IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advanced Hybrid Feature Extraction Techniques for Signature Authentication

R Rajkumar, R Shravan, V Nagabhuchchayya Chowdry

U.G. Student, Department of CSE, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

Associate Professor, Department of CSE, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

ABSTRACT: The feature Obtainment stage of offline systems for authentication of signatures is considered critical and significantly affects performance of these systems. The quantity and calibration of the extracted features determine the systems' ability to differentiate between real and fake signatures. Using a combination of Convolutional Neural Network and a Histogram of Oriented Gradients (HOG), feature selection technique (Decision Trees) to isolate critical characteristics, we devised a advanced approach to attribute elicitation from signature photos in this research. At last, we integrated the CNN and HOG approaches. Long short-term memory, support vector machine, and K-nearest Neighbor were three classifiers used for assessing the hybrid method's effectiveness. Based on the outcomes of the experiments, our proposed model performed adequately when tested on the CEDAR dataset, both efficiency and predictive power. Given that we verified expertly fabricated signatures, which are harder to come by than other kinds of forgeries, including (simple or opposite), this precision is considered to be of great importance. We achieved a perfect score of 100 for improved signature verification using the project's additions, which include an Exception, Feature Obtainment method (HOG-RFE), and a Voting Classifier for Dataset analysis. Using CNN & HOG Multi-Classification Approach. To guarantee practical usability in cybersecurity apps, a user-friendly Flask framework with SQLite integration makes registration and sign in for user testing a breeze. Search terms: deep learning, offline signature verification, CNN, and HOG.

I. INTRODUCTION

Biometrics represents the utmost significant technology approach for identifying persons and assessing their power based on physiological and behavioral traits. The biological category includes measurements of features like ears, fingerprints, iris, DNA, whereas the conduct category includes features like expression, voice, stride, and signature, and uses them to identify people. Among the most commonly employed biometric authentication globally is the handwritten signature [1]. As a distinct behavioral biometric, handwritten signatures are used in financial papers, passports, credit cards, banking, and check processing. Particularly they not legible, these signatures are a pain to authenticate. Consequently, to minimize the likelihood of fraud or theft, a system is required to differentiate between a real signature and a false one. While there is many study in this area over the last 30 years, covering everything from expert opinion-based verification for ML algorithms and, more recently, DLalgorithms, there is still a great deal of room for improvement in offline signature verification systems[2]. Web-based methods accessible for automated signature verification [3, 4, 5, 6, 7], whereas offline approaches are available [8, 9, 10]. In the absence of pen-tip pressure, velocity, and acceleration, which are accessible when using online signature photos, old study have demonstrated that offline signature verification is more harder than online verification [1, 2, 8, 10].

The online method is also not applicable in some contexts because of the specific processes involved in collecting Signatures. Despite signature verification's reputation as the most lenient biometric method, many research finding indicate that it is not a walk in the park. This is because signatures include special characters and symbols that aren't always easy to read, and signer behaviors can vary greatly. Focus on developing a reliable signature system based on real-world scenarios, and examine the signature as a whole rather than breaking it down into its individual letters or phrases.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE.SURVEY

Organizations take the signing procedure very seriously to protect their data from illegal access and to guarantee its confidentiality. A typical approach for human verification using biometric characteristics, study of paper-based handwritten signatures has increased in prominence during the previous decade [1]. The difficulty the strength of this method stems from the fact that no two people can ever sign the same thing precisely identical way, which makes it exceedingly difficult to implement. In addition, we are curious in the dataset's characteristics that may impact the model's efficiency; specifically, we want to know what characteristics to extract from the signature photos using the HOG method. Using the UTSig and CEDAR datasets as input, we proposed an LSTM neural network architecture signature authentication in this research. The prediction power of our model is very remarkable: While CEDAR's LSTM ran for 2.98 seconds, UTSig's ran for 1.67 seconds, and both achieved 87.7 percent accuracy in classification. In comparison to previous methods for validating paperbased signatures, our suggested technique achieves higher accuracy, surpassing those of K-nearest neighbor, svm , convolution neural network, speededup robust features, and Harris [10]. firmly and accurately confirming the legitimacy of formal documents, including bonds, contract forms, bank checks, and certificates, is still tough issue. If the signatures on the papers match the original signatures of the authorized individual, then it may be said that documents are authentic.

It is believed that signatures signatures of authorized individuals are known in advance. [2] This study presents a new set of feature for signature authentication that are grounded on the quasistraightness of border pixel runs. After obtaining the feature set from different classes of quasi-straight lines, we use elementary combinations of the directional codes from the signature border pixels to extract the segments of these lines. A strong feature set for signature authentication is created by the quasistraight line segments, which combine straightness with tiny curvatures. Utilizing SVM for classification, we have shown efficacy on industry- standard signature datasets such as CEDAR and GPDS100.

The results prove that suggested approach is superior to the current gold standard. An important challenge in biometrics is the authentication of identity via authenticity evaluation of handwritten signatures. Considering the dynamics of the signing process, there are multiple effective methods for verifying signatures. Among them, techniques founded on partitioning are quite significant. [5] Our research introduces a new approach for signature partitioning. To enhance the precision of test signature analysis, its most valuable feature is ability to choose and analyze hybrid partitions. The signature's vertical and horizontal axes work together to create partitions. The three vertical parts represent the beginning, middle, and end of the signature procedure. Also, on a graphics tablet, the signature regions for high and low pen pressure and velocity are on the horizontal parts. the three, four This paper's method relies on our earlier work on the dynamic signature's vertical and horizontal parts, which were developed separately. Among other things, section selection lets us specify the partition consistency of signing process, which in turn promotes more stable signature regions. The method was evaluated using two databases: the openly accessible MCYT-100 and the paid Bio Secure.

III. METHODOLOGY

i) Proposed Work: To extract characteristics from signature photos the proposed approach use a hybrid technique. It incorporates the powerful methods convolutional neural networks and histogram of oriented gradients, both of which excel in capturing gradient information and intricate patterns. Feature extraction is followed by the use of DT to prioritize the features. By eliminating extraneous data and improving classification accuracy, this approach produces a feature vector that includes just the most important parts, making it more efficient for classification tasks, particularly in signature recognition. We achieved a perfect score of 100 for improved signature authentication using the project's other components, which include an Exception, a feature extraction method (HOG-RFE), and a voting classifier for dataset analysis. To guarantee practical usability in cybersecurity apps, a user-friendly Flask framework with SQLite integration makes registration and sign in for user testing a breeze.

ii) Network Design: " Advanced Hybrid Feature Obtainment Techniques for Signature Authentication" is the name of the project. design of system is multi-stage, and it uses convolutional neural networks (CNNs) and hidden Markov models (HOGs) for classification. The procedure starts with training set signature image preprocessing, and then uses a CNN along with HOG hybrid method to extract features. Various classifiers, such as SVM, KNN, LSTM, and a Voting

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Classifier, are trained using the collected features [2]. Also included in the extension are Voting Classifier, HOG- RFE, and Exception. To ensure a strong and accurate multi-classification approach for signature authentication, the testing phase involves preprocessing and feature extraction of signature photographs before they are tested against the knowledge base. The verification process uses the diverse classifiers and the knowledge based to differentiate between real and fake signature. This section provides a concise description of the feature extraction approach and classification algorithms utilized by the signature verification system. This signature classification approach is suggested for use with the following two attribute derivation methods and three classifiers.

This research used the HOG method to extract features from signature photos. Dalal and Triggs first proposed traitshape representation at the 2005 CVPR conference, and HOG for implement it. One common use of Histograms of Oriented Gradients (HOG) is in person detection. To identify and recognizing trademark photos, this research used HOG as a feature extraction methodology either alone or conjunction with the CNN method.

iii) Collecting datasets: We investigate the CEDAR and UTSig databases to learn about their layout, characteristics, and contents. At this stage, we import the datasets, analyze the statistics, visualize the samples, and learn about the spread of real and fake signatures.

iv) Image Processing: When it comes to autonomous driving systems, object identification relies heavily on image processing, which involves several critical phases. The initial action is to optimize the input picture for analyzing and modification by turning it into a blob object. Subsequently, the following action is to specify which object classes the algorithm ought to search for by defining their classes. In similar breath, bounding boxes are defined, defining the areas of the picture that are of interest and where objects are suppose to be. An essential step for efficient numerical computing and analysis is the transformation of the processed data into a NumPy array. Subsequently, the following action is to load a pretrained model that makes use of previous information from large datasets. To do this, it is essential to read the pre-trained model's network layers, which include the parameters and learnt feature are vital for precise object identification. Furthermore, the extraction of output layers allows for successful object discrimination and categorization and provides final predictions. Additionally, the picture and annotation file are attached in the image processing pipeline, guaranteeing thorough information for the next analysis. A mask is made to emphasize important characteristics, and the color space is changed by changing it from BGR to RGB. The final step involves reduce the image's size so can be better processed and analyzed. This all-encompassing image processing workflow lays the groundwork for reliable object recognition in the ever-changing environment of autonomous driving systems, which improves road safety and decision-making capacities.

v) Feature Extraction: This ML method enables us to decrease the quantity of processing resources required without sacrificing any vital or relevant information. To handle data efficiently, it is important to reduce its dimension, and feature obtainment helps with that. To rephrase, feature extraction is the process of developing improved feature from source data while retaining all of the relevant information.

Data having many characteristics, some of that may be superfluous or unimportant, is typical while dealing with big dataset, particularly in fields such as signal processing, image processing, or natural language processing. Algorithms may function more efficiently and quickly after feature extraction simplifies the data. • Lowering the Computational Cost: ML models can function more rapidly with reduced data dimensionality. When handling complicated algorithms or massive datasets, this becomes even more crucial. • Enhanced Efficiency: Less features usually means higher performance for algorithms. Because extraneous information is filtered out, the algorithm is able to pinpoint the crucial parts of the data. For models to have the ability to generalize well to new, unknown data, it is essential to mitigate overfitting, which occur when there are too many features. This is something that feature extraction may help you avoid by making the model simpler. • Deeper Data Understanding: By identifying and highlighting key elements, we might obtain a better grasp of the processes that created the data.

vi) Algorithms: CNN, a DL architecture, is utilized for automatically and hierarchically learn features from signature photos, allowing the design to capture variations and complicated patterns. The hybrid technique takes use of both approaches' capabilities by combining them with HOG, which is great at capturing local gradient information. This complementary set of features renders the system into powerful tool for authentication and verification by increasing

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

the precision, pace of signature verification and facilitating the efficient classification of signaturesacross various classes.

Support Vector Machine (SVM) is a type of supervised learning technique applicable to both classification, regression tasks. Using the characteristics acquired from CNN and HOG, SVM, can be utilized to signature verification to categorize signatures into multiple groups. With SVM, a decision boundary is found whose margin between classes' characteristics is maximized.

LSTM is a different kind RNN designed for modeling sequential data. For this project, LSTM can be utilized for process time-series data pertaining to signatures or feature extractions from CNN and HOG.

In context of sequential signature data, can detect on patterns and long-term dependencies, which helps with signature verification.

Exception is an framework for DL that use depth wise separable convolutions to classify images. To achieve integrate spatial information across channels, this invention uses a 1x1 convolution after conducting depth wise convolutions on each input channel. By using this route, Exception is able to reduce computing complexity without sacrificing accuracy, making it more parameter-efficient than conventional systems. In particular, Exception has done quite well in machine vision tasks that call on the obtainment of hierarchical features from raw data.

For the goal of making predictions, a Voting Classifier integrates several machine learning models. Random Forest (RF) integrates multiple Decision Trees (DT) part of an ensemble learning strategy. By building several decision trees and aggregating their predictions, Random Forest enhances prediction accuracy. For categorization purposes, decision trees are useful since they resemble trees. To enhance the model's overall prediction accuracy and resilience, the Voting Classifier combines RF and DT via a voting mechanism.

IV. EXPERIMENTAL RESULTS

Precision: The accuracy rate, or precision, is the percentage of correct hits relative to overall count of occurrences or samples. Consequently, the following is the formula for determining the accuracy.

Recall: The capacity of a framework to detect all significant occurrences of a given class is measured by recall, a statistic in machine learning. The completeness of a design in capturing instances of a particular class is shown by ratio of properly predicted positive observations to total actual positives.

Accuracy: To gauge how well a model performs in general, we may look at its accuracy, which is defined as proportion of right predictions in a classification test.

F1 Score: The F1 Score is suitable for correcting imbalanced dataset as it balances the regard of both false positives and false negatives. It is computed as the harmonic average of precision and recall.

V. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

i. EXISTING SYSTEM A small number of geometric properties are the basis of the method outlined in the old literature. These qualities could be discriminating, but they might miss certain key detail that are requierd for strong signature verification. If system included more complicated or texture-based elements, it may work better. For a signature verification system to work, the preprocessing phase that separates components and gets rid of noise must be of high quality. The feature extraction process's accuracy and dependability might be compromised if the preprocessing step isn't strong enough or doesn't account for all kinds of fluctuation or noise. When presented with fresh signatures or signatures from various persons, the prototype-based authentication mechanism is might not be able to generalize well.

ii. ALTERNATIVE MODEL SETS

The hybrid model may potentially enhance performance by combining its robust feature set with a low complication classifier. The significance of the hybrid strategy utilization.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

for feature obtainment may be further confirmed by using three DL and ML classifiers. Efficiently Extracting Features: CNNs can learn hierarchical features from unprocessed picture input, while HOG features pick up on local gradient details. More complete feature representations are produced by combining global and local signature qualities in this way. The study's main goal is for determine most discriminative characteristics for classification by using characteristics selection techniques that use decision trees. This method can improve precision.

VI. FUTURE SCOPE

The feature obtainment process, a crucial step in signature verification. By enhancing this process, you aim to better capture the unique characteristics of signatures, making the verification system more accurate and reliable. Refining the feature obtainment stage is expected to improve general effectiveness of signature verification system. This includes increasing accuracy, reducing false positives/negatives, and enhancing the system's ability to predict whether a given signature is real or forged. Adapting the signature verification system for multiple applications such as mobile authentication and e-signatures expands its practical utility. This diversification can cater to a broader range of needs, making the technology applicable in various secure access points. Refining the user interface ensures that the system is user-friendly and accessible, which is essential for wider adoption. Real-time inference is crucial for applications like banking transactions and security access points. Optimizing the system to provide quick and accurate results in real-time scenarios ensures practical deployment in environments where timely verification is essential for security and efficiency.

VII. CONCLUSION

Effective signature verification is the goal of this investigation, which presents a advanced approach that uses CNN and HOG. To obtain the combined feature obtainment way and guarantee its efficacy and accuracy, DT is used. A variety of feature sets collected from CNN, HOG, and Exception are utilized fortraining the models, showcasing how versatile the suggested technique is. In terms of successfully categorizing signatures using the collected features, the selected classifiers—Support Vector Machine, KNearest Neighbors, and Long Short-Term Memory— show to be effective. A Flask-based user interface is created to make the way of uploading and analyzing signature images simple. Integrating user authentication enhances the system's usability and security. When it comes to analyzing datasets, advanced models like Exception, Voting Classifiers, and feature extraction utilizing HOG with Recursive Feature Elimination (HOG-RFE) reach an astounding 100% accuracy. Because of its high reliability and performance, this is fantastic option for signature verification with CNN and HOG. During system testing, data is entered to evaluate performance, and the user experience is generally improved by integrating a user-friendly Flask interface. By limiting enter system to authorized users only, secure authentication improves the system's security.

PROJECT OUTLINE

Important to the verification of signatures is the feature obtainment procedure. The goal of improving this procedure is render verification system more accurate and dependable by better capturing the distinctive qualities of signatures. The signature verification method is anticipated to perform better overall with improved feature extraction. This involves improving the system's capacity to detect fake or authentic signatures, decreasing count of false alarms and negatives, and boosting accuracy. signature verification system's usefulness may be increased by tailoring it to various uses, such e-signatures and mobile authentication. The technology may be utilized in several types of secure access points because of this diversity, which can meet more demands. Making the system more accessible and user-friendly via UI refinement is crucial for increasing adoption. Financial transactions and security access points are two examples of applications that greatly benefit from realtime inference. Practical application in situations where speedy verification is crucial for security and efficiency is achieved by optimizing the system to offer quick and accurate results in real-time circumstances.

REFERENCES

[1] "Offline signature authentication LSTM and HOG." is published in the journal Bull. Elect. Eng. Inform. in 2023 and can be found in volume 12, issue 1, pages 283-292.
[2] Thirunagalingam, Arunkumar, Transforming Real-Time Data Processing: The Impact of AutoML on Dynamic Data Pipelines. (July 06, 2024). Available at SSRN: https://ssrn.com/abstract=5047601 or http://dx.doi.org/10.2139/ssrn.5047601

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] M. Ajij, S. Pratihar, S. R. Nayak, T. Hanne, and D. S. Roy published an article titled "Off-line signature authentication Through Basic Combinations of Directional Codes from Edge Pixels " in the March 2021 issue of Neural Comput. Appl. with the DOI 10.1007/s00521-021-05854-6.
[4] "Online signature authentication through segment-level fuzzy modelling," published in 2014 by IET Biometrics, was written by A. Q. Ansari, M. Hanmandlu, J. Kour, and A. K. Singh.
[5] In 2014, K. Cpałka and M. Zalasiński published an article titled "On-line signature authentication using vertical signature partitioning" in the journal Expert Systems Technology, chapter 41, issue 9, pages 4170- 4180.
[6] Research by K. Cpałka, M. Zalasiński, and L. Rutkowski was published in June 2016 in the journal Appl. Soft Comput. and introduced a new approach to verifying an individual's identification by analyzing a handwritten dynamic signature.
[7] Griechisch, Malik, and Liwicki's work on online signature Authentication with help of KolmogorovSmirnov distribution distance was published in the proceedings from 14th International Conference on Advances in Handwriting Recognition in September 2014, pages 738-742.
[8] "Online signature Authentication on mobile devices," published in the IEEE Transactions on Industrial Forensics Security, volume 9, issue 6, June 2014, pages 933-947, was written by N. Sae-Bae and N. Memon.
[10] In Proc. Int. Conf. Pattern Recognit. (ICPR), 2006, pp. 869-872, S. Chen and S. Srihari detailed a new path for off-line signature authentication that relies on the graph matching.
[11] Mohit, Mittal (2018). Federated Learning: An Intrusion Detection Privacy Preserving Approach to Decentralized AI Model Training for IOT Security. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 7 (1):1-8.
[12] Geometric parameters for offline, fixed-pointarithmetic-based automated signature authentication, Published in the June 2005 issue of the IEEE Transaction on Pattern Analysis and Machine Intelligence, this article was written by M. A. Ferrer, J. B. Alonso, and C. M. Travieso.
[13] Pattern Recognition, vol. 48, no. 1, pp. 103-113, 2015, discusses the utilization of the oneclass SVM classifier for writer-independent handwritten signature authentication. Y. Guerbai, Y. Chibani, and B. Hadjadji wrote the paper.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details