International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Signature Verification System using CNN & SNN

Robin Nadar[1], Heet Patel[2], Abhishek Parab[3], Akhilesh Nerurkar[4], Ruchi Chauhan[5]

[1,2,3,4] B.E. Student, Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India
[5] Professor, Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India

---

Abstract - *Signature verification is the most rudimentary method for identity validation. Signatures can be verified in many ways however the Machine Learning algorithms provide the best method for verifying a signature whilst comparing it to the original signature of the person in question. Criminal acts of forging a signature on financial documents, checks, exam papers, consent forms, etc., are not uncommon and are a detriment to an organization. Signatures carry many traits and quirks unique to the individual creator. Character/alphabet spacing, dots, curves, and many other such parameters can be determined with Neural networks, allowing for a threshold to be created for comparison of original signatures to the ones in objection. The proposed work is a Signature Verification algorithm hosted as a web application that uses Convolution Neural network and Siamese Neural Networks in conjunction. Our objective is to produce a system with high accuracy and for user convenience make the UI with the best possible accessibility.*

Key Words: **Signature verification system, CNN, SNN, CNN & SNN, Convolutional, Siamese, Neural Networks, Deep Learning.**

1. INTRODUCTION

Identity implies the uniqueness or individuality of a person, something that sets him apart from his peers so that he can be uniquely identified for who he is. Its importance is huge because otherwise, society might fall into chaos. A name is a common identifier. Identity verification is simply the cross-checking of the identity of a person to ensure that he is indeed the same person that his identification tells him to be. It is necessary in various sectors like banking, insurance, medical, government, etc. to ensure order in the working of the organization and prevent fraud and other such crimes.

A person's unique identity can be proved with the help of his physiological characteristics which in legal/technical terms can be referred to as Biometrics. The most commonly used biometric features for identification are fingerprint, iris, voice, and handwritten signatures.

Fingerprint identification is the physical process of authentication using the fingerprint scanner converting the fingerprint into digital code and optimizing it. We don't have to remember complex passwords but sometimes due to injuries, it can interfere with the scan. Using ink prints is also a possible method but keeping its records requires physical documents which makes it a bulky, easily perishable, and inconvenient method.

In Iris recognition, the iris, located between the eyelashes is scanned using a high-powered camera and converted into digital data. As the iris is an internal organ and has sensitive membranes it cannot be injured easily, making it highly unlikely to influence verification. But this technology requires specialized hardware and software making it costly, unwieldy, fragile, and unable to be implemented everywhere.

Voice recognition works by recording the voice and analyzing its various features like pitch, tone, accent, speaking habits, etc., and matching it to another voice to be verified. Voice is difficult to falsify for a common person. But this process requires clear voice samples for proper verification and it forbids any external noises that can interfere with the verification process. Also, the equipment though robust is bulky and the storage requirement is large.

The main advantages of handwritten signatures over other means of identity verification are:

- It can be performed anywhere with a simple pen and paper
- Fast, easy, and cheap compared to other means
- No specialized gadgets or instruments are necessary, though could be used for better results and user experience
- Being literate is not necessary for this means of identity verification if the signature is memorized
- Its history of several centuries has spread this method to all corners of the globe so it is a universally known and trusted method that everyone is aware of and used to, unlike the more recent methods or methods that are used only in certain regions or amongst certain groups or circles

An identity verification system works on the principle of individual identification based on the unique traits of the said individual as discussed previously. The advantage of using such a system over manual verification is that they are cheaper in the longer term, accuracy is higher, can be installed anywhere and availability is ensured.

A signature verification system is a computerized or mechanized system that compares an original signature with a signature that needs to be verified. Using image processing algorithms, it compares the various features that are pre-programmed into the system and gives an output based on

predetermined parameters whether the signature is genuine or a forgery.

Compared to the other verification systems it requires low storage and has a fast response. But in case of an injury or inability to make a signature properly, or in case of people having inconsistent signatures, using this type of technology for identity verification is not possible and we have to resort to other methods. Also, this method only requires a single computer system in case the scanned images of the signatures already exist, but will require a camera, scanner, or stylus input otherwise.

The ease of access is also a concern as, if the system is installed on a device that is currently inaccessible to a user due to any reason it will cause undesirable user inconvenience. Internet solves this problem. A system that works online, can be accessed through any device connected to the internet solving the problem of accessibility and storage.

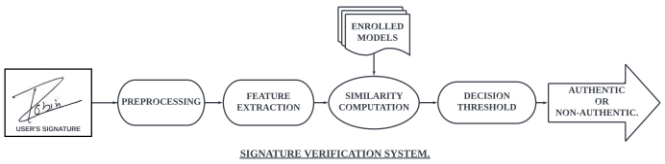

Fig 1. Block Diagram

2. PREPROCESSING [1]

We all know that images come in a variety of pixel sizes and values. Grayscale images are created by converting ordinary color images to grayscale ones. Because batch training a neural network normally requires images of the same size, the signature images we evaluate range in size from 153x258 to 819x1137. It is vital to establish a uniform size for input images in order to get effective results in image processing. As a result, we use bilinear interpolation to scale all of the images to a constant size of 155x220. The images are then inverted such that the background pixels have 0 values. In addition, we normalize each picture by dividing the pixel values by the standard deviation of the pixel values of the images in the collection.

3. CONVOLUTION NEURAL NETWORK & SIAMESE NEURAL NETWORK (CNN & SNN) [1][2][3][4][5][6][7]

A Convolutional Neural Network is a neural network that is constructed by combining any number of data-processing layers centered on a convolutional layer. A CNN used for Image Processing is often divided into two stages: feature extraction and feature categorization. The convolution layer is made up of a network of numerous learnable convolution kernels (also known as filters) that compute feature maps. When an elementwise non-linear activation function is applied to the convolution of the input with the kernel, a feature map is generated. A CNN is often used for tasks such as image classification, object detection, image segmentation, and so forth.

A Siamese Neural Network is a type of neural network that is used to compute the similarities and differences between two separate sets of input data. It is made up of two identical sub-networks (which may be any sort of neural networks, such as Convolutional Neural Networks (CNN)[15], Single-Layer or Multi-Layer Perceptrons (MLP), Recurrent Neural Networks (RNN), and so on) each having a distinct input node and a shared output node. The two identical subnetworks collaborate on two separate pieces of data to produce two distinct sets of outcomes. These two outputs are compared to get a result defining the degree of similarity between the two starting inputs.

4. ARCHITECTURE [1]

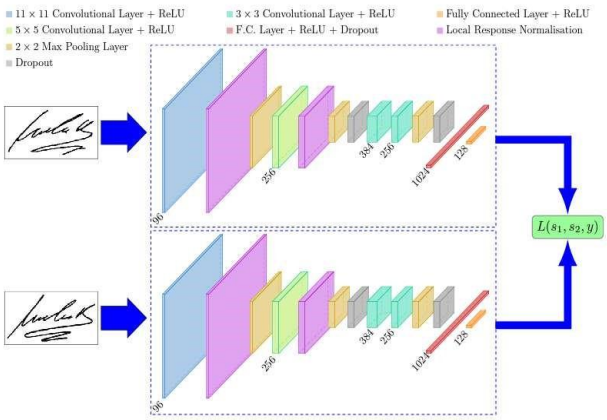

Fig 2. Architecture [3]

The size of the filters for convolution and pooling layers is listed as NxHxW, where N is the number of filters, H is the height, and W is the width of the associated filter. Stride is the distance between the application of filters for convolution and pooling processes, and pad denotes the width of additional borders to the input. Padding is required in order to convolve the filter from the very first pixel in the input picture. Rectified Linear Units (ReLU) are used as the activation function for the output of all convolutional and fully connected layers throughout the network. Local Response Normalization is used with the parameters to help generalize the learned characteristics. We employ a Dropout with a rate of 0:3 and 0:5, respectively, with the final two pooling layers and the first fully connected layer.

The initial convolutional layers use 96 kernels of size 11x11 with a stride of 1 pixel to filter the 155x220 input signature picture. The first convolutional layer's (response-normalized and pooled) output is sent into the second convolutional layer, which filters it using 256 kernels of size 5x5. The third and fourth convolutional layers are linked to one another without the use of layer pooling or normalization. The third layer has 384 kernels of size 3x3 that is coupled to the second convolutional layer's (normalized, pooled, and dropout) output. The fourth convolutional layer contains 256 kernels with a size of 3x3. As a result, the neural network learns fewer lower-level information for smaller

receptive fields and more higher-level or abstract features. The first completely linked layer has 1024 neurons, while the second fully connected layer contains 128 neurons. This means that the largest learned feature vector from either side of our Model has a size of 128.

This framework has been utilized successfully in weakly supervised metric learning for dimensionality reduction. At the top, a loss function computes a similarity metric incorporating the Euclidean distance between the feature representations on either side of the Siamese network, which connects these subnetworks. The contrastive loss is a commonly used loss function in the Siamese network, and it is defined as follows:

$L(s1, s2, y) = \alpha(1 - y)D2w + \beta y\max(0,m - Dw)^2$ .....(1)

where s1 and s2 are two samples (here signature images),

y is a binary indicator function denoting whether the two samples belong to the same class or not,

α and β are two constants and m is the margin equal to 1 in our case;

$Dw = f(s1; w1) - f(s2;w2)$ .....(2)

is the Euclidean distance computed in the embedded feature space,

f is an embedding function that maps a signature image to real vector space through CNN, and w1, w2 are the learned weights for a particular layer of the underlying network.

This space will have the feature that pictures of the same class (authentic signature for a particular writer) will be closer to each other than images of other classes due to the loss function used (Eqn. 1). (forgeries or signatures of different writers). A layer computes the Euclidean distance between two locations in the embedded space and connects both branches. Then, to assess if two photos are similar (genuine, genuine) or dissimilar (genuine, fabricated), a threshold value on the distance must be determined.

5. METHODOLOGY [8][9]

Thresholding in a Signature Verification System is the method of identifying an input signature as genuine or forged by comparing its dissimilarity ratio to a predetermined threshold. The decision threshold is used to maintain a balance between the most stable and least stable signatures. If the dissimilarity ratio is less than the threshold, the input is considered genuine; otherwise, it is classed as a forgery.

The length of a line segment between two specified locations represents the Euclidean distance between two points in Euclidean space, as we know from mathematics. The Euclidean Distance is the distance between two signature characteristics in a Signature Verification System. The characteristics might include Critical Points, Center of Gravity, Slope, and so on. Assuming that all of the features present in the original signatures are also present in the query signature, the Euclidean distance is calculated, and if the query signature image's Euclidean distance with respect to the mean signature is within the set range, the query signature is genuine; otherwise, it is classified as forged.

FAR AND FRR

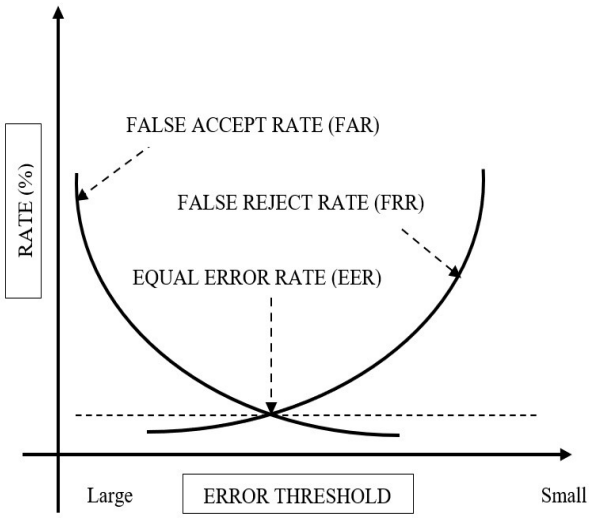

Fig 3. Characteristics of FAR & FRR

The following error rates are used to assess the performance of biometric systems:

False Acceptance Rate (FAR): The percentage of identification instances in which unauthorized persons are incorrectly accepted.

False Rejection Rate (FRR): The percentage of identification instances in which authorized persons are incorrectly rejected.

As the number of false acceptances (FAR) decreases, the number of false rejections (FRR) increases, and vice versa (see the figure above). The intersection of the lines is also known as the Equal Error Rate (EER). This is the point at which the percentage of false acceptances and false rejections is the same.

6. REQUIREMENTS

6.1 HARDWARE REQUIREMENTS

- Laptop / PC
- Processor: Intel i5 processor or above
- Graphics Card: AMD or NVIDIA at least 2GB
- RAM: More than 4 Gb
- Storage: 1 Gb disk space
- Internet connection: Above 10mbps

6.2 SOFTWARE REQUIREMENTS

- Operating System: 64 Bit Operating Windows 10 or higher
- Python (3.8.8)
- Visual Studio Code

7. WORKING OF THE WEBSITE

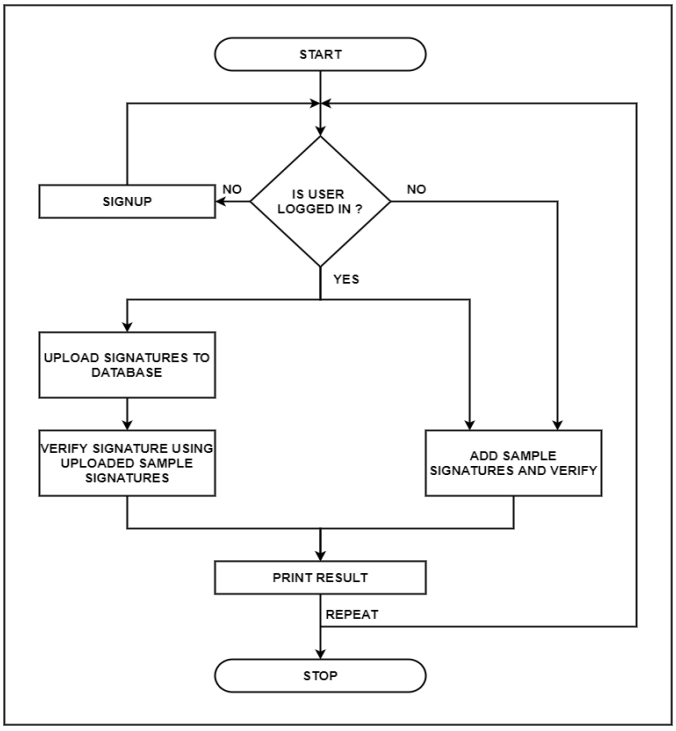

Fig 4. Website Flowchart

The figure below shows the guest page of our system where an individual can verify their signature.

This shows that the signature is authentic.

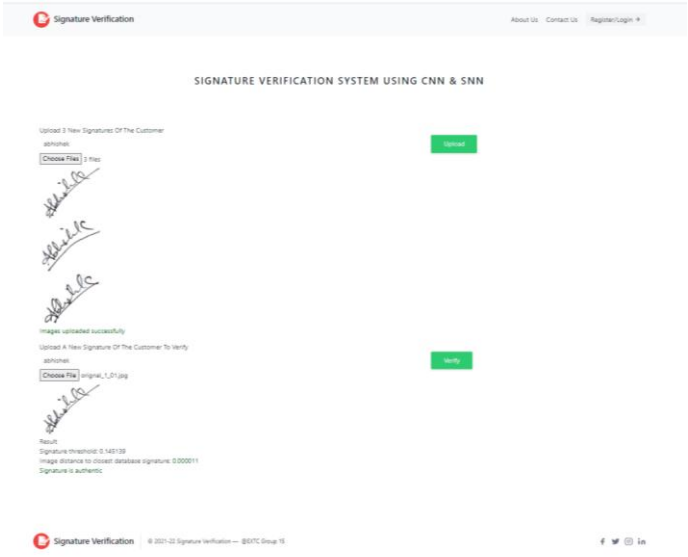

Fig 5. Guest User Authentic

This shows the image is non-authentic

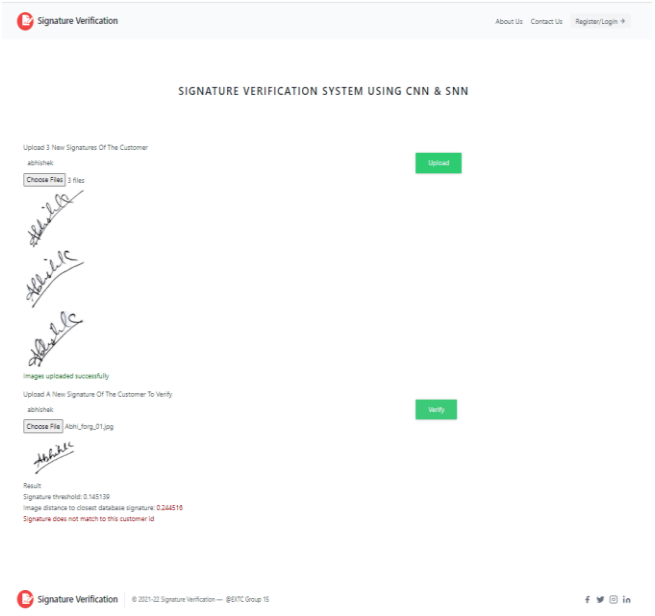

Fig 6. Guest User Not Authentic

The figure below shows the main page of our system where an individual can register their details and create a permanent profile.

This shows that the signature is matching

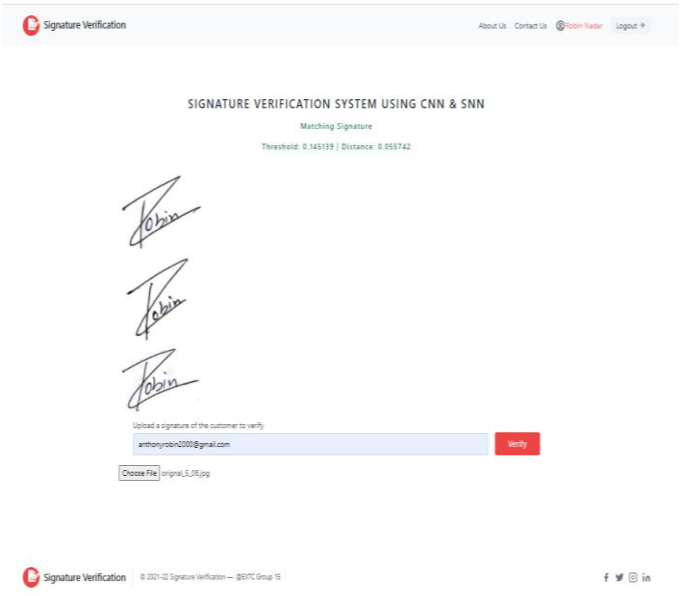

Fig 7. Authentic Profile User

This shows that the signature is not matching

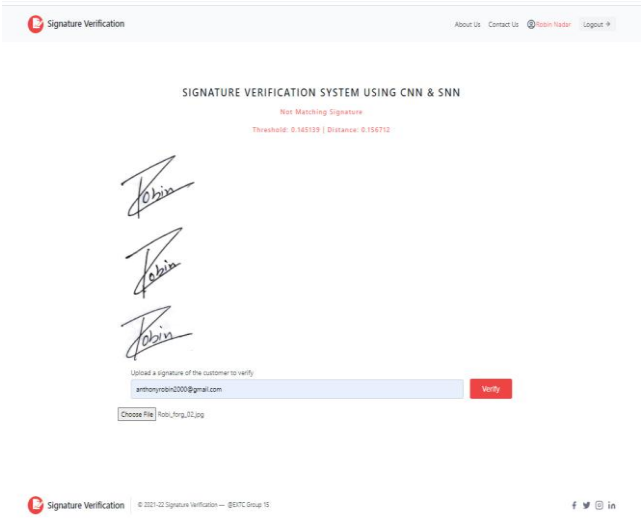

Fig 8. Not Authentic Profile User

8. TABULATION

Table -1: Accuracy Table

Sr. No	Datasets	Signers	Accuracy	FAR	FRR
1.	Cedar	55	86.56%	13.44	13.44
2.	Self-made	10	85.36%	14.64	14.64

9. RESULT

Signature Verification System, like any other Human Verification System, is not fully infallible, and there is a probability that it may provide incorrect results regardless of the technique or methodology used. However, when we compare the various Signature Verification Systems, we can find that CNN and SNN are the most often utilized techniques owing to their ease of development, usage, and accuracy. The model has an accuracy of 86% with a 3% tolerance.

Also, this system has a guest page where the user can validate a questionable signature immediately without creating a profile. On the other hand, the profile system allows the user to permanently save their valid signatures on the system which allows them for quick verification and saves the user the inconvenience of uploading the signatures again.

REFERENCES

[1] Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llados, Umapada Pal, "SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification", 30 September 2017 journal, September 2017.

[2] Sultan Alkaabi, Salman Yussof, Sameera Almulla, Haider Al-Khateeb, Abdulrahman A Abdulsalam, "A Novel Architecture to verify Offline Hand-written Signatures using Convolutional Neural Network", 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), September 2019.

[3] Atefeh Foroohzandeh, Ataollah Askari Hemmat, Hossein Rabbani, "Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning Using Convolutional Neural Networks (A Literature Review)", 2020 International Conference on Machine Vision and Image Processing (MVIP), February 2020.

[4] S V Bonde, Pradeep Narwade, Rajendra Sawant, "Offline Signature Verification Using Convolutional Neural Network", 2020 6th International Conference on Signal Processing and Communication (ICSC), March 2020.

[5] Avani Rateria, Suneeta Agarwal, "Off-line Signature Verification through Machine Learning", 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), November 2018.

[6] Shayekh Mohiuddin Ahmed Navid, Shamima Haque Priya, Nabiul Hoque Khandakar, Zannatul Ferdous, Akm Bahalul Haque, "Signature Verification Using Convolutional Neural Network", 2019 IEEE International Conference on Robotics, Automation, Artificialintelligence and Internet-of-Things (RAAICON), November 2019.

[7] Ladislav Vizváry, Dominik Sopiak, Miloš Oravec, Zuzana Bukovčiková, "Image Quality Detection Using The Siamese Convolutional Neural Network", 2019 International Symposium ELMAR, September 2019.

[8] Vikramaditya Agarwal, Akshay Sahai, Akshay Gupta, Nidhi Jain, "Human Identification and Verification based on Signature, Fingerprint and Iris Integration", 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), September 2017.

[9] A. Hamadene, Y. Chibani, "One-Class WriterIndependent Off-line Signature Verification Using Feature Dissimilarity Thresholding", IEEE Transactions on Information Forensics and Security (Volume: 11, Issue: 6, June 2016), January 2016.

[10] Brinzel Rodrigues, Anita Chaudhari, Pratap Sakhare, Dimpy Modi, "Prototype for Signature Verification System Using Euclidean Distance", 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), October 2015.

[11] Rui Xi, Mengshu Hou, Mingsheng Fu, Hong Qu, Daibo Liu, "Deep Dilated Convolution on Multimodality Time Series

For Human Activity Recognition", 2018 International Joint Conference on Neural Networks (IJCNN), July 2018.

[12] Snehal K. Jadhav, M. K. Chavan, "Symbolic Representation Model for Off-line Signature Verification", 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), July 2018.

[13] Soumya Jain, Meha Khanna, Ankita Singh, "Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network", 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), February 2021.

[14] Omid Mersa, Farhood Etaati, Saeed Masoudnia, Babak Nadjar Araabi, "Learning Representations from Persian Handwriting for Offline Signature Verification, a Deep Transfer Learning Approach", 2019 4th International Conference on Pattern Recognition and Image Analysis (IPRIA), March 2019.

[15] M. Hanmandlu, A. Bhanu Sronothara, Shantaram Vasikarla, "Deep Learning based Offline Signature Verification", 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), November 2018.

[16] M. Hanmandlu, A. Bhanu Sronothara, Shantaram Vasikarla, "Deep Learning based Offline Signature Verification", 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), November 2018.

[17] Shalaw Mshir, Mehmet Kaya, "Signature Recognition Using Machine Learning", 2020 8th International Symposium on Digital Forensics and Security (ISDFS), June 2020.

[18] Bhushan S. Thakare, Dr. Hemant R. Deshmukh, "A Novel End-To-End Approach For Offline Signature Verification System", 2018 3rd International Conference for Convergence in Technology (I2CT), April 2018.

[19] Alireza Alaei, Srikanta Pal, Umapada Pal, Michael Blumenstein, "An Efficient Signature Verification Method based on an Interval Symbolic Representation and a Fuzzy Similarity Measure", IEEE Transactions on Information Forensics and Security (Volume: 12, Issue: 10, Oct. 2017), May 2017.

[20] Atefeh Foroozandeh, Ataollah Askari Hemmat, Hossein Rabbani, "Offline Handwritten Signature Verification Based on Circlet Transform and Statistical Features", 2020 International Conference on Machine Vision and Image Processing (MVIP), June 2020.

[21] K.Tamilarasi, S.Nithya Kalyani, "A Survey on Signature Verification Based Algorithms", 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), April 2017.

[22] Rahul D Rai, J.S Lather, "Handwritten Signature Verification using TensorFlow", 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2018.