Office of the Controller General of Patents, Designs & Trade Marks
Department for Promotion of Industry and Internal Trade
Ministry of Commerce & Industry,
Government of India

(http://ipindia.nic.in/index.htm)

(http://ipindia.nic.in/index.htm)

Application Details	
APPLICATION NUMBER	202541026004
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	21/03/2025
APPLICANT NAME	1 . Dr. C. Keerthana 2 . Dr L Sankari 3 . Dr.S.S. Ananthan 4 . Dr.S.Sivapriya 5 . Mrs.T.Banuthangalakshmi 6 . Hariharasudan.A 7 . J Malarvizhi 8 . B.Arulmozhi 9 . Dr.C.Poornima 10 . Ms.R.Greeshma
TITLE OF INVENTION	Signature Verification Using CNN, SNN, CSNN
FIELD OF INVENTION	COMMUNICATION
E-MAIL (As Per Record)	senanipindia@gmail.com
ADDITIONAL-EMAIL (As Per Record)	editorsipofficial@gmail.com
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	28/03/2025

Application Status

FORM 2

THE PATENTS ACT 1970

39 OF 1970

&

THE PATENT RULES 2003

COMPLETE SPECIFICATION

(SEE SECTIONS 10 & RULE 13)

1. TITLE OF THE INVENTION

Signature Verification Using CNN, SNN, CSNN

2. APPLICANTS (S)

NAME	NATIONALITY	ADDRESS
Dr. C. Keerthana	Indian	Assistant professor, Department of Computer Technology, Nallamuthu Gounder Mahalingam College, Pollachi , Coimbatore, Tamilnadu.
Dr L Sankari	Indian	professor & Head -B.Sc (IT), Department of Computer science, Sri Ramakrishna College of Arts & Science for Women ,Coimbatore 641044, Tamilnadu.
Dr.S.S. Ananthan	Indian	Associate Professor, Department Of mathematics, Erode Sengunthar Engineering college, thdupathi, perundurai(tk) 638 057, Erode, Taminadu
Dr.S.Sivapriya	Indian	Assistant Professor, PG& Research Department of Commerce, Dharmamurthi Rao Bahadur Calavala Cunnan Chetty's Hindu College, Pattabiram, Chennai - 600 072, Thiruvallur, Tamilnadu
Mrs.T.Banuthangalakshmi	Indian	Assistant Professor, Department of Computer Application, St.Joseph's College (Arts & Science), Kovur, Chennai - 600

		128, Kanchipuram, Tamilnadu
Hariharasudan.A	Indian	Assistant professor,Department of Cyber Security, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore , TamilNadu
J Malarvizhi	Indian	Assistant Professor, Department of Computer science, Dharmamurthi Rao Bahadur Calavala Cunnan Chetty's Hindu College, Pattabiram, Chennai - 600 072, Thiruvallur, TamilNadu
B.Arulmozhi	Indian	Assistant professor, Department of Management science, Sri Ramakrishna College of Arts and Science,Nava India-641006, Coimbatore, Tamilnadu
Dr.C.Poornima	Indian	Assistant Professor,Department of BCom-A&F,Sri Ramakrishna College of Arts & Science,Coimbatore, Tamilnadu
Ms.R.Greeshma	Indian	Assistant Professor,Department of BCom-A&F,Sri Ramakrishna College of Arts & Science,Coimbatore, Tamilnadu

2. PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION

The following specification particularly describes the invention and the manner in which it is to be performed

Signature Verification Using CNN, SNN, CSNN

Abstract:

A signature is a person's name, or a mark, often stylized and handwritten that a person writes, indicating his/her identity and genuine intent. The handwritten signature of a person is commonly accepted as a means of verifying the legality of documents such as certificates, checks, drafts, letters, approvals, visa, passport etc. and is indispensable in countering the forgery and falsification of such documents in diverse financial, legal, bureaucratic, academic, and other commercial settings. Take for example, in any bank whenever a cashier receives a cheque from a client, such cheque is verified with signature in it. The cashier compares that signature with a stored record of genuine signatures before proceeding with any legal transaction.

This convention of using signatures as the route for confirming the authenticity of documents has been followed from mediaeval time to present and will continue in future. Such authentication with signature is at times very critical and crucial in legal scenarios. For instance, a signature in any contracts has a vital role to indicate the identity of a person of interest and also to provide evidence of intent and informed consent. Any falsification and fraudulent regarding such signature may result severe damages in persons lives and assets. In such cases, a systematic approach to verifying the signature is very necessary to prevent such forgery. Traditionally, authentication of specimen signature is achieved by person, comparing and evaluating the specimen with copies of genuine signature specimens acquired previously or with the help of some sort of witness. In case of Nepal especially in banking sector, signature verification is important subject and very critical in various transaction and approvals processes. Bank verifies the signature of the applicant/drawer of the checks on the basis of specimen signature retained in the bank's custody. In modern banking ICDM (Image Capturing and Display Module) is an important tool, which captures specimen signatures of the applicant and displays as and

when required. But such simple approach may not be sufficient in all cases as various advanced forgery and falsification techniques are emerging. This project tries to assist and improve the verification process of human signature using machine learning techniques.

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 organisation 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 optimising 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 specialised 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 memorised
- 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 computerised or mechanised 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 preprogrammed 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. The 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.

CLAIMS:

1. Signature verification is the process of comparing a presented signature to a reference signature to assess the validity of the presented signature.
2. Financial institutions, election monitors, and other entities use signature verification techniques to look for forgeries.
3. Traditionally, humans manually performed this process, and they continue to do so for many applications.
4. However, there is also signature verification software that can automate the process.
5. Most analysts agree that the best approach is a hybrid of automated software with human oversight.

Elements Assessed in the Signature Verification Process

Whether a human or digital tool is analysing a signature, they look at the following elements:

- How the name is spelled.
- The use of print or cursive letters.
- Individual preferences in font style, such as how loops are rendered, dots are drawn, or letters are crossed.
- Direction and angle of the signature's slant.
- Size of the signature.
- Proportion of different signature elements in relation to each other.
- How the signature starts and ends, such as sudden ends, long tails, or loops.
- The strokes connecting different elements of the signature.
- Spacing between the first and last name and between the letters in the signature.
- The positioning of pen lifts.
- Speed of the writing.

1.1 Acceptable Variations in Signatures

People don't always sign their names in the exact same way. When someone is manually checking signatures, they must keep in mind that some level of variation is inevitable. In particular, they should consider the following acceptable variations:

- Shaky signatures — If the other elements such as the size and the position of pen lifts appear to be consistent, shakiness can often be a sign of health issues, ageing, or just too much coffee on a bad day.
- Name variations — Ideally, customers should sign their checks with the same legal name noted on the account, but common variations such as nicknames (for example, Don for Donald or Toby for Tobias), initials, or using their middle name as their first name, are not necessarily signs of forgery. In fact, a forger is less likely to make these types of mistakes than an authentic signer.
- Slight changes in style — People make slight changes to their signature over time. In these situations, it's especially important to pay attention to the fluidity of the signature.
- Aberrations from electronic signature tools — If someone signs their name with an electronic pen onto a screen, the signature may appear fuzzy or larger than usual. However, it should still have similar proportions and pen lift spots.
- Odd bumps — This can indicate that the signature was done on an uneven or bumpy surface.

When in doubt, verifiers should get a second opinion. If they still can't come to a conclusion, they should reach out to the person whose signature they're assessing.

What if a Bank Can't Verify a Signature:

If a bank cannot verify a signature, they should stop the transaction. They should reach out to the customer to verify the legitimacy of the transaction. If the customer's signature has changed drastically, they should update the reference signature on file.

What Is Signature Verification Software:

Signature verification software refers to applications that automatically compare signatures to look for forgeries. These tools help banks and other institutions to authenticate signatures without paying people to manually review signatures. Like manual reviewers, signature verification software compares a presented signature with a reference signature.

After comparing the two signatures, the software issues a confidence score. A high score indicates authenticity, while a low score indicates a

data. The CNN architecture comprises three main layers: convolutional layers, pooling layers, and a fully connected (FC) layer. There can be multiple convolutional and pooling layers. The more layers in the network, the greater the complexity and (theoretically) the accuracy of the machine learning model. Each additional layer that processes the input data increases the model's ability to recognize objects and patterns in the data.

The Convolutional Layer:

Convolutional layers are the key building block of the network, where most of the computations are carried out. It works by applying a filter to the input data to identify features. This filter, known as a feature detector, checks the image input's receptive fields for a given feature. This operation is referred to as convolution.

The filter is a two-dimensional array of weights that represents part of a 2-dimensional image. A filter is typically a 3×3 matrix, although there are other possible sizes. The filter is applied to a region within the input image and calculates a dot product between the pixels, which is fed to an output array. The filter then shifts and repeats the process until it has covered the whole image. The final output of all the filter processes is called the feature map. The CNN typically applies the ReLU (Rectified Linear Unit) transformation to each feature map after every convolution to introduce nonlinearity to the ML model. A convolutional layer is typically followed by a pooling layer. Together, the convolutional and pooling layers make up a convolutional block.

Additional convolution blocks will follow the first block, creating a hierarchical structure with later layers learning from the earlier layers. For example, a CNN model might train to detect cars in images. Cars can be viewed as the sum of their parts, including the wheels, boot, and windscreen. Each feature of a car equates to a low-level pattern identified by the neural network, which then combines these parts to create a high-level pattern.

The Pooling Layers:

A pooling or downsampling layer reduces the dimensionality of the input. Like a convolutional operation, pooling operations use a filter to sweep the whole input image, but it doesn't use weights. The filter instead uses an aggregation function to populate the output array based on the receptive field's

values.

There are two key types of pooling: