e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

SURVEY REPORT ON FORGERY SIGNATURE DETECTION SYSTEM

T. Arivanantham[*1], Pratiksha Shirsath[*2], Zainab Sayyed[*3], Kiran Potdar[*4], Shubham Sagar[*5]

[*1]Guide, Department Of Computer Engineering, Dr. D. Y. Patil College Of Engineering And Innovation, Varale, Talegaon Dabhade, Pune, Maharashtra, India.

[*2,3,4,5]Student, Department Of Computer Engineering, Dr. D. Y. Patil College Of Engineering And Innovation, Varale, Talegaon Dabhade, Pune, Maharashtra, India.

DOI: https://www.doi.org/10.56726/IRJMETS63632

ABSTRACT

In this review, we present an offline signature forgery detection system utilizing Convolutional Neural Networks (CNN) and Principal Component Analysis (PCA). Handwritten signatures are often forged for fraudulent purposes, necessitating robust detection methods. Our system aims to classify signatures as genuine or forged by extracting key features using CNN, which captures the intricate details of the signature, such as strokes and angles. PCA is applied to reduce the dimensionality of the feature set, ensuring efficient computation without losing critical information. This hybrid approach leverages CNN for its strength in feature extraction and PCA for enhancing the discriminative power of those features. Our model is trained and tested on public datasets, demonstrating significant accuracy improvements over traditional methods, achieving up to 99.7% recognition accuracy. By applying fixed parameter thresholding, our system effectively detects both genuine and random forgeries, minimizing false positives and negatives. This research lays the groundwork for further improvements in forgery detection, proposing a scalable solution for real-world applications.

Keywords: Convolutional Neural Networks, Principal Component Analysis, Feature Extraction, Parameter Thresholding.

I. INTRODUCTION

Signature verification is a critical biometric technique used extensively in legal and financial domains for identity authentication. However, the widespread use of handwritten signatures has led to an increase in forgery attempts, ranging from simple imitations to sophisticated forgeries. Traditional methods for detecting such forgeries rely heavily on manual examination, which is time-consuming and prone to human error. With advancements in machine learning, automated systems using Convolutional Neural Networks (CNN) and Principal Component Analysis (PCA) have proven highly effective in addressing this challenge. CNNs are particularly suited for extracting complex features from signature images, capturing subtle details that differentiate genuine signatures from forged ones. PCA complements this by reducing the dimensionality of the extracted features, thus improving computational efficiency while retaining the most discriminative information. In this paper, we explore an offline signature forgery detection system that integrates CNN and PCA, offering a robust and scalable solution for accurately classifying signatures as genuine or forged. This hybrid approach shows significant promise in overcoming the limitations of traditional methods, enhancing both the accuracy and speed of forgery detection.

II. LITERATURE REVIEW

The field of forgery detection has evolved over the years, with numerous researchers proposing various models and techniques for improving the accuracy of detecting forged signatures.

A. A Signature Recognition Technique with a Powerful Verification Mechanism Based on CNN and PCA

Gibrael Abosamra and Hadi Oqaibi et al. (2024) proposed a system for Forgery detection in signature verification has been a persistent challenge due to the complexity of distinguishing genuine signatures from forgeries, especially in dynamic biometric systems. Recent advances leverage deep learning techniques like Convolutional Neural Networks (CNNs) combined with Principal Component Analysis (PCA) to enhance accuracy in detecting both in-distribution (IND) and out-of-distribution (OOD) forgeries. CNNs, particularly with architectures such as ResNet, serve as feature extractors to capture distinct spatial features from signature

images, while PCA aids in dimensionality reduction, preserving discriminative features critical for classification. Studies show that using distance-based metrics, such as cosine similarity combined with k-nearest neighbors (k-NN), effectively differentiates between genuine and random forgery signatures. By applying a threshold-based approach to determine authenticity based on feature distance metrics, these methods yield high accuracy rates and robust verification capabilities. This technique is tested across various datasets, including SVC2004 and SCUT-MMSIG, demonstrating superior resilience against random forgeries and ensuring minimal false positive and false negative rates.

