Signature Fraud Detection using combined CNN and SIFT

K Venkata Ramana Devi
Department of Information Technology
Institute of Aeronautical Engineering
Hyderabad, India
k.venkataramanadevi@iare.ac.in

P Hari Bharadwaj
Department of Information Technology
Institute of Aeronautical Engineering
Hyderabad, India
haribharadwaj6@gmail.com

K Aravind
Department of Information Technology
Institute of Aeronautical Engineering
Hyderabad, India
aravind.kammari07@gmail.com

P Pradham Kushal Reddy
Department of Information Technology
Institute of Aeronautical Engineering
Hyderabad, India
pradhamreddy300@gmail.com

Abstract- Ensuring an individual's identification is mostly dependent on secure authentication. Everybody has a distinctive signature that serves as their means of identification in all their business dealings. Traditional signatures are still used in day to day life including government offices, check payments and they still require human verification even though many things have been digitalized. Therefore, forgery detection is important to lowering these kinds of overheads. In addition to being time consuming, manual verification makes it difficult to determine whether two signatures are identical. The pandemic also forced to complete duties online, including digitally posting their own signatures. This makes it much more urgent to put in place a system that can recognize and validate the user's signature. In addition to using techniques like the Convolutional Neural Network (CNN) and Scale Invariant Feature Transform (SIFT) to detect forged signatures and compare the outcomes with different parameters, this research suggests a way to pre- process the signature to make verification easier.

Keywords – Signature Verification, Forgery Detection, Convolutional Neural Network (CNN), Scale Invariant Feature Transform (SIFT), Deep Learning, Feature Fusion, Image Preprocessing.

I. INTRODUCTION

A. Domain Overview

The subject of biometric authentication has been completely transformed by the quick development of computer vision and pattern recognition, which is mostly due to advancements in deep learning. Convolutional neural Networks (CNN), one of these technologies, have shown remarkable efficiency in allowing systems to directly learn complex patterns from picture data. These developments have greatly helped signature verification, a crucial area of biometrics that deals with the difficult issue of recognizing and categorical handwritten signatures as "genuine" or "forged" [7].

Algorithms such as SIFT were created to extract particular geometric or textual qualities from a signature, and automated signature verification has historically mostly depended on handmade feature engineering [12].

By automatically learning feature hierarchies from raw pixels, deep learning and CNNs in particular offered a new paradigm and produced potent writer independent models [3]. However, the fine grained, local keypoints such as stroke crossings, pressure points and endpoints that are essential for identifying complex forgeries can occasionally be missed by a deep learning only technique. Conventional techniques such as SIFT are quite good at capturing these kinds of information [1].

As a result, hybrid models that combine the accurate, local feature extraction of handcrafted techniques with the comprehensive, stylistic feature learning of CNNs have been investigated [10].

B. Motivation

Accurate signature verification is essential for the security of legal and financial operations, but the existing approaches have serious drawbacks. Fine grained local characteristics are captured by conventional algorithms such as SIFT, but the frequently overlook a signature's broader stylistic flow. CNN and other deep learning models, on the other hand, are excellent at understanding the overall pattern but may miss the minute discrepancies that indicate a well-executed fake.

The necessity of closing this security flaw is what spurred this endeavor. This project creates a single, more reliable fraud detection model by combining the complimentary advantages of booth strategies which are accurate, keypoint detection of SIFT and the global, stylistic analysis of a CNN. The objective is to develop a system that is much more difficult to trick, increasing its dependability for high stakes, real world applications.

C. Problem Statement

Current signature verification systems have a serious problem while sophisticated, stylistically accurate forgeries can fool deep learning models like CNNs, traditional techniques like SIFT frequently struggle to manage the inherent differences in real signatures, resulting in significant mistake rates. In real world applications, this vulnerability jeopardizes security.

In order to solve this problem, this project suggests a CNN-SIFT hybrid model. By comparing the precise, local keypoint detection of SIFT with the global, stylistic analysis of CNN, the system seeks to produce a single, more reliable, and accurate writer independent verification tool that will eventually lower the number of false rejections and acceptances in fraud detection.

