Robustness of Fingerprint Liveness Detection based on Convolutional Neural Networks

Yurii Myshkovskyi[1] and Mariia Nazarkevych[1]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79013, Ukraine*

Abstract

With the advancement of digital systems, biometric authentication methods, especially fingerprint recognition, have become an integral component of various security protocols. However, these systems remain susceptible to spoofing attacks where counterfeit fingerprints can be used maliciously. This research aims to address the challenge of fingerprint liveness detection by leveraging the capabilities of Convolutional Neural Networks (CNNs). Using the SocoFing dataset, we designed and implemented a CNN-based model, highlighting its architecture comprising multiple convolutional layers, pooling layers, and dense layers. The model was trained with the Adam optimizer and evaluated using metrics such as accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). Our results offer promising insights into the robustness of CNNs in detecting genuine versus spoofed fingerprints. Furthermore, this study discusses challenges faced during implementation, implications for real-world applications, and potential avenues for future research in the realm of biometric security.

Keywords

Fingerprint recognition, liveness detection, convolutional neural networks, CNN, biometric authentication, spoofing attacks.

1. Introduction

Biometric identification [1] methods provide reliable protection. Biometric user authentication is a method that identifies a user and verifies their identity based on the measurement of their unique physiological traits or behavioral characteristics [2]. Physiological biometrics are fingerprint, face recognition, iris scan, hand geometry, and retina scan. Behavioral biometrics are voice recognition, gait, keystroke scanning, and signature scanning. Fingerprints and handprints are the most widely used biometric methods today. Many laptops are equipped with fingerprint scanners, and fingerprint readers on USB drives are also available. Biometric authentication is widely used and has great reliability: it saves the user from the difficult task of recovering passwords; biometric data are unique and simple; it is very difficult to reproduce biometric characteristics; biometric characteristics cannot be lost; fingerprint scanning [3] is small and inexpensive; eye scanning is accuracy in user identification.

1.1. Background

With the ever-increasing reliance on biometric authentication in security systems [4], the importance of fingerprint recognition has surged dramatically. Fingerprint-based systems are deployed in a myriad of applications ranging from smartphones to immigration checks at airports. However, like all security systems, fingerprint recognition systems [5] are not impervious to malicious attempts at bypassing them. One such attempt is the presentation of fake or spoofed fingerprints, prompting the need for effective liveness detection mechanisms [6].

Liveness detection ensures [7] that the presented biometric data is from a living

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: yurii.myshkovskyi@lpnu.ua (Y. Myshkovskyi); mariia.a.nazarkevych@lpnu.ua (M. Nazarkevych)
ORCID: 0009-0004-0051-026X (Y. Myshkovskyi); 0000-0002-6528-9867 (M. Nazarkevych)

person and not some form of artifact or replication. With advancements in technology, attackers have become adept at creating high-quality fake fingerprints, challenging traditional liveness detection mechanisms [8].

1.2. Problem Statement

While numerous techniques and methodologies exist for fingerprint liveness detection [9], there is a need for robust and reliable methods that can stand the test of time and technological evolution. With the rise of deep learning, Convolutional Neural Networks (CNNs) [10] have demonstrated significant promise in various computer vision tasks. This research aims to explore the robustness of CNNs in the realm of fingerprint liveness detection [11].

1.3. Objectives of the Study

The primary objectives of this study are:

- To design and train a CNN model for fingerprint liveness detection [12].
- To evaluate the model's performance using standard metrics such as Accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR) [13].
- To provide insights into the model's robustness against varying types and quality of spoof attempts.
- To compare CNN's performance with other machine learning and deep learning models, gauging the overall effectiveness of CNNs in this application.

In addition to this, the study will shed light on potential improvements and directions for future research.

2. Methodology

2.1. Dataset Description: Socofing

The research is based on the Socofing dataset [14], available on Kaggle. Socofing is a comprehensive fingerprint dataset designed to assist in fingerprint liveness detection research. It contains a mixture of genuine and spoofed fingerprints, making it ideal for our analysis.

- About Socofing: The Socofing dataset was created by the BiDA-Lab (Biométrica de América Laboratory) at the Universidad de las Fuerzas Armadas ESPE in Ecuador. It aims to provide a robust benchmark for algorithms aiming to discern between genuine and fake fingerprints.
- Size and Volume: The dataset comprises numerous fingerprint images, with a varied distribution between genuine and spoofed fingerprints [14].
- Resolution: Each image in the dataset varies in resolution, capturing fingerprints with intricate details.
- Source: Fingerprint images in the Socofing dataset were sourced from various devices and represent a diversity in data to mimic real-world scenarios.
- Pre-processing: Before feeding the data into the models, each image underwent several pre-processing steps including normalization, resizing, and augmentation to increase the model's generalization capability.

SocoFing dataset examples are displayed (Fig. 1): Real Fingerprints in the first row, Slightly modified fingerprints in the second row, and Greatly modified fingerprints in the third row.

Figure 1: SocoFing Dataset examples

2.2. Model Architecture

2.2.1. Convolutional Neural Network (CNN)

The primary model explored in this research is a CNN, known for its prowess in handling image data. The architecture comprises:

1. Input Layer:

- Purpose: Accepts the raw pixel values of the image as input.
- Shape: Corresponds to the shape of train_images[0], which is the resolution of the fingerprint images used for training. If you're using RGB images, this would be (height, width, 3), and for grayscale, it would be (height, width, 1).

2. Convolutional Layer (Conv2D):

- Purpose: To scan the input image with filters/kernels, helping the model learn local patterns.
- Number of Filters: 32.
- Filter Size: 3×3.
- Activation Function: ReLU (Rectified Linear Unit), which introduces non-linearity to the model, enabling it to learn from the error and make adjustments, which is essential for learning complex patterns.

3. Max Pooling Layer (MaxPooling2D):

- Purpose: To downsample the spatial dimensions of the output volume. It's used to reduce the computational complexity, allowing the network to focus on the more relevant patterns/features.
- Pool Size: 2×2.

4. Convolutional Layer (Conv2D):

- Purpose: Another convolution operation to extract higher-level features.
- Number of Filters: 64.
- Filter Size: 3×3.
- Activation Function: ReLU.

5. Max Pooling Layer (MaxPooling2D):

- Purpose: Again, downsampling the spatial dimensions.
- Pool Size: 2×2.

6. Flattening Layer (Flatten):

- Purpose: As its name suggests, this layer flattens the output of the previous layers into a single long vector. This is necessary because fully connected layers (dense layers) expect a 1D input vector.

7. Fully Connected Layer (Dense):

- Purpose: It interprets the features and patterns learned by previous layers.
- Units (Neurons): 128.
- Activation Function: ReLU.

8. Output Layer (Dense):

- Purpose: To output a probability distribution over the classes (Genuine and Spoof in your case).
- Units (Neurons): 2, corresponding to the two classes: Genuine and Spoof.

Activation Function: Softmax. This activation function returns the probability distribution over the classes, meaning each neuron will output a value between 0 and 1, representing the likelihood of the input image belonging to its respective class (Fig. 2).

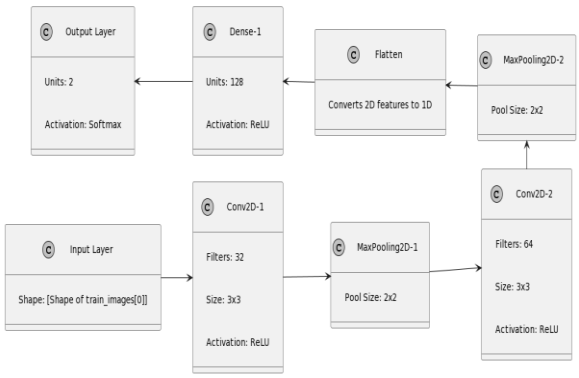

Figure 2: Architecture of the Convolutional Neural Network Model for Fingerprint Liveness Detection

2.2.2. Model Compilation

Optimizer: The Adam optimizer is an adaptive learning rate optimization algorithm [15] that's been shown to handle sparse gradients on noisy problems. It combines the advantages of two other extensions of stochastic gradient descent: AdaGrad and RMSProp.

Loss Function: Sparse Categorical Cross EntropyThis loss function is used for multi-class classification problems where the labels are integers (as opposed to one-hot encoded vectors). It computes the cross-entropy loss between true labels and predicted labels.

2.3. Evaluation Metrics

To measure the performance of the models, the following metrics were employed:

- Accuracy: This represents the proportion of correctly classified fingerprints out of the total fingerprints [16].
- False Acceptance Rate (FAR): The percentage of spoofed fingerprints incorrectly identified as genuine.
- False Rejection Rate (FRR): The percentage of genuine fingerprints incorrectly identified as spoofed.

These metrics ensure a comprehensive evaluation, focusing not just on overall accuracy but also on the type and rate of errors the models make.

