International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SIGNATURE FORGERY DETECTION

GAJULA VISHWATEJ CHANDRASHEKHAR

Master in Computer Applications (MCA)
ASM's Institute of Management & Computer Studies, Thane , Maharashtra, India

ABSTRACT :

To avoid forgery and ensure the confidentiality of information in the field of information technology security, security is an inseparable part of it. In order to deal with security, authentication plays an important role. A person's signature is a representative of his identity. For us at the bank, a signed document by a customer is an instruction from him to carry out an approved transaction for him. To avoid forgery and ensure the confidentiality of information in the field of information technology, security is an inseparable part of it. In order to deal with security, authentication plays an important role.

This project is basically a type of machine learning algorithm in which you will put on images of signatures that banks have of their customers, and this algorithm will compare them with forged signatures and tell whether the signature submitted while making a check payment or DD payment is true or not. The purpose of this project is to ensure that the rendered services are accessed only by a legitimate user and not anyone else. By using this method, it's possible to confirm or establish an existent's identity.

The plan of action of this project was to develop a sophisticated algorithm and code using the different identified liberties and tools with the methods mentioned in this report and to design a web app and implement the project. Basically, we want to build a system that can help distinguish forgeries from actual signatures. This system should be suitable to study hand signature parameters similar as strokes, curves, dots, dashes, and writing fluidity and style in a writer-independent manner and produce features for the identification of the signature.

Key Words: Offline Signature Recognition, Siamese Neural Network, Contrastive loss, Euclidean Distance.

I. INTRODUCTION :

A person's signature is a representative of his identity. For us at the bank, a signed document by a client is an instruction from him to carry out an approved transaction for him. To avoid forgery and ensure the confidentiality of information in the field of information technology, security is an inseparable part of it. In order to deal with security, authentication plays an important role.

This design is primarily a type of machine learning algorithm in which you'll put on images of signatures that banks have of their guests, and this algorithm will compare them with forged signatures and tell whether the signature submitted while making a check payment or DD payment is true or not. The purpose of this project is to ensure that the rendered services are accessed only by a legitimate user and not anyone else. By using this system, it's possible to confirm or establish an entity's identity.

On onboarding a customer, we capture an image of his signature in our systems, and on receiving a signed document (checks, DDs, and others) from him, we match the signature on the document with the one recorded in the database before pacing with the instruction. When someone masterfully forges anything, it becomes incredibly challenging to confirm the customer's identity.. This design is a system that can help distinguish forgeries from actual signatures. This system will be suitable to study hand signature parameters such as strokes, curves, dots, dashes, and writing fluidity and style in a writer-independent manner and produce features for the identification of the signature.

II. TECHNOLOGY :

Signature forgery detection involves various technologies to ensure the authenticity of signatures. Key technologies include:

Image Processing: Utilizes techniques such as edge detection, binarization, and noise reduction to analyse the visual features of signatures.

Machine Learning: Algorithms, including Support Vector Machines (SVM), Neural Networks, and Random Forests, are trained to distinguish between genuine and forged signatures based on extracted features.

Deep Learning: Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are employed for their ability to automatically learn hierarchical features from raw signature images.

Feature Extraction: Techniques like Histogram of Oriented Gradients (HOG), Scale-Invariant Feature Transform (SIFT), and Local Binary Patterns (LBP) are used to extract relevant features that describe the signature's characteristics.

Dynamic Signature Analysis: Captures the signing process using tablets or smartphones, analyzing dynamic features like speed, pressure, and stroke order.

Statistical Analysis: Applies statistical methods to measure variations and patterns in the signature, helping to detect inconsistencies.
Graphometric Techniques: Focus on the geometry and topology of the signature, analyzing the structure and spatial relationships of its components.

III. PROBLEM STATEMENT :

The problem statement in signature forgery detection revolves around accurately distinguishing between genuine and forged signatures to prevent fraud and ensure authenticity. Key challenges include:

1. Variability in Genuine Signatures: Authentic signatures can exhibit significant natural variations due to different signing conditions, emotional states, and other factors.
2. Sophisticated Forgeries: Forgeries can range from simple imitations to highly sophisticated, skilled copies that closely resemble genuine signatures.
3. Feature Extraction: Identifying and extracting relevant features that effectively capture the distinct characteristics of signatures while being robust to variations and noise.
4. Dataset Limitations: Availability of a sufficiently large and diverse dataset of genuine and forged signatures to train and evaluate detection models.
5. Scalability and Real-time Processing: Developing methods that are not only accurate but also efficient enough to be deployed in real-time applications.
6. Dynamic vs. Static Analysis: Balancing the use of dynamic signature data (captured during the signing process) and static images, each with its own set of features and challenges.

