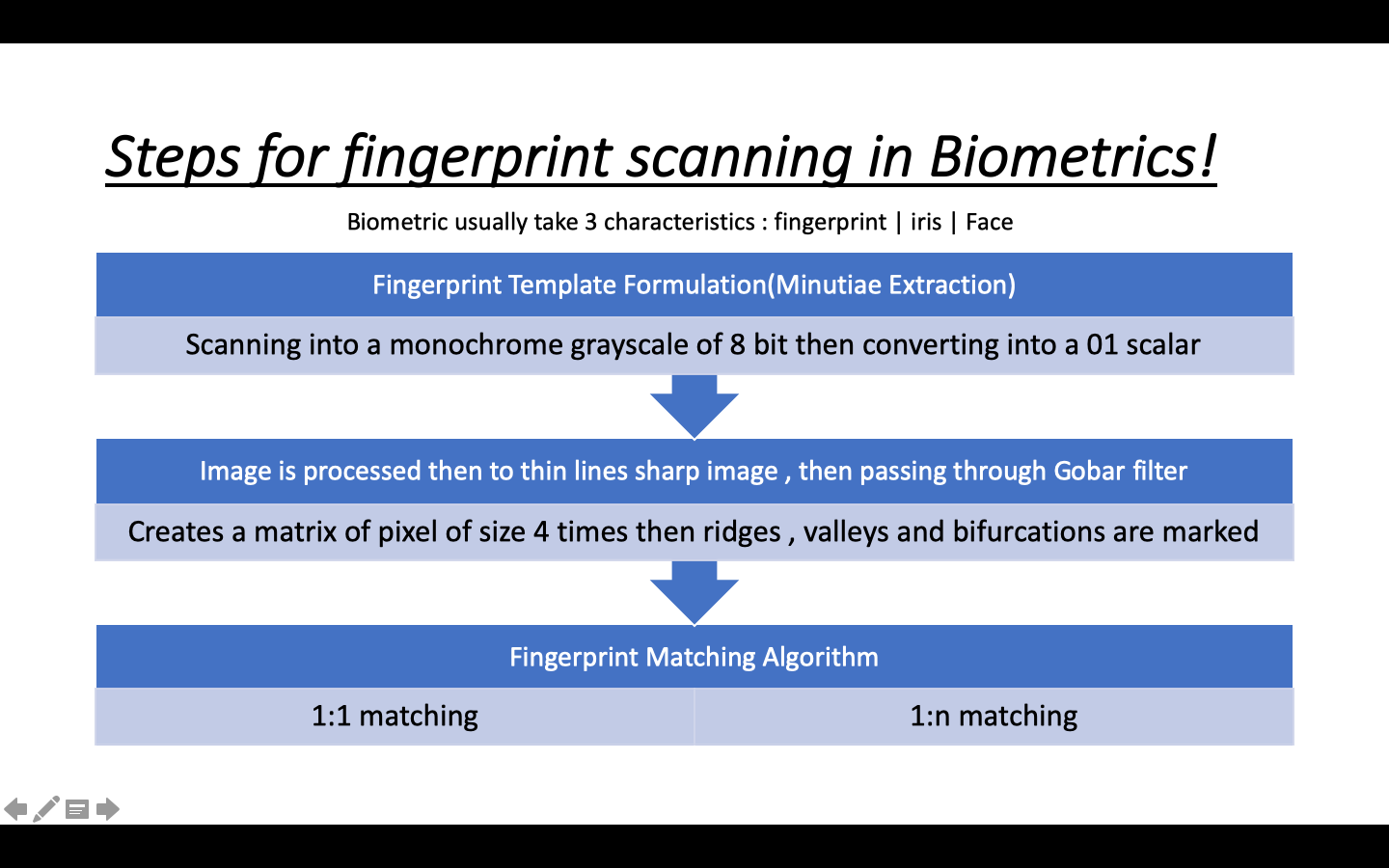
Today, fingerprints biometrics are taking place of traditional IDs, used in forensics, border crossing security, mobile authentications, payment transactions , ATM machines , laptops and places where user authentication is required. Locks can be stolen , safes can be broken, passwords can be guessed sooner or later . So how do we protect the things that we value?

Passwords and tokens are highly vulnerable to being lost or stolen..

Further, the costs of maintaining password and token based systems are very high and inefficient. Resetting lost or forgotten passwords takes up IT support time and reduces employee productivity. Fingerprint recognition looks for the unique patterns of ridges and valleys that are present in an individual’s fingerprint.

