SIGNATURE VERIFICATION USING NEURAL NETWORKS

TEAM GUIDE:
Mrs.Jananee J
Head of the Department Biomedical Engineering

TEAM MEMBERS:

BINCY M JACOB [1RG19BM006] MOHAMMED NIHAL [1RG19BM017] RHIYA ELIZABETH ROJI [1RG19BM022]VISHNU [1RG19BM032]

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University, Belgaum)Cholanagar, R. T. Nagar Post, Bengaluru-560032 DEPARTMENT OF BIOMEDICAL ENGINEERING

ABSTRACT

Signatures are predominantly used to verify an individual's authenticity. In this project we present new improved off-line signature verification system using global and texture features of signatures.The proposed technique in this research will assist individuals in characterizing signatures in order to check whether they are genuine or forged. In this proposed project an algorithm to validate signatures using CNN (Convolution neural network), Siamese neural network and VGG16 (Visual geometry group of transfer learning) models in our system. Authentic and competent forging signatures are used to test the approach. Results obtained by our proposed algorithm are more efficient than most of the existing techniques.

INTRODUCTION

Person identification is being one of the most complicated tasks. Signature and fingerprint have played the major role in reducing the burden on the same. In many real time scenarios like employment, defense security clearance, fraud detection, and so on, signature and fingerprint playan effective role in identifying the person and validating. Authentication, in computing means a process of verifying the identity of a person. The increase in the need of security for the data and to avoid the illegal activities, the authentication has been the much-needed process in real time scenario. The Multi-factor authentication is a method of authenticating a person with comprising of more than two factors. Considering the strength of authentication, signature and fingerprint arethe most prominent parameters in the field of biometric authentication.

The system is developed for validation of signature and fingerprint on an embedded platform usingConvolution Neural network (CNN). The signature of the individual is captured using webcam. These images will be pre-processed and used as inputs to recognition algorithm using a neural a network. The neural network model is a trained with an 80 percent of the images and remaining 20 percent are used for testing. The necessary action is taken only if the accepted biometric inputs are authenticated by the system. The signature captured by the camera needs to be pre-processed before training the data. The most accurate systems almost always take advantage of dynamic features like acceleration, velocity, and the difference between up and down strokes In the past decade a bunch of solutions has been introduced, to overcome the limitations of signature verification and to compensate for the loss of accuracy. Most of these methods are:

1. Artificial Intelligence
2. Neural networks
3. Machine Learning.

A signature is one of the many techniques used in the authentication of a person. In today's life, signatures play an important role in validating whether a sign is forged or real, which raises legalissues about a person's right. Person verification relies heavily on biometrics. A person's identity is verified using two types of attributes: biological (such as iris, fingerprint, and face) and behavioral (such as gait, voice, and writing signatures). A handwritten signature is a well-known and commonly utilized behavioral trait for the authorization of critical documents.

OBJECTIVE

In this project we verify the Signature in the given database using the neural network algorithms.And matching the performance of all the algorithms such convolution neural network (CNN), , Siamese, visual geometric group Transfer Learning, To finally determine the best algorithm for the Signature verification.

PROBLEM STATEMENT

As we have seen the importance of signature in authenticating and verifying a person. Like anyone, one can access any data belonging to that person and use that data to commit crimes and forge theirsignatures. For this reason, we try to build a model to verify whether a viewer's signature isgenuine or fake. The models used in this project are:

1. Convolutional Neural Network
2. Siamese Model
3. Transfer Learning

LITERATURE SURVEY

1. Maltoni D, Maio D, Jain A K and Prabhakar(S), has proposed how significant efforts arecontinuously being made in designing new fingerprint recognition algorithms both in academic and industrial institutions. However, the accuracy of each algorithm is usually evaluated on relatively small databases. An evaluation on small databases makes the accuracy highly estimates data dependent; as a result, they do not generalize well on fingerprint images captured in different applications and different environments. A sharable large database of fingerprints (thousands or tens of thousands of images) is required to evaluate and compare various fingerprint recognition algorithms due to the very small error rates that must be estimated.

2. Kai Cao and Anil K Jain , has proposed the model which uses set of minutia points to be the most distinctive feature for fingerprint representation and is widely used in fingerprintmatching. It was believed that the minutiae set does not contain sufficient information to reconstruct the original fingerprint image from which minutiae were extracted. However, recent studies have shown that it is indeed possible to reconstruct fingerprint images from their minutiae representations. Reconstruction techniques demonstrate the need for securing fingerprint templates, improving the template interoperability, and improving fingerprint synthesis.

3. Taraggy M Ghanim and Ayman M Nabil ,explained how Signature verification and forgery detection is a challenging field with a lot of critical issues. Signatures forgery drives cooperates and business organizations to huge financial loss and affects their security reputation. Highly accurate automatic systems are needed to prevent this kind of crimes. This paper introduces an automatic off-line system for signature verification and forgery detection. Different features were extracted and their effect on system recognition ability was reported. The computed features include run length distributions, slant distribution, entropy, Histogram of Gradients features (HOG) and Geometric features. Finally, different machine learning techniques were applied on the computed features: bagging tree, random forest and Support Vector Machine (SVM).

4. Kritika Vohra, et.al proposed a model where Signature is considered as a mark that an individual write on a paper for his/her identity or proof. It is used as a unique feature foridentifying an individual. There are chances of signature getting forged. In this paper,

identification of signature as genuine or forged is done using two approaches. First approach is using SVM and second is using CNN. For SVM, pre-processing of signatureimage is done, and feature extraction is performed. In the second approach, signature image is pre-processed, CNN is used to classify signature as genuine or forged and accuracy is determined. Dataset used here is ICDAR Dutch dataset along with 80 signatures taken from 4 people. Dutch dataset consists of 362 signature images and signature images taken from 4 people consists of 10 genuine and 10 forged signatures which sums to 442 signature images.

5. Luiz G. Hafemann, Robert Sabourin proposed Automatic Offline Handwritten Signature Verification has been researched over the last few decades from several perspectives, using insights from graphology, computer vision, signal processing, among others. Despite the advancements on the field, building classifiers that can separate between genuine signatures and skilled forgeries (forgeries made targeting a particular signature) is still hard. We propose approaching the problem from a feature learning perspective. Our hypothesis is that, in the absence of a good model of the data generation process, it is better to learn the features from data, instead of using hand-crafted features that have no resemblance to the signature generation process.

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- Hard Disk : 250 Gb
- Floppy disk
- Monitor
- Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP and above
- Coding Language : Python
- Software used : Anaconda, Jupyter notebook

Select items to perform actions on them.

envs
examples
pkgs
public
Welcome.txt

Fig: Jupyter Notebook window

Fig: Jupyter Notebook icon

METHODOLOGY

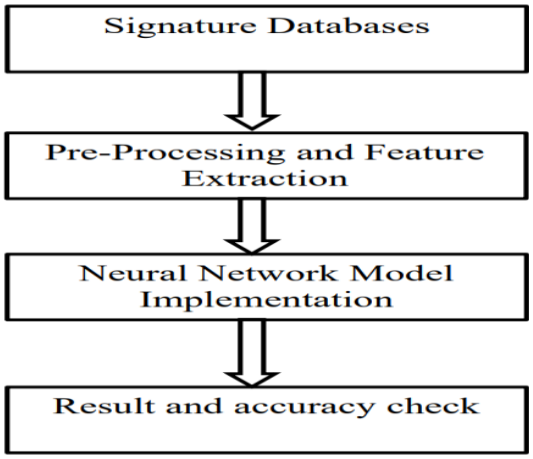

Signature Databases
Pre-Processing and Feature Extraction
Neural Network Model Implementation
Result and accuracy check

Figure- Methodology

➢ Signature Database

Signature databases are structured sets of collected signatures from a group of individuals that areused either for evaluation of recognition algorithms or as part of an operational system. Signature databases can be collected from Kaggle, Cedar, etc.

➢ Pre-Processing and feature extraction

After the database being collected these images needs to be pre-processed. In this step the featuresare extracted from the pre-processed image. Feature extraction refers to the process of transforming raw data into numerical features that can be processed while preserving the information in the original data set. Signature Databases Pre-Processing and Feature Extraction Neural Network Model Implementation Result and accuracy check Signature Verification using

Neural Networks Signature features represent magnitudes that are extracted from digitized signature samples, with the aim of describing each signature as a vector of values. The extraction and selection of optimum signature features is a crucial step when designing a verification system.

➢ Neural network model implementation

In this step the pre-processed data and features extracted are implemented in different models such as MLP, CNN, Siamese, VGG-16(TL)

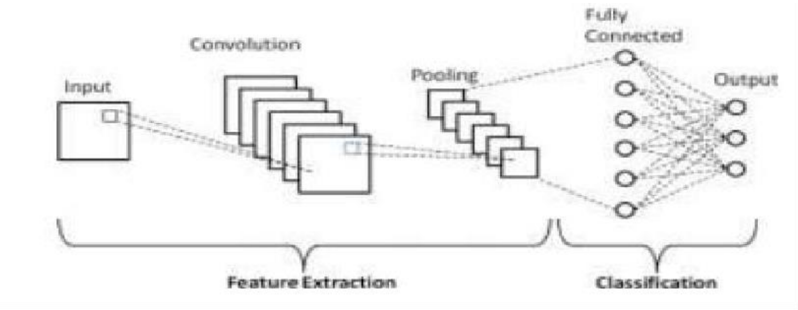
➢ Result and Accuracy Check

Once the signature is matched with the database using the different models the signature is verifiedwhether it is genuine or forged along with accuracy check.

IMPLEMENTATION

2. Convolutional Neural Network:

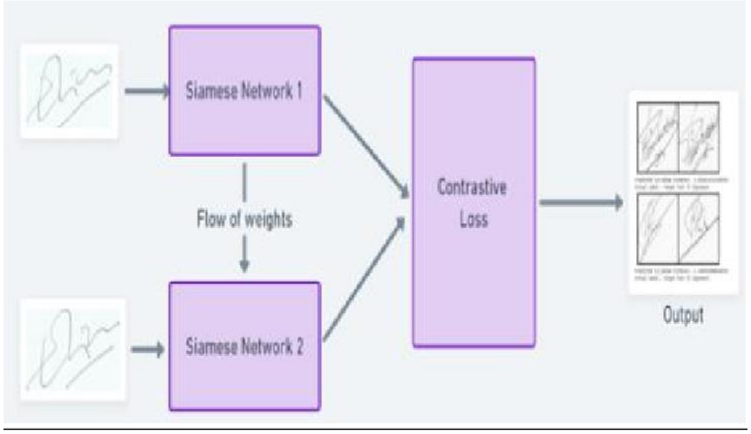
A Convolutional Neural Network, also known as CNN, is a class of neural networks that specializes in processing data that has a grid-like topology, such as an image. Their applications range from image and video recognition, image classification, medical image analysis, computer vision and natural language processing. The term 'Convolution" in CNN denotes the mathematical function of convolution which is a special kind of linear operation where in two functions are multiplied to produce a third function which expresses how the shape of one function is modified by the other. In simple terms, two images which can be represented as matrices are multiplied to give an output that is used to extract features from the image.



3. Siamese Networks:

A Siamese Neural Network is a class of neural network architectures that contain two or more identical subnetworks. 'identical' here means, they have the same configuration with the same

parameters and weights. Parameter updating is mirrored across both sub-networks. It is used to find the similarity of the inputs by comparing its feature vectors, so these networks are used in many applications.



4. Transfer Learning

- It's a machine learning (ML) algorithm. We are using VGG-16 to classify our dataset.
- VGG-16 mainly has three parts: convolution, Pooling, and fully connected layers.

- VGG-16 is neural network which includes 16 deep layers, we could create this neural network by our self – and from scratch – then find out the best hyper parameters to finallytrain it.

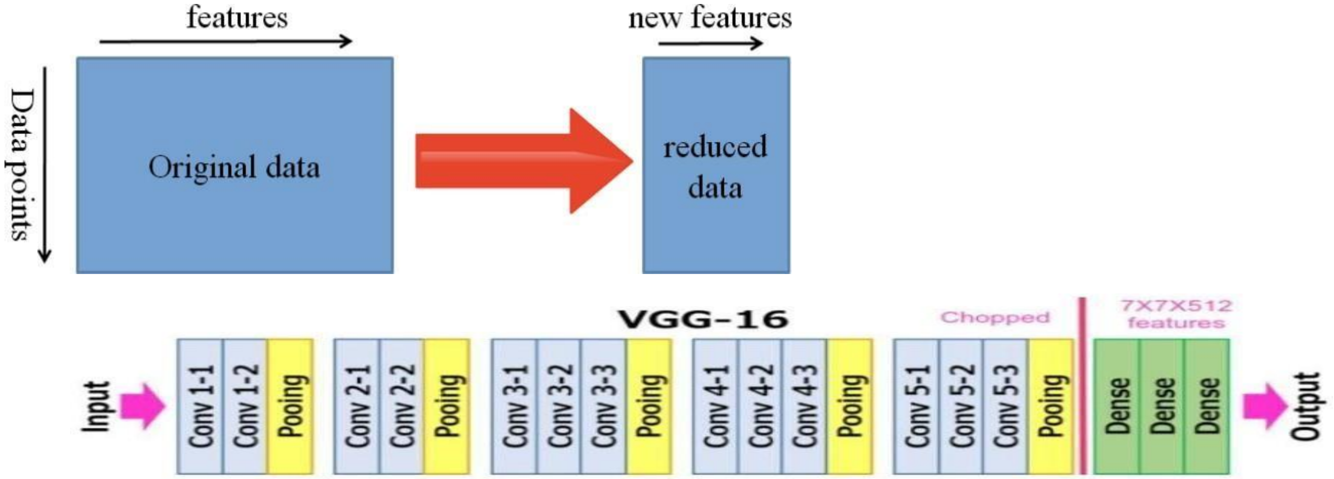


Fig Layers in VGG-16

RESULTS

1. Results of CNN mode

We used the Kaggle dataset of 69 people for this model, with each person having 12 real and 12 fake images of signature. The model does most of the work here, extracting all of the characteristics. The model is now fitted after being trained for 20 iterations. As illustrated in Figures , a graph is shown for training and validation accuracy as well as training and validation loss for the model. Finally, using the Kaggle dataset, the model produces the result based on the testing dataset our and achieves a 96.39 percent accuracy

Fig 5.2.1(a) :CNN model accuracy plot

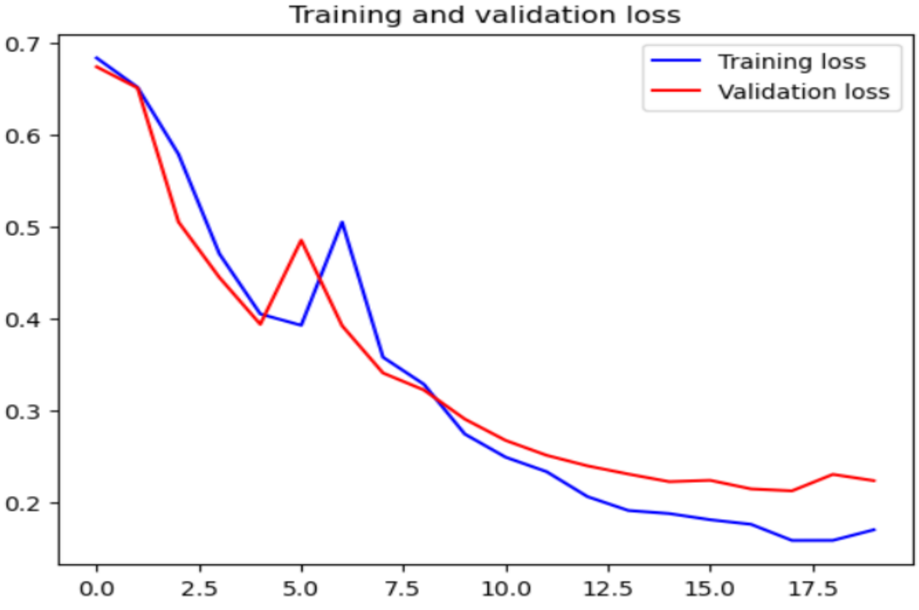
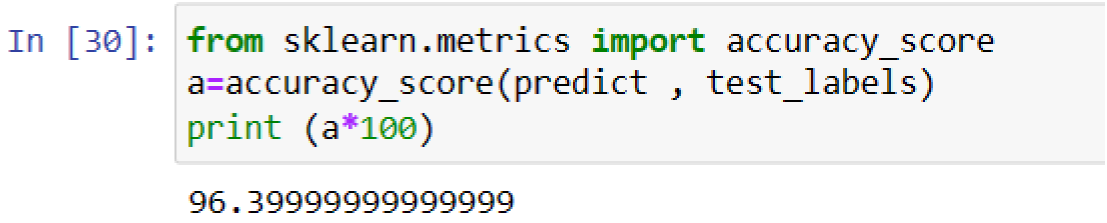


