Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, Issue. 2 : 2022
ISSN : **1906-9685**

THE USE OF CNN AND SNN IN SIGNATURE VERIFICATION SYSTEMS

[#1]Mr.PEDDI KISHOR, *Assistant Professor*
[#2]Mrs.BHEERAM SANKEERTHANA, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

Abstract: Checking a person's signature is the simplest way to ensure that they are who they say they are. Because they directly compare the verified signature to the subject's original signature, machine learning techniques are the most reliable way for validating signatures. Employees forging signatures on checks, permission slips, exams, and other financial papers are illegal and detrimental to the organization. A signature has certain qualities that are unique to the person who produced it. Character/alphabet spacing, dot sizes, and other features can be discovered using neural networks. This enables the creation of a standard against which questionable signatures can be compared to the originals. A web-based solution for signature verification that uses Siamese and Convolution neural networks is being investigated. Our goal is to deliver an exceedingly precise system with the most user-friendly interface possible.

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

1. INTRODUCTION

The identity of a person is what distinguishes them from others and allows others to recognize them as an individual. Without it, society as we know it would most certainly crumble. A person's name is frequently used to identify them. To put it simply, identity verification is the process of verifying a person's credentials to guarantee they are who they say they are. Many industries, including banking, insurance, healthcare, and government, place a high value on maintaining order and combating fraud and other illegal behavior. A person's fingerprints or other identifying traits may be used to establish their identification in court or on the job. The most prevalent kinds of identification verification include fingerprints, iris scans, audio recordings, and written signatures. Fingerprinting can be used to obtain proof of identity. Your fingerprint is turned into a unique digital code using a fingerprint scanner. Complex passwords are not required, however the scan may fail inadvertently if they are used. Another option is ink printouts, but these require physical paper for storage, which is time-consuming, inefficient, and inconvenient. A high-powered camera is used to scan and digitalize the iris, which is located in the colorful area of the eye. The iris is a thin membrane-encased inner structure. This means that its impact on verification is at best minor. Unfortunately, because it requires specialized hardware and software, this technology is expensive, difficult, and fragile. It also has limitations in terms of application. A voice is recorded, its intonation, tone, accent, and speech patterns are evaluated, and its authenticity is verified by comparing it to another voice. Most people struggle with voice imitation. This approach, on the other hand, necessitates isolated speech samples and forbids the use of any background noise that could interfere with the verification process. The equipment is extremely strong, but it is also extremely huge and unwieldy.

The following are some of the benefits of handwritten signatures over other types of ID verification. Bring some paper and a pen, and

you'll be OK. It's a quick, easy, and low-cost alternative to the alternatives.

While specialist gear is not essential, it may improve productivity and user experience.

Even if you can't read or write, you can use the signature as proof of identification if you recall it.Many people are already familiar with it because it has been around for hundreds of years and has spread throughout the world.

The ultimate goal of identity verification methods is to locate a specific person using the aforementioned characteristics. Consider this approach as an alternative to manual verification that will save you money in the long term. It provides greater precision, a broader range of installation options, and a guarantee of availability.

A "signature verification system" is a piece of software or hardware that compares a suspect signature to a known good signature. Using image processing techniques, it investigates the many factors that have been pre-programmed into the system. Based on these parameters, it determines the legitimacy of the signature.

This verification device is perfect for usage in small locations because it responds quickly and is small in size. If a signature is illegible or incomplete, or if two people have contradictory signatures, this technique of authentication fails. Alternative strategies are required. Furthermore, if scanned photographs of the signatures are already available, this method can be completed on a single computer. If this is not the case, a camera, scanner, or stylus is necessary.

The system's accessibility has also been questioned. Users will be frustrated if it is put up on a device that they cannot access right now. The problem is being handled through the Internet. Because any device with an internet connection can join an online system, access and storage issues are eliminated.

Fig 1. The diagram of Block explains

2. PREPROCESSING

We're all aware that picture pixels come in a variety of sizes. Converting color photographs to monochrome can result in grayscale images. We chose trademark photos spanning in size from 153x258 to 819x1137 pixels for this purpose, as images of consistent size are often required for batch training a neural network. All supplied images must have the same dimensions for image processing to work properly. We use bilinear interpolation to ensure that all photos have the same 155 by 220 pixel resolution. After then, the photos are flipped so that the black backgrounds are translucent. Furthermore, the average standard deviation of all the pixel values in the photographs is utilized to normalize the pixel values in the pictures.

3. CONVOLUTION NEURAL NETWORK & SIAMESE NEURAL NETWORK (CNN & SNN)

The network is said to be convolutional when numerous data-processing layers are connected to a single convolutional layer. A CNN uses two subsystems to process images: feature extraction and feature classification. A convolutional neural network equipped with a set of trainable convolution kernels or filters generates feature maps. A feature map is created by combining the input and the kernel on a per-element basis with a non-linear activation function. CNNs find widespread use in image classification, object identification, and segmentation. Siamese Neural Networks are a form of neural network that is specifically built to compare and contrast two data sets. Each of its two identical subnetworks has a single input node and a single exit node that are shared. CNN, MLP, RNN, or another network entirely is a possibility. When applied to different datasets, the two identical subnetworks produce different results. This analysis will assist you in determining how closely the first two entries are related.

4. ARCHITECTURE

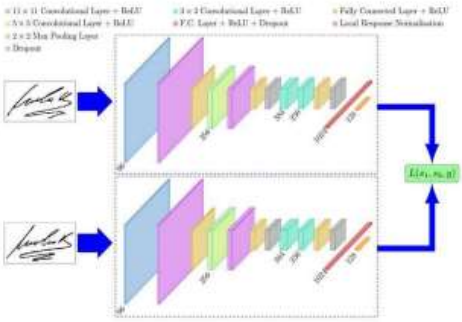

Fig 2. Architectural Design

The filter sizes used in the convolution and pooling stages are shown by the dimensions N x H x W. N denotes the number of filters, H their height, and W their width in this formula. Filters used for convolution and pooling have a stride, whereas those employed with extra input limitations have a pad. By including padding, the filter can be convolved with the input image from the first pixel. Rectified Linear Units (ReLU) are a function that activates each network's entirely linked and convolutional layers. The parameters are paired with local reaction normalization to maximize the applicability of the acquired skills. Dropout rates of 0.3 and 0.5 are used in the final two pooling layers and the first totally linked layer, respectively.

A 155x220 signature picture is passed through 96 11x11 kernels with a 1 pixel step in the first convolutional layer. The first convolutional layer's output is filtered by a second convolutional layer made up of 256 response-normalized and summed 5x5 kernels. Without using normalization or layer pooling, the third and fourth convolutional layers can be linked. The third layer employs 384 3x3 kernels to connect to the normalized, merged, and dropped-out output of the second convolutional layer. Each kernel in the fourth convolutional layer is 3x3, with a total of 256 of them. As a result, the neural network is trained to recognize fewer particular details and more general categories, so narrowing its receptive range. The first layer is made up of 1024 fully linked neurons, while the second layer only comprises 128.

The maximum learned feature vector in our model is 128, and it may come from either side. This line of thought has been used successfully to minimize the number of dimensions in poorly supervised metric learning. Siamese networks are used to connect these smaller networks, and their loss functions, placed at the network's top, calculate a similarity measure based on the Euclidean distance between the feature representations on either side. In Siamese networks, loss functions such as contrastive loss are typically used. The following is an explanation:

ymax = L(s1, s2)2 + (1 y)(1) D2w, where s1 and s2 are two samples (in this case, signature images), y is a binary indicator function that tells us if the two samples are from the same class, and and are two constants. Dw = f (s1; w1) f(s2; w1), where m is the margin, which is set to one.In this scenario, f embeds a signature image into a real vector space using a convolutional neural network, while w1, w2 are the learned weights for a given layer of the underlying network.

Because of the loss function used (Eqn. 1), images in the same class (a valid signature from a specific author) will be closer together than photos in other classes. a sign that it is not real or belongs to someone else. An intermediary layer, which connects the two forks, calculates the Euclidean distance between any two points in the embedded space. A distance threshold must be defined to assess whether two photos are similar (genuine, authentic) or dissimilar (authentic, fabricated).

5. METHODOLOGY

A signature verification system uses thresholding to determine the authenticity of an input signature. A threshold value is used to compare the signature dissimilarity ratio. At the decision level, both the most and least stable signatures are equally stable. The input is judged to be genuine if the dissimilarity ratio is less than the threshold. If the value exceeds the cutoff, it is marked as potentially fraudulent. The Euclidean distance between two points in Euclidean space is equal to the length of the line slice that connects the two points, according to the mathematical formula. The Euclidean Distance measures the distance between two components of a signature and is used to validate it. There could be key spots, the center of gravity, the slope, and other factors. Calculate the Euclidean distance between the two signatures, assuming the query signature has the same features as the original signature.

If the distance is within the acceptable range, the questioned signature is valid. If it isn't, the signature was most likely falsified.

FAR AND FRR

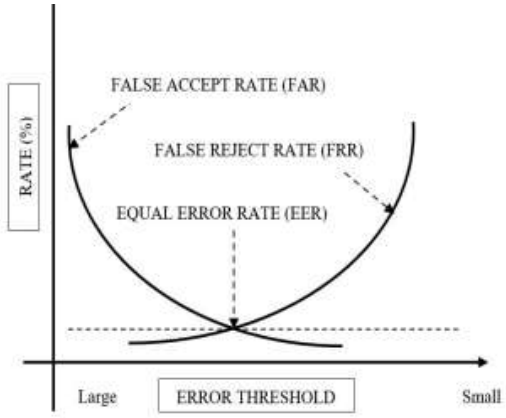

Fig 3. Factors that influence the FAR and FRR

The following are some error rates for biometric programs: The False Acceptance Rate (FAR) quantifies how frequently an inaccurate identification is accepted. The False Rejection Rate (FRR) is the percentage of genuine ID attempts that are wrongly refused. According to the data presented, FRR appears to be increasing while FAR appears to be decreasing. The convergence point is also known as the Equal Error Rate (EER). The proportion of false positives and false negatives is now equal.

6. REQUIREMENTS

HARDWARE REQUIREMENTS

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

SOFTWARE REQUIREMENTS

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

7. WORKING OF THE WEBSITE

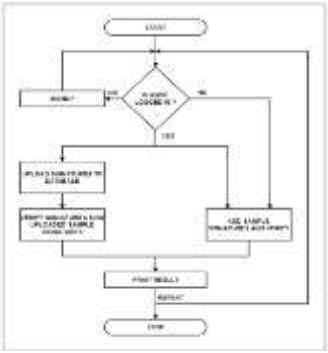

Fig 4. plans for websites

On the system's visitor page, as shown in the image below, users can double-check that their name is spelled correctly. The legitimacy of the signature is proven in this case.

Fig 5. User Permission Is Requested

This shows that the signature is invalid.

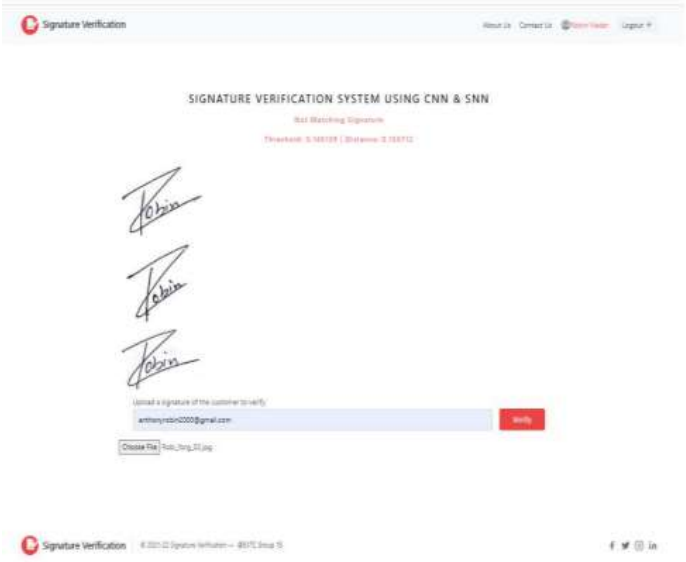

Fig 8. This is not an authentic account.

8. TABULATION

Table -1: Table with Rectification

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

RESULT

Regardless of how well it is implemented, the Signature Verification System, like any Human Verification System, may provide false results. However, when comparing alternative Signature Verification Systems, it is evident that CNN and SNN are the most popular options because to how simple they are to create, deploy, and master. The model has an 86% hit rate and a 3% margin of error.

There is also a "guest page" for individuals who want to investigate a name that appears suspicious without making an account. The profile technique, on the other hand, permanently saves the user's actual signatures, allowing for quick verification without forcing the user to continuously submit their signatures.

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.