MSDSM Final Year Project Presentation

Presentation Attack Detection in Biometric Security Using Deep Learning Techniques - A Comparative Analysis

Dev Nandan Sarkar

MSDSM Batch 2

Roll no 2204107017

19 June 2024

Agenda

- A quick overview of the problem
- Previous works on the problem
- Current work by presenter
- Observations and conclusion

What is FRS?

- Fingerprint Recognition System [3]

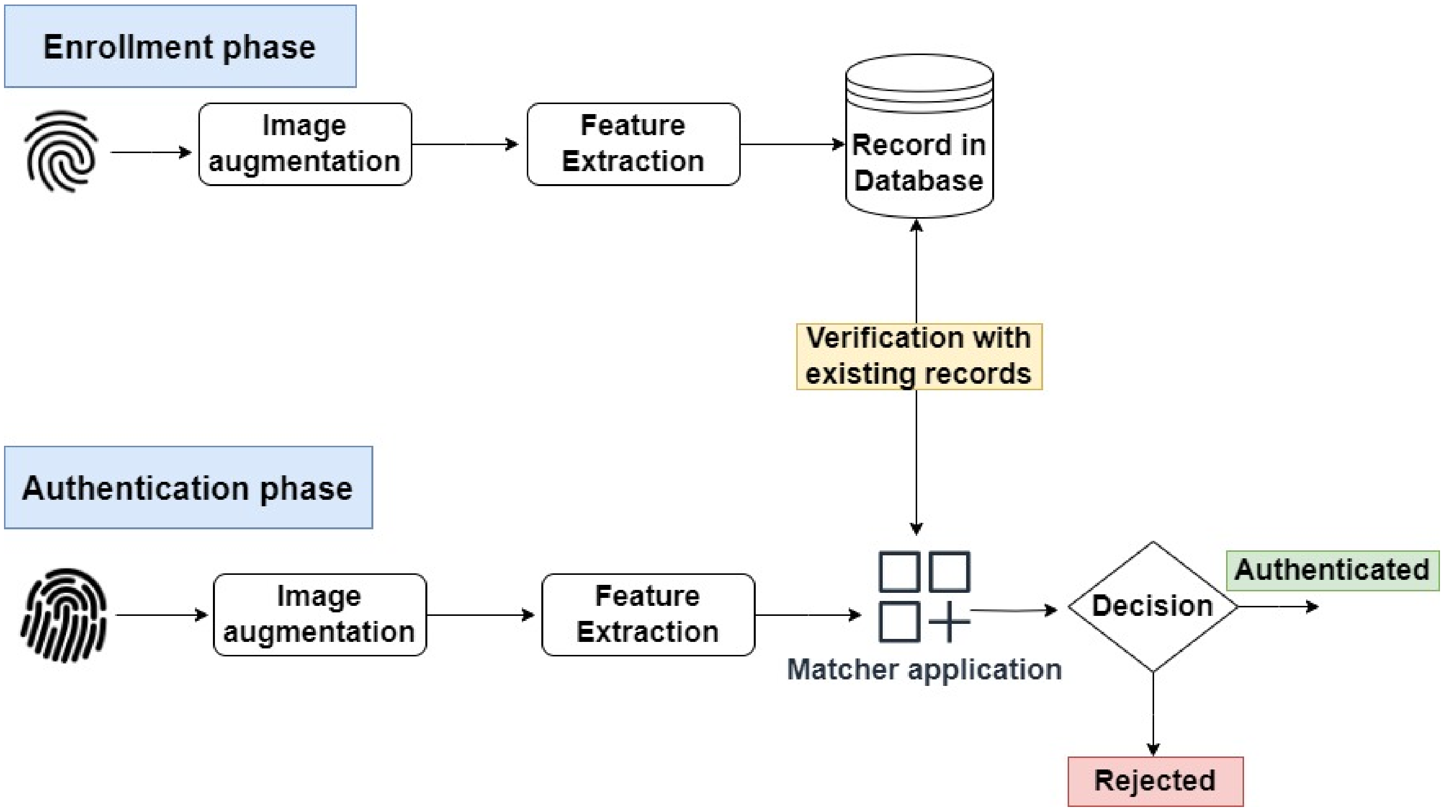

Figure 1

What are PA and FPAD?

- Presentation Attack (PA) – methods to deceive the FRS
- Fingerprint Presentation Attack Detection (FPAD) – methods to detect the deception

What are fake fingerprints?

- Fake finger prints can be made from various materials like Ecoflex, Wood Glue, Play-doh, Gelatin etc using direct or latent fingerprint impressions of subjects.