Fig5.2.1(b) :CNN model loss plot

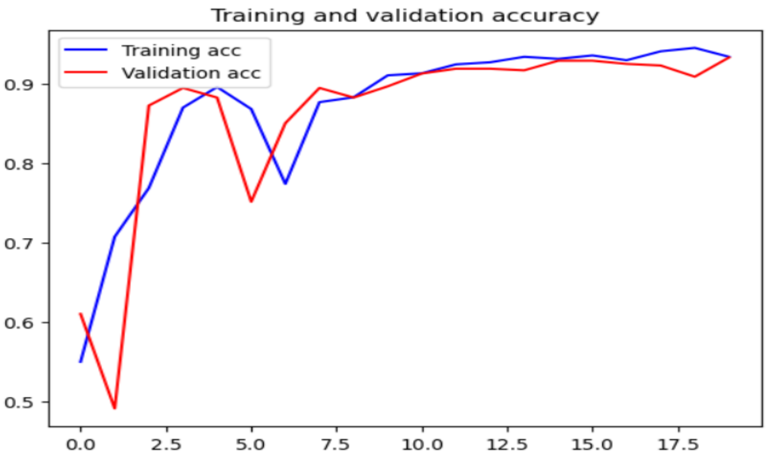


```
In [30]: from sklearn.metrics import accuracy_score
         a=accuracy_score(predict , test_labels)
         print (a*100)

         96.39999999999999
```

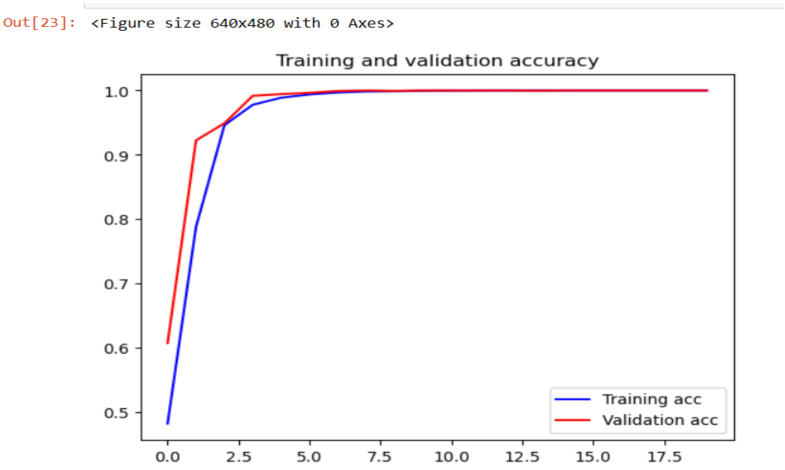
Fig5.2.1(c): Accuracy of CNN model

.



2. Results of Siamese mode

We use the same Kaggle dataset but instead of 69 people signature, half of the dataset is taken i.e., 35 peoples' signature with 12 genuine and 12 forged images of signature. This dataset is divided into training and testing dataset, the model is trained through all the layers and fitted. Graphs are plotted for training and validation accuracy as well as training and validation loss for the model as shown in Fig. Finally, Siamese model achieves an accuracy of 50% out of 50% and while considering it as a 100% it gives an accuracy of 100% as showing Fig . Now, load the model and test it on unseen images.



```
Out[23]: <Figure size 640x480 with 0 Axes>
```

Fig 5.2.2(a) :Siamese model accuracy plot

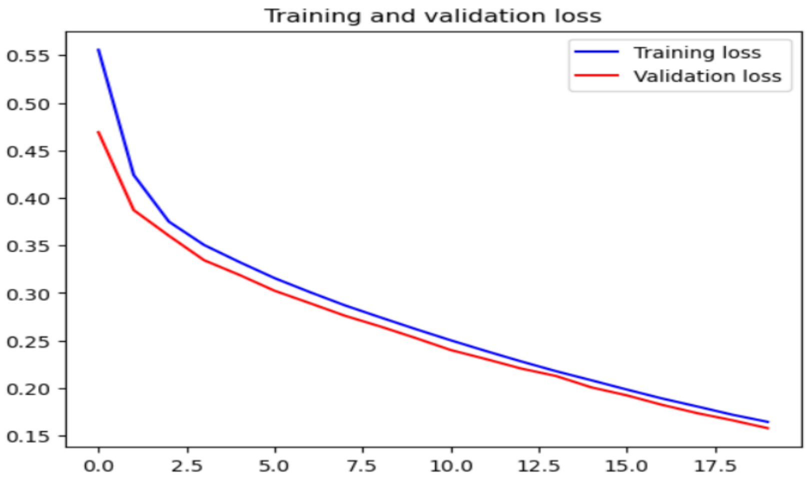
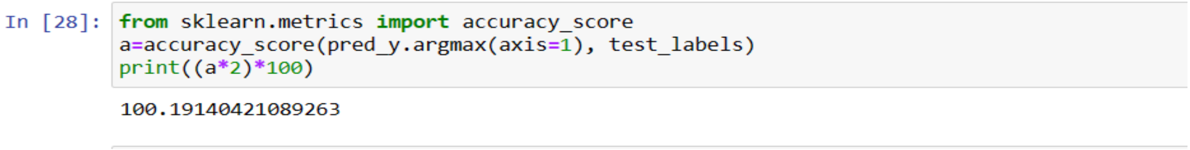


Fig 5.2.2(b)Siamese model loss plot



```
In [28]: from sklearn.metrics import accuracy_score
         a=accuracy_score(pred_y.argmax(axis=1), test_labels)
         print((a*2)*100)

         100.19140421089263
```

Fig5.2.2(c): Accuracy of Siamese model

3. Results of Transfer Learning of VGG-16 model

In Transfer Learning VGG-16 model, modified Kaggle dataset is used which is extracted from the pre-trained model to reduce the original dataset to increase the accuracy of the output. As we can see a model is built where the original dataset undergoes training through all the layers and then the obtained reduced dataset is trained in VGG-16 model. Graphs are plotted for training and validation accuracy as well as training and validation loss for the model as shown in Fig. Finally transfer learning model achieves an accuracy of 97% as shown in Fig .

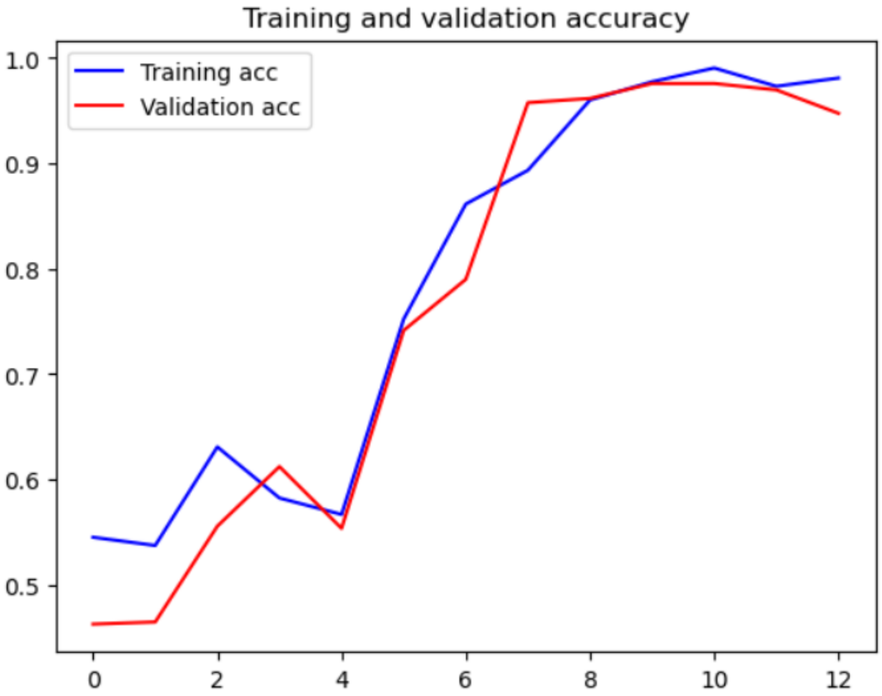


Fig 5.2.3(a)VGG-16 model accuracy plot

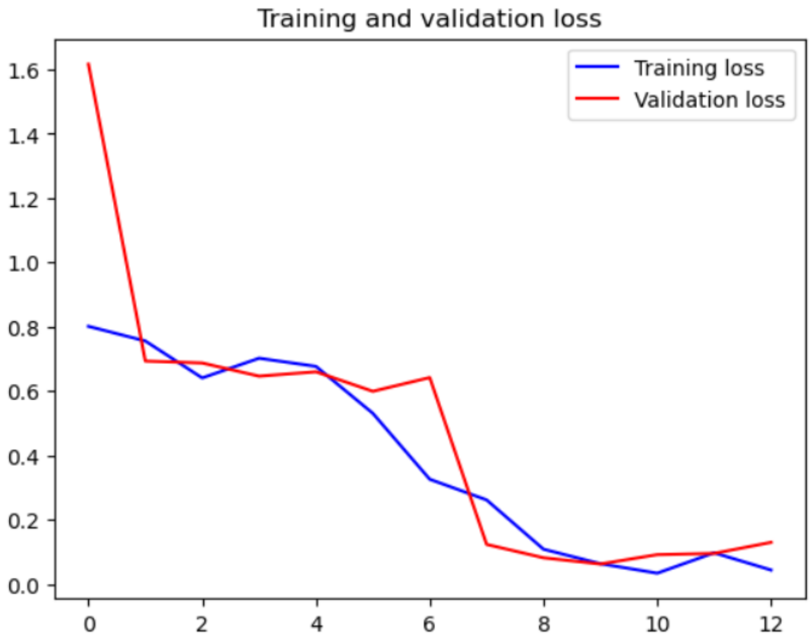
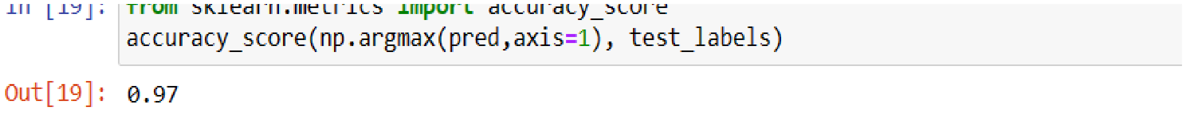


Fig5.2.3(b):VGG-16 model loss plot

Fig5.2.3(c): Accuracy of VGG-16 model



```
In [19]: from sklearn.metrics import accuracy_score
         accuracy_score(np.argmax(pred,axis=1), test_labels)

Out[19]: 0.97
```

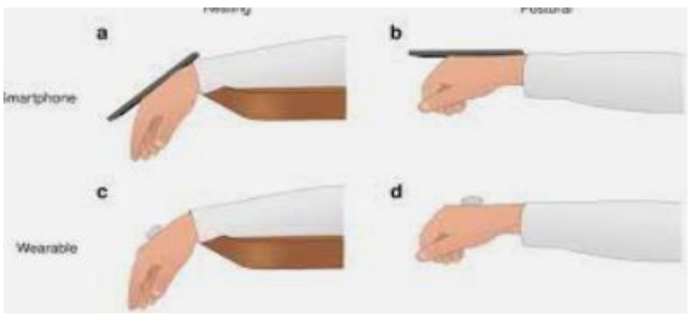
CONCLUSION

Neural networks have been developing very rapidly in this 21st century. In our present day, we have seen several advantages and disadvantages of Neural Networks which has had both achievements as well as problems encountered in the course of their use. Signature verification is widely used in many applications such as Banking, Aadhaar card verification etc. In the proposed work signature verification using CNN model is developed to measure the performance parameter. The pre-processing is carried out to resize the image. The features like Eccentricity, Centroid, Solidity, Skew and Kurtosis are measured then CNN module is used to measure the accuracy. For CNN model the accuracy is 96.39% is validated. The Siamese model, on the other hand, was built to reduce the current dataset in half with an accuracy of 100 percent out of 100 percent. All of the models were highly accurate, yet we tried to construct the Transfer Learning VGG-16 model, which decreased the work in half by taking already processed data from a sequential model and training it with VGG-16, resulting in a 97% accuracy. Thus Siamese model was the breakthrough compared to all the other models and has the highest accuracy possible.

APPLICATIONS

1. Behavioural traits

a signature can be used to detect any form of muscle tremor or any issues with the hand muscle
. it can also be used for detection of Parkinson’s disease through an individuals signature.



2. Biometric

signature is the oldest form of biometrics and is used still this day. It is a form of biometric is many organisations.

3. Forensic

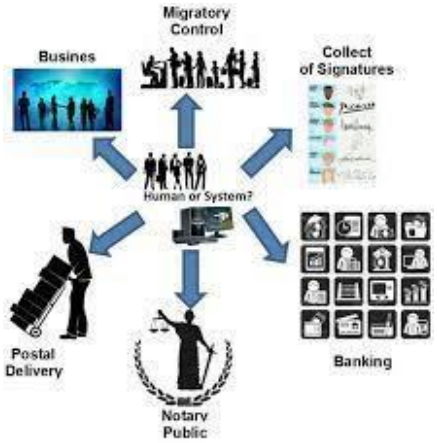
A signature verification forensic test is used to find out if the signature on a document is faked (forged) by someone.

4. Banking and financial services

Banks and financial service institutions still put their trust in signature verification and use it for customer identification, identity verification, and authorization.

5.Government services

From lawmakers to government officials and citizens accessing government services have to sign papers to verify their identity or authorize a transaction.



REFERENCES

[1] Maltoni, D., Maio, D., Jain, A. K. and Prabhakar, S, “Handbook of Fingerprint Recognition”,2e, ISBN: 978-1-84882-2535, Springer, 2015.

[2] Kai Cao and Anil K. Jain, “Learning Fingerprint Reconstruction: From Minutiae to Image”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, 104119, January 2015.

[3] Taraggy M Ghanim and Ayman M Nabil, “Offline Signature Verification and Forgery Detection Approach”, 13th International Conference on Computer Engineering and Systems, 2018.

[4] Kritika Vohra, “Signature Verification Using Support Vector Machine and Convolution NeuralNetwork”, 2021.

[5] Luiz G. Hafemann, Robert Sabourin, “Writer-independent feature learning for Offline Signature Verification using Deep Convolutional Neural Networks”, International JointConference on Neural Networks, 2016

[6] S V Bonde, Pradeep Narwade, “Offline Signature Verification Using Convolutional Neural Network”, 6th International Conference on Signal Processing and Communication, 2020.

[7] Hurieh Khalajzadeh, Mohammad Mansouri, and Mohammad Teshnehlab, “Persian Signature Verification using Convolutional Neural Networks”, International Journal of Engineering Research and Technology Vol. 1 Issue 2, 2012.

[8] Vahab Iranmanesh, Sharifah Mumtazah Syed Ahmad, “Online handwritten signature verification using neural network classifier based on principal component analysis”, 2014.

[9] Shayekh Mohiuddin Ahmed Navid and Shamima and others, “Signature Verification Using a Convolutional Neural Network”, IEEE International Conference on Robotics, Automation, Artificial intelligence, and Internet-of-Things, 2019.

[10] V A Bharadi and H B Kekre. “Off-Line Signature Recognition Systems. International Journal of Computer Applications”, 1(27):48–56, Published by Foundation of Computer Science, 201