On onboarding a customer, we capture an image of his signature in our systems, and on receiving a signed document (checks, DDs, and others) from him, we match the signature on the document with the one recorded in the database before pacing with the instruction. The system will be able to study signature parameters such as strokes, curves, dots, dashes, and writing fluidity and style in a writer-independent manner and create features for the identification of the signatures.

The work is done in 2 steps:

Step 1: Accept and store a genuine signature image. Take an actual, signed image of the onboarding and store it in a database against a unique customer ID.
Step 2: Accept and Compare Hand Signature Images: Accepts inputs of the customer (client) ID and corresponding hand signature image. Compare the hand signature store in DB against the given customer (client) ID and return a confidence match score between the two hand signature images.

Advantages:

- This project increases the percentage of accuracy in recognizing the signature.
- This increases the percentage of accuracy in recognizing the signature.
- By reducing the cost, maintenance, and personnel.
- It reduces the chance of losing data due to hardware failures.
- Time saving.

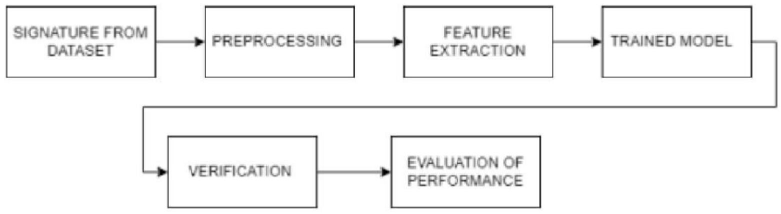
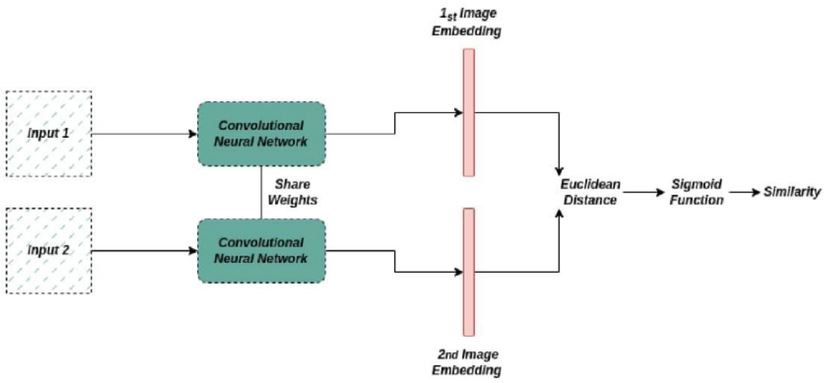


Figure 3.3: Block Diagram



V. PROPOSED ALGORITHM :

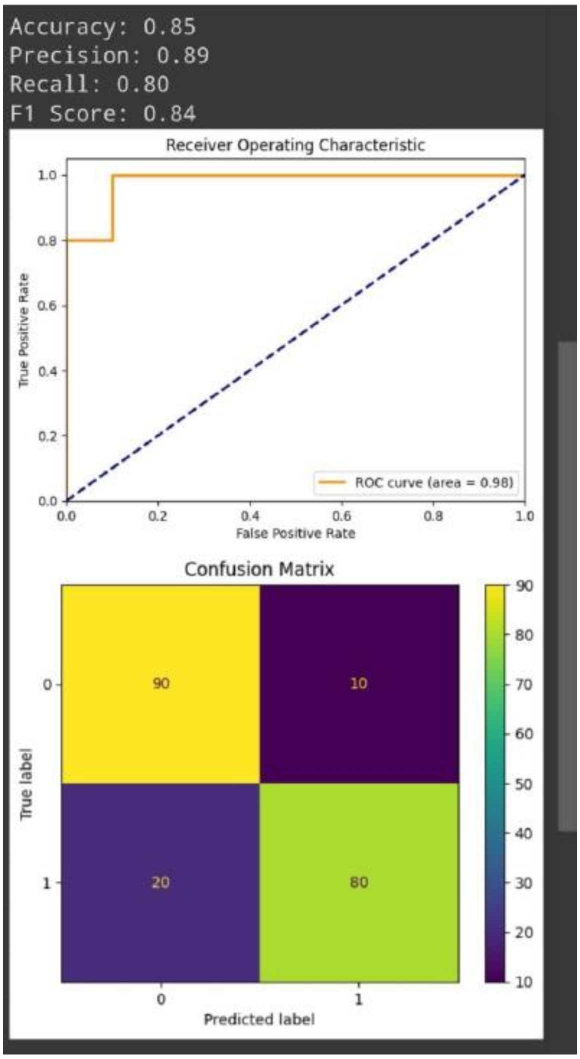
A Siamese neural network is a type of community architecture made up of two or more equal subnetworks; here, the two CNNs are set up in the same way, with the same parameters and weights. The updating of parameters is mirrored across subnetworks. This framework has been successfully applied to dimensionality discounting and verification in weakly supervised metrics. Those subnetworks are connected at the top by a loss characteristic that computes a similarity metric based on the Euclidean distance between the characteristic representations on each facet of the Siamese community. The contrastive loss is one such loss function that is commonly used in the Siamese community.

1. Data Preparation: The first step is to prepare the input data pairs that will be used to train the Siamese network. Each input pair typically consists of two data points, such as two images or two text documents, that are semantically related.
2. Network Architecture: The Siamese neural network consists of two identical neural networks that share the same weights. The input data pairs are fed into the two networks, and the output of each network is compared using a similarity metric.
3. Training: The Siamese neural network is trained using a set of labeled input data pairs. The network is optimized using a loss function that measures the difference between the predicted similarity score and the true similarity score. Popular loss functions for Siamese networks include contrastive loss and triplet loss.
4. Testing: Once the Siamese neural network is trained, it can be used to compare new input data pairs and compute a similarity score. This score can be used to determine the degree of similarity between the two input data points.
5. Fine-tuning: In some cases, the Siamese neural network may need to be fine-tuned on a new dataset to improve its performance on a specific task or domain. Fine-tuning involves retraining the network using the new dataset while keeping the original network architecture and weights intact.

VI. PERFORMANCE ANALYSIS :

When analyzing the performance of signature forgery recognition systems, key metrics such as accuracy, precision, recall, and F1 score are crucial. These metrics help evaluate the system's ability to correctly identify forged signatures while minimizing false positives and false negatives. Additionally, techniques like receiver operating characteristic (ROC) curves and confusion matrices provide deeper insights into the system's performance across different thresholds. By carefully examining these metrics and visualizations, researchers and developers can fine-tune their signature forgery recognition algorithms for optimal performance.

DefiLlama tracks TVL across multiple blockchains and protocols, offering insights into the DeFi ecosystem’s growth and performance.



```
Accuracy: 0.85
Precision: 0.89
Recall: 0.80
F1 Score: 0.84
```

VII. CONCLUSION :

Signature identification and verification deal with the problem of identifying and verifying signature samples from a set of samples available to us. The task of static signature verification is a difficult vision problem within the field of biometrics because the signature of an individual may change depending on the psychological factors of the person. Through this project, I am trying to develop a deep learning model for offline handwritten signature recognition that can extract high-level representations. Most of the models work well in the field only if the system can extract or create the right feature vector for a given image. However, the task is equally difficult. Thus, we use a different kind of model, in which we tend to extract a high-level representation of the model and thereby optimize the feature vector required. In our project, we conclusively demonstrated how we can optimize feature vectors and improve the accuracy of the overall task. Accurate signature verification models have a wide range of applications, ranging from banking to online transactions, access control systems, etc.

VIII. REFERENCES :

1. Shiwani Sthapak, Minal Khopade, Chetana Kashid,, Artificial Neural Network based signature, recognition and verification, International Journal of Emerging Technology and Advanced. Engineering, August 2013.
2. Neural network-based offline signature recognition and verification system. Research Journal of Engineering Sciences (Shikha, P., & Shailja S)
3. Offline Signature Recognition and Forgery Detection using Deep Learning (Jivesh Poddara, Vinanti Parikha, Santosh Kumar Bharti)
4. SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification (Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llad´os, Umapad
5. Ciresan, Dan; Meier, Ueli; Gambardella, Luca; Schmidhuber, Jürgen (2010). "Deep big simple neural nets for handwritten digit recognition". Neural Computation. 22 (12): 3207–3220. arXiv:1003.0358. doi:10.1162/NECO_a_00052. PMID 20858131.
6. Krizhevsky, Alex; Sutskever, Ilya; Hinton, Geoffrey E.

7. (2017-05-24). "ImageNet classification with deep convolutional neural networks" (PDF). Communications of the ACM. 60 (6): 84–90. doi:10.1145/3065386. ISSN 0001-0782.
8. LeCun, Yann. "LeNet-5, convolutional neural networks". Retrieved 16 November 2013.
9. Offline Handwritten Signature Recognition Using Polar-Scale Normalization,
10. https://ieeexplore.ieee.org/document/7863302