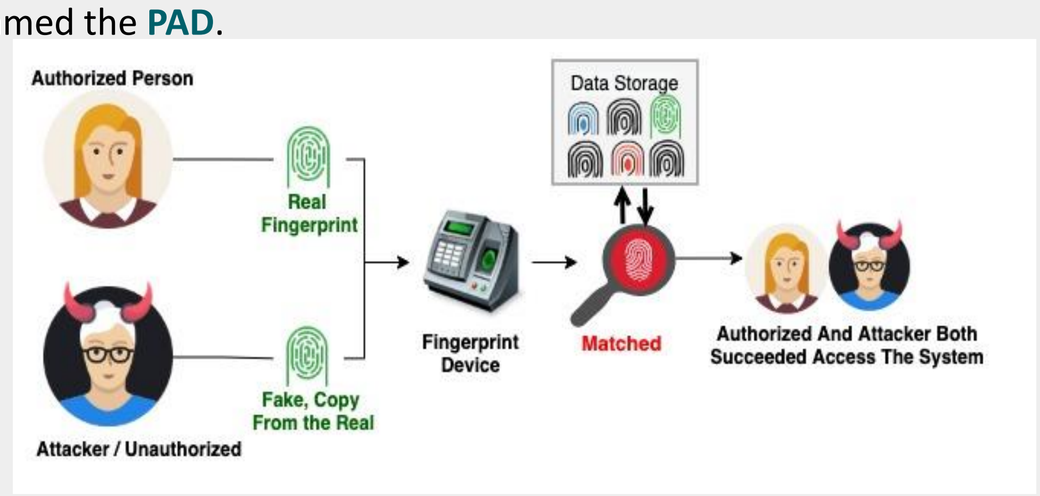
المؤتمر الوطني الخامس لكليات الحاسب الآلي بالجامعات السعودية
The Fifth National Conference of Saudi Computers Colleges 2022
21-22 December 2022

Fingerprint Presentation Attack Detection Algorithm

Alaa Alsubhi and Dr. Nawal Alsufyani
cyber security, computers and information technology, Taif University

Introduction

Unfortunately, as with any authentication technology, biometric systems have been exposed to external attacks. An attacker does not need to learn about the system to defraud it; rather, they can use a **presentation attack (PA)** by merely proffering to the biometric capture tool a presentation attack instrument (PAI), which is something like a synthetic finger [1]. The "*ISO/IEC 30107-1:2016 Information technology* — Biometric presentation attack detection" guide mentions the PA attack, indicating that it is a serious problem because it violates integrity and authentication [2]. We can detect the presentation of a biometric spoof to the sensor by a general method named the **PAD**.



Objective

- Apply an algorithm that will successfully work against PA attacks.
- Offer a good solution for PAD by implementing a DL algorithm, especially the CNN model.

To achieve these objectives, the following steps were taken:

- Small and publicly available ATVS-FFp DB datasets were used.
- The dataset images are split between training, validation, and test sets.
- The algorithm was programmed with Python, Anaconda, TensorFlow, and Keras.

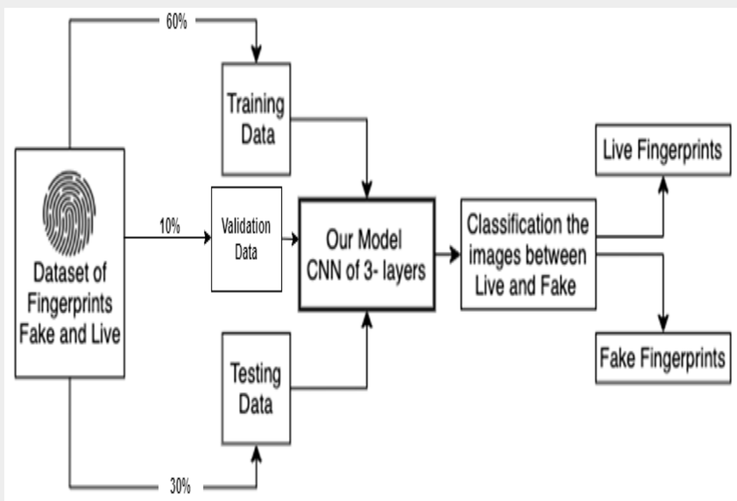
Dataset

In this project, we work on the ATVS-FFp DB dataset, which includes two types of datasets, real and fake fingerprint images, in Bitmap Image File (.bmp) format [3].

ATVS-FFp DB	1- DS_WithCooperation	17 users (index and middle fingers)	68 Fingers	68 fingers × 4 patterns x 3 different sensors	816 images
	2- DS_WithoutCooperation	17 users (index and middle fingers)	64 Fingers	64 fingers × 4 patterns x 3 different sensors	768 images

Methodology

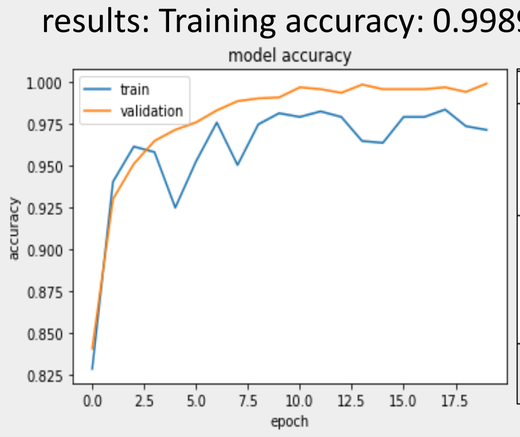
- The proposed model is a binary classification system that distinguishes between live and fake fingerprint images.
- The images were divided into two classes: fake fingerprints and original fingerprints.
- The algorithm in this work has 3 layers in the CNN model.
- The ATVS-FFp DB dataset was divided into 60% for training, 10% for validation, and 30% for testing the model.




```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 298, 298, 16)      448

 max_pooling2d (MaxPooling2D  (None, 149, 149, 16)     0
 )

 conv2d_1 (Conv2D)           (None, 147, 147, 32)      4640

 max_pooling2d_1 (MaxPooling  (None, 73, 73, 32)       0
 2D)

 conv2d_2 (Conv2D)           (None, 71, 71, 64)        18496

 max_pooling2d_2 (MaxPooling  (None, 35, 35, 64)       0
 2D)

 flatten (Flatten)           (None, 78400)             0

 dense (Dense)               (None, 512)               40141312

 dense_1 (Dense)             (None, 1)                 513

=================================================================
Total params: 40,165,409
Trainable params: 40,165,409
Non-trainable params: 0
_________________________________________________________________
```

Result

- We tried two different splits of the data. The first time, the proportions were training = 60%, valid = 20%, and testing= 20%. The results: training accuracy 0.9983% and test accuracy 0.9621%
- In the second division, we reduced the images for validation, increased them in the test, training = 60%, valid = 10%, and testing = 30% . We succeeded in raising the accuracy rate, as we obtained the following results: Training accuracy: 0.9989% and test accuracy: 0.9704%.



Ref.	Dataset	Algorithm	Results
[4]	ATVS-FFp	Distinguish real biometric data from data as used in presentation / sensor spoofing attacks.	Accuracy = 90%.
[5]	ATVS-FFp	Convolutional Neural Networks and Long Short Term Memory networks.	Accuracy = 97%
	ATVS-FFp	Our CNN-3 layers model.	Accuracy =97.1%

Conclusion

There is a need to protect the safety and security of authentication systems against PA through automatic presentation attack detection (PAD). The current researchs showed promising results after the application of PAD to deep learning (DL) algorithms. The proposed model is a software-based approach, namely a binary classification system to distinguish between live and fake fingerprint images as these were the most appropriate in terms of cost. In order to achieve the goal of this research, we applied a three-layer convolutional neural network (CNN) using the ATVS-FFp DB dataset for training and testing. The model showed that it is affected by the number of images in the test and shows higher results the more the test phase is given. The trained model achieved 99% training accuracy and 97% testing accuracy.

Future work

- we will apply the same algorithm to another dataset.
- we will also apply another algorithm (like VGG16) to the ATVS-FFp DB dataset.
- we will also improve the algorithm so that we can suggest it to some parties to apply it to their systems in order to increase their protection and security.

References

[1] Keilbach, P., Kolberg, J., Gomez-Barrero, M., Busch, C., & Langweg, H. (2018, September). Fingerprint presentation attack detection using laser speckle contrast imaging. In 2018 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-6). IEEE.
[2] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-1. Information Tech-nology - Biometric presentation attack detection - Part 1: Framework, International Organization for Standardization, 2016.
[3] ATVS - Biometric Recognition Group » Databases » ATVS-FFp. (n.d.). BiDA Lab. Retrieved December 2, 2021, from http://atvs.ii.uam.es/atvs/ffp_db.html
[4] A. P. S. Bhogal, D. Söllinger, P. Trung and A. Uhl, "Non-reference image quality assessment for biometric presentation attack detection," 2017 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1-6, doi: 10.1109/IWBF.2017.7935080.
[5] Nunez, J. C., Cabido, R., Pantrigo, J. J., Montemayor, A. S., & Velez, J. F. (2018). Convolutional neural networks and long short-term memory for skeleton-based human activity and hand gesture recognition. *Pattern Recognition*, *76*, 80-94.