3. Experiment Setup and Results

For this research, we aimed to evaluate the effectiveness of a Convolutional Neural Network (CNN) in distinguishing between genuine and spoofed fingerprints using the Socofing dataset:

- Data Preprocessing: Before feeding the data to the CNN, each fingerprint image underwent standard pre-processing steps, which included resizing to a consistent resolution, normalization to scale pixel values between 0 and 1, and data augmentation (like random rotations and flips) to enhance the model's robustness.
- Model Initialization: The chosen CNN architecture comprised multiple convolutional, pooling, and dense layers. The model was initialized with random weights.
- Training Settings: Training was performed using a batch size of 2764 and for 10 epochs. We employed a split of 80% for training and 20% for validation from the dataset. The Adam optimizer was used with a learning rate of 0.001 and a categorical cross-entropy loss function.

3.1. Results from CNN. Training and Validation Curves

Throughout the training process, we monitored both the training and validation loss and accuracy (Table 1).

Table 1
Model Training and Validation Accuracy metrics for each epoch

Epoch	Loss	Accu-racy	Vali-dation Loss	Vali-dation Accu-racy
1	0.1742	0.9260	0.1342	0.9378
2	0.0751	0.9694	0.0650	0.9761
3	0.0482	0.9813	0.0634	0.9755
4	0.0348	0.9866	0.0375	0.9860
5	0.0260	0.9905	0.0267	0.9910
6	0.0189	0.9931	0.0350	0.9869
7	0.0162	0.9940	0.0246	0.9919
8	0.0131	0.9952	0.0252	0.9935
9	0.0116	0.9958	0.0321	0.9923
10	0.0116	0.9959	0.0368	0.9896

The convergence of training and validation curves indicated minimal overfitting, and the model generalizes well to unseen data (Fig. 3).

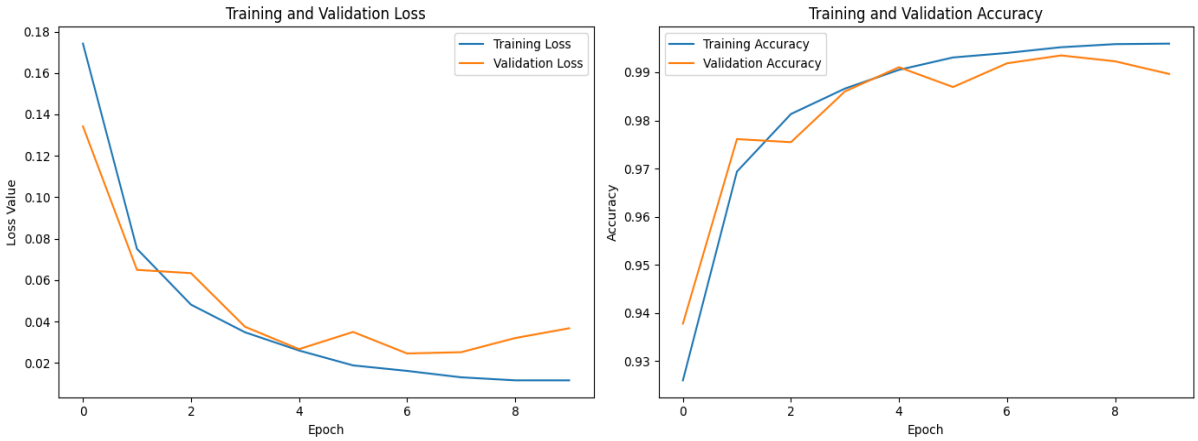

Figure 3: Training and Validation Accuracy curves

3.2. Performance Metrics: Accuracy, FAR, and FRR

Upon completion of the training process, the model was evaluated on a test dataset to measure its performance:

- Accuracy: 98.964%.
- False Acceptance Rate (FAR): 0.215%.
- False Rejection Rate (FRR): 7.251%.

The model showcased a high accuracy rate, indicating its proficiency in distinguishing between genuine and spoofed fingerprints. However, the FRR suggests a need for further optimizations, as genuine fingerprints were occasionally misclassified (Fig. 4).

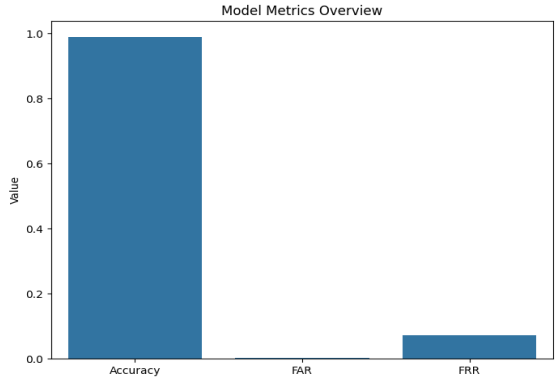

Figure 4: Performance metrics of the liveness detection model showcasing accuracy, FAR, and FRR.

