iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44861

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Comparison of Signature Forgery Detection Architectures

Teja E[1], N Arpith Mathew[1], Pragathi M[2]
[1]*Scholar,* [2]*Assistant Professor, Department Of Computer Science & Engineering,*
Sir M Visvesvaraya Institute Of Technology, Bengaluru, Karnataka, India.

Abstract: ***In today's society, we use signatures for many important documents like passports, driving licenses, bank cheques, etc. But signatures can be forged in multiple ways, which can create a number of problems, such as identity theft, hacking, fake identification, etc. To reduce these problems, our project is about developing a system for detecting whether a signature is forged or real from a dataset of signatures. For our project, we are developing an offline signature verification system. This system is based on CNN (Convolutional Neural Network) and SNN (Siamese Neural Network). In this project, we will be comparing both CNN's and SNN's to find which produces a better result. We are implementing the project using a custom CNN, a CNN with VGG16 architecture, a custom SNN and a SNN using the SigNet architecture.***
Keywords: CNN, SNN, VGG16, SigNet, Signature, Verification.

I. INTRODUCTION

A signature is a distinct form of a person's name that represents the said person. A signature acts as a form of identification for a person. It is a critical means of identification as it is used in many things such as legal documents, identification cards, and cheques, etc. Since signatures are used widely, there are many malicious actors trying to forge signatures for some personal gain. Handwritten signatures are one of the most important forms of biometric authorization that is used universally to authorize and verify documents. Therefore, sophisticated signature verification methods are necessary. Online signature verification methods extract features and record the trajectory and variations in the signature while it is being performed. They record features with time and compare them to a database containing the signature sample. It usually yields very high accuracy in identifying forged signatures. Offline signature verification methods use feature extraction and check for discrepancies in the signature. It is less accurate than online verification methods. We are implementing offline signature verification methods using CNN (Convolutional Neural Network) and SNN (Siamese Neural Network) models. A Convolutional neural network (CNN) is a neural network that has convolutional layers and is used mainly for image processing, classification, segmentation, and other auto-correlated data. Siamese networks are used when performing verification, identification, and recognition tasks, with the most popular examples being face recognition and signature verification. Hence, we are comparing the accuracy produced by a custom CNN, a CNN based on VGG16, which is trained on the ImageNet dataset using transfer learning, and a SNN that implements the SigNet Architecture, and hence we proposed an SNN implementation with fewer parameters and faster training time.

II. LITERATURE REVIEW

A. HANDWRITTEN SIGNATURES FORGERY DETECTION - Kshitij Swapnil Jain, Udit Amit Patel, Rushab Kheni

Kshitij Swapnil Jain, et al. (2021) have defined the objective of their research to verify if a signature is original or forged, while understanding the characteristics of the signatures and implementing a system to detect if the signature is forged. Due to the many variations in handwriting styles and the professionalism of forgers, even highly skilled experts cannot achieve a high degree of accuracy in the detection of forged signatures. An automatic recognition system can be significantly more effective in verifying signatures with high accuracy and differentiating between a genuine and a forged signature. In the proposed method, a CNN is used as a feature extractor and classifier. The feature extractor extracts features from the input data via convolution filtering and down sampling. The research was carried out under the assumption that upon training a CNN classifier for forged and genuine signatures, the trained CNN should be capable of distinguishing behavioral characteristics, such as delays and hesitation in the signature with the extracted features. Deep networks will pose a problem for this implementation as the gradient decreases exponentially and reaches zero as the backpropagation continues from the final to the first layer. Hence, a ResNet is used since it can skip a few connections and prevent the gradient from falling to an insignificant value. The proposed methodology increases the efficiency and accuracy of forgery detection.

B. *Digital signature Forgery Detection using CNN - Lakkoju Chandra Kiran, Gorantla Akhil Chowdary, Manchala Shalem Raju, Kondaveeti Gopi Krishna*

Kiran, Lakkoju Chandra, et al. (2021) are presenting an analysis of the methods for verifying the integrity of visual media, i.e., the detection of manipulated images. A signature consists of a combination of individual features and is the most significant means of verifying the authenticity of the signature. This methodology can be implemented for both online and offline methods. Offline methods verify the identity of an individual by comparing the current signature with reference signatures that have already been written. Online methods are stable and have high accuracy using dynamic knowledge related to the script. In offline verification methods, a signature is verified after it has been produced. Online verification is performed by comparing a signature to previous samples in a database. This research implements an online verification system with a dataset of 2000 images of forged and original images of signatures in the RGB format. The image is converted to grayscale and then a binary image, noise is removed, and the signature is resized. The preprocessed features are extracted and saved in a .CSV file. A CNN with three input layers bearing different weights and biases with three hidden layers uses the .CSV file as an input and output layer, which shows if the signature is genuine or forged. An optimizer and a loss function were also defined to minimize the loss. A Soft max layer is used to calculate the accuracy.

C. *OFFLINE SIGNATURE FORGERY DETECTION USING CONVOLUTIONAL NEURAL NETWORK - Raj Balsekar, Rashi Gundapwar, Aditi Parekh, Manasi Desai, Swapnil Shinde*

Raj Balsekar, et al. (2020) proposed a signature recognition and verification system based on CNN. This implementation creates a knowledge base by extracting unique features for signatures from a dataset of 150 individuals with 5 signatures each, for a total of 750 signatures. The signatures are converted to grayscale images and undergo geometric transformations. These pre-processed signatures have their features extracted and compared with those in the system to determine whether they are real or fake, using a CNN with multiple convolutional, pooling, and fully connected layers to get the output.

