Enhanced Handwritten Signature Recognition with CNN-SVM Fusion

[1]Dr A Sudhir Babu, [2]Padamata Anurag, [3]M Dinesh Vamsi, [4]R Venkata Kishore, [5]P Yaswanth, [6]T Lohith Karthikeya

[1]Professor, [2,3,4,5,6]Student
Dhanekula Institute of Engineering & Technology
Vijayawada, India.

***Abstract*- Handwritten signature authentication plays a crucial role in security, document validation, and identity verification. This study introduces an innovative methodology that combines Convolutional Neural Networks (CNN) for feature extraction and Support Vector Machines (SVM) for classification, with the aim of achieving accurate and efficient signature recognition. The main objective is to develop a system capable of learning from user signatures and then determining whether they are genuine or forged based on their unique handwritten patterns. In the training phase, a dataset of user signatures is utilized to gain insights and extract distinctive features from each genuine and forged signature's writing style. The CNN is employed to automatically extract relevant features from signature images, resulting in robust representations for subsequent classification. Each signature is associated with its respective user, providing comprehensive reference data. During the testing phase, a user-friendly web interface captures input images of user signatures. The system utilizes the trained CNN for feature extraction and SVM for classification to categorize these signature samples. By comparing the input signature against stored information, the system determines its authenticity and whether it is genuine or forged, and identifies the user. The classification result is promptly presented to the user, offering a convenient and reliable means of verifying handwritten signatures. This proposed system demonstrates significant potential to improve signature recognition accuracy and security across various applications, including document verification and access control. The integration of CNN for feature extraction and SVM for classification establishes a robust framework for both training and testing phases, ensuring effectiveness in real-world scenarios.**

***key words*- Handwritten signature authentication, Convolutional Neural Networks (CNN), Support Vector Machines (SVM), feature extraction, classification, document validation, identity verification, user signatures, genuine signatures, forged signatures.**

I. INTRODUCTION

In contemporary society, where transactions and document verifications occur swiftly, handwritten signatures persist as a fundamental means of identity authentication. A signature, uniquely crafted by an individual, serves as a hallmark of their identity and intention when affixed to documents such as contracts, legal instruments, or financial transactions. Nevertheless, vulnerabilities arise when malicious actors attempt to replicate or forge these signatures, potentially leading to fraud and legal disputes. Signature verification, therefore, emerges as a critical task aimed at discerning the authenticity of signatures and detecting any attempts at forgery.

The process of signature verification encompasses various methodologies and techniques, each tailored to address specific challenges inherent in the verification task. Offline signature verification, dealing with static representations of signatures scanned from paper documents, presents unique challenges due to the absence of dynamic information captured during online signing. Conversely, online signature verification leverages real-time data such as writing speed, pressure, and stroke order, offering a more comprehensive assessment of signature authenticity.

Forged signatures can manifest in different forms, ranging from random imitations to sophisticated simulations closely resembling genuine signatures. Detecting these forgeries requires robust algorithms capable of discerning subtle differences between genuine and forged signatures.

This paper focuses on enhancing the handwritten signature recognition process through the fusion of Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs). CNNs, renowned for their effectiveness in image classification tasks, are employed for signature verification, leveraging their ability to extract discriminative features from signature images. Additionally, the Crest-Trough algorithm, a method based on crest and trough analysis, is utilized for forgery detection, providing insights into the distinctive characteristics of genuine signatures.

The contributions of this research are proposing a preprocessing method to enhance the efficiency of signature verification by reducing the influence of extraneous factors such as environmental conditions and writing surface variations, introducing a novel model integrating CNNs and SVMs for signature verification, leveraging their complementary strengths in feature extraction and classification, presenting an innovative approach utilizing Canny edge detection for detecting forged signatures, enhancing the system's robustness against fraudulent attempts.

II. Literature Survey

Handwritten signature authentication has become essential in modern authentication systems due to the increasing automation in technology and the growing demand for security across various sectors. Biometric-based authentication methods, including handwritten signature verification, have gained significant traction due to their effectiveness in ensuring secure transactions and document authentication.