Real Fakes

Ecoflex Gelatin Latex Wood glue

Figure 2 : Real and fake fingerprint samples

Related Works

- Adversarial Representation Learning Coupled with Style Transfer for Cross-Sensor Generalization [4]

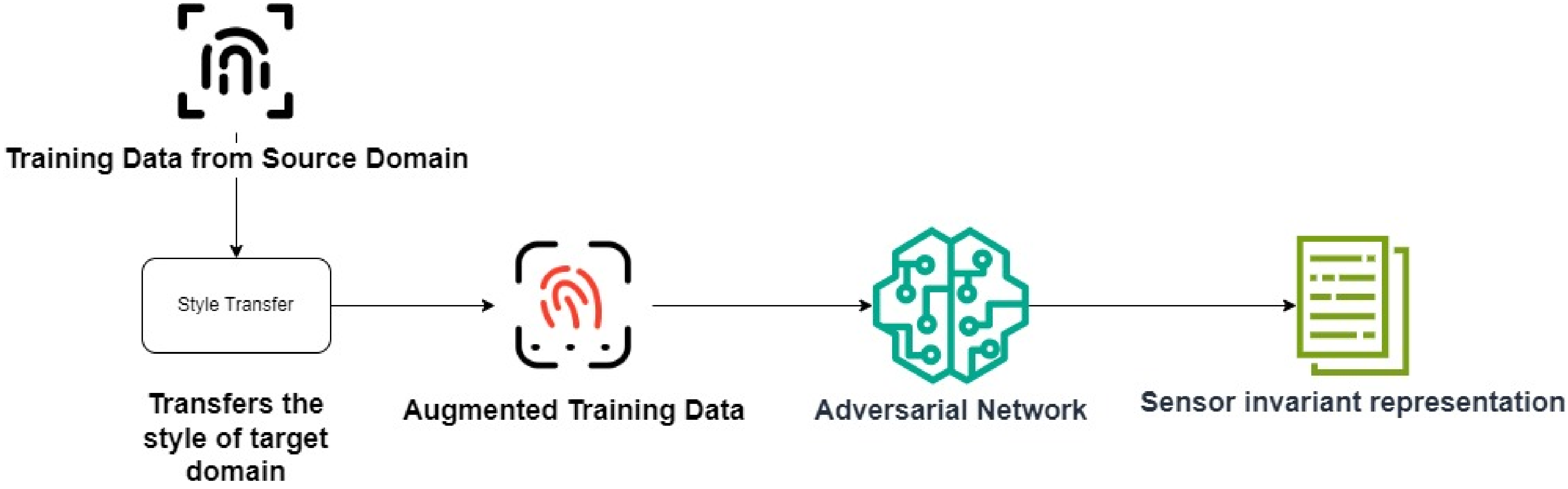

Figure 3 : Flow diagram for this approach

Related Works

- Convolution Auto-encoders on Short Wave Infrared (SWIR) Images of Fingerprints [5]

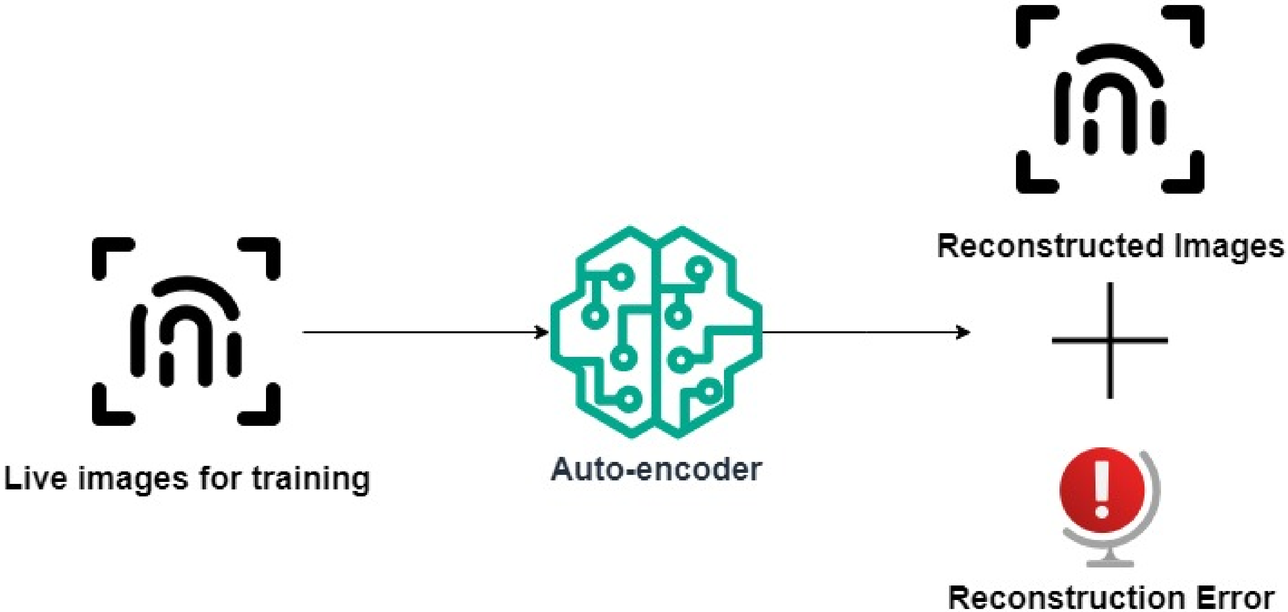

Figure 4 : Flow diagram for this approach

Related Works

- Feature Denoising through Suppression of Noise Channels [6]

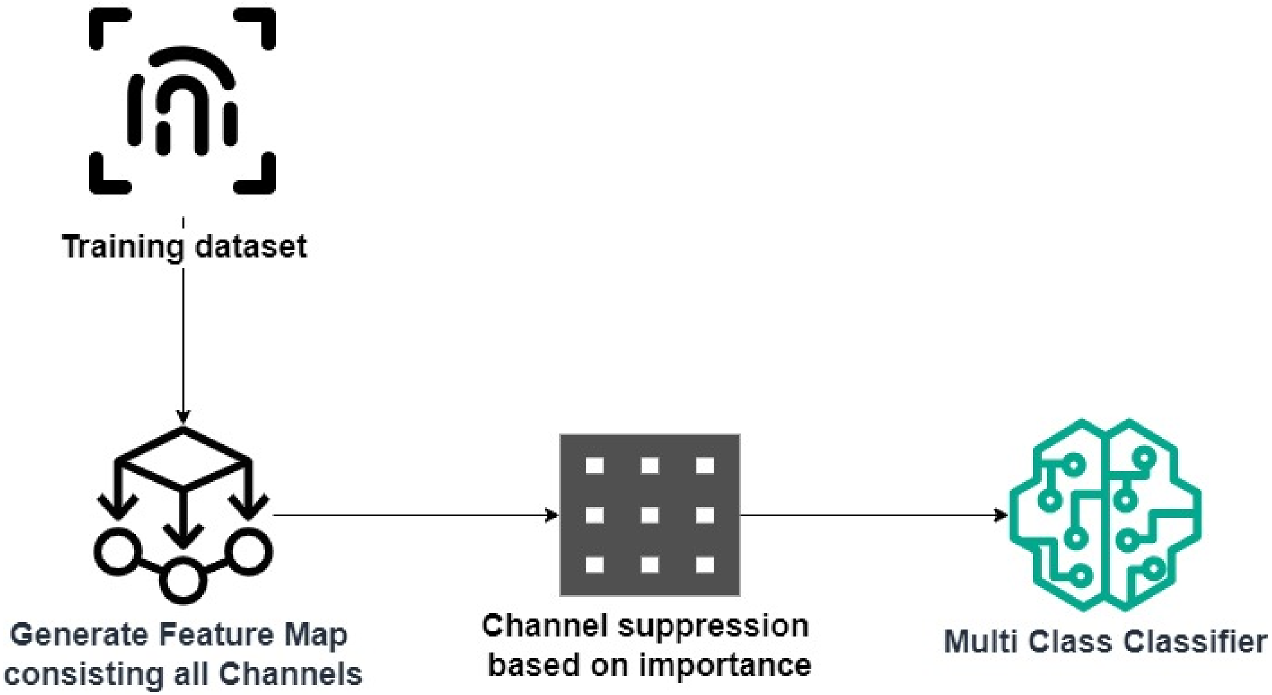

Figure 5 : Flow diagram for this approach

Objectives

- Study the performance a state-of-the-art CNN model, namely VGG16 [2], on LivDet-2011 [1] dataset

- Compare the performance of 2 shallow CNN models with that of the VGG16 [2] model on the same dataset

Dataset used

- LivDet-2011 Dataset [1] has been used to train the models
- Contains roughly 16000 fingerprint images from 4 sensors – Biometrika, Italdata, Digper and Sagem
- 4000 from each sensor, equally divided into training and testing

Exploring VGG16 Model

- Training a pre-trained VGG16 [2] model on LivDet 2011 (Sagem sensor) dataset [1]
- Model accuracy peaks at around 50 epochs of training

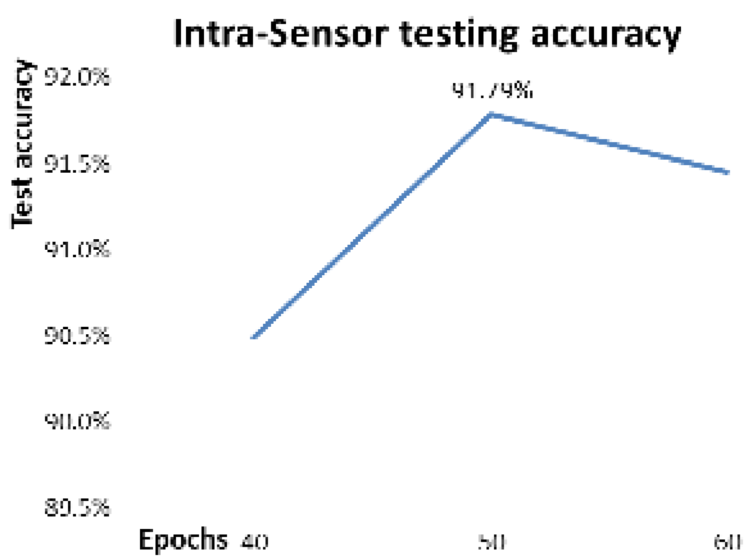

Figure 6

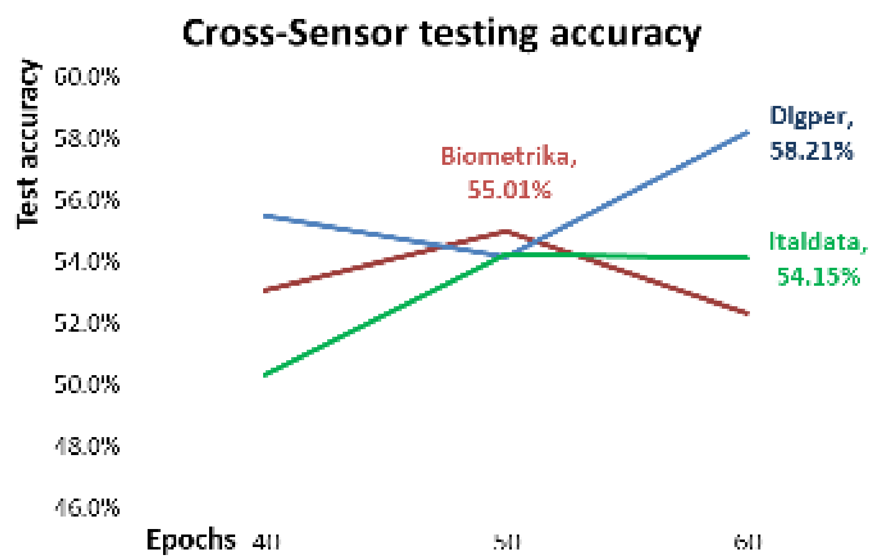

Figure 7

Exploring shallow CNN architectures

Shallow CNN on LivDet-2011 Dataset (Sagem Sensor) [1]

- 8 layers
- 2 convolution layers, 2 max-pooling layers, 2 dense layers, 1 flatten layer and a final Softmax layer

Shallow CNN on LivDet-2011 Dataset (Digper Sensor) [1]

- 9 layers
- 2 convolution layers, 2 max-pooling layers, 3 dense layers, 1 flatten layer and a last Softmax layer

Shallow CNN (Sagem Sensor)

Table 1: Testing accuracy of this model

Sensor	Testing Accuracy
Sagem	88.95%
Digper	55.29%
Biometrika	50.05%
Italdata	46.42%

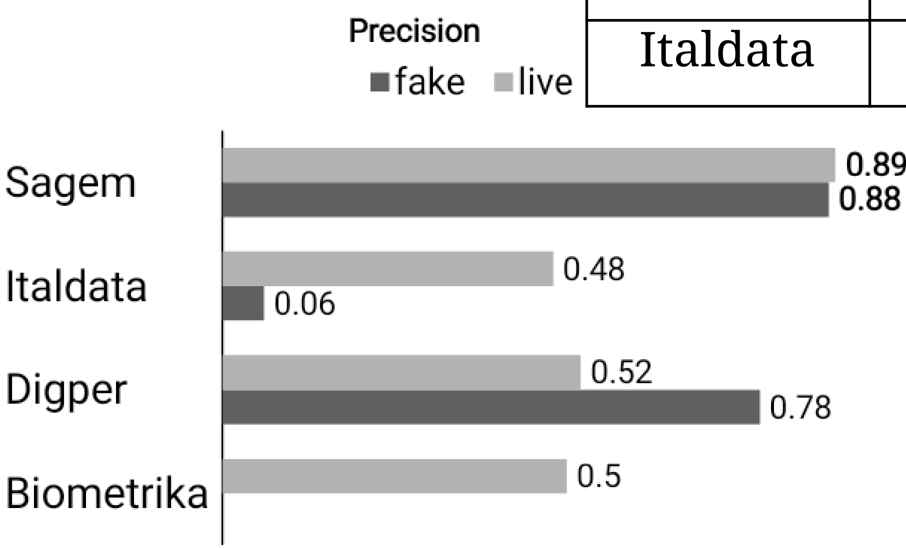

Figure 8

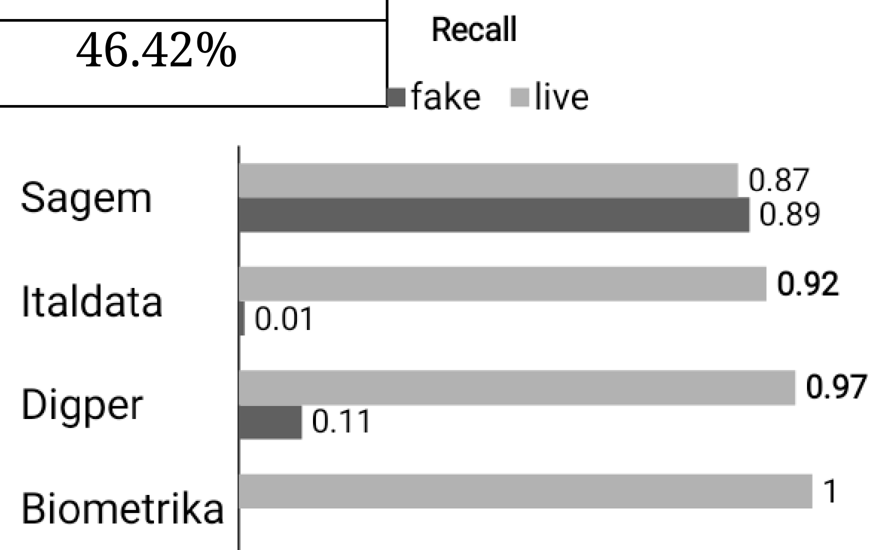

Figure 9

Shallow CNN on LivDet-2011 Dataset (Sagem Sensor) using Adam optimizer

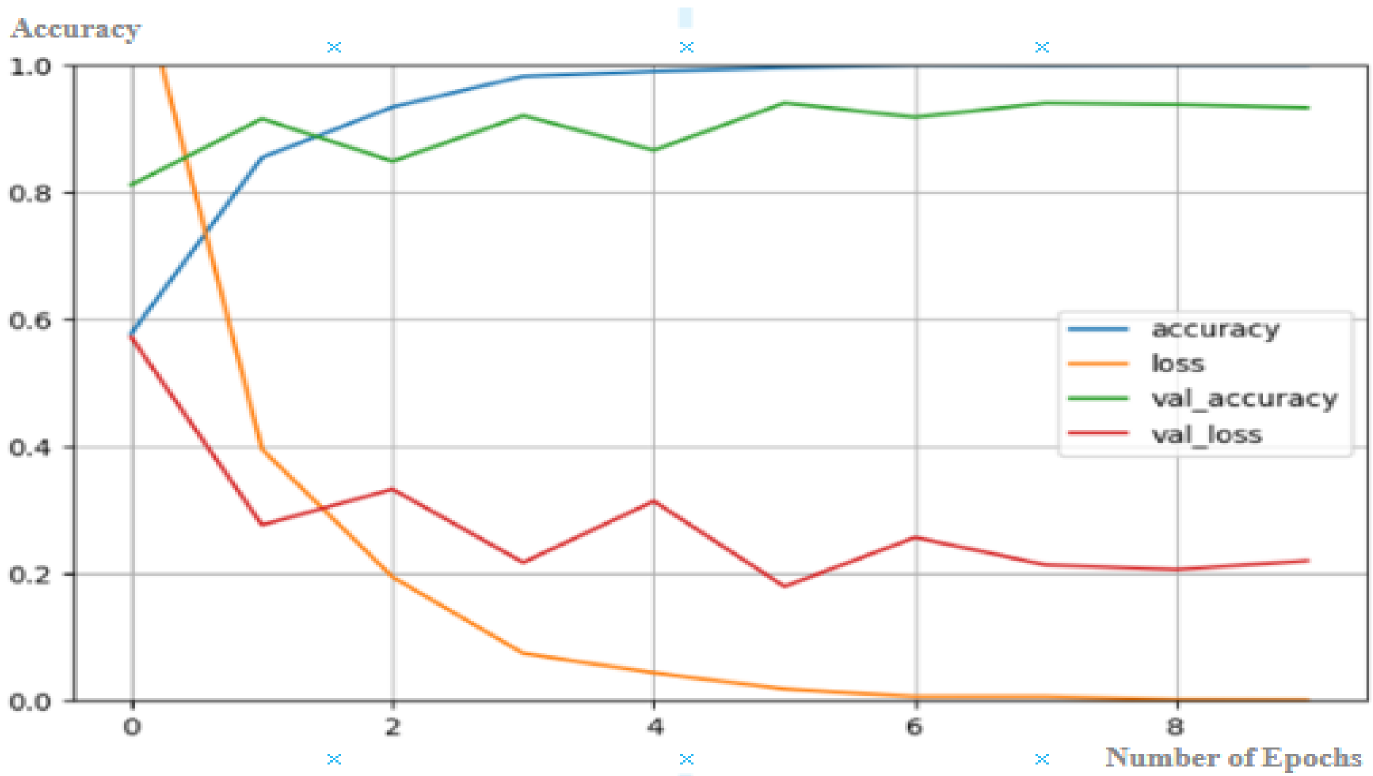

Figure 10 : Accuracy and loss curve using Adam optimizer

Shallow CNN on LivDet-2011 Dataset (Sagem Sensor) using SGD optimizer

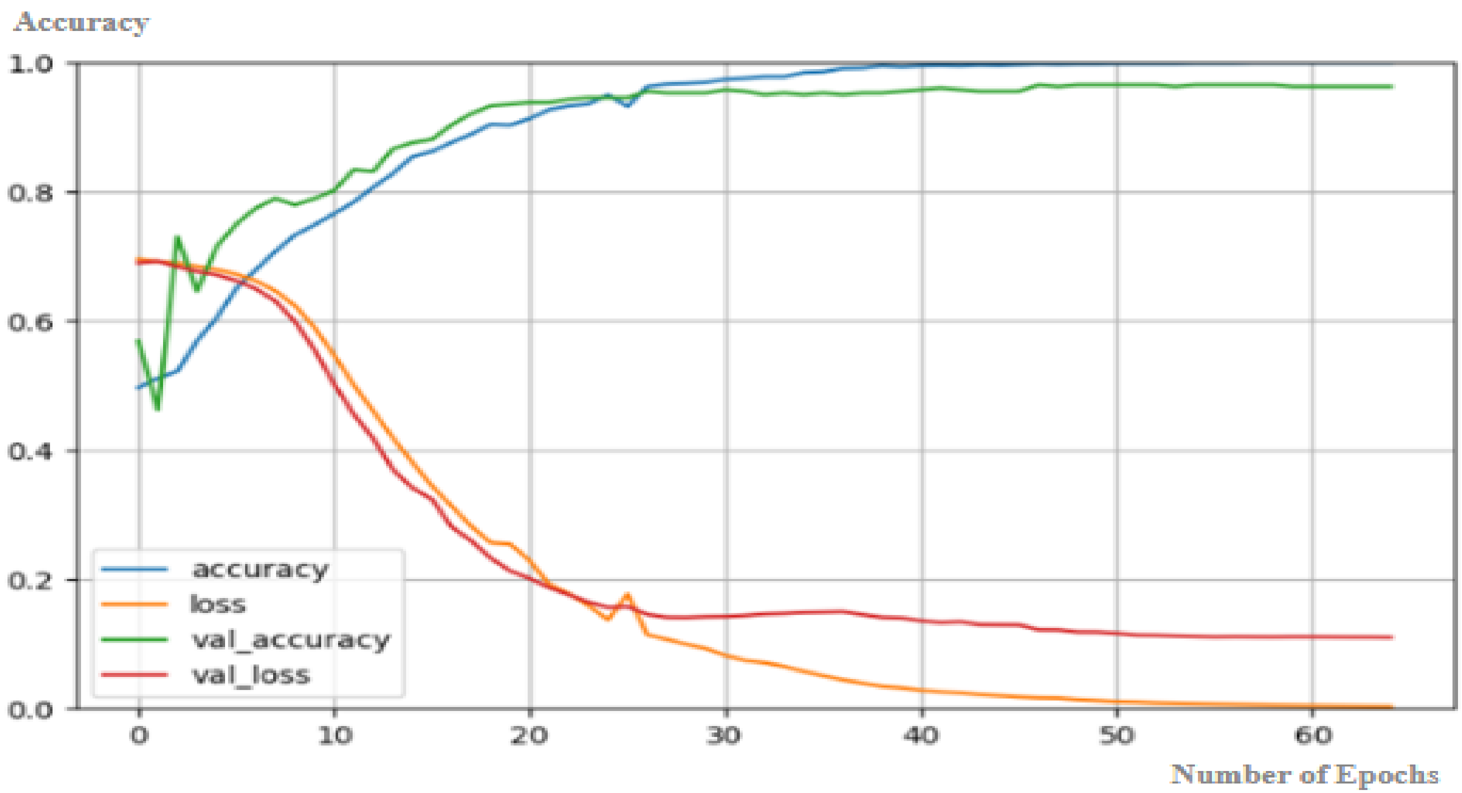

Figure 11 : Accuracy and loss curve using SGD optimizer

Shallow CNN (Digper Sensor)

Table 2: Testing accuracy of this model

Sensor	Testing Accuracy
Sagem	94.72%
Digper	54.01%
Biometrika	51.50%
Italdata	51.90%

