

Signature Fraud Detection Using Deep Learning

K. Lakshmi Prasanna, N. Ramya, I. Ganesh, K. Edukondalu, N. Lakshmi Janaki
Under The Esteemed Guidance of Mr. Y. Vamsi Krishna Teja M. Tech. Assistant Professor

Department Of Computer Science & Engineering
Bachelor Of Technology

Tirumala Engineering College
Jonnalagadda, Narasaraopet, GUNTUR(Dt.),A.P. 2020-2024

ABSTRACT

The use of signatures for personal identification and verification is quite common. Signatures are validated for many documents such as Bank cheques and legal transactions. The necessity for effective automated solutions for signature verification has grown as signatures are now a prerequisite for both authorization and authentication in legal activities. Two images—the original signature and the test signature—are used as input in this process. To determine whether the signature is fake or not, the characteristics that were extracted are compared, and the difference in error values between them is examined.

The growing digital landscape has increased the need for robust and efficient fraud detection systems. This project presents a unique approach to detecting signature fraud using deep learning techniques, specifically employing Siamese Neural Networks, implemented in Python.

With a dataset comprising 2149 signature images, encompassing both genuine and fraudulent samples from Dutch users, our model demonstrates remarkable accuracy. The Siamese Neural Network architecture excels in signature verification tasks by learning to distinguish between genuine and fraudulent signatures through contrastive learning.

The key achievement of this project is the exceptional accuracy levels attained during the training and validation phases. The model's training accuracy stands at an impressive 98.00%, while the validation accuracy reaches an astonishing 99.00%. These high accuracy rates are a testament to the effectiveness of Siamese Neural Networks in signature fraud detection.

In a world where the security of digital signatures is paramount, this project showcases the power of deep learning and Siamese Neural Networks in safeguarding against fraudulent activities. The model's success in accurately distinguishing between authentic and forged signatures offers promising potential for enhancing security measures in various domains, including finance, legal, and document management.

1. INTRODUCTION

Introduction to Signature Fraud:

Signature fraud, also known as forgery or signature-based fraud, is a prevalent and enduring form of financial and identity-related deception. It occurs when an individual or entity illicitly replicates or imitates another person's signature with the intention of committing fraudulent activities. Signatures are frequently employed as a means of authentication and authorization in various sectors, such as finance, legal, and government, making them a prime target for fraudsters seeking to gain unauthorized access, forge documents, or engage in other malicious activities.

The act of signature fraud involves the imitation of an individual's handwriting or signature style in an attempt to deceive institutions, authorities, or organizations into believing that the forged signature is genuine and legally binding. Fraudsters may use forged signatures to conduct unauthorized transactions, access confidential information, or falsify documents for financial gain or other unlawful purposes.

In the digital age, signature fraud has evolved to encompass both traditional and technologically sophisticated methods. While traditional forgery techniques involve the manual replication of signatures on paper documents, modern signature fraud may involve the use of digital tools, such as image editing software or advanced printing technologies, to create convincing forged signatures.

The consequences of signature fraud can be severe, leading to financial losses, legal disputes, damaged reputations, and compromised security. As a result

LITERATURE SURVEY

1) Automatic online signature verification: A prototype using neural networks AUTHORS: S. K. Ahmed, A. K. Ramasamy, A. S. Mohd. Khairuddin, and J. Omar

Signature verification is the process used to recognize an individual's handwritten signature to prevent fraud. In this paper pressure at the pen-tip together with the x, and y coordinates of the signature are measured and features extracted from these are used to verify the signature. A pressure pad was used to obtain signature samples. A signature verification system using SOM neural network was designed in MATLAB to verify the signatures. Results obtained using a prototype system are encouraging. The attractive features of this system are its low cost, low intrusion, good performance and use of an acceptable and natural biometric (the signature).

2) Signature verification using global and grid feature AUTHORS: Y. Qi and B. R. Hunt
In this work, algorithms for extracting global geometric and local grid features of

signature images were developed. These features were combined to build a multi-scale verification function. This multi-scale verification function was evaluated using statistical procedures. Results indicated that the multi-scale verification function yielded a lower verification error rate and higher reliability than the single-scale verification function using either global geometric or local grid feature representation. The correct verification rate of the multi-scale system was more than 90% in rejecting skilled forgeries and was perfect in rejecting simple forgeries based on a limited database.

3) Hand Written Signature Verification based on Geometric and Grid Features

AUTHORS: B. Kareem Abd, Q. Khaled Abood, and N. A.Z. Abdullah

The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system. Verification can be performed either Offline or Online based on the application. Offline systems work on the scanned image of a signature.

In this paper an Offline Verification of handwritten signatures which use set of simple shape based geometric features. The features used are Mean, Occupancy Ratio, Normalized Area, Center of Gravity, Pixel density, Standard Deviation and the Density Ratio. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. Features Extracted for whole signature first, then extracted for every part after dividing the signature into four sections. For verification, statistical verification techniques are used (Euclidean Distance, Hellinger Distance and Square Chord Distance). The system is trained on three datasets of signatures. The system has been tested on every dataset. The experimental results show that the Euclidean Distance has the average accuracy of 94.42, the Hellinger Distance has the average accuracy of 95.27 and the Square Chord Distance has the average accuracy of 93.14. That result for whole the image and the following average accuracy for image using grid the Euclidean Distance has the average accuracy of 93.54, the Hellinger Distance has the average accuracy of 95.87, and the Square Chord Distance has the average accuracy of 95.93.

4) Signature Recognition Using Backpropagation Neural Network AUTHORS: Y. Inan and B. Sekeroglu

Imitation or the fake signatures is the global fraud that cause the waste of financial

sources, time and human effort. For this reason, signature recognition is the most widely used biometrics system for security and personal identification. Signatures are the most complex human patterns which are used to identify and approve the authorized persons. They can be varied according to the paper and pen influences, and human psychology and characteristics at the signature moment. Therefore, effective recognition of signatures is required in order to minimize the fraud.

2. SYSTEM ANALYSIS AND DESIGN

2.1 Existing System

Before the adoption of deep learning techniques, the existing system for signature fraud detection relied on image processing methods to tackle the challenge of distinguishing genuine from fraudulent signatures. This system, developed using traditional computer vision and image processing techniques, played a crucial role in detecting fraud but had its limitations.

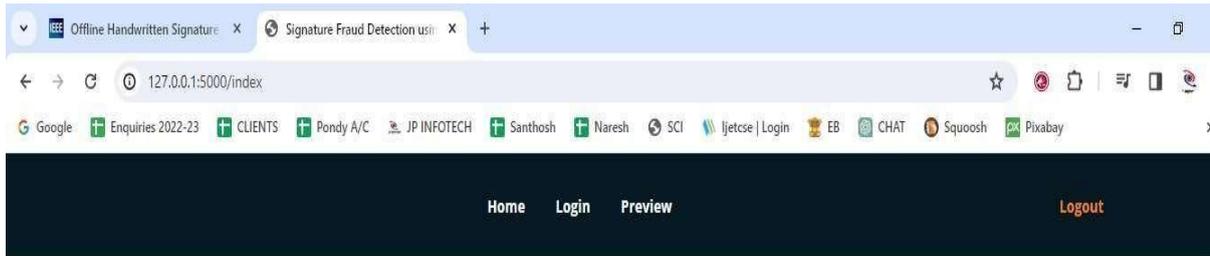
The existing system leveraged techniques such as feature extraction, texture analysis, and edge detection to process signature images. These methods aimed to capture distinctive characteristics of genuine and fraudulent signatures. Features like the curvature of strokes, pen pressure, and geometric properties were commonly used to build a foundation for signature verification.

Despite the efforts invested in the existing system, it faced several inherent challenges. Firstly, the performance heavily depended on the quality and consistency of the input images. Variations in lighting conditions, image resolution, and signature styles often led to suboptimal results, making it less robust for real-world applications. Additionally, the system struggled to adapt to evolving signature forgery techniques.

Furthermore, the dataset used in the earlier system often contained a limited number of samples, which hindered the

ability to learn and generalize from diverse signature styles and forgery methods. As a result, the accuracy of signature fraud detection was not always reliable.

In summary, the existing system for signature fraud detection using image processing techniques served as an important initial step in combating fraudulent



Signature Verification

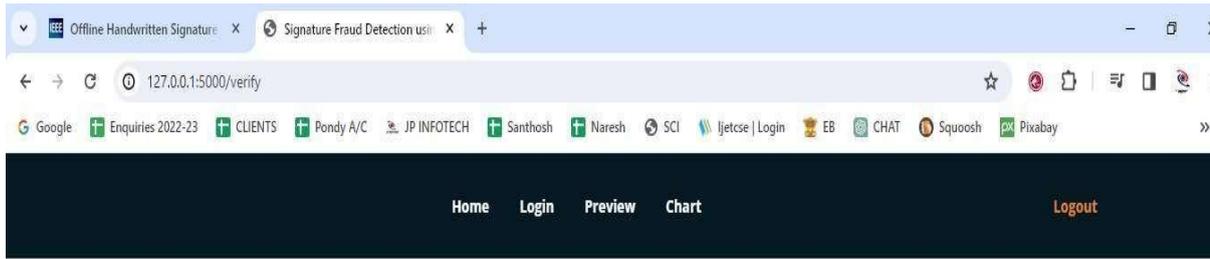
Preview.

Upload Image:

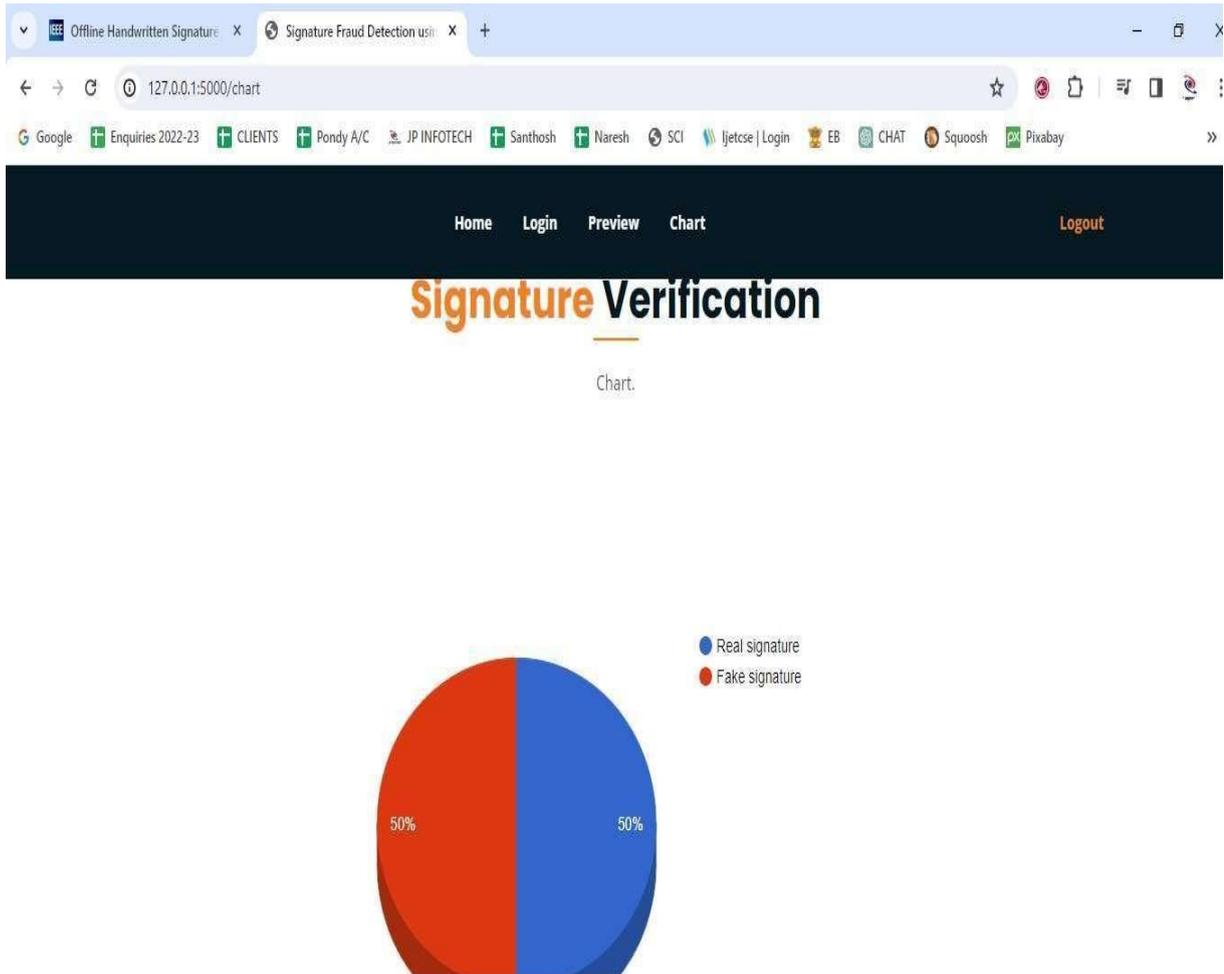
Choose File 01_023.png

Choose File 02_023.png

Submit



Prediction is : *The signature is Real*



3. SYSTEM TESTING

3.1 TEST STRATEGIES

System testing is a critical phase in the software development life cycle that focuses on assessing the overall quality, functionality, and performance of a software system. It is a comprehensive and systematic process that aims to identify defects, ensure that the system meets specified requirements, and verify its readiness for deployment. System testing plays a crucial role in delivering reliable, robust, and high-quality software solutions.

Importance of System Testing:

System testing serves as the final gatekeeper before a software system is released to users. It helps identify and rectify defects, glitches, and inconsistencies that might have gone unnoticed during earlier testing phases. By rigorously testing the complete system, organizations can ensure that the software behaves as intended, performs well under various conditions, and meets user expectations.

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

3.1.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Unit testing is an essential practice in software development that involves testing individual units or components of a software application in isolation. Each unit, typically a small piece of code or a function, is tested to ensure that it functions correctly and produces expected outcomes. Unit testing plays a pivotal role in maintaining code quality, catching bugs early, and facilitating efficient debugging and maintenance.

Importance of Unit Testing:

Unit testing focuses on verifying the correctness of code at its smallest functional level. By isolating and testing individual units, developers can identify issues early in the development process, preventing defects from propagating through the entire application. This practice promotes better

4. BIBLIOGRAPHY

- [1] S. K. Ahmed, A. K. Ramasamy, A. S. Mohd. Khairuddin, and J. Omar, “Automatic online signature verification: A prototype using neural networks,” IEEE Xplore, Jan. 01, 2009.
- [2] Y. Qi and B. R. Hunt, “Signature verification using global and grid features,” Pattern Recognition, vol. 27, no. 12, pp. 1621–1629, Dec. 1994, doi: 10.1016/0031-3203(94)90081-7.
- [3] B. Kareem Abd, Q. Khaled Abood, and N. A.Z. Abdullah, “Hand Written Signature Verification based on Geometric and Grid Features,” Jan. 2015.
- [4] F. Leclerc and R. Réjean, “Automatic Signature Verification: The State of the Art - 1989-1993.,” International Journal of Pattern Recognition and Artificial Intelligence, 8(3), Jun. 1994.
- [5] R. Sabourin, R. Plamondon, and G. Lorette, “Off-line Identification With Handwritten Signature Images: Survey and Perspectives.” Accessed: Nov. 25, 2022.
- [6] Y. Inan and B. Sekeroglu, “Signature Recognition Using Back propagation Neural Network,” 13th International Conference on Theory and Application of Fuzzy Systems and Soft Computing — ICAFS-2018, pp. 256–261, Dec. 2018, doi: 10.1007/978-3-030-04164-9_35
- [7] R. Plamondon and S. N. Srihari, “Online and off-line handwriting recognition: a comprehensive survey,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 63–84, 2000, doi: 10.1109/34.82482