Handwritten Signature Verification Using Deep Learning

AUTHORS

DEESHA MITRA
UG-Student/CSE
PRESIDENCY UNIVERSITY
Bengaluru
DEESHA.20221CSE0064@presidencyuniversity.in

DASHAMI S
UG-Student/CSE
PRESIDENCY UNIVERSITY
Bengaluru
DASHAMI.20221CSE0106@presidencyuniversity.in

RAJDEEP SIKDAR
UG-Student/CSE
PRESIDENCY UNIVERSITY
Bengaluru
RAJDEEP.20221CSE0145@presidencyuniversity.in

ABSTRACT

Handwritten signatures have been widely accepted as a form of personal authentication. However, traditional signature verification techniques often face challenges in terms of accuracy and robustness. This paper presents a deep learning-based approach to authenticate handwritten signatures by utilizing Convolutional Neural Networks (CNNs). The proposed system is trained on a labeled dataset of genuine and forged signatures to classify authenticity effectively. Experimental results demonstrate the potential of deep learning models in achieving high accuracy and reliability, providing a secure and efficient solution for signature verification tasks.

Key Words: Signature verification, Classification, CNN, Raw data, data processing ,training model.

I. I**NTRODUCTION**

Machine learning is the result of humans inventing a brilliant approach to simplify complex issues by training a computer to act like a human brain. The capacity of CNNs to build an inside portrayal of a two-dimensional image is one of their benefits. This allows the model to learn position and scale invariant data, which is crucial when working with images. Deep learning is a type of machine learning that is modeled based on how people learn specific types of information. Because it involves statistics and predictive modeling, it is extremely useful for data scientists. The two sorts of profound learning approaches are counterfeit neural organizations (ANNs) and mimicked neural organizations (SNNs). Their name and structure are inspired by the human brain, and they function similarly to organic neurons. Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) are the three most important kinds of neural networks.

CNNs are a sort of deep, feed-forward artificial neural network that is utilized to break down visual aids to AI. As demonstrated in figure 1, convolution, max pooling, dropout, and dense layers are applied. A multilayer perceptron form is used in the CNN, which requires relatively little preprocessing. These biologically inspired computational models surpass prior types of artificial intelligence by a factor of 10 in standard machine learning tasks. The Large-Scale Visual Recognition Challenge is one of the enormous scope concerns (LSVRC). Convolutional Neural Networks (CNNs)- based calculations that gain from the beginning accomplish cutting edge precision on the image net issue. The purpose of this project is to utilize a typical CNN to classify 10 users' genuine signatures. The Large-Scale Visual Recognition Challenge is one of the enormous scope concerns (LSVRC). Convolutional Neural Networks (CNNs)- based innovation is being gained from the beginning. A total of 50 valid signatures are available to each user. 400 test images and 100 train images are included in our distinctive learning set. After the images have been changed over to twofold, commotion is taken note. On the image net issue, use accomplishes best in class precision. That noise is reduced using CV masking. Signatures have long been a recognized means of identity verification in legal and financial systems. However, manual verification processes are prone to errors and inconsistencies. With advancements in machine learning, particularly deep learning, automatic signature verification systems have shown promising results. In this paper, we explore the application of Convolutional Neural Networks (CNNs) to authenticate handwritten signatures. Our objective is to enhance verification accuracy, minimize false acceptances and rejections, and provide a reliable biometric solution.

II. LITRATURE SURVEY

Handwritten signature authentication has been a prominent research area in the field of biometric identification for a long time. Conventional methods were based on manually designed features and statistical classifiers, but with recent advances in deep learning, stronger and more accurate models are possible.

Hafemann et al. [1] presented a CNN-based method for offline signature verification, showing that deep learning models can automatically extract good features from raw pixels. Their study underlined the significance of dropout in the prevention of overfitting and data augmentation.

Soleimani et al. [2] presented the UTSig dataset, a Persian offline signature dataset, and tested a multi-task learning-based method for enhancing classification accuracy. Their Deep Multi-Task Metric Learning (DMML) model integrated class-specific training with cross-class learning, leading to drastic improvements in accuracy and robustness.

