Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

Verification System for Handwritten Signatures with Modular Neural Networks

T. Vijayakumar

Professor, Department of ECE, M P Nachimuthu M Jaganathan Engineering College, Chennimalai, Erode, Tamil Nadu, India

E-mail: vijayprahu@gmail.com

Abstract

Handwritten signature is considered as one of the primary biometric processes for human verification in various applications including banking and legal documentations. In general, the handwritten signatures are verified with respect to the pressure, direction and speed followed on a plain document. However, the traditional methods of verification are less accurate and time consuming. The proposed work aims to develop a deep learning -based approach for handwritten signature verification process through a Modular Neural Network algorithm. The work utilized the handwritten signatures dataset downloaded from the kaggle website that consists of original and forged signatures of 30 individuals. The work also included a set of 20 individual signatures for improving the sample count on training and verification process.

Keywords: Fake detection, pattern recognition, signature classification, segmentation, image enhancement

1. Introduction

Signature verification software are widely used in many sectors, where a digital signature image or direct signature is loaded to the software for analyzing its genuineness over the given original signature. The automation tools are fast and reduces the human error significantly in the verification process. The algorithm placed in the software generates a confidence score and a threshold value specified in the software determines the signature as original or fake. Similarly the software has the ability to process multiple signatures at a time with a simultaneous estimation approach [1, 2]. However, the signature verification methods are broadly classified into three types as-

- Digital,

DOI: https://doi.org/10.36548/jaicn.2022.3.007
Received: 28.08.2022, received in revised form: 15.09.2022, accepted: 06.10.2022, published: 15.10.2022

- Electronic and
- Handwritten signatures.

Digital signature is one of the most secure signing methods that verifies the authenticity through an encrypted approach named as public key infrastructure. The original sign is converted into a digital form to generate a digital certificate on the certificate authority tool. The certificate authority has the provision to store the digital certificate on their software and can compare the future signatures by creating a corresponding hash value data. The similarity score estimation among the newly generated hash value to the existing one confirms the originality of the signature [3].

The electronic signature verification method also works same as of the traditional method that considers the location, date, time and other more parameters for its analysis. These kinds of software mostly verify the originality by verifying the overwriting and alteration made on the signatures. The electronic signature verification tools are less expensive and that be higher when it is incorporated with encrypted type of certificates and security checks [4].

The handwritten signature verification model converts the ink signatures into a digital image for comparing it over the existing signature. It is done by estimating the contours ratio followed in the signature. The iterative analysis on the signature image is also done in some e-signature software [5].

Although the signature verification methods are considerably less accurate than the fingerprint and iris biometrics, it is widely accepted in many institutes due to its simplicity and cost efficiency. Unless like other biometrics here the individual need to be present at the institutional office for verification. Similarly, the technology based fraud and forgeries are less in signature based verifications [6, 7].

2. Related Works

A shallow convolution neural network algorithm was used to verify the handwritten signatures in GPDS-300 and GPDS-960 datasets. The research outcome indicates an accuracy rate of 96.87 and 97.19 percentages respectively [8]. An off-line handwritten signature verification systems was developed with Siamese neural networks with a dense layer count of 500 numbers in GAVAB and MCYT datasets. The experimental outcome indicates an accuracy outcome of 99.06 and 99.44 percentages in GAVAB and MCYT datasets [9]. A

Caps-Net based algorithm was designed to verify the handwritten signatures through a data augmentation process in GPDS and MCYT datasets. The research outcome indicates an equal error rate of 12.34% in GPDS dataset and 2.58% in MCYT75 dataset [10]. A feature weighting technique was implemented on relief algorithm to verify the handwritten signatures in online. An experiment was performed with a self-made dataset and SVC2004 dataset and that indicates a false acceptance rate of 1.2% in the self-made dataset and 5.125% on SVC2004 dataset [11]. A region restricted adversarial based technique was developed to address the black-box attacks on handwritten signature verification. The experimental analysis found an outcome of 92.1% of accuracy in the estimations [12].

An online handwritten signature verification approach was structured with curvature association and torsion feature technique. The result indicates an equal error rate of 1.2% in average on MCYT-100 dataset [13]. A wrapper metaheuristic based algorithm was developed to verify the handwritten signatures at SVC2004 dataset. The experimental outcome indicates a maximum mean accuracy of 97.58% [14]. A writer-independent dichotomy transformation model was proposed to verify the offline handwritten signatures in GPDS dataset. The research outcome indicates an equal error rate of 3.32% when the model is incorporated with a CNN based SVM model [15]. A secure kNN technique was framed based on combinational features in MCYT100 dataset. The result indicates an equal error rate of 0.64% on 10 training samples when the features are combined and 1.10% on utilizing the global features [16]. An adversarial variation network was structured for handwritten signature verification application and its performance was verified with four different datasets. The experimental output gave a maximum accuracy of 96.16% in CEDAR dataset and least accuracy of 90.32% in GPDS dataset [17].

From the literature study, it has been found that different types of image processing and machine learning based algorithms were developed for verifying the originality of the handwritten signatures. However, the research outcomes were not steady and get changes with respect to dataset to dataset. The proposed work aims to develop an algorithm that suits a openly available dataset and the self-made dataset using modular neural networks.

3. Proposed Work

The proposed work is employed with a Modular Neural Network (MNN) that comprises of more than one neural network in its architecture which makes the algorithm to complete its process on different segregations. In general the modular neural networks

require a high computational system and memory space for its operation. However, the modular neural networks are very efficient over the traditional neural networks and the hybrid network approaches. Figure 1 represents an architectural overview of the modular neural network.

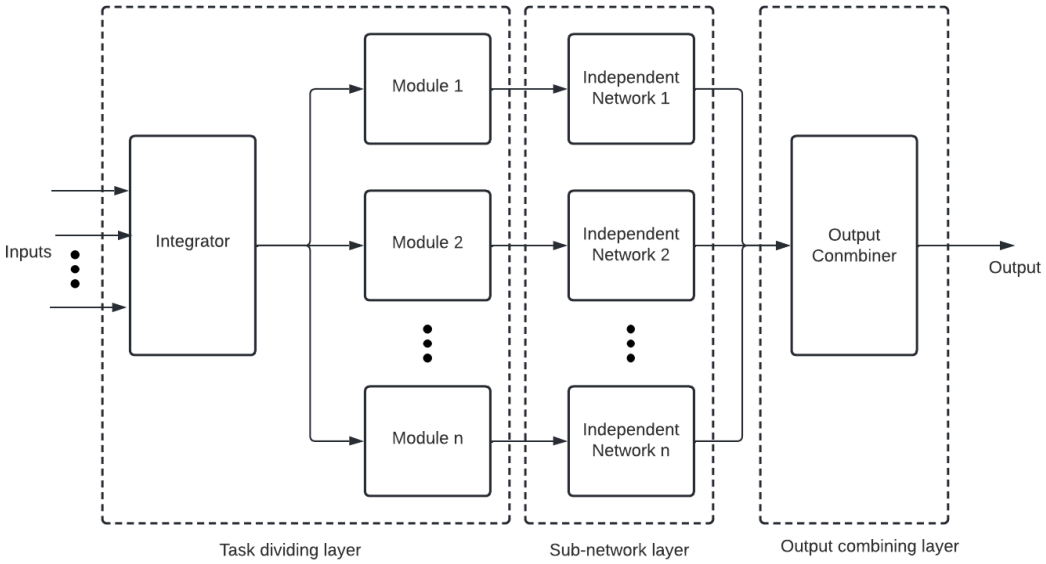

Figure 1. Architecture of a modular neural network

Modular neural networks are basically designed with three layers namely task diving layer, sub-network layer and output combining layer. The task diving layer is structured with an integrator module that receives all the inputs taken from the dataset and the responsibility of the integrator is to sub-divide the tasks that are needed to be done by the algorithm. The sub-divided tasks are forwarded to the sub-network layer that consists of ‘n’ independent network which equals to the module or problem sub-divided in the task dividing layer.

The independent network layer represents a feed forward neural network in general that consists of an input, hidden and output layer. A lightweight neural network architecture is placed generally to reduce the computational complexity of the network. Instead of a regular output layer an output combining layer is place in the flow to combine all the outputs received from the independent network layers. The combiner regulates the output to form a solution for the given problem.

4. Experimental Work

The proposed work is verified with a dataset downloaded from kaggle [18] website for estimating the efficacy of the proposed modular neural networks. The dataset contains

original and forged signature images of 30 individuals and that consists of an even number of images in each category. Therefore, the total number of images available in the dataset is 300 and that is utilized with 60:40 ratio for training and testing process. Figure 2 represents a few sample images from the dataset.

Figure 2. Dataset samples

Apart from the dataset images, the work is also incorporated with 200 images that are developed by the authors with 20 individual signatures consists of equal number of samples on each class. The experiment was performed in the Google Colab platform with Windows 10 operating system that utilizes the cloud RAM of 32GB.

Table 1. Performance comparison of the proposed work

Algorithm	Kaggle Dataset			Self-made dataset		
	Accuracy	EER	AUC	Accuracy	EER	AUC
CNN	88.3	3.4	92.78	81.62	4.32	92.37
ANN	94.56	1.89	98.1	83.94	3.4	94.3
SVM	90.78	2.6	97.89	90.1	2.04	97.11
MNN	96.29	1.16	99.36	91.13	1.84	98.07

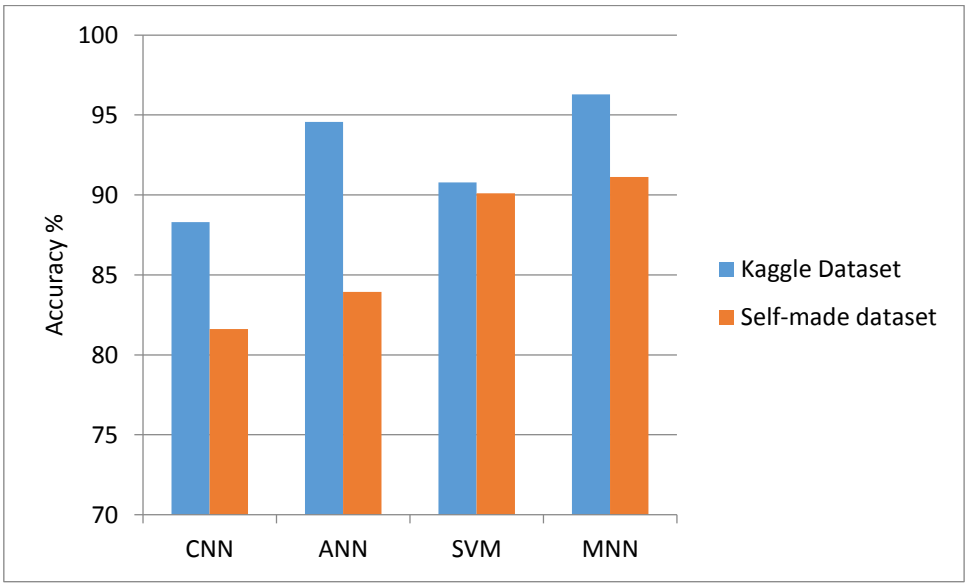

Figure 3. Accuracy attainment of the verified algorithms

Similarly, the MNN is structure with a basic artificial neural networks and it is compared in the work with the traditional Artificial Neural Network (ANN), Convolutional Neural Network (CNN) and the Support Vector Machine (SVM). To prove the efficacy of the proposed work the accuracy, Equal Error Rate (EER) and the Area Under the Curve (AUC). Table 1 represents the research comparison of the proposed model with the existing ones.

The experimental outcome indicates a betterment on the accuracy of MNN algorithm on both kaggle and self-made dataset. However, the accuracy of SVM reaches almost closer to the outcome of MNN on self-made dataset category alone. The accuracy differences among the verified two datasets show a huge variation in the algorithm except the SVM. The performance outcomes are far better in the kaggle dataset images than the self-made dataset.

5. Conclusion

Handwritten signature verification is one of the primary tasks for most of the institutions on verifying the individual's originality. Due to simplicity, the handwritten signatures are widely accepted in many countries. Fingerprint and iris based detection models are complex and requires the individual's presence during the verification process. The signature verification tools don't require the presence of an individual but same as of other biometric verification, this also requires a computational system for analysis. The proposed work is designed with a modular neural network that consists of a lightweight ANN as its individual network and its combined output produces an accuracy of 96.29% on an openly available dataset and 91.13% on the self-made dataset. The performance of the self-made

dataset can be improved when it is operated with a preprocessing technique before the training process.

References

[1] Stauffer, Michael, Paul Maergner, Andreas Fischer, and Kaspar Riesen. "A survey of state of the art methods employed in the offline signature verification process." New Trends in Business Information Systems and Technology (2021): 17-30.

[2] Bibi, Kiran, Saeeda Naz, and Arshia Rehman. "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities." Multimedia Tools and Applications 79, no. 1 (2020): 289-340.

[3] Hafemann, Luiz G., Robert Sabourin, and Luiz S. Oliveira. "Offline handwritten signature verification—literature review." In 2017 seventh international conference on image processing theory, tools and applications (IPTA), pp. 1-8. IEEE, 2017.

[4] Diaz, Moises, Miguel A. Ferrer, Donato Impedovo, Muhammad Imran Malik, Giuseppe Pirlo, and Réjean Plamondon. "A perspective analysis of handwritten signature technology." Acm Computing Surveys (Csur) 51, no. 6 (2019): 1-39.

[5] Beresneva, Anastasia, Anna Epishkina, Sergey Babkin, Alexey Kurnev, and Vladimir Lermontov. "Handwritten signature verification: the state of the art." First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures (2017): 234-238.

[6] Hameed, M. Muzaffar, Rodina Ahmad, Miss Laiha Mat Kiah, and Ghulam Murtaza. "Machine learning-based offline signature verification systems: a systematic review." Signal Processing: Image C

[7] Ooi, Shih Yin, Andrew Beng Jin Teoh, Ying Han Pang, and Bee Yan Hiew. "Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network." Applied Soft Computing 40 (2016): 274-282.

[8] Jain, Anamika, Satish Kumar Singh, and Krishna Pratap Singh. "Handwritten signature verification using shallow convolutional neural network." Multimedia Tools and Applications 79, no. 27 (2020): 19993-20018.

[9] Ruiz, Victoria, Ismael Linares, Angel Sanchez, and Jose F. Velez. "Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks." Neurocomputing 374 (2020): 30-41.

[10] Yapıcı, Muhammed Mutlu, Adem Tekerek, and Nurettin Topaloğlu. "Deep learning-based data augmentation method and signature verification system for offline handwritten signature." Pattern Analysis and Applications 24, no. 1 (2021): 165-179.

[11] Yang, Li, Yuting Cheng, Xianmin Wang, and Qiang Liu. "Online handwritten signature verification using feature weighting algorithm relief." Soft Computing 22, no. 23 (2018): 7811-7823.

[12] Li, Haoyang, Heng Li, Hansong Zhang, and Wei Yuan. "Black-box attack against handwritten signature verification with region-restricted adversarial perturbations." Pattern Recognition 111 (2021): 107689.

[13] He, Lang, Hua Tan, and Zhang-Can Huang. "Online handwritten signature verification based on association of curvature and torsion feature with Hausdorff distance." Multimedia Tools and Applications 78, no. 14 (2019): 19253-19278.

[14] Hancer, Emrah, Ilya Hodashinsky, Konstantin Sarin, and Artyom Slezkin. "A wrapper metaheuristic framework for handwritten signature verification." Soft Computing 25, no. 13 (2021): 8665-8681.

[15] Souza, Victor LF, Adriano LI Oliveira, Rafael MO Cruz, and Robert Sabourin. "A white-box analysis on the writer-independent dichotomy transformation applied to offline handwritten signature verification." Expert Systems with Applications 154 (2020): 113397.

[16] Xia, Zhihua, Tianjiao Shi, Neal N. Xiong, Xingming Sun, and Byeungwoo Jeon. "A privacy-preserving handwritten signature verification method using combinational features and secure kNN." IEEE Access 6 (2018): 46695-46705.

[17] Li, Huan, Ping Wei, and Ping Hu. "AVN: An Adversarial Variation Network Model for Handwritten Signature Verification." IEEE Transactions on Multimedia 24 (2021): 594-608.

[18] https://www.kaggle.com/datasets/divyanshrai/handwritten-signatures

Author's biography

T. Vijayakumar is currently working as Professor in the Department of ECE at Jai Shriram Engineering College, Avinashipalayam, Tamil Nadu, India. His research includes Computer Vision, Motion Analysis, Stereo Vision, Object Recognition, computer graphics, photo interpretation, image retrieval, Embedded Image Processing and Real-time image and video processing applications.