A Survey on 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 - *Handwritten Signature verification is the most basic and the most common method of authenticating a person's profile and/or identity. This paper, therefore, is focused on providing an accurate analysis of various signature verification systems that are available on the market and the various signature databases that can be used for training and testing purposes. We have also compiled a list of methods and algorithms that can be and are frequently used for constructing Signature Verification Systems that we reviewed. We also performed a comparative analysis on the accuracy and efficiency of the reviewed systems and Signature datasets and their various drawbacks.*

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

1.INTRODUCTION

Human verification gets increasingly difficult as the count of people to be verified increases. Thus, it is impossible for an individual or an organization to correctly verify the identity of every single person, and hence, it's not very difficult for an impersonator to acquire access to someone else's assets, if they're being maintained by a third party like the Government, Healthcare services, Banks, etc. Human verification is the tool for combatting these fraudulent practices by ensuring that an individual is indeed the same person and not an imposter.

Human verification can be performed by biological and behavioral characteristic identification and verification which includes methods such as signature verification, fingerprint verification, DNA verification, iris scanning[1], voice recognition, activity recognition[2], etc. Of these, Handwritten Signature Verification (HSV) is the most widely used and accepted method thanks to the ease with which it can be procured and its high reliability as an identity verification method. While, Iris and Fingerprint methods are relatively modern with a better rate for distinguishing between people, the hardware and software required for procurement and analysis for these methods are costly, bulky, and has a larger amount of constraints attached to it and thus are not as popular as Handwritten Signature Verification method.

But this method too has its disadvantages when faced with forgeries and manual verification errors. To get around these verification methods, forgers and frauds are becoming skilled too[3]. The types of forgeries can be progressively classified as Blind or Random forgery, Trace-over or Unskilled forgery, and Skilled forgery[4]. Other types include Simulations, Cut and Paste method and Electronic forgeries[1]. When confronted with a huge number of people to be verified, there are bound to be manual errors especially if there are no tools to aid the verifier. Forgeries skilled enough to surpass manual verification and genuine identities getting rejected when faced with the inadequacies of human scrutiny are a valid concern.

With the advent of technology, human verification has become easier. The use of technology does a great job combatting these disadvantages by using various hardware implements and software tools for procuring, storing, and verifying the signatures. The methods for procuring signatures include scanning a hard copy of the signature, using an electronic writing pad and stylus for direct input among the more prominent methods. The verification method can be online or offline, each with its own set of merits and demerits. Generally, online methods are preferred over offline methods because of their ease of access over the internet.

2. DEEP LEARNING[5][6][7]

Deep learning is a machine learning method that gradually derives higher-level characteristics from raw input. whereas the word deep refers to the usage of many layers in the network A linear perceptron cannot be a universal classifier, but a network with a nonpolynomial activation function and one hidden layer of unlimited breadth can be. Deep learning, as a contemporary variant, focuses on layers of defined size, allowing for practical application and efficient implementation while preserving theoretical universality under moderate conditions. Deep learning allows layers to be heterogeneous and depart significantly from physiologically informed connectionist models in terms of efficiency, trainability, and understandability, hence the structured component.

3. CONVOLUTION NEURAL NETWORK (CNN) [8][9][10][11][12][13]

A convolutional neural network can be said to be a chain of multiple data-processing layers, centered around a convolution layer, which when paired with other necessary blocks forms a complete neural network. Usually, a CNN employed for Image processing can be divided into two stages: feature extraction stage and feature classification stage. The convolution layer can be further broken down to yield a multitude of learnable convolution kernels or filters which perform the task of computing feature maps. A feature map is produced when an elementwise non-linear activation function is applied to the convolution of the input with the kernel. The tasks for which a CNN is usually employed can be

broadly classified as Image classification, Object Detection, and Segmentation.

4. SIAMESE NEURAL NETWORK (SNN)[10][13][14]

A Siamese neural network is a neural network that is primarily used to compute the similarities or dissimilarities between two different sets of input data. It consists of two identical subnetworks (which can be another type of neural network like Convolutional Neural Networks (CNN)[15], SingleLayer or Multi-Layer Perceptrons (MLP), Recurrent Neural Networks (RNN), etc.) each with a separate input node and a common output node. The two identical subnetworks work in parallel with each other on two different sets of data, the outputs of which are compared to provide a result in a format predefined by the user.

5. THRESHOLDING[16]

Thresholding in Signature Verification System is the practice of classifying a particular input signature as Genuine or Forgery by comparing its dissimilarity ratio with a predefined threshold t. The decision threshold t is selected from a set S_{ord} such that, $t = S_{\upsilon(L-1)}$ and $0 < \upsilon < 1$. We call υ as the stability parameter that allows controlling the frontier between the most stable and the least stable signatures, respectively. The input will be classified as Genuine only if the dissimilarity ratio is less than t, else it is classified as a Forgery.

6. EUCLIDEAN DISTANCE [17]

As we know in mathematics, the Euclidean distance between two points in Euclidean space is the length of a line segment between the two points. With respect to a Signature Verification System, the Euclidean Distance is the distance between two features of a signature. The features can be the Critical Points, Centre of Gravity, Slope, etc. If the Euclidean distance of query signature image with respect to mean signature is within the set range, the query signature is genuine else it is classified to be forged.

7. DATASETS

7.1 CEDAR[10]

CEDAR signature database contains 24 genuine as well as 24 forged signatures of 55 signers (24 + 24) × 55 = 1320(genuine) + 1320(forged) = 2640 signatures in grayscale mode. This, paired with its consistent quality and clearly defined and segregated sections make it an excellent resource for training and testing of signature verification tools.

7.2 GPDS300[10][18][19]

GPDS300 signature corpus contains 24 genuine and 30 forged signatures of 300 signers (24 + 30) × 300 = 7200(genuine) + 9000(forged) = 16200 signatures. The Binary form of the images in the corpus makes it a great resource.

7.3 GPDS960[6]

GPDS960 signature corpus contains 24 genuine and 30 forged signatures of 960 signers (30 + 24) × 960 = 23040(genuine) + 28800(forged) = 51840 signatures. The varying sizes of the images in the corpus makes it an excellent resource.

7.4 GPDS Synthetic[10][18]

GPDS SYNTHETIC signature corpus contains 24 genuine and 30 forged signatures of 4000 signers (24 + 30) × 4000 = 96000(genuine) + 120000(forged) = 216000 signatures. The database is constructed in accordance with the synthetic individuals protocol.

7.5 BHSig260[10][19]

The BHSig260 signature dataset contains 24 genuine as well as 30 forged signatures of 260 signers, 100 of which are Bengali and 160 are Hindi, (24 + 30) × (100 + 160) = [2400(genuine) + 3000(forged)]Bengali + [3840(genuine) + 4800(forged)]Hindi = 14,040 signatures in total. Also, the BHSig260 signature dataset has been constructed while following the same protocols as of GPDS300 signature corpus mentioned previously.

7.6 NISDCC Signature Collection[8]

The NISDCC signature collection of the ICDAR 2009 online SV competition consists of 60 authentic signatures written by 12 authors. A total of 31 forgers produced forgeries for all the signatures with a ratio of 1 genuine to 5 forgeries.

7.7 MCYT-75[20]

MCYT-75 signature corpus contains 15 genuine and 15 forged signatures of 75 individuals (15 + 15) × 75 = 1125(genuine) + 1125(forged) = 2250 signatures. The contents include complex Latin signatures and skilled forgeries for the same.

Other datasets that were reviewed include GPDS140[19] and GPDS160[19] which due to their small size make it easier to manage for training and testing process but this also limits the efficiency of the system.

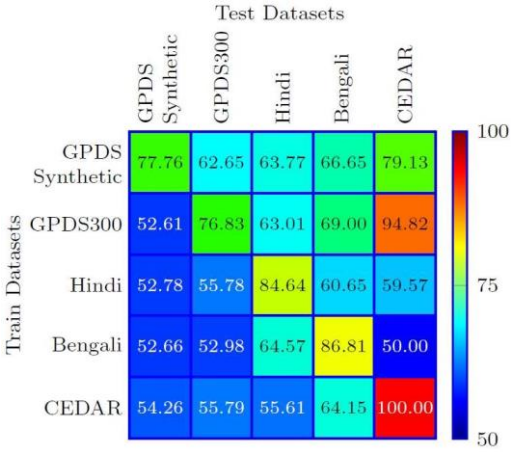
8. TABULATION

Table -1: Comparison Of Methods

Sr. No.	Method	FAR	FRR	ERR
1	GLCM[21]	13.67	8.08	11.61

2	Threshold[21]	1.60	3	-
3	Svm[21]	0	30	20
4	Pso-nn[21]	26.85	17.33	-
5	HOG & HoC with SVM[22]	16.3	15.6	-
6	Pyramid HOG[22]	1.5	14.49	-
7	HSV using TensorFlow[22]	5	5	-

Table -2: Comparisons of Datasets[10]



9. RESULT

Signature Verification, just like any other Human Verification System, is not completely foolproof and there are chances of it giving an inaccurate output irrespective of what method or algorithm we might be using. But comparing the various Signature Verification Systems, we can see that CNN and SNN are the more frequently used methods amongst others due to their ease of implementation, use and accuracy.

Amongst the various Signature Datasets that we compared, CEDAR database showed the most promising results as mentioned earlier.

10. CONCLUSION

In this paper, we evaluated the architecture, working, and efficiency rates of various algorithms, programs, experimental models, and systems for handwritten signature verification.

As future work, we will be working on an online signature verification system (based on python) using CNN and SNN.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

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

[16] 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.

[17] 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.

[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.