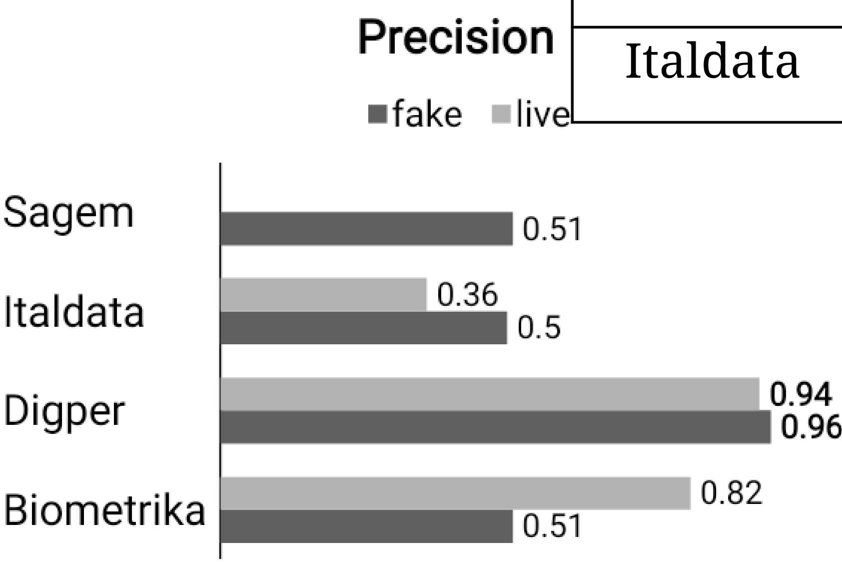

Figure 12

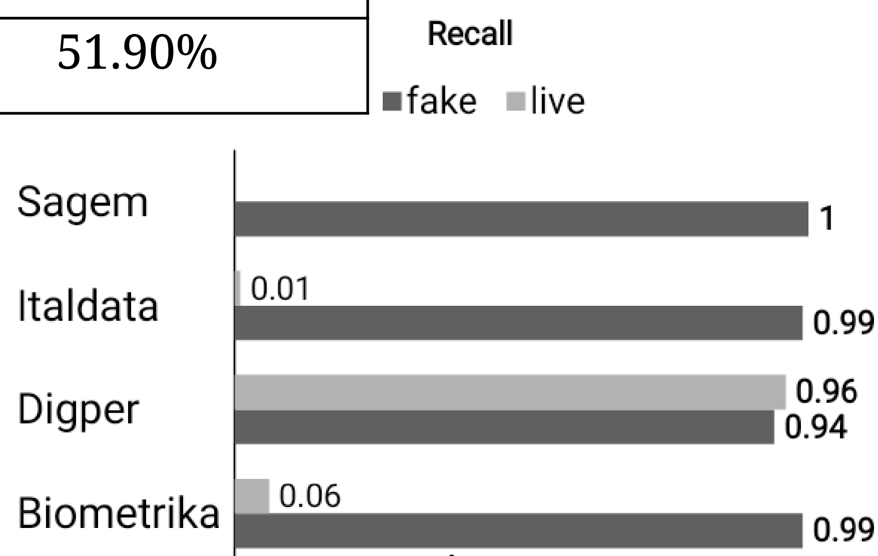

Figure 13

Shallow CNN on LivDet-2011 Dataset (Digper Sensor) using Adam optimizer

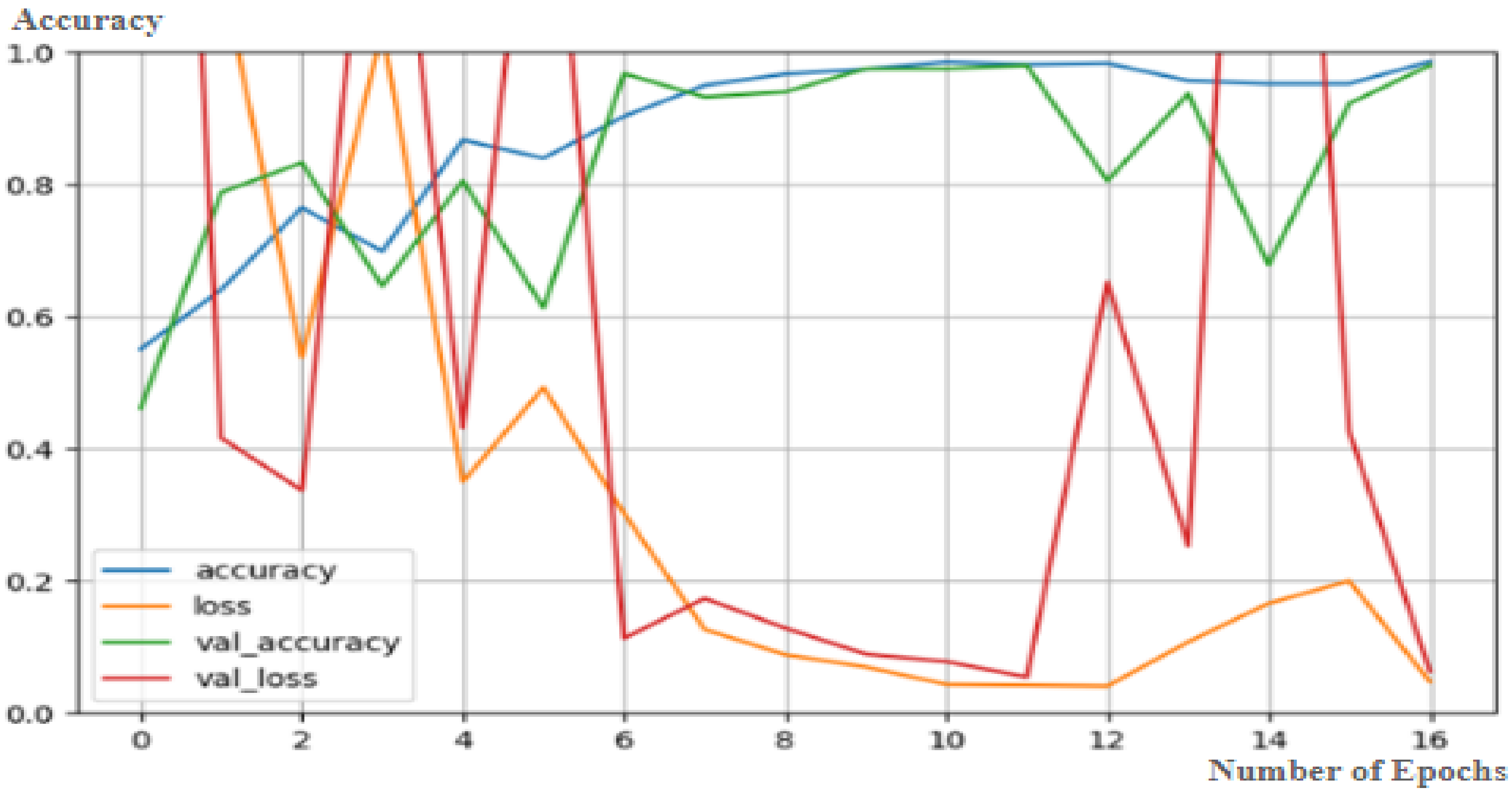

Figure 14 : Accuracy and loss curve using Adam optimizer

Observations

- VGG16 model (Sagem sensor) shows intra-sensor testing accuracy of 91.79% , cross sensor testing accuracy of 58%.
- Shallow CNN network (Digper sensor) exceeds this intra-sensor testing accuracy, attaining 94.72%
- Shallow CNN network (Sagem sensor) attains a comparable cross-sensor accuracy 55.29%
- Both shallow networks exhibit high recall values, specially the one trained on Digper sensor data.
- Both shallow networks took up to 70% less time to train

Conclusion

- The observations suggest potential effectiveness of shallow CNN models over deep architecture models
- If used collectively in form of **Ensemble Classifiers** they might prove to be more efficient as well as more practical

Acknowledgements

My sincere gratitude to the following esteemed persons and institutions.

- Dr. Somnath Dey, Project guide
- MSDSM Committee members
- Indian Institute of Technology Indore

Thank You

References

[1] D. Yambay, L. Ghiani, P. Denti, G. Marcialis, F. Roli, S. Schuckers. LivDet 2011 - Fingerprint liveness detection competition 2011. In Proceedings of 5th IAPR International Conference on Biometrics (ICB), 2011, New Delhi (India).

[2] S. Liu and W. Deng. Very deep convolutional neural network based image classification using small training sample size. In Proceedings of the 3rd IAPR Asian Conference on Pattern Recognition (ACPR), pp. 730–734, 2015 Kuala Lumpur, Malaysia.

[3] M. Ali, V. Mahale, P. Yannawar, A. Gaikwad. Overview of fingerprint recognition system. In the Proceedings of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, Chennai, India.

References

[4] S. A. Grosz, T. Chugh and A. K. Jain. Fingerprint Presentation Attack Detection: A Sensor and Material Agnostic Approach. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), 2020, Houston, Texas, USA.

[5] J. Kolberg, M. Grimmer, M. Gomez-Barrero and C. Busch. Anomaly detection with convolutional autoencoders for Fingerprint Presentation Attack Detection. In IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021.

[6] F. Liu, Z. Kong, H. Liu, W. Zhang and L. Shen. Fingerprint Presentation Attack Detection by Channel-wise Feature Denoising. IEEE Transactions on Information Forensics and Security, Volume: 17, pp. 2963 – 2976, 2022.

Appendix

Plagiarism report