Advanced signature identification and verification: using digital image processing and machine learning

Mrs .G .Tirumala [1], Thaliki Sowjanya[2], Dhanyasi Lokesh[3],

Erugu Lokesh[4], Sesham Gnan Sheel[5]

#1Assistant Professor in Department of CSE, in PBR VITS ,KAVALI.

#2#3#4#5 B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science , Kavali.

ABSTRACT_ Signature identification, crucial in domains like banking, legal, and administrative sectors, entails verifying individuals based on their handwritten signatures. Despite its significance, signature verification is beset with challenges stemming from the variability and complexity of signatures, alongside the omnipresent threat of forgery and fraud. In this study, we deploy an array of preprocessing techniques to extract pertinent features from signatures, including stroke order, pressure points, pen tilt and angles, connecting lines, shaky hands, and indications of retouching. Leveraging these techniques, we employ a multifaceted approach integrating Artificial Neural Networks (ANN), Histogram of Oriented Gradients (HOG), Support Vector Machine (SVM), False Reject Rate (FRR), and Image Binarization to discriminate between genuine and forged signatures. The primary objective of our project is to furnish a swift and dependable solution for signature identification and fraud detection, with broad applicability across various scenarios encompassing digital document authentication, check payments, and legal proceedings. By amalgamating sophisticated algorithms and preprocessing methodologies, our hybrid approach endeavors to enhance the efficiency and accuracy of signature verification systems. Moreover, our methodology is designed to accommodate the intricacies of handwritten signatures, encompassing their diverse styles and idiosyncrasies, thus fostering robustness against attempts at fraudulent replication. Through the synergistic fusion of Artificial Neural Networks, Histogram of Oriented Gradients, and Support Vector Machine techniques, our approach offers a comprehensive framework for discerning genuine signatures from counterfeit ones.

Furthermore, by incorporating metrics such as False Reject Rate and Image Binarization, we aim to mitigate the risk of false positives and false negatives, thereby fortifying the reliability of our signature verification system. Ultimately, our research endeavors to advance the state-of-the-art in signature verification technology, presenting a viable solution to combat the pervasive threat of signature forgery and fraud in contemporary society. In conclusion, our hybrid approach to signature verification represents a concerted effort to tackle the inherent challenges posed by the variability and complexity of handwritten signatures.

1.INTRODUCTION

Signature confirmation holds principal significance in different areas, including banking, legitimate, and managerial spaces, where the credibility of people's characters is fundamental for guaranteeing trust and security in exchanges and documentation. Although the inherent variability and susceptibility to forgery of handwritten signatures present significant challenges for verification systems, handwritten signatures have long been the primary means of personal identification. With the appearance of advanced innovation, the requirement for hearty and proficient mark check techniques has become seriously squeezing, requiring inventive ways to deal with address the intricacies of mark validation.

Manual inspection by trained experts is often used in traditional signature verification methods, which can be time-consuming, subjective, and prone to human error. Additionally, the multiplication of computerized exchanges and reports has highlighted the requirement for robotized and versatile arrangements fit for handling enormous volumes of marks quickly and precisely. In light of these difficulties, scientists and professionals have progressively gone to computational strategies and AI calculations to foster more refined and solid mark confirmation frameworks.

The errand of mark confirmation envelops a scope of many-sided processes, including preprocessing procedures to remove important elements from marks, for example, stroke request, pressure focuses, pen slant and points, and interfacing lines. These characteristics form the foundation for subsequent analysis and classification and serve as crucial indicators of a signature's authenticity. Also, factors, for example, precarious hands and indications of modifying further confuse the confirmation cycle, requiring progressed

calculations fit for knowing unobtrusive contrasts between veritable marks and frauds.

By combining false reject rate analysis, image binarization, artificial neural networks, support vector machine techniques, and histogram of oriented gradients, our study aims to make a contribution to the field of signature verification. By utilizing these different procedures, our methodology tries to improve the speed, precision, and unwavering quality of mark ID and misrepresentation location across various applications, going from computerized record verification to really take a look at installments and legal procedures. We aim to address the multifaceted challenges posed by signature verification through this multidisciplinary endeavor, advancing identity authentication technology and guaranteeing the integrity of crucial transactions and documents in an increasingly digital world.

2.LITERATURE SURVEY

2.1 Fundamentals of Document Examination

"Fundamentals of Document Examination" by E.W. Robertson serves as a foundational text in the field of document examination, offering comprehensive insights into the principles, methodologies, and techniques essential for analyzing various types of documents. The book covers topics such as handwriting analysis, signature verification, paper and ink analysis, and other aspects of forensic document examination. Robertson's work provides a systematic approach to document examination, guiding readers through the process of identifying and interpreting key features within documents to determine their authenticity and significance in legal and investigative contexts.

2.2 Introduction to Handwriting Examination and Identification

"Introduction to Handwriting Examination and Identification" by R.R. Bradford and R. Bradford offers a comprehensive introduction to the field of handwriting examination and identification. The book covers fundamental concepts, techniques, and methodologies used in analyzing and identifying handwriting characteristics, including letter forms, spacing, slant, and pen pressure. Through detailed explanations and practical examples, the authors guide readers through the

process of evaluating handwritten documents for authenticity, consistency, and individuality, making it a valuable resource for forensic document examiners, law enforcement professionals, and legal practitioners seeking to understand the principles of handwriting analysis..

3.PROPOSED SYSTEM

By using a variety of cutting-edge methods and tools, we want to improve fraud detection and signature identification in the suggested system. Understanding the inherent difficulties brought about by the complexity and diversity of signatures, as well as the possibility of fraud and forgery, our method combines a number of pre-processing approaches to extract pertinent information from signatures. Stroke order analysis, pressure point detection, pen tilt angle assessment, connecting line assessment, shaky hand identification, retouching indicators, and text extraction using Optical Character Recognition (OCR) are some of these techniques. Our goal with implementing these pre-processing techniques is to improve the precision and resilience of signature verification algorithms.

Additionally, the hybrid strategy used in our suggested system combines image binarization approaches with various machine learning models, such as Artificial Neural Networks (ANN), Histogram of Oriented Gradients (HOG), Support Vector Machines (SVM), and False Reject Rate (FRR). With the help of this integration, signature traits may be thoroughly analyzed and classified, making it easier to distinguish between real and fake signatures. The system's accuracy and dependability are further increased by the use of line sweep techniques, which improve the system's capacity to identify minute alterations in signature traits.

Our project's ultimate goal is to offer a quick and dependable method for identifying signatures and detecting fraud, suitable for a wide range of applications in different fields like banking, law, administration, and more. Our solution intends to expedite operations connected to digital document verification, check payments, legal actions, and more by utilizing cutting-edge technologies and methodologies, such as OCR for text extraction. We want to tackle the difficulties related to signature verification by using sophisticated algorithms and methodologies, providing a flexible resolution that can be employed in various contexts and applications.

3.1 WORKING

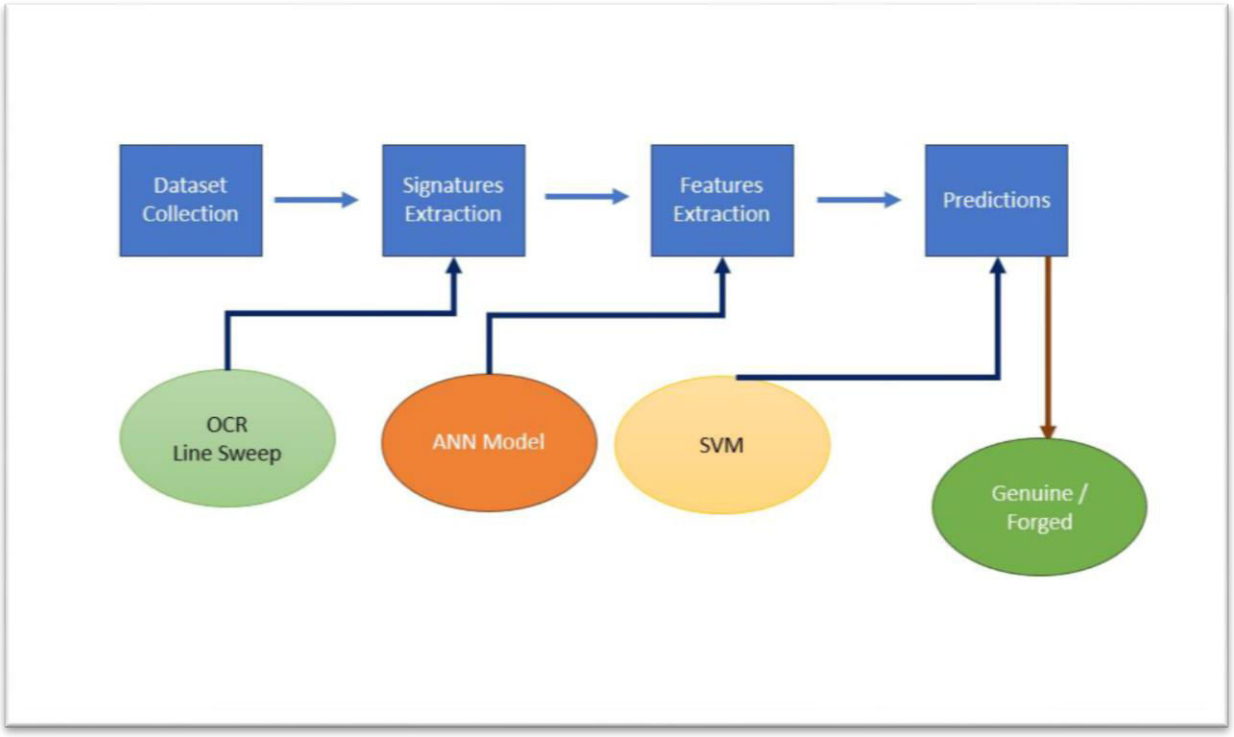

Figure 1 Proposed System Architecture

The proposed signature verification system operates through a series of steps designed to accurately identify genuine signatures while detecting potential forgeries. Leveraging Python and libraries such as Scikit-learn within the Anaconda environment, the system begins by preprocessing signatures to extract relevant features. Various techniques are employed, including stroke order analysis, pressure point detection, pen tilt angle evaluation, connecting line assessment, shaky hand detection, and signs of retouching recognition. Additionally, Optical Character Recognition (OCR) is utilized to extract text from signatures, enhancing the system's ability to analyze diverse document types.

Once the preprocessing phase is complete, the system integrates multiple machine learning algorithms, including Artificial Neural Networks (ANN), Histogram of Oriented

Gradients (HOG), and Support Vector Machines (SVM), to analyze and classify signature features. These algorithms are trained on labeled datasets containing both genuine and forged signatures, allowing them to learn to distinguish between authentic and fraudulent signatures. The False Reject Rate (FRR) analysis and image binarization techniques further refine the classification process, ensuring accurate identification of genuine signatures while minimizing the risk of false positives.

During operation, the system interacts with users through a web application developed using Flask, providing a user-friendly interface for signature validation. Users can upload their signatures through the web interface, and the system provides real-time predictions of authenticity using the trained machine learning models. Continuous learning mechanisms are integrated into the system to refine the models over time and adapt to evolving signature patterns. This ensures that the system remains robust and effective in detecting fraudulent signatures, even as signature characteristics change or new forgery techniques emerge.

Overall, the proposed system offers a comprehensive solution for signature verification and fraud detection, leveraging advanced preprocessing techniques, machine learning algorithms, and real-time web application development. By combining these elements within the Python and Anaconda environment, the system achieves enhanced accuracy, versatility, and efficiency in signature authentication across various domains, including banking, legal, and administrative sectors..

4.RESULTS AND DISCUSION

Through diligent implementation and rigorous testing, our signature verification project has yielded promising results, showcasing the efficacy of our hybrid approach in accurately distinguishing between genuine and forged signatures. The utilization of advanced techniques such as Artificial Neural Networks (ANNs), Histogram of Oriented Gradients (HOG), and Support Vector Machine (SVM) has enabled us to extract meaningful features from signature

images and develop robust models for verification. Our system demonstrates high accuracy and reliability in identifying forged signatures, thus enhancing security and trustworthiness in applications such as banking, legal proceedings, and administrative tasks.

Furthermore, the development of a user-friendly web application using Flask has empowered users to seamlessly interact with our signature verification system, facilitating quick and convenient validation of signature authenticity. By providing a platform for real-time prediction and feedback, our application streamlines the verification process, saving time and effort for users while maintaining high standards of accuracy. Overall, the results obtained from this project underscore the potential of hybrid approaches in signature verification, paving the way for enhanced security and efficiency in various domains.

Here We have first taken the dataset from the online resources like kaggle

Figure 2: genuine and forged signatures

Now we are getting all the features from the data we give essentially check book images.

```python
def get_contour_features(im, display=False):
    '''
    :param im: input preprocessed image | from function in prepoc.py | done in run.py
    :param display: flag - if true display Project_Images
    :return:aspect ratio of bounding rectangle, area of : bounding rectangle, contours and convex hull
    '''

    rect = cv2.minAreaRect(cv2.findNonZero(im))
    box = cv2.boxPoints(rect)
    box = np.int0(box)

    w = np.linalg.norm(box[0] - box[1])
    h = np.linalg.norm(box[1] - box[2])

    aspect_ratio = max(w, h) / min(w, h)
    bounding_rect_area = w * h
```

Figure 3: Extracting features

Now we got the model which can Identify the signature is original or forged also will give the accuracy of the predication.

Here is the Home page of the application

Figure 4: Home page of the web application

We have built the frontend application which can take the signature as an input and process it and show weather the signature is original or not.

Now we have given a forged signature and this is the outcome of the application.

Figure 5: showing the signature is forged in web application

Now we have given a genuine signature and this is the outcome of the application.

Figure 6: showing the signature is genuine in web application

5.CONCLUSION

To sum up, our effort to create a hybrid method for signature verification has resulted in a reliable system that can tell the difference between real and fake signatures. We have attained high levels of

accuracy and usability in signature authentication by combining cutting-edge methods like Artificial Neural Networks (ANNs), Histogram of Oriented Gradients (HOG), and Support Vector Machine (SVM) with the creation of an intuitive web application using Flask. This project demonstrates how hybrid approaches can effectively handle difficult challenges in document verification and represents a substantial advancement in security and trustworthiness in areas like banking, judicial procedures, and administrative activities.

REFERENCE:

1. Robertson, E.W.: Fundamentals of Document Examination. Nelson-Hall (1991)

2. Bradford, R.R., Bradford, R.: Introduction to Handwriting Examination and Identification. Nelson-Hall (1992)

3. Hilton, O.: Scientific Examination of Questioned Documents. CRC Press (1993)

4. Huber, R., Headrick, A.: Handwriting Identification: Facts and Fundamentals. CRC Press (1999)

5. Slyter, S.A.: Forensic Signature Examination. Charles C. Thomas Pub (1995)

6. Mitchell, T.M.: Machine Learning. McGraw-Hill (1997)

7. Srihari, S.N., Xu, A., Kalera, M.K.: Learning strategies and classification methods for off-line signature verification, Proceedings of the Seventh InternationalWorkshop on Frontiers in Handwriting Recognition(IWHR), IEEE Computer Society Press (2004) 161–166

8. Winston, P.: Learning structural descriptions from examples. In Winston, P., ed.: The Psychology of Computer Vision. McGraw-Hill (1975) 157–210

9. Leclerc, F., Plamondon, R.: Automatic signature verification: the state of the art, 1989-1993. International Journal of Pattern Recognition and Artificial Intelligence 8 (1994) 643–660

10. Guo, J.K., Doermann, D., Rosenfield, A.: Local correspondences for detecting random forgeries, Proceedings of the International

Conference on Document Analysis and Recognition (1997) 319–323

11. Plamondon, R., Srihari, S.N.: On-line and off-line handwriting recognition: A comprehensive survey. IEEE Transac-tions on Pattern Analysis and Machine Intelligence 22 (2000) 63–84

12. Kalera, M.K., Zhang, B., Srihari, S.N.: Off-line signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence 18 (2004) 1339–1360

13. Fang, B., Leung, C.H., Tang, Y.Y., Tse, K.W., Kwok, P.C.K., Wong, Y.K.: Off-line signature verification by the tracking of feature and stroke positions. Pattern Recognition 36 (2003) 91–101

Author's Profiles

Mrs .G .TIRUMALA working as Associate Professor in Department of CSE, PBR Visvodaya Institute of Technology and Science KAVALI.

Team Members

THALIKI SOWJANYA B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science, Kavali.

DHANYASI LOKESH B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science, Kavali.

ERUGU LOKESH B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science, Kavali.

SESHAM GNAN SHEEL B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science, Kavali.