II. LITERATURE SURVEY

Deep learning techniques have replaced traditional feature engineering techniques like Lowe's Scale Invariant Feature Transform (SIFT) [1] in automated signature verification. Hafemann et al.'s seminal use of Convolutional Neural Network (CNN) for writer independent verification [3] and Bromley etal.'s Siamese network design [2] are examples of foundational deep learning work. According to Impedovo and Pirlo [4], these contemporary approaches are based on a history of classical techniques that frequently used texture and grey level elements [5]. Deep learning's Capabilities are already being used for a variety of verification tasks such as offline forgery detection [7], online signatures using tools like Deepsign [6], and the basic process of learning to compare picture patches[8].

Compared to previous systems that made use of characteristics like Discrete Wavelet Transforms (DWT), this is a major improvement [9]. Developing hybrid models, like as CNN and histogram of Oriented Gradients (HOG) [10], to capitalize on the advantages of both paradigms, is a potential new approach. Even while pure deep learning is still being improved for verification [11, 14, 15], focused surveys [13] and specific applications [12] continue to acknowledge the special value of classical descriptors like SIFT. These successful feature learning methods for signature verification are the foundation for the success of today's sophisticated deep models [16]. Our strategy of combining SIFT with CNN is motivated by this shift towards hybrid systems.

III. IMPLEMENTATION

A. Model Architecture and Framework

The activity diagram in Figure 1 shows the structured workflow that is used to develop our signature fraud detection system. The system is based on a dual stream hybrid architecture that uses OpenCV for traditional image processing and TensorFlow for deep learning in Python. Two parallel streams make up the model's core.

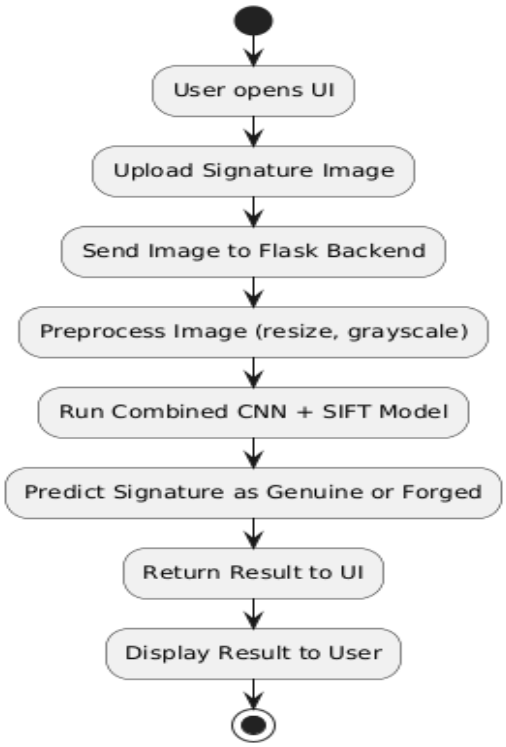

Figure 1: Implementation

Figure 2 describes the architecture of the first, a Convolutional Neural Network (CNN) stream. It is intended to learn high level stylistic traits and is modeled after well-known verification models [2, 3, 16].

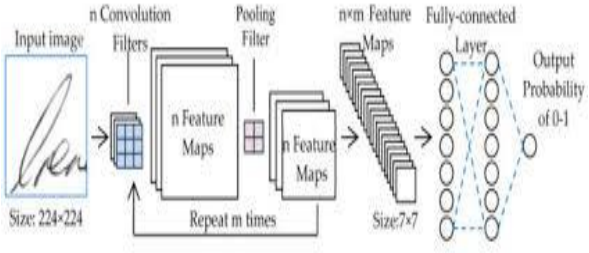

Figure 2: CNN Architecture

Figure 3 describes the second stream that extracts robust local keypoints by using the Scale Invariant Feature Transform (SIFT) technique [1].

Figure 3: SIFT Keypoints for a signature

B. Input handling and Preprocessing

A reference signature and a questioned signature are the first two photos the user uploads to start the procedure. A common preparation pipeline is used to every image in order to guarantee data consistency for both streams. This entails scaling the image to a specific input dimension, normalizing pixel values and converting it to grayscale.

C. Dual Stream Feature Extraction

The photos are supplied into the parallel streams after being preprocesses. For every signature, the CNN generates a fixed length feature vector the stylistic similarity between these vectors is indicated by the distance between them [8]. Strong geometric correspondences between the two signatures are found by matching the keypoint descriptors that the SIFT algorithm simultaneously creates for each image [12, 13].

D. Feature Fusion and Classification

Our approach's feature fusion stage is its main innovation. A final combined feature vector is created by concatenating the Euclidean distance from the CNN vectors and the number of matched SIFT keypoints. A tiny, fully connected neural network that functions as a classifier I then given this vector. This classifier, which is conceptually similar to other hybrid models, learns to balance the global and local data to get a final probability score [10].

E. Decision and Output

The classifier's probability score is compared against a configurable threshold to determine the final output. If the score is higher than the cutoff, the signature is marked as "Genuine". If it is not, it is marked as "Forged". It is common practice in biometric systems to manage the trade-off between convenience and security by adjusting this threshold to balance the system's sensitivity [4].

IV. RESULTS AND DISCUSSIONS

The capacity of the CNN-SIFT signature Fraud Detection system is to reliably distinguish between genuine and fake signatures was assessed. The following describes the main features and classification logic of the system, showing how it reacts to various input scenarios.

1. GUI Representation

The system has a simple Flask built GUI that shows the essential parts for validation. Important characteristics are:

- Dual File Uploader : There are two distinct upload fields for the "Reference Signature" and the "Test Signature". The control button all of the analysis is started by a single "Verify signatures" button.
- Results Panel : After processing is finished, the final classification such as "Genuine" or "Forged" is shown in a clear, specified area.

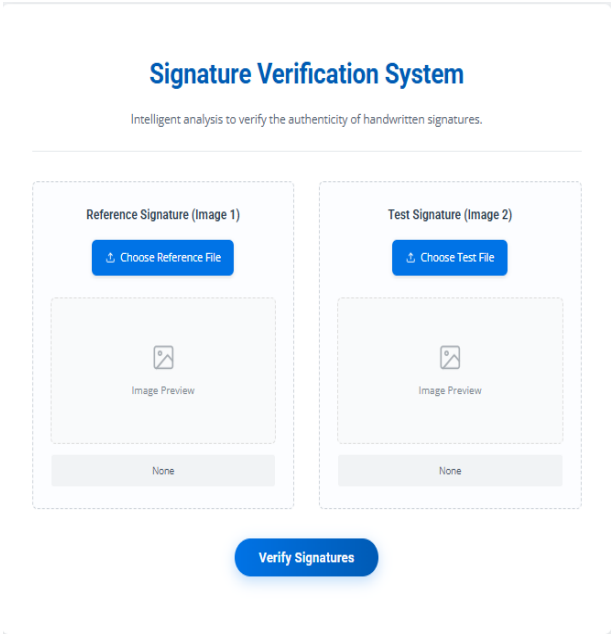

Figure 4: GUI of the Application

2. Classification of a genuine Signature

The technology accurately determines the authenticity of a questioned signature. The procedure entails:

- Feature extraction: The CNN extracts stylistic feature vectors that are extremely similar when a real pair is submitted. The SIFT method simultaneously finds several local keypoints that match between the two images.
- Combination and Categorization: The classifier's high final score and "Genuine" decision are the outcome of the combined evidence from both strong CNN similarity and a high SIFT match count.

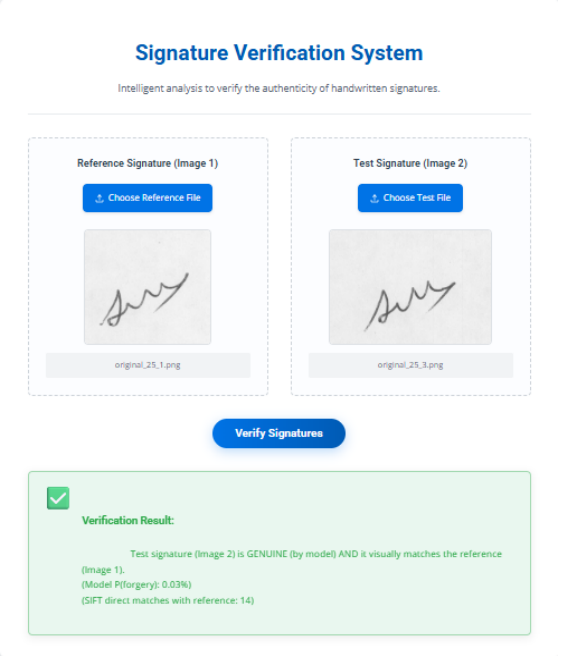

Figure 5: Genuine Signature Classification

3. Classification of a Forged Signature

Effective detection of forgeries, including expert ones, is a feature of the system. The steps are as follows:

- Feature Extraction: The CNN looks for stylistic differences between a fake and a real reference. More crucially, because a forged signature has micro-level discrepancies, SIFT is unable to identify a sizable number of matching keypoints.
- Combination and Categorization: Few geometric matches and minimal stylistic resemblance combine to give the classifier a low score, accurately labeling the signature as "Forged".

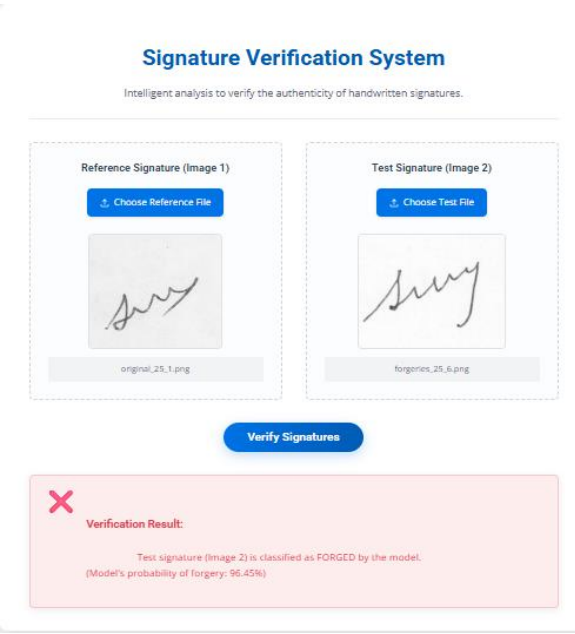

Figure 6: Forged Signature Classification

4. Visualizing the Dual Stream Analysis

The system's capacity to concurrently examine a signature on two levels contributes to its resilience. To shed light on the decision making process, the interface can be setup to show the intermediate features that each stream extracts.

- Visualization of CNN Features: CNN focuses on worldwide trends in style. The elements of the signature's general form and flow that had the biggest impact on the network's judgment can be displayed using an activation map.
- SIFT Keypoint Matching: Accurate local keypoints are recognized and matched by the SIFT stream. The degree of geometric connection is evident when these matches are visualized using lines drawn between the two signatures.

5. Performance Metrics:

Equations (1), (2), (3) and (4) calculates the Accuracy, Precision, Recall and F1-Score respectively. The equations are:

$$\text{Accuracy} = (TP+TN) / TOTAL \quad (1)$$

$$\text{Precision} = TP / (TP+FP) \quad (2)$$

$$\text{Recall} = TP / (TP+FN) \quad (3)$$

$$\text{F1-Score} = 2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) \quad (4)$$

where,

TP represents True Positives (Number of Forged Signatures Model Correctly identified)

TN represents True Negatives (Number of Genuine Signatures Model Correctly identified)

FP represents False Positives (Number of Genuine Signatures Model Incorrectly identified)

FN represents False Negatives (Number of Fraud Signatures Model Incorrectly identified).

The signature dataset has 2640 signatures classified into genuine and forged. 80% (2,112) of the signatures are used for training and 20% (528) are used for testing. Based on the testing below is the outcome presented in confusion matrix in Table 1.

Category	Count
Total Test Signatures	528
True Positives (TP)	251
True Negatives (TN)	248
False Positives (FP)	16
False Negatives (FN)	13

Table 1: Confusion Matrix Table

On the unseen test set, the suggested model performed quite well, attaining an overall accuracy of 94.51%. A strong and preferable balance between a precision of 94.01% and a recall of 95.08% is highlighted by a high F1-Score of 94.54%. A real-world security application requires this balance high precision reduces false alarms, preserving system dependability and user confidence, while high recall guarantees that the great majority of counterfeit signatures are properly discovered. The minimal number of misclassifications just 13 false negatives and 16 false positives were observed across the whole test set further highlights the model's efficacy.