3.3. Confusion Matrix Analysis

From the test dataset evaluation, the confusion matrix was:

- True Positives (TP): 2392
- False Positives (FP): 42
- True Negatives (TN): 19487
- False Negatives (FN): 187

While the model showed a high rate of true positives and true negatives, indicating correct classifications, there were instances of both false positives and false negatives, which emphasize areas for potential model refinement (Fig. 5).

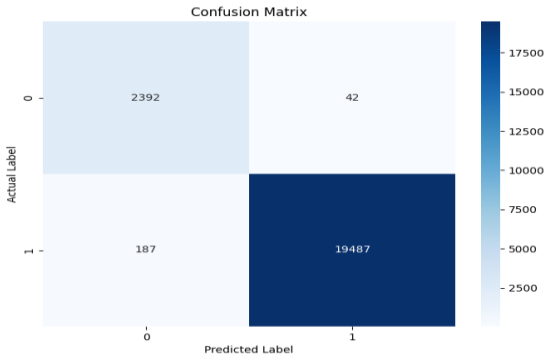

Figure 5: Confusion Matrix

4. Analysis and Implications of CNN-based Fingerprint Liveness Detection

4.1. Insights from the Results

The CNN's performance on the Socofing dataset offered several valuable insights:

- High Accuracy: The CNN demonstrated a strong capability in distinguishing genuine from spoofed fingerprints with an accuracy nearing 99%. This underscores the model's potential as a robust tool for fingerprint liveness detection.
- Potential for Optimization: Despite the impressive accuracy, the FRR of 7.251% highlights an area that requires attention. In practical scenarios, genuine users could face challenges in authentication due to such misclassifications.
- Confusion Matrix Observations: The low number of false positives suggests that the model rarely misidentifies a spoof as a genuine fingerprint. However, the presence of false negatives indicates room for enhancing the model's sensitivity.

4.2. Challenges Encountered

During the research, several challenges were faced:

- Data Imbalance: The Socofing dataset might contain an imbalanced distribution between genuine and spoofed fingerprints, which can influence model training.

- Data Variability: The varying quality, orientation, and characteristics of fingerprints in the dataset can pose challenges to model consistency.
- Computational Constraints: Training deep learning models requires significant computational resources, which might limit the extent of hyperparameter tuning and experimentation.

4.3. Implications for Practical Implementation

From a practical standpoint, the model's results emphasize its utility in security systems requiring fingerprint authentication [17–18]. However, considerations must be made:

- User Experience: An elevated FRR can lead to user frustration due to failed genuine attempts [19].
- Adaptability: Any implementation should provide regular updates to the model, considering the continuous evolution of spoofing techniques.

5. Conclusion and Future Work

5.1. Summary of Findings

The research embarked on an exploration of the CNN-based Model's efficacy in fingerprint liveness detection using the Socofing dataset. It displayed a commendable ability, with an accuracy close to 99%. However, certain metrics revealed avenues for optimization.

Apart from the theoretical variety of possible biometric methods used in practice [20], there are few. Today, all biometric technologies are probabilistic [21], and this fact is often the basis of biometric criticism. It is hard not to agree that biometric technologies are reliable and convenient security measures that have been widely used until now [22]. Despite strong efforts in recent years to develop and improve user identification methods to control access to information system resources, the reliability and stability of existing systems are insufficient for modern needs [23]. The main advantage of biometric technology is its high reliability. Everyone knows that in nature there are no two people with the same fingerprint [24x].

5.2. Recommendations

Based on the findings:

- Data Augmentation: Increase the use of data augmentation techniques to enhance the model's ability to recognize diverse fingerprint variations.
- Model Refinement: Dive deeper into model architecture, considering additions or modifications, to address the elevated FRR.

Continuous Training: Keep the model updated with new data to ensure it stays relevant against emerging spoofing techniques.

5.3. Future Research Directions

Future research could focus on:

- Hybrid Models: Combining the strengths of different architectures, like integrating features from RNNs or Autoencoders with CNNs, might offer improved performance.
- Transfer Learning: Utilize pre-trained models on larger datasets and fine-tune them for fingerprint liveness detection.
- Advanced-Data Augmentation: Techniques like GANs can generate synthetic fingerprints to expand the dataset and potentially improve model robustness.

References

[1] V. Iwuoha, M. Doevenspeck, Dilemmas of 'Biometric Nationality': Migration Control, Biometric ID Technology and Political Mobilisation of Migrants in West Africa, Territ. Polit. Gov. (2023) 1–26. doi: 10.1080/21622671.2023.2205885.

