SIGNATURE EXTRACTION AND VERIFICATION FOR BANKING SECTOR

FINAL REVIEW DOCUMENT

March 28, 2023

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING (SITE)

COURSE NAME : *BIOMETRIC SYSTEMS*

COURSE CODE *: SWE 1015*

SLOT*: G2*

FACULTY *: Dr.RAMYA G*

Submitted by

VIGNESH M - 20MIS0175

SADHANA S - 20MIS00185

KAUSHIK M- 20MIS0306

ROHITH RJ - 20MIS0324

KAVIYA K - 20MIS02399

1 ABSTRACT:-

The verification of handwritten signatures is one of the oldest and the most popular biometric authentication methods in our society. As technology improved, the different ways of comparing and analysing signatures became more and more sophisticated. Personal identification can be accomplished through the use of the signature. It is used for authentication or concluding document. In order to reduce frauds in banks, signature verification is very much important. The main aim of the proposed system is to use signature verification to enhance security in the financial environment.Our system extract handwritten signature from scanned documents using Open CV and scikit-image on python. We use connected component algorithm to extract signature from the scanned documents. Then we mathematically evaluates the similarity of scanned signature with a comparison signature. The signatures compared and the percentage of their match will be displayed on the screen.

2 INTRODUCTION:-

Over the years, biometric systems have exponentially evolved and adapted to grant access to systems, devices, and data [42]. They provide high level of security compared to other authentication methods such as Personal Identification Number (PINs) and passwords. The biometric personal verification and identification rely on measurable, distinctive physical traits (such as fingerprints, hand geometry,faces, iris scans, or DNA) or behavioural traits have experienced an accelerat- ing expansion (gait, voice etc.).

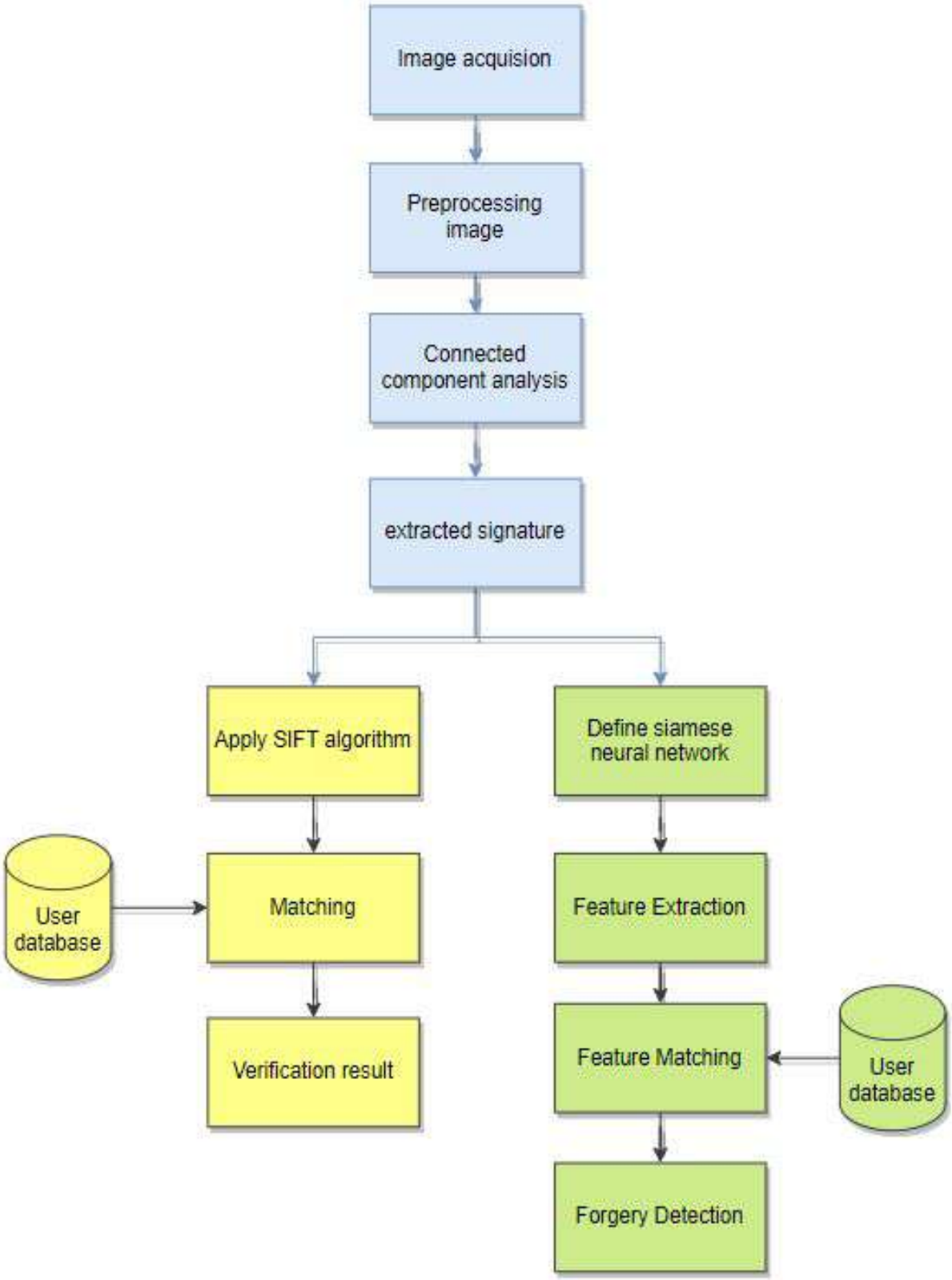
A signature is a behavioural biometric system. In the field of banking, signature recognition will reduce the time of bank transactions, and customer authentication with these technologies does not require memorization of personal identification numbers to identify the legal cardholder, which makes it quite user-friendly [46]. A signature is conventionally accepted as a biometric for identification of an individual, it represents some behavioural properties of a person, thus widely accepted in schools, banks, organisations hospitals as a means for verification and identification [15].

There are two methods that may be used for offline signature verification. the second method, known as writer-independent signature verification [13]. In offline systems the input is a static image that is scanned and used for analysis. Both of- fline and online systems are used to detect various types of forgeries [23]. Our system takes various feature points of a given signature and compares them with the test signatures feature points by graph matching classifier [33].

3 KEYWORDS:-

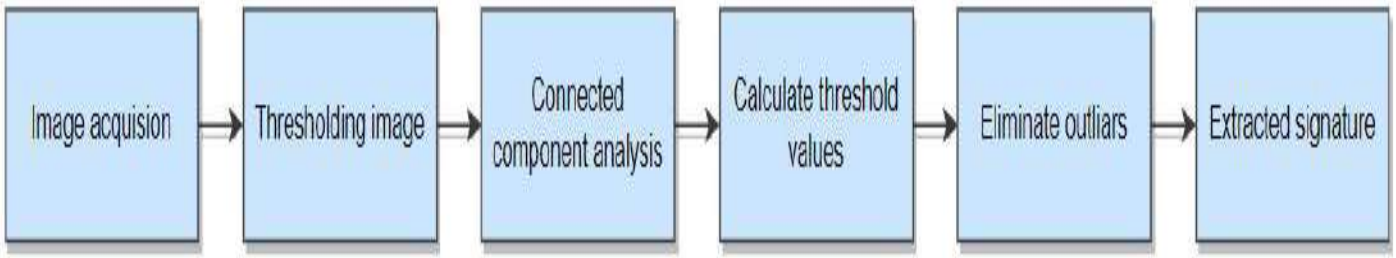
1. Signature verification
2. Cheque Authorization
3. Computer Vision
4. Python
5. Feature extraction

4 ARCHITECTURE OF THE PROPOSED SYSTEM:-



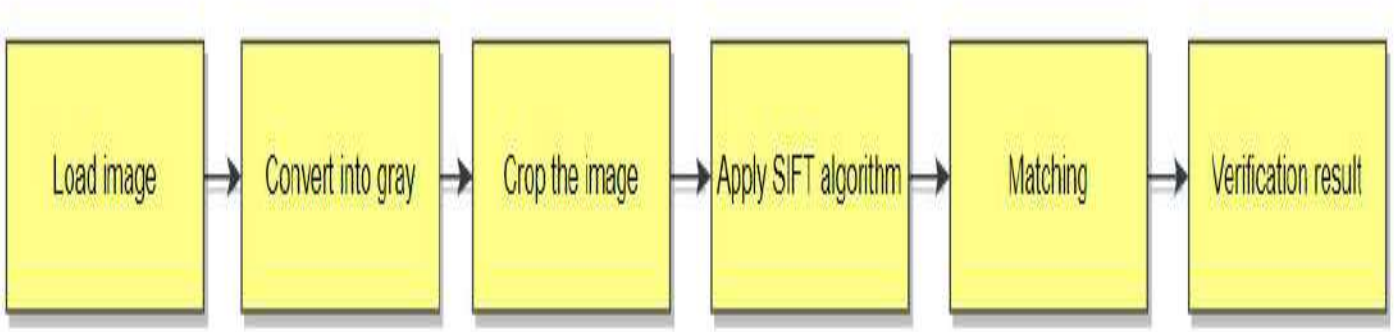
5 MODULE EXPLANATION:-

5.1 MODULE 1:- SIGNATURE EXTRACTOR



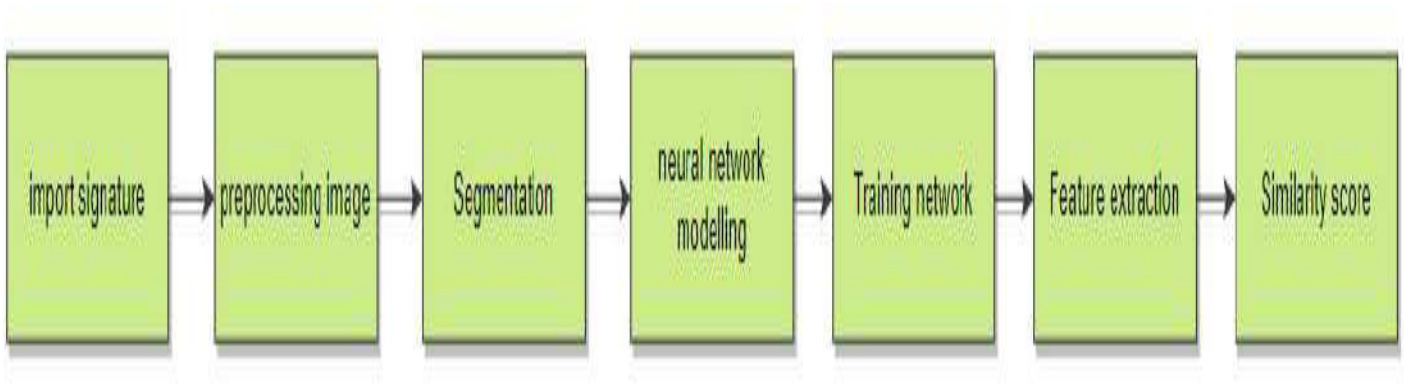
In this module, we extract the signatures from scanned documents based on "connected component analysis". In image processing, a connected components algorithm finds regions of connected pixels which have the same value. We calculate the threshold value to detect the outliars.

5.2 MODULE 2:- SIGNATURE VERIFICATION



In this module, We verify signature by using scale invariant feature transform (SIFT) algorithm. we find the key points from the signature then compare those key points (nodal points) with the test signature and then we will print the match score and shows whether the signature match or not.

5.3 MODULE 3:- SIGNATURE FORGERY DETECTION



In this module, we use Siamese neural network to extract the features of the signature. Then we determine the signature status using the similarity score between the signatures.

6 DETAILED MODULE DESCRIPTION:-

IMAGE ACQUISION:

In a signature verification system, image acquisition refers to the process of capturing a digital image of a signature using a device such as a scanner. The signature image is then used as input for the signature verification algorithm to determine if the signature is genuine or not.

PRE PROCESSING IMAGE:

Pre-processing of the signature image is an essential step in signature verification systems, as it helps to improve the quality of the image and enhance the accuracy of the signature verification algorithm.

The following are some common pre-processing techniques used in signature verification systems:

1. Image resizing and normalization
2. Noise reduction
3. Edge detection and segmentation
4. Feature extraction

CONNECTED COMPONENT ANALYSIS:

Connected component analysis (CCA) is a technique used in signature verification systems for the segmentation and extraction of individual characters or components from a signature image. The basic idea behind CCA is to group together pixels that belong to the same object, based on their connectivity or proximity.

EXTRACTED SIGNATURE:

In signature verification systems, the extracted signature refers to the portion of the signature image that has been segmented and processed to create a digital template for comparison with other signatures. The extracted signature typically includes the individual components or strokes that make up the signature, along with any additional features or information that has been extracted during preprocessing or feature extraction.

SIFT ALGORITHM:

The Scale-Invariant Feature Transform (SIFT) algorithm is a feature extraction technique used in signature verification systems to identify and match individual features or keypoints in a signature image. The SIFT algorithm is designed to be invariant to scale, rotation, and translation, making it well-suited for the recognition of complex and variable signatures.

In a signature verification system, the SIFT algorithm works by identifying keypoints in the signature image, which are areas that have distinct and recognizable features, such as corners, edges, or blobs. The algorithm then extracts a set of descriptors for each keypoint, which capture the local characteristics of the region around the keypoint, such as gradient orientation and magnitude.

SIGNATURE MATCHING:

Signature matching is a crucial step in signature verification systems, which involves comparing the features of the extracted signature with a reference signature to determine whether the signature is genuine or fraudulent. The comparison is typically based on various features of the signature, such as stroke direction, curvature, and spacing, which are extracted using pre-processing and feature extraction techniques such as CCA and SIFT.

SIAMESE NEURAL NETWORK:

Siamese neural network is a deep learning architecture that has been successfully applied in signature verification systems for matching and comparing signatures. The Siamese network consists of two identical neural networks, which are trained simultaneously with the same input data. The networks are used to extract and compare features from two signature images and produce a similarity score, which indicates how similar the two signatures are.

FEATURE EXTRACTION:

Feature extraction is a critical step in signature verification systems, which involves identifying and extracting unique features or characteristics of a signature image that can be used to differentiate between genuine and forged signatures. These features are typically used to create a digital representation or template of the signature, which can be compared to a reference signature to determine authenticity.

FEATURE MATCHING:

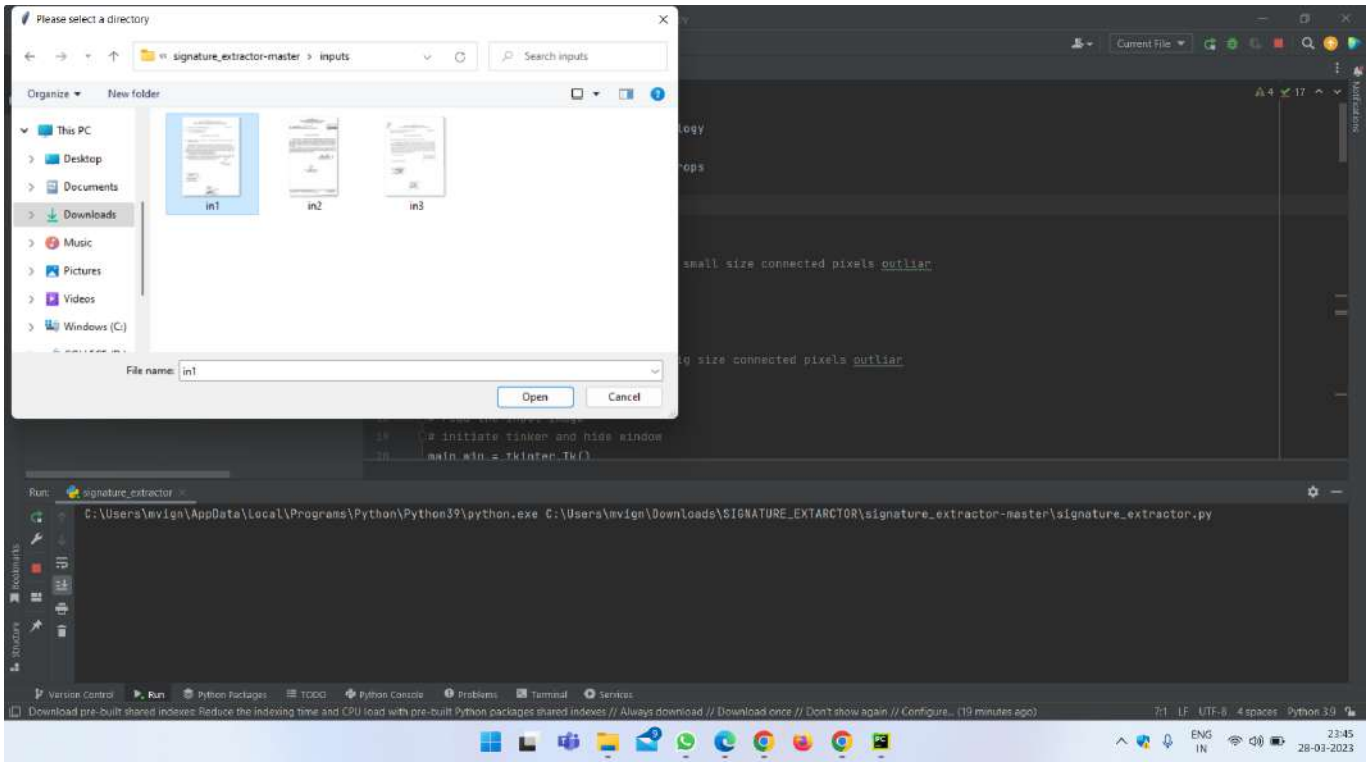
Feature matching is a critical step in signature verification systems, which involves comparing the extracted features of a signature image with those of a reference signature to determine if the signature is genuine or forged. The feature matching process is typically performed using a similarity metric, which calculates the similarity score between the extracted features and the reference features.

FORGERY DETECTION:

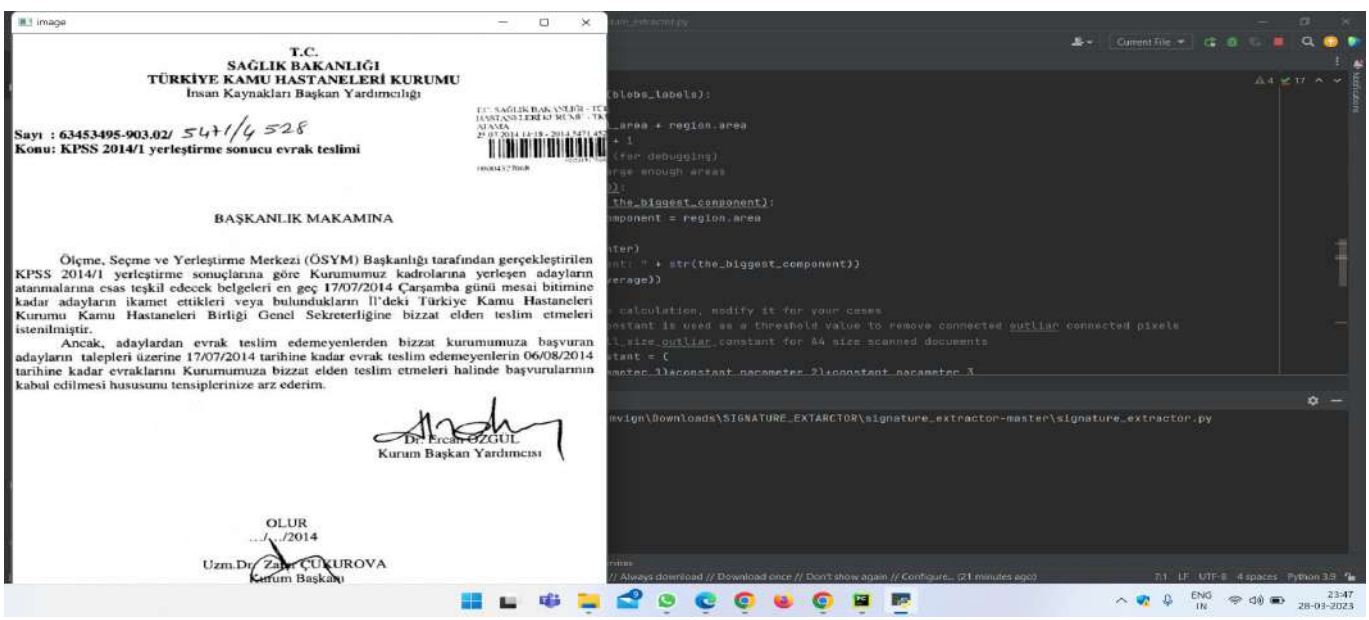
Forgery detection is a critical component of signature verification systems, which involves detecting and identifying forged signatures that are attempting to deceive the system. There are several techniques used for forgery detection in signature verification systems

7 DEMONSTRATION SCREENSHOTS:-

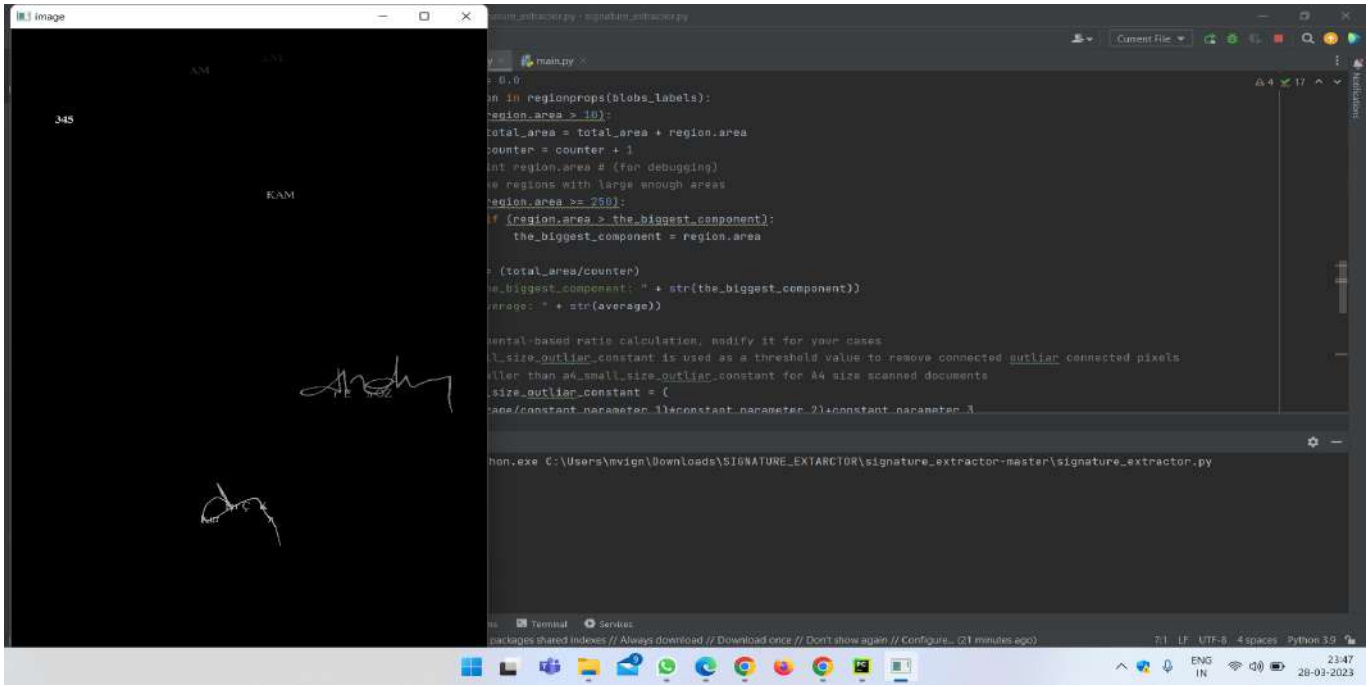
7.1 MODULE 1:- SIGNATURE EXTRACTION



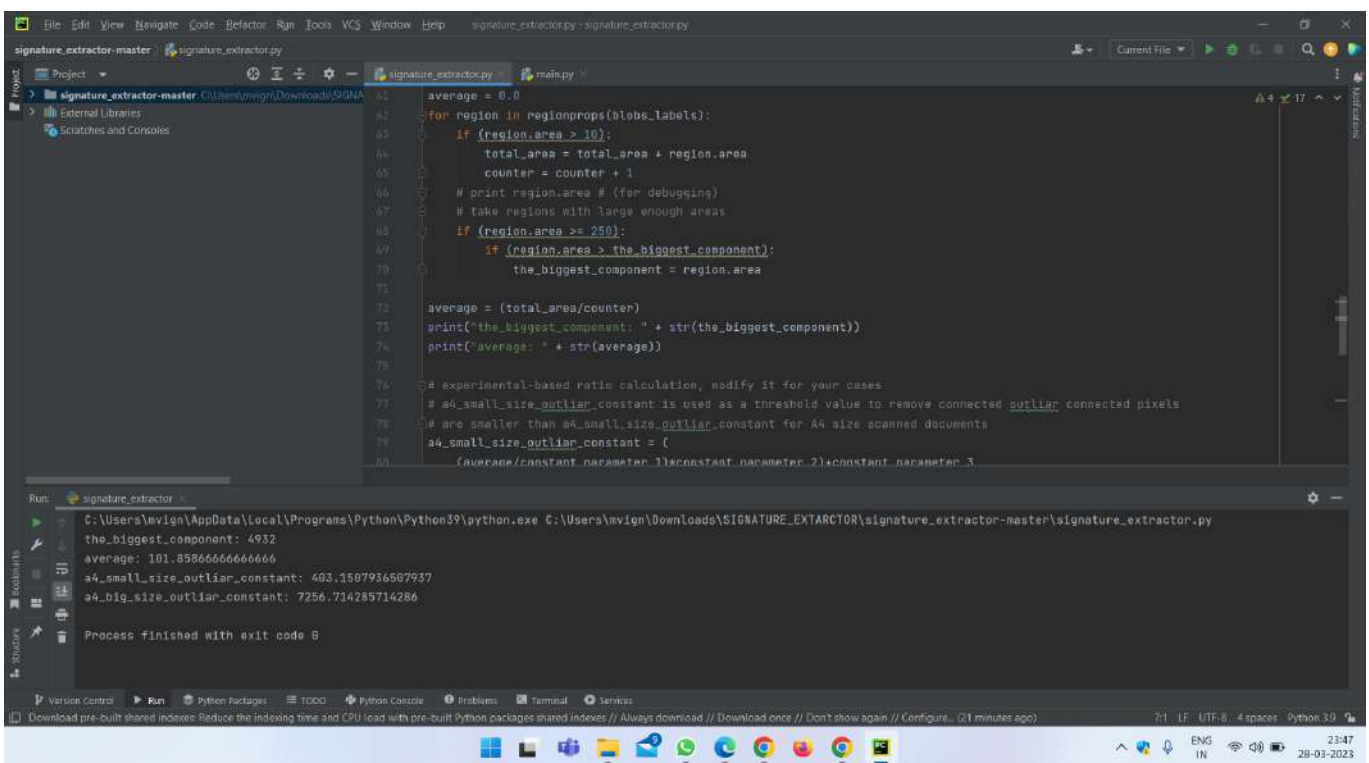
Explanation: *In this we are selecting the input image for signature Extraction process.*



Explanation: *Now the selected input image is display in the separate window for conformation of the image.*

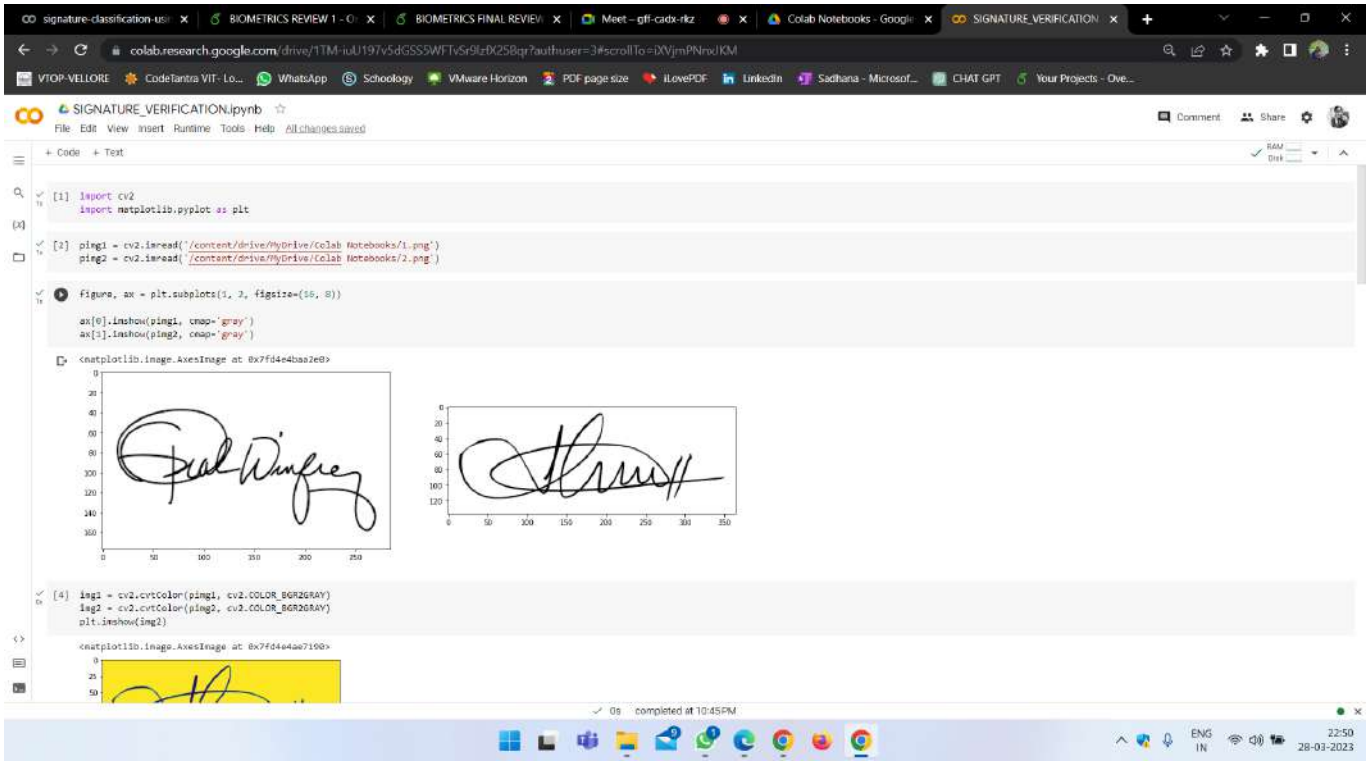


Explanation: *Once the window is closed then the input image undergoes Connected Component Analysis and give the extracted signature image as output. Then the output result is stored in the output folder.*

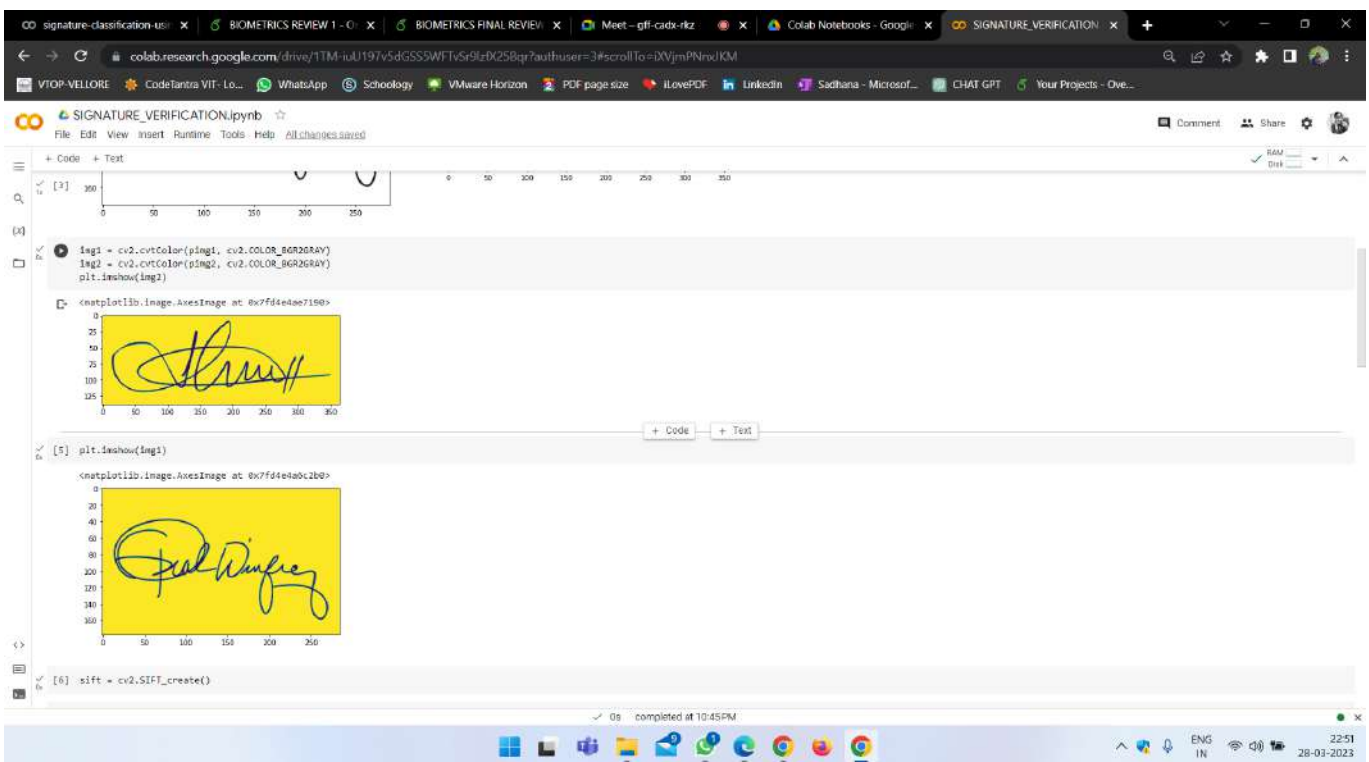


Explanation: *Finally, we are printing the Biggest Component Value and Average value.*

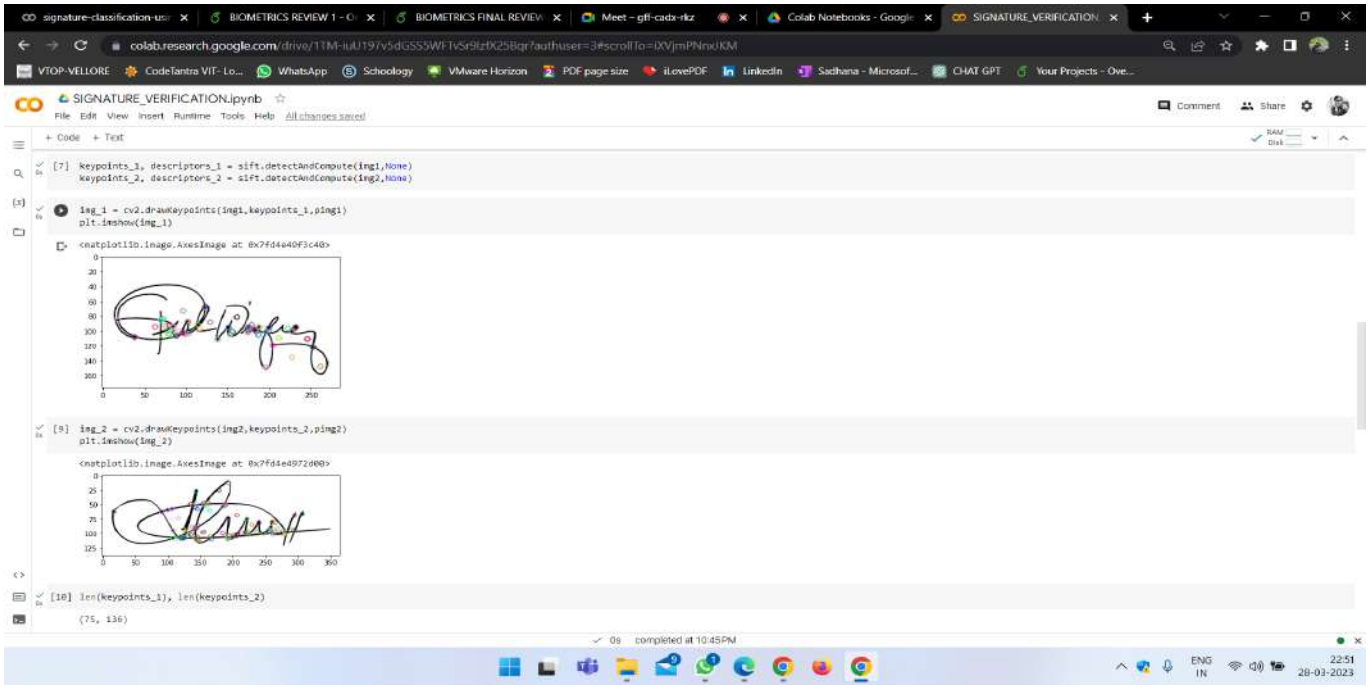
7.2 MODULE 2:- SIGNATURE VERIFICATION



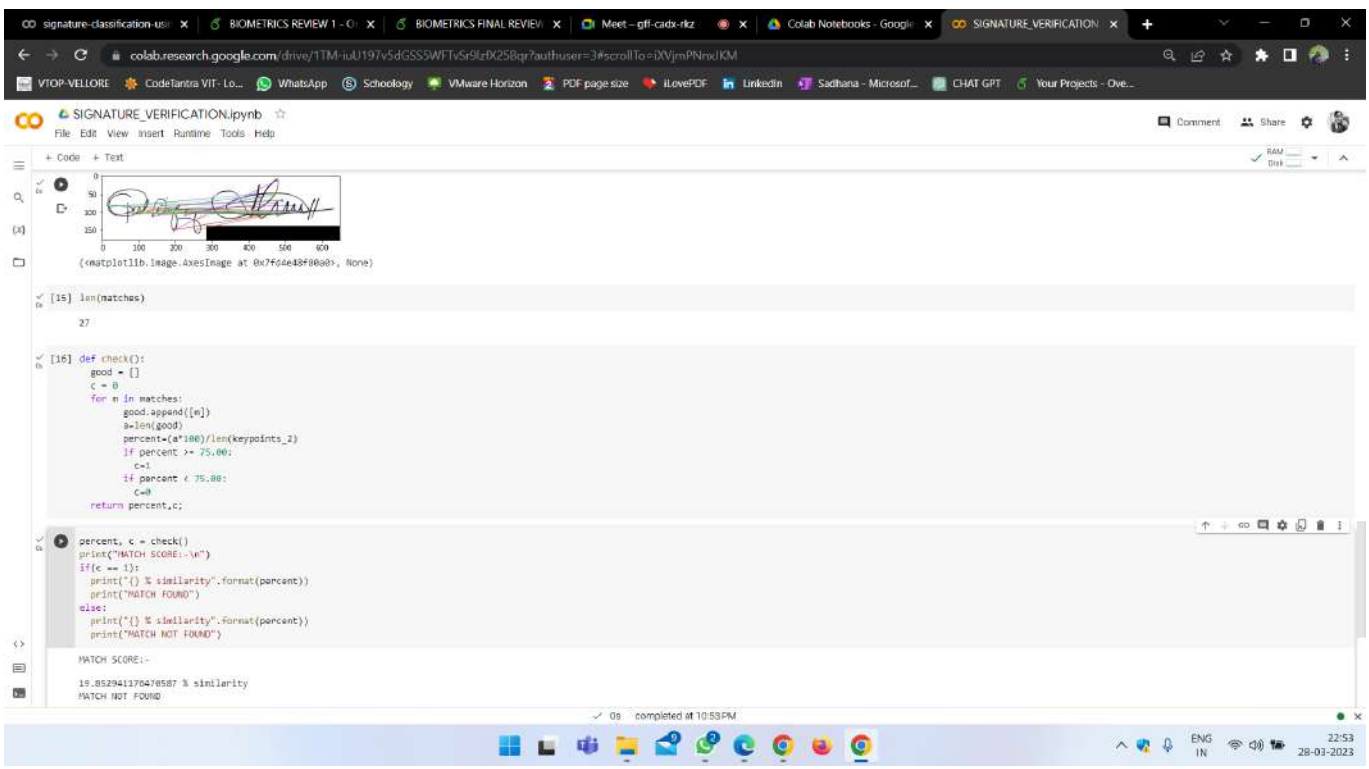
Explanation: *In this we are import the input images from google drive and displaying it.*



Explanation: *Converting the original image into gray scale image for feature extraction.*

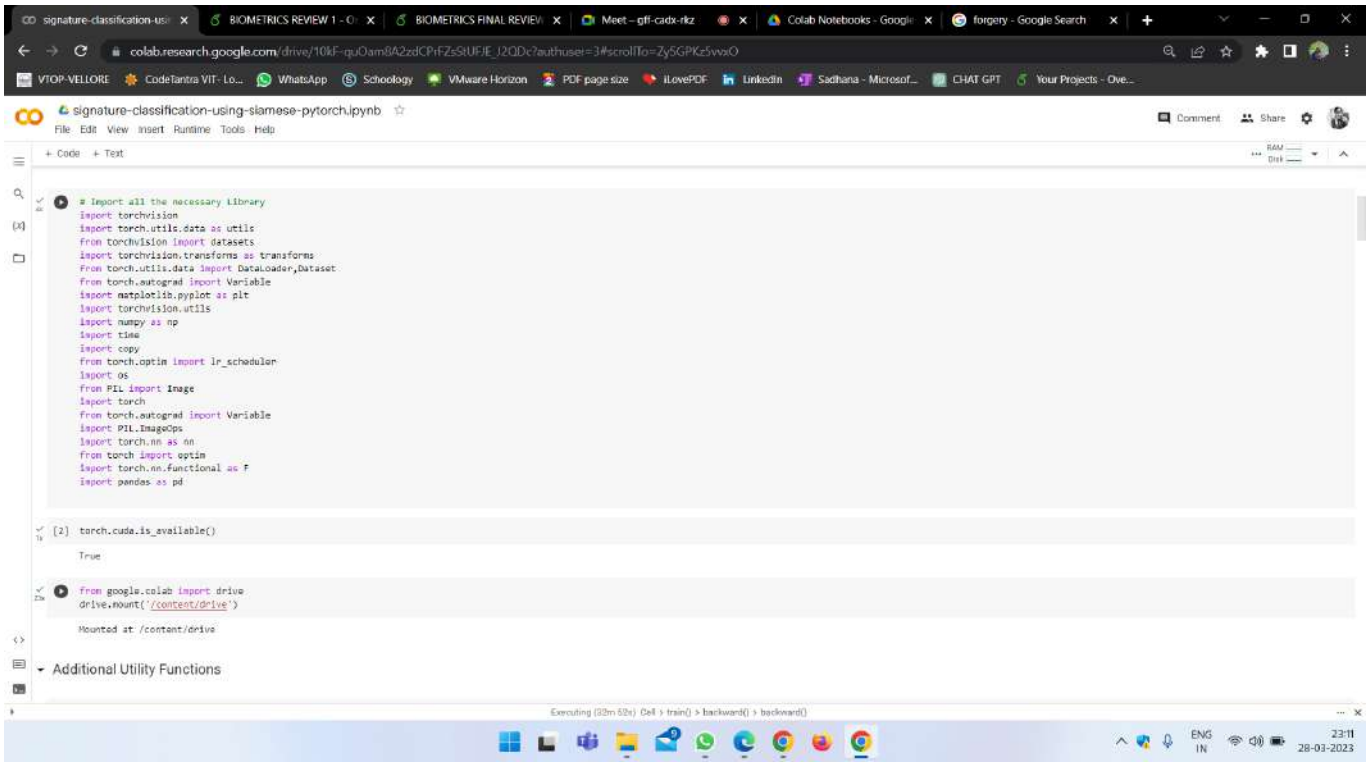


Explanation: *In this we are mapping the Key points of the input signature image by using SIFT Algorithm.*

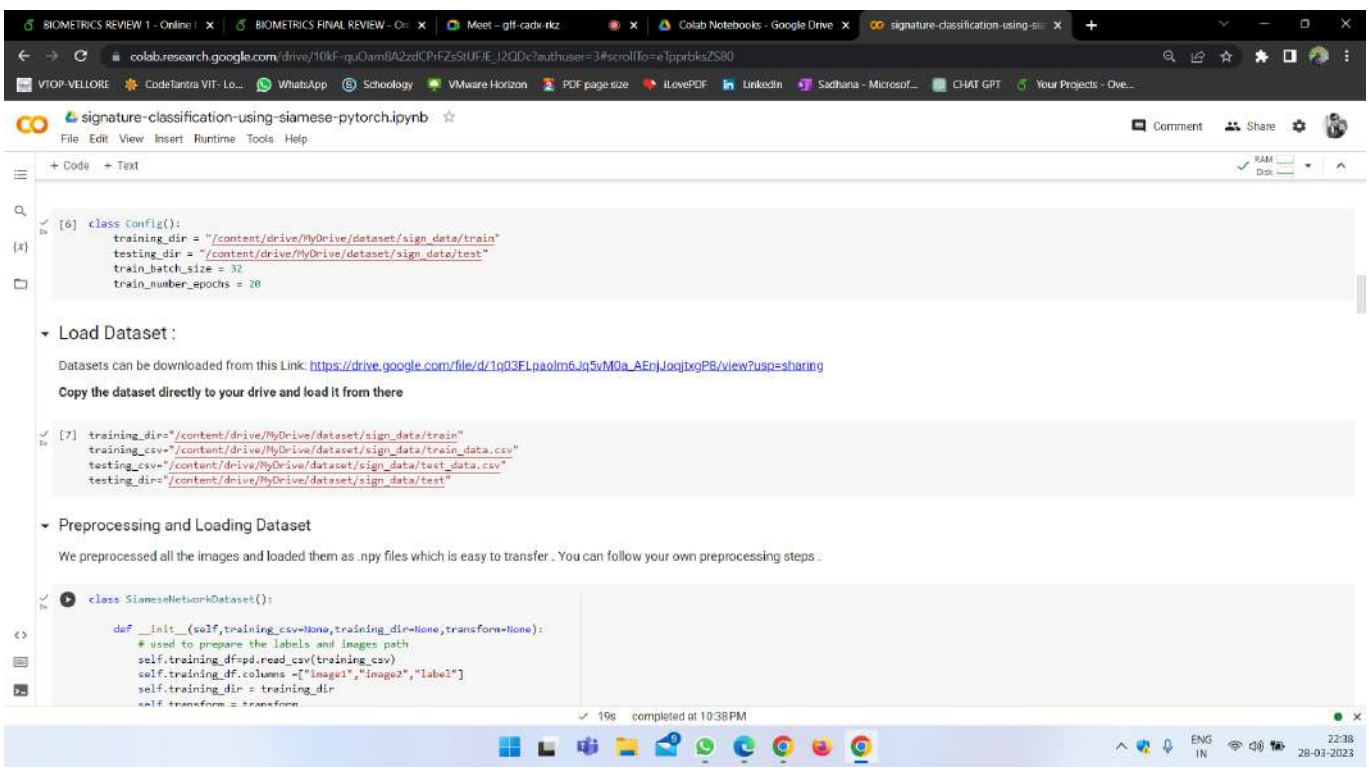


Explanation: *Now we are mapping the key points of both the signature and analysing how many key points are mapped correctly. Then we are going print the match score and match result.*

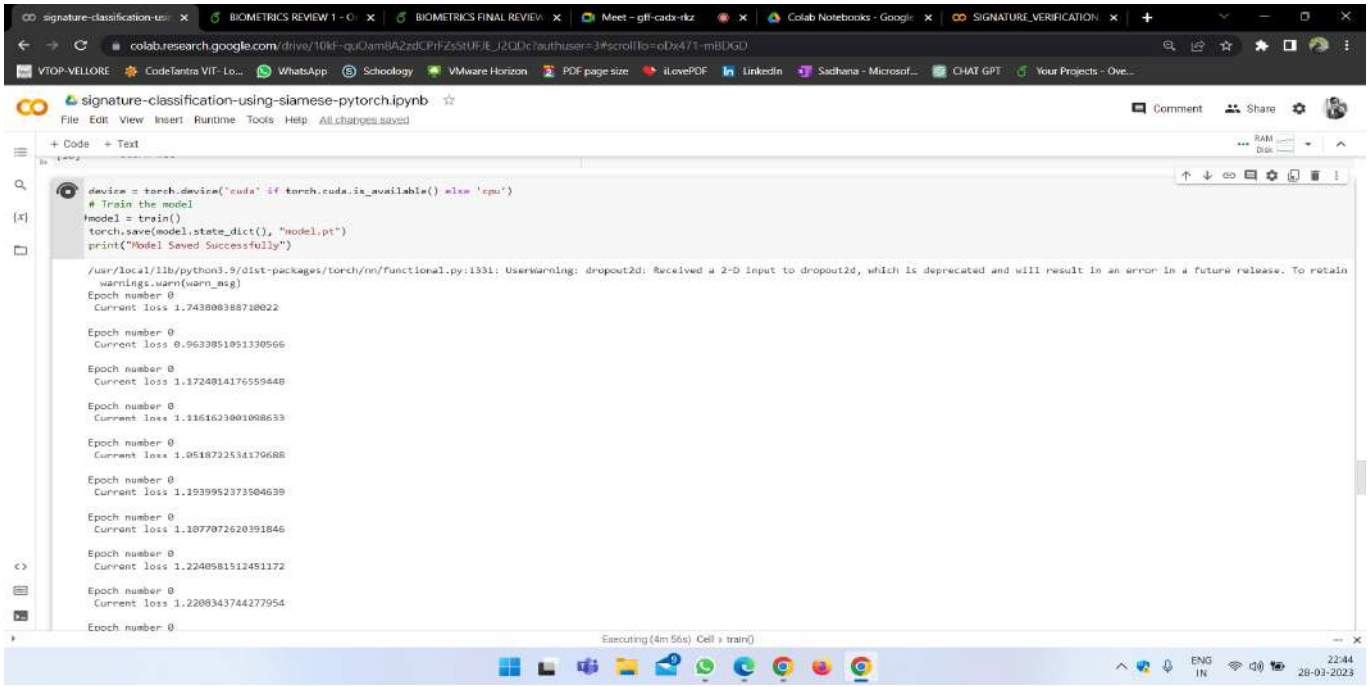
7.3 MODULE 3:- SIGNATURE FORGERY DETECTION



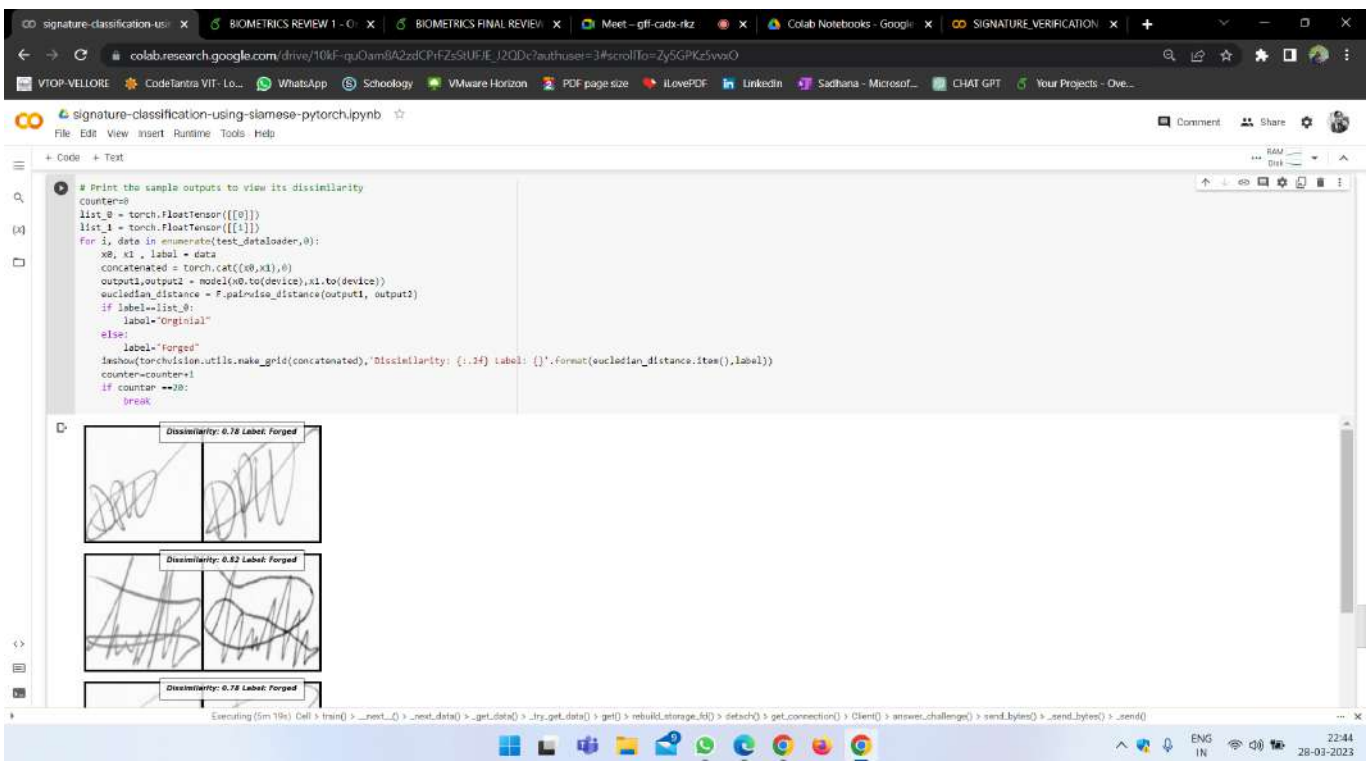
Explanation: *In this we are import the packages and connecting the google drive to google colab.*



Explanation: *Now we are loading the pre-processed dataset of signature to colab and splitting the dataset to train and test set.*



Explanation: *In this we are training the dataset for the detection of signature whether it is forged or not.*



Explanation: *Finally, we are printing the similarity or dissimilarity score and label whether the signature is forged or not.*

8 SAMPLE CODE:-

8.1 MODULE 1:- SIGNATURE EXTRACTION

signature_extractor

File Edit View

```
import cv2
import matplotlib.pyplot as plt
from skimage import measure, morphology
from skimage.color import label2rgb
from skimage.measure import regionprops
import numpy as np
import tkinter
from tkinter import filedialog

# the parameters are used to remove small size connected pixels outliar
constant_parameter_1 = 84
constant_parameter_2 = 250
constant_parameter_3 = 100

# the parameter is used to remove big size connected pixels outliar
constant_parameter_4 = 18

# read the input image
# initiate tinker and hide window
main_win = tkinter.Tk()
main_win.withdraw()

main_win.overrideredirect(True)
main_win.geometry('0x0+0+0')

main_win.deiconify()
main_win.lift()
main_win.focus_force()

# open file selector
main_win.sourceFile = filedialog.askopenfilename(parent=main_win, initialdir="/",
                                                 title='Please select a directory')

# close window after selection
main_win.destroy()

img = cv2.imread(main_win.sourceFile)

cv2.imshow('image', img)
cv2.waitKey(0)
```

Ln 1, Col 1 100% Unix (LF) UTF-8

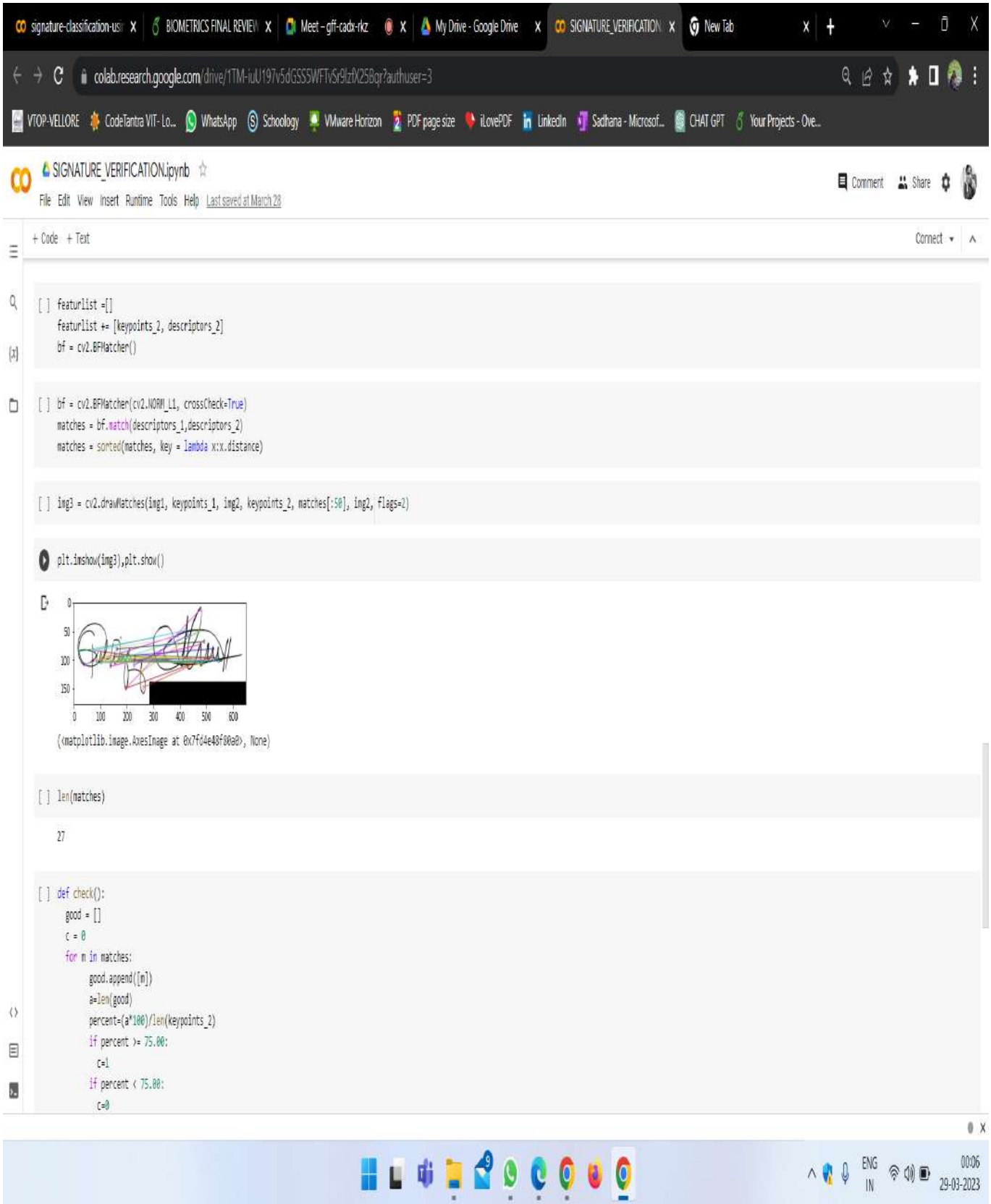
ENG IN 00:01 29-03-2023

8.2 MODULE 2:- SIGNATURE VERIFICATION

signature-classification-using-siamese-pytorch.ipynb

```
class SiameseNetwork(nn.Module):
    def __init__(self):
        super(SiameseNetwork, self).__init__()

        # Setting up the Sequential of CNN Layers
        self.cnn1 = nn.Sequential(

            nn.Conv2d(1, 96, kernel_size=11,stride=1),
            nn.ReLU(inplace=True),
            nn.LocalResponseNorm(5,alpha=0.0001,beta=0.75,k=2),
            nn.MaxPool2d(3, stride=2),

            nn.Conv2d(96, 256, kernel_size=5,stride=1,padding=2),
            nn.ReLU(inplace=True),
            nn.LocalResponseNorm(5,alpha=0.0001,beta=0.75,k=2),
            nn.MaxPool2d(3, stride=2),
            nn.Dropout2d(p=0.3),

            nn.Conv2d(256,384 , kernel_size=3,stride=1,padding=1),
            nn.ReLU(inplace=True),
            nn.Conv2d(384,256 , kernel_size=3,stride=1,padding=1),
            nn.ReLU(inplace=True),
            nn.MaxPool2d(3, stride=2),
            nn.Dropout2d(p=0.3),

        )

        # Defining the fully connected layers
        self.fc1 = nn.Sequential(
            nn.Linear(30976, 1024),
            nn.ReLU(inplace=True),
            nn.Dropout2d(p=0.5),

            nn.Linear(1024, 128),
            nn.ReLU(inplace=True),

            nn.Linear(128,2))
```

8.3 MODULE 3:- SIGNATURE FORGERY DETECTION



9 LITERATURE SURVEY:-

S. NO	PAPER NAME	AUTHOR	PUBLISHER AND YEAR	DESCRIPTION	METHOD USED	FUTURE SCOPE
[14]	Online Signature Verification Using Neural Network and Pearson Correlation Features	Vahab Iranmanesh, Sharifah Mumtazah Syed Ahmad	IEEE 2013	There are two methods for the signature verification system: online and offline. The off-line method involves taking a picture of the signature.via the scanner.Based on Pearson correlation coefficients, the proposed feature extraction approach on an individual's online signature is used in this study.	Pearson Correlation coefficient feature Extraction,Multilayer Perceptron.	Focusing more on accuracy by retrieving additional features from the database's signature features that are already available.Additionally, a fresh training method, like the genetic algorithm for weight adjustment,might be developed.
[11]	Signature based Document Image Retrieval Using Multilevel DWT Features	Umesh D.Dixit,M. S.Shirdhonkar	MECS 2017	A signature is a distinct entity that plays a key role in the database's indexing of huge documents. Using multiple shape representations, such as salient contour, for signature-based document retrieval, the skeleton is detected and segmented after being directly pulled from the database's labelled signature region.	To detect and extract signature from document image.Signature based document retrieval.	A technique for retrieving and extracting signatures from documents automatically signature as a search term For document images, DWT features that were extracted at single- and multi-level levels are utilised.

[1]	OFFLINE SIGNATURE VERIFICATION USING ORDINAL STRUCTURE FUZZY LOGIC AND INTEGRATED FEATURES BASED ON SINGLE SIGNATURE	GHASSANM ARWAN ABDUL-FATTAH	University Teknologi2019	The primary goal of this research is to suggest an improved offline signature verification system over the one that is currently in use, which has issues relating to inconsistent human behaviour and the vast array of given signatures.The more effective proposed system can be implemented by defining and employing an adaptive binarizing module based on background estimation.	Global Binarization Techniques,Descriptors Extraction,Decision Algorithms.	A reliable image enhancement phase, which can remove noise and correctly position the provided signature before sending it to the engine, as well as defining and utilising an adaptive binarizing module based on background estimation.
[21]	Online Signature Verification Using Energy,angle and Directional Gradient Feature with Neural Network	Subhash Chandra,Sushila Maheska	(IJCSIT) 2014	The use of biometrics for human identification is crucial in daily life. Given that each signature is unique, they can be utilised as biometrics. The issue occurs Because a person's signature might change depending on their mood, health, etc., it can be difficult to determine whether two separate signatures made by the same legitimate signer are identical or not in a signature verification system.	Chain-Code Method.Artificial Neural network,Energy Density.	The signatures obtained using a signature pad can also yield global features. Accuracy can be increased by combining local and global features. Incorporating a multimodal technique that combines signature data from signature pads put in various locations with other biometric data collected from cameras will make for interesting future work.

[7]	Automatic Extraction of Signatures from Bank Cheques and other Documents	Vamsi Krishna Madasu, Mohd. Hafizuddin	Digital Image Computing: Techniques and Applications 2003	The primary focus of researchers interested in document analysis and recognition for the past ten years has been the automatic extraction of user entered components from bank checks and other document types. Despite the overall rapid rise of ecommerce and internet banking, traditional bank checks and financial documentation are still in high demand.	Crop Method,a sliding window	We intend to automate the entire bank check authentication process by integrating this approach with signature verification in future development.hidden in the recommendati on of the users.
[8]	Offline signature verification based on geometric feature extraction using artificial neural network	Subhash Chandra,Sushila Maheskar	RAIT 2016	There are two types of signature verification systems: online systems and offline methods. Using six global features, a features extraction technique is used to extract the characteristics of the signature image. Geometrical aspects like size and shape are the foundation for the retrieved features of a signature image.	Binarization,Cropping,Feature Extraction,Kurtosis.	Using the back propagation learning technique and 18 sets of unique users with variable numbers of training and testing samples, the effectiveness of the suggested method is evaluated.

[24]	Off-Line Signature Confirmation based Statistical Features through Support Vector Machine Classifiers	Aravinda Chikmagalur Ventakaramu,Suresha Devaraj,Prakash Hebbakavadi,Kyasambally Rajasekhar	The International Arab Journal of Information Technology 2022	The unique methods and broad range of features for query signature testing. The focus of our current research is on verifying reliable feature sets that were created utilising geometric and statistical elements found in the signature image. Using k-means clustering, the generated characteristics for the authentic	Neural Network Training and Classification,Geometrical Feature Extraction (GeFE)	OER has much smaller Vector Distance than other ways, according to the analysis, and the results are equivalent to those of other approaches in the literature.
[30]	Human Authenticat ion through Signature Recognition	Víctor Nàcher Castellet	Universitat Oberta de Catalunya 2019	Since Even, Goldreich, and Micali created a classification criterion, several approaches have been proposed, and they are primarily grouped into two groups. They are typically divided into offline and online verification systems depending on the data's accessibility. The complete final signature is utilised for offline verification.	Levenshtein Distance ,Iterative with full matrix,K-nearest Neighbours Approach,Data Preprocessing.	By resolving this final issue, more initiatives might be made possible, including a mobile signature scanning app that would be loaded on small, batterypowered devices and would categorise signatures as authentic or fake.

[3]	Signature Recognitio n Using Discrete Fourier Transform	Ghazi Ibrahem Raho ,Muzhir Shaban AlAni ,Abd Al-Karim Al-Alosi ,Lobna Anwar Mohammed	International Journal of Business and ICT 2015	Provided a method for offline signature verification that makes use of Receiver Operating Characteristic (ROC) curves to examine the selection of different fusion methods by combining partial decisions made using the Support Vector Machine (SVM) methodology.	Pattern Recognition, Signature Verification, Signature Recognition, Discrete Fourier Transform (DFT).	Through a built-in signature database, many people are enrolled. The results showed that there is a good and effective recognition rate.
[15]	Analysis of pattern recognition for in air signature biometric.	Gonzalo Bailador , Carmen Sanchez Avila, Javier Guerra Casanova, Alberto de Santos Sierra.	ELSEVIER 2011	This paper carried out a survey on the reasons for choosing the gestures concluding that the main ones were the uniqueness of the gesture and ease of remembering. Hence this survey confirmed our decision of using the handwritten signature in the air since it is considered unique and the subjects get used to performing it frequently.	K-nearest Neighbours Approach,Data Preprocessing	Thus it supposes that the combined technique will need less computational power and therefore it could be implemented in a mobile platform.

[18]	Biometric signature verification	Suraiya Jabin and Farhana Javed Zareen	IEEE 2015	This paper aims to present a comprehensive literature survey of the most recent research papers on biometric signature verification. It highlights the most important methods and addresses variations in the methods and features that are being taken up in the most recent research in this field along with the possible extensions.	Convolution Neural Network	The possible extension of these works can be to find the optimal size of signature sample set that can be used for training which is neither too small that it decreases the interclass variations
[26]	Signature recognition for banking system	Madhu K N1 , Mrs. Bhavana	IEEE 2022	This paper deals with signature verification of banking systems on online mode to find out forgeries and prevent scams in banks.	SVM, Artificial Neural network	Further research in offline signature verification is necessary. Future research may combine different classifiers to produce better validation results.
[10]	Signature using Biometric methods	A. S. Syed Navaz1 , K. Durairaj2	IEEE 2016	This paper is developed by using Vb.net as a front end Ms Access as backend. Our method validates the signature based on hand movement when a person signs his signature. Our method has a unique advantage over existing systems.	Artificial Neural network	The future works can able to provide the user to give their Specimen signature and later it is used for verification. The signature whether recognized or not is given in the form of accuracy result of comparison.

[36]	Dynamic Signature Verificatio n System Based on One Real Signature	Moises Diaz, Member, IEEE, Andreas Fischer, Miguel A. Ferrer, and Réjean Plamondon	IEEE 2018	This paper deals with duplicating the given signature a number of times and training an automatic signature verifier with each of the resulting signatures. The duplication scheme is based on a sigma lognormal decomposition of the reference signature.	Convolution Neural Network	The future direction of this research follows up the study of the real stroke variability under the sigmalognormal model. During signature execution the strokes are in general not con- sistent across several genuine signatures.
[16]	Algorithm For Signature Verificatio n System	Sikander Hans	IEEE 2012	This paper describes an efficient algorithm that can be used for signature verification. This algorithm may prove useful in many real life applications like banking systems etc. The basic steps are preprocessing, feature extraction and classification.	SVM, HMM	The future work of this algorithm is that the preprocessing does not involve thinning which helps in preventing the loss of useful information from the image. Hence it gives better and more accurate results.
[34]	Offline Handwritte n signature verification system: Using Artificial Neural Networks Approach	Nura Musa Tahir, Kamal Abubakar, Usman Bature, Ibrahim Gambo	IEEE 2021	This paper contains some set of simple shaped geometric features are used in achieving offline Verification of signatures.	ANN	The future works of this research can be greatly enhanced by the use of optimization algorithms that yield faster convergence than the gradient descent algorithm used in this work.
[17]	Approache s and issues in offline Signature verification system	Kanak Chandra Sarma	IEEE 2012	This paper contains a survey of various approaches and issues related to offline signature verification systems.	Convolution Neural Network	The future works of this paper is to create an automatic signature verification system with minimal number of errors.

[33]	Online signature verification system	Fauziyah Salehuddin, Zahariah Manap, Hazura Haroon	IEEE 2009	This paper aims to create an online signature verification system to enhance verification of signature in online with less defects.	SIFT and LBP, Artificial Neural network	The future works of this system is to create a better signature verification system that is accepted in real world and people can able to use it worldwide.
[46]	Online signature verification on Mobile devices	Napa Sae-Bae, Nasir D.Memon	IEEE 2014	This paper studies online signature verification on touch interface based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space.	Artificial Neural network	One interesting area for future work is the design of an enroll- ment protocol that can capture a intra-user variation effectively within a single session.
[43]	Presentatio n Attacks in signature biometrics: Types and Introductio n to Attack detection	Ruben Tolosana, Ruben Vera Rodriguez, Julian Fierrez and Javier Ortega Garcia	IEEE 2017	This paper is in line with recent efforts in the Common Criteria standardization community towards security evaluation of biometric systems, where attacks are rated depending on, among other factors, time spent, effort and expertise of the attacker, as well as the information available and used from the target being attacked.	GMM, HMM	The future work of this project is to prevent PA attacks and developing the best algorithm to prevent PA attacks.

[23]	A combined feature extraction model using SIFT and LBP for offline signature verification system	Bhushan S. Thakare Dr. Hemant R. Deshmukh	International Conference for Convergence in Technology 2018	Bio-metric applications are considered as most promising technique for user identity verification and identification..To deal with this issue, here we presented a combined approach for feature extraction where SIFT (Scale Invariant Feature Transform) and improved LBP (Local Binary Pattern) are combined together to obtain the robust feature model.	SIFT and LBP	The system also focuses on Western scripts for signature verification along with offline Hindi signature verification system. This work uses gradient features, Zernike moment features and support vector machine classifier for verification purpose.
[28]	OFFLINE HANDWR ITTEN SIGNATU RE VERIFICA TION USING SIFT FEATURE S	KARANJA EVANSON MWANGI	International Conference for Convergence in Technology 2008	For legality most documents like bank cheques, travel passports and academic certificates need to have authorized handwritten signatures. In modern society where fraud is rampant, there is the need for an automatic HSV(Handwritten signature verification) system to complement visual verification.	SIFT and LBP	Future work could evaluate inclusion of SIFT features as image descriptors and various distance measures discussed above in online handwritten signature verification problems.

[4]	Offline handwritte n signature verification using local and global features	The-Anh Pham· Hong-Ha Le·NangToan Do	Springer 2014	In contrast to many existing systems, we are interested in makingsoft decision rather than a purely binary classification for the signatures under verification. , the finer features are computedfor every sample point of a signature using histogram of intensities, and the geometrybased features are extracted using an adaptation of the shape context descriptor.	Finer intensity based features and global geometry based features.	In future work, the signature is represented by a sequence of feature vectors constructed from pixel densities of local square cells of the columns in the grid.
[37]	A new wrapper feature selection method for languageinvariant offline signature verification	Debanshu Banerjee, Bitanu Chatterjee, Pratik Bhowal, Trinav Bhattachary ya, Samir Malakar, Ram Sarkar	IEEE 2021	we have designed a novel wrapper feature selection method based on Red Deer Algorithm, to keep only the relevant features to be used during signature authentication and verification process.	Naïve bayes and red deer algorithm	As a future scope, we plan toextend our work by applying it on the signature images written in other languages except those are considered here.

[5]	Signature Recognitio n and Verificatio n: The Most Acceptable Biometrics for Security	Deepali H. Shah, Dr. Tejas V. Shah	IJAIEM 2015	Duplicity of signature gives rising demand for processing of individual identification faster and more correctly such as an automatic signature verification system. Online approach uses an electronic tablet and a stylus connected to a computer which extracts information about a signature.	Finer intensity based features and global geometry based features.	The future scope is to hybridize the BRDA method with some classical meta heuristic algorithms or local search techniques in order to improve the classification performance of the FS model using far less number of features.
[31]	Ofine Signature Verifcation :An Applic ation of GLCM Features in Machine Learning	Prashant Sin gh, Prashant Ve rma, Nikhil Sing h	Springer 2021	This paper focuses on automated verifcation for Ofine written signatures based on diferent machine learning algorithms. The objective of the study is to maxi mize forgery prevention using minimal human intervention. Forgeries can be of two types: Skilled Forgery and Random Forgery.	Convolution Neural Networks and Support Vector Machine algorithms.	We believe that accuracy can be improved further using more hidden layers in the CNN algorithm, using parallelism to meet the computational costs (through GPU/FPGA/A SIC).
[44]	Static Handwritte n Signature Verificatio n Using Convolutio n Neural Network	Tanzeel Sultan Rana, Hafiz Muhammad Usman, Sheraz Naseer	ICIC 2019	In this, we propose a method of offline signature verification in which convolution is applied to address the maximum accuracy and we present how the problem was being handled in the past few decades. The experimented result reveals the efficiency of algorithm.	Convolution Neural Network	In future work, we will incorporate some ideas looking for more effective preprocessing method which gives better contour, explores better grids of the digital images; considering global and local information simultaneously.

[49]	Offline Handwritt en Signature Verificati on System Using Random Forest Classifier	Maduhansi Thenuwara, Harshani R. K. Nagahamulla	IEEE 2010	The scope has been narrowed down to offline signatures which contains static inputs and outputs. The classifiers were trained and tested using a signature database available for the public use. The best performance was obtainedfrom RFC with and accuracy score 0.6. For an average, the system created has been successful in verifying signature images provided with a considerable accuracy level.	Random Forest Classifier	In future work, it is a promising research that how to use less reference signatures for verification and the result is the same as before. Python get strengthen with the passage of time so in near future it provide us relatively better platform to get more accurate and better results.
[29]	Off-line signature verificatio n based on grey level informati on using texture features	J.F. Vargas, M.A. Ferrer, C.M. Travieso,J.B. Alonso	IEEE 2010	It works at the global image level and measures the grey level variations in the image using statistical texture features. The co-occurrence matrix and local binary pattern are analysed and used as features. This method begins with a proposed background removal. A histogram is also processed to reduce the influence of different writing ink pens used by signers.	Random Forest Classifier	Signature authentication machine is implemented to provide a simple, safe, fast biometric behavioral security system. By using some equations from coordinate geometry makes this method faster than other methods.

[39]	Writerindependent Offline Handwritt en Signature Verification using Novel Feature Extraction Techniques	Md. Aminur Rahman, Sarker Miraz Mahfuz, S. M. Abdullah Al-Mamun	International Journal of Computer Applications 2 019	Signature is critical for authentication and authorization in commercial, financial and legal transactions and fittingly, it is one of the most commonly used biometrics for authentication. Hence, an accurate and efficient signature verification system is required. The objective of signature verification is to discriminate the original signatures from the forged ones.	SIFT and LBP	Since online handwritten signature verification problems involves descriptors like velocity, acceleration and capture time of each point on the signature trajectory. Future work could evaluate inclusion of SIFT features as image descriptors and various distance measures discussed above in online handwritten signature verification problems.
[27]	ServerSide Encryptin g and Digital Signature Platform with Biometric Authoriza tion	Leszek Siwik, Lukasz Mozgowoj	MECS 2015	BioPKI is a server-side encryption and digital signature platform with biometric authorization. A moresecure approach is storing the key inside an external, physically-separated hardware element. Traditional methods don't provide an appropriate level of security and privacy, since it is typical for the keys to be stored directly in the file system.	Techniques based on recognition of the blood vessel system are more secure than fingerprint or face recognition, and equally secure as eye-iris recognition.	Many contemporary communication applications are equipped with built-in data encryption and protection mechanisms.

[50]	Feature Extraction for Signature Verificati on Using Hilditch Algorithm	Ravikumar B Panchal, Dr. Dhaval R Bhojani	IJERT 2014	The signature verification system is one of the most widely used biometrics in the banking industry for authentication. The main goal is to use a graph-matching classifier to compare the feature points of a given signature to the feature points of a test signature.	SVM, HMM, Cross validated Graph Matching algorithm	The features can be extracted from inside a personal device such as a smart card. The classification of the feature points can be done using mean and variance.
[42]	OFFLINE SIGNAT URE VERIFIC ATION WITH USER BASED AND GLOBAL CLASSIF IERS OF LOCAL FEATUR ES	MUSTAFA BERKAY YILMAZ	Sabancı University 2015	It captures the signature's stable parts and alleviates the difficulty of global matching, local features (histogram of oriented gradients, local binary patterns) are used, based on gradient information and neighboring information inside local regions.	support vector machine (SVM), Scale invariant feature transform (SIFT)	In the future, systems research needs to concentrate on increasing the robustness of systems towards larger variations encountered in real life. For instance, signatures signed in smaller spaces, in a hurry, or on documents with interfering lines.
[48]	Evaluatin g biometric s for online banking: The case for usability	Rana Tassabehji, Mumtaz A. Kamala	ELSEVIER 2012	This paper suggests a biometric system for authenticating ebanking and applied the established System Usability Scale (SUS) to evaluate its effectiveness from the perspective of potential users. The case demonstrates that on the whole users are very favorable towards a biometric banking system and ostensibly found the system developed usable.	Brooke's "quick and dirty usability scale" (SUS)	We should evaluate its usability in the early stages of development to minimise wastage of time and resources on a system that was not usable.

[45]	Update Strategies for HMM Based Dynamic Signature Biometric Systems	Ruben Tolosana, Ruben Vera Rodriguez, Javier Ortega Garcia and Julian Fierrez	IEEE 2015	The HMM-based and GMM-based systems that are used in this study have configurations that are optimal for the amount of training signatures that can be used to create the user template. When there are more training signatures accessible to create the user template, it emphasises the value of optimising system configuration as opposed to a set configuration system.	Hidden Markov Model (HMM) and Gaussian Mixture Models (GMM)	Utilizing various databases, the system configuration update procedures suggested in this work will be examined. We will purchase a new database in order to evaluate the performance of the Proposed Systems utilising a different group of users for system development and testing due to the absence of databases with a higher number of legitimate signatures per user.
[32]	Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification	RUBENTOLOSANA, RUBEN VERA RODRIGUEZ, JAVIER ORTEGA GARCIA,AND JULIAN FIERREZ	IEEE 2013	This paper suggests an approach that makes data acquired from different devices process to normalize the signals in similar ranges. The second one is based on feature selection taking into account the device interoperability case, to select to select features that are robust in these conditions.	DTW(Dynamic Time Warping),HMM (Hidden Markov Models),NN (Neural Networks) and SVM (Support Vector Machines)	It will be interesting to see the performance of the system using devices with the same quality for interoperability cases and also, using newer devices such as tablets and smartphones.

[22]	Increasing the Robustnes s of Biometric Templates for Dynamic Signature Biometric Systems	Ruben Tolosana, Ruben Vera Rodriguez, Javier Ortega Garcia and Julian Fierrez	IEEE 2015	In this paper, two approaches to time functions-based systems for dynamic signature verification are investigated: the Standard System and an optimal time functions-based system. In the development stage of the system, an optimal time-functions vector was chosen per system (i.e. Standard and Secure Systems) using the SFFS algorithm	Sequential Forward Features Selection (SFFS), Dynamic Time Warping (DTW)	For future work, it would be interesting to analyze the performance of the Secure System also for mobile scenarios using the finger instead of the pen stylus.
[40]	Automati c Extraction of Signature s from Bank Cheques and other Document s	Vamsi Krishna Madasu , Mohd. Hafizuddin Mohd. Yusof, M. Hanmandlu , Kurt Kubik	IEEE 2003	In this approach, a window of adaptable height and width is moved over the image; one pixel at a time and the density of pixels within the window is calculated. This density is then used to find the entropy, which in turn helps fit the box that can segment the signature.	fuzzy enhancement method	We intend to integrate this system with signature verification in the future so that the entire process of bank cheque authentication is automated.

[19]	Bank Cheque Signature Verificati on System	Vamsi Krishna Madasu , Mohd. Hafizuddin Mohd. Yusof, M. Hanmandlu , Kurt Kubik	IJRESM 2018	In this work, an artificial neural network based on the well-known Backpropagation algorithm is used for recognition and verification. To test the performance of the system, the False Reject Rate, the False Accept Rate, and the Equal Error Rate (EER) are calculated. s. The aim of this work is to limit the computer singularity in deciding whether the signature is forged or not, and to allow the signature verification.	Backpropagation algorithm, image processing	Online signature can be captured using electronic devices like writing pad or stylus attached to a computer.
[35]	A Bank Cheque Signature Verificati on System using FFBP Neural Network Architect ure and Feature Extraction based on GLCM	Ashok Kumar. D and Dhandapani. S	IJETTCS 2014	Verification of signatures can be done on-line or offline depending upon the application. In this study, a Neural Network model is designed for the signature verification and testing using the Offline Bank Cheque Signature Verification System. T	Gray Level Cooccurrence Matrix (GLCM), Feed Forward Back Propagation Neural Network (FFBPNN).	The system modeled can be improved in future by minimizing the number of input samples to train the network. Further the system classifies signatures only into genuine or forged one. Further the classification can be extended to find whether the forgery is a skilled, random or simple one.

[9]	The study of the applicatio ns of biometric s systems: a literature review.	Nur Fatinhieyah Azizan, Wan Alia Izzati Wan Abdul Razak, Normi Sham Awang Abu Bakar , Norzariyah Yahya	Journal Of Engineering Science And Technology 2021	Though the benefits of security features promoted by the biometric system, reciprocally, biometric systems also have limitations. This paper reports on reviews conducted on articles with the aim to identify different types of biometric systems, the application domains, constraints,and limitations of existing biometric systems.	GLCM	Explores different biometrics system and their suitable metrics to observe their characteristical perspective.
[13]	online signature verificatio n for secure transactio ns	keerthana chintapudi , prof. Suresh. H. Ballala , p. Renuka	IJSETR 2015	This paper involves the study to develop an authentication system based on personal signatures. Signature verification is an important research topic in the area of biometric authentication. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity.	HMM	A method proposed to develop an authentication system based on personal signatures where the user signature is compared with the database signature and the authenticated persons are allowed for banking procedure.
[2]	A study on handwritten signature	l.b.mahanta, alphana deka	International Journal of Computer Applications 2013	This paper provides some basic concepts of signature and also explores on different approaches for verification using signature.	SVM,ANN	The manual forgeries can be stopped with signature verification.Thus to increase the security, an automatic signature verification system can be applied that avoids human intervention.

[6]	offline signature verification using pixel matching technique	indrajit bhattacharya a,prabir ghoshb,swarup biswasb	cimta 2013	The core of a signature biometric system is behavioural, and this paper proposes an offline signature verification and recognition system using pixel matching technique. Pmt (pixel matching technique) is used to verify the signature of the user with the sample signature which is stored in the database.	PMT	signature authentication machine is implemented to provide a simple, safe, fast biometric behavioural security system. By using some equations from coordinate geometry makes this method faster than other methods.
[25]	The Use Of Biometric Technologies For Bank Transacti on Security Management Against The Backgrou nd Of The Internatio nal Experienc e: Evidence From Ukraine	mykola kurylo, alyona klochko,natalia volchenko,nataliia klietsova, anna bolotina	consulting publishing company 2021	Contradictions arising between the state of regulatory support and the actual needs for the use of biometric technologies in the field of banking in ukraine decelerate the use of effective security tools with a high degree of reliability in the banking sector.	SVM	Systems that combine several different types of biometric identification, combined types of authentication, in particular, hardware and biometric technologies, can provide maximum protection for banking operations.
[20]	Signature verificatio n for automated cheque authentica tion system based on shape contexts	sangeeta girish narkhede, prof. Dinesh d. Patil	IJCSIT 2014	Research here is related to offline signature verification. Shape contexts have been used to verify whether 2 shapes are similar or not. It has been used for various applications such as digit recognition, 3d object recognition, trademark retrieval.	KNN classifier	Proposed a modified shape context for offline signature recognition that uses shape distance of test signature with template signatures and there is no alignment work needed total computation time is reduced, hence usefull for bank system.

[41]	online signaturebased biometric recognitio n.	sudeep tanwar, mohammad s. Obaidat, sudhanshu tyagi, and neeraj kumar	Springer 2019	Banking sectors are also using the signatures very promptly for clearing the paper-based checks. Manual- or computer-based signature matching mechanisms have been used by the banks. In a manual system, the authorized person cross-examines the signatures of the account holder from database, while in the computer-based system, authentic software tools.	HMM	A couple of case studies have been covered in this paper for online signature-based biometrics in ecommerce to deal with financial and commercial activities taking place through the medium of internet.
[12]	handwritt en signature verificatio n	h. M. H. P. Abewardana, dr. L. Ranathunga	International Research Conference on Smart Computing and Systems Engineering 2018	using some of the present signature solutions that are scale and rotation invariant such as signature pixel ratio of concentric circles and number of cross points while others are rotation variant such as baseline slant angle, aspect ratio, normalized area and slope of the line connecting center of gravities.	image processing, feature extraction, ANN	The above proposed system helps in detecting the exact person and it provides more accuracy for signature verification.

[38]	Analysis of user authentica tion methods	abdul samad shaikh , mohammed waseem ashfaque	IJRITCC 2014	explori+F50ng the different nature of biometrics and observing existing method's pattern of cracking-resistant, temper resistant, fraudulent usage.	DTW ,HMM, SVM	Idea for developing multi-level security aspects any of these two authentication methods preferably password/pin, should be primary way to first authentication and 'the palm vein technology' should be secondary way of authentication in the banking sector.
[47]	Reducing the template ageing effect in on-line signature biometric s	ruben tolosana , ruben vera rodriguez , julian fierrez , javier ortega garcia.	IETDL 2019	this study carries out an exhaustive experimental analysis of template update strategies for three well-known on-line signature verification approaches, extracts various practical findings related to the template ageing effect in signature biometrics, and configures time adaptive improved versions of the considered baseline approaches overcoming to some extent the template ageing.	HMM,GMM and DTW	Future work will be oriented to incorporating recent advances in deep learning to the described signature biometrics system.

References

[1] GHASSAN MARWAN ABDULFATTAH. "OFFLINE SIGNATURE VERIFICATION USING ORDINAL STRUCTURE FUZZY LOGIC AND INTEGRATED FEATURES BASED ON SINGLE SIGNATURE". PhD thesis. Universiti Teknologi Malaysia, 2019.

[2] alphana deka l.b.mahanta alphana deka. "a study on handwritten signature". In: *international journal of computer applications* ().

[3] Gonzalo Bailador et al. "Analysis of pattern recognition techniques for in-air signature biometrics". In: *Pattern Recognition* 44.10-11 (2011), pp. 2468–2478.

[4] Debanshu Banerjee et al. "A new wrapper feature selection method for language-invariant offline signature verification". In: *Expert Systems with Applications* 186 (2021), p. 115756.

[5] Faiza Eba Batool et al. "Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM". In: *Multimedia Tools and Applications* (2020), pp. 1–20.

[6] Indrajit Bhattacharya, Prabir Ghosh, and Swarup Biswas. "Offline signature verification using pixel matching technique". In: *Procedia Technology* 10 (2013), pp. 970–977.

[7] Subhash Chandra and Sushila Maheskar. "Offline signature verification based on geometric feature extraction using artificial neural network". In: *2016 3rd international conference on recent advances in information technology (RAIT)*. IEEE. 2016, pp. 410–414.

[8] Aravinda Chikmagalur et al. "Off-Line Signature Confirmation based on Cluster Representations of Geometrical and Statistical Features through Vector Distance, Neural Network and Support Vector Machine Classifiers". In: ().

[9] Keerthana Chintapudi, SURESH H BALLALA, and P RENUKA. "Online Signature Verification for Secure Transactions". In: *International Journal of Scientific Engineering and Technology Research* 4 (2015), pp. 7283–7286.

[10] Moises Diaz et al. "Dynamic signature verification system based on one real signature". In: *IEEE transactions on cybernetics* 48.1 (2016), pp. 228–239.

[11] Umesh D Dixit and MS Shirdhonkar. "Signature based Document image retrieval using multi-level DWT features". In: *International Journal of Image, Graphics and Signal Processing* 9.8 (2017), p. 42.

[12] Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. "Offline handwritten signature verification—literature review". In: *2017 seventh international conference on image processing theory, tools and applications (IPTA)*. IEEE. 2017, pp. 1–8.

[13] Sebastiano Impedovo and Giuseppe Pirlo. "Verification of handwritten signatures: an overview". In: *14th International Conference on Image Analysis and Processing (ICIAP 2007)*. IEEE. 2007, pp. 191–196.

[14] Vahab Iranmanesh et al. "Online signature verification using neural network and pearson correlation features". In: (2013), pp. 18–21.

[15] Suraiya Jabin and Farhana Javed Zareen. "Biometric signature verification". In: *International Journal of Biometrics* 7.2 (2015), pp. 97–118.

[16] Mujahed Jarad, Nijad Al-Najdawi, and Sara Tedmori. "Offline handwritten signature verification system using a supervised neural network approach". In: *2014 6th international conference on computer science and information technology (CSIT)*. IEEE. 2014, pp. 189–195.

[17] A Julita et al. "Online signature verification system". In: *2009 5th International Colloquium on Signal Processing & Its Applications*. IEEE. 2009, pp. 8–12.

[18] Shubhangi L Karanjkar and PN Vasambekar. "Signature recognition on bank cheques using ann". In: *2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*. IEEE. 2016, pp. 44–47.

[19] D Ashok Kumar and S Dhandapani. "A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM". In: *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 3.3 (2014), pp. 46–52.

[20] Mykola Kurylo et al. "The use of biometric technologies for bank transaction security management against the background of the international experience: Evidence from Ukraine". In: *Banks and Bank Systems* 16.2 (2021), p. 47.

[21] Vamsi Krishna Madasu et al. "Automatic Extraction of Signatures from Bank Cheques and Other Documents." In: *DICTA*. Vol. 3. Citeseer. 2003, pp. 591–600.

[22] Vamsi Krishna Madasu et al. "Automatic Extraction of Signatures from Bank Cheques and Other Documents." In: *DICTA*. Vol. 3. Citeseer. 2003, pp. 591–600.

[23] Karanja Evanson Mwangi. "Offline handwritten signature verification using SIFT features". In: *Faculty of Computing and Information Technology, Makerere University* (2008).

[24] Vıctor Nàcher Castellet. "Human authentication through signature recognition". In: (2019).

[25] Sangeeta Girish Narkhede and Dinesh D Patil. "Signature verification for automated cheque authentication system based on shape contexts". In: *(IJCSIT) International Journal of Computer Science and Information Technologies* 5.3 (2014), pp. 3297–3300.

[26] AS Syed Navaz and K Durairaj. "Signature Authentication Using Biometric Methods". In: *January–2016, International Journal of Science and Research, Vol No-5, Issue No-1* (), pp. 1581–1584.

[27] Ravikumar B Panchal and Dhaval R Bhojani. "Feature Extraction for Signature Verification Using Hilditch Algorithm". In: ().

[28] The-Anh Pham, Hong-Ha Le, and Nang-Toan Do. "Offline handwritten signature verification using local and global features". In: *Annals of Mathematics and Artificial Intelligence* 75 (2015), pp. 231–247.

[29] Md Aminur Rahman, Sarker Miraz Mahfuz, and SM Abdullah Al-Mamun. "Writer-independent Offline Handwritten Signature Verification using Novel Feature Extraction Techniques". In: *International Journal of Computer Applications* 975 (), p. 8887.

[30] Ghazi Ibrahem Raho et al. "Signature recognition using discrete fourier transform". In: *International Journal of Business and ICT* 1.1-2 (2015), pp. 17–26.

[31] Tanzeel Sultan Rana, Hafiz Muhammad Usman, and Sheraz Naseer. "Static handwritten signature verification using convolution neural network". In: *2019 International Conference on Innovative Computing (ICIC)*. IEEE. 2019, pp. 1–6.

[32] Javier Ortega-Garcia Ruben Tolosana Ruben Vera-Rodriguez and Julian Fierrez. "Increasing the Robustness of Biometric Templates for Dynamic Signature Biometric Systems". In: *IEEE* ().

[33] Napa Sae-Bae and Nasir Memon. "Online signature verification on mobile devices". In: *IEEE transactions on information forensics and security* 9.6 (2014), pp. 933–947.

[34] Hemanta Saikia and Kanak Chandra Sarma. "Approaches and issues in offline signature verification system". In: *International Journal of Computer Applications* 42.16 (2012), pp. 45–52.

[35] Mulagala Sandhya and Munaga VNK Prasad. "Biometric template protection: A systematic literature review of approaches and modalities". In: *Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era* (2017), pp. 323–370.

[36] Mohammad M Shafiei and Hamid R Rabiee. "A new online signature verification algorithm using variable length segmentation and hidden Markov models". In: *Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings.* IEEE. 2003, pp. 443–446.

[37] Deepali H Shah and V Tejas. "Signature recognition and verification: The most acceptable biometrics for security". In: *International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume* 4 (2015).

[38] Abdul Samad Shaikh and Mohammed Waseem Ashfaque. "Analysis of User Authentication Methods & Impact on Identification Especially in Banking". In: *International Journal on Recent and Innovation Trends in Computing and Communication* 3.2 (2015), pp. 391–398.

[39] Leszek Siwik and Lukasz Mozgowoj. "Server-side encrypting and digital signature platform with biometric authorization". In: *International Journal of Computer Network and Information Security* 7.4 (2015), pp. 1–13.

[40] Vaibhav Tambade, Priyanka Varma, and Aditya Sonawale. "Bank Cheque Signature Verification System". In: *International Journal of Research in Engineering, Science and Management* 1.9 (2018), pp. 265–267.

[41] Sudeep Tanwar et al. "Online signature-based biometric recognition". In: *Biometric-based physical and cybersecurity systems* (2019), pp. 255–285.

[42] Rana Tassabehji and Mumtaz A Kamala. "Evaluating biometrics for online banking: The case for usability". In: *International Journal of Information Management* 32.5 (2012), pp. 489–494.

[43] Bhushan S Thakare and Hemant R Deshmukh. "A combined feature extraction model using SIFT and LBP for offline signature verification system". In: *2018 3rd International Conference for Convergence in Technology (I2CT)*. IEEE. 2018, pp. 1–7.

[44] Maduhansi Thenuwara and Harshani RK Nagahamulla. "Offline handwritten signature verification system using random forest classifier". In: *2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer)*. IEEE. 2017, pp. 1–6.

[45] Ruben Tolosana et al. “Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification”. In: *IEEE Access* 3 (2015), pp. 478–489.

[46] Ruben Tolosana et al. “Presentation attacks in signature biometrics: types and introduction to attack detection”. In: *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection* (2019), pp. 439–453.

[47] Ruben Tolosana et al. “Reducing the template ageing effect in on-line signature biometrics”. In: *IET Biometrics* 8.6 (2019), pp. 422–430.

[48] Ruben Tolosana et al. “Update strategies for HMM-based dynamic signature biometric systems”. In: *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE. 2015, pp. 1–6.

[49] JF Vargas et al. “Off-line signature verification based on grey level information using texture features”. In: *Pattern Recognition* 44.2 (2011), pp. 375–385.

[50] Mustafa Berkay Yılmaz. “Offline signature verification with user-based and global classifiers of local features”. PhD thesis. 2015.

20MIS0399
Kaviya.k

Principal Component Analysis

- Sidharth Mishra; Uttam Sarkar; Sushash Tarophder

PCA, Principal Component Analysis is the oldest and best known technique of multivariate data analysis. The central idea of PCA is to reduce the dimensionality of the data set consisting of a larger number of interested or interrelated variables, while retaining as much as possible of the variation present in the data set.

Achieved by transforming to a new set of variables, the PCA which are uncorrelated and which are ordered so that the first few retain most of the variation present in all of the original variables, by reducing the no. of dimensions, without much loss of information.

Method:

$$SD = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x')(x_i - x')}{(n-1)}}$$

$$Var(x) = \frac{\sum_{i=1}^{n}(x_i - x')(x_i - x')}{(n-1)}$$

$$Cov(x, y) = \frac{\sum_{i=1}^{n}(x_i - x')(y_i - y')}{(n-1)}$$

$$C^{M \times N} = (c_{ij}), c_{ij} = cov(Dim_i, Dim_j)$$

Technique used in image Compression:

→ Organize a data set as an m x n matrix, m is the number of measurement types and n is the number of trials.

→ Data is spread out and on matrix algebra by calculating eigenvectors and eigenvalues which is the fundamental principle to determine PCA.

20M180399
Kavya.K

Suppose for a 3x3 square matrix,
we have 3 eigenvectors, multiplied it by the square matrix,
we get 4 times the scaled vector as our result.
The single-eigenvector decomposition has removed the contribution due to the smaller eigenvector and left us with data.

Conclusion:

→ One benefit of PCA is that we can examine the variances associated with the principle components.

→ Often one finds that large variances associated with the first k<m principal component and a precipitous drop up.

→ Most interesting dynamics occur only in the first k dimension

→ strength and weakness of PCA is a non-parametric analysis there are no parameters to tweak and no coefficients to adjust based on user experience the answer are unique and independent of the user and this same strength can be viewed as a weakness.

→ Main application of PCA is multivariate data analysis and image compression.

10/02/23

BIOMETRICS

M. VIGNESH
20MIS0175.

LINK: https://www.researchgate.net/publication/316672806_principle_Component_Analysis.

* PCA is a regular unsupervised learning Technique for reducing dimensionality of data.
* PCA is a multivariate Technique that analyze a data table in which observations are described by several inter-correlated quantitative dependent variable.
* Goal → Extract important information from the statistical table to represent in a set of new orthogonal variables called principle component and to display the pattern of similarity between the observations & of the variable as points in spot maps.
* First coined by Pearson (1901) & developed by Hotelling (1933).
* PCA is a best known technique of multivariable data analysis.
* Goals of PCA :-
  1. Extract the most important information from the data table.
  2. Simplify the description of the data size and compress the size of the data
  3. Technique used in image compression.

Methodology :

Steps for calculating PCA :-

1. Get some data set.
2. Subtract the mean.
3. Calculate the covariance matrix.
4. Calculate the Eigenvectors & Eigenvalues of the covariance matrix.

5. Choosing Component and forming a feature vector.

6. Deriving the new data set.

GEOMETRICAL INTERPRETATION:-

* PCA projects the data along the directions where the data varies the most

* The magnitude of the eigenvalues corresponds to the variance of the data along the eigenvector directions

Conclusion:-

* Benefits of PCA is that we can examine the variance associated with the principle components.

* Both strength & weakness of PCA is that it is a non-parametric analysis.

* performing PCA is quite simple in practice.

* organise a dataset as an m×n matrix.

where $m \rightarrow$ no. of measurement types.

$n \rightarrow$ number of trials.

* Substrate the mean for each measurement type or row or,

* calculate SVD.

* Hence we have learnt about principle Component Analysis (PCA).

Flipped class on PCA : [16 Feb] 4:06.

@ www.ijlr.org DOI : 10.5455/ijlr.20170415115235

M. Kaushik
20MIS0306

Defination:

Principal component analysis is a technique that analyzes a data table in which observation are described by inter correlated quantitative dependant variable, the main goal is to transform the correlated variable into small variables (Principle components) - Multi-variate technique.

Main aim or central idea - reduce dimensionality of large data set into small variables retaining the variation.

History:

→ Preseinderorfer & Mobley - Singular value decomposition.

→ Later Pearson & Hotelling - Two approach - standard algebraic deviation
Pearson - Finding planes and lanes.

→ Hotelling - mathematical solution.

↳ Chooses components to succensive correlation - avoid confusion.

Goal:

→ Extract vital information.

→ Compren size - safe guarding details.

→ Simplify data set.

→ Analyze structure of observations & variable.

→ Reduce dimesion - image compression.

→ Standard deviation
→ Variance
→ Covariance
→ Covariance matrix

→ Orthogonal.
→ Eigen values & vectors.

Methodology: [Steps]

1. Get some data
2. Subtract mean.
3. Find covariance matrix
4. Calculate Eigen values of covariance.
5. Choosing components to form a feature vector
6. Derive a new dataset.

Interpretation:

- Finds the data directions where the data changes are observed.
- Changes - Observed by eigen vectors and values.
- Magnitude in eigen value - variance of data along vector.

Conclusion.

→ Finds variance associated with principle components.
→ Helps to find ~~pur~~ pragmatic algorithm for the selected parameter
→ Helps in handling multivariate data and image compression.

Biometrics

S. Sadhana
20MIS0185

Principle component Analysis

Title:

Autonomous Profile based anomaly detection System

The autonomous anamaly detection system based on the statistical method principle component analysis creates a network profile called Digital signature of network segment using flow analysis. This denotes the predicted normal behaviour of a network traffic activity through historical data analysis

The principal component analysis for digital signature and anomaly detection is divided into two steps: traffic characterization and anomaly detection. The traffic characterization is performed by using principal component analysis as a mechanism analyze historical

Input data from network activity, identify the most relevant traffic time intervals amongst the dataset and then reduce them so that this new set can efficiently represent the regular behaviour of a network segment

In detection phase, abnormal events are detected based on digital signature network segment using flow analysis, which acts as a threshold to generate alarms. Aiming to minimize false alarm generation, Information extracted from the principle Component analysis performed during the traffic Characterization phase

The normalised mean square error measures the differences between the series predicted by a model. A receiver operating characteristics measures the performance of classifiers and widely used in signal detection theory to describe performance

20MIS0324
ROHITH·R·J

PRINCIPAL COMPONENT ANALYSIS.

Sasan Karamizadeh, Sahkidan M. Abdullah, et. al,

The principal component analysis (PCA) is a kind of algorithm in biometrics. PCA also is a tool to reduce multi dimensional data to lower dimensions while retaining most of the information. It covers standard deviation, covariance and Eigen vectors. This background knowledge is mean to make the. Principal Component Analysis also known as PCA (Karhuen- Loeve expansion) and data representation technique widely used in the areas of pattern recognition and Computer Vision. such as face recognition. The strategy of the Eigenfaces method consist of extracting the characteristic features on the face and representing the face in question as a linear combination of the so called 'eigenfaces' obtained from the feature extraction process. The principal component of the faces in the training set are calculated.

Recognition is achieved using the projection of the face in to the space formed by the eigenfaces. A comparison on the basis of Euclidean distance of the eigen vectors of the eigen faces and eigen face of the image under question is made.

20MIS0324
ROHITH R.J.

PCA Algorithm:-

Step-1 : Column or row vector of size N^2. represents the set of M images $(B_1, B_2, B_3 \cdots B_M)$ with size $N*N$

Step-2 :- The training set image average is described as

$$\mu = \frac{1}{m} \sum_{n=1}^{M} B_n.$$

Step-3 :- The average image by vector (ω) is different for each trainee image

$$W_i = B_i - \mu.$$

Step-4 :- Total Scatter Matrix or covariance matrix is calculated from ϕ as shown below:

$$C = \sum_{n=1}^{M} w_n w_n^T = AA^T$$

$$\text{Where } A = [W_1 W_2 W_3 \ldots W_n].$$

Step-5 :- Measure the eigen vectors U_L and eigen values λ_L of the covariance matrix C.

Step-6 :- For image classification, this feature space can be utilized. Measure the vector of weights

$$\Omega_T = [\omega_1; \omega_2, \ldots, \omega_M']$$

$$\text{Where } \omega_K = U_K^T (B - \mu), \quad K = 1, 2, \ldots M'$$

The PCA method is an unsupervised technique of learning that is mostly suitable for databases that contains images with no class labels.