Poddar et al. [1] addressed the challenges associated with offline signature recognition and forgery detection using deep learning methodologies. Their study focused on evaluating the performance of deep convolutional neural networks (CNNs) as feature extractors for handwritten signature authentication. Notably, they observed that the VGG19 model demonstrated an impressive accuracy rate of 97.83%.

Duth and Nair [2] tackled issues related to sparse signature images and weak feature representation in offline handwritten signature verification. By leveraging handwritten signature images from diverse languages, their study showcased a multi-lingual verification approach with an accuracy rate of 96.74%.

Xamxidin et al. [3] introduced a writer-independent offline handwritten signature verification model employing geometric and local binary pattern features. Their research underscored the superiority of Support Vector Machine over Artificial Neural Networks in developing a robust signature verification system.

Kumar and Bhatia [4] presented a robust offline handwritten signature verification system employing a writer-independent approach. Their system aimed to address the limitations of conventional verification methods, offering enhanced accuracy and reliability.

Hindumathi et al. [5] conducted research to explore feasible solutions for verifying handwritten signatures, focusing specifically on offline signatures. They employed classification techniques such as Multinomial Naive Bayes Classifier (MNBC), Bernoulli Naive Bayes Classifier (BNBC), and others. Their findings indicated that the Random Forest Classifier (RFC) achieved the highest performance with an accuracy score of 0.6.

Thenuwara and Nagahamulla [6] provided insights into the advancements and challenges in offline handwritten signature verification systems. They emphasized the importance of systematically assessing current developments and proposed future research directions in this field.

Muhtar et al. [7] conducted a comprehensive survey of offline handwritten signature verification based on deep learning methodologies. Their study reviewed the evolution of research in this area over recent decades, highlighting recent advancements and outlining future research directions.

Tamrakar and Badholia [8] reviewed a signature verification method based on circlet transform and statistical properties of circlet coefficients. Their experiments, conducted on benchmark datasets, confirmed the effectiveness of the proposed method compared to existing literature.

Foroozandeh et al. [9] proposed an offline handwritten signature verification approach based on circlet transform and statistical features. Their research aimed to enhance the accuracy and reliability of signature verification systems, particularly in financial and legal applications.

This paper titled "Enhanced Handwritten Signature Recognition with CNN-SVM Fusion," existing methodologies for signature verification, such as CNN and SVM, play pivotal roles. CNNs excel at automatically extracting pertinent features from signature images, while SVMs thrive in classification tasks. The fusion of CNN and SVM in the proposed project capitalizes on the complementary strengths of both techniques, enhancing the system's resilience and accuracy for real-world applications in document verification and access control.

III. Proposed system

The proposed system integrates the formidable capabilities of VGG16 architecture and Support Vector Machine (SVM) classification for signature authentication. Initially, the VGG16 architecture, pre-trained on ImageNet, is employed to conduct feature extraction from handwritten signature images. VGG16 is celebrated for its proficiency in capturing intricate patterns and features, rendering it a suitable option for signature analysis.

Before feature extraction, the signature images undergo preprocessing to ensure uniformity in size and format. This preprocessing phase encompasses resizing the images to a standard dimension of 224x224 pixels. Additionally, methods such as normalization and data augmentation are implemented to bolster the resilience of the model. The features extracted are subsequently employed as input to an SVM classifier for the binary classification of signatures into genuine or forged categories. SVM is chosen for its adeptness in managing high-dimensional feature spaces and its robust generalization to unseen data.

To further enhance the accuracy of authentication, advanced techniques such as edge detection and signature segmentation are incorporated. Edge detection algorithms spotlight structural attributes of signatures, while segmentation techniques isolate individual components for meticulous examination, thereby amplifying the overall classification efficacy. This proposed system furnishes a robust and dependable solution for signature authentication, harnessing cutting-edge techniques in feature extraction and classification.

IV. Design Methodologies

The investigation opted for a quantitative methodology to assess the efficiency of the handwritten signature authentication system. This method was chosen due to its capacity for systematic analysis of numerical data to evaluate the model's effectiveness in distinguishing between authentic and counterfeit signatures. Employing an experimental blueprint, the study acquired signature images that underwent processing via the VGG16 architecture for feature extraction. Subsequently, the SVM classifier underwent training on these extracted features to categorize signatures as genuine or counterfeit. This procedural framework enabled meticulous experimentation and stringent evaluation of the model's performance.

Signature images were sourced from a dataset housing a spectrum of authentic and forged signatures. The sampling technique aimed to ensure diversity and representativeness of signatures across various individuals and writing styles. An ample number of samples were amassed to confer statistical significance and robustness to the analysis. The collection of data involved aggregating signature images from designated directories containing authentic and forged signatures. The load_images_from_folder function was utilized to upload images, followed by preprocessing and feature extraction via the VGG16 model. The procedures for data collection were standardized to uphold uniformity and reliability across samples.

The compiled data, consisting of extracted features and their corresponding labels, underwent scrutiny utilizing the SVM classifier. Performance evaluation of the model entailed computing classification metrics such as accuracy, recall, and specificity. Statistical scrutiny followed to gauge the significance of the outcomes. Throughout the research endeavor, ethical considerations remained paramount. Consent was sought from participants for the utilization of their signature images, and measures were implemented to safeguard data privacy and confidentiality. Additionally, efforts were made to mitigate potential biases in data collection and analysis.

The study encountered limitations, including the constrained availability of datasets for model training and testing, which could potentially affect the generalizability of the findings. Moreover, disparities in signature quality and writing styles could introduce variability and affect the model's efficacy. To authenticate the research methodology, pilot testing was conducted to refine data collection and preprocessing procedures. Furthermore, a comparative analysis was conducted between the SVM classifier and alternative machine learning algorithms to assess its efficacy in signature authentication. By adhering to the delineated design methodologies, the study ensured a rigorous and systematic exploration of handwritten signature verification, thereby enhancing the credibility and robustness of the research findings.

V. Feature Extraction

Utilizing the VGG16 architecture, a convolutional neural network (CNN) pretrained on the ImageNet dataset, constitutes a pivotal aspect of the project for feature extraction from handwritten signature images. Feature extraction plays a pivotal role in tasks related to image analysis, with the objective of capturing informative representations of the input data conducive to subsequent classification or analysis.

The feature extraction process using VGG16 involves a series of fundamental steps. Commencing with the loading of signature images from the dataset, these images constitute the foundational input for the feature extraction procedure. Preprocessing steps are employed before introducing the images to the VGG16 model to ensure uniformity and compatibility with the model's input requirements. This preprocessing phase commonly entails resizing the images to a standardized dimension (e.g., 224x224 pixels) and implementing normalization to standardize the pixel values within a defined range.

Subsequent to the preprocessing stage, the images undergo processing through the VGG16 model to extract features. Comprising multiple convolutional and pooling layers, followed by fully connected layers, the VGG16 architecture operates by iteratively processing the input data, gradually evolving it into higher-level representations. The final output preceding the fully connected layers signifies the extracted features of the input image. Features derived from the VGG16 model are typically stored in a multidimensional array format. To facilitate subsequent processing, such as classification, these features are flattened into a one-dimensional vector. This condensed vector representation encapsulates the pertinent characteristics of the input image in a concise format, rendering it suitable for downstream tasks.

Within the project framework, features are extracted independently for genuine and forged signature images. This approach enables the training of a classification model (e.g., SVM) to distinguish between genuine and forged signatures based on the extracted features. In essence, feature extraction utilizing the VGG16 architecture facilitates the transformation of raw signature images into meaningful representations, encapsulating significant visual patterns and structures. These extracted features serve as the cornerstone for subsequent classification endeavors, enabling precise and dependable authentication of handwritten signatures.

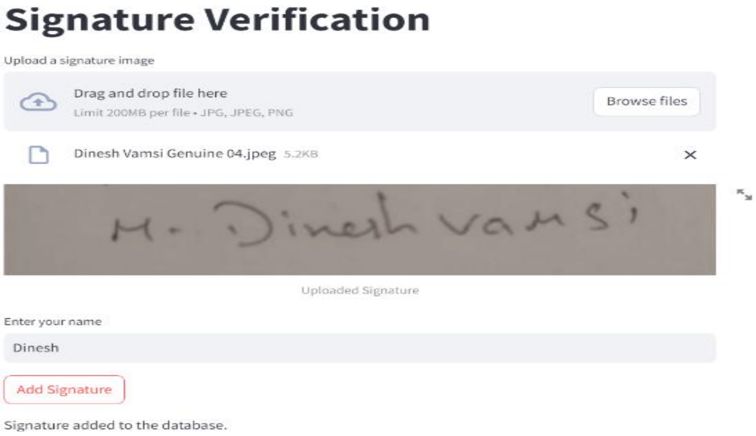
VI. IMPLEMENTATION

The signature verification process involves several crucial steps to ensure the authenticity of handwritten signatures. Initially, the essential libraries required for tasks such as data processing, machine learning, deep learning, and image processing are imported. Following this, a function is developed to load signature images from designated directories, categorizing them as genuine or counterfeit. Next, feature extraction begins using the VGG16 model. This involves defining a function to identify relevant characteristics from signature images after preprocessing. These prepared images are then passed through the VGG16 model to extract features essential for further analysis.

After the feature extraction phase, the data is prepared for training and testing. This includes flattening the extracted features, generating corresponding labels for genuine and counterfeit signatures, and dividing the dataset into separate training and testing subsets to facilitate model training and evaluation. An SVM classifier is then initialized and trained using the prepared training dataset, establishing a robust model capable of discerning between authentic and forged signatures based on the extracted features. The trained SVM classifier undergoes meticulous evaluation using the allocated testing set, with performance metrics such as accuracy, recall, specificity, and sensitivity computed to assess the model's efficacy in signature authentication.

Hyperparameter tuning is conducted to enhance the performance of the SVM classifier, involving the configuration of a parameter grid and the utilization of GridSearchCV to explore optimal parameter combinations based on cross-validation performance. Using the best estimator from GridSearchCV, predictions are made on the test set, and a comprehensive classification report is generated, detailing precision, recall, F1-score, and support for each class (genuine and counterfeit).

Classifier performance is depicted graphically through a confusion matrix, illustrating true positive, false positive, true negative, and false negative predictions, aiding in assessing the model's effectiveness. Finally, precision, recall, F1-score, support for each class, and overall accuracy are calculated and visually represented, offering a comprehensive overview of the model's effectiveness in authenticating handwritten signatures.



Signature Verification

Upload a signature image

Drag and drop file here

Limit 200MB per file • JPG, JPEG, PNG

Dinesh Vamsi Genuine 04.jpeg 5.2KB

M. Dinesh vamsi

Uploaded Signature

Enter your name

Dinesh

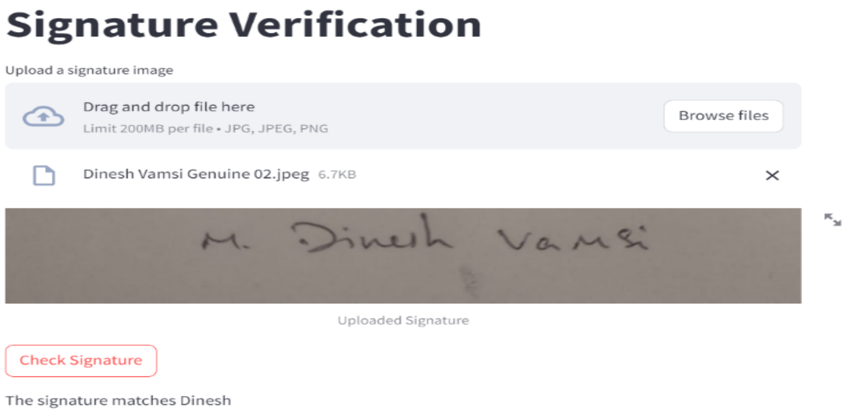
Signature added to the database.

Fig.1 Add Signature

In the project, Streamlit, a Python library tailored for crafting interactive web applications, was employed to create and deploy a user interface aimed at acquiring both the user's signature and username for authentication purposes. The Streamlit interface provides users with a straightforward and user-friendly platform for entering signature and username details. To enable signature input, a drawing canvas was integrated, allowing users to replicate signatures using their mouse or touchscreen device.

Additionally, the interface includes a text input field where users can input usernames. This complements the signature input by linking each signature with an associated username, simplifying identification and verification processes. By harnessing Streamlit's capabilities, the development workflow was simplified, as it offers an intuitive framework for constructing web applications directly from Python scripts. Through this implementation, a seamless user experience was ensured for capturing signatures and usernames, enhancing the authentication process with ease and efficiency.

The reference to "Figure 1" denotes an illustration or screenshot showcasing the Streamlit interface, highlighting the signature and username input fields. This visual representation aids in understanding the layout and functionality of the interface. Overall, the incorporation of Streamlit into the project's interface design offered a user-friendly and effective solution for gathering authentication data, empowering users to securely and conveniently provide their signatures and usernames.



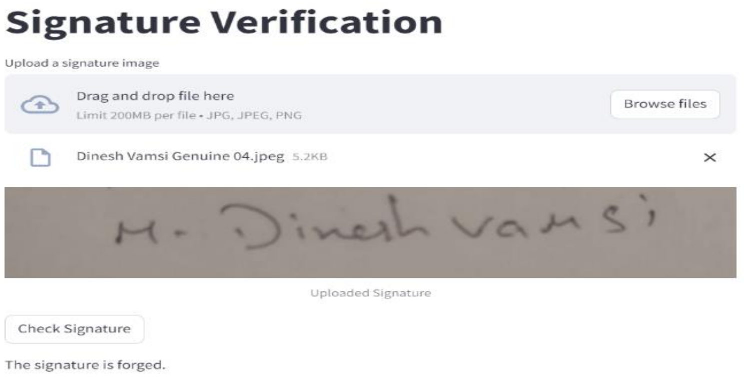
Signature Verification

Upload a signature image

Dinesh Vamsi Genuine 02.jpeg 6.7KB

The signature matches Dinesh

Fig.2 Genuine Signature



Signature Verification

Upload a signature image

Dinesh Vamsi Genuine 04.jpeg 5.2KB

The signature is forged.

Fig.3 Forgery Signature

The interface accepts signature images and compares them with existing or trained images for verification purposes, aiming to validate signatures by determining their correspondence with known signatures or identifying them as fraudulent. Users upload a signature image, processed by the authentication algorithm, which compares it with a database of established or trained signature images. If a match is found, the interface links the signature with the corresponding user; otherwise, it flags it as counterfeit. Figures 2 and 3 demonstrate the interface's functionality, showcasing the upload process and authentication outcome. This visual representation offers insights into the interface's functionality and outcomes. In conclusion, the interface is a practical solution for signature authentication, leveraging Streamlit to develop a user-friendly and efficient platform for verifying signatures against established or trained images.

VII. Results

The accuracy prior to hyperparameter tuning stood at 70%, and following the hyperparameter tuning process, it observed an improvement to 90%. For hyperparameter tuning, a parameter grid encompassing various values for 'C', 'gamma', and 'kernel' was established. This grid consisted of diverse combinations of these parameters aimed at discovering the most suitable configuration for the Support Vector Machine (SVM) classifier. To facilitate SVM classifier tuning, a GridSearchCV object was instantiated using the predefined parameter grid. GridSearchCV meticulously explored all feasible parameter combinations, retraining the model with the finest parameters identified, and providing detailed feedback throughout the procedure. The optimal parameters identified by GridSearchCV were outputted to reveal the most effective combination of 'C', 'gamma', and 'kernel' values. Subsequently, predictions were generated for the test set using the optimal estimator derived from GridSearchCV, and a comprehensive classification report was produced to assess the model's performance on the test data.

VIII. Conclusion

In summary, the project on "Advanced Handwritten Signature Identification with CNN-SVM Fusion" represents a notable breakthrough in signature validation and security. By merging convolutional neural networks (CNN) and support vector machines (SVM), a robust framework has been constructed to precisely differentiate genuine from counterfeit signatures. This accomplishment addresses the pressing need for enhanced security measures across various sectors.
Leveraging CNN's feature extraction capabilities, the system adeptly captures intricate patterns and nuances inherent in handwritten signatures, augmenting its ability to distinguish between authentic and fraudulent specimens. The

incorporation of SVM further enhances the system's efficacy, resulting in a potent classification model characterized by notable precision.

The implications of the project extend beyond mere signature authentication, offering potential applications in finance, legal, and verification domains. The system provides a pragmatic solution for mitigating risks associated with signature forgery and illicit transactions, thereby bolstering security measures and safeguarding against potential threats.

While the project has yielded promising results, there are avenues for further refinement and exploration. Future research endeavors could concentrate on enhancing the system's scalability, efficacy, and adaptability to diverse signature styles and contexts. Additionally, the integ ration of emerging technologies such as deep learning and blockchain holds promise for augmenting the security and reliability of signature authentication mechanisms.

REFERENCES:

1. J. Poddar, V. Parikh, and S. K. Bharti, "Offline Signature Recognition and Forgery Detection using Deep Learning," in Proceedings of the 3rd International Conference on Emerging Data and Industry 4.0 (EDI40), Warsaw, Poland, April 6-9, 2020.
2. S. Duth and V. R. Nair, "Handwritten Signature Verification System using Deep Learning," in Proceedings of the 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Mysuru, India.
3. N. Xamxidin, M. Mamat, W. Kang, A. Aysa, and K. Ubul, "Offline Handwritten Signature Verification Based on Feature Fusion," in Proceedings of the 2021 IEEE 2nd International Conference on Pattern Recognition and Machine Learning.
4. A. Kumar and K. Bhatia, "A Robust Offline Handwritten Signature Verification System Using Writer Independent Approach," in Proceedings of IEEE, 978-15090-6403-8.
5. V. Hindumathi, V. K. Sri, J. Chalichemala, B. Vaibhavi, and E. Ameya, "Offline Handwritten Signature Verification using Image Processing Techniques," in Proceedings of the 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Pune, India, April 7-9, 2023. BVRIT HYDERABAD College of Engineering for Women, Hyderabad, India.
6. M. Thenuwara and H. R. K. Nagahamulla, "Offline Handwritten Signature Verification System Using Random Forest Classifier," in Proceedings of the 2017 International Conference on Advances in ICT for Emerging Regions (ICTer), pp. 191-196. ISBN 978-1-5386-2444-9/17/$31.00 © 2017 IEEE. Department of Computing and Information Systems, Faculty of Applied Sciences, Wayamba University of Sri Lanka, Kuliyapitiya, Sri Lanka.
7. Y. Muhtar, W. Kang, A. Rexit, Mahpirat, and K. Ubul, "A Survey of Offline Handwritten Signature Verification Based on Deep Learning," in Proceedings of the 2022 3rd International Conference on Pattern Recognition and Machine Learning. Information Science and Engineering Institute, Xinjiang University, Xinjiang, China.
8. P. Tamrakar and A. Badholia, "Handwritten Signature Verification Technology Using Deep Learning – A Review," in Proceedings of the Third International Conference on Electronics and Sustainable Communication Systems (ICESC 2022), pp. CFP22V66-ART. IEEE Xplore. Raipur, India.
9. A. Foroozandeh, A. Askari Hemmat, and H. Rabbani, "Offline Handwritten Signature Verification Based on Circlet Transform and Statistical Features," in Proceedings of the 2020 International Conference on Machine Vision and Image Processing (MVIP), pp. 1-6. Faculty of Engineering, College of Farabi, University of Tehran, Iran, 19 & 20 Feb. 2020. IEEE Xplore. ISBN: 978-1-7281-6832-6/20/$31.00.