Here then we use biometrics say fingerprint scan , Retinal Scan , iris scan , Face scan as they cannot be forged. In specific fingerprints have, —the tiny **friction ridges** on the ends of our fingers and thumbs make it easier to grip things. What makes fingerprints such a brilliant way of telling people apart is that they are virtually unique.

These patterns are unique to every individual and thus help to identify individuals from an entire population. Fingerprints are inherent to individuals and can neither be lost nor stolen which makes it highly accurate and reliable Moreover, the availability of low-cost fingerprint readers coupled with easy integration capabilities has led to the wide spread deployment of fingerprint biometrics in a variety of organizations.



To avoid spoof detection automated fingerprint detectors were trained to distinguish between live and bonafide fingerprint from known spoof materials. But they were still vulnerable to spoofs made with materials not given in training

To solve this many Deep convolution networks using whole image and minutiae based local patches are used.

**Different Spoof Attacks :**

* In general , spoof attack is providing false data to gain illegitimate access to the system
* Spoof artifacts are provided to sensor to fool the system
* These artificial objects imitates biological and behavioral characteristics
* There are number of unknown & known spoof materials & techniques for the forgery of data or other resources.

**Example of Spoof Attacks:**

* In smartphones unlocking and accessing with fingerprint has become very common , hackers are gaining access by scanning and printing fingerprints by using conductive inks and printing on paper cut accessing mobile phones.
* In MSU , they have developed wearable finger that mimics human skin in optical , mechanical and electrical Properties
* Similarly various other cloning materials like playdoh, dental molding, 3D fingerprinting



1.Fingerprint cloning using fevicol. 2.Fingerprint Playdoh Cloning

1. **APPROACHES**

So there are two approaches: One we use GANs with considering spoof detection as a one class classification problem[3]. Another approach is to Extract Minutiae based patches and given them spoof score using MobileNets[2]. Hence our aim will be to implement these approaches and get better results as compared to the given binary CNN classifiers and CNN models using whole fingerprint images or randomly selected patches in a fingerprint Image

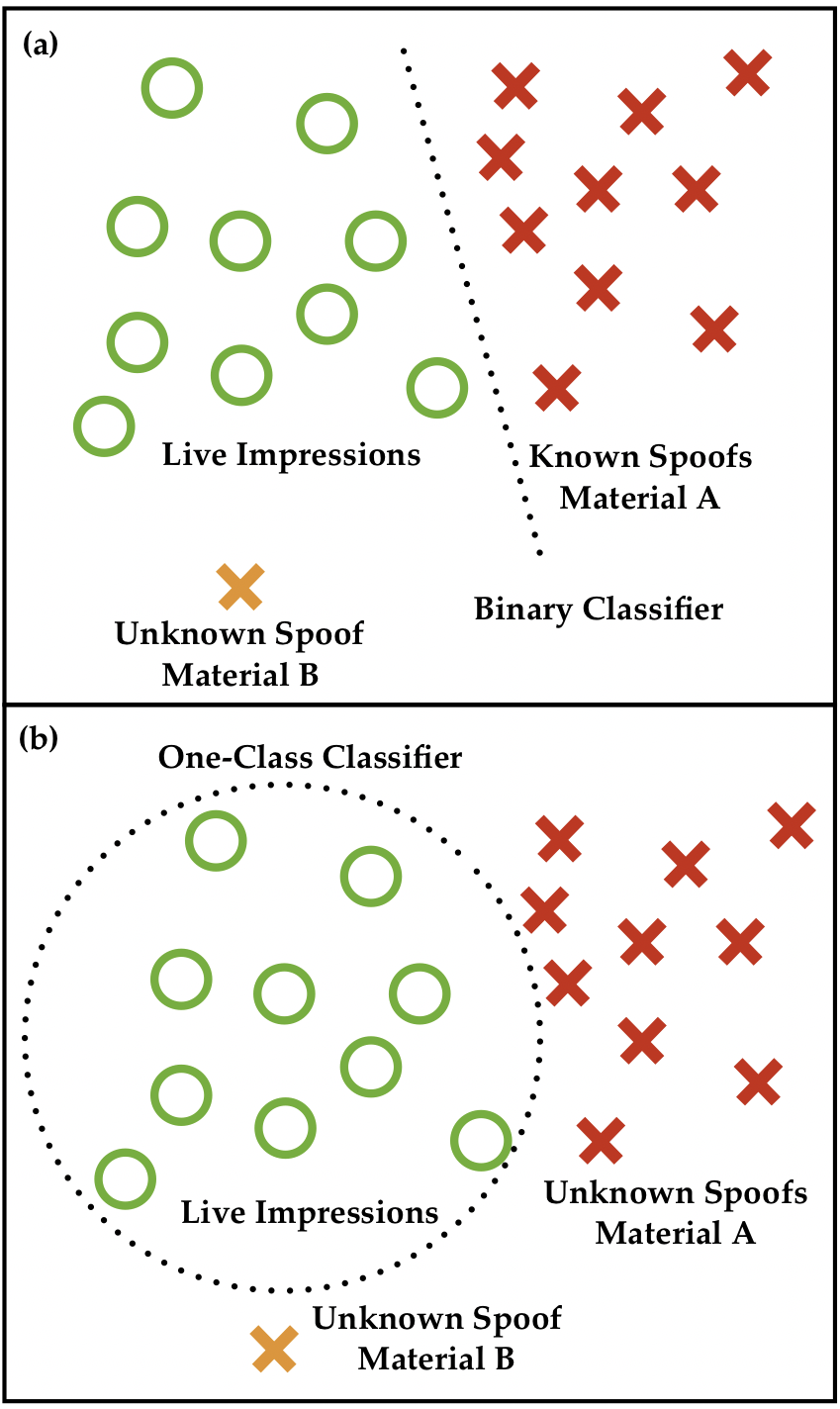
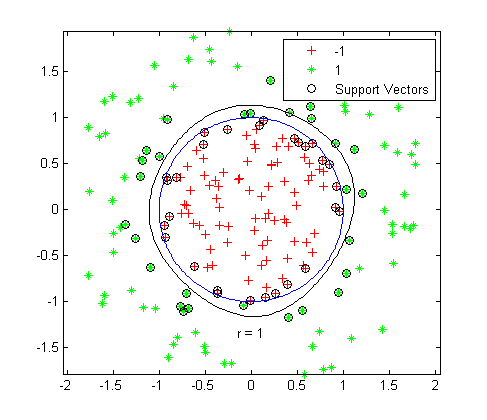
**2.1 Adversarial Liveliness Detection : One Class Classifier**

To avoid spoof detection automated fingerprint detectors were trained to distinguish between live and bonafide fingerprint from known spoof materials. But they were still vulnerable to spoofs made with materials not given in training. To solve this one class classification was proposed. Goal is to train the detector only to detect live fingerprints then spoof of any other material will be rejected. We accomplish this by training over our dataset with GANs network.

We consider spoof detection as a one class classification problem.

**2.1.1.Advantages of one class classifier over binary classifier?**

* Only live samples are needed for training thus eliminating task of fabricating large number of spoof impressions from multiple materials
* One class classifier do not overfit the data while binary does hence cross performance decreases
* It only learns what constitutes live fingerprint & do not use spoof material of any specific material during training.
* So they have a tight decision boundary around one class say live samples and all other class samples are unknown (i.e. spoof)

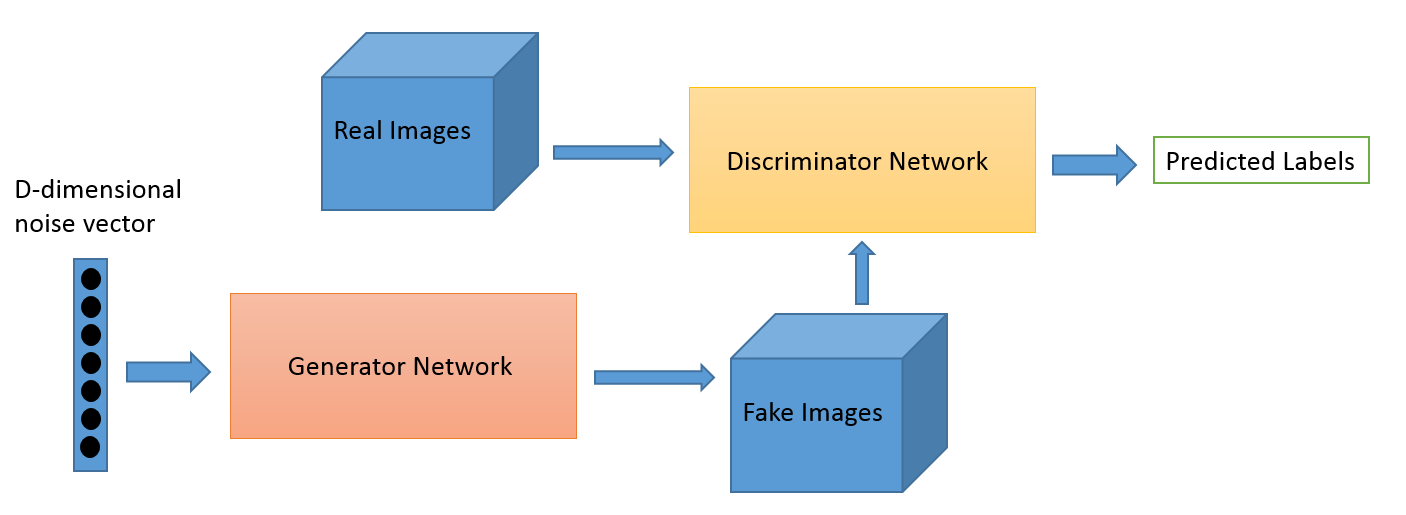
**2.1.2 Deep Convolution Generative Adversarial Networks .**

Generative Adversarial Network where two networks compete with each other in a zero sum game and converge at Nash Equilibrium . Gans have two components generator and discriminator.

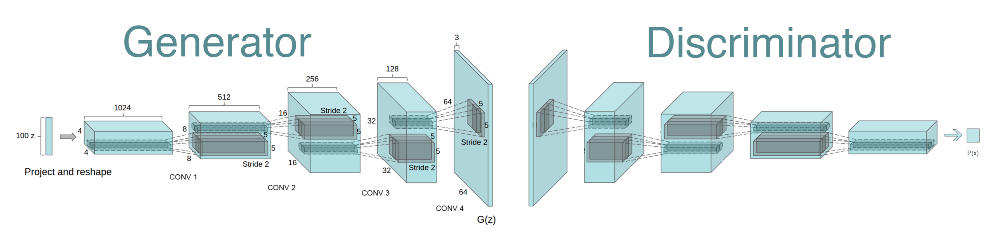
Discriminator is fed both generator synthesized and live fingerprints .

Generator learns to synthesize better fingerprints and discriminator learns to distinguish between synthesized and real.

Basically , Generator and Discriminator both are two CNN models coupled together.



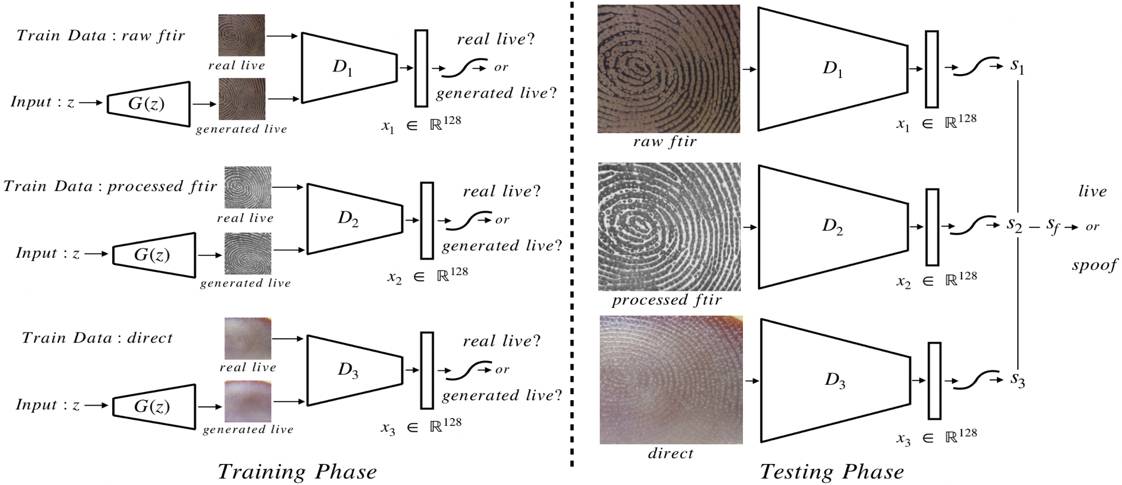
Generator network And Discriminator Network