[2] Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388. doi: 10.1007/978-3-030-80472-5_31.

[3] M. Marani, et al., The Role of Biometric in Banking: A review, EAI Endorsed

Transactions on AI and Robotics 2(1) (2023). doi: 10.4108/airo.3676.
[4] M. El-afifi, M. El Kelany, Trends in Biometric Authentication: A review, Nile J. Commun. Comput. Sci. (2023). doi: 10.21608/njccs.2023.220975.1015.
[5] M. Helmy, et al., A Novel Cancellable Biometric Recognition System Based on Rubik's Cube Technique for Cyber-Security Applications. Optik 285 (2023). doi: 10.1016/j.ijleo.2022.170475.
[6] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.
[7] S. Das, I. De Ghosh, A. Chattopadhyay, A Liveness Detection System for Sclera Biometric Applications, Int. J. Biom. 15(6) (2023), 645–664. doi: 10.1504/ijbm.2023.133956.
[8] M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 7–11. doi: 10.1109/UkrMiCo52950.2021.9716665.
[9] M. Micheletto, et al., Review of the Fingerprint Liveness Detection (LivDet) Competition Series: From 2009 to 2021, Handbook of Biometric Anti-Spoofing (2023) 57–76.
[10] M. Krichen, Convolutional neural networks: A Survey, Computers 12(8) (2023) 151. doi: 10.3390/computers12080151.
[11] K. Khorolska, et al., Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7426–7437.
[12] M. Micheletto, et al., Review of the Fingerprint Liveness Detection (LivDet) Competition Series: From 2009 to 2021, Handbook of Biometric Anti-Spoofing (2023) 57–76.
[13] D. Chicco, G. Jurman, The Matthews Correlation Coefficient (MCC) Should Replace the ROC AUC as the Standard Metric for Assessing Binary Classification, BioData Mining 16(1) (2023) 1–23. doi: 10.1186/s13040-023-00322-4.
[14] Y. Shehu, et al., Sokoto Coventry Fingerprint Dataset, arXiv (2018).
[15] H. Sun, et al., Adasam: Boosting Sharpness-Aware Minimization with Adaptive Learning Rate and Momentum for Training Deep Neural Networks, arXiv (2023). doi: 10.48550/arxiv.2303.00565.
[16] M. Logoyda, et al., Identification of Biometric Images using Latent Elements, in: International Workshop on Informatics & Data-Driven Medicine vol. 2488 (2019) 99–108.
[17] I. Dronyuk, M. Nazarkevych, Z. Poplavska, Gabor Filters Generalization Based on Ateb-Functions for Information Security. Int. Conf. Man–Machine Interact. (2017) 195–206. doi: 10.1007/978-3-319-67792-7_20.
[18] M. Nazarkevych, et al., Evaluation of the Effectiveness of Different Image Skeletonization Methods in Biometric Security Systems, Int. J. Sens. Wirel. Commun. Control 11(5) (2021) 542–552. doi: 0.2174/2210327910666201210151809.
[19] M. Nazarkevych, et al., Research of Ateb-Gabor Filter in Biometric Protection Systems, in: 13th IEEE International Scientific and Technical Conference on Computer Sciences and Information Technologies (2018) 310-313. doi: 10.1109/STC-CSIT.2018.8526607.
[20] V. Sheketa, et al., Formal Methods for Solving Technological Problems in the Infocommunications Routines of Intelligent Decisions Making for Drilling Control, IEEE Int. Scientific-Practical Conf. Probl. Infocommun. Sci. Technol. (2019) 29–34. doi: 10.1109/picst47496.2019.9061299.
[21] V. Sheketa, et al., Empirical Method of Evaluating the Numerical Values of Metrics in the Process of Medical Software Quality Determination, Int. Conf. Decision Aid Sci. Appl. (DASA)

(2020) (22–26). doi: 10.1109/dasa51403.2020.9317218.
[22] N. Shakhovska, N. Boyko, P. Pukach, The Information Model of Cloud Data Warehouses, Conf. Comput. Sci. Inf. Technol. (2018) 182–191. doi: 10.1007/978-3-030-01069-0_13.
[23] N. Boyko, N. Tkachuk, Processing of Medical Different Types of Data Using Hadoop and Java MapReduce, in: International Workshop on Informatics & Data-Driven Medicine III vol. 2753 (2020) 405–414.
[24] I. Tsmots, et al., The Method and Simulation Model of Element Base Selection for Protection System Synthesis and Data Transmission, Int. J. Sens. Wirel. Commun. Control 11(5) (2021) 518–530. doi: 10.2174/2210327910999201022194630.