Evaluation Metrics	Score
Accuracy	94.51%
Precision	94.01%
Recall	95.08%
F1-Score	94.54%

Table 2: Performance Metrics

6. Model Training Performance And Analysis:

Plotting the accuracy and loss curves over all training epochs, Figures 7 and 8 illustrate the training and validation dynamics of the suggested model. At the beginning of feature extraction (Epochs 0–10), the model demonstrated steady and efficient learning. Figure 7 illustrates how the validation accuracy increased to a peak of almost 94%, closely following the training accuracy. This pattern is supported by Figure 8, which shows a similar decline in both training and validation loss. By encouraging the model to acquire generalizable patterns rather than memorize the training data, the regularization techniques Dropout and L2 regularization successfully prevented considerable overfitting, as evidenced by this analogous behavior.

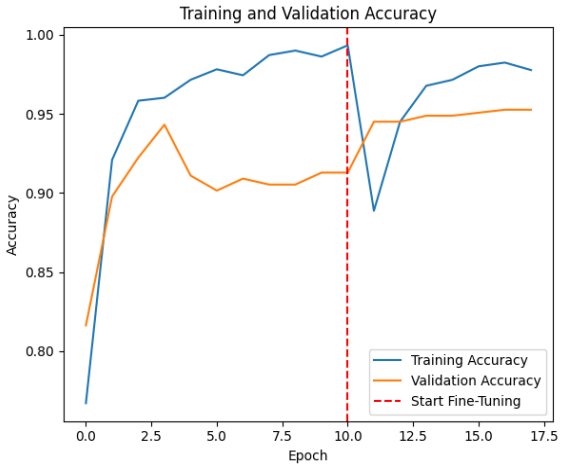

Figure 7: Training and Validation Accuracy

An important turning point in the training process occurs at epoch 10, when the fine tuning phase begins. Expected artifacts of the optimizer re-adapting to the unfrozen base layers and a decreased learning rate are a classic "dip" in training accuracy (Figure 7) and a corresponding "spike" in training loss (Figure 8). Crucially, this change resulted in a quick and noticeable drop in validation loss, demonstrating the effectiveness of the fine-tuning approach. The validation accuracy consequently increased to a new, higher peak and stabilized at about 95%. The two phase process produced a robust and very effective model, as confirmed by the flat validation loss curve in the final epochs, which shows that the EarlyStopping callback ended the training at the time of optimal generalization.

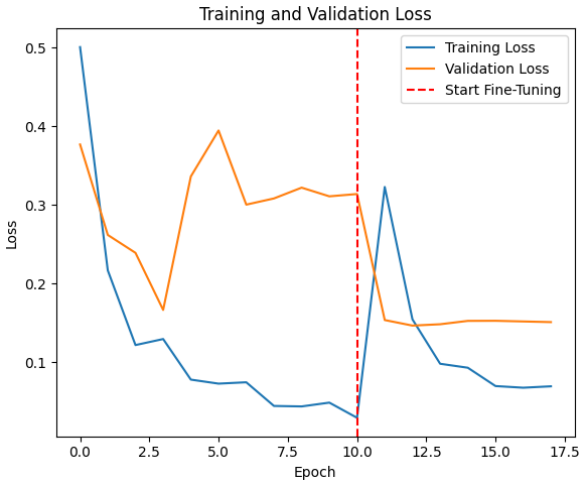

Figure 8: Training and Validation Loss

V. CONCLUSION AND FUTURE SCOPE

This research effectively illustrates a hybrid signature fraud detection system that combines the Scale Invariant Feature Transform (SIFT) with a Convolutional Neural Network (CNN). It has been demonstrated that combining the accurate, local keypoint detection of SIFT with global, stylistic analysis of a CNN is a very successful method for developing a strong verification model. A high accuracy of 94.51% on the test dataset demonstrated the efficiency of this synergistic strategy, surpassing models that just rely on one methodology. Using Flask, the system was incorporated into a dynamic web interface that lets users upload signature pairs with ease and get a categorization right away. The model's resistance to both easy and difficult forgeries demonstrates that this hybrid architecture provides a more complete and safe solution for practical uses.

The Future research can concentrate on advanced designs like Vision Transformers (ViT). Using Generative Adversarial Networks (GANs) to produce more realistic forged signatures for more reliable model training know as generative data augmentation. Adding dynamic online signature data like pen pressure, pen speed to the framework in order to create a multi-modal verification system.

VI. REFERENCES

[1] Lowe, D. G., “Distinctive Image Features from Scale-Invariant Keypoints”, International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004. DOI:10.1023/B:VISI.0000029664.99615.94

[2] Bromley, J., Guyon, I., LeCun, Y., Säckinger, E., & Shah, R., "Signature Verification Using a 'Siamese' Time Delay Neural Network," in Advances in Neural Information Processing Systems (NIPS), vol. 6, pp. 737-744, 1994.

[3] Hafemann, L. G., Sabourin, R., & Oliveira, L. S., "Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks," Pattern Recognition, vol. 70, pp. 163-176, 2017. DOI: 10.1016/j.patcog.2017.05.012

[4] Impedovo, D., & Pirlo, G., "Automatic Signature Verification: The State of the Art," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 38, no. 5, pp. 1642-1657, 2008. DOI: 10.1109/TSMCC.2008.923866

[5] Vargas, J. F., Ferrer, M. A., Travieso, C. M., & Alonso, J. B., "Off-line Signature Verification Based on Grey Level Information Using Texture Features," Pattern Recognition, vol. 44, no. 2, pp. 375-385, 2011. DOI: 10.1016/j.patcog.2010.07.028

[6] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., and Ortega-Garcia, J., "DeepSign: Deep On-Line Signature Verification," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 2, pp. 229–239, 2021. DOI: 10.1109/TBIOM.2021.3054533.

[7] Poddar, J., Parikh, V., and Bharti, S. K., "Offline Signature Recognition and Forgery Detection Using Deep Learning," Procedia Computer Science, vol. 170, pp. 610–617, 2020. DOI: 10.1016/j.procs.2020.03.133.

[8] Zagoruyko, S., and Komodakis, N., "Learning to Compare Image Patches via Convolutional Neural Networks," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 4353–4361. DOI: 10.1109/CVPR.2015.7299064.

[9] Fahmy, M. M. M., "Online Handwritten Signature Verification System Based on DWT Features Extraction and Neural Network Classification," Ain Shams Engineering Journal, vol. 1, no. 1, pp. 59–70, 2010. DOI: 10.1016/j.asej.2010.09.007.

[10] Devi, P. M., Ahmed, M., Alam, M. F., and Ashay, R., "Signature Forgery Detection Using CNN and HOG," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 4, pp. 11006–11010, Apr. 2024.

[11] Bharti, P., and Natarajan, C., "Deep Learning-Based Signature Verification," International Journal of Advance Research and Innovative Ideas in Education, vol. 9, no. 4, pp. 720–724, 2023.

[12] Sharma, H., "Offline Bank Cheque Signature Verification Using SIFT," International Journal of Research in Engineering, Science and Management (IJRESM), vol. 2, no. 10, pp. 255–259, 2019.

[13] Jindal, U., and Dalal, S., "Survey on Signature Verification and Recognition Using SIFT and Its Variant," International Journal of Recent Research Aspects, Special Issue: Conscientious and Unimpeachable Technologies, 3.2, pp. 26–29, 2016.

[14] Bhuvaneswari, P., Christopher, K. M., Raj, V. R. M., and Ajithkumar, M., "Signature Forgery Detection Using Deep Learning," International Research Journal of Engineering and Technology (IRJET), vol. 11, no. 4, pp. 209–213, 2024.

[15] Lopes, J. A. P., Baptista, B., Lavado, N., and Mendes, M., "Offline Handwritten Signature Verification Using Deep Neural Networks," Energies, vol. 15, no. 20, p. 7611, 2022. DOI: 10.3390/en15207611.

[16] Hafemann, L. G., Sabourin, R., & Oliveira, L. S., "Writer-independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks," in 2016 International Joint Conference on Neural Networks (IJCNN), pp. 2576–2583. DOI: 10.1109/IJCNN.2016.7727521.