**2.1.3 DCGAN Architecture and training over the fingerprint Dataset**

The DCGAN training involved three steps

1. Generating fake fingerprint images by passing gaussian noise into generator and updating binary entropy loss with Adam optimiser and learning rate = 0.0002 using stride over pooling
2. Then using the dataset having only real fingerprints and generated fingerprints as input to discriminator and a sigmoid output giving value between 0 and 1.
3. In testing phase removing the generator and using only discriminator to give the sigmoid output.
4. Generator is using Deconvolution and having an output of image of 64\*64 and Discriminator is just mirror network of Generator.
5. Initially in DCGAN training we freeze the weight updating of Discriminator and only our generator get trained hence getting synthesised images and saving them.
6. Then using real and generated images to train the discriminator again



* Architecture discriminator had 5 convolution layers each having 5x5 filter and stride of 2, an average pooling layer, and two fully connected layers (128-dimensional for feature representation, followed by 1-dimensional for sigmoid classification layer). Every convolution layer is followed by Leaky Relu activation.
* Initially batch normalization brought some instability which was improved by group normalization
* We trained our GANS with a batch size of 64, a learning rate of 0.0002, and the Adam optimizer.
* Here to stop training we used spoof data for validation to determine when to stop training or tune hyper – parameters

**2.2.Fingerprint Spoof Buster using Minutiae Extraction Centered Patches**

Sometimes spoofing add noise and absence of points like friction ridges, bifurcations , islands etc. In this approach they utilize this observation to train a 2 class CNN using a local patches around extracted minutiae.

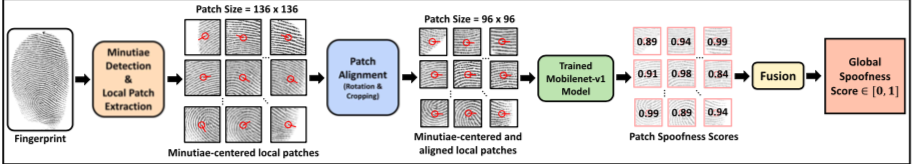
This approach is more robust to novel fabrications materials than earlier approaches that utilize the whole image or randomly selected patches.

In this approach utilizing the local patches of size 96x96, the drawback of downsizing whole fingerprint images to train the CNN is addressed.

ii) provides a large amount of data on average of 48 patches per fingerprint.

iii)learns textural features from patches robust to differentiate between spoof and live fingerprints.

iv)provides a graphical fine grained representation of fingerprint images capable of localizing partial spoof fingerprint output of CNN spoof score.

****

The proposed approach is able to achieve a significant reduction in the error rates for intra-sensor (63%), cross-material (43%), cross-sensor (4%) as well as cross-dataset scenarios (29%) compared to state-of- the-art on public domain LivDet datasets.

**2.3 Comparison between two Approaches:**

Previous works[3] has also experimented to use the deeper state of architecture of DCGAN for discriminator such as MobileNets but it was found that it did not converge for the generator.

But in the DCGAN approach there just using the whole image of live fingerprint datasets while in the other approach they are extracting patches minutiae based from the fingerprint and then giving them spoof using CNN

**3.Implementation Details:**

**Dataset :**  We used dataset from Sokoto Coventry Fingerprint Dataset (SOCOFing), a biometric fingerprint database is made of up 6000 fingerprint images from 600 African subjects, have attributes like gender, hand, finger and have altered images for 3 different levels such as obliterations, z-cut, central rotations. Used it for training and validation.

For testing we used LIVDET dataset 2011 , 2013 ,2015 (Clarkson University- University of Cagliari, Joint Multi-modal Biometric Dataset)

MNIST dataset was also used for digit generation using simple GAN model.

**LIBRARIES USED:**

Keras is used for implementing the one class classification dcgan spoof detection and minutiae based extraction. Pytorch has been used for synthesizing fake images in GAN experimented with MNIST data.

**Data Analysis Strategies** In SOCOFing dataset they have altered fingerprint images with a strange toolbox over 500dbi resolution and settings easy, medium, hard giving total images of 55734 altereds images of size 1x96x103.

