Grenze International Journal of Engineering and Technology, June Issue

Intelligent Systems for Signature Recognition and Authentication

Dr Manjula G[1], K Vennela[2], C Niharika[3] and G Gayathri[4]
[1-4]Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, India
Email: manjula-ise@dsatm.edu.in, vennelar581@gmail.com, nihamsd2002@gmail.com, chowdarygayathri96@gmail.com

***Abstract*— In this paper, a novel method of writer-independent online signature verification is put forward, employing Siamese-architected recurrent neural networks (RNNs). A bidirectional strategy for accessing past and future contexts, as well as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) systems, are investigated. The study compares the benefits and drawbacks of each recurrent Siamese network while doing a thorough examination of system performance and training time. The suggested recurrent Siamese networks outperform the most advanced online signature verification systems, as shown by the experimental findings on the BiosecurID database, which has 11,200 signatures from 400 individuals. Furthermore, the study uses the GPDS Synthetic Signature Database to classify signatures using deep learning, more precisely Convolutional Neural Networks (CNNs) based on the GoogLeNet architecture (Inception-v1 and Inception-v3). The models receive a high level of validation.**

***Index Terms*— SURF Algorithm, Harris Technique, CNN, Signature Identification, the Signature Validation, and Forgeries Detection**

I. INTRODUCTION

The importance of biometrics—especially handwritten signatures—in access control and other applications is covered within the first series of papers. It examines current research, highlighting machine learning methods for signature verification and filling in knowledge gaps. The emphasis is on classification tasks, where CNNs such as Google Net Inception-v1 and Inception-v3 are used to assess the accuracy, validating grief, curve of ROC, AUC, and metrics for accuracy of real and fake signatures. The text that follows explores the intricacy of signature verification and notes its susceptibility to fraud. It presents techniques that make use of the Harris-Surf framework to improve system-wide effectiveness, the Crest-Trough technique for forgery detection, and neural network convolution (also known as CNN for evaluation. The study highlights CNN's effectiveness in classification and offers improvements in preprocessing and streamlined verification.

The third volume looks at the broader area of biometric technology, focusing on physiological and behavioral traits for identification, particularly in developing countries. It divides signature verification into online and offline methods, investigating dynamic and static approaches. The progression from manually generated features to the latest deep learning methods is emphasized, encompassing the phases of data collection, preprocessing, feature extraction, and classification. The study delves into engineering-based and deep learning-based models, as well as considerations of performance factors and datasets for offline verification of signatures. The third volume of

Grenze ID: 01.GIJET.10.2.113
© Grenze Scientific Society, 2024

writings discusses the growing importance of Recurrent Neural Networks (RNNs), notably the LSTM and GRU architectures, in applications such as handwriting recognition and verification. It discusses the limits of traditional RNNs and suggests LSTM and GRU designs inside a Siamese framework for online signing.

II. Literature Survey

A. A Comprehensive Study on Offline Signature Verification

The evolution of signature verification spans over 30 years, initially involving manual checks and progressing to computer-based methods for increased accuracy. Notably, North America Aviation proposed the first electronic signature verification method in 1965. Subsequent milestones include the introduction of offline verification algorithms in 1973 by Nagel and Rosenfeld. Pioneering pseudo-dynamic feature extraction techniques emerged in 1986. The paper provides a comprehensive survey of signature verification research, showcasing advancements such as deep learning-based approaches, convolutional neural networks (CNN), and Siamese neural networks. Performance metrics, including Equal Error Rate (EER) and accuracy, demonstrate varying success across different datasets and methodologies.

B. Offline Signature Recognition and Forgery Detection using Deep Learning

In recent studies on offline signature verification using deep learning techniques, limited research has been reported, with only a few authors working in this specific direction. Noteworthy studies include Shahane et al. [1], which focused on noise removal, preprocessing, feature extraction, and learning modules. They utilized different thresholds for matching to enhance system potency but faced challenges in using edge values universally across various signatures. Fahmy [3] employed separate wavelet transform for feature extraction and a feedforward backpropagation error neural network for recognition, achieving a 95% accuracy for real signatures. However, the dataset used was small, leading to potential overfitting. Zhu et al. [9] introduced a supervised learning framework combining shape data from different metrics via LDA. They addressed signature extraction from document images but noted the complexity of their structural framework. Overall, the studies highlight the early stages and challenges in incorporating deep learning for offline signature verification.

C. Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics

The paper delves into the application of Recurrent Neural Networks (RNNs) in on-line signature verification, a field where deep learning systems with traditional architectures struggle due to limited training data. By introducing LSTM and GRU RNNs within a Siamese architecture and exploring bidirectional schemes, the study aims to learn a dissimilarity metric from signature pairs, addressing skilled and random forgery types. Despite previous attempts with LSTM for signature verification proving unfeasible due to training constraints, this work pioneers the application of recurrent Siamese networks to this domain. It proposes a writer-independent verification system, analyzes RNN performance in distinguishing forgery types, and conducts a comprehensive examination of system effectiveness and training time. The study uses the BiosecureID database and outperforms existing on-line signature verification systems, paving the way for improved signature verification methodologies.

D. A Comparative Study among Handwritten Signature VerificationMethods Using Machine Learning Techniques

The text underscores the growing interest of researchers from various institutions in the field of handwritten signature verification, recognizing the pivotal role of signatures in biometric technologies as personal verifiers. Previous reviews have comprehensively covered work up to 1989 and from 1989 to 1993. The current review focuses on the last decade, from 2012 to the present, providing insights into novel advancements and emerging issues in handwritten verification systems. A comparative analysis is presented, detailing techniques used for feature extraction and classifiers in identification and verification systems. Notable studies include the work of Hamadene et al. [41], who proposed a method based on contourlet transform and co-occurrence matrix for offline signature verification, achieving competitive results. Other studies by Nemmour and Chibani [6], Kamihira et al. [42], and Fayyaz et al. [20] employed ridgelet transform, gradient features, and autoencoder classifiers, respectively, showcasing varying levels of accuracy. The use of convolutional neural networks (CNNs) in studies by Mersa et al. [48] demonstrated promising results on multiple datasets. Overall, these diverse approaches highlight the multifaceted nature of challenges and advancements in the evolving landscape of handwritten signature verification

E. Offline Signature Verification using Deep Learning Convolutional Neural Network (CNN) Architectures GoogLeNet Inception-v1 and Inception-v3

This study delves into deep learning methods, specifically GoogLeNet's Inception-v1 and Inception-v3 architectures, applied to handwritten signature classification using the extensive GPDS Synthetic Signature Database. Inception-v1 demonstrated superior performance in distinguishing 2D signatures compared to Inception-v3, despite the latter's success in other image classification tasks. The paper emphasizes the societal and legal acceptance of signature verification among various biometric systems for individual identification. It surveys prior techniques like Dynamic Time Warping (DTW), Neural Networks (NNs), Wavelet-Based Approaches, Structural Approaches, and Support Vector Machines (SVM), showcasing diverse strategies in this field. Additionally, it highlights Convolutional Neural Networks' (CNNs) pivotal role in visual imagery analysis, particularly their success in the ImageNet task, showcasing their prominence in machine learning tasks. The objective is to classify genuine and skilled forged signatures from 1000 users, employing metrics such as Equal Error Rate (EER), Receiver Operating Characteristic Curve (ROC curve), Area Under the ROC Curve (AUC), validation loss, and validation accuracy for model evaluation.

III. Proposed System

The proposed methodology involves a systematic approach to signature verification. Initially, the dataset is acquired, marking the phase of data acquisition. Subsequent pre-processing steps, including data resizing and normalization, are applied to enhance the dataset quality. The dataset is then divided into training and testing sets. Following this, a Convolutional Neural Network (CNN) model is implemented for signature verification. The model's performance is subsequently evaluated. The paper introduces a novel method for signature recognition and forgery detection. The proposed system involves recognizing test signatures using Convolutional Neural Networks (CNNs) and the Crest-Trough method. The CNN comprises layers for feature extraction and a linear classifier. The layers' parameters are learned through backpropagation. The signature verification system addresses data retrieval, pre-processing, feature extraction, identification method, and performance analysis. In off-line signature verification, images obtained by a scanner or camera depict an individual's signature. The system aims for a balanced approach between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR). After classifying the image into a subject class, the system employs two algorithms, Harris and Surf, for forgery detection, producing a binary result indicating whether the signature is genuine or forged. The project implemented and trained Inception-v1 and Inception-v3 models using TensorFlow and Keras on the GPDS Synthetic Signature Database. It involved a local machine with Jupyter Notebook and focused on offline handwritten signature classification. The models were fine-tuned with callback functions, achieving high accuracy and low Equal Error Rate (EER). Inception-v1 outperformed Inception-v3 in classification, and the Area under the Receiver Operating Characteristic Curve (AUC ROC) scores highlighted the effectiveness of Inception-v1 in distinguishing between genuine and forged signatures. The project provided valuable insights into training characteristics and model performance metrics. The proposed methodology integrates LSTM and GRU Recurrent Neural Networks (RNNs) within a Siamese architecture for online signature verification, exploring bidirectional schemes as well. The Siamese architecture aims to learn a similarity metric from pairs of genuine and forged signatures, while LSTM RNNs leverage memory blocks to control information flow in time steps. Additionally, GRU RNNs, inspired by LSTM but simpler in computation, employ two gates to manage information flow. Bidirectional RNNs (BRNNs) enhance systems by accessing both past and future contexts, potentially improving performance in tasks like handwriting recognition. The methodology compares these RNN architectures in online signature verification, considering their specific functionalities and computational approaches for handling temporal data. The process of signature verification, whether offline or online, involves a systematic series of steps, including data acquisition, preprocessing, feature extraction, and classification. Offline signature data is obtained through image scanning, while online signatures are captured using digital devices. Preprocessing techniques include color-to-gray conversion, noise removal, and size normalization. Feature extraction categorizes signatures into global, mask, and grid features, utilizing methods like wavelet coefficients, mask features for line direction, and grid features for overall appearance. Classification methods like Support Vector Machines, template matching, hidden Markov models, and neural networks are commonly employed to determine signature authenticity by comparing extracted features with stored database entries. The process aims to differentiate between genuine and forged signatures and relies on comprehensive datasets for training and testing. Both offline and online databases have varying characteristics, such as resolution and sampling rate, influencing the complexity of feature extraction and verification.

