iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60271

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Comparing Traditional and Digital Methods for Detecting Forged Signatures in Forensic Analysis

Tanuja Bhadarge[1], Devyani Parkhe[2]
Department of Applied Sciences, Parul University

Abstract: ***Signatures are considered proofs for the validation of documents. Forgery of the signature is seen in almost all documents, ranging from bank checks, property papers, legal documents, and so on. The analysis of the signature can be a challenging task for forensic experts as fewer alphabets are used, so finding characteristics is difficult. In this research paper, we have discussed two ways of analyzing forged signatures: traditional and digital methods (Matlab and Python software). Traditional method: manual analysis of forged signatures with the help of a stereomicroscope and magnifying glass; digital method: using Matlab and Python software for analysis. In Matlab software, a curve fitting function is used in which the deviation of the graph is analyzed for both original and forged signatures. In Python software, two samples are added, one of which is the original signature and the other is the questioned sample. For analysis, 400 samples of signatures were used: 200 samples of the original signature and 200 samples of the questioned signature. The main aim of the paper is to find an easy and less time-consuming method for the analysis of the forged signature. The digital method has shown an accuracy of 95%. So it can be said that the digital method requires less time than the traditional method, and the accuracy and efficiency are almost the same.***

Keywords: Signature analysis, traditional method, digital methods, Matlab software, Python software, stereomicroscope.

I. INTRODUCTION

With the growth of the digital era, we require more attention and carefulness in our signatures. A signature is the consequence of a specific prototype that a person uses, and then, after continuous practice, it forms a uniform appearance of every person's writing. The differing movements of the pointer create an person's personal handwriting style; e.g A movement's evidence may be seen in the relationships between the letters, their size, their speed of writing, their consistency and continuity of execution, their hesitations and pauses, and the pressure of writing [1]. Forensic-questioned documents have become the most common and important study. The analysis of handwriting, signatures, documents, etc. can aid in crime scene investigation. Handwriting is an acquired skill that we have learned since childhood; mainly, it is referred to as a neuromuscular task. Each and every individual has different handwriting because the arm is made up of 30 bones and controlled by more than 40 muscles. So, the function of bones and muscles is different for every individual. As you know about handwriting, there are basically two principles of handwriting:

1) No two handwriting samples will be 100% the same.
2) All the writing contains natural variation, so no two handwriting samples by the same person will be exactly alike.

Handwriting identification is a discriminatory process that is derived when we compare writing habits and then evaluate the significance of their similarities or differences. It has to be stated that the methodical foundations of forensic handwriting expertise were developed in the second half of the 20th century, when the texts of documents were written by hand [4]. Rules for identification of handwriting:

a) Each mature writer has a handwriting that is personal and individual to him alone.
b) Deterioration in the handwriting of any individual due to any cause will affect all the properties of writing and is not confined to change.
c) Attempted disguise leads to inferior quality and never-better handwriting samples.
d) A writer cannot exceed his maximum writing ability or skill without regressing over a period of time.
e) Writing variation is an integral part of handwriting, and this is a property of identification.

For the judicial and law enforcement systems, it is crucial to know if a person's handwriting can be used to identify them [9]. Other divisions of crime examination of evidence, such as blood-urine sample examination and testing of fibers, paint, and other materials, are supported by a wealth of chemical and biological scientific knowledge that has been proven by scientific study. A biometric attribute is a handwritten signature. Biometric recognition and corroboration systems are being used more and more in our nature. Well-accepted biometric methods contain face, fingerprint, iris, and cornea-based identification and confirmation.

©IJRASET: All Rights are Reserved

Though qualities like iris, cornea, and fingerprints have depleted intra division difference and do not change over occasion, they need exclusive hardware to take the picture. One significant benefit of the signature over additional biometric ascribes is its time-consuming history in numerous frequently faced confirmation tasks. It has remained consumed for eras in inhabitant treatments, though other techniques (like fingerprints) motionless carry the disgrace of being connected to offender investigations. It is widely acknowledged that a person's signature is unique, even though we are not aware of any studies that support this claim. However, even forensic experts are not always able to determine whether a signature is authentic or not because intra-class variants—that is, the signature of a single person—can be quite big, making signature confirmation a challenging design detection difficulty. In addition, signatures are calmer to falsify than other biometric qualities. In many cases, the forged signature resembles the original handwriting of the forger. The skills and style designs of any writing are usually different for each individual, so when someone tries to forge the writing due to its natural tendency, the movement of the hand will be similar to a forger's handwriting. It follows that the counterfeit will naturally have better handwriting than the original when a skilled penman forges the signature of a less skilled penman without making any attempt to replicate or imitate it. However, if the forger is a stronger penman than the genuine writer, this outcome may also occur in some situations where there is a purposeful attempt to imitate a signature being used as a model [5]. Every individual has the habit of writing an alphabet in a particular way or style. When the individual tries to change the habit, hesitation marks will be seen. In most cases of signature forgery, it has been difficult to detect the forgery and the person who forged it. Whenever we have little space to write, we try to compact the alphabets and write, which can affect various characteristics of the handwriting identification. The same applies when we have enough space to sign or write; we do it in a good flow, and this can also change the characteristics of the handwriting identification. In most of the cases where we take a sample signature in one size, we usually do not pay attention to the size, which can prove our analysis report wrong. The signatures of different dimensions are statistically dissimilar, which can affect the characteristic origin process in online and offline signature verification [24] . Signatures are an important detail of the documents. Due to the limited quantity of writing in the signature and short notes, forensic handwriting experts are not able to find out enough characteristics, and usually the case remains unsolved. As of now, in the digital age, everything is present on the internet, and various open-source high-tech tools are also present. With the help of these things, they try to forge the handwriting. Criminals even learn to imitate the pressure characteristics of handwriting objects, which becomes the main problem in forensic handwriting examination [3]. As signatures and short notes are smaller, more cases of forgery are registered. There is a need for appropriate methods for solving this problem. Signatures are used as biometric applications in many places. It can be said that signatures that are complex in nature are difficult to forge. A complex signature has various strokes that are placed on each other diagonally, so forging them is not easy. A signature is used as an authentication for the verification of an individual. The signature of an individual is used in various bank statements, property papers, bank checks, and many other legal documents. Therefore, the analysis of the signature is important as it can be forged for personal benefits. Analysis is usually based on the writing characteristics. The writing characteristics are classified into two types:

- Class characteristics are shared features or traits that are typical of a particular style or class of handwriting. The common characteristics of the handwriting that are observed are size, slant, style, speed, spacing, movement, pen position, alignment, skill, etc. They serve as the basis for categorizing the handwriting in a particular class. Class characteristics provide us with valuable information about the general characteristics of a piece of writing. Size can be categorized into three categories: small, medium, and large. Style chiefly varies upon the personalise teaching, but it gets adapted according to person wills and the espousal of alphabet shapes that plea to the particular person. It may be simple or artistic; it can also be circular, bony, or a combination of the two. The movement of the writing may be executed using the entire arm, the forearm, the wrist, the fingers or a mix of some of these. Skill acquired by a person depends upon his initial training, writing experience, and physical, emotional, and intellectual personality. Spacing of the words in a line, of lines in a paragraph, and of paragraphs in a text are valuable points. Alignment of writing lines with respect to an imaginary baseline and with other lines, of signatures with the baseline, and of various lines in an address are distinctive features of a writer. The pen position may be held at an angle to the writing surface, varying from 15 degrees to 90 degrees. The angle of the pen and nib with reference to the baseline also varies and is useful in the identification of handwriting. The line quality of the handwriting is the smoothness, strength, and flow of the letters. In the original signature, all the class characteristics seem to be smooth and natural.
- Individual Characteristics: These are the unique and distinctive features that are specific to an individual person's writing style. These features are highly personalized and differentiate one individual's handwriting from another within the same class. The individual characteristics that are observed are the position of the i dot, the position of the t-bar, letter design, connectivity of strokes, embellishments, retouching, pen pressure, etc.

Forensic examiners focus on identifying these distinctive features to compare the questioned sample to an original sample. Individual characteristics play a crucial role in forensic handwriting analysis by offering a level of specificity. The position of the i dot and t bar varies for each individual. Pen pressure is the pressure applied by fingers in the process of writing. Usually, high pen pressure is seen in forged signatures. The indentation marks are seen if high pressure is applied while writing. Pen pauses deposit extra ink at the position of the stoppage. The pen pauses in forgery are in the starting stroke, ending stroke, embellishments, difficult formations, and connectives. Letter designs are the unique formation of the alphabets. It is smooth in the original signature. Embellishments are the extra strokes added to the signature to make it look attractive. Usually, in forged signatures, hesitation marks are seen in letter designs and embellishments. Pen lifts are the lifting of the pens for certain letter formations. In forged signatures or writing, more pen lifts are observed. Retouching is the overwriting of the alphabets in a genuine signature that is not seen, but in a forged signature. Most of the time, it is intended to imitate the shading pattern or to hide pen lifts. While forging the signatures, the connection of the strokes is interrupted due to pen pauses, whereas in a genuine or original signature, continuity is seen in the signature.

The processes underlying identification are:

1) Analysis or discriminating Element Determination: The questioned sample and the original sample should be examined or observed on the basis of different handwriting characteristics. These characteristics are the features of the handwriting that can be directly observed.

2) Comparison: The questioned sample, which is examined or observed, is compared with the original sample, which is the standard sample provided by the court.

3) Evaluation: Similarities and dissimilarities of the samples are evaluated, and an explanation for each feature is provided.

4) Forgery is the act of creating, altering, or falsifying a signature with the intention to mislead others. In our childhood, we also did some kind of forgery, such as forging parents' signatures on the marksheet, results, complaint letters, etc. In India, forgery is addressed under the Indian Penal Code Section 463. The types of signature forgery are:

a) Simulated Forgery: The act of attempting to replicate someone else's signature. In simulated forgery, the characteristics of the signatures are intentionally imitated to mislead others into believing that the document is genuine. Signs for simulated forgery: -

- High pen pressure.
- Multiple pen lifts.
- Retracing or retouching of strokes.
- Hesitation marks.

b) Traced Forgery: The forger contains a standard sample of the signature, which is then traced by the forger to make the document genuine. The forged signature will be 100% similar to the standard sample. Ways for traced forgery - using tracing paper, using carbon paper, using a projector or screen. Signs for traced forgery: -

- High pen pressure.
- Thicker strokes.
- Multiple pen lifts.
- Retracing or retouching of strokes.
- Wrist or finger movement is seen.

c) Tricked Forgery: In tricked forgery, the forger takes three to four samples of the same signature and then distributes the signature into equal parts and combines the signature. Signs for tricked forgery: -

- Ink negativity.
- Widening of alphabets.
- Spacing inconsistent.
- Uneven connecting strokes.

d) Spurious Forgery: In this case, someone else signs the document on your behalf. For example, your friend collects your report card and signs it on your behalf. Signs of spurious forgery: Everything will vary.

e) Transplanted Forgery: In this kind of forgery, the signature is transplanted from one document to another. In this case, the main question is in the context of the document.

Sophisticated techniques are needed to extract handwriting specimens from documents for computer-assisted handwriting analysis utilizing digital technologies, especially to eliminate document backdrops. The two digital methods shown in this paper can be used in forensic signature analysis, but they require software that is installed on the computer.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

The software requires source code, which can be used to start with the analysis procedure. Coding is the process of allocating a code to something for identification. In the context of computer programming, coding involves putting human-readable instructions into a format that a computer can understand and execute. The aim of coding is to create software, applications, and scripts that perform particular tasks or solve problems. The key aspects of the coding are: Algorithm design is a set of step-by-step procedures for solving a particular problem. Programming languages include Python, Java, C++, JavaScript, and many more. Code implementation, in which the writer writes the code based on the programming language, following the rules and syntax of that language. In this process, the errors are identified and fixed to ensure that it functions as intended. Testing involves verifying the code's correctness and efficiency. Coding has numerous benefits in various areas: software development, app development, web development, game development, embedded systems, data analysis and machine learning, cybersecurity, artificial intelligence, etc. Coding requires a lot of patience and consistency. In this paper, coding is used in the software for signature verification.

II. MATERIALS AND METHODOLOGY

A. Sample Collection

For the signature samples, a total of 200 participants were used. Each participant has provided their original signature on a plain sheet of paper. The simulated forgeries of the samples were done. So a total of 400 samples of signatures were used, which is 200 original signatures and 200 forged signatures. All the participants were students of various departments, and a consent letter was readied and signed before providing the signatures.

1) Traditional Method

For our traditional method, a stereo microscope was used for the analysis. The features that were extracted from each signature were length, height, mean, slant, and initial and terminal strokes. For calculating the length and height of each signature, a measuring scale was used. The mean was calculated with the help of readings of length and height, which were already calculated. For finding the angle of the slant protector, Slant tells us about the angle at which the pen was held while signing. The initial and terminal strokes of the signatures were observed and compared. For analysis, a set of signatures was made, consisting of one original sample of an individual and one questioned sample of the same individual.

2) Digital Method

For our digital method, two software programs were used: MATLAB and Python.

a) MATLAB software: MATLAB was first adopted by researchers and practitioners. Soon, it spread to various other domains. Today, it is also used in education for teaching linear algebra and numerical analysis. The MATLAB application is built in the MATLAB language. The simplest way to use the MATLAB code is to type it in the command window, which is present on the MATLAB desktop. Sequences of commands can be saved in a text file by using the MATLAB editor or a script into a function for extending the commands available.

Features of MATLAB:

- A high-level language designed for technical computing.
- A development environment for handling code, files, and data
- Interactive tools for iterative discovery, design, and issue resolution
- Data visualization using 2D and 3D graphic
- Add-on toolboxes expand the MATLAB environment
- MATLAB also has a high-level language and programming tools, allowing you to swiftly create and evaluate methods and applications.

For using MATLAB for signature verification, a curve-fitting technique was used. Curve fitting is a mathematical technique used to find the best-fitting curve or function to a firm of data points. Two features were used for signature verification – curve-fitting graph and mean value of signature image.

Source code for Curve-fitting graph is [1] –

```
X = input('Enter list of abscissas: ');
Y = input('Enter list of ordinates: ');
F = input('Enter 1 for linear fit, 2 for parabolic and so on: ');
n = length(X);
```

©IJRASET: All Rights are Reserved

```
N = F+1; %for dimension of matrix A
A = zeros (N,N);
for i=1:N
        for j=1:N
        A(i,j) = sum(X.^(i+j-2));
        end
end
B = zeros(N,1);
for k=1:N
        B(k) = sum((X.^(k-1)).*Y);
end
U = A\B;
%displaying polynomial
disp('Your polynomial is:')
for k=N:-1:2
        fprintf('+(%.2fx^%d)',U(k),k-1)
end
fprintf('+(%.4f)\n' ,U(1))
%plotting
P = flip(U);
x = linspace(X(1),X(n),100);
y = polyval (P,x);
plot(x,y,'r')
hold on
```

Step 1 – Save the above given source code in the new script.
Step 2 – Run the code.
Step 3 – Now enter the list of abscissas (x value) of original signature. The abscissas here are the length of the alphabets or curves present in the signature.
Step 4 – Enter the list of ordinates (y value) of original signature. The ordinates here are the height of the alphabets or curves present in the signature.
Step 5 – Enter 2 for parabolic fit. For signature verification we need parabolic fit.
Step 6 – Now a graph will be shown.
Step 7 – Again, run the code.
Step 8 - Enter the list of abscissas (x value) of questioned signatures.
Step 9 - Enter the list of ordinates (y value) of questioned signature.
Step 10 – The questioned sample graph will be plotted on the original sample graph.

