Handwritten signature fraud detection system using Python.

Cynthia Chepkoech

146739

CNS

Supervisor Name

James Gikera

Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer Networks and Cybersecurity at the Strathmore University

School of Computing and Engineering Science

Strathmore University

Nairobi, Kenya

May 2023

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student Name: Cynthia Chepkoech

Admission Number: 146739

Student Signature: _____Date: _____

The Proposal of Cynthia Chepkoech has been reviewed and approved by Mr. James Gikera

Supervisor Signature: _____ Date: _____

Acknowledgement

Abstract

Forgery is a common issue in various sectors such as banking and government agencies. A signature can be accepted only if it is from the intended person. It is extremely unlikely that two signatures created by the same person will be identical. Many signature properties may vary even when the same individual signs two documents. As a result, detecting a forgery becomes a challenging task. This project aims to develop a Handwritten Signature Detection Fraud System using Python, which can detect the authenticity of handwritten signatures.

The project will use image processing techniques such as binarization, noise reduction and edge detection. The next step is extracting features from the pre-processed signature images that can be used to train the signature fraud detection. We will use a machine learning algorithm to train the model to distinguish between genuine and forged signatures. We will then evaluate the performance of the model using various metrics such as accuracy and precision. Once the model is trained, it can be used to verify the authenticity of signatures in new documents. The system can take a scanned image of a signature and compare it to the signatures in the trained dataset to determine whether it is genuine or forged. This project's outcome will provide a reliable and efficient solution to detect fraud and prevent potential losses for businesses and organizations.

List of Figures

List of Tables

List of Abbreviations

CHAPTER 1: INTRODUCTION

1.1 Background information

A handwritten signature can be described as the scripted name or legal mark of an individual, executed by hand with the present intention to authenticate a writing in permanent form. It is one of the most common techniques for determining the identity of individuals. The act of signing using a pen or stylus, or other marking instrument remains preserved. Signatures have three main attributes: form, movement, and variation. Movement is the most important aspect since the signatures are produced by moving a pen on a paper. Little variations occur over time once a signature style has been adopted. The signing process can be described at high level as how the brain recovers information from long term memory in which parameters such as size, shape and timing are specified.

Signature verification and forgery detection is the process of verifying signatures to establish whether the signature is genuine or forged. There are two main types of signature verification: static and dynamic. Static, also known as offline verification, is the process of verifying an electronic or paper signature after it has been made while dynamic or online verification takes place as an individual creates the signature on a digital tablet or a similar device. Forgery can be categorized broadly into three types: skilled forgery, unskilled forgery, and random forgery.

(i) Skilled forgery refers to forgeries created by professional impostors or persons who have spent a lot of time practicing and can replicate the actual signatures create the most difficult of all forgeries that looks both accurate and relatively fluent to the naked eye.

(ii) Unskilled forgery refers to when the signer tries to copy the signature in his own style, without having any knowledge of the spelling.

(iii) Random forgery, also known as blind forgery, refers to when the forger has no idea what the signature to be forged looks like. This is the easiest type of forgery to detect since it is usually not close to the appearance of a genuine signature.

Handwritten signature is one of the most widely accepted personal attributes for confirmation with identity whether it may be from banking or business sector. Many organizations still use signatures as their primary method of authenticating a transaction despite the growing digitalization over the past years. Among the essential business operations that require

signatures are the signing of cheques, authorizing documents and contracts and validating of activities. However, the higher the risk of signatures, the higher the risk of signature fraud. Furthermore, this risk is expected to increase as organizations shift from manual to electronic signatures. Therefore, designing an automatic signature system is necessary due to the rising demand for personal identity protection.

1.2 Problem Statement

The act of forgery has existed since the development of writing. In many cases, a person's signature does not represent typical handwriting, nor does it always contain the same individual characteristics. It is often difficult to prove that an actual signature forgery is a forgery in cases of a kind of forgery that may be too skillfully written.

Skilled forgers are competent at imitating the unique features of the genuine signature. They carefully replicate stroke patterns, line thickness, and general appearance to make the forgery resemble the genuine signature. Forgers may create convincing imitations that can be difficult to identify from the original.

According to recent studies, the banking sector accounts for roughly 22% of all signature forging incidents, with counterfeit checks costing an estimated $900 million each year. In most instances, after discovery of the forgery, there is no trace of the forger who, after his success, departs for other fields.

Therefore, these challenges emphasize the need for a system that can distinguish between genuine and forged signatures to avoid the chances of theft and fraud.

1.3 Objectives.

1.3.1 General objectives.

The main aim of this project is to develop a system for detecting whether a signature is genuine or forged.

1.3.2 Specific Objectives.

i. To develop a feature extraction algorithm which can capture the unique characteristics of handwritten signatures.

ii. To build a signature database consisting of genuine signatures from many individuals.
iii. To evaluate and compare different machine learning models for detecting signature frauds.
iv. To review signature verification techniques.
v. To build an interface for practical deployment of the fraud detection system.

1.4 Research questions.

i. How can the unique features of handwritten signatures be effectively extracted and represented as features in Python for accurate verification?
ii. What machine learning methods and algorithms may be used in Python to accurately identify handwritten signatures as genuine or forged?
iii. How can the integration of signature verification techniques improve the performance of the Python-based signature verification system?
iv. What are the main challenges and constraints of handwritten signature verification using Python, and how may they be addressed to improve the efficiency and performance of the system?

1.5 Justification

Signature forgery poses a significant threat to individuals, businesses, and institutions. Developing a system capable of detecting forgeries can mitigate financial losses, prevent identity theft, and improve security in general.

Signatures are an essential method of authentication in a variety of legal and regulatory contexts. Ensuring the integrity of signatures is essential to comply with legal requirements and maintain the validity of contracts, agreements, and official documents. A reliable forgery detection system reduces the risk of conflicts and legal issues while upholding legal and regulatory standards.

Python is a great option for creating a signature fraud detection system because of how simple it is to use and its extensive community support. Python offers a reliable and adaptable environment for implementing machine learning techniques. Its extensive libraries enable efficient feature extraction and dynamic signature analysis.

1.6 Scope and Limitations

The scope of this project is developing a handwritten signature fraud detection system using Python programming language. The system will analyze and compare handwritten signatures present in the database to detect any signs of forgery.

The limitations of the project are:

i. The system's effectiveness may be influenced by the quantity and of training data.
ii. The model may take a long time to train if there are many signatures in the training dataset.
iii. The system may be less accurate when used with signatures that are very small or very large.
iv. The accuracy of the system is dependent on the quality of the input signature images. Low- resolution or poorly scanned images may impact the detection accuracy.