IV. CONCLUSION

The conclusion regarding fabric fault detection using image processing techniques underscores both the progress made and the persistent challenges in this domain. The advancements in image processing and machine learning have significantly enhanced the potential for automated fabric defect detection, offering increased accuracy, speed, and consistency compared to traditional manual inspection methods. These technological developments, particularly the utilization of Convolutional Neural Networks (CNNs) and sophisticated algorithms, have demonstrated impressive capabilities in identifying various fabric faults with high precision. However, despite these advancements, several challenges remain. The diverse and complex nature of fabric defects continues to pose a significant obstacle, requiring robust algorithms capable of distinguishing subtle variations in textures, patterns, and colors. Variations in lighting conditions and the need for extensive, diverse datasets for training further impact the accuracy and generalization of detection models. Moreover, the integration of automated fabric fault detection systems into industrial settings demands careful planning and implementation to ensure seamless operation without disrupting production workflows. Additionally, considerations related to computational resources, cost-effectiveness, and scalability remain crucial factors to address for wider adoption across different scales of textile production facilities.In conclusion, while image processing techniques have shown great promise in fabric fault detection, further research and technological advancements are necessary to overcome the existing challenges. Future efforts should focus on refining algorithms to handle diverse defects, improving model generalization, addressing lighting variability, optimizing computational resources, and facilitating smooth integration into existing production lines. Ultimately, continued innovation in image processing and machine learning methodologies holds the key to developing more robust, efficient, and practical solutions for automated fabric fault detection in industrial applications.

REFERENCES

[1] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017, November). Offline handwritten signature verification—Literature review. In 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-8). IEEE

[2] Bibi, K., Naz, S., & Rehman, A. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79(1), 289-340.

[3] Ghandali, S., and M.E. Moghaddam. (2009) “Off-Line Persian Signature Identification and Verification Based On Image Registration and Fusion.” J. Multimedia 4 (3): 137–144.

[4] Ramachandra A.C., J. Ravi, K.B. Raja, K.R. Venugopal, and L.M. Patnaik. (2009) “Signature Verification using Graph Matching and Cross Validation Principle.” 1 (1)

[5] Fahmy, M. M. (2010). “Online handwritten signature verification system based on DWT features extraction and neural network classification.”Ain Shams Engineering Journal, 1(1), 59–70.

[6] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). “Imagenet classification with deep convolutional neural networks.” In Advances in neural information processing systems (pp. 1097-1105).

[7] M. A. Taha and H. M. Ahmed, “Iris features extraction and recognition based on the local binary pattern technique,” in Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA), pp. 16–21, Maysan, Iraq, July2021

[8] M. A. Taha and H. M. Ahmed, “A fuzzy vault development based on iris images,” Eureka: Physics and Engineering, no. 5,pp. 3–12, 2021.

[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning.Cambridge, MA, USA: MIT Press, 2016. [Online].

[10] Sutskever, O. Vinyals, and Q. V. Le, ‘‘Sequence to sequence learning with neural networks,’’ in Proc. Adv. Neural Inf. Process. Syst. (NIPS), 2014,pp. 3104–3112.

[11] Jagtap, A. B., Sawat, D. D., Hegadi, R. S., & Hegadi, R. S. (2020). Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). MULTIMEDIA TOOLS AND APPLICATIONS

[12] Kruthi, C., & Shet, D. C. (2014, January). Offline signature verification using support vector machine. In 2014 Fifth International Conference on Signal and Image Processing IEEE. (pp. 3-8).