D. *Handwritten Signature Verification using Deep Learning - Eman Alajrami, Belal A. M. Ashqar, Bassem S. Abu-Nasser, Ahmed J. Khalil, Musleh M. Musleh, Alaa M. Barhoom, Samy S. Abu-Naser*

Alajrami, Eman, et al. (2019) proposed a deep learning system for signature verification and forgery detection. In this research, template matching and the Hidden-Markov model were used as methodologies. The research was implemented using a CNN, which extracts behavioral changes in signatures. A knowledge base of unique signature characteristics is compiled, preprocessed, resized, and distributed into two sub-directories. This is used as the CNN's input, and the evaluation is carried out with Keras and a Tensorflow backend. A dataset of 300 images is used, of which 150 each are original and forged. The original signatures were obtained from 30 individuals. The result of this methodology is a dataset with a split ratio of 8:2 that has the highest accuracy, ranging from 99.7 to 99.9%. We can conclude that the methodology has been implemented successfully.

E. *SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification - Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llad´os, Umapada Pal*

Sounak Dey, et al. (2017) proposed an offline writer-independent signature verification system based on a convolutional Siamese network, which is named SigNet. This paper covers signature verification and its types, namely offline and online, writer-dependent approach, writer-independent approach, and various related works. The images of signatures must undergo changes to fit certain standards for this system and are preprocessed to fit the needs. The system was evaluated using four datasets, which are CEDAR, GPDS300, GPDS Synthetic Signature Database, and BHSig260 Signature Corpus. The proposed SigNet architecture has achieved very high accuracy for the offline signature verification domain.

F. *Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network - Soumya Jain, Meha Khanna, Ankita Singh*

Soumya Jain, et al. (2021) are doing a comparison among various CNN architectures for a signature forgery detection system that is based on the Siamese neural network. This comparison will provide meaningful insights and comparative analysis. The dataset used for this system comprises 2149 image files and two CSV files. The image flies have 69 unique signers and the 2 CSV files are train.csv and test.csv. The dataset is labeled, and image paths are generated, and the dataset is shuffled into batches of 8 images. The contrastive loss function was used in the implementation. Three different variations of CNN were covered in the paper and were compared using a different Euclidian distance, producing different losses and f1 scores.

G. Signature Verification Using Convolutional Neural Network – Shayekh Mohiuddin Ahmed Navid, Shamima Haque Priya, Naibul Hoque Khandakar, Zannatul Ferdous , Akm Bahalul Haque

Shayekh Mohiuddin Ahmed Navid, et al. (2019) proposed a signature verification system based on convolutional neural networks (CNN). In this paper, the proposed model was a pre-trained model with the VGG-19 architecture and is connected to multiple CNN layers. The datasets used for this model were ICDAR, Kaggle, and CEDAR. For this implementation, the datasets have been augmented for training and testing. The VGG-19 architecture was used to train the model. The results obtained from this model are that this model has 100% accuracy for ICDAR, 94.44% accuracy for Kaggle, and 88% accuracy for CEDAR.

H. Off-line Signature Verification through Machine Learning - Avani Rateria, Suneeta Agarwal

Avani Rateria, et al. (2018) proposed an offline signature verification system based on machine learning using CNN (Convolutional Neural Network) and deep learning. The images are preprocessed and inverted for this implementation. Two methodologies were used; the first, a CNN feature extractor and an SVM classifier, and the second, a Siamese network. Various datasets such as CEDAR, GPDS Synthetic Signature, and BHSig260 signature corpus were used in this implementation. The results of the models were thus compared.

I. Offline Handwritten Signature Verification And Recognition Based On Deep Transfer Learning Using Convolutional Neural Networks - Atefeh Foroozandeh, Ataollah Askari Hemmat, Hossein Rabbani

Atefeh Foroozandeh, et al. (2020) proposed an offline signature verification and recognition system based on Deep Transfer Learning using CNN (Convolutional Neural Network). GPDS Synthetic Signature, MCYT-75, UTSig, and FUM datasets were used for the implementation. For preprocessing, the images are converted to grayscale and normalized, then resized to a 256 x 256 size. In this system, the t-SNE (t-Distributed Stochastic Neighbor Embedding) algorithm is used to visualize the signatures in feature space. Its results are compared with those in the other papers which were surveyed. This paper describes another proposed system in which signature recognition is based on deep transfer learning using CNN.

J. Verification of genuine and forged offline signatures using Siamese Neural Network (SNN) - Amruta B. Jagtap, Dattatray D. Sawat, Rajendra S. Hegadi, Ravindra S. Hegadi

Amruta B. Jagtap, et al. (2020) proposed an offline signature verification system based on SNN (Siamese Neural Network). The proposed system has been tested with various challenging datasets, such as MCYT-75, GPDS, and CEDAR. Useful data such as geometric mean, standard deviation, inter-quartile range (IQR), and median absolute deviation (MAD) were computed to understand the usefulness of this methodology. The results from this system are evaluated using the following parameters: TP (True Positive), TN (True Negative), FAR, and FRR.

III. OBJECTIVE

A. To analyse the current methodologies used in signature verification systems
B. To implement a few of the popular methodologies used in signature verification systems
C. To compare the accuracy and efficiencies of the methodologies
D. To propose new efficient methodologies

IV. SYSTEM ANALYSIS

E. Existing System

As signature verification is a domain that is highly applicable in the real world, there are various systems that have been proposed for signature verification systems to verify if a signature is real or forged. Signature verification is very important as signatures are used in a wide number of documents and as a means of identification for a particular person. There have been many systems that implement CNNs and SNNs that have been proposed over the years for signature verification and forgery identification. While the existing methods have good accuracy, they have too many parameters and hence need a long time for training and cannot be used on simple systems.

F. Proposed System

We intend to implement offline signature verification methods using a couple of models that are popular and have high accuracy, and do a comparative study to see which is more efficient and faster to train. We are using four different models two based on CNN (Convolutional Neural Network) and two based on SNN (Siamese Neural Network), two of the models are custom defined in each category while two are popular methods used for this problem domain. We are thus implementing a custom CNN, a CNN with VGG16 architecture, a custom SNN, and a SNN with SigNet architecture.

The system is divided into 9 main parts:

- Data Frame Generator – A pandas data frame is generated with paths and the labels of each signature or signature pairs for CNNs and SNNs respectively.
- Dataset Split function – The data frame is split into training, validation and testing sets.
- Signature Processing – The signature images are preprocessed according to the Models requirements.
- Input Generator for the Model – The input images are converted into data and features are extracted for the Model training.
- Functions – The various functions used such as accuracy and loss functions.
- The four Neural Network models – The neural network models that are implemented.
- Training the Models – Training the Models we implemented.
- Plotting Graphs – Plotting graphs for loss and accuracy.
- Accuracy evaluation – Evaluating the models loss and accuracy.

V. SYSTEM ARCHITECTURE

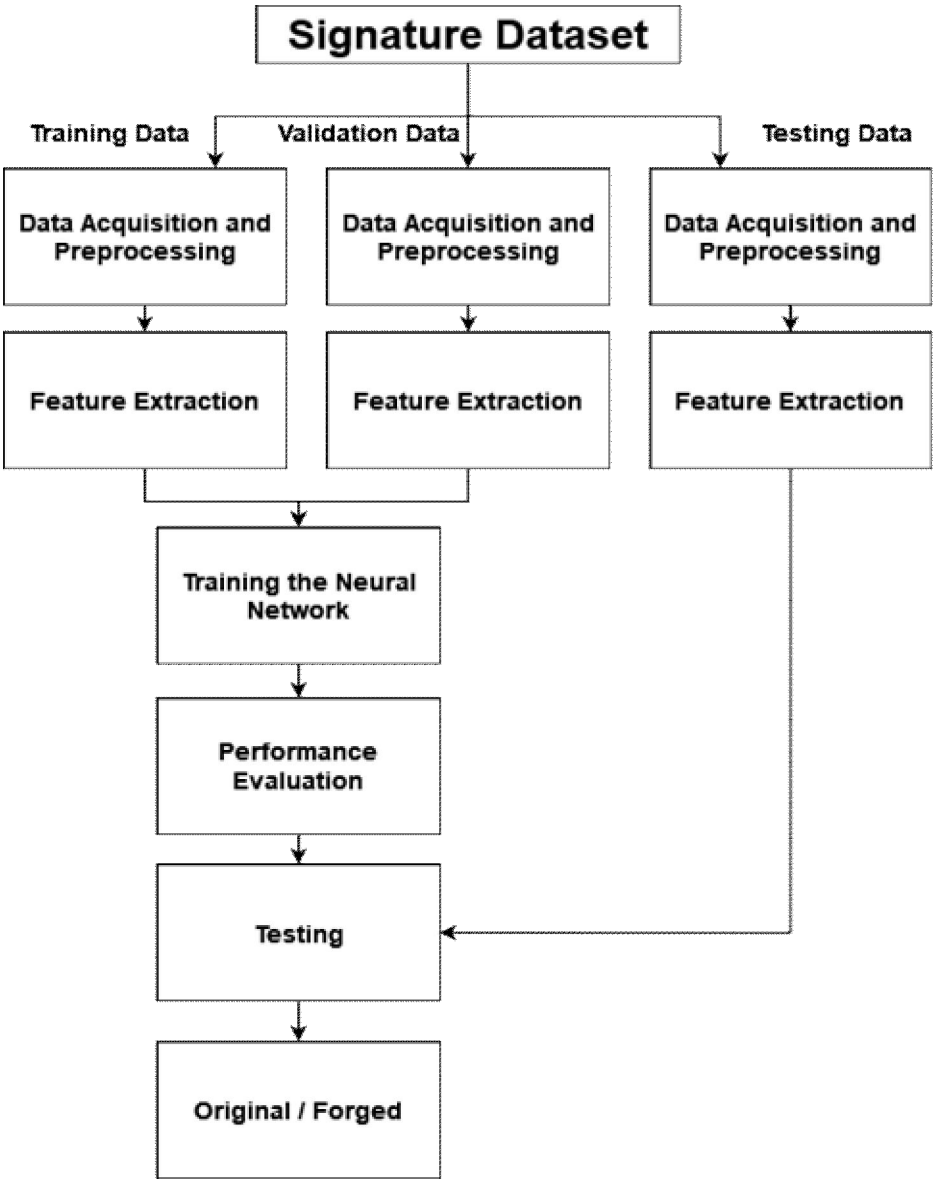


Fig. 1 System Architecture Diagram

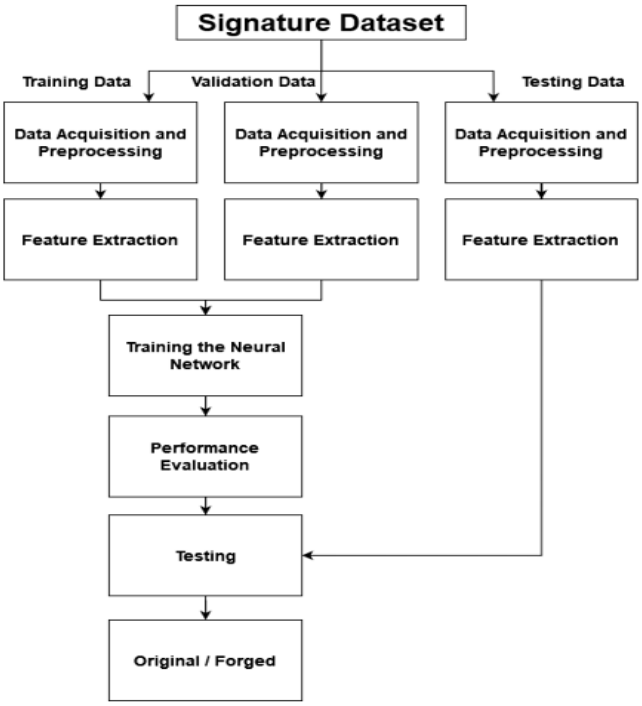


Fig. 2 Block Diagram of CNN and VGG16 Architecture

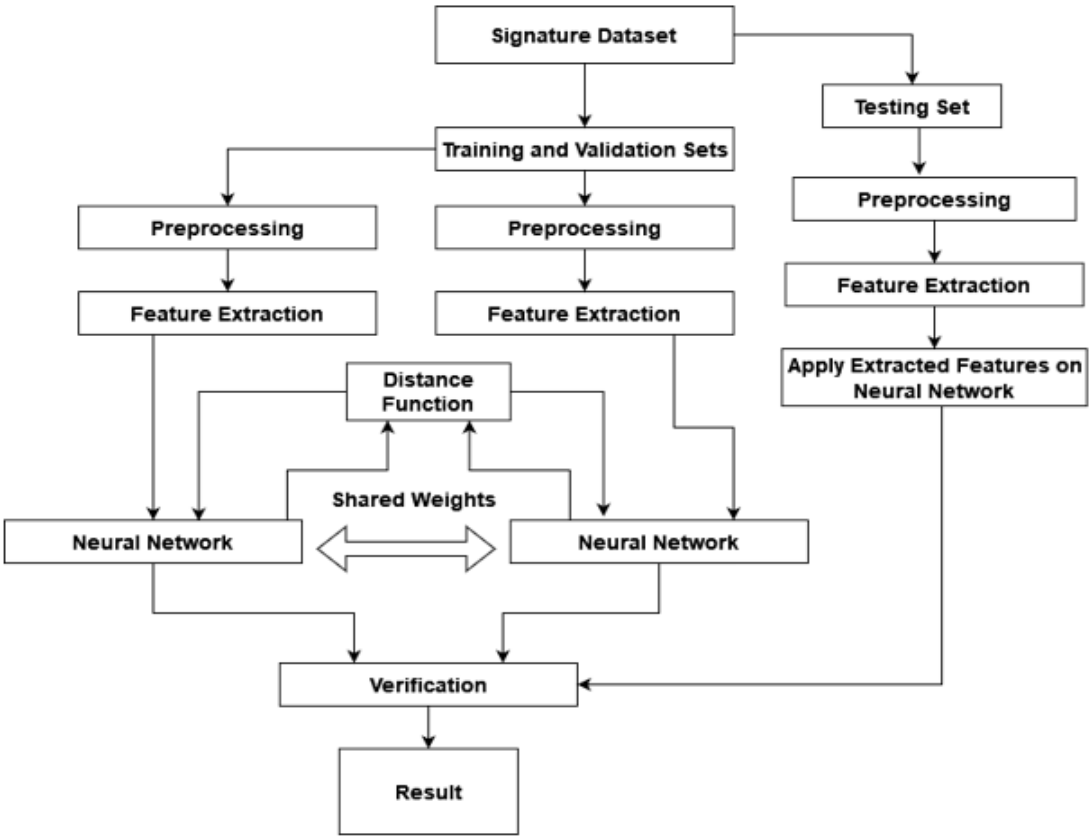


Fig. 3 Block Diagram of SNN and SigNet Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

VI.MODEL ARCHITECTURE

A. CNN Model

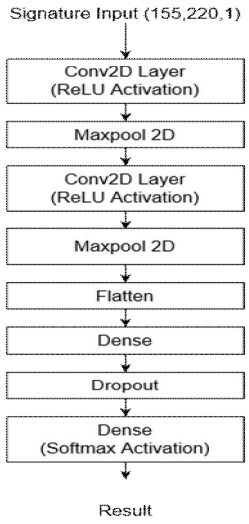


Fig. 4 Architecture of CNN

B. VGG16 Model

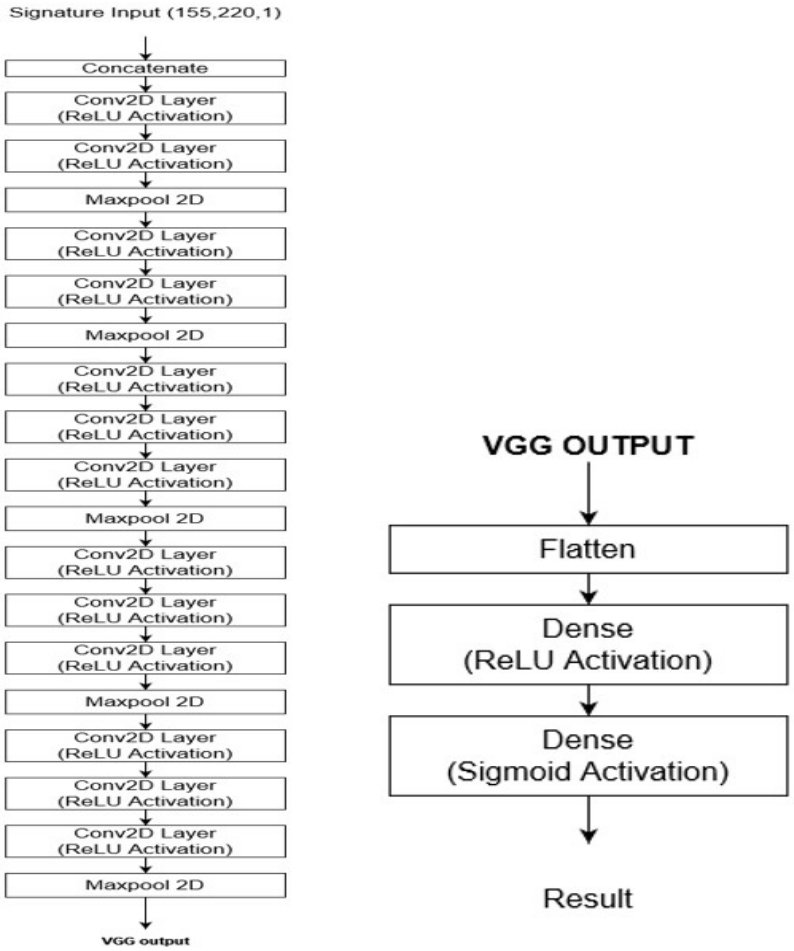


Fig. 5 Architecture of VGG16

C. SNN Model

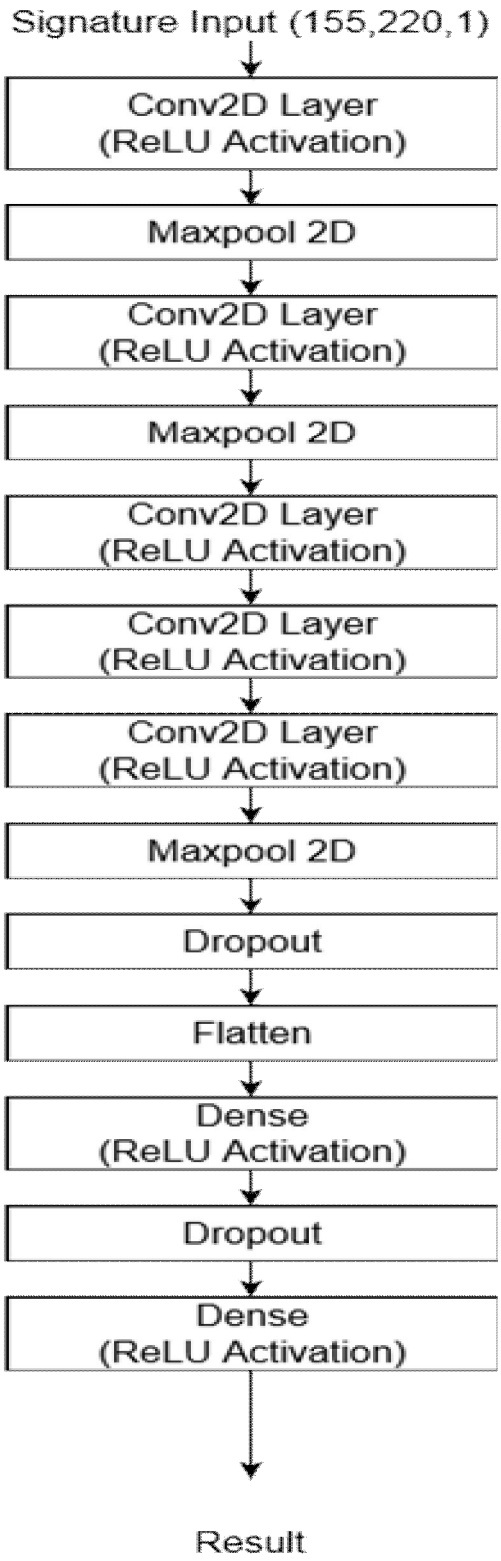


Fig. 6 Architecture of SNN

D. SigNet Model

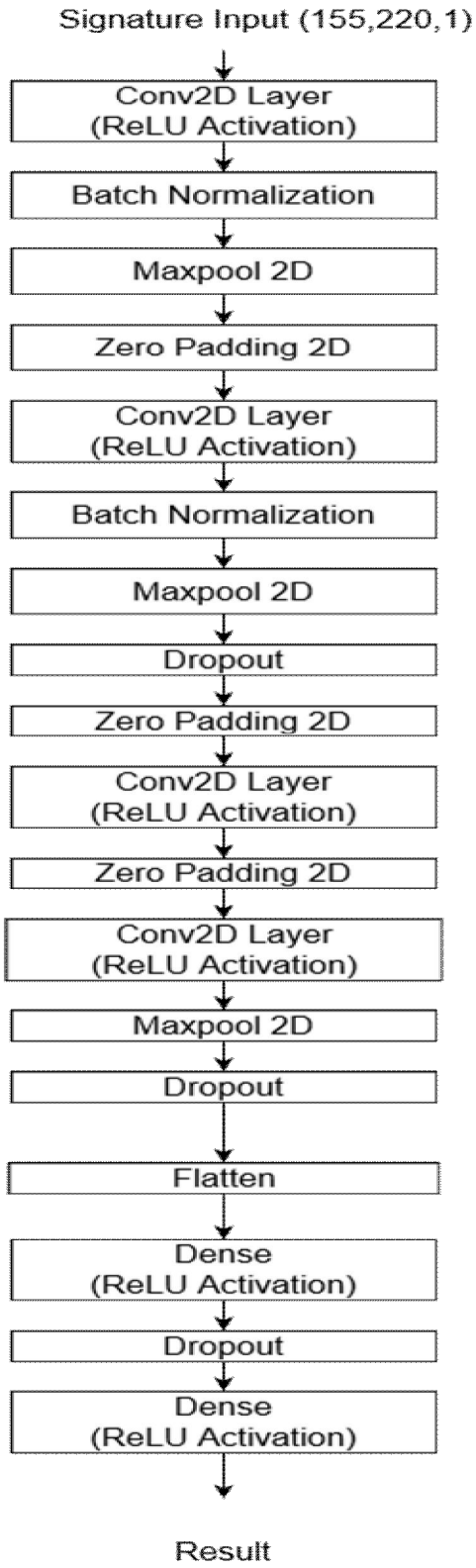


Fig. 7 Architecture of SigNet

VII. RESULTS

A. *CNN Model*

For the CNN, the Adam optimizer was used, with a learning rate of 3e-4 and the sparse categorical crossentropy loss, trained for 50 epochs.

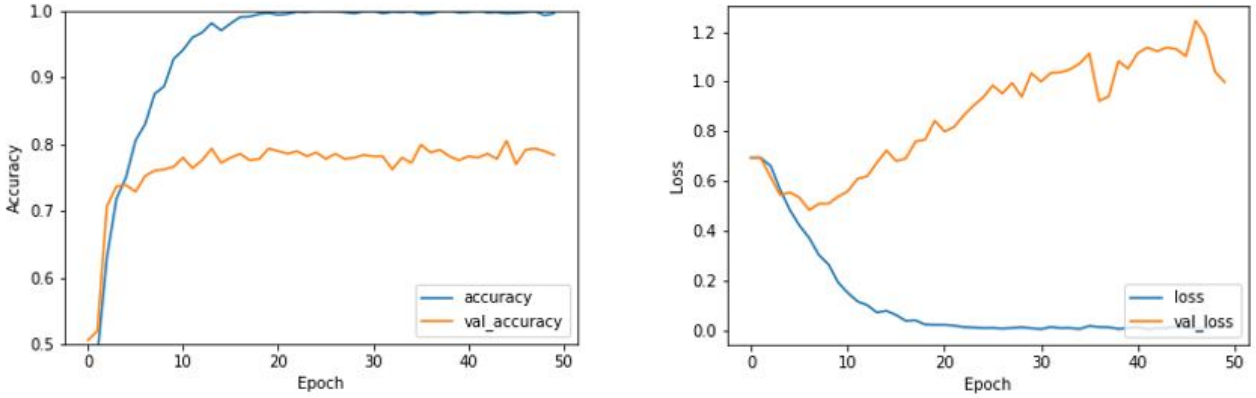


Fig. 8 Accuracy and Loss of CNN

B. *VGG16 Model*

For the VGG16, the Adam optimizer was used, with a learning rate of 3e-4 and the binary crossentropy loss, trained for 50 epochs.

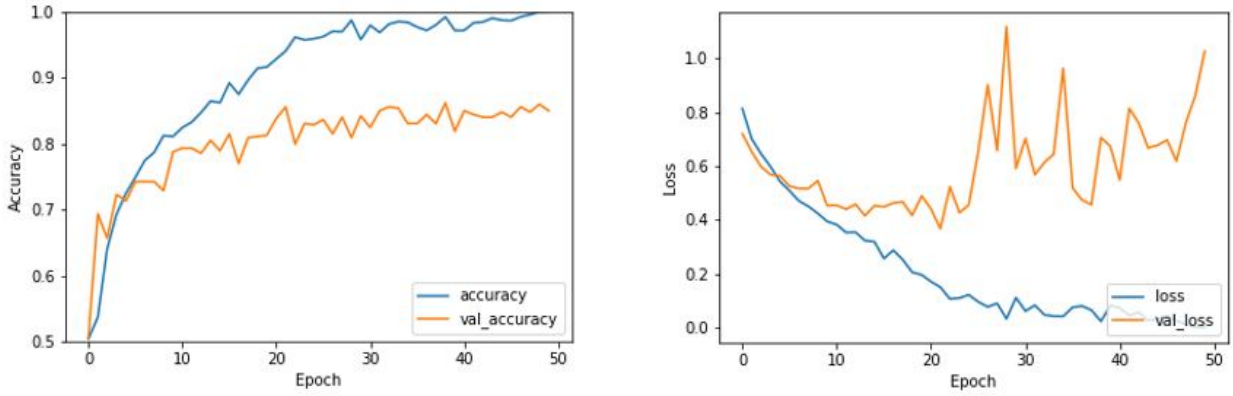


Fig. 9 Accuracy and Loss of VGG16

C. *SNN Model*

For the SNN, the Adam optimizer was used, with a learning rate of 3e-4 and the contrastive loss function, trained for 50 epochs.

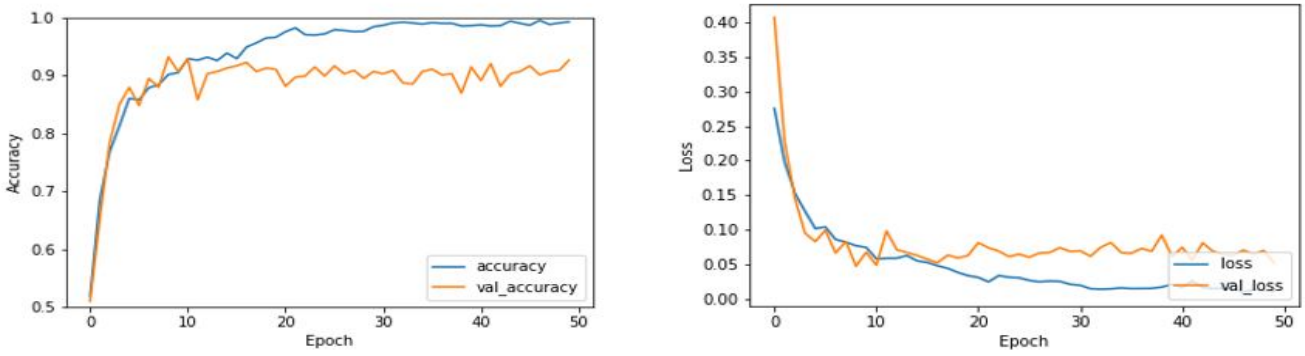


Fig. 10 Accuracy and Loss of SNN

D. SigNet Model

For the SigNet, the RMSprop optimizer was used, with a learning rate of 1e-4 and the contrastive loss function, trained for 50 epochs.

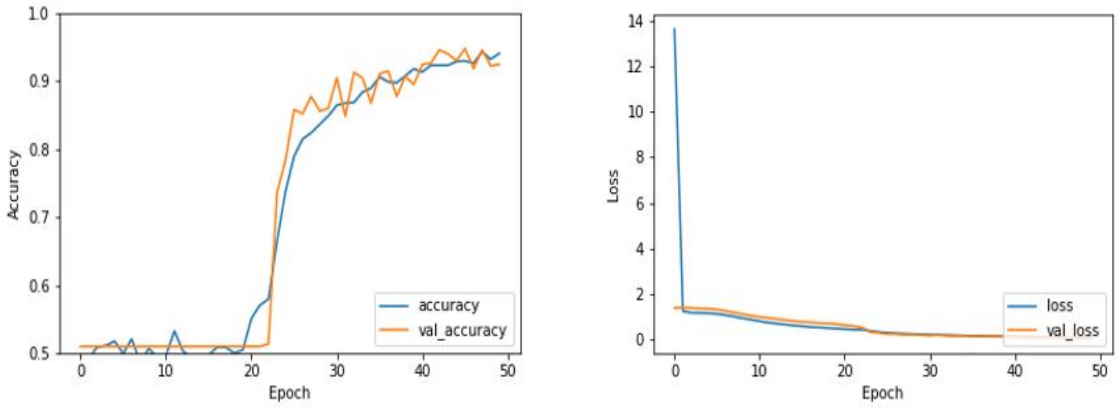


Fig. 11 Accuracy and Loss of SigNet

After training and evaluating the models, we have achieve the following accuracy in detecting signature forgery, the testing set was not used during training or validation.

Accuracy Table

Model	Training Accuracy	Validation Accuracy	Testing Accuracy
CNN	100%	78.32%	82.03%
VGG16	100%	84.96%	83.59%
SNN	99.35%	92.57%	92.38%
SigNet	94.01%	92.38%	90.23%

Fig. 12 Accuracy Table

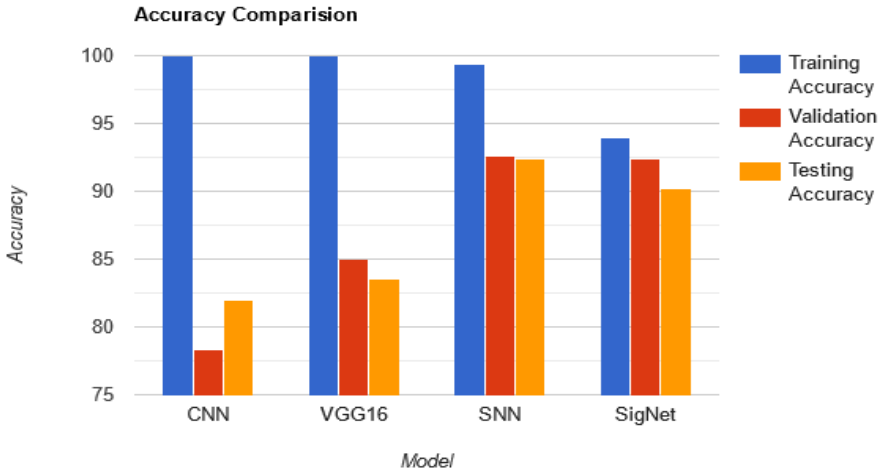


Fig. 13 Accuracy Bar Graph

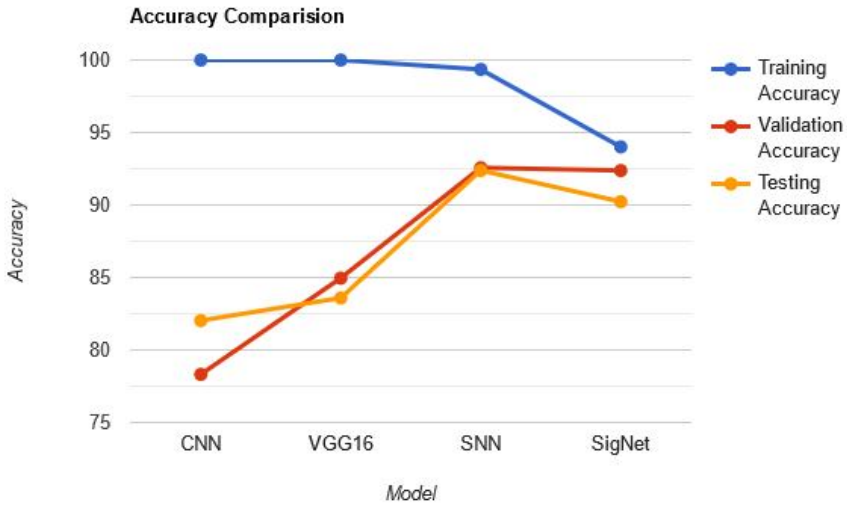


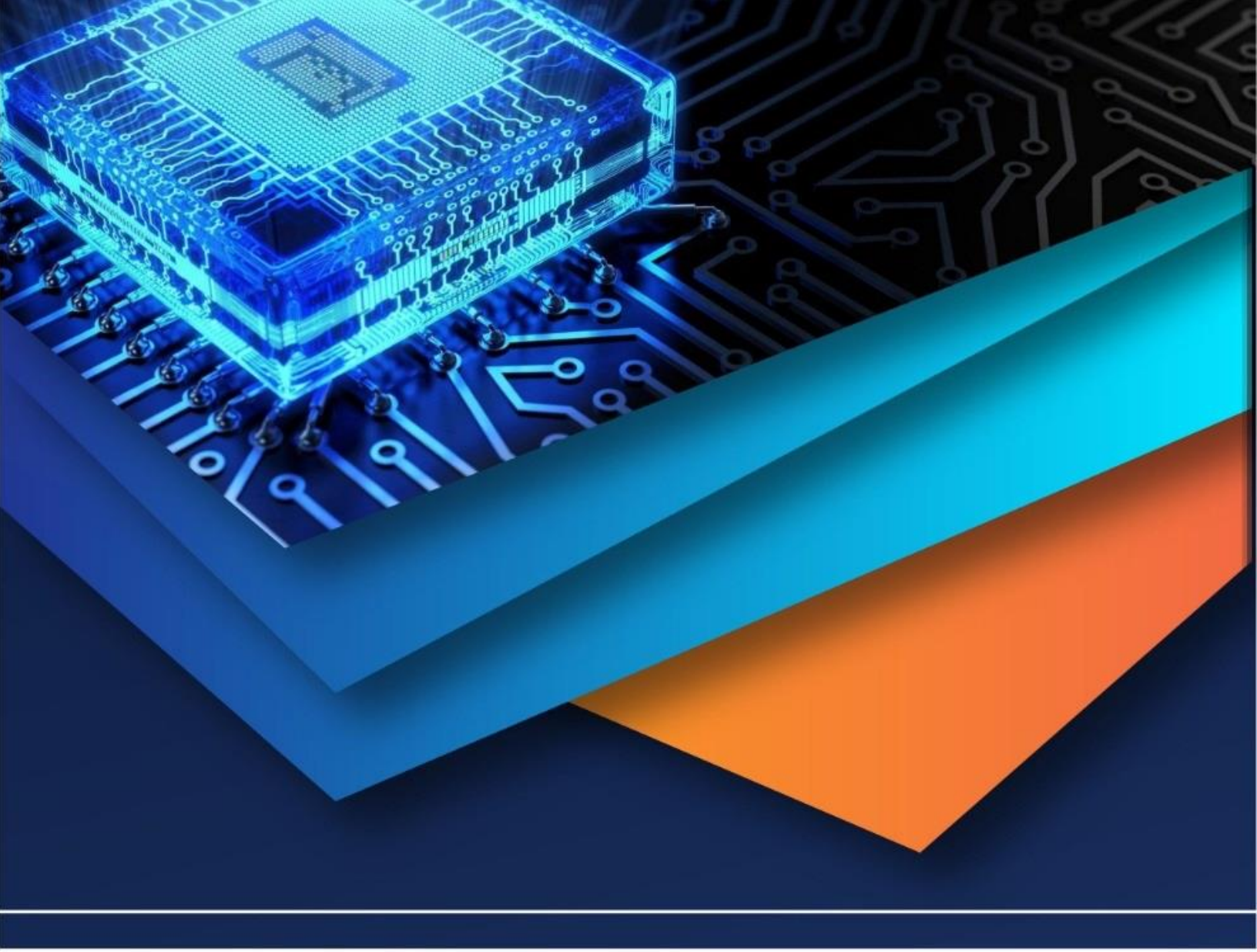
Fig. 14 Accuracy Line Graph

VIII. CONCLUSION

In this study, we have experimented with four signature verification models: a custom CNN (Convolution Neural Network), VGG16, a custom SNN (Siamese Neural Network), and SigNet architectures, respectively. The models were trained on the CEDAR dataset. With the results obtained, we can conclude that Siamese Neural Networks (SNN) are more efficient and produce higher accuracy than a Convolution Neural Network (CNN). With multiple rounds of experimentation, we have verified the accuracies and hence can conclude that the custom SNN architecture proposed in this study has achieved a better result than SigNet in our test while having fewer parameters. Despite the high accuracy produced by the models in this study, many techniques can be used for optimising the data, such as data augmentations, regularisation, etc. More data samples can be used to further train the model to improve its accuracy. Further studies can be conducted using highly optimised data and using better architectures such as VGG19 for this problem domain.

REFERENCES

[1] Kshitij Swapnil Jain, et al. “HANDWRITTEN SIGNATURES FORGERY DETECTION” (2021). International Research Journal of Engineering and Technology (IRJET) Volume: 08 Issue: 01 | Jan 2021
[2] Kiran, Lakkoju Chandra, et al. "Digital signature Forgery Detection using CNN." (2021).