B. A NOVEL METHOD OF FAKE SIGNATURE DETECTION USING DEEP LEARNING TECHNIQUES

Gaurav Yagvalya, Shreya Rawat, Saumya Gupta, Muskan Srivastava, Ashish Shrivastava et. al. (2024) aims to present Recent advancements in offline signature verification leverage deep learning, particularly Convolutional Neural Networks (CNNs), to enhance the accuracy of forgery detection. Early work explored traditional methods like template matching and statistical feature extraction; however, these approaches struggled with high variability in handwriting styles and sophisticated forgery techniques. Studies now focus on CNNs due to their hierarchical structure, which autonomously learns and extracts intricate features from signature images. For instance, research on CNN architectures has shown promising results, with models trained on diverse datasets exhibiting high accuracy in distinguishing genuine signatures from forgeries. Some approaches incorporate fine-tuned transfer learning or fusion techniques, as demonstrated in systems like Deep Signature, which achieved robust performance in offline signature verification tasks. Other studies employ self-supervised learning for writer-independent verification, addressing the challenge of generalization across different writing styles. These CNN-based methods offer adaptability, efficiency, and scalability, underscoring their suitability for real-time applications in digital transactions and document verification systems.

C. SIGNATURE VERIFICATION AND FORGERY DETECTION SYSTEM

Navya V K, Abhilasha Sarkar, Aditi Viswanath, Akshita Koul, Amipra Srivastava et al. (2023) proposed a system **for** Forgery detection in signature verification has been an area of intensive research due to its relevance in fields such as banking, legal documentation, and identity verification. Recent advancements focus on combining deep learning techniques, particularly Convolutional Neural Networks (CNNs), with feature extraction and dimensionality reduction methods like Principal Component Analysis (PCA) to enhance detection accuracy. CNNs are widely employed to identify distinct characteristics in both genuine and forged signatures by analyzing local and global features. This approach allows systems to capture signature-specific patterns, such as stroke direction, pressure, and geometric structure. Various studies have also explored using Siamese networks and support vector machines (SVMs) for comparison of signature features, while others utilize machine learning and OCR to assess signatures in real-time applications. Researchers highlight that incorporating hybrid methods, such as CNNs with feature-level fusion and distance-based metrics, further improves accuracy in forgery detection, as these models can analyze signature nuances effectively. The use of CNNs and PCA together shows promise for reliable and computationally efficient signature verification systems, achieving significant accuracy on datasets like CEDAR and yielding high reliability in detecting even skilled forgeries.

D. FAKE SIGNATURE DETECTION USING NEURAL NETWORKS

Ashish Kumar Srivastava, Dr. Tauseef Ahmad, Jay Chand et. al. (2023) proposed a system for Forgery detection in handwritten signatures, especially in offline systems, has advanced through varied techniques focusing on feature extraction and classification. Early methods included Hidden Markov Models (HMMs), which leveraged probabilistic matching for dynamic signature analysis, yielding an 18.4% error rate under certain conditions. Neural networks, on the other hand, have gained prominence due to their flexibility in recognizing complex patterns in static images, achieving up to 91% accuracy in some studies. Template matching has also been explored, where contour similarities between genuine and test signatures inform forgery detection, achieving moderate success rates but often requiring extensive datasets for reliability. Statistical approaches analyze signature pixel distributions, using correlation coefficients to differentiate genuine and forged signatures based on predefined metrics. Recently, Support Vector Machines (SVMs) have shown promise by optimizing class separations in high-dimensional feature spaces, particularly when used alongside descriptors like histograms of

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

oriented gradients (HOG). These models collectively highlight ongoing progress in signature verification, though challenges remain in balancing accuracy, computational cost, and adaptability to varied forgery techniques.

