IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

A Hybrid Method of Feature Extraction for Signature Verification Using Deep Learning

S Karthik, Sheksha Vali P, Rajeswari R P, Shivarama Reddy K, Vinay Kumar K M
Department of Computer Science and Engineering
Rao Bahadur Y Mahabaleswarappa Engineering College, Ballari, India

Abstract: *The offline signature verification system's feature extraction stage is regarded as crucial and has a significant impact on how well these systems perform because the quantity and calibration of the features that are extracted determine how well these systems can distinguish between authentic and fake signatures. In this study, we introduced a method for extracting features from signature images, wherein a Convolutional Neural Network (CNN) is used, followed by the feature selection algorithm (Decision Trees) to identify the key features. Three classifiers were employed to evaluate the efficacy of the hybrid method (long short-term memory, support vector machine, and K-nearest Neighbour). Theseare deemed to be of high significance, particularly given that here they checked skilled forged signatures that are more difficult to recognize the other forms of forged signatures like (simple or opposite).*

Keywords: Convolutional Neural Network

I. INTRODUCTION

Signature verification is a critical aspect of security systems, authentication processes, and legal transactions, where the authenticity of a person's identity is verified through their handwritten signature. Offline signature verification, which involves analyzing static images of signatures, is a challenging yet essential task due to the diversity of individual writing styles and the potential for skilled forgeries. The success of these verification systems heavily relies on the efficacy of the feature extraction stage, as the extracted features determine the system's ability to discriminate between genuine and forged signatures.

In recent years, the advent of deep learning, particularly Convolutional Neural Networks (CNNs), has significantly impacted the field of image analysis and pattern recognition. CNNs excel at learning hierarchical representations from data, making them well-suited for complex tasks such as signature verification. In this context, the integration of deep learning and traditional methods presents a promising approach to enhance the robustness and accuracy of signature verification systems.

In this study, we propose a method for feature extraction in offline signature verification, by using the strengths of CNN. Our approach goes beyond mere integration, incorporating a feature selection algorithm based on Decision Trees to identify crucial features. The fusion of these methods aims to leverage their complementary advantages, capturing both local and global characteristics of signatures. The subsequent evaluation involves employing three diverse classifiers long short-term memory, support vector machine, and K-nearest Neighbour to comprehensively assess the performance and generalization capabilities of our method.

Crucially, the focus of our study extends beyond conventional forgeries to address the challenges posed by skilled forgeries, which are intentionally crafted to deceive signature verification systems. The outcomes of our experiments, conducted on widely-used datasets, demonstrate the effectiveness of the proposed hybrid method in achieving high accuracy rates, thus showcasing its potential for real-world applications where secure and reliable signature verification is paramount.

II. EXISTING SYSTEM

The existing offline signature verification systems predominantly rely on traditional methods for feature extraction. However, these methods often struggle to capture intricate details in skilled forged signatures. The proposed hybrid system augments this by integrating Convolutional Neural Network (CNN), enhancing the system's ability to discern

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

complex patterns. The inclusion of a feature selection algorithm based on Decision Trees further refines the extracted features, resulting in improved accuracy. Experimental evaluations on the Kaggle datasets demonstrate the superior performance of the hybrid method, highlighting its potential to surpass the limitations of existing systems.

III. PROBLEM STATEMENT

Signature verification systems face a critical challenge in achieving accurate discrimination between authentic and forged signatures, as the efficacy of these systems heavily relies on the quality and calibration of extracted features. Existing methods often struggle to handle the intricacies of skilled forged signatures, which pose a more formidable recognition task compared to simpler forms of forgery. To address this issue, this study proposes a hybrid feature extraction method using Convolutional Neural Network (CNN), augmented with a Decision Trees-based feature selection algorithm. The goal is to enhance the system's ability to reliably distinguish between genuine and skilled forged signatures, thereby improving the overall performance of offline signature verification systems.

