IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125298

HANDWRITTEN SIGNATURES FORGERY DETECTION

Prof.Netravathy V[1], Spoorthy Udayakumar Kulkarni[2]

Assistant Professor, Dept of CSE, BIT, Karnataka, India[1]

Student, Dept of CSE,BIT, Karnataka, India[2]

Abstract: Signature plays a very import role in sectors like banking, finance, Passport, Driving License, legal documentation etc. Signature varies from person to person and may be unique each time. Some time signatures may seem similar if the people have same name. But the features may still vary. Now a days there are problems like identity theft, fake ids, hacking etc.

To reduce such type of issue, this project is focused on developing a system to detect such theft and to know and verify if the signature is real or fake, from the data sets using CNN and deep learning.The reason for using CNN and deep learning is that, the signature can vary with change in personalities and behaviour. With deep learning we can train the data sets and increase the accuracy of the detection. The Signatures can be hand written or signed online, depending on the type of signature the process takes place. Here we are referring to few papers which implement the project using both online and offline methods based on deep learning models. Using these we can try and achieve a better accuracy

Keywords: Signature, CNN, Forgery, Authentication, Deep learning

I. INTRODUCTION

In the present scenario, Signatures play a very important role in keeping one's security, unlike passwords, signatures cannot be changed, they also need the verification that needs to be done. The signature is a unique form of a person's name. But the signatures can be identical because people can have same names. Hence it tries to act as a unique identifier. Passwords can be changed or forgotten because it needs to be unique for everyone and is considered very important for the verification purposes. Whether the signatures or online or offline they legally represent a particular person. Science signatures are used widely all over, some people my try to copy people's signature or forge them for their own benefit. That is whya very good signature forgery detections are required.

A forged signature is a kind of signature that is not genuine. There are two types of signature verifications they are: offline signatures and online signatures. In offline signatures we take the picture of hand signed signature and give it for verification. But in case of online verification writing pad is connected to the computer and can be signed digitally.

Foorgery detection using online method by tracking trajectory and variations which are recorded with time as the signature is being done, and in offline signature it is an authentication method where it usually uses dynamics of a person's handwritten signature to measure and analyze the process of signing. For the forgery detection we suggest a method for training models using Support Vector Machine(SVM), which are used to do both linear and non-linear classifications using kernels. SVMs do the work of extracting data from particular types, making them a successful systems for recognition works. It also takes the help of K-means method to obtain similar signature images.

We use following methods in this paper:

- Pre-processing technique to simplify signature verification.
- K-means algorithm based model for SVM based signature verification.
- A Support Vector Classifier (SVC) for signature forgery detection.

II. OBJECTIVE

The Objective of the Software is:

- To verify and check if the given Signature is Original or Fake.
- To Understand the characteristics of a Signature.
- To implement the system

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125298

III. LITERATURE SURVEY

Ruiz et al [5], (2020), have proposed the use of Siamese Neural Networks for performing the task of forgery detection in offline signature verification process with a writer independent context. Additional training is not required for adding new signs for verification. Further, three types of data were analysed so as to increase the amountof samples and variability needed for training the deep neural network. The datasets used were the GAVAB dataset, a proposal of compositional synthetic signature generation from shape primitives and the GPDSSynthetic dataset. The first two approaches can be categorised as on-demand approaches and can produce infinitely many signatures which are synthetic in nature. In the givenapproach, initially training is done by Siamese Neural Networks using the first mentioned dataset. When original and synthetic signatures are mixed it leads to the best result for training. Further few other datasets such as GPSythetic, MCYT, Sigcomp11 etc, were also used to test and create a general model.

Xiao et al [4], (2020), have explored a two-part splicing forgery detection method. The two parts consist of a coarse- to-refined convolutional neural network(C2RNet) and a diluted adaptive clustering network. In the proposed model the differences in the image are found by cascading a coarse CNN and refined CNN (C-CNN and R-CNN respectively). The cascading results in making scales where theimage has been tampered finding difference in their properties. The computational complexity of the whole model is reduced by an imagelevel CNN rather than using a patch level CNN into C2RNet. Since the difference in properties is compared therefore it results in stabilised results. It was found that the proposed method produces better results than the already existent splicing techniques for forgery detection even in conditions of attack. However, the size of these datasets restricts training and hence optimal results are not yet obtained from this proposed model.

Gideon et al. [23], (2018), have proposed a method for the classification of offlinesignatures as genuine or forged. The database of signatures is collected, image processing techniques such as RGB to grayscale, removal of noise, grayscale to bitmap and resizing arecarried outon images as preprocessing techniques using MATLAB. Thetrainingofthe model is used by Keras library in python with TensorFlow backend to implement Convolutional Neural Networks. The dataset used is a collection of 6000 signatures with 1000 genuine and 1000 forged signatures per subject. High accuracy was obtained on splitting the data as 8:2 ratio of training and test data which decreases on making the ratio as 7:3 and 6:4. The drawback was that the structure of the fully connected layer is not optimal. Future work includes deriving a custom loss function to predict the user to which signature belongs and to detect if it is genuine orforged.

Hadjadji et al. [24], (2017), have proposed an Open Handwritten Signature Identification System (OHSIS) for offline handwritten signature identification by using conjointly the Curvelet Transform (CT) and the One-Class classifier based on Principal Component Analysis (OCPCA). Binarization of acquired signature is done as a pre- processing method. CT is explored for feature generation due to its efficient characterization of curves contained into the local orientations within the signature image. While OC- PCA is used for its effectiveness to absorb the high feature size generated by the CT and allows achieving at the same time an open system new combination approach based on Choquet fuzzy integral is proposed to combine multiple individual OHSISs in order to improve the robustness of the OHSIS. Evaluation is done on the basis of Identificationrate which is the number of instances correctly identified to the total number of instances in percentage.

Ooi et al. [28], (2016), have proposed a method to compensate the lack of dynamic information from static signature images through the use of discrete Radon transform (DRT), principal component analysis (PCA) and probabilistic neural network (PNN). Median filter and grey- scaling of images is done to remove noise and minimize databasestorage of images. transforms thetwodimensional images with lines into a domain of possible line parameters. PCA is utilizedhere for feature data compression. Thispaper uses a Probabilistic neural network (PNN) instead of similarity matching concept. A PNN has three layers – pattern layer which has one neuron for each input layer vector in the training set, summation layer which has one neuron for each user class and an output layer which holds the maximum value ofsummation ofneurons toproducethe probability score. The dataset used has 1000 genuine signatures, 500 casual forgeries and 500 skilled forgeries, which were collected from 100 writers and 10 forgers.

Future works include using a large database of signatures with forgeries and a powerful specification of PC support to obtain a more reliable system.

Yilmaz and Yanikoglu [11], (2016), presented a system that uses a score-level fusion of complementary classifiers that use different local features (histogram of oriented gradients, local binary patterns and scale invariant feature transform descriptors), where each classifier uses a feature- level fusion to represent local features at coarse-to-fine levels. For classifiers, two different approaches are investigated, namely global and user-dependentclassifiers.

DOI: 10.17148/IJARCCE.2023.125298

User-dependent classifiers are trained separately for each user, to learn to differentiate that user's genuine signatures from other signatures; while a single global classifier is trained with difference vectors of query and reference signatures of all users in the training set, to learn the importance of different types of dissimilarities.

Blanco et al [8], (2014), observed that biometric verification is increasingly being used ever since the use of mobile has increased and handwritten signatures are perhaps the most common way to carry out this task. This study obtained multiple results from 43 users signing 60 times, which were divided in three sessions and captured in 8 specific devices out of which six were mobile devices and the remaining were made specifically for signature collection. Each session captured 20 signatures per user and stored it in ISO/IEC 19794–7 format. The algorithm applied is a DTW-based algorithm which is particularly useful for mobile environments. Thus, theresultswhichwereobtained were based on interoperability, feedbackandmodalitytests. Theseconclusions will finally help in creatingmoreaccurate models for the purpose of signature verification.

Sigari et al. [19], (2011), have proposed a new method for offline (static) handwritten signature identification and verification based on Gabor wavelet transform. The whole idea is offering a simple and robust method for extracting features based on Gabor Wavelet which the dependency of the method to the nationality of signer has been reduced to its minimal. The advantages of this system is its capability of signature identification and verification of different nationalities; thus it has been tested on four signature dataset with different nationalities including Iranian, Turkish, South African and Spanish signatures.

Bertolini et al [10], (2010), highlighted two important issues of off-line signature verification. The first one regards feature extraction. They introduce a new graphometric feature set that considers the curvature of the most importantsegments, perceptuallyspeaking,ofthesignature.

Hanmandlu etal.[1],(2005), haveidentifiedandproposed a new system for handwritten signature verification. Using the quadtree structure of the histogram template, the paper proposes a new descriptor. The methodology used for the verificationofsignaturesincludesusageofArtificialImmune Recognition System (AIRS). The classifier derives its implementation from a natural immune system. By using AIRS training, new cells are developed which are subsequently recognised by a KNN (k-nearest neighbour classifier). The paper shows 6 KNN classifiers can also be substituted by an SVM (support vector machine) in order to getrobustand better classification. Threedatasetsthatwere usedtoperform experimentson: namelytheMYCT75,GPDS- 300 and GPDS-4000. Using the AIRSVM gives better results as compared to AIRS or SVM classifier.

a. BACKGROUND

Signature forgery in legal documents, Passports, Doctor's prescriptions, Bank checks and so on can lead to serious consequences. For such cases signature verification acts as a important application in the field of bio metrics. These bio metrics measures human behaviour and act accordingly to construct the recognisation system. Such systems are useful in achieving high sense of security.

b. MOTIVATION

Forged signatures were often manually detected by experts, still the accuracy was not up to the point.There are many difficulties involved in mannual forgery detection. Sometimes professionalism also does not matter if the forgers are really good at forging. The Automatic recognition comes in handy in such cases, as they play effective role in verifying signatures with very high accuracy and also in differentiating between original and forged.

IV. METHODOLOGY

In this project we use Convolutional Neural Network (CNN). To implement the offline authentication methods, we plan to use a convolutional neural network (CNN). Since a CNN can categorise the extracted features from the signature, it is preferable to use a CNN since all offline methods exploit the content-based features and the visual information of the signature.

Convolutional Neural Network

Convolutional neural networks (CNNs) are multi-layer neural networks with deep supervised learning architectures that are rumoured to be capable of extracting features for classification on their own. An autonomous feature extractor and a trainable classifier are the two components of CNN. The feature extractor uses convolution filtering and down sampling to extract features from the input data.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

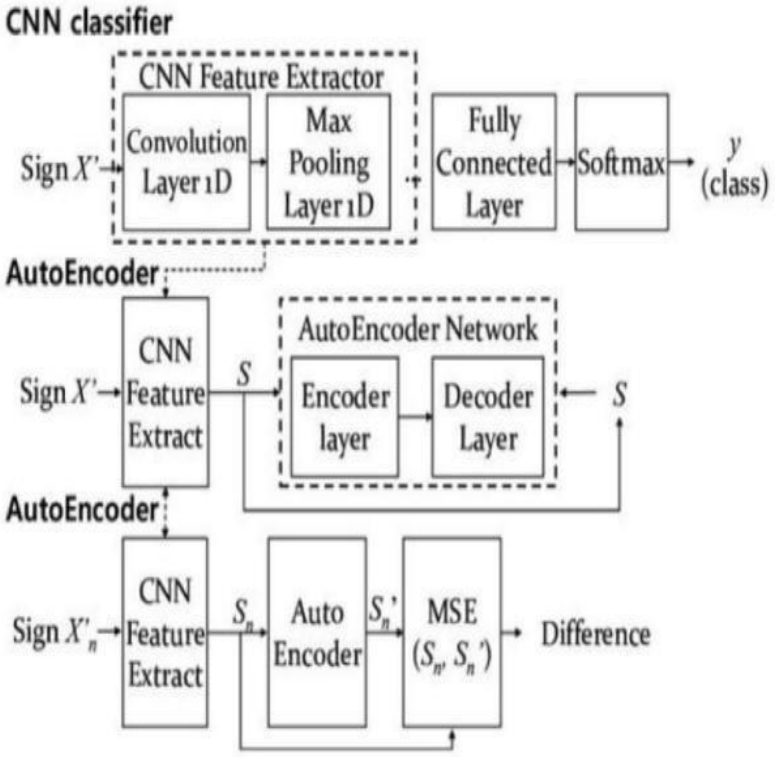
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125298

The Proposed method uses a CNN as a feature extractor and as a classifier. The suggested CNN-AE model's architecture is depicted in the figure below. In CNN, the extraction procedure is a "black box," and the precise details of the features' properties are still unknown. We assume that a trained CNN can extract useful features for differentiating behaviour characteristics of forgery, such as reluctance and delay before drawing the difficult part of a signature, if the CNN is taught for classifying forged and authentic signatures. As a result, the S-vector (represented by S in diagrams and equations) is utilised as a feature vector to represent the output of the CNN feature extractor. An auto encoder receives the Svector as input to build the topic mode.

An artificial neural network called an autoencoder is used to unsupervised learn effective data codings. An autoencoder trains the network to ignore signal "noise" in order to learn a representation (encoding) for a set of data, generally for dimensionality reduction.

Unsupervised learning of efficient data codings is accomplished using an artificial neural network called an autoencoder. A network is trained to ignore signal "noise" using an autoencoder in order to learn an encoding (representation) for a set of data, typically for dimensionality reduction.



CNN classifier with AutoEncode Drawback of Convoluted Neural Networks

Deep networks' main advantage is its ability to represent numerous complicated functions and learn features at various levels of abstraction, progressing from edges, which are often found in much lower layers, to complex features that reside in the deepest of the layers.

However, a major difficulty with deep networks is that as we back propagate from the top layer to the bottom layer, the gradient rapidly and exponentially declines tozero. The gradient is a numerical computation that teaches us how to modify a network's parameters so that the output divergence is kept to a minimum. In extremely unusual circumstances, it could abruptly and quickly increase or erupt into very huge values.

Layers of CNN

Each input image is sent through a sequence of convolution layers using filters (Kernels), Pooling, fully connected layers (FC), and the Softmax function to identify an object with probabilistic values between 0 and 1. This is done in order to train and test deep learning CNN models. The flow of CNN to process an input image and classify the objects based on values is shown in the following figure.

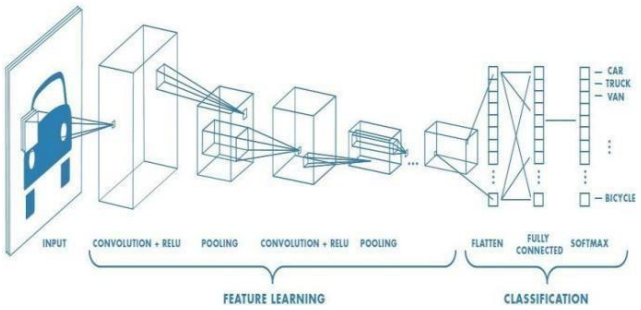
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125298

Neural network with many convolution layer



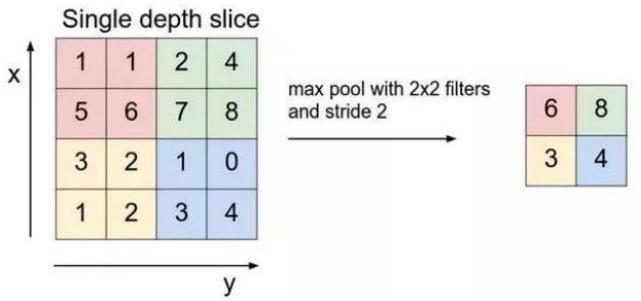
Convolution Layer : The first layer to extract features from an input image is convolution. Convolution learns visual features from small input data squares, preserving the link between pixels. It is a mathematical process that requires two inputs, such as an image matrix and a kernel or filter.

Non Linearity(ReLU) : For a non-linear operation, ReLU stands for Rectified LinearUnit. It results in (x) = max(0,x). Why ReLU is crucial The goal of ReLU is to add nonlinearity to our ConvNet.

Pooling Layers : When the photos are too huge, the section on pooling layers would lower the number of parameters. Spatial pooling, which lowers the dimensionality of each map while preserving crucial data, is also known as subsampling or downsampling. Multiple forms of spatial pooling are possible:

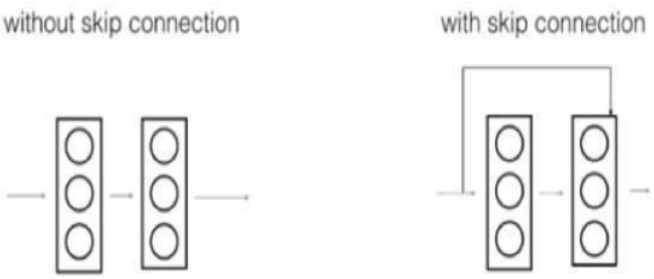
- Max Pooling
- Average Pooling
- Sum Pooling

The largest element in the corrected feature map is selected using max pooling. The average pooling could be taken instead of just the largest element. Sum pooling refers to the totalof all feature map elements.



Max Pooling

Residual Network(ResNet) : Implementing ResNet, a kind of neural network, can improve system functionality because of the phenomenon of gradient decrease. The disappearing gradient issue, which is brought on by sigmoid-like non-linearities (the gradient disappears because of the flat areas of the sigmoid), is resolved via ReLU activation.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125298

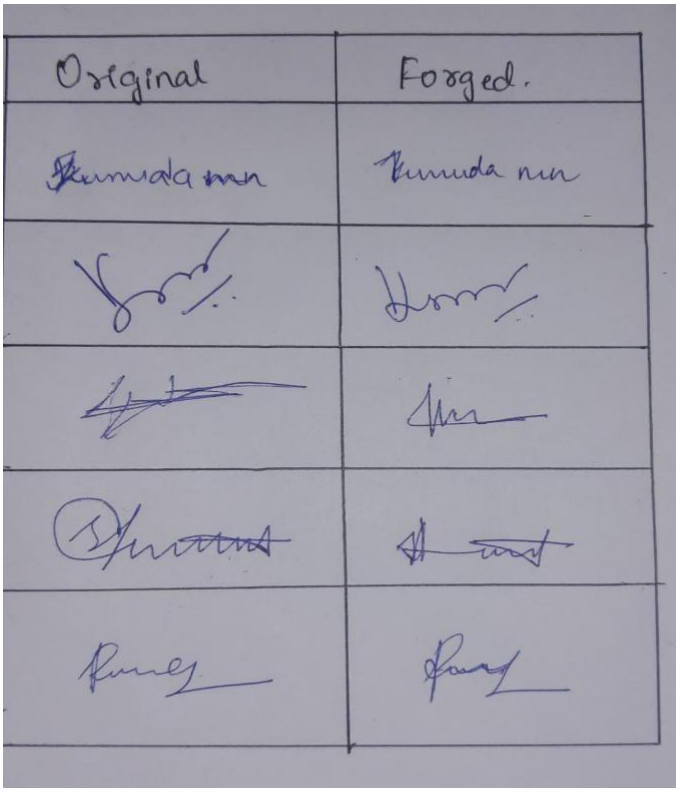
Left : Shows the working of deep Networks and Right : Shows how residual Networks work.

Residual networks support the development of deeper neural networks, which is crucial for preventing the deterioration of handwritten signature accuracy and error rate.

As you proceed through the layers, the matrix weights keep doubling. By normalising the input layer by re-centering and re-scaling, batch normalisation is a technique used to make artificial neural networks faster and more stable. This method efficiently improves speed and performance, enabling the layer to train more successfully. ResNet blocks are sorted into two categories based on how dissimilar or similar they are:

- Identity Block
- Convolution Block

Sample Data set :



V. CONCLUSION

In our social and legal lives, handwritten signatures are crucial for authenticity and verification. Only if a signature comes from the appropriate recipient will it be accepted. It is extremely unlikely that two signatures created by the same person will be identical. Even if two signatures are made by the same person, many signature characteristics might change. As a result, finding a forgery becomes difficult.

VI. FUTURE WORK

Effective user verification techniques are essential given the growing digitalization of many facets of daily life as well as emerging problems in workplaces and agencies. It is clear that new and better approaches and algorithms are needed in tandem with new technology that is opening up new possibilities. The suggested approach can be utilised as a

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125298

reliable mechanism for verifying signatures.The suggested method made offline signature verification successful with improvements to efficiency and accuracy, and it was simple to spot expert forgeries. In order to properly identify signature fraud, we combined a Convolutional Neural Network (CNN) solution with Python and its tools. Future work will entail reducing the model's Fault Rejection rate. Another potential project is to merge offline and online signature verification systems. This will strengthen the system by taking into account both execution speed and a real visual signature, making it more difficult to fabricate signatures. This can be utilised in security systems in public locations like ATMs, official government buildings, colleges, legal institutions, etc., or it can be developed into apps or web pages.

REFERENCES

[1]. Luiz G. Hafemann , Robert Sabourin and Luiz S. Oliveira (2017). Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks. Pattern Recognition. 70:163-176.
[2]. Wen, Jing Fang, Bin Tang, Yuan Zhang and TaiPing (2009). Model-based signature verification with rotation invariant features. Pattern Recognition. 42(7):1458- 1466.
[3]. Qi, Yingyong Hunt and Bobby (1994). Signature verification using global and grid features. Pattern Recognition. 27(12):1621-1629.
[4]. S Jerome Gideon, Anurag Kandulna, Aron Abhishek Kujur, A Diana and Kumudha Raimond (2018). Handwritten Signature Forgery Detection Using Convolutional Neural Networks. Procedia Computer Science. 143:978-987.
[5]. Hadjadji, Bilal Chibani, Youcef Nemmour and Hassiba (2017). An Efficient Open System for Offline Handwritten Signature Identification basedon Curvelet Transform and One-Class Principal Component Analysis. Neurocomputing. 265(12):66-77.
[6]. Vargas-Bonilla, J.Ferrer-Ballester, Miguel Travieso, Carlos Alonso and Jesús (2011). Off-line signature verification based on grey level information using texture features. Pattern Recognition.44(2):375-385.
[7]. Sabourin, Robert Plamondon, Réjean Beaumier and Louis (1994). Structural Interpretation of Handwritten Signature Images. International Journal of Pattern Recognition and Artificial Intelligence.8(03):709-748.
[8]. Saeid Fazli & Shima Pouyan,(2015). High Performance Offline Signature Verification and Recognition Method usingNeuralNetwork.InternationalJournalofadvanced studiesinComputer Scienceand Engineering.4(6):9-13.
[9]. Shih Yin Ooi, Andrew Beng JinTeoh, Ying HanPang and Bee Yan Hiew (2016). Image-Based Handwritten Signature Verification Using Hybrid Methodsof Discrete Radon Transform, Principal Component Analysis and Probabilistic Neural Network. Applied Soft Computing. 40(7): 274-282.
[10]. Diego Bertolini, Luiz Soares de Oliveira, Edson Justino, and Robert Sabourin (2010). Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition. 43(1):387-396.
[11]. Mustafa Berkay Yilmaz and Berrin Yanikoglu (2016). Score Level Fusion of Classifiers in Off-line Signature Verification. Information Fusion. 32: 109-119.
[12]. Robert Sabourin, Ginette Genest and F.J.Preteux,(1997). Off-line signature verification by local granulometric size distributions. Pattern Analysis and Machine Intelligence. 19(9):976-988.
[13]. Jun Cao, Majid Ahmadi and M. Shridhar (1995). Recognition of handwritten numerals with multiple feature and multistage classifier. Pattern Recognition. 28(2):153-160.
[14]. Hong Yan (1994). Handwritten digit recognition using an optimized nearest neighbor classifier. Pattern Recognition Letters. 15(2):207-211.
[15]. Ching Suen (1982). Distinctive features in automatic recognition of handprinted characters. Signal Processing. 4(2-3):193-207.
[16]. Toru Wakahara (1993). Toward robust handwritten character recognition. Pattern Recognition Letters. 14(4):345-354.
[17]. Drouhard, J.P Sabourin, Robert Godbout and Mario (1996). A neural network approach to off-line signature verification using directional PDF. Pattern Recognition. 29(3):415-424.
[18]. Guerbai, Yasmine Chibani, Youcef Hadjadji and Bilal (2015). The effective use of the one-class SVM classifier for handwritten signature verification based on writer- independent parameters. Pattern Recognition. 48(1):103–113.
[19]. I.S.I Abuhaiba and Pervez Ahmed (1993). A fuzzy graph theoretic approach to recognize the totally unconstrained handwritten numerals.Pattern Recognition. 26(9):1335-1350.
[20]. C. L. Walker, M. Brown and Temple H. Fay (1988). Handprinted symbol recognition system. Pattern Recognition. 21(2):91-118.