E. SIGNATURE FORGERY DETECTION USING MACHINE LEARNING

Ms. Manjula Subramaniam*[1], Teja E*[2], N Arpith Mathew*[3] et al. (2022) proposed a system for Signature forgery detection has become critical in verifying document authenticity, given signatures' extensive use for identification in legal and financial contexts. Recent studies explore both offline and online signature verification methods, leveraging convolutional neural networks (CNNs) for their ability to capture and classify complex features from signature images. CNNs serve as effective feature extractors, identifying forgery-specific traits like pen pressure and stroke hesitations. For offline detection, researchers have utilized CNN architectures, including ResNet, to enhance accuracy by maintaining high-level feature stability during training. In addition, techniques like Principal Component Analysis (PCA) are used for dimensionality reduction, focusing on the most discriminative signature features while reducing computational load. This approach has demonstrated strong performance, with models achieving accuracies as high as 99.7% by training on large, labeled datasets such as CEDAR. Studies continue to optimize these methods, integrating hybrid approaches like Crest-Through for better visual processing and Harris corner detection for geometric analysis, further supporting CNN's robustness in handling signature variability across datasets.

III. METHODOLOGY

We intend to use a Convolutional Neural Network (CNN) and Principal Component Analysis (PCA) to implement the online authentication methods, since all the other online methods cannot properly classify which type of forged signature is it. We will use a dataset each group member's signature stored in it, and then at the time of execution of the system, we will provide input as forged signatures to the system and the system will analyze whether it is genuine or or forged. If forged then, which type of forged signature it is, skilled/unskilled/random. The data we are using will be preprocessed, salt pepper noise removal and slant normalization will be used on the data to remove some noise and straighten the slanted signatures, and we will further preprocess it to fit with our training model and make the signature verification easier to detect signature forgeries using a CNN. We will normalize the signature data while preprocessing, it will help in the feature extraction process. The data is used as training data and a part of it is used as test data. The next step to perform is feature extraction, it is a dimensionality reduction process, and it derives data using the signature images which can be used for processing and train the neural network. Feature Extraction aims to reduce the number of features in a dataset by creating new features from the existing ones. In feature extraction the rich features of the signature are extracted and converted into attributes for training the model. It will basically take the signature images and generates data like angles, curvature, and arc length, etc. of the signature images.

The system integrates Convolutional Neural Networks (CNN) and Principal Component Analysis (PCA) to classify signatures as genuine or forged, with further classification of forgery type into skilled, unskilled, or random. Initially, genuine and forged samples, including different forgery types, are collected from our provided dataset. Preprocessing steps prepare these samples for analysis by converting them to grayscale, removing background noise with Gaussian filtering, and normalizing them to a fixed size for consistency. Feature extraction through CNN captures detailed hierarchical features such as strokes, curves, and textures essential for distinguishing between skilled and unskilled forgery traits. Convolutional layers detect these signature patterns, pooling layers reduce data dimensions while retaining core information, and fully connected layers form comprehensive feature vectors that encapsulate unique characteristics like pressure and flow, vital for recognizing forgery types. To further streamline processing and avoid overfitting, PCA reduces the feature vector dimensions by selecting principal components that capture the most essential details, enabling efficient classification with minimal noise.

In the classification stage, the system uses cosine similarity measurement to assess the closeness between test samples and genuine signatures. A threshold value determines the boundary for genuine or forged classification. If a forgery is detected, additional analysis is applied to identify the type of forgery. Skilled forgeries show minimal deviation from genuine signatures, suggesting carefully replicated patterns, while unskilled forgeries display larger inconsistencies in fundamental traits. Random forgeries exhibit significant

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

deviations, lacking structural similarity to genuine samples. This robust methodology leverages CNN for in-depth feature extraction and PCA for computational efficiency, providing a high-accuracy solution for both signature authenticity verification and forgery type identification, making it suitable for practical applications in digital transactions and security systems.

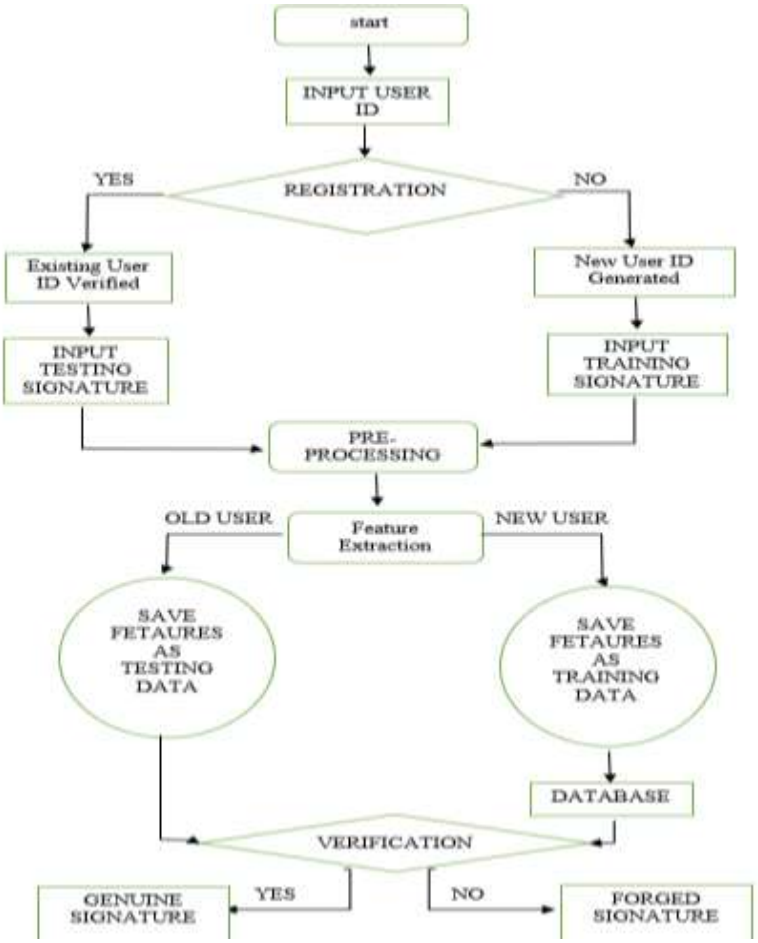

Figure 1: Flow chart of the forgery signature detection system based on CNN and PCA

So, we are going to provide such a system that will be useful in government sectors to identify forged signatures to avoid data duplicity. The fully connected layers of the CNN interpret these features, producing a unique feature vector for each signature. To prevent overfitting and streamline processing, PCA is applied to these feature vectors, retaining only the most informative components. This dimensionality reduction identifies principal components that encapsulate essential signature characteristics. Finally, a classification stage employs cosine distance measurement and thresholding to compare the similarity between test and genuine signatures, effectively distinguishing forged from authentic samples based on a similarity threshold. By combining CNN's robust feature extraction with PCA's efficiency, this system achieves a reliable and computationally feasible solution for forgery detection.

IV. ANALYSIS

In this project, a Convolutional Neural Network (CNN) is employed for feature extraction from signature images, and Principal Component Analysis (PCA) is used for dimensionality reduction. The CNN model is designed with multiple convolutional and pooling layers to capture key features of both genuine and forged signatures. The architecture parameters, such as the number of layers, filters, and kernel sizes, are selected based on experimentation to achieve optimal performance.

Materials used include:

- **Dataset**: Signature datasets like CEDAR or SVC2004, which contain samples of both genuine and forged signatures.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

- **Software and Libraries**: Python programming language, TensorFlow or PyTorch for implementing CNN, and Scikit-Learn for PCA.
- **Hardware**: Training is performed on a system with GPU capabilities to accelerate computation.

CNN Model Architecture: -

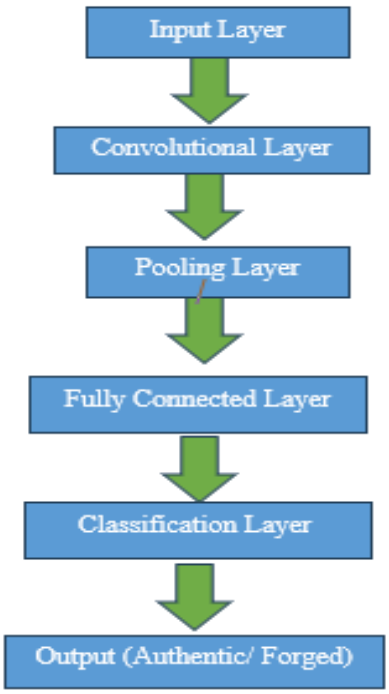

Figure 2: CNN Model Architecture

The CNN model consists of:

- **Input Layer**: Accepts pre-processed grayscale signature images of fixed dimensions.
- **Convolutional Layers**: The CNN applies filters to these images, detecting features like edges, curves, and textures, which are important for recognizing unique patterns in signatures.
- **Pooling Layers**: This layer reduces the size of the image data, keeping the important features while discarding unnecessary details.
- **Fully Connected Layers**: The extracted features are then passed through fully connected layers that help the CNN understand if the signature is genuine or forged.
- **Classification Layer**: This final layer categorizes the signature as either authentic or forged based on the patterns and features learned during training.
- **Output**: Finally, the system predicts whether a signature is real or fake based on the patterns learned during training.

PCA for Dimensionality Reduction: -

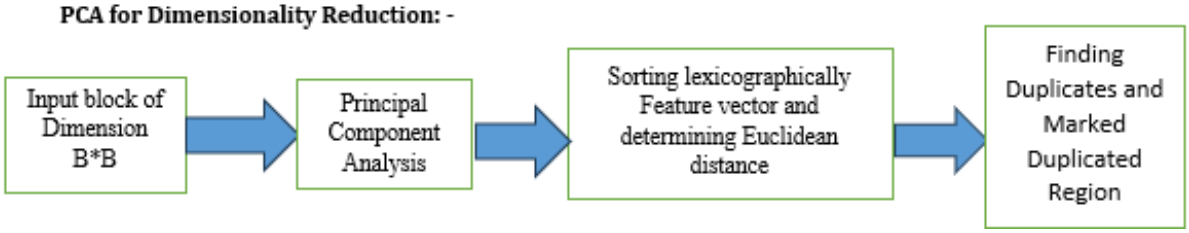

Figure 3: PCA Model Architecture

PCA is applied to the feature vectors produced by the CNN model to reduce their dimensionality, which helps in improving processing efficiency and reducing overfitting. The number of principal components are selected based on the amount of variance needed to retain most of the useful information.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Analysis and Evaluation

The model is analysed based on several performance metrics:

- **Accuracy**: Percentage of correctly classified signatures.
- **False Positive Rate**: Instances where genuine signatures are misclassified as forgeries.
- **False Negative Rate**: Instances where forged signatures are incorrectly classified as genuine.
- **Processing Time**: Time required classifying a single signature image.

The performance of the model is evaluated by training it on a portion of the dataset and testing it on unseen samples. Results are tabulated, showing accuracy and error rates, to demonstrate the effectiveness of the model in forgery detection.

1. Feasibility of the Project

First, the project leverages Convolutional Neural Networks (CNNs), a proven technology for image recognition tasks, which allows for high accuracy in detecting subtle differences between genuine and forged signatures. Coupled with Principal Component Analysis (PCA), the project can efficiently reduce dimensionality and enhance feature extraction, optimizing the training process and improving performance. The availability of datasets for handwritten signatures, alongside accessible tools and libraries such as TensorFlow and OpenCV, ensures that development and implementation are manageable within the academic timeframe. Additionally, the growing relevance of security and authentication solutions in various sectors further underscores the project's potential impact and applicability in real-world scenarios. Overall, the integration of these advanced techniques positions the project as both technically viable and socially relevant.

2. Scope of the Project

The scope of our system encompasses the design, development, and implementation of a reliable and efficient tool for detecting forged signatures. This system is aimed at providing high accuracy in classifying signatures as genuine or forged, with further categorization of forgery types (skilled, unskilled, or random). Leveraging Convolutional Neural Networks (CNN) for feature extraction and Principal Component Analysis (PCA) for dimensionality reduction, the project explores state-of-the-art deep learning methods to optimize processing efficiency without sacrificing performance. The system's scope extends to practical applications across various sectors, including banking for fraud prevention, legal fields for contract verification, and digital services for secure authentication in electronic transactions. A well-defined training pipeline is established to optimize the CNN model's architecture for accurate classification, and the model's effectiveness is rigorously evaluated using metrics such as accuracy, precision, recall, F1-score, and a confusion matrix. Additionally, the project includes a user interface allowing for seamless interaction, where users can upload signatures for verification. Future scalability of the system is also considered, with potential for multi-factor authentication by integrating biometric methods, as well as adaptation for real-time use on mobile or cloud-based platforms. The system includes a user-friendly interface that allows users to upload signature images for verification, with attention to usability for an enhanced user experience. Overall, the project addresses an essential security need, offering a solution with high applicability in both institutional and commercial settings, while contributing valuable insights to the fields of image processing and machine learning.

V. CONCLUSION

In end, the application of Convolutional Neural Networks (CNN) mixed with Principal Component Analysis (PCA) for forgery signature detection represents a effective technique to enhancing protection in signature verification. The CNN excels at learning and extracting complicated features from signature photographs, making an allowance for particular differentiation between genuine and solid signatures. Meanwhile, PCA effectively reduces dimensionality, which no longer most effective hastens processing instances however additionally mitigates the impact of noise and inappropriate versions inside the data.

This hybrid method has tested a marked improvement in detection accuracy as compared to traditional strategies, making it in particular precious in excessive-stakes environments such as banking, legal documentation, and agreement signing. Moreover, the adaptability of CNNs allows for continuous improvement as greater facts turn into to be had, paving the manner for even more state-of the-art detection structures in the

destiny. Further studies should consciousness on refining the model via incorporating larger and more various datasets, exploring advanced neural community architectures, and investigating real time implementation possibilities. The potential of this approach should revolutionize how we authenticate signatures, appreciably

Decreasing fraud and improving accept as true with in signature based totally transactions. Overall, this examines highlights the crucial position of device mastering in preventing forgery and enhancing security features in various domains.

VI. REFERENCES

[1] Gaurav Yagvalya, Shreya Rawat, Saumya Gupta, Muskan Srivastava, Ashish Shrivastava, "A Novel Method of Fake Signature Detection Using Deep Learning Techniques", International Journal of Scientific Research in Engineering and Management, Vol.08, Issue 05, May-2024

[2] Navya V K, Abhilasha Sarkar, Aditi Viswanath, Akshita Koul, Amipra Srivastava, "Signature Verification and Forgery Detection System", International Journal of Creative Research Thoughts, Vol.11, Issue 6, June-2023

[3] Ashish Kumar Srivastava, Dr. Tauseef Ahmad, Jay chand, "Fake Signature Detection Using Neural Networks", International Journal of Engineering Inventions, Vol.12, Issue 9, Sept. 2023, pp 31-28.

[4] Ms. Manjula Subramaniam, Teja E, N Arpith Mathew, "Signature Forgery Detection Using Machine Learning", International Research Journal of Modernization in Engineering Technology and Science, Volume.04, issue 02, Feb. 2022.