**MAJOR PROJECT-02 ON**

**DETECTION OF FORGED SIGNATURES**

**Submitted by:**

|  |  |  |
| --- | --- | --- |
| **Devansh Khanna** | **500076674** | **R120219035** |
| **Kartik Garg** | **500077422** | **R134219053** |
| **Jagdish** | **500077088** | **R134219050** |

**Under the guidance of**

**KESHAV KAUSHIK**

**Asst. Professor-Senior Scale Department of Systemics**



# CANDIDATE’S DECLARATION

We hereby certify that the project work entitled “DETECTION OF FORGED SIGNATURES ” in partial fulfilment of the requirements for the award of the Degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with specialization in Cyber Security And Forensics and submitted to the School of Computer Science, Department of Systemics, University of Petroleum & Energy Studies, Dehradun, is an authentic record of our work carried out during a period from January-2023 to May-2023 under the supervision of Mr Keshav Kaushik

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: Jan - May 2023 Dr. Neelu Jyoti Ahuja HOD – Systemics

School of Computer Science

University of Petroleum & Energy

Studies Dehradun – 248 001 (Uttarakhand)

Project Guide

Mr. Keshav Kaushik

# ACKNOWLEDGEMENT

We wish to express our deep gratitude to our guide Mr. Keshav Kaushik, for all advice,

encouragement and constant support he have given us throughout our project work. This work would not have been possible without her support and valuable suggestions.

We sincerely thank our respected Program Head of the Department, Dr Neelu Jyoti Ahuja, for her great support in doing our project.

We would like to thank all our friends for their help and constructive criticism during our project work. Finally, we have no words to express our sincere gratitude to our parents who have shown us this world and for every support they have given us.



###### Department of Systemics

**School of Computer Science Engineering University of Petroleum & Energy Studies, Dehradun**

**Project Title Approval Form (2022-23)**

#### Major II

###### Project Title: DETECTION OF FORGED SIGNATURES

**Project Objective:**

**This project will somewhere help the user to detect the forged signatures that has been used by any unauthenticated user to gain access by using k-means algorithm.**

###### Team Member(s):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Name of the Student** | **Specialization & Semester** | **Roll Number** | **SAP ID** |
| **01** | **Devansh Khanna** | **BTech CSE-CSF** | **R120219035** | **500076674** |
| **02** | **Kartik Garg** | **BTech CSE-CSF** | **R130219053** | **500077422** |
| **03** | **Jagdish** | **BTech CSE-CSF** | **R134219050** | **500077088** |

**Role of Each Student:**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Role of the Student** | **Sign of the student** |
| **1.** | **Researching, Programming, Testing, Presentation** |  |
| **2.** | **Researching, Programming, Testing, Presentation** |  |
| **3.** | **Researching, Programming, Testing, Presentation** |  |

###### Approved By

**Project Guide Head of the Department**

###### Dr. KESHAV KAUSHIK Dr. Neelu Jyoti Ahuja

**Assistant Professor-Senior Scale Professor, Dept. of Systemics**

**SYNOPSIS REPORT ON**

**DETECTION OF FORGED SIGNATURES**

**Submitted by:**

|  |  |  |
| --- | --- | --- |
| Devansh Khanna | 500076674 | R120219035 |
| Jagdish | 500077088 | R134219050 |
| Kartik Garg | 500077422 | R134219053 |

**Under the guidance of**

#### Keshav Kaushik

###### Asst. Professor-Senior Scale Department of Systemics



**Department of Virtualization**

**School of Computer Science and Engineering**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Topic** | | **Page No** |
| Table of Content | | 01 |
| 1 | Abstract | 02 |
| 2 | Introduction | 02 |
| 3 | Problem Statement | 02 - 03 |
| 4 | Literature Review | 03 |
| 5 | Objective | 04 |
| 6 | SWOT Analysis | 04 - 05 |
| 7 | System Requirements | 05 |
| 8 | Schedule | 06 |
| 9 | Reference | 06 |

**SYNOPSIS REPORT (2022-23)**

#### ABSTRACT

The detection of forged signatures is a critical issue that affects various industries, including finance, legal, and government. Forged signatures are often used for fraudulent activities such as identity theft, forgery of legal documents, and other criminal activities. Therefore, the ability to accurately detect and prevent the use of forged signatures is crucial in maintaining the integrity of these industries.

The project on detection of forged signatures aims to develop a machine learning algorithm that can accurately identify forged signatures from genuine ones. The algorithm will be trained on a large dataset of signatures, both genuine and forged, using various deep learning techniques to analyze and extract relevant features. These features may include the shape, size, pressure, and stroke of the signature.

#### INTRODUCTION

Offline signatures are significant today. Offline signature verification and forgery detection are complex and fraught with serious problems. The forging of signatures causes cooperating and commercial organizations to suffer substantial financial losses and damages their security reputation. Forgery is frequently observed in the banking industry since it involves sensitive information, official paperwork, and government regulations (LIC) that could be vulnerable to fraud and its effects.

* Data protection
* Security
* Integrity maintained
* Ensured compliance
* Therefore, a system that can tell the difference between a real signature and a forgery is needed to reduce the likelihood of theft or fraud.

#### PROBLEM STATEMENT

The problem addressed by the project on detection of forged signatures is the prevalence of fraudulent activities that involve the use of forged signatures. Forged signatures are often used to deceive people or organizations for financial gains or other criminal activities, such as identity theft or forgery of legal documents. These fraudulent activities can result in significant financial losses, reputational damage, and other negative impacts on individuals and organizations.

Currently, there is a lack of effective methods to detect forged signatures. Traditional signature verification methods, such as manual inspection or signature comparison by experts, are time-consuming and often inaccurate. These methods are also limited in their ability to handle large volumes of signatures, which are common in industries such as finance, legal, and government.

#### LITERATURE REVIEW

* + The use of signatures as a means of authentication dates back to ancient times and is still prevalent today, despite the availability of alternative authentication methods.
  + Traditional signature verification methods rely on the visual inspection of signatures by experts or comparison of signatures to a known reference. These methods can be subjective, time-consuming, and may not be reliable in detecting advanced forms of forgery.
  + Various automated signature verification methods have been proposed in recent years, including machine learning techniques such as artificial neural networks, support vector machines, and decision trees. These methods have shown promising results in detecting forged signatures with high accuracy and efficiency.
  + One key challenge in developing machine learning algorithms for signature verification is the availability of large datasets of signatures, especially those containing both genuine and forged signatures. Various public datasets, such as the CEDAR Signature Verification Competition and the GPDS-100 dataset, have been developed to address this issue.
  + Deep learning techniques, such as convolutional neural networks and recurrent neural networks, have shown significant improvements in signature verification accuracy, particularly for complex forms of forgery, such as skilled forgery or disguised forgery.
  + The use of additional data sources, such as pressure data or acceleration data, can improve the accuracy of signature verification algorithms, particularly in identifying skilled forgeries.
  + The performance of signature verification algorithms can be impacted by factors such as variations in writing style, age of the signature, and the use of different writing instruments or surfaces.
  + The successful implementation of machine learning algorithms for signature verification has significant implications for various industries, including finance, legal, and government, as it provides a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures.

#### OBJECTIVE

The objective of the project on detection of forged signatures is to develop a machine learning algorithm that can accurately distinguish between genuine and forged signatures. The algorithm will be trained on a large dataset of signatures, using various deep learning techniques to analyze and extract relevant features. The final model will be optimized for high accuracy and real-time processing, capable of handling large volumes of signatures with minimal errors. The success of this project will have significant implications for fraud detection and prevention in various industries, including finance, legal, and government. The ultimate goal of this project is to provide a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures.

#### SWOT ANALYSIS

###### Strength:

###### The use of machine learning algorithms provides a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures.

###### The project's focus on developing a large and diverse dataset of signatures will improve the accuracy and reliability of the algorithm.

###### The use of deep learning techniques, such as convolutional neural networks and recurrent neural networks, has shown promising results in detecting and identifying forged signatures.

###### The algorithm's ability to handle large volumes of signatures in real-time processing makes it suitable for implementation in various industries, including finance, legal, and government.

###### Weakness:

###### The success of the algorithm depends on the availability of a large and diverse dataset of signatures containing both genuine and forged signatures.

###### The performance of the algorithm can be affected by variations in writing styles, age of the signature, and the use of different writing instruments or surfaces.

###### The use of advanced deep learning techniques can result in increased computational complexity and training time.

###### Opportunities:

###### The development of a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures can have significant implications for various industries, including finance, legal, and government.

###### The use of machine learning algorithms for signature verification can be extended to other applications, such as biometric authentication or fraud detection in online transactions.

###### Threats:

###### The prevalence of advanced forms of forgery, such as skilled forgery or disguised forgery, can pose significant challenges to the accuracy and reliability of the algorithm.

###### The use of adversarial attacks, where malicious actors intentionally modify signatures to evade detection, can also pose a threat to the accuracy of the algorithm.

###### The algorithm's success depends on its integration and adoption by various industries, which may require significant changes in existing signature verification systems and processes.

#### SYSTEM REQUIREMENTS

User Interface

The User Interface needed to run the project is Google Collab with Python 3 with installed in it.

Software Interface

Linux/Ubuntu/Windows XP /Windows 7 / Windows 10 /Windows 11/Python 3 Database Interface

Excel/Notepad

#### SCHEDULE

January:

Week 1-2: Research and finalize the project topic

Week 3-4: Create a detailed project plan, including tasks and deadlines February:

Week 1-2: Set up a development environment and gather the necessary resources Week 3-4: Start working on the project's main features

March: April: May:

Week 1-2: Continue working on the project's main features

Week 3-4: Start implementing secondary features and begin testing

Week 1-2: Continue implementing secondary features and testing Week 3-4: Refine the project and fix any issues or bugs

Week 1-2: Complete final testing and debugging

Week 3-4: Finalize project documentation and prepare for presentation or submission

#### REFERENCE

* + - National Institute of Standards and Technology (NIST) - Signature Verification Competition: https://www.nist.gov/itl/iad/mig/signature-verification-competition-svc-2020
    - IEEE Transactions on Information Forensics and Security: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
    - International Conference on Document Analysis and Recognition (ICDAR): http://icdar2019.org/
    - Springer - Signature Verification: The State of the Art: https://link.springer.com/book/10.1007/978-1-4471-2169-5
    - IEEE Transactions on Biometrics, Behavior, and Identity Science: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424
    - International Journal of Document Analysis and Recognition (IJDAR): https://link.springer.com/journal/10032

**Software Requirements Specification**

For Detection of forged signatures

April 2023

### Prepared by

|  |  |  |
| --- | --- | --- |
| **Specialization** | **SAP ID** | **Name** |
| Btech CSE-CSF | 500076674 | Devansh khanna |
| Btech CSE-CSF | 500077088 | Jagdish |
| Btech CSE-CSF | 500077422 | Kartik Garg |



Department of Informatics School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

## Table of Contents

|  |  |  |
| --- | --- | --- |
| **Topic** | | **Page**  **No** |
| Table of Content | | 02 |
| Revision History | | 03 |
| 1 | Introduction | 04 - 05 |
|  | 1.1 Purpose of the Project | 04 |
|  | 1.2 Target Beneficiary | 04 |
|  | 1.3 Project Scope | 04 - 05 |
|  | 1.4 References | 05 |
| 2 | Project Description | 05 - 08 |
|  | 2.1 Reference Algorithm | 05 |
|  | 2.2 Data/ Data Structure | 05 |
|  | 2.3 SWOT Analysis | 05 - 06 |
|  | 2.4 Project Features | 06 - 07 |
|  | 2.5 User Classes and Characteristics | 07 |
|  | 2.6 Implementation | 07 |
|  | 2.7 Design and Implementation Constraints | 07 |
|  | 2.8 Design diagrams | 08 |
| 3 | System Requirements | 08 -09 |
|  | 3.1 User Interface | 08 |
|  | 3.2 Software Interface | 08 |
|  | 3.3 Database Interface | 09 |
| 4 | Non-functional Requirements | 09 |
|  | 4.1 Software Quality Attributes | 09 |
| Appendix A: Glossary | | 09 |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Change** | **Reason for Changes** | **Mentor Signature** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

##### INTRODUCTION

* 1. Purpose of the Project

The purpose of the project on detection of forged signatures is to develop a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures. The project aims to leverage machine learning and deep learning techniques to analyze and extract relevant features from signatures and develop a robust algorithm capable of handling large volumes of signatures with minimal errors.

The project also aims to develop a large and diverse dataset of signatures containing both genuine and forged signatures to improve the accuracy and reliability of the algorithm. By achieving these goals, the project aims to have significant implications for fraud prevention and detection in various industries, including finance, legal, and government.

* 1. Target Beneficiary

The target beneficiaries of the project on detection of forged signatures are organizations and individuals who rely on signature verification for security and fraud prevention purposes.

In particular, industries such as finance, legal, and government can benefit from this project, as they often handle large volumes of signed documents and contracts that require accurate and reliable signature verification. By implementing the algorithm developed through this project, these organizations can prevent financial losses, reduce the risk of identity theft, and improve the overall security of their operations.

Individuals who use signatures for identity verification and authentication purposes, such as for accessing bank accounts or making online purchases, can also benefit from the project. The algorithm developed through this project can improve the accuracy and reliability of biometric authentication systems, reducing the risk of identity theft and fraud.

1.3 Project Scope

The project scope for detection of forged signatures may include the following points:

* Developing a dataset: Collecting and developing a diverse dataset of genuine and forged signatures to be used for training and testing the algorithm.
* Signature extraction and pre-processing: Developing a method to extract relevant features from the signature, such as stroke width, pressure, and direction, and pre-processing the signature images to remove noise and distortions.
* Algorithm development: Developing a machine learning or deep learning algorithm that can analyze the extracted features to detect forged signatures accurately and efficiently.
* Performance evaluation: Evaluating the performance of the developed algorithm using standard evaluation metrics such as accuracy, precision, recall, and F1 score.
* Integration with existing systems: Integrating the algorithm with existing signature verification systems, such as biometric authentication systems, to enhance their accuracy and reliability.
* User interface development: Developing a user-friendly interface for the signature verification system to enable easy and efficient use by users.
* Documentation: Preparing documentation of the project, including design documents, user manuals, and technical reports.
* Future work: Identifying future directions for improving the algorithm and making recommendations for further research.
  1. References
     + National Institute of Standards and Technology (NIST) - Signature Verification Competition: https://www.nist.gov/itl/iad/mig/signature-verification-competition-svc-2020
     + IEEE Transactions on Information Forensics and Security: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
     + International Conference on Document Analysis and Recognition (ICDAR): http://icdar2019.org/
     + Springer - Signature Verification: The State of the Art: https://link.springer.com/book/10.1007/978-1-4471-2169-5
     + IEEE Transactions on Biometrics, Behavior, and Identity Science: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424
     + International Journal of Document Analysis and Recognition (IJDAR): https://link.springer.com/journal/10032

##### PROJECT DESCRIPTION

* 1. Reference Algorithm

The project on detection of forged signatures involves the development of a machine learning or deep learning algorithm that can analyze and extract relevant features from signature images to accurately detect forged signatures. The specific algorithm used may vary, but it would typically involve some combination of image processing, feature extraction, and classification techniques.

The data used for the project would consist of a large and diverse dataset of genuine and forged signatures. The dataset would need to be carefully curated to ensure that it includes a wide variety of signatures from different individuals, with varying writing styles, sizes, and shapes. The dataset may also need to include signatures in different contexts, such as on different types of documents or in different languages.

Characteristics of Data

Characteristics of the data may include:

* Signature size: Signatures may vary in size, with some signatures being very small and others being much larger.
* Signature style: Signatures may be written in different styles, with some individuals having very distinctive signatures while others have more generic ones.
* Writing pressure: Signatures may be written with different pressures, which can affect the thickness and consistency of the signature lines.
* Writing speed: Signatures may be written at different speeds, which can affect the shape and consistency of the signature.
* Noise and distortion: Signature images may contain noise and distortions due to scanning or other factors, which can affect the accuracy of the signature verification algorithm.

3. SWOT Analysis

###### Strength:

###### The use of machine learning algorithms provides a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures.

###### The project's focus on developing a large and diverse dataset of signatures will improve the accuracy and reliability of the algorithm.

###### The use of deep learning techniques, such as convolutional neural networks and recurrent neural networks, has shown promising results in detecting and identifying forged signatures.

###### The algorithm's ability to handle large volumes of signatures in real-time processing makes it suitable for implementation in various industries, including finance, legal, and government.

###### Weakness:

###### The success of the algorithm depends on the availability of a large and diverse dataset of signatures containing both genuine and forged signatures.

###### The performance of the algorithm can be affected by variations in writing styles, age of the signature, and the use of different writing instruments or surfaces.

###### The use of advanced deep learning techniques can result in increased computational complexity and training time.

###### Opportunities:

###### The development of a reliable and efficient method for detecting and preventing fraudulent activities involving forged signatures can have significant implications for various industries, including finance, legal, and government.

###### The use of machine learning algorithms for signature verification can be extended to other applications, such as biometric authentication or fraud detection in online transactions.

###### Threats:

###### The prevalence of advanced forms of forgery, such as skilled forgery or disguised forgery, can pose significant challenges to the accuracy and reliability of the algorithm.

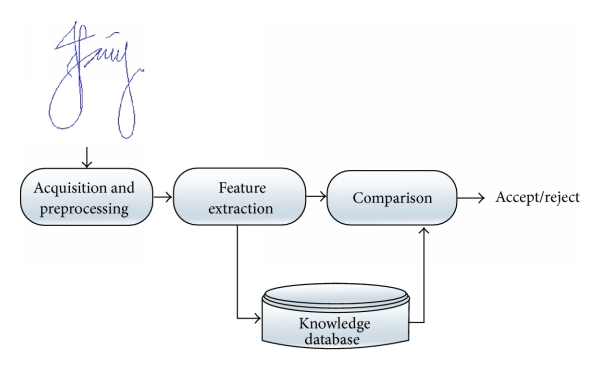
###### The use of adversarial attacks, where malicious actors intentionally modify signatures to evade detection, can also pose a threat to the accuracy of the algorithm.

###### The algorithm's success depends on its integration and adoption by various industries, which may require significant changes in existing signature verification systems and processes.

* 1. Project Features

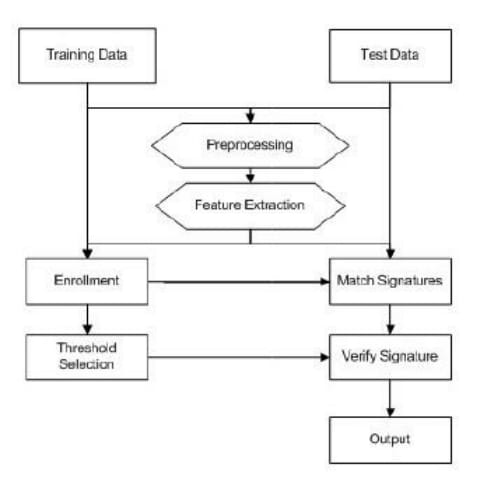
The project on detection of forged signatures aims to develop a signature verification system that can accurately distinguish between genuine and forged signatures. The project involves collecting a diverse dataset of signature images and using machine learning or deep learning algorithms to analyze and extract relevant features from the images. The performance of the algorithm needs to be evaluated using standard evaluation metrics, and the algorithm needs to be integrated with existing signature verification systems to enhance their accuracy and reliability. The project also involves developing a user-friendly interface and documentation of the design, development, and testing of the system.

* 1. Base Diagram



2.6 Implementation

* Collect a dataset of genuine signatures: To develop a forged signature detection system, you need a dataset of genuine signatures that can be used as a reference for comparison.
* Collect a dataset of forged signatures: Collect a dataset of forged signatures that have been identified and confirmed as fraudulent. This will allow you to train the system to identify and differentiate between genuine and forged signatures.
* Preprocess the data: Preprocess the signature images by converting them into a digital format and normalizing them for size, contrast, and orientation.
* Feature extraction: Extract features from the signature images that can be used to identify similarities and differences between genuine and forged signatures. Features can include things like line thickness, pressure, and curvature.
* Choose a machine learning model: Choose a machine learning model that is well-suited for signature detection. Common models include Support Vector Machines (SVM), Random Forest, and Convolutional Neural Networks (CNN).
* Train the model: Train the machine learning model using the preprocessed data and extracted features. Use techniques like cross-validation to evaluate the performance of the model.
* Test the model: Test the performance of the model using a separate dataset of genuine and forged signatures. Measure the accuracy, precision, and recall of the system.
* Deploy the model: Deploy the model in a production environment, such as a mobile app or web service, where it can be used to detect forged signatures.
* Update the model: As new data becomes available, continue to train and update the model to improve its accuracy and performance over time.
  1. Design and Implementation Constraints
* Data availability: The availability of genuine and forged signature data is crucial for the development of the system. A lack of sufficient data can result in a poorly performing model.
* Data quality: The quality of the data used to train and test the system can have a significant impact on its accuracy. Poor quality data can lead to erroneous results and can make it challenging to build a reliable system.
* Hardware constraints: The performance of the system may be affected by the available hardware resources. Depending on the complexity of the model and the size of the data set, a high-performance computer or cloud-based infrastructure may be required.
* Algorithmic complexity: The complexity of the chosen algorithm or model can also impact the performance of the system. Complex algorithms may require more computational resources, which can increase the time required for training and testing.
* Ethical considerations: The use of signature detection systems can raise ethical concerns, such as privacy and security issues. It is essential to ensure that the system is designed and implemented with appropriate safeguards in place to prevent misuse.
  1. Flow Chart



##### SYSTEM REQUIREMENTS

* 1. User Interface

The User Interface needed to run the project is Google Collab with Python 3 with installed in it.

* 1. Software Interface

Linux/Ubuntu/Windows XP /Windows 7 / Windows 10 /Windows 11/Python 3

* 1. Database Interface Excel/Notepad

##### NON-FUNCTIONAL REQUIREMENTS

* 1. Software Quality Attributes
     + Usability: The application will be designed to be user-friendly and easy to use, with intuitive navigation and clear instructions for users.
     + Maintainability: The application will be easy to maintain and update, with clear code organization and documentation.
     + Testability: The application will be designed to be easily testable, with clear test cases and procedures.
     + Portability: The application will be designed to be easily portable across different computing environments, with minimal dependencies on specific hardware or software configuration

Appendix A: Glossary

* + - Signature Verification - The process of comparing an original signature with a purported signature to determine whether they match or not.
    - Forensic Document Examination - The scientific analysis of physical and chemical characteristics of a document to determine its authenticity and/or authorship.
    - Biometric Authentication - The use of unique physical or behavioral characteristics, such as fingerprints, iris scans, or handwriting patterns, to verify a person's identity.
    - Forgery Detection Software - Computer programs designed to analyze digital images of signatures or documents and detect potential signs of forgery or tampering.
    - Handwriting Analysis - The examination of handwriting characteristics, such as stroke pattern, pressure, and spacing, to determine the authorship of a signature or document.
    - SWOT: Strength, Weakness, Opportunities, Threats