IV. PROBLEM IDENTIFICATION

The existing offline signature verification systems face a critical challenge in achieving accurate discrimination between authentic and forged signatures. Conventional methods lack the ability to effectively extract features that differentiate skilled forgeries from genuine signatures. This gap hampers the overall performance and reliability of signature verification systems, impacting their applicability in security-sensitive domains. To address this problem, our proposed hybrid feature extraction method integrates Convolutional Neural Networks (CNN), leveraging the strengths of both traditional and deep learning-based approaches. The study aims to enhance the discriminatory power of signature verification systems, particularly when confronted with skilled forged signatures that pose a heightened recognition challenge.

V. RELATED WORK AND MOTIVATION

The collection of features used for the verification model determines its performance. There has been a significant amount of work on offline signature verification, which uses several feature sets to operate the model. Topology, geometric data, gradient, structural data, and concavity bases are the features found in the majority of the works. For instance, an approach using a collection of geometric properties described in the specification of the signature envelope and the patterns of strokes was presented. The hidden Markov model, support vector machines, and Euclidean distance classifier are then used in the verification process.

With the aim of improving signature verification offline. They used a voting-based classifier in addition to a Euclidean classifier to categorize the data. Studies based on characteristics related to curvature, directional run of pixels, pixel surroundings, gray value distribution and pixel surroundings have been a variety of systems have been developed published. Further publications in the literature use graphometric features. To examine upper and lower signature envelopes, here we introduced a shape property termed the chord moment.

Multiple features have frequently been combined to increase the classification accuracy of the models. For instance, minute information and a grey value distribution were employed together with the directional characteristic. The distribution of pixels in the thinned signature strokes was utilized by the authors to create a 16-directional feature. The feature extraction process is expensive because many distinct types of characteristics are involved. With the model being utilized for real-time applications, it is evident that computing moment information coupled with the 16-directional feature is computationally expensive.

We used CNN to improve signature forgery detection, indicating that CNN is more accurate and faster in the detection of forged signatures. Here we used CNN to enhance signature verification and mentioned that using CNN obtained leading with the Kaggle Dataset. In addition, used this module to improve signature verification and forgery detection and confirmed the effectiveness of CNN in detecting forged signatures and developing an offline signature verification system. Additionally, used deep learning algorithms CNN, in addition we also used artificial neural networks to improve offline signature verification systems, and the proposed method used many features.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Based on research, there is still a need to develop an offline signature verification system, as there is a need to improve the dataset quantity and quality to train the model, use more types of algorithms when training the model while including features extracted in different scenarios, and enhance the feature extraction phase considering its significant impact on the performance of the classification stage. Despite the development of several techniques and recognition models, the outcomes of these techniques confirm that there is still much room for improvement in accuracy and robustness. It also has the potential to provide a strong feature set that can enhance the performance of a classifier with minimal complexity. It would be advantageous if the feature set could be readily determined from signature images.

VI. PROPOSED METHOD

The feature extraction method and classification algorithms utilized for the signature verification system are briefly described in this section. The following is the feature extraction technique that recommended signature classification algorithm.

Convolutional Neural Network

Convolutional neural network is the special type of feed forward artificial neural network in which the connectivity between the layers are inspired by the visual cortex. Convolutional Neural Network (CNN) is a class of deep neural networks which is applied for analyzing visual imagery. They have applications in image and video recognition, image classification, natural language processing etc. Convolution is the first layer to extract features from an input image. Convolution preserves the relationship between pixels by learning image features using small squares of input data. It is a mathematical operation that takes two inputs such as image matrix and a filter or kernel. Each input image will be passed through a series of convolution layers with filters (kernels) to produce output feature maps. Here is how exactly the CNNworks.

Basically, the convolutional neural networks have 4 layers that is the convolutional layers, ReLU layer, pooling layer and the fully connected layer.

Convolutional Layer

In convolution layer after the computer reads an image in the form of pixels, then with the help of convolution layers we take a small patch of the images. These images or patches are called the features or the filters. By sending these rough feature matches is roughly the same position in the two images, convolutional layer gets a lot better at seeing similarities than whole image matching scenes. These filters are compared to the new input images if it matches then the image is classified correctly. Here line up the features and the image and then multiply each image, pixel by the corresponding feature pixel, add the pixels up and divide the total number of pixels in the feature. We create a map and put the values of the filter at that corresponding place. Similarly, we will move the feature to every other position of the image and will see how the feature matches that area. Finally, we will get a matrix as an output.

ReLU Layer

ReLU layer is nothing but the rectified linear unit, in this layer we remove every negative value from the filtered images and replaces it with zero. This is done to avoid the values from summing up to zeroes. This is a transform function which activates a node only if the input value is above a certain number while the input is below zero the output will be zero then remove all the negative values from the matrix.

Pooling Layer

In this layer we reduce or shrink the size of the image. Here first we pick a window size, then mention the required stride, then walk your window across your filtered images. Then from each window take the maximum values. This will pool the layers and shrink the size of the image as well as the matrix. The reduced size matrix is given as the input to the fully connected layer.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Fully Connected Layer

We need to stack up all the layers after passing it through the convolutional layer, ReLU layer and the pooling layer. The fully connected layer used for the classification of the input image. These layers need to be repeated if needed unless you get a 2x2 matrix. Then at the end the fully connected layer is used where the actual classification happens.

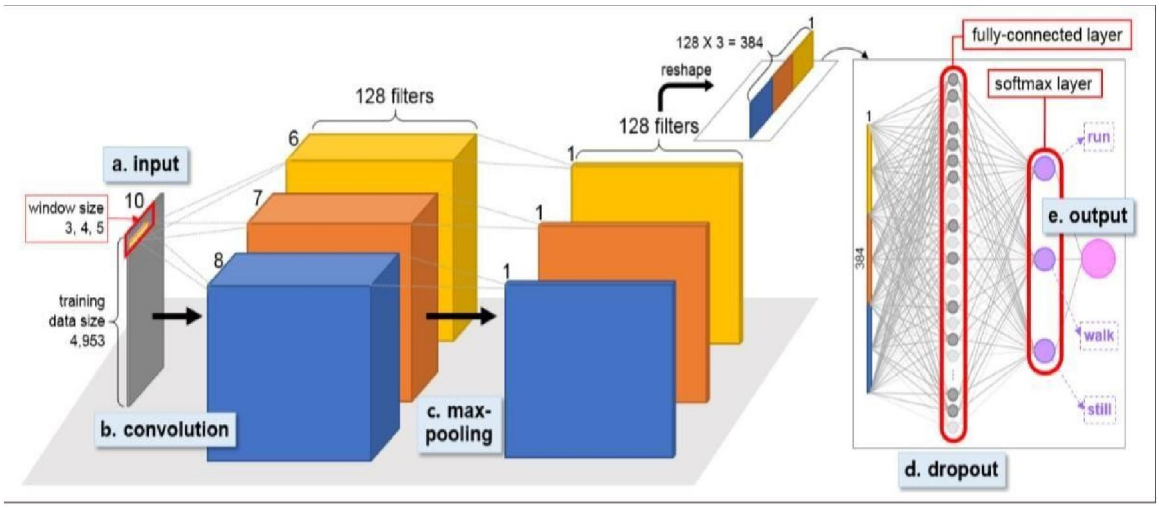

Fig. 1: CNN Architecture

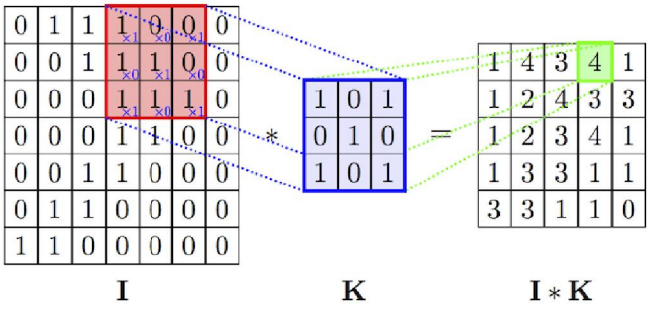

Fig.1.1: Basic Convolutional Operation

Conversion From RGB to Gray scale:

The first step in pre-processing is converting the image from RGB to Greyscale. It can be obtained by applying the below formula to the RGB image. The figure 4.5 depicts the Conversion from RGB to grayscale.

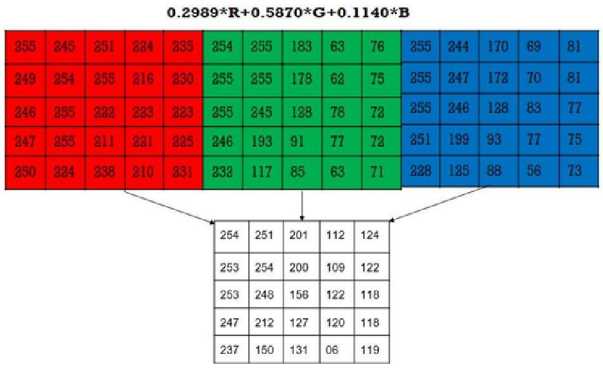

Fig.1.2: Conversion From RGB to Gray scale

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

DATASET

Kaggle hosts various datasets related to signature verification and handwriting recognition tasks.These datasets are commonly used for training and evaluating signature verification systems, which aim to automatically verify the authenticity of signatures. Datasets may be split into training, validation, and testing sets to facilitate model training and evaluation.

Fig.2: Dataset

FLASK

First, set up a Flask application by installing Flask and creating a basic directory structure. Implement user authentication using Flask's built-in features or popular extensions like Flask-Login or Flask-Security. Users will need to log in before accessing the image selection page. Create a page where users can select an image to upload. Train or use a pre-trained machine learning model to classify images as real or fake. Integrate the image classification model into your Flask application. When the user uploads an image, pass it through the model to get predictions. Display the result (real or fake) along with its accuracy to the user.

VII. METHODOLOGY

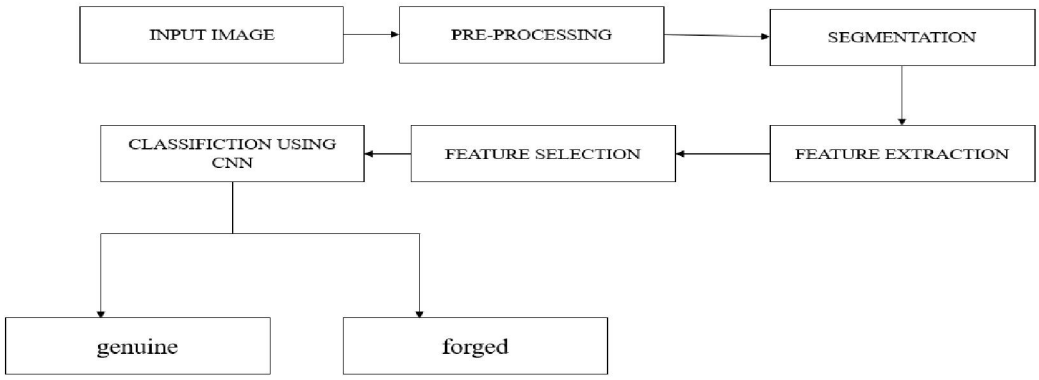

Fig.3: Architecture Diagram

Gather a dataset containing genuine and forged signature images. Preprocess the images to standardize size, enhance contrast, and remove noise. Augment the dataset to increase its size and diversity. Apply random rotations, flips, and slight distortions to simulate real-world variations. Design a CNN architecture tailored for signature forgery detection. Include convolutional layers for feature extraction and dense layers for classification. Train the CNN on the augmented

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

dataset. Utilize a binary classification approach, labelling images as genuine or forged signatures. Extract features from intermediate layers of the trained CNN. These features represent high-level patterns learned by the model. Determine an optimal decision threshold for distinguishing between genuine and forged signatures based on the model's confidence scores. Utilize the trained CNN and the optimized decision threshold to detect forged signatures in new, unseen data. Implement post-processing steps to refine the detection results. This may involve filtering out false positives or applying additional checks. Evaluate the performance of the forgery detection system using metrics such as accuracy, precision, recall, and F1 score. Fine-tune the CNN based on the performance metrics. Adjust hyperparameters or consider transfer learning for further improvement. Deploy the trained model into a production environment for real-world signature forgery detection.

Pre-processing

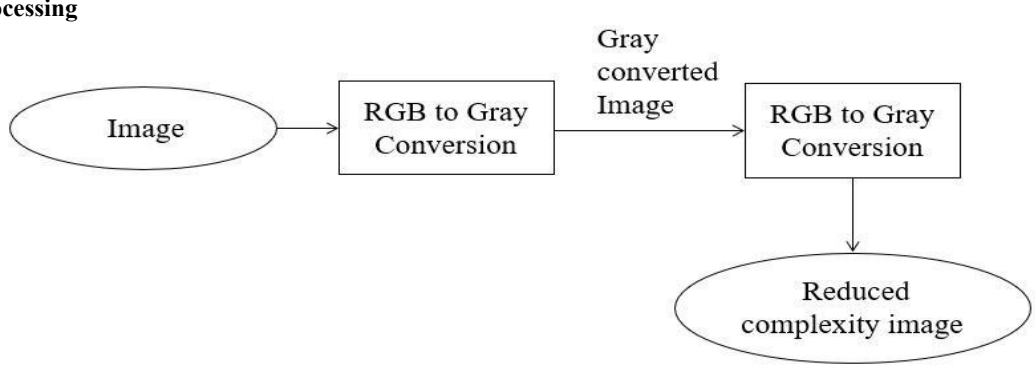

Fig.4: Pre-processing Diagram

Here signature images serve as inputs for the signature forgery model. The pre-processing module prepares input images for subsequent analysis, enhancing the model's efficiency. Converting input medical images from RGB to grayscale for simplified feature extraction. Extracting relevant features from pre-processed images to inform vitamin deficiency Streamlining the feature space to reduce computational complexity and enhance model efficiency.

Identification

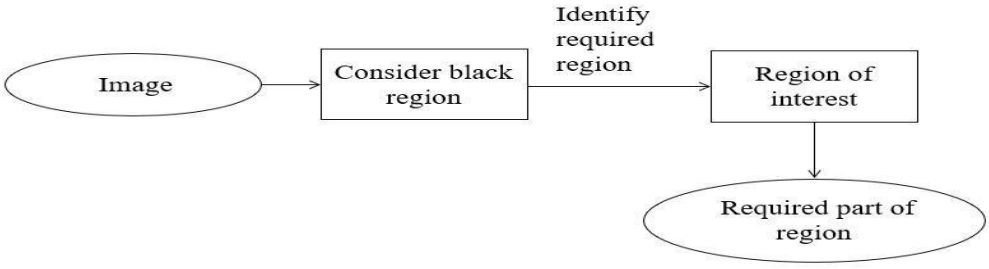

Fig.5: Diagram representing Identification Process

Represents the image or video data that serves as input for the identification system. The central system responsible for the identification process. Identifies the back region within the input data. Determines the required region within the input data based on specific criteria. Identifies the region of interest within the input data. Focuses on identifying specific parts within the identified region based on predefined requirements. Represents the output of the identification system, which includes the identified parts or regions.

Feature Extraction

The process Feature Extraction represents the overall feature extraction procedure. Region of Interest (ROI) signifies the selection of specific regions from the input data or image. Convolutional Neural Network (CNN) Algorithm represents the application of the convolutional neural network for feature extraction. Convolutional Layer involves the application of convolution operations to extract features. Max Pooling Layer performs down-sampling by selecting the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

maximum values from specific regions. Feature Maps represent the output of convolutional and pooling layers. Flattening Matrix converts the 2D feature maps into a one-dimensional array. One-Dimensional Array signifies the final output containing the extracted features in a linear format.

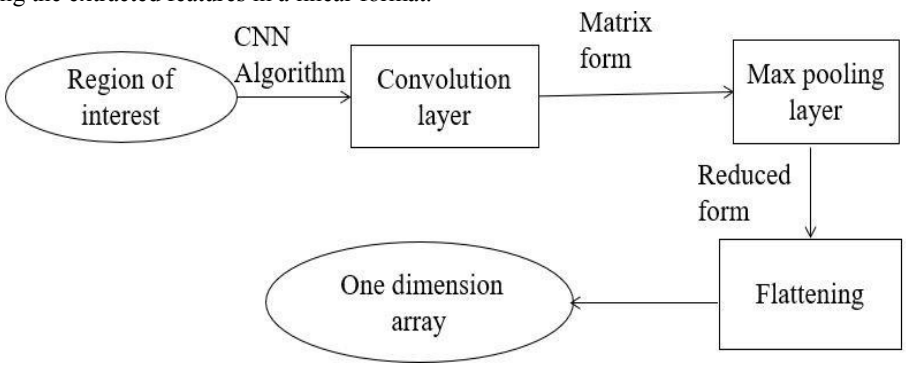

Fig.6: Diagram representing Feature Extraction Process

Classification and Detection

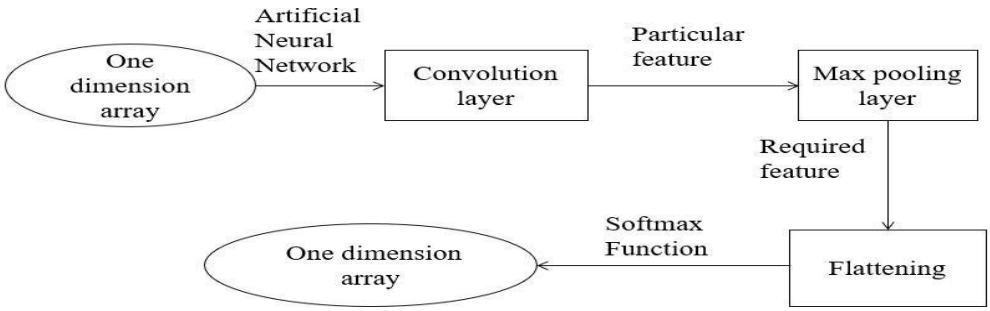

Fig.7: Diagram representing Classification and Detection Process

Initial data includes images and relevant information for classification and detection. The machine learning model trained on historical data for classification and detection. Image enhancement and feature extraction processes to prepare data for the classification and detection algorithms. Execution of algorithms using pre-processed data for classifying and detecting patterns. Data resulting from the algorithms, including enhanced features and metadata. Presentation of the detected and classified results for users and other systems. Final output includes classified labels and detection results.

VIII. FUTURE SCOPE

Enhanced Security Measures: The future could see advancements in the integration of additional security layers within the proposed hybrid method. This could involve incorporating encryption techniques or biometric authentication to further enhance the security of signature verification systems.

Real-time Verification Applications: As technology progresses, there could be a growing demand for real-time signature verification systems, especially in financial transactions, legal documents, and access control systems. Future research could focus on optimizing the proposed hybrid method for real-time processing without compromising accuracy.

Adaptation to Varied Signature Styles: Signatures can vary significantly in style and complexity. Future research may explore techniques to adapt the hybrid feature extraction method to accommodate a wider range of signature styles, including cursive, printed, or stylized signatures.

Robustness to Environmental Variations: Signature verification systems must be robust to environmental variations such as lighting conditions, paper quality, and noise. Future work could focus on developing techniques to improve the robustness of the hybrid method under diverse environmental conditions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Integration with Blockchain Technology: With the increasing adoption of blockchain technology for secure transactions, there could be potential for integrating the proposed hybrid method with blockchain-based signature verification systems. This integration could provide an additional layer of security and immutability to digital.

IX. CONCLUSION

In this work, we presented a new method for extracting features from signature images by selecting the important features in CNN methods, then merging the output of the two methods together, and testing the extracted features. Two classifiers SVM, and KNN) were used. With an accuracy of (95.4%, 95.2%, and 92.7%, respectively) with the dataset, the testing findings showed that our suggested model worked well in terms of performance and predictive capacity, which is regarded as a high value, especially considering that we evaluated sophisticated forgeries, which are more difficult to spot than other kinds of forgeries, such as basic or opposite-hand forgeries, because skillful forgeries are usually very close to the original signatures. Future signature verification performance and prediction capability are anticipated to be improved by refining the feature-extraction process. In this paper, a system that can generate synthetic fingerprints and detect fake fingerprints is proposed. The experiments show that fingerprints generated by the proposed algorithm well capture the nature of real fingerprints. The presentation attack detection algorithm outperforms the existing algorithms in term of accuracy and processing time.

REFERENCES

[1] F. M. Alsuhimat and F. S. Mohamad, ‘‘Offline signature verification using long short-term memory and histogram orientation gradient,’’ Bull. Elect. Eng. Inform., vol. 12, no. 1, pp. 283–292, 2023.
[2] M. Ajij, S. Pratihar, S. R. Nayak, T. Hanne, and D. S. Roy, ‘‘Off-line signature verification using elementary combinations of directional codes from boundary pixels,’’ Neural Comput. Appl., vol. 35, pp. 4939–4956, Mar. 2021, doi: 10.1007/s00521-021-05854-6.
[3] F. E. Batool, M. Attique, M. Sharif, K. Javed, M. Nazir, A. A. Abbasi, Z. Iqbal, and N. Riaz, ‘‘Offline signature verification system: A novel technique of fusion of GLCM and geometric features using SVM,’’ Multimedia Tools Appl., pp. 1–20, Apr. 2020, doi: 10.1007/s11042-020-08851-4.
[4] F. M. Alsuhimat and F. S. Mohamad, ‘‘Histogram orientation gradient for offline signature verification via multiple classifiers,’’ Nveo-Natural Volatiles Essential OILS J., vol. 8, no. 6, pp. 3895–3903, 2021.
[5] N. M. Tahir, N. Adam, U. I. Bature, K. A. Abubakar, and I. Gambo, ‘‘Offline handwritten signature verification system: Artificial neural network approach,’’ Int. J. Intell. Syst. Appl., vol. 1, no. 1, pp. 45–57, 2021.
[6] A. B. Jagtap, D. D. Sawat, R. S. Hegadi, and R. S. Hegadi, ‘‘Verification of genuine and forged offline signatures using Siamese neural network (SNN),’’ Multimedia Tools Appl., vol. 79, nos. 47–48, pp. 35109–35123, Dec. 2020.
[7] B. Kiran, S. Naz, and A. Rehman, ‘‘Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities,’’ Multimedia Tools Appl., vol. 79, no. 1, pp. 289–340, 2020.
[8] M. Sharif, M. A. Khan, M. Faisal, M. Yasmin, and S. L. Fernandes, ‘‘A framework for offline signature verification system: Best features selection approach,’’ Pattern Recognit. Lett., vol. 139, pp. 50–59, Nov. 2020.
[9] N. Sharma, S. Gupta, and P. Metha, ‘‘A comprehensive study on offline signature verification,’’ in Proc. J. Phys., Conf., 2021, Art. no. 012044, doi: 10.1088/1742-6596/1969/1/012044.
[10] H. H. Kao and C. Y. Wen, ‘‘An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach,’’ Appl. Sci., vol. 10, no. 1, p. 3716, 2020