SIGNATURE VERIFICATION USING ANN
-TRU-SIGN

A PROJECT REPORT
IV YEAR / VIII SEM
R2019

Submitted by

S. FAZEER MOHAMED	**(130719104024)**
G.D. GAUTHAM	**(130719104026)**
S. GOKUL SELVAN	**(130719104028)**

in partial fulfillment for the award of the degree
of

BACHELOR OF ENGINEERING

in

Department of COMPUTER SCIENCE AND ENGINEERING

JERUSALEM COLLEGE OF ENGINEERING
(An Autonomous Institution, Affiliated to Anna University, Chennai)
NBA & NAAC ACCREDITED INSTITUTION
Velachery Main Road, Narayanapuram, Pallikaranai, Chennai - 600100

MARCH 2023

JERUSALEM COLLEGE OF ENGINEERING

(An Autonomous Institution Affiliated to Anna University)

ANNA UNIVERSITY : CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report "**DIGITAL SIGNATURE VERIFICATION USING ANN - TRU-SIGN"** is the bonafide work of **S.FAZEER MOHAMED (130719104024), G.D.GAUTHAM (130719104026) and S.GOKULSELVAN (130719104028)** who carried out the project workunder my supervision.

SIGNATURE
Dr. MAYA EAPEN, M.E.,Ph.D.,
HEAD OF THE DEPARTMENT

Department of Computer
Science and Engineering,
Jerusalem College of Engineering,
Pallikaranai, Chennai – 600 100.

SIGNATURE
Mrs. H. Mercy, M.E.,
SUPERVISOR,
Associate Professor,
Department of Computer
Science and Engineering,
Jerusalem College of Engineering,
Pallikaranai, Chennai – 600 100.

Submitted for the University examination held on_____.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ABSTRACT

Bio-metrics play a crucial role in establishing an individual's identity. A signature is one of the most widely recognized way to authorize transactions and authenticate the human identity as compared to other electronic identification methods such as fingerprint and retina scans. Due to a huge demand for authentication, fast algorithms need to be assimilated for signature recognition and verification. Human signatures can be treated as an image and the techniques of neural networks can be applied to them for recognition and verification. This project exploits a database of samples of signatures that are captured in an image format, and this system and database is used to train the neural network. The authenticated signature data is then encrypted for security and confidentiality

ACKNOWLEDGEMENT

We extend our warmest gratitude to **Dr. M. Mala,** Chairperson, Jerusalem College of Engineering for her enduring support.

We express our sincere thanks to **Dr. Ramesh S, Ph.D.,** Principal, Jerusalem College of Engineering for his kindness, which enabled us to do this project.

We express our sincere thanks to **Dr. Maya Eapen, Ph.D.,** Professor and Head, Department of Computer Science and Engineering, Jerusalem College of Engineering for his support throughout the project.

We would like to take this opportunity to express our sincere thanks to our supervisor, **Mrs. H. Mercy, M.E.,** Associate Professor, Department of Computer Science and Engineering, Jerusalem College of Engineering for her valuable guidance, inspirations and technical support throughout the project.

We express our gratitude to our project coordinators, **Mrs. H. Mercy, M.E.,** Associate Professor and **Mrs. S. Vinitha, M.E.,** Assistant Professor, Department of Computer Science and Engineering, Jerusalem College of Engineering for their valuable guidance and support.

We thank all the faculty and supporting staff of the Department of Computer Science and Engineering, Jerusalem College of Engineering, for their co-operation and assistance in the successful completion of the project.

S. FAZEER MOHAMED (130719104024)

G.D. GAUTHAM (130719104026)

S. GOKUL SELVAN (130719104028)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

Sl. No	ABBREVIATION	EXPANSION
1	ANN	Artificial Neural Network
2	NN	Neural Network
3	CMOS	Complementary Metal Oxide Semiconductor
4	CCD	Charge-Coupled Device
5	API	Application Programming Interface
6	UI	User Interface

CHAPTER 1

INTRODUCTION

1.1 General

Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password). Things like keys or cards, however, tend to get Stolen or lost and passwords are often forgotten or disclosed. To achieve more reliable verification or identification we should use something that really characterizes the given person. Bio-metrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a signature or a voice sample. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample. Signature authentication technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring script pressure and angle used by the person when a signature is produced. This technology uses the individual's handwritten signature as a basis for authentication of entities and data. The authentication is mostly accurate and reliable. It uses one-way hash functions to encrypt the signature dynamics and data, and then append it to the document being signed in order to secure the authenticated signature.

1.2 Artificial Neural Network

Artificial neural networks (ANNs), usually simply called neural networks (NNs) or neural nets, are computing systems inspired by the biological neural networks that constitute animal brains. An ANN is based on a collection of connected units or nodes called artificial neurons, which loosely model the neurons in a biological brain. Each connection, like the synapses in a biological brain, can transmit a signal to other neurons. An artificial neuron receives signals then processes them and can signal neurons connected to it. The "signal" at a connection is a real number, and the output of each neuron is computed by some non-linear function of the sum of its inputs. The connections are called edges. Neurons and edges typically have a weight that adjusts as learning proceeds. The weight increases or decreases the strength of the signal at a connection. Neurons may have a threshold such that a signal is sent only if the aggregate signal crosses that threshold.

Typically, neurons are aggregated into layers. Different layers may perform different transformations on their inputs. Signals travel from the first layer (the input layer) to the last layer (the output layer), possibly after traversing the layers multiple times. ANNs have evolved into a broad family of techniques that have advanced the state of the art across multiple domains. The simplest types have one or more static components, including number of units, number of layers, unit weights and topology. Dynamic types allow one or more of these to evolve via learning. The latter are much more complicated but can shorten learning periods and produce better results. Some types allow/require learning to be "supervised" by the operator, while others operate independently. Some types operate purely in hardware, while others are purely software and run-on general-purpose computers.

1.3 Summary

A number of biometric techniques have been used for authentication such as face recognition, fingerprint recognition, voice recognition and signature recognition. However, signature verification is most widely used. Signature being the most prominent handwritten proof of identity is used for authentication of documents in the fields of financial, commercial, and legal transactions which requires high level of secured authentication. This project discusses signature verification and recognition using neural network approach. The method uses scanned signature fed to computer where its image quality is enhanced and compared, finally verifies the authenticity using neural network training. The system involves several stages such as image preprocessing, feature extraction and neural network training. Various classifiers can be used to train the system. The method uses features extracted from pre-processed signature images. The extracted features are used to train a neural network. Each technique has its own advantages and disadvantages. However, a lot of work has already been done yet there are many challenges in verification field.

CHAPTER 2

LITERATURE SURVEY

2.1 General

A literature review is an overview of the previously published works on a topic. The term can refer to a full scholarly paper or a section of a scholarly work such as a book, or an article. Either way, a literature review is supposed to provide the researcher/author and the audiences with a general image of the existing knowledge on the topic under question. This report focuses on signature verification, characterized by the usage of static images of signatures, where the objective is to distinguish if a given signature is produced by the claimed individual, or a produced by an impostor. This project presents a neural network-based recognition of handwritten signatures system that is trained with low-resolution scanned signature images.

2.2 Related Works

Title : Online Signature Verification using Deep Descriptors.

Authors : Abigail Singh and Serestina Viriri

Year : 2020

Description :

Signature verification is a technique used to counter signature forgery. In the past, the process began with staff at a bank, who is an expert, would confirm if a signature is genuine or forged. With the development of technology, now people no longer sign on paper, rather on a digital pad which can take more data which is recorded on paper, for example, pressure, azimuth and altitude angles. Examples of details captured from a

digital pen include pen pressure, azimuth and altitude angles. This data is now used in various dynamic signature verification systems that achieve high accuracy on evaluation tests using different forms of artificial intelligence. This paper investigates using artificial intelligence in the form of a Convolutional Neural Network (CNN) followed by a Recurrent Neural Network (RNN) to verify signatures using the SVC 2004 and SigComp2009 online datasets and it achieved a testing accuracy of 97.05%

Title : Static Signature Recognition and Verification using Neural Networks.

Authors : Gopichand G, Sailaja G, N. Venkata Vinod Kumar, T. Samatha

Year : 2019

Description :

Identification and verification of hard written signature from images is major issue. This is very difficult as even human eye does not have that much visual ability to identify every detail of the in handwritten. Signature changes every time so it is difficult for humans to identify the original and forged ones. By using deep learning which uses the sophisticated is digital configured replica of human brain, we can identify the forgery done in signature with higher accuracy.The robustness of human brain has always been an enigma and this has caused people to replicate it digitally. The human eye has a great efficiency of recognition due its architecture. This inspiration has led to people constructing artificial neural network and so deep learning. In this we generally are going to assess the ways a human being would give his signature using some deep learning algorithms and artificial neural networks by which we can train the system accordingly and verify if the signature is real or forged. It would be a great way to authenticate the signatures and verify them accordingly. It would be a better option to verify the signatures using this model rather than visual recognition through human eye which have a high chances of making a mistake.

Title : Online Handwritten Signature Verification System Based on Neural Network Classification.

Authors : Othman o-khalifa, Md. Khorshed Alam and Aisha Hassan Abdallai

Year : 2013

Description :

The signature verification is the oldest security technique to verify the identification of persons. Recently, the signature recognition schemes are growing in the world of security technology. It offers two different types of schemes those are offline and online method. The offline technique means to verify a signature written on paper which is scanned to convert it into a digital image, whereas the online system required an online device such as Tablet PC, touch screen monitor by a pressure sensitive pen to verify the signature. This paper discusses a review of offline signature verification schemes which considered as a highly secured technique to recognize the genuine person's identity. It addresses the offline signature verification technique using ANN approach.

Title : Signature recognition using artificial neural network.

Authors : Debnath bhattacharyya and Tai-hoon kim

Year : 2010

Description :

To avoid forgery and ensure the confidentiality of Information in the field of Information Technology Security an inseparable part of it. In order to deal with

security, Authentication plays an important role. This paper presents a view on the signature recognition technique and we also discussed about a technology of Signature Authentication by Back-propagation Algorithm with application. The purpose of this technique is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using this method it is possible to confirm or establish an individual's identity. We have also outlined opinions about the usability of signature authentication systems, comparison between different techniques and their advantages and disadvantages in this paper. Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password). Things like keys or cards, however, tend to get stolen or lost and passwords are often forgotten or disclosed.

2.3 Summary

There are numerous verification, authentication and encryption techniques and papers with several advantages and disadvantages. All of them follow different algorithms for every procedure in order to achieve most efficiency and accuracy. Still, they are all open to be updated, modernized and improved. This project has a combination of a few of those techniques and work more effectively in all aspects.

CHAPTER 3

SYSTEM ANALYSIS

3.1 General

Systems analysis is the process of studying a procedure or business to identify its goal and purposes and create systems and procedures that will efficiently achieve them. An individual(s) studies a system such that an information system can be analyzed, modeled, and a logical alternative can be chosen. Systems analysis projects are initiated for three reasons: problems, opportunities, and directives. In this project, system analysis is progressed in initiating the project.

3.2 Existing System

Authentication methods used currently are mostly inaccurate and efficient only to some extent leading to various minor and major crimes, non ethical activities and fraudulent acts. Encryption, Decryption, Verification and Authentication are all done using multiple systems in different stages, by huge algorithms. This project is capable of carrying out the methods in whole as a single process using way lesser systems, resources and algorithms comparatively and achieving efficient security verification technique.

3.3 Proposed System

Input of this system is a document, preferably an image document in common file formats like JPEG or PNG, with any kind of signature as its subject. Output of the system is digitalization of the signature, verification of the signature, and authentication of the given document.

Steps through which the system works are as follows,

i. Original signature document is scanned and upload to our software.

ii. The original document is encrypted for security.

iii. The input signature is scanned, uploaded and Preprocessed.

iv. The signature is verified and output is displayed.

3.4 Block Diagram

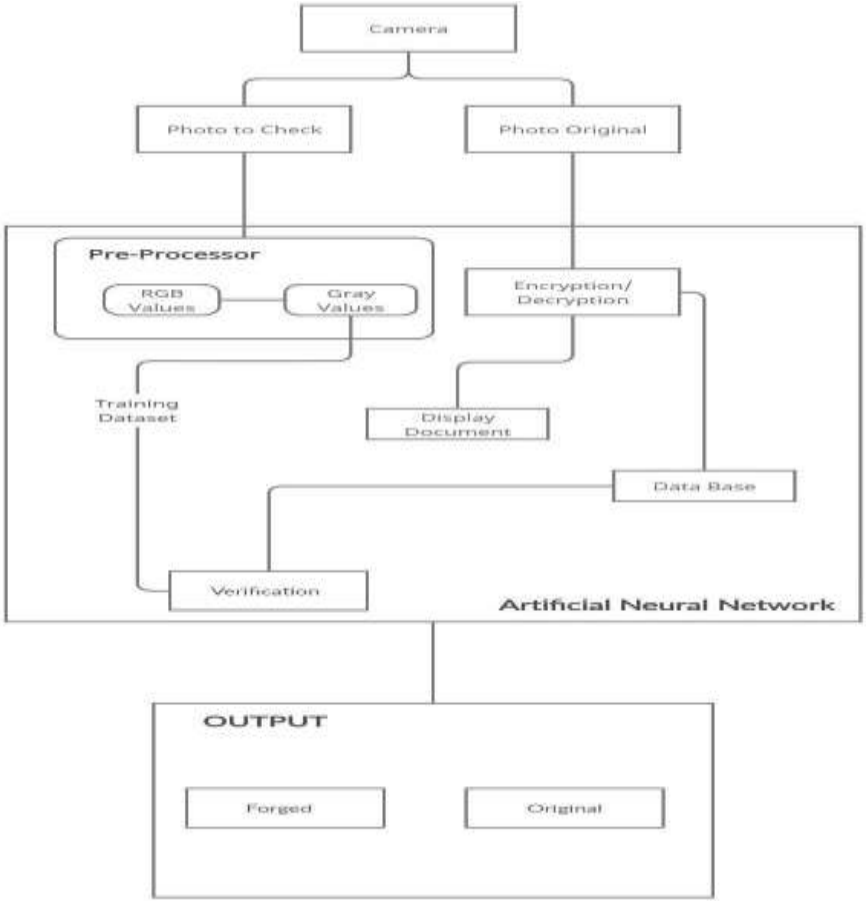

Fig 3.1 - Block Diagram

3.5 Hardware Requirements

- Camera.

Mobile phone cameras typically feature **CMOS active-pixel image sensors (CMOS sensors)** due to largely reduced power consumption compared to charge-coupled device (CCD) type cameras, which few camera phones use. Some use CMOS back-illuminated sensors, which use even less energy, at higher price than CMOS and CCD.

Fig 3.2 - Mobile Camera

- Sensor.

A sensor is a device that detects and responds to some type of input from the physical environment. The input can be light, heat, motion, moisture, pressure or any number of other environmental phenomena.

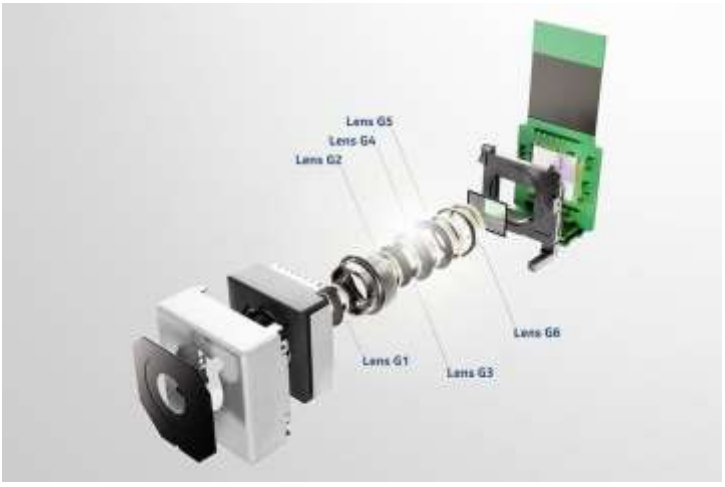

Fig 3.3 - Parts of Sensor

- Power Supply.

A power supply is an electrical device that supplies electric power to an electrical load. The main purpose of a power supply is to convert electric current from a source to the correct voltage, current, and frequency to power the load.

3.6 Software Requirements

- Python 3 and above.

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming. Python is a multi-paradigm programming language. Object-oriented programming and structured programming are fully supported, and many of their features support functional programming and aspect-oriented programming. Many other paradigms are supported via extensions, including design by contract and logic programming. Python uses dynamic typing and a combination of reference counting and a cycle-detecting garbage collector for memory management.

- Open CV

Open CV is a library of programming functions mainly aimed at real-time computer vision. Originally developed by Intel, it was later supported by Willow Garage then Itseez. The library is cross-platform and free for use under the open-source Apache 2 License. Open CV runs on the following desktop operating systems: Windows, Linux, macOS, FreeBSD, NetBSD, OpenBSD. Open CV runs on the following mobile operating systems: Android, iOS, Maemo, BlackBerry 10. The user can get official releases from SourceForge or take the latest sources from GitHub. Open CV uses CMake.

- NumPy

NumPy is a library for the Python programming language, adding support for large, multidimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays. It targets the CPython reference implementation of Python, which is a non-optimizing bytecode interpreter. Mathematical algorithms written for this version of Python often run much slower than compiled equivalents due to the absence of compiler optimization. NumPy addresses the slowness problem partly by providing multidimensional arrays and functions and operators that operate efficiently on arrays; using these requires rewriting some code, mostly inner loops, using NumPy.

- Tensor Flow

TensorFlow is a free and open-source software library for machine learning and artificial intelligence. It can be used across a range of tasks but has a particular focus on training and inference of deep neural networks. TensorFlow serves as the core platform and library for machine learning. TensorFlow's APIs use Keras to allow users to make their own machine learning models. In addition to building and training their model, TensorFlow can also help load the data to train the model, and deploy it using TensorFlow Serving.

- Figma

Figma is a cloud-based design and prototyping tool that is widely used in user interface and user experience (UI/UX) design. It allows designers to create, collaborate, and share design files in real-time with other team members, clients, or stakeholders. Figma provides a range of features that make it easy to design and prototype interfaces for web, mobile, and desktop applications.

- Multi-layer Perceptons (MLP)

A multilayer perceptron (MLP) is a feedforward artificial neural network that generates a set of outputs from a set of inputs. An MLP is characterized by several layers of input nodes connected as a directed graph between the input and output layers. MLP uses backpropagation for training the network. MLP is a deep learning method.

A multilayer perceptron is a neural network connecting multiple layers in a directed graph, which means that the signal path through the nodes only goes one way. Each node, apart from the input nodes, has a nonlinear activation function. An MLP uses backpropagation as a supervised learning technique. Since there are multiple layers of neurons, MLP is a deep learning technique.

3.7 Summary

System analysis of this project provides clear view on this project with points about existing system and proposed system, comparison between existing system and proposed system, a block diagram of the system architecture, hardware requirements and software requirements, and several other aspects of this project. Thus problems, opportunities, and directives of the project is defined and established. System analysis therefore helps in initiation and early implementation of the project.

CHAPTER 4

SYSTEM DESIGN

4.1 General

Systems design is the process of defining elements of a system like modules, architecture, components and their interfaces and data for a system based on the specified requirements. Systems design interfaces, and data for an electronic control system to satisfy specified requirements. System design could be seen as the application of system theory to product development. There is some overlap with the disciplines of system analysis, system architecture and system engineering.

System Architecture

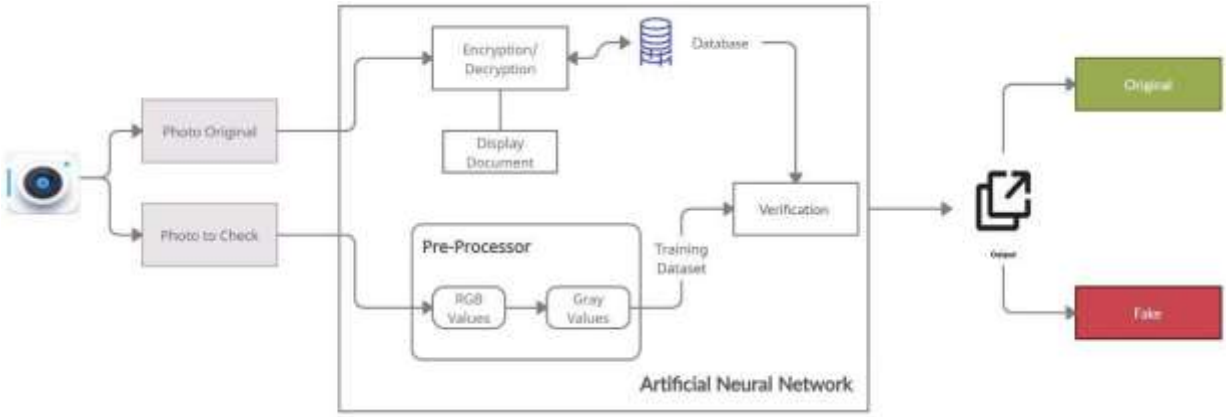

Fig 4.1 - System Architecture

4.2 Module Description

A module is a collection of source files and build settings that allow you to divide your project into discrete units of functionality. Your project can have one or many modules, and one module may use another module as a dependency. You can independently build, test, and debug each module. Projects module provides evidence and administration of contracts and projects. For some projects arrange a request for a subsidy,

others creates projects for manufacturing and delivering contracts. This project contains four modules in design. Digitalization of the signature, Encryption/Decryption, Verification of the signature and Software UI development. In this phase, Digitalization of signature module and Encryption/Decryption module are carried out. The remaining modules will be proceeded with in the next phase.

4.3 Digitalization of the Signature

Digitization is the process of converting information into a digital format. The result is the representation of an object, image, sound, document, or signal obtained by generating a series of numbers that describe a discrete set of points or samples. Digitalization is basically data acquisition. Data acquisition actually means giving data to the system. In this system the data is provided to the system in the form of a scanned image using the device of the user. An image of the signature is scanned using the signature is scanned and stored as a digital image.

Fig 4.2 - Scanning a document

4.4 Encryption and Decryption

Encryption:

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. In computing, unencrypted data is also known as plain text, and encrypted data is called cipher text. Encryption is a simple method of

protecting the data on your removable media. By encrypting your media (such as a USB), you are essentially creating a password to protect that specific media and the files it holds.

Decryption:

Decryption is the conversion of encrypted data into its original form. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password. The act of decryption may also be called unencrypt or unencryption. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data to protect company data and trade secrets. If this data needs to be view-able, it may require decryption. If a decryption passcode or key is unavailable, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

4.5 Verification of the Signature

Steps involved in signature verification:

- Data acquisition
- Pre processing
- Feature extraction
- Classification

1. Data acquisition:

Data acquisition actually means giving data to the system. In this system the data is provided to the system in the form of a scanned image. The signature is scanned and stored as a digital image.

2. Pre-processing:

Data pre-processing describes any type of processing performed on raw data to prepare it for another processing procedure. Hence, pre-processing is the preliminary step which transforms the data into a format that will be more easily and effectively processed. Therefore, the main task in pre-processing the captured data is to decrease the variation that causes a reduction in the recognition rate and increases the complexities.

3. Feature extraction:

In pattern recognition and in image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant (much data, but not much information) then the input data is transformed into a reduced representation set of features (also named features vector). Transforming the input data into the set of features is called feature extraction. The various feature extraction techniques are reported in

4. Classification:

Image classification analyses the numerical properties of various image features and organizes data into categories. Classification algorithms typically employ two phases of processing: training and testing. In the initial training phase, characteristic properties of typical image features are isolated and, based on these, a unique description of each classification category, i.e. training class, is created. In the subsequent testing phase, these feature-space partitions are used to classify image features.

4.6 Software UI Development

The software is designed using Figma with following pages,

- Home Page
- Upload page
- Encryption/Decryption page
- Result page

1. Home Page:

   This page contains general information about our project and the software.

2. Upload Page:

   This page contains the drop box option where we can upload our desired document for verification.

3. Encryption/Decryption Page:

   This page has encryption and decryption options for the document which the user wants to encrypt or decrypt.

4. Result Page:

   This page is important in our project where the verification of the digital signature of the document has been verified and shows the output to the user.

4.7 UML Diagrams

Use Case Diagram:

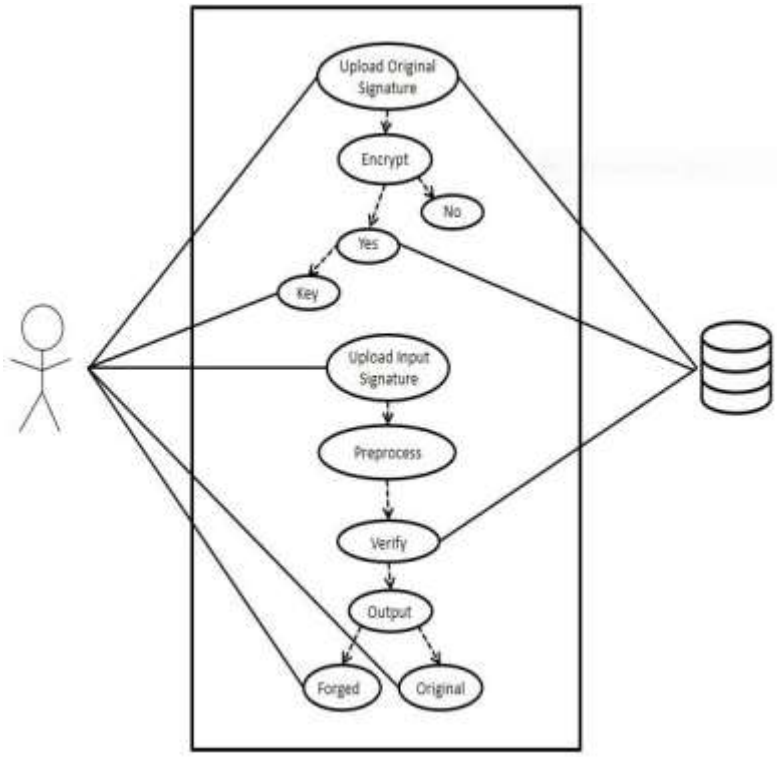

Fig 4.3 – Use Case

Sequence Diagram:

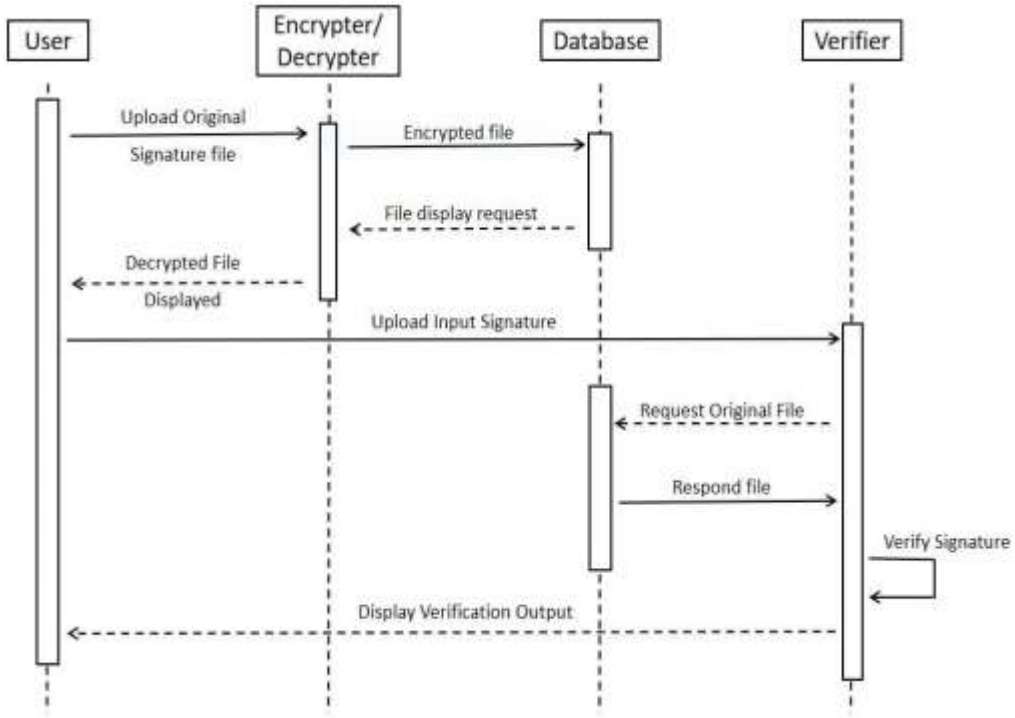

Fig 4.4 - Sequence Diagram

Class Diagram:

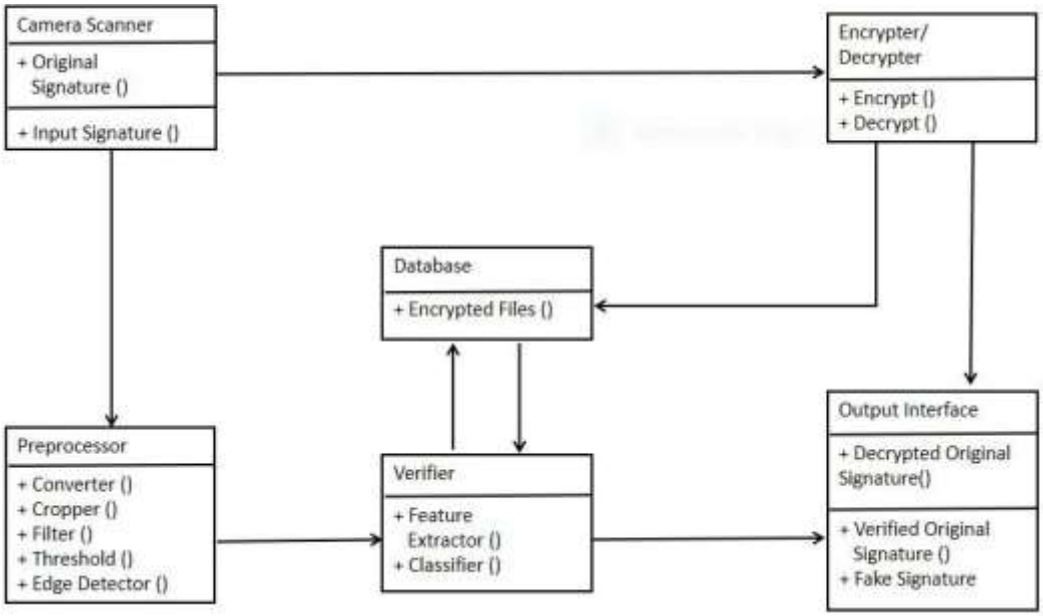

Fig 4.5 - Class Diagram

4.8 Conclusion

The goal of system design is to allocate the requirements of a large system to hardware and software components. The system design activity starts after the system requirements analysis has been completed. Irrespective of the tools used to create it, a good design system is one which is reusable, robust, and well-documented. Most importantly, a good design system helps make the design process more efficient, and ultimately, more cost-effective. The system design of this project achieved and fulfilled all these criteria.

4.9 Program Output:

Fig 4.6 – Encryption / Decryption work Page

Fig 4.7 - Open Signature

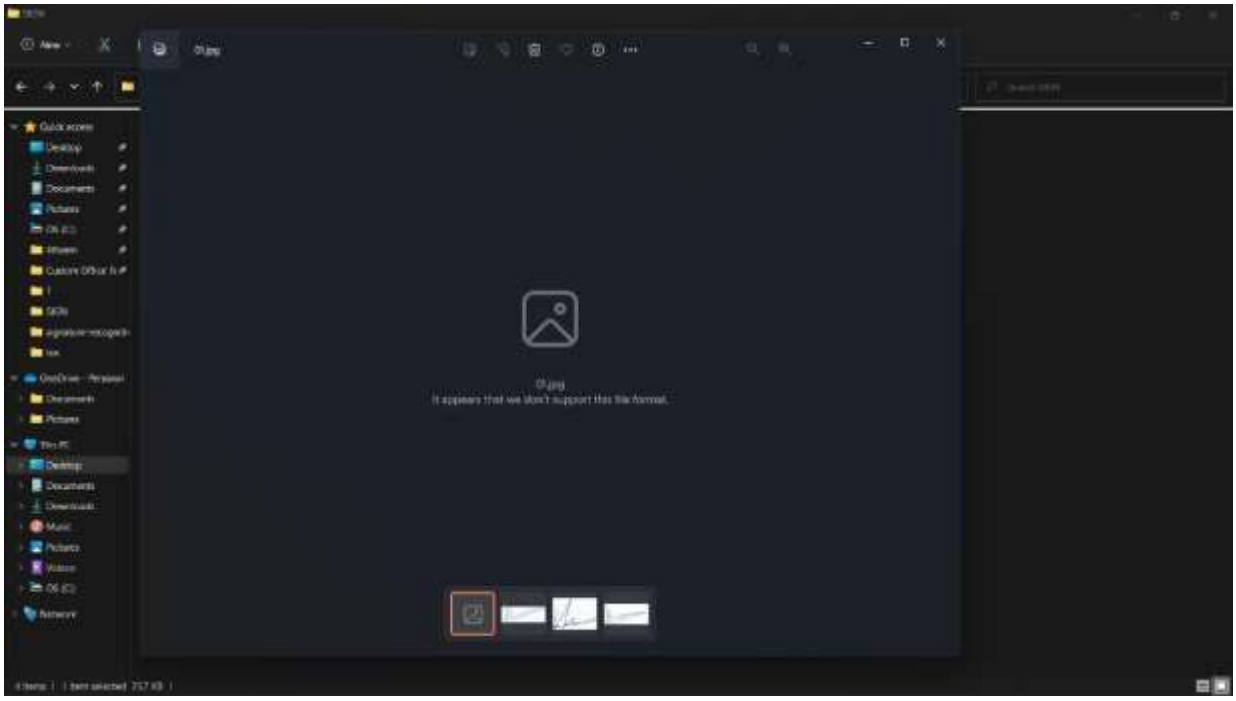

Fig 4.8 - Encryption

Fig 4.9 - Encrypted Signature

Fig 4.10 – s Page

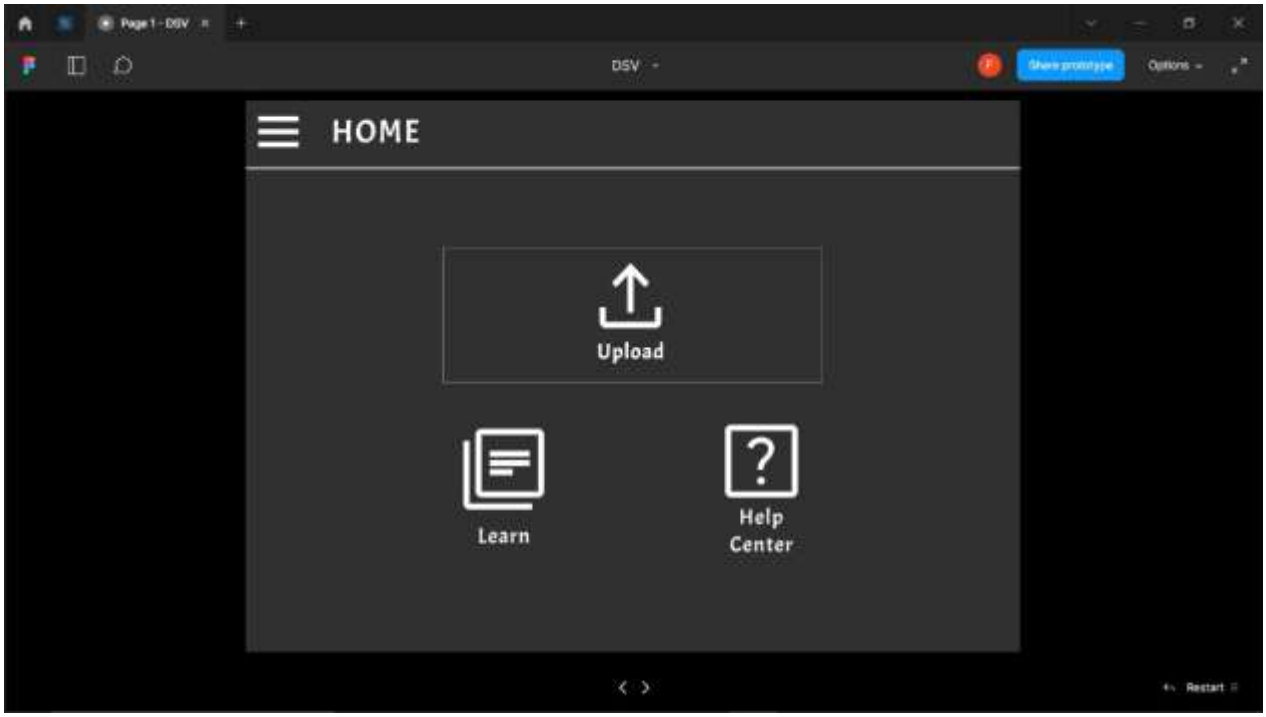

Fig 4.11 – Home Page

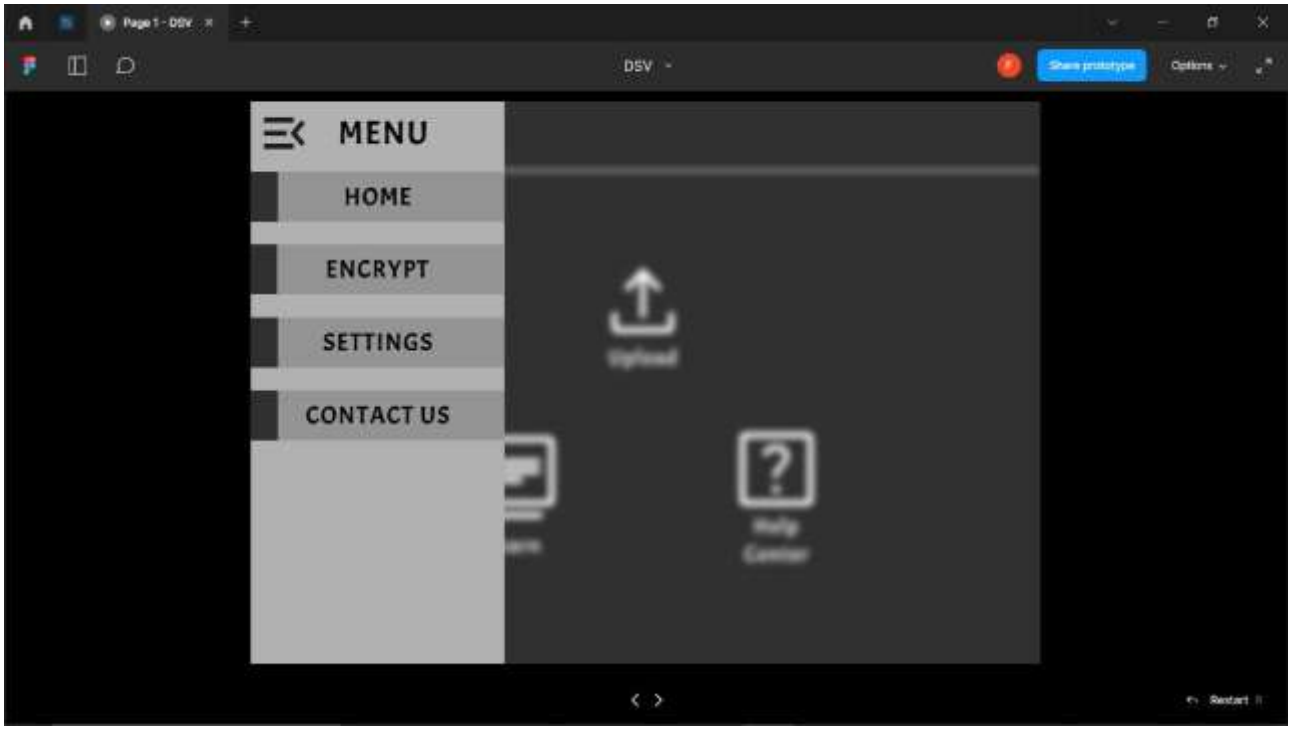

Fig 4.12 – Menu

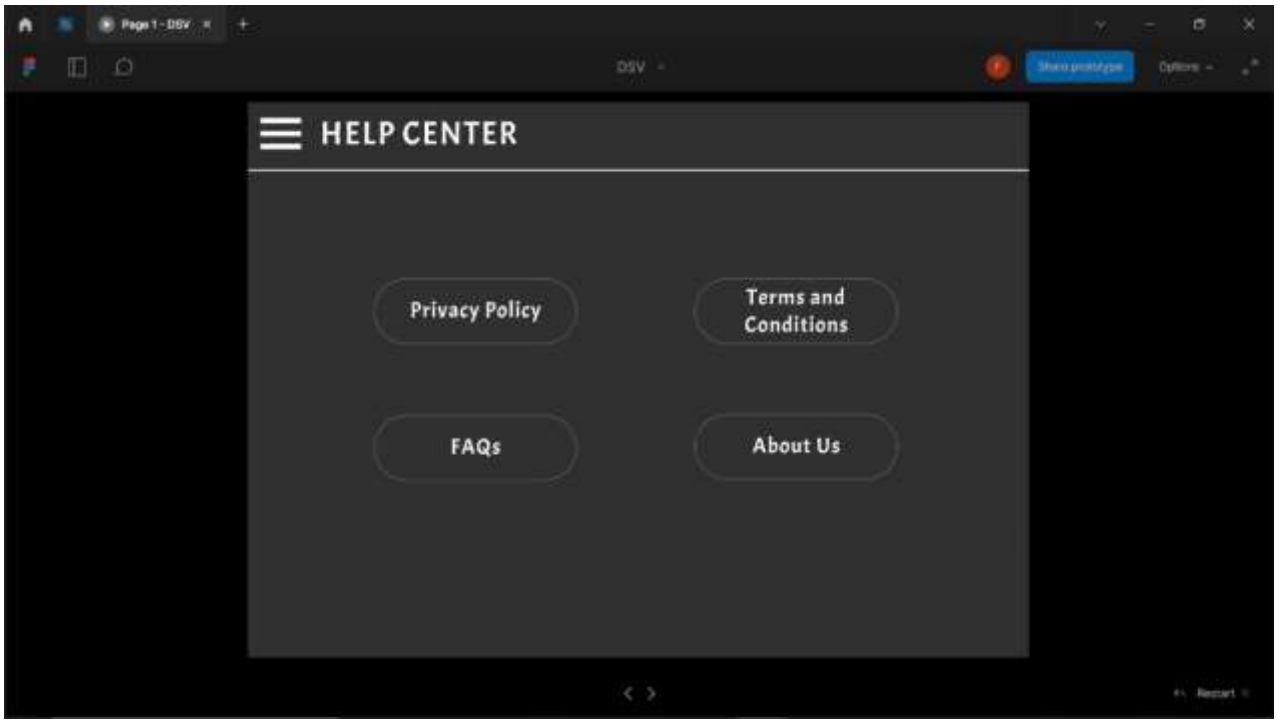

Fig 4.13 – Help Center Page

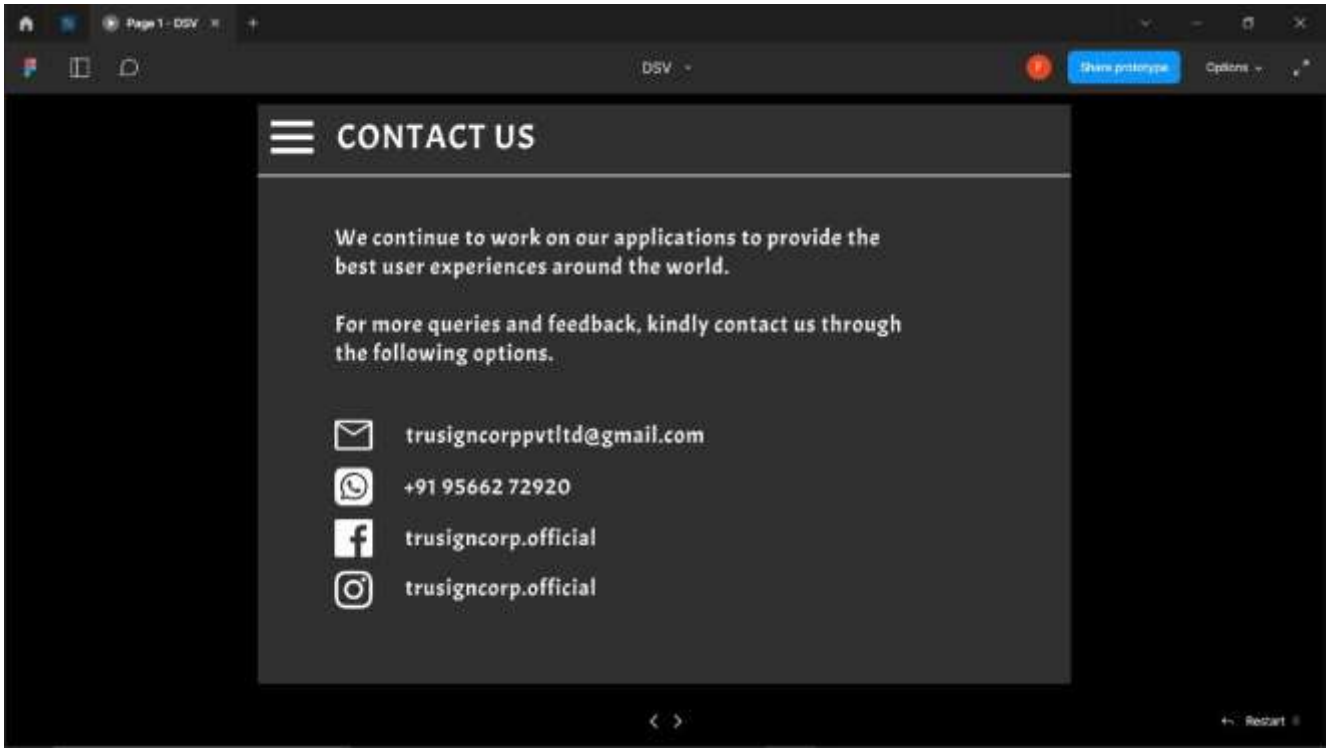

Fig 4.14 – Contact Page

Fig 4.15 – Upload Page

Fig 4.13 – Encryption / Decryption Page

Fig 4.13 – Result Page

CHAPTER 5

CONCLUSION

5.1 Summary on Phase I

This project discussed signature verification using neural network. This phase included modules of Digitalization of the signature and Encryption/Decryption of the scanned original signature. Digitalization or Data acquisition actually means giving data to the system. Encryption is the method by which information is converted into secret code that hides the information's true meaning. Decryption is the conversion of encrypted data into its original form. It is generally a reverse process of encryption. The two modules were analysed and designed and thus is ready to be moved to the next phase.

5.2 Future work on Phase II

The next phase will be dealing with modules of Verification of the input signature and Software development. Major processes are done in the Verification module like Pre-processing that carry out several steps to provide ready-to-process data, Feature extraction and Classification. UI design and Software Development include UI design and development of the interface, connection of code and database, which are final tasks to deploy the software.

5.3 Conclusion

A number of biometric techniques have been used for authentication. However, signature verification is most widely used. Signature being the most prominent handwritten proof of identity is used for authentication of documents. This project provides best service in encryption and verification of authenticated signatures.

REFERENCES

[1] Abigail Singh and Serestina Viriri School of Mathematic, Statistics and Computer Science University of Kwa-Zulu Natal Durban, South Africa Date of Conference: 11-12 March 2020 Date Added to IEEE Xplore: 30 April 2020

[2]Gopichand G, Sailaja G, N. Venkata Vinod Kumar, T. Samatha"Signature Verification using AI Network" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6S, March 2019

[3] Prachi Chauhan, Subhash Chandra and Sushila Maheshkar Static Digital Signature Recognition and Verification using Neural Networks Date of Conference: 12-14 August 2016 Date Added to IEEE Xplore: 13 July 2017

[4] Othman o-khalifa, Md. Khorshed Alam and Aisha Hassan Abdalla "An Evaluation on Offline Signature Verification using Artificial Neural Network" Approach Date of Conference: 26-28 August 2013 Date Added to IEEE Xplore: 17 October 2013

[5] Debnath Bhattacharyya And Tai-Hoon Kim "Signature Recognition Using Artificial Neural Network" January 2010

[6] Dmitrii I. Dikii , Viktoriia D. Artemeva "Online Handwritten Signature Verification System Based on Neural Network Classification" proposed in 2019