Then minutiae extraction algorithms are used to extract patches

**4. EXPERIMENTAL RESULTS AND INFERENCE**

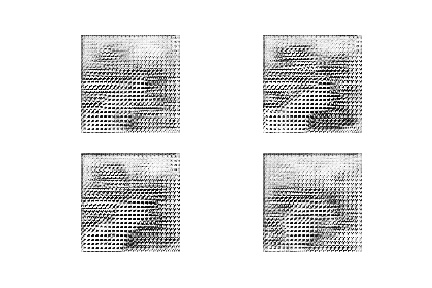
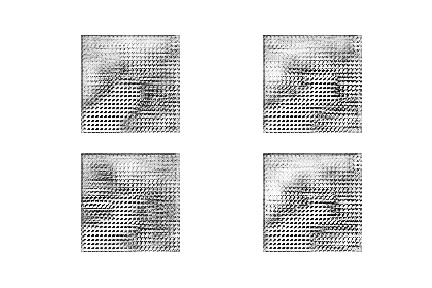
After implementing one class classifier over the dataset mentioned in section 7. we got the following results:

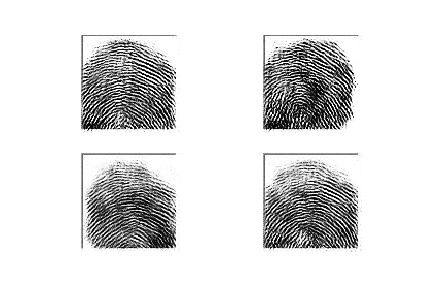
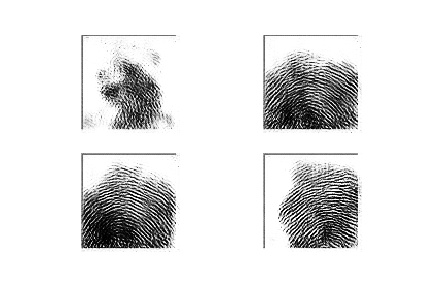
The sigmoid output of the discriminator gave the spoof score for the input image and hence over the complete testing dataset the spoof score were measured and the average was taken. Gans work well for materials which are anomalous such as playdoh and gold fingers.

This approach had an average of true detection rate of at least 10% as compared to more for all 12 spoof materials as compared to any other CNN model. **Training accuracy was 98.3% and validation accuracy was 96%. And precision was 51.2% as compared to the previous work where it has been 49% only.**

|  |  |  |
| --- | --- | --- |
| Training Set | Socofing Dataset was used with 4800 real fingerprint images | 98.3% Accuracy |
| Validation Set | Socofing Dataset 1200 real fingerprints and 600 spoof fingerprints used | 96% Accuracy |
| Testing Set | Livdet 2015 , a dataset of size 1000 GreenBit images including real fingerprint and spoof material like Gelatin. , Ecoflex , Latex | True Detection Rate : 51.3% and Fake Detection Rate : 19% |

**Generated Images output :**





.Hence images showing starting from noise to the final output of fingerprint from image 1 to 4 respectively.

**5.Conclusion and Future Work:**

We have improved the generalization problem for spoof detection system though one class classifier using DCGANs which requires large dataset but eliminates the poor generalization to unknown spoof materials

The proposed spoof detection system still leaves room for improvement on transparent spoof materials.

Indeed, transparent spoofs were also reported as the most challenging materials due to the fact that much of the live finger color transmits through the clear spoof materials

GANs struggle to distinguish clear spoofs like ecoflex from live fingers, since much of the live finger can be seen from behind the spoof.

**6.REFERENCES:**

***1.UNSUPERVISED REPRESENTATION LEARNING WITH DEEP CONVOLUTIONAL GENERATIVE ADVERSARIAL NETWORKS Alec Radford & Luke Metz indico Research Boston, MA {alec,luke}@indico.io Soumith Chintala Facebook AI Research New York, NY*** [***soumith@fb.com***](mailto:soumith@fb.com)

***2.Fingerprint Spoof Buster: Use of Minutiae-Centered Patches , Tarang Chugh , Student Member, IEEE, Kai Cao, and Anil K. Jain, Life Fellow, IEEE***

***3.Generalizing Fingerprint Spoof Detector: Learning a One-Class Classifier Joshua J. Engelsma and Anil K. Jain Michigan State University  
East Lansing, Michigan, USA***

***4.Sokoto Coventry Fingerprint Dataset Yahaya Isah Shehu1✉, Ariel Ruiz-Garcia1✉, Vasile Palade1 and Anne James2 1 Coventry University, Faculty of Engineering, Environment and Computing. Priory Street, CV1 5FB, Coventry, UK 2 Nottingham Trent University, Faculty of Science and Technology, Clifton Campus, NG11 8NS, Nottingham, UK shehuy2,ariel.ruiz-garcia,vasile.palade@coventry.ac.uk,*** [***anne.james@ntu.ac.uk***](mailto:anne.james@ntu.ac.uk)

5.<https://github.com/jacobgil/keras-dcgan>