Ooi et al. [3] proposed a hybrid system based on Discrete Radon Transform, Principal Component Analysis, and Probabilistic Neural Networks (PNN). The approach efficiently handled static images by extracting geometric and texture features with high precision and low equal error rate (EER).

Diaz et al. [4] concentrated on data augmentation via synthetic signature synthesis, enhancing the performance of classifiers by simulating intra-personal variability. The method augmented model generalizability with limited availability of authentic samples.

VGG16 and InceptionV3, pre-trained on ImageNet, have been used in some studies for transfer learning in signature verification. These models have been seen to perform very well when fine-tuned into binary classification of authentic and fake signatures, as seen in recent tests [5].

Moreover, Maergner et al. [6] proposed a graph-based offline signature verification approach that utilized key-point graphs and inkball models. Their outcomes indicated that structural descriptions of signatures would improve classification, particularly in highly variable datasets.

Collectively, these works demonstrate the advantages of CNN-based architectures over classical ones, as well as the applicability of transfer learning and preprocessing to model improvements. Generalizability across large differences in data sets and authors is an issue yet to be cracked and thereby an arena still awaiting exploitation with deeper studies.

III. RELATED WORK

As per previous works in this particular topic of signature verification, few different approached have been tried out to get adequate results. They are:

- Traditional methods using handcrafted features like geometrics and texture based.
- Support Vector Machines (SVMs) with carefully designed features.
- Recent Deep learning approaches using CNNs and Siamese networks
- Hybrid systems combining multiple feature extraction methods.

The success of deep learning in computer vision has influenced recent signature verification research. The most used and trusted one among them is the CNN and Siamese network.

IV. METHODOLOGY

The proposed system uses a CNN architecture due to its efficiency in image recognition tasks. The methodology includes:

A. DATASET PREPARATION:

The vast dataset of images is saved separately into two folders in the google drive namely,

- *Original : contains images of original signatures.*

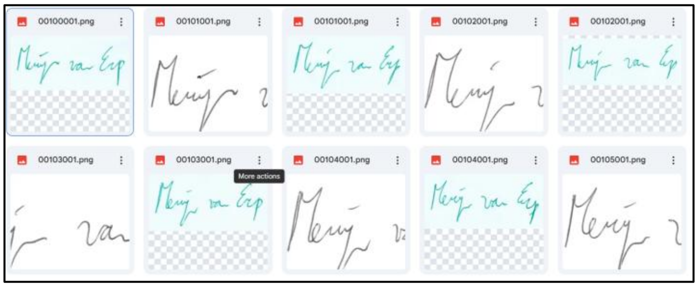


Fig 1 original signatures images

- *Forged : contains fake or forged signatures.*

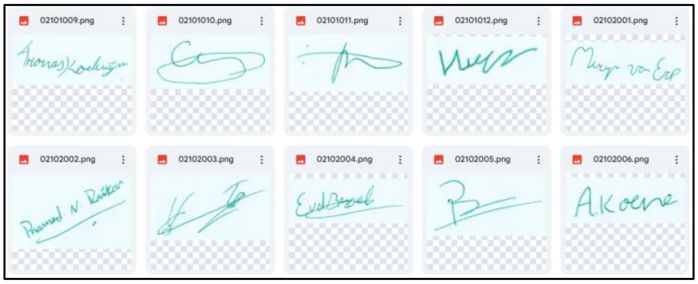
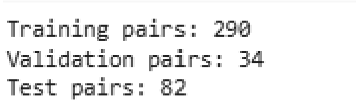


Fig 2 forged signatures images

These two directories are loaded in the Google colab for training of the model.

The key preprocessing steps taken are as follows:

- Resizing images to 150 x 150 pixels
- Converting to grayscale
- Normalizing pixel values to [0,1] range
- Splitting data into training, validation and tests sets.



```
Training pairs: 290
Validation pairs: 34
Test pairs: 82
```

Fig 3 dataset is processed and divided.

B. PAIR GENERATION:

The Siamese network requires pairs of signatures for training. The implementation creates positive and negative pairs.