[3] Raj Balsekar, et al. "OFFLINE SIGNATURE FORGERY DETECTION USING CONVOLUTIONAL NEURAL NETWORK", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.7, Issue 5, page no.13-18, May-2020.
[4] Alajrami, Eman, et al. "Handwritten signature verification using deep learning." International Journal of Academic Multidisciplinary Research (IJAMR) 3.12 (2020).
[5] Dey, Sounak et al. “SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification.” ArXiv abs/1707.02131 (2017): n. pag.
[6] S. Jain, M. Khanna and A. Singh, "Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 481-486, doi: 10.1109/ICCCIS51004.2021.9397114.
[7] S. M. A. Navid, S. H. Priya, N. H. Khandakar, Z. Ferdous and A. B. Haque, "Signature Verification Using Convolutional Neural Network," 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), 2019, pp. 35-39, doi: 10.1109/RAAICON48939.2019.19.
[8] A. Rateria and S. Agarwal, "Off-line Signature Verification through Machine Learning," 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, pp. 1-7, doi: 10.1109/UPCON.2018.8597090.
[9] A. Foroozandeh, A. Askari Hemmat and H. Rabbani, "Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning," 2020 International Conference on Machine Vision and Image Processing (MVIP), 2020, pp. 1-7, doi: 10.1109/MVIP49855.2020.9187481.
[10] Jagtap, A.B., Sawat, D.D., Hegadi, R.S. et al. Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). Multimed Tools Appl 79, 35109–35123 (2020). https://doi.org/10.1007/s11042-020-08857-y



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY