# BONAFIDE CERTIFICATE

Certified that this project report **" OFFLINE SIGNATURE VERIFICATION USING DEEP LEARNING** "is the bonafide work of "**ALLOCIUS JEBAN S P(212221060012), BALAJI B(212221060026), RAGHAVAN T M(212221060220)"** who carried out the project work under my/our supervision.

**SIGNATURE**
**Dr.Sheeba Joice, M.E., M.B.A, Ph.D**
**HEAD OF THE DEPARTMENT**
Saveetha engineering college
(Autonomous)
Chennai-602105

**SIGNATURE**
**Dr.Nirmala Devi K, B.E,M.Tech,Ph.D**
**SUPERVISOR**
Saveetha engineering college
(Autonomous)
Chennai-602105

Submitted for the project viva-voice examination held on_____

**INTERNAL EXAMINER** **EXTERNAL EXAMINER**

# MINI PROJECT APPROVAL SHEET

The project approval sheet " **OFFLINE SIGNATURE VERIFICATION USING DEEP LEARNING** "submitted by **ALLOCIUS JEBAN S P(212221060012), BALAJI B (212221060026), RAGHAVAN T M(212221060220)"**is approved for submission, as partial requirement for the award of the **Degree of Bachelor of Engineering in Electronics and Communication**, Anna University during the academic year 2022- 2023.

Submitted for the University Project Viva Voice examination held on

_____.

**INTERNAL EXAMINER** **EXTERNAL EXAMINER**

# ACKNOWLEDGMENT

We convey our sincere thanks to **Dr.N.M.Veeraiyan** - President(SMET) and Chancellor-SIMATS, Saveetha Amaravathi University, **Dr.S.Rajesh**, Director - Saveetha Engineering College and **Dr. V. Saveetha Rajesh** – Director, Saveetha Medical College and Hospital for providing us with the facilities for the completion of our project. We are grateful to our Principal, **Dr.N.Duraipandian M.E,Ph.D.**, for his continuous support and encouragement in carrying out our project work. We are deeply indebted to our beloved Head of the Department, **Dr.Sheeba Joice, M.E., M.B.A, Ph.D** Department of Electronics and Communication, for giving us the opportunity to display our professional skills through this project.

We are greatly thankful to our Project Coordinator, **Dr.S. Asha M.Tech, Ph.D** and our Project Guide **Dr.Nirmala Devi K, B.E,M.Tech,Ph.D** for their valuable guidance and motivation which helped to complete our project on time.

We thank all our teaching and non- teaching faculty members of the Department of Electronics and Communication for their passionate support, for helping us to identify our mistakes and also for the appreciation they gave us. We heartily thank our library staff and the management for their extensive support in providing the resources and information that helped us to complete the project successfully. Also, we would like to record our deepest gratitude to our parents for their constant encouragement and support, which motivated us a lot to complete our project work.

# ABSTRACT

Signature verification is one of the biometric techniques frequently used for personal identification. In many commercial scenarios, such as bank check payment, the signature verification process is based on human examination of a single known sample. Although there is extensive research on automatic signature verification, yet few attempts have been made to perform the verification based on a single reference sample. In this work, propose an offline handwritten signature verification method based on an explainable deep learning method (deep convolutional neural network, DCNN) and BRISK based feature extractionapproach. Binary Robust Invariant Scalable Key-points (BRISK) is characterized by the fact that computations are significantly less complex, its use distance rather than Euclidean distance and it is faster than the Fast algorithm and the SURF algorithm. We use the open-source dataset, Document Analysis and Recognition (ICDAR) 2011 SigComp, to train our system and verify a questioned signature as genuine or a forgery. All samples used in our testing process are collected from a new author whose signatures are not present in the training or other stages. From the experimental results, we get the higher accuracy in our testing dataset

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| **SIFR** | SIGNATURE FRAUD RECOGNITION |
| **DBS** | DYNAMIC BIOMETRIC SIGNATURE |
| **DTW** | DYNAMIC TIME WRAPPING |
| **SSIM** | STRUCTURAL SIMILARITY INDEX MEASURE |
| **SVM** | SUPPORT VECTOR MACHINE |
| **DCNN** | DEEP CONVOLUTIONAL NEURAL NETWORK |
| **CNN** | CONVOLUTIONAL NEURAL NETWORK |
| **BRISK** | BINARY ROBUST INVARIANT SCALABLE KEY-POINTS |
| **MLP** | MULTILAYER PERCEPTRON |

# CHAPTER-1
# INTRODUCTION

All of us have wondered at one time or another why it is that we are asked to sign a document rather than simply applying an inked fingerprint to the paper as a method of identification. Wouldn't it be just as simple to place a thumbprint on a check instead of a maker's signature? Wouldn't that foil forgeries? The argument that a signature is easier to read is invalid, as many signatures have evolved until they are nothing more than a symbolic representation of what was at one time handwriting and are now unreadable.

The answer to this riddle lies in the word "intent." By placing a signature on a document we are implying intent on our part to agree with circumstances provided by that check, codicil, agreement, contract, etc. One could easily place the fingerprint of someone recently deceased or unconscious upon a document if that was all that was required for authentication. This does not presuppose however, that the placement of an inked thumbprint next to a maker's signature on a check, about to be negotiated at a check cashing counter in a grocery store, would not be a help. The fingerprint's universal connotation would certainly, at the very least, be a deterrent to the individual intent upon passing a forged instrument.


Fig 1.1 HANDWRITING SIGNATURE EXAMINATIONS

The development, and examination, of a personal signature follows almost all of the concepts relating to **handwriting**. A signature may be nothing more than an extension of one's normal cursive handwriting, or it may have been personalized to such an extent that it now has few, if any, recognizable letter formations.

Signatures examined by the forensic document examiner for authenticity will eventually be categorized as genuine, or not genuine, if the examination leads to a definitive opinion. "Forgery" in a strict sense is a legal term and it's use as a conclusion should probably be avoided by the questioned document examiner. Often a signature in of itself may be valid, but the manner in which it

has been acquired or affixed to the document, or the sequence of events involved in its use are fraudulent. The product of a rubber stamp or autopen is certainly not a genuine signature but is most frequently used in a previously authorized capacity. While these signatures are not genuine, they are undeniably not forgeries in the legal sense. Terms such as "Forgery" and "Fraud" are perhaps best used by the legal community. Having said that, the reader may find that these terms are occasionally used in a descriptive manner throughout this text.

By definition, a genuine signature is the personal mark of an individual, written by that specific individual. It normally serves to indicate his or her acceptance of some set of circumstances, or to be the symbol associated with such an agreement. Keeping this definition in mind, we can discuss those other "signatures" that are not genuine.

**a.Indicators of Forgery**

General indications of non-genuineness may include the following:

**b.Blunt starts and stops**

The forger places the pen point in contact with the paper, and then starts writing. When he is finished with the name or some portion thereof, he stops the pen and lifts it from the surface. This may cause an emphasized blunt start or ending where the pen was placed in contact with the surface. At times this contact is held so long that if the pen contains a fluid ink it will wet the paper and migrate outward from the contact point or even through to the back of the paper.

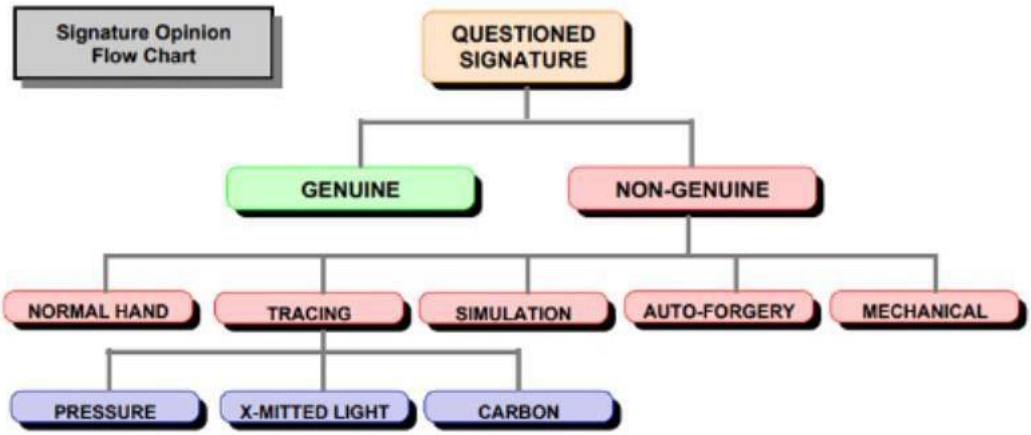



Fig 1.2: FORGERYOPINIONS FLOW CHART

There may be unnecessary and extraneous marks caused by pen starts and stops. The writer may decide after putting his pen in contact with the paper, that it is in the wrong spot, picks it up and moves it to a position considered to be more correct. Normally a signature's starts and stops are much more dynamic. The pen is moving horizontally before it contacts the paper and is lifted at the end while still in flight. This leaves a tapered appearance at the beginnings and endings of names or letters. There are, of course, exceptions to this.

**c.Pen lifts and hesitation**

This is occasioned when the pen stops at an unusual point in the writing; perhaps where a radical change in direction is about to take place or a new letter formation is about to be started. This may take on the appearance of a small gap in the written line where one is not expected, or an overlapping of two ink lines where there should be only one continuous line.

**d.Tremor**

Because the creation of most forms of non-genuine signatures are little more than drawings, the pen is moving so slowly that small, sometimes

microscopic changes in direction take place in what should be a fluid-looking line. The resultant line is not smooth, but reflects the "shaking" pen.

**e.Speed and pressure**

Again, because the pen is moving slowly rather than with the dynamic movement associated with most genuine writings, the ink line remains constant in thickness, resulting from the same constant pressure exerted on a slowly moving pen. There will be little, if any, tapering of internal lines.

**f.Patching**

Infrequently, but at one time or another, most of us have made an error while writing our own signature. Some individuals may leave the signature alone, caring little about the mistake or imperfection, while others will simply "fix" the signature by correcting the offending portion. This may be done in order to make the signature more readable, or because a defect in the pen or paper has affected what we perceive to be our "normal" signature, or for some other reason that may even be subconscious. These "fixes" are usually patent, with no attempt made on the part of the writer to mask or otherwise hide the correction.

These signature corrections are quite different than the patching that is frequently found in non-genuine signatures. On these occasions, the writer is not attempting to make the signature more readable, but to make its appearance more pictorial correct. He is fixing an obvious defect that he perceives as detectable, and might uncover his fraudulent product and foil his scheme. Theseusually take the form of a correction to a flaw in the writing line rather than in the form of a letter. Extensions to entry or terminal strokes, or to lower descending portions of letters, along with corrections to embellishments, are typical of non-genuine patching.

There are times when some of these same forgery indicators will be displayed in genuine signatures. Aged or infirmed writers will frequently display similar patterns. The mere presence of these indicators does not mean that the signature under scrutiny is non-genuine, but should contribute to the overall determination as to genuineness. Alternately, the signature devoid of these indications may not be assumed to be genuine. The signature of an elderly individual may, for instance, be expected to contain tremor and hesitation. If, however, the questioned signature appears to be written in a fluid manner, on a higher skill level than what is expected, the red warning flag should be waving. This occurrence may itself be indicative of non-genuineness. Often, a forger, because of an inherent high skill level in his writing, may produce a product that contains fewer "indications" of forgery than the genuine writer's signature.

**g.Non-Genuine Signatures – Handwritten**

Non-genuine handwritten signatures may be generally categorized into one of four possibilities. While a determination of forgery may be possible, it is not always possible to assign the signature to one of these categories. It may, however, be prudent for the document examiner to do so when possible as the demonstration of non-genuineness may be much more effective.

**h.Normal Hand Forgery**

During the creation of this of non-genuine signature, the writer simply writes someone else's name. There is no attempt made to duplicate or make the forgery look like a genuine signature. Any resemblance to the genuine signatureis coincidental. Usually, the perpetrator of this signature does not have a model signature at hand and/or the skill level or forethought to attempt an emulation. If he does not attempt to impart disguise to the writing, the resultant product will display characteristics of the forger's own handwriting. Armed with

adequate standards of both the individual whose name is being used and exemplars of the suspect, the document examination may be definitive to the point that not only is the signature opined not genuine, but the forger is also identified. (**Normal Hand Forgery**).

**i.Simulation**

The simulated signature, or "free hand forgery" as it is sometime known, is the usual bill of fare for the questioned document examiner. This forgery is constructed by using a genuine signature as a model. The forger generates an artistic reproduction of this model. Depending on his skill and amount of practice, the simulation may be quite good and bear remarkable pictorial similarity to the genuine signature.

Many simulations created with a model at hand will contain at least some of the general indicators of forgery, such as tremor, hesitation, pen lifts, blunt starts and stops, patching, and static pressure. They will have a slow "drawn" appearance. The practiced simulation is most often a higher quality creation in that the model signature has been memorized and some of the movements used to produce it have become semi-automatic. This simulation can be written with a more natural fluid manner.

Closely related to this form of identification process is that of determining the number of different forgers from a quantity of simulations. On occasion there will be two or more forgers attempting to reproduce the same signature. It may be possible to group or associate simulations of the same name by the combinations of defects within the forgeries. By associating and grouping the similar defects (when compared to the genuine signature) it may be possible to conclude and illustrate that there are indeed, two or more different forgers. (**Simulation**).

**j.Tracing**

Traced forgeries are generally created by one of three methods: "transmitted light," "carbon intermediate," or "pressure indented image." While tracings may not normally present much of a challenge to the document examiner trying to determine genuineness, the ability to identify the perpetrator is totally precluded. Tracing another's signature, or for that matter another's handwriting, is the paramount form of disguise.

signature by stylus or pen or other pointed implement is usually indicative of a pressure or carbon tracing. Again, caution must be exercised if a second ink line is present in a genuine signature. The immediate assumption by the uninitiated examiner that this signature is itself a carbon-type tracing can be a source of error.

On occasion, signatures that were executed while the writing paper was on a rough surface (matte finish) contain the illusion of tremor created by simulation or tracing. Close examination will reveal that this tremor is much too abundant and evenly spaced. There will be little, if any, variation in the tremor and the peaks and valleys of the rough surface will be embossed into the written line. (**Tracing**).

**k.Transmitted Light Tracing**

The transmitted light tracing is the simplest of the tracings to produce and the one most often encountered. The paper that is to receive the spurious signature is placed over a document bearing the genuine signature. These documents are then aligned so as to put the genuine signature directly under the selected location for the forgery. These two papers are then held up to a window or other light source, and the transmitted signature image is traced on the receiving document.

The indicators of a transmitted light tracing are similar to that of a simulation and the two are difficult to tell apart (unless the model for the tracing is located). Height ratios and proportions in the transmitted light tracing are generally right on the money, however. These two features are frequently incorrect in the simulation.

**l.Carbon-Medium Tracing**

At times, a carbon-medium tracing is the method of choice, especially if the document to receive the tracing is too heavy a weight, such as cardboard, to allow for a good light transmitted image.

Normally, the area to receive the signature is covered with a piece of carbon paper which in turn has the model signature placed upon it and aligned with the area that is to receive the image. The model signature is then traced over with a pen or other pointed implement. This procedure will impart a carbonimage of the signature on the receiving document. This image is then overwritten with a pen. Often this pen will be a broad-tipped instrument such as a felt-tip or fountain pen. This wider ink line serves to hide the carbon image better than a ballpoint pen.

**m.Pressure Indented Tracing**

Similar to a carbon paper tracing, the indented line tracing is produced in essentially the same manner, but does not employ any intermediate reproduction medium. Heavier pressure is used when tracing over the model signature. This pressure leaves an indented “signature” on the receiving document. This is then covered over with a broad-tipped pen, although ballpoint is found on occasion. Almost invariably, the writer misses portions of the indented line. This error may be easily observed using glancing (oblique) light. Other general indications of non-genuineness are similar to those found in simulated forgeries. In both the carbon-medium and indented line tracing, the forger is faced with an paradoxical situation.

**n.Transferred Forgery**

On rare occasions, an innovative form of spurious signature may be encountered that can best be equated with a tracing, but in actuality differs from the conventional concepts of tracing because of its method of production.

Most traditional ballpoint pen inks employ an ethylene glycol medium as the base ingredient to carry dyes, extenders, plasticizers, and other ink components. A signature made by employing a pen using this ink may be "transferred" to another document by using ordinary waxed paper or freezer paper. By placing this form of medium over a genuine signature and rubbing the top of the paper vigorously, the wax that is in conjunction with the signature will melt and subsequently absorb some of the ethylene glycol-based ink line. This paper now containing a mirror image of the genuine signature is placed over another document that is to receive the forgery. The waxed paper is again rubbed briskly, melting the wax and ink composite. This process will result in a forgery that does not conform to, nor contain, the normal observable conditions that are associated with simulated or traced signatures. This is because, in essence, this signature was created by the signature holder's hand rather than the forger's. Indications of this process will be in the form of wax left behind that covers and surrounds the signature line. The signature itself will have a discernibly faded appearance and the edge of the ink line when viewed under low magnification will have a mottled look rather than sharp appearance.

**o.Auto-forgery**

The signature that does not satisfy the requirements for genuineness must necessarily be non-genuine. To use an old cliché, anything in between is similar to being slightly pregnant. It matters not how the conception (or in this case, deception) took place.

These signatures, commonly referred to as auto-forgeries, will usually be found on promissory notes, contracts, Constitutional Rights forms, confessions, closed-account checks, etc.

Initial observations of an auto-forgery often appear similar to what might be expected in a simulated forgery. Further inspection will almost always reveal remarkable internal similarities to the genuine signature. Why does this happen? The auto-forger, not knowing the perceptual abilities of someone that might examine the signature, incorporates gross changes to the larger, initial, or prominent letters. His usual response when confronted with a signature that he is denying is "I never make that letter(s) that way." Indeed he doesn't, but neither would a real forger. (**Auto-forgery**).

In essence then, while the forger creating a simulation does his best to make the prominent focal points of the signature look like the corresponding features in a genuine signature, the auto-forger goes out of his way to make them appear different. Similarly, the forger misses, or does not pay as much attention to the interior subtleties of a signature, while the auto-forger, because he is a creature of habit, produces these smaller intricate details correctly. Piece by piece, the simulation and auto-forgery are almost diametrical opposites. When an auto-forgery may be at hand, the questioned document examiner must remember the old adage that if something "looks that bad, it may be that good."

**p.Non-Genuine Signatures – Mechanical**

Mechanical signatures most often are those produced without the direct aid of the human hand. Signatures produced by auto-pens or writing machines, rubber stamps, and offset printing are examples of mechanical signatures. These imitation signatures differ from other non-genuine signatures in that they maybe legally genuine when their use has been authorized by the signature holder. These are prime examples of forensically non - genuine but legally authenticsignatures . However, when mechanical signatures are used in non-authorized capacities, they are quite simply forgeries. Rubber stamp signatures used by a secretary to sign company checks for the boss look the same as those produced by a burglar who stole the rubber stamp.

# CHAPTER-2

# LITERATURE SURVEY

## 2.1 SIFR-Signature Fraud Recognition

Mokshaguandam et al presented an Offline Signature Verification system, where a Convolutional neural network is made to learn appropriate features and classify the signature based on the user as well as its genuineness.

## 2.2 Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries

Sanchez et al implemented a methodology for evaluating the robustness of handwritten signature biometrics against forgeries. A particular emphasis has been applied in consider the viability of the attacks under operational environments. In order to carry out this work, not only a methodology but a toolbox has been developed. Such toolbox stores data, not only from a signing pad connected to a computer, but also from touch-screen devices such as smartphones and tablets. The proposed methodology has been tested by performing a robustness evaluation of a DTW-based algorithm, and with a database of genuine signatures acquired using a STU-500 pad as an input for the evaluation toolbox. Securing Document by Digital Signature through RSA and Elliptic Curve Cryptosystems.

## .2.3 Generating Off-line and On-line Forgeries from On-line Genuine Signatures

Ferrer et al developed a method based on the Kinematic Theory of Rapid Movements to generate both on-line and off-line skilled synthetic forgeries froma single on-line genuine specimen. The method consists of three steps: 1. The genuine on-line signature is decomposed as a sum of overlapped lognormal strokes, 2. The trajectory is modified by distorting the virtual target points andthe lognormal parameters, and 3. A new velocity profile is automatically synthetized from the 8-connected modified trajectory.

## 2.4 Offline Signature Verification and Forgery Detection Approach

Ghanim et al presented an automatic off-line system for signature verification and forgery detection. Different features were extracted and their effect on system recognition ability was reported. The computed features include run length distributions, slant distribution, entropy, Histogram of Gradients features (HoG) and Geometric features. Finally, different machine learning techniques were applied on the computed features: bagging tree, random forest and Support Vector Machine (SVM). it was noticed that SVM outperforms the other classifiers when applied on HoG features. Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries.

## 2.5 A Biometric Attack Case Based on Signature Synthesis

Ferrer et al analysed a new conceivable attack for an on-line signature biometric scheme. The attack consists in interpolating a smoothed 8-connected version of the forged signature and selecting the most relevant salient points, skipping those that belong to tremor or indecisive movements due to the faking procedure. The Sigma-Lognormal model is then used to synthetize the new on-line signature in the hope of obtaining an improved imitation.Digital signature scheme based on truncated polynomial over finite fields.

## 2.6 Image Forgery detection on cloud

James et al presented a paper that was based on image forgery detection on cloud. Image forger detection is classified into two: passive and active. Active approach includes digital signature and watermarking whereas the Passive approach includes detection of the tampered area using copy move and splicing techniques. Here we are using Canny Edge Detection Algorithm which mainly uses splicing. In this paper, we are also comparing canny edge detection and SSIM. Enhanced on-line signature verification based on skilled forgery detection using Sigma-LogNormal Features.

# CHAPTER-3

# EXISTING SYSTEM

## Handwritten Signature Verification using Deep Learning

Every person has his/her own unique signature that is used mainly for the purposes of personal identification and verification of important documents or legal transactions. There are two kinds of signature verification: static and dynamic. Static(off-line) verification is the process of verifying an electronic or document signature after it has been made, while dynamic(on-line) verification takes place as a person creates his/her signature on a digital tablet or a similar device. Offline signature verification is not efficient and slow for a large number of documents. To overcome the drawbacks of offline signature verification, it have seen a growth in online biometric personal verification such as fingerprints, eye scan etc.

The handwritten signature is a behavioral biometric which is not based on any physiology characteristics of the individual signature but on the behaviorthat change over time. Since an individual's signature alters over time the verification and authentication for the signature may take a long period which includes the errors to be higher in some cases. Inconsistent signature leads to higher false rejection rates for an individual· who did not sign in a consistent way.

### 3.1 Data Acquisition

Handwritten signatures are collected and some unique features are extracted to create knowledge base for each and every individual. A standard database of signatures for every individual is needed for evaluating performance of the signature verification system and also for comparing the result obtained using other techniques' on the same database. Fig.3. 1 and Fig.3. 2 show samples of indivisible forged and real signatures respectively.

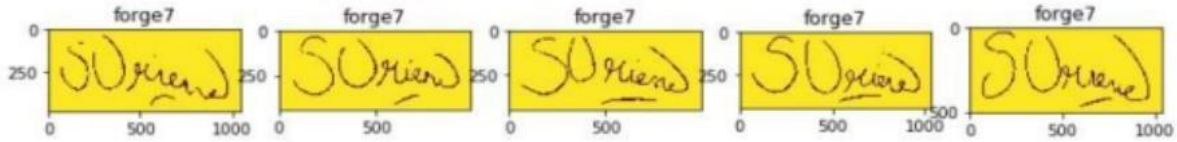



Fig 3.1 FORGED SIGNATURE

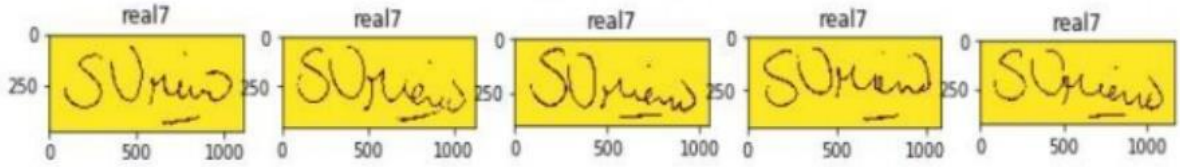



Fig 3.2 REAL SIGNATURE SAMPLES

### 3.2 Pre-processing

The system must be able to maintain the high performance regardless of the size and slant given for the signature. It should be important that the system must be insensitive enough for the correction in the signature image. The image matrix is rescaled to standard resolution which is 512 X 512 in this case.

### 3.3 FileManagement

Firstly, we take the name of the subject as an input. Then the directory of the raw images is loaded in to the file system. We have to include Real signatures as well as Forgeries in batches for bulk processing. The destination directory has to be included which consists of Training and Testing as sub-directories. This will make the system avoid directory error. Then, the images from the selected source directories, i.e., Real and Forgery are loaded as lists into the system. Each image from the list is loaded, processed and then final image file is created. The images are split into the respective ratio between the destination path sub-directories.

### 3.4 TRAINING THE MODEL

In this application, we use CNNs(or ConvNet) which is a class of deep, feed-forward artificial neural networks that has successfully been applied to analyzing visual imagery. CNNs were inspired by biological processes in that

the connectivity pattern between neurons resembles the organization of the animal visual cortex. In our work, we use the Keras library with the TensorFlow backend to implement SVM. The directory of preprocessed images is loaded and then we train the model to evaluate the performance.

### 3.5 IMPLEMENTATION

In this work, the signature images are stored in a file directory structure which the Keras Python library can work with. Then the SVM has been implemented in python using the Keras with the TensorFlow backend to learn the patterns associated with the signatures. Then the model derived has been verified using accuracy and loss me trics to see how well the model has fit the data. Finally, the model has been tested by using a signature from a holdout set to see if the predictions are correct. Table1 contains a detailed architecture model of the implementation.

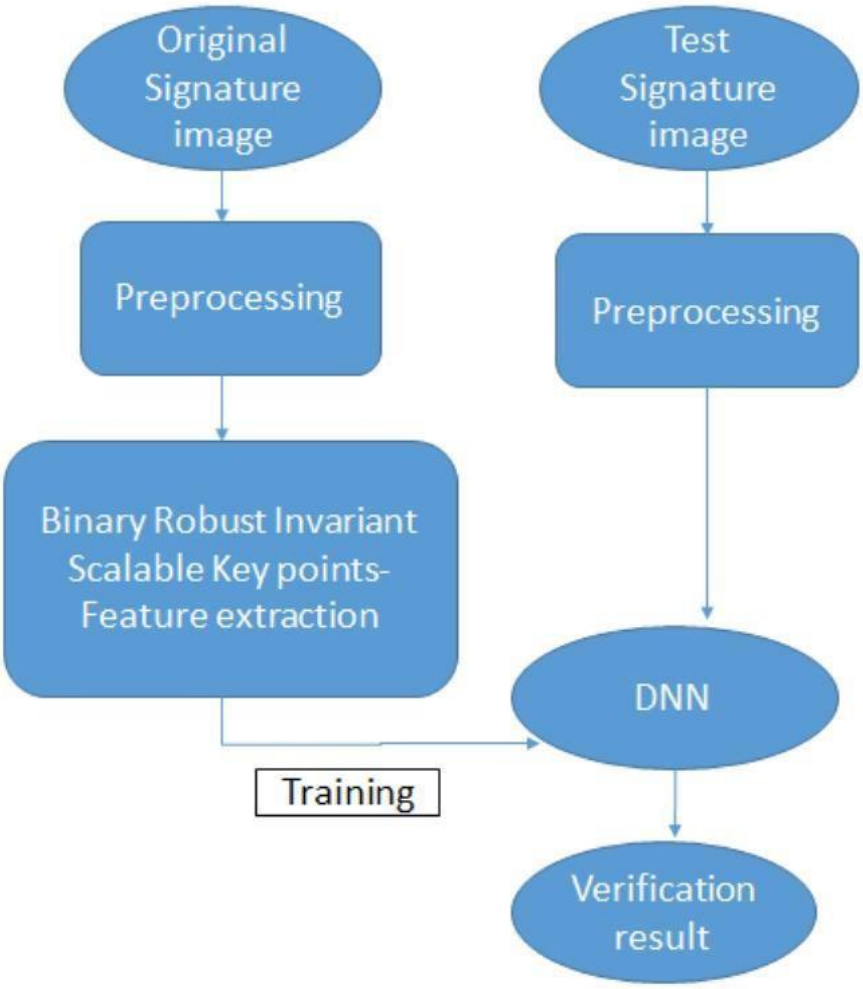
An image goes through a series of convolution and max pooling layers which are in an alternating fashion. When the image goes through convolution process, a predefined number of feature maps are created which are fed into a max pooling layer, which creates pooled feature m aps from the feature maps received from the convolution layer which is before it. This pooled feature map is sent into the next convolution layer and this process continues until we reach the fourth max pooling layer. The pooled feature map from the last m ax pooling layer is flattened and sent into the fully connected layers. After several rounds of forward and backward propagation, the model is trained and a prediction can now be made.

# CHAPTER-4

## PROPOSED METHODOLOGY

Signature verification is one of the biometric techniques frequently used for personal identification. In many commercial scenarios, such as bank check payment, the signature verification process is based on human examination of a single known sample.Few attempts have been made to perform the verification based on a single reference sample.

In this project, an off-line handwritten signature verification method based on an explainable deep learning method (deep convolutional neural network is proposed, DCNN) and Binary Robust Invariant Scalable Key-points (BRISK) feature extraction approach used.




PROPOSED FLOWCHART FOR SIGNATURE VERIFICATION

### 4.1 Convolutional Neural Network (CNN)

A convolutional neural network (CNN) is a class of deep learning networks that has achieved state-of-the-art performance in many computer vision areas, such as image classification, pattern recognition, object detection, etc. Typically, CNN consists of three main types of components: convolutional layer, pooling layer, and fully-connected layer, as illustrated in Figure 4.2.

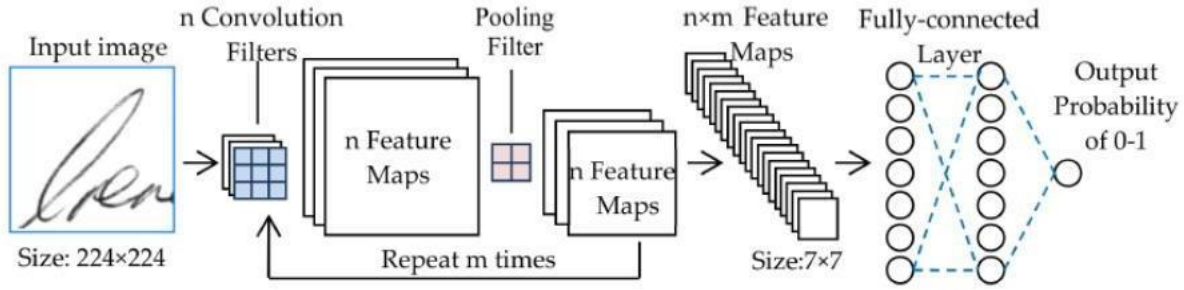



Fig 4.2 SCHEMATIC DIAGRAM OF CNN

The convolutional layer uses multiple convolution filters (or convolution kernels) to extract the higher-level features from the low-level information, such as detecting the edges, corners, connection points, and other features from input images. Since multiple convolution filters will dramatically increase the size of the feature map and accompanied by tedious calculations, we use the pooling layer to reduce the feature map size and thus leads to a faster convergence rate for networks.

Finally, all of the multi-dimensional feature maps are converted into a one-dimensional feature vector and input to the fully-connected layer. The fully-connected layer is basically a regular multilayer perceptron (MLP) and is used to generate class predictions for the further classification task. In this paper, we use VGG19 architecture in our experiments, since both architectures are well-designed and have shown their great ability in ImageNet competition.

## 4.2 Explainable Deep Learning

Although deep learning models have shown their superior performance in various areas, they often lack interpretability. That makes them hard to adopt for forensics and other areas that require rigorous evidence. Therefore, explainable (or interpretable) deep learning methods have attracted more and more attention in recent years. In the field of computer vision, it is proposed a gradient-based visual saliency method to visualize the decision-making process of neural networks. Its main idea is to show the image pixels (a saliency map) which is sensitive to the predictions of a network. This saliency map is obtained by computing the gradient of the class-specific score from a given classifier. The gradient indicates how much the change in a pixel that influences the classifier output. The gradient map itself can be considered as the saliency map in our cases, as shown in Figure 4.3.

**Strategies for Using Only Single Genuine Reference Signature**

The handwriting signatures have high intra-class variability. This key factor presents a particularly difficult condition for signature verification with single reference signature.

1. We assume that there are a lot of useful local features (such as the features of strokes lines, starting, turning, and ending points) generally scattered across the whole signature image. Based on this condition, we convert a single signature image into many overlapping sub-image blocks. Since our method has the capability of extracting local features, these sub-image blocks can be used as training samples. In addition, we also apply some data preprocessing techniques which are commonly used for deep learning and image processing tasks (such as sample screening and data augmentation). In this way, the number of training samples can be expanded.

### 4.3 Data Preprocessing

Before extracting the features by our CNN network, some data preprocessing must be performed: background noise reduction, data augmentation, and screening. The goal of our preprocessing approach is to increase the number of samples by converting a single original signature image into many sub-image blocks, and to filter the sub-image with enough stroke pixels as the training dataset which is done by using BRISK algorithm.

For example, the No.1 genuine signature from author ID 14 is converted to 6.828 new sub-images for the VGG19 training dataset. The steps of the preprocessing are shown as follows:

1. We convert the raw image into a grayscale image and then save it as a 24-bit BMP file.

2. We use a block-based method for data augmentation. We set a window as a sliding mask to get a sub-image block from the original image. The window size depends on the network architecture. In our case, the VGG19 network uses 224 _ 224 window size and the Inception-v3 network uses 299 _ 229 one. Then we shift the mask window by 20 pixels each time to repeat the process fromleft-to-right then top-to-bottom. After finishing the processes above, we can obtain about 6.828 overlapping sub-image blocks from an original signature image.

3. To reduce paper texture and background noise caused by the optical scanning unit, we brighten the sub-image by 7.5%, and the method is to multiply each RGB pixel values by 1.075 directly.

In our experiment, the background noise is biased towards light colors. Therefore, this method can remove most of the noise without destroying the features of the handwriting strokes (the excessive brightness may damage the features of handwriting signature).

4. We rotate each sub-image blocks clockwise by a predefined angle and repeat

the process until a full 360 degrees rotation is done. Note that our experiment involves 6 sub-datasets includes: genuine signature for training, forged signature for training, genuine signature for verification, forged signature for verification, genuine signature for testing, and forged signature for testing.

For each sub-datasets, we set the rotation angle as follows: the genuine signature used for training is rotated by 10 degrees each time. The forged signature used for training is rotated by 20 degrees each time, and the rest of the sub-datasets are only used for verification and testing, so we set it to 60 degrees to save the computation cost. In order to prevent the large class-skew of our training dataset (due to the number of genuine samples is far less than the forgeries). We deliberately use a smaller rotation angle (10 degrees) to increase the sample size of the genuine signature dataset which is used for training.

5. We check each sub-image block to see if it contains enough information for feature extraction and set some inspection thresholds based on experience. We set 250 as the threshold grayscale value, and consider a pixel whose grayscale exceeds the threshold as a valid pixel. Then, if a sub-image block has over 7.5% valid pixels, we classify it as a valid sample. Conversely, we regard it as an invalid sample and drop it.

### 4.4 BRISK Algorithm

Binary Robust Invariant Scalable Key-points (BRISK) is characterized by the fact that computations are significantly less complex, its use distance rather than Euclidean distance and it is faster than the Fast algorithm and the SURF algorithm. According to [8], BRISK is a new algorithm designed to identify key points that match the description by evaluating this algorithm

shows that the performance of high quality compared to calculations less complex. In addition, the algorithm BRISK has faster implementation than the SurF algorithm.

From the above figure, we can see that they consist of a binary series and the comparison tests between the points are simple and that the neighborhood points are in specific circles with one center and equal spacing. BRISK is easily scalable for faster execution by reducing the number of sampling-points in the pattern at some expense of matching quality, which might be affordable in a particular application. Moreover, scale and/or rotation invariance can be omitted trivially, increasing the speed as well as the matching quality in applications where they are not needed [8].

Sub-image blocks are theoretically qualified as training samples. Furthermore, our preprocessing methods not only augment the number of samples and increase the feasibility of deep learning, but also have the following benefits:

Firstly, using sub-image blocks as the training and verification data can effectively prevent a small number of local features from dominating the whole CNN and BRIISK system. Secondly, by applying the rotation process, we can make our CNN system focus on the rotation-invariant features and reduce the unnecessary influence from di_erent handwriting angles. Thirdly, the created rotation sub-image blocks can simulate the signature intra-class variability to a certain extent. And we have found that increasing the number of rotations can help improve system performance.

# CHAPTER-5

# SOFTWARE SPECIFICATION

SOFTWARE REQUIRED:MATLAB 2022

HARDWARE REQUIRED:

System : Windows Xp Professional Service Pack 2

Processor : Up to 1.5 GHz

Memory : Up to 512 MB RAM

DIP:

Introduction

Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image de-blurring, feature detection, noise reduction, image segmentation, spatial transformations, and image registration. Many functions in the toolbox are multithreaded to take advantage of multi-core and multiprocessor computers. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, giga-pixel resolution, ICC-compliant color, and tomographic images. Graphical tools let you explore an image, examine a region of pixels, adjust the contrast, create contours or histograms, and manipulate regions of interest (ROIs). With the toolbox algorithms you can restore degraded images, detect and measure features, analyze shapes and textures, and adjust the color balance of images.

**Key Features**

Image enhancement, filtering, and de-blurring

Image analysis, including segmentation, morphology, feature extraction, and measurement

Spatial transformations and image registration

Image transforms, including FFT, DCT, Radon, and fan-beam projection

Workflows for processing, displaying, and navigating arbitrarily large images

Modular interactive tools, including ROI selections, histograms, and distance measurements

ICC color management

Multidimensional image processing

Image-sequence and video display

DICOM import and export

Importing and Exporting Images

Image Processing Toolbox supports images generated by a wide range of devices, including digital cameras, satellite and airborne sensors, medical imaging devices, microscopes, telescopes, and other scientific instruments. You can visualize, analyze, and process these images in many data types, including single- and double-precision floating-point and signed and unsigned 8-, 16-, and 32-bit integers.

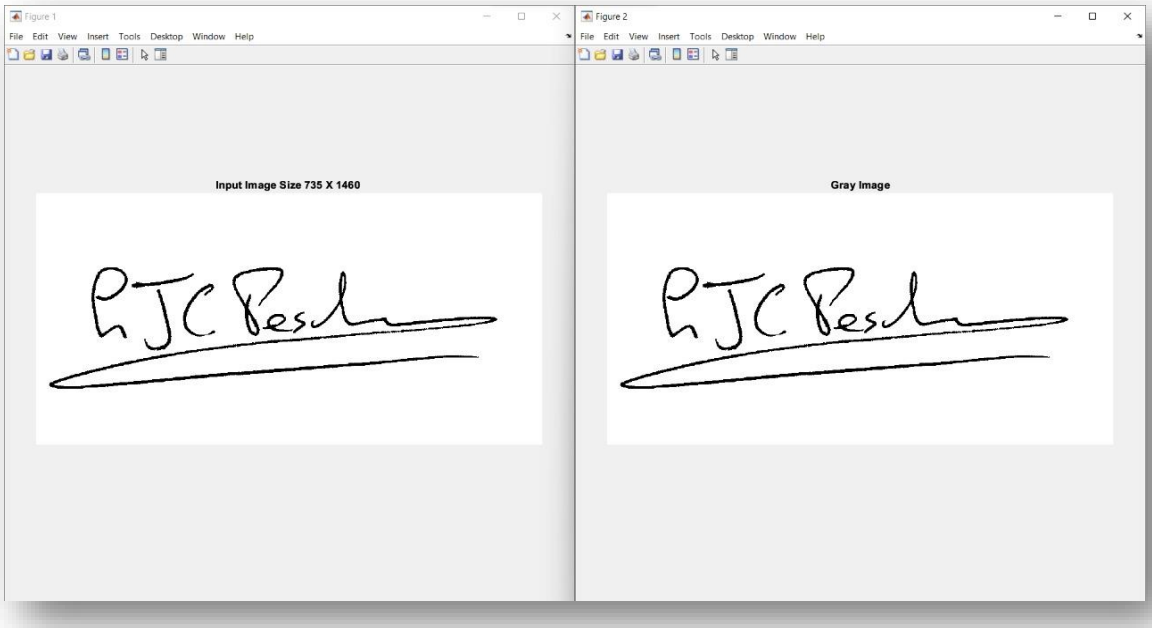
There are several ways to import and export images into and out of the MATLAB® environment for processing. You can use Image Acquisition Toolbox™ to acquire live images from Web cameras, frame grabbers, DCAM-compatible cameras, and other devices. Using Database Toolbox™, you can access images stored in ODBC/JDBC-compliant databases.

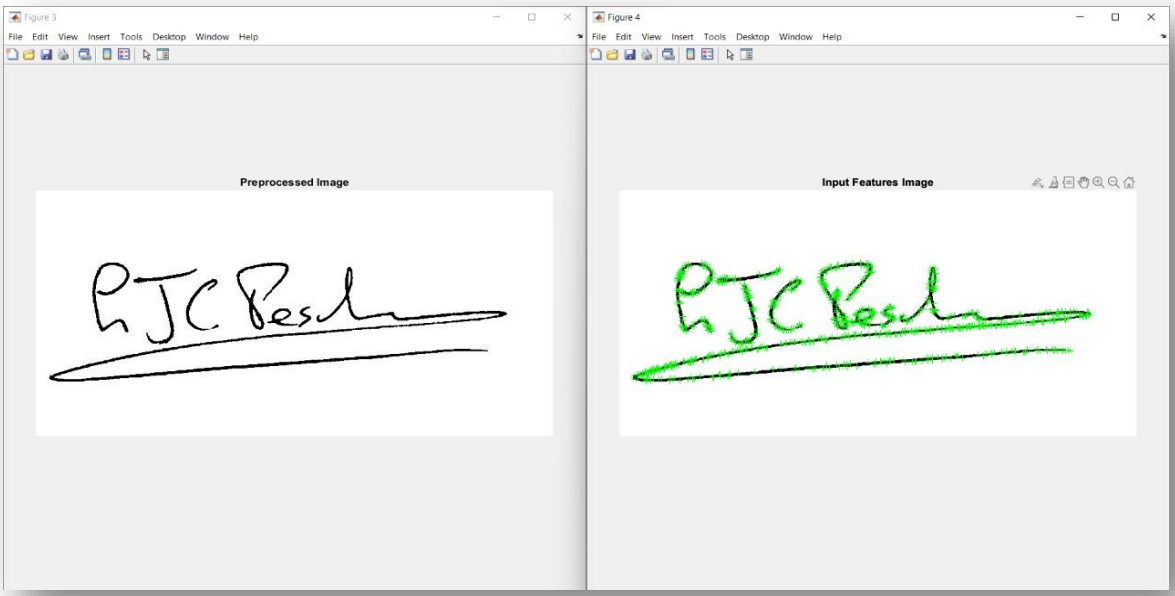
MATLAB supports standard data and image formats, including JPEG, JPEG-2000, TIFF, PNG, HDF, HDF-EOS, FITS, Microsoft® Excel®, ASCII, and binary files. It also supports the multiband image formats BIP and BIL, as used by LANDSAT for example. Low-level I/O and memory mapping functions enable you to develop custom routines for working with any data format.

Image Processing Toolbox supports number of specialized image file formats. For medical images, it supports DICOM file format,including associated metadata Interfile formats. The toolbox can also read geospatial images in the NITF format and high dynamic range images in the HDR form

# CHAPTER-6

# RESULT AND DISCUSSIONS



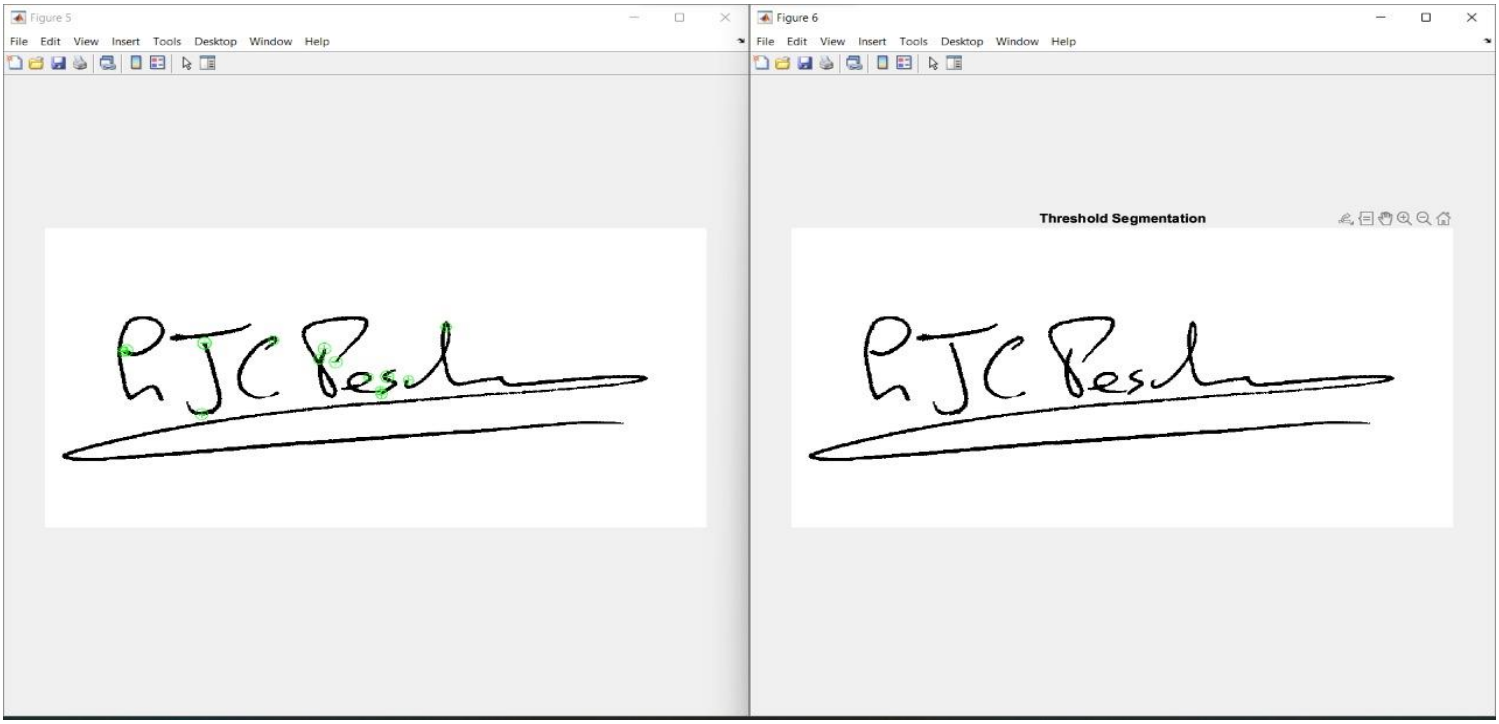
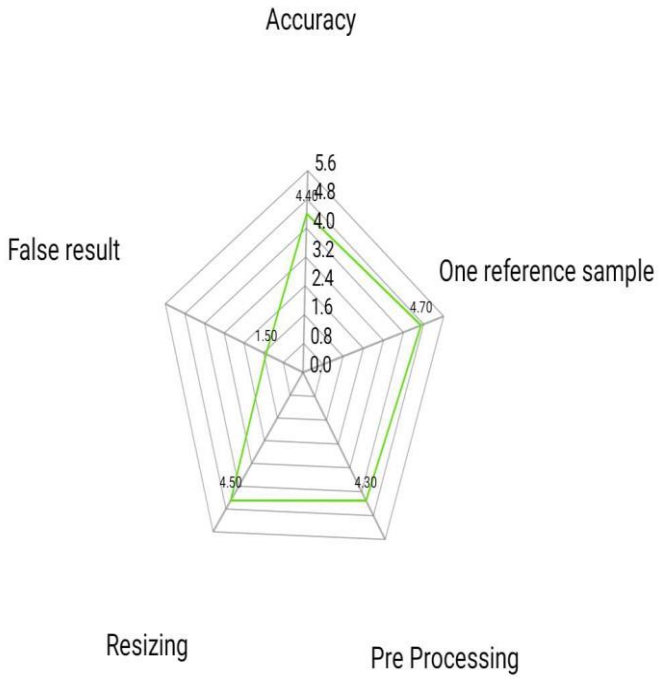
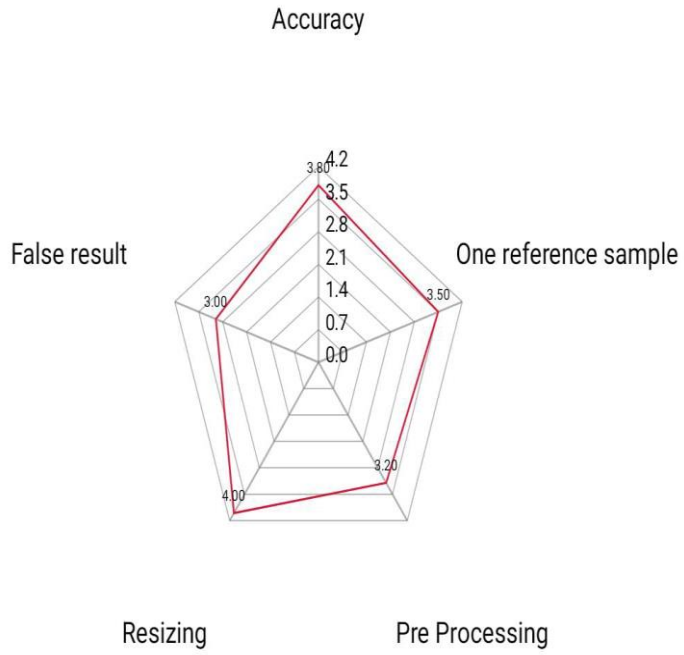


Figure 5
File Edit View Insert Tools Desktop Window Help
Figure 6
File Edit View Insert Tools Desktop Window Help
Threshold Segmentation


Help Dialog
Detected Status: Original
OK

| SIGNATURE VERIFICATION USING DEEP LEARNING | SIGNATURE VERIFICATION USING OTHER APPLICATIONS |
| --- | --- |
|  |  |

# CHAPTER-7

# CONCLUSION

In this project, we proposed an off-line handwritten signature verification method by using single known sample and based on a deep CNN network and BRISK algorithm. We ensure the reliability of the experimental results through a series of methods, including preprocessing (removing background noise), designing controlled groups for different sample sizes and network architectures, and applying visualization techniques (to provide interpretability of the model). The experimental results indicate that it is possible to perform automatic signature verification by single known sample.

**REFERENCES:**


- Jiang, Jiajia, et al. "DsDTW: Local Representation Learningwith Deep soft-DTW for Dynamic Signature Verification." IEEE Transactions on Information Forensics and Security (2022).

- Okawa, Manabu. "Online Signature Verification UsingLocally Weighted Dynamic Time Warping via Multiple Fusion Strategies." IEEE Access 10 (2022):

- Li, Huan, Ping Wei, and Ping Hu. "AVN: An Adversarial Variation Network Model for Handwritten Signature Verification." IEEE Transactions on Multimedia 24 (2021):

- Patil, Punam R., and Bhushan V. Patil. "A Review-SignatureVerification System Using Deep Learning: A Challenging Problem." (2021).

- Tolosana, Ruben, et al. "DeepSign: Deep on-line signature verification." IEEE Transactions on Biometrics, Behavior, andIdentity Science 3.2 (2021): 229-239.

- Wei, Wei, et al. "Spline interpolation and deep neural networks as feature extractors for signature verificationpurposes." IEEE Internet of Things Journal (2021)

- Malik, Jameel, et al. "Deepairsig: End-to-end deep learningbased in-air signature verification." IEEE Access 8 (2020):

- Diaz, Moises, et al. "Investigating the common authorship of signatures by off-line automatic signatureverification without the use of reference signatures." IEEE Transactions on Information Forensics and Security15 (2019):

- Ren, Yanzhi, et al. "Signature verification using criticalsegments for securing mobile transactions." IEEE Transactions on Mobile Computing 19.3 (2019):

- Karouni, Ali, Bassam Daya, and Samia Bahlak. "Offline signature recognition using neural networks approach."Procedia Computer Science 3 (2011)

-