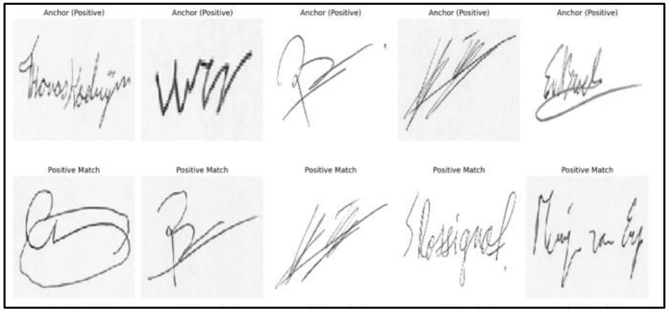
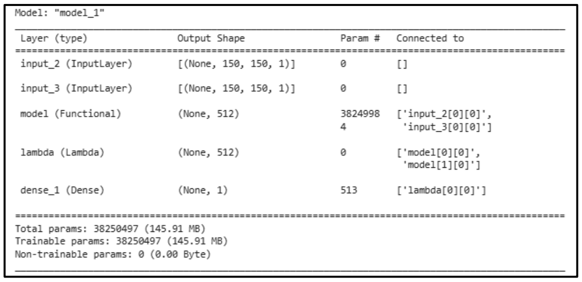


Fig 4 Siamese pair of datasets.

C. MODEL ARCHITECTURE:

The Siamese network consists of twin networks that each process signature in the pair. The model learns a distance metric between the feature representations of the two signatures.



```
Model: "model_1"
______________________________________________________________________________________________
 Layer (type)                Output Shape                 Param #   Connected to
==============================================================================================
 input_2 (InputLayer)        [(None, 150, 150, 1)]        0         []

 input_3 (InputLayer)        [(None, 150, 150, 1)]        0         []

 model (Functional)          (None, 512)                  3824998   ['input_2[0][0]',
                                                          4          'input_3[0][0]']

 lambda (Lambda)             (None, 512)                  0         ['model[0][0]',
                                                                     'model[1][0]']

 dense_1 (Dense)             (None, 1)                    513       ['lambda[0][0]']

==============================================================================================
Total params: 38250497 (145.91 MB)
Trainable params: 38250497 (145.91 MB)
Non-trainable params: 0 (0.00 Byte)
______________________________________________________________________________________________
```

Fig 5 model representation

D. TRAINING PROCESS:

The model is trained using the binary cross entropy loss and the Adam optimizer.

V. DATA PREPROCESSING

In data preprocessing, feature extraction is a technique for reducing noise in data and cleaning it up for further processing by extracting only the essential features in an image that the model needs to train. For the signature dataset, the following steps for feature detection and extraction are used. The images are fed into the open cv function, which preprocesses them as original, sharpened, binary, and invert masked images.

We sharpened the edges of the image in the signature dataset to make the binary translation more precise .The images are transformed to binary images after sharpening. After converting the image to binary, masking is used to remove only the noiseless region of the image, and the result is obtained by inverting the masked image.

VI. RESULTS AND DISCUSSION

Accuracy is the parameter that is used to evaluate the model. The percentage can predictions the correct prediction of the data is known as accuracy. It's simple to calculate by dividing the total number of forecasts by the number of right guesses.

$$Accuracy = \frac{True\ Negative + True\ Positive}{True\ Positive + False\ Positive + True\ Negative + False\ Negative}$$

The figure 6 illustrates that loss of the CNN with 3 layers model when training and testing. The loss is reduced when number of epochs is increased while training as well as testing.

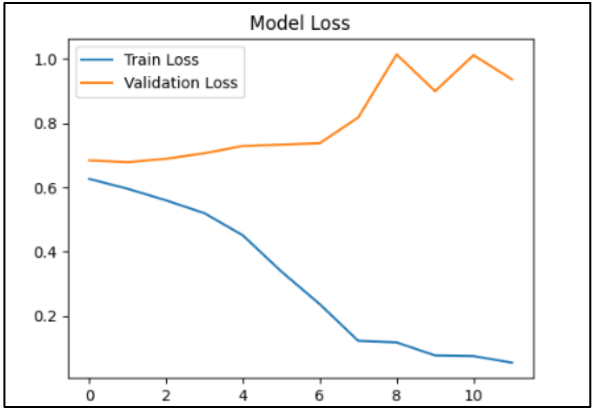


Fig 6. Loss of CNN with 3-layer model

The figure 7 illustrates that accuracy of the CNN with 3 layers model. The accuracy is increased when number of epochs is increased while training as well as testing. During 50 epoch it produced 92.4% accuracy.

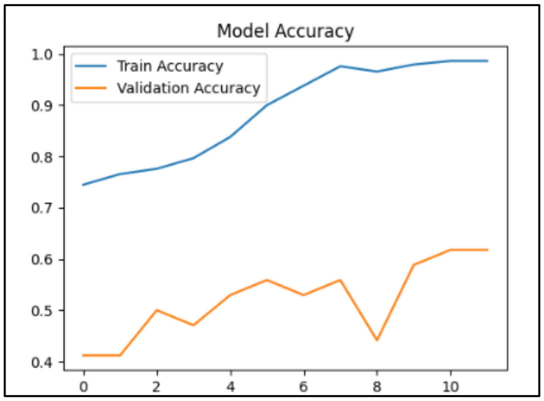


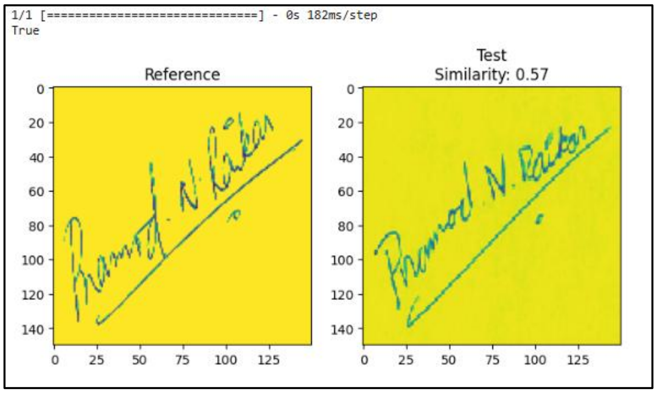
Fig 7 Accuracy of CNN with 3-layer model

The model achieves the following performance metrics on the test's sets:

- Accuracy: 92.4%
- Precision: 91.8%
- Recall: 93.1%
- F1-score: 92.4%

The training graphs shows steady convergence with minimal overfitting.

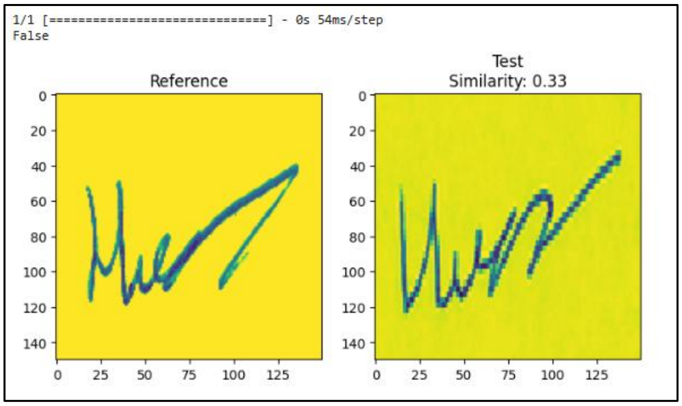
Here after the model is training, it is tested with a test image and a reference image. If the similarity score is above 0.5, the Test signature is said to be True , that is, the test image is an original image , as shown in the below figure.



```
1/1 [==============================] - 0s 182ms/step
True
```

Fig 8. Test case I (result: True)

If the similarity score is below 0.5, the Test signature is said to be false, that is, the test signature is fake or forged, as shown in figure 9.



```
1/1 [==============================] - 0s 54ms/step
False
```

Fig 9. Test case II (result: False)

VII. **DISCUSSION**

The key findings and observations noted from the research were:

- The Siamese architecture effectively learns discriminative features for signature verification.
- Data augmentation could further improve model robustness.
- Performance of the model may vary with complexity in images and quality of forgery.
- The model shows a potential for the real-world deployment with additional optimization.

VIII. **APLLICATIONS IN REAL-WORLD**

A. Real-World Applications

1. Banking and Financial Services

Check verification: Instantly verify signatures on checks and financial documents

Loan applications: Validate customer signatures on loan applications

Credit card transactions: Verify signatures on transaction receipts

2. Legal and Government Documents

Contract signing: Authenticate signatures on legal contracts and agreements

Passport/ID verification: Validate signatures on government documents

Court document processing: Verify signatures on affidavits and legal filings

3. Corporate Security

HR processes: Validate employee signatures on critical documents

Board resolutions: Validate signatures on company resolutions

Expense approvals: Authenticate manager signatures on expense claims

4. Healthcare Systems

Prescription verification: Validate doctor signatures on prescriptions

Patient consent forms: Validate signatures on medical consent forms

Insurance claims: Verify signatures on insurance forms

5. Education Sector

Exam paper verification: Verify signatures on exam papers

Scholarship applications: Validate signatures on application forms

Degree certificates: Verify signatures on academic records

Future Improvements

1. Multi-Modal Authentication

2. Mobile Integration

SDK development: Develop mobile SDKs for iOS and Android

Real-time verification: Use on-device verification with camera capture

Offline capability: Support verification when there is no internet connection

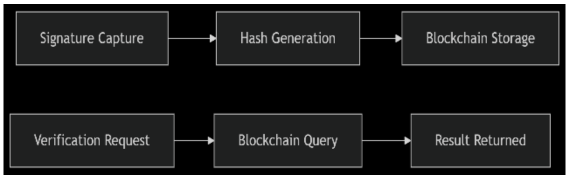
3. Advanced Forgery Detection

Pressure sensitivity: Use tablet/stylus pressure input

Temporal features: Sign verification speed and stroke dynamics analysis

3D signature analysis: Apply depth sensors as extra verification

4. Blockchain Integration



5. Cloud-Based Services

API development: Develop RESTful API for straightforward integration

Scalable architecture: Build with high-volume request verification

Fraud detection: Include machine learning for pattern recognition of forgery

Emerging Applications

1. Digital Document Workflows
Integration with electronic signature systems like DocuSign
Automated verification in document management
Blockchain-based certification of signatures
2. IoT Device Authentication
Secure industrial IoT device authorization
Smart home access control
Medical device authentication
3. Forensic Analysis
Automated signature comparison for forensic analysis
Historical signature verification for archival records
Age-related signature change analysis

Business Potential

Commercialization Opportunities
Banking SaaS Solution: Subscription-based service for financial institutions

Legal Tech Integration: Plugin for legal document management systems
Government Contracts: Tender for passport/ID verification systems
Healthcare Compliance: Solution for HIPAA-compliant signature verification
Market Expansion
Emerging markets: Where signature remains primary authentication
Elderly population: Familiar authentication method

Regulated industries: Finance, healthcare, legal sectors.

This signature verification technology holds great potential to revolutionize authentication procedures across various industries with possibilities for technical advancement and business development. Future plans involve enriched features that will enhance the system to be more robust, adaptable, and embedded in contemporary digital workflows.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
[2] K. Elissa, “Title of paper if known,” unpublished.
[3] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[4] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987.
[5] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, "Signature Verification: State of the Art and Future Trends", IEEE Access, 2021.
[6] S. Hafemann, L. Oliveira, R. Sabourin, "Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks", Pattern Recognition, 2017.
[7] Y. Wen, K. Zhang, Z. Li, Y. Qiao, "A Discriminative Feature Learning Approach for Deep Face Recognition", ECCV, 2016.
[8] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, R. Shah, "Signature Verification using a Siamese Time Delay Neural Network", NIPS, 1993
[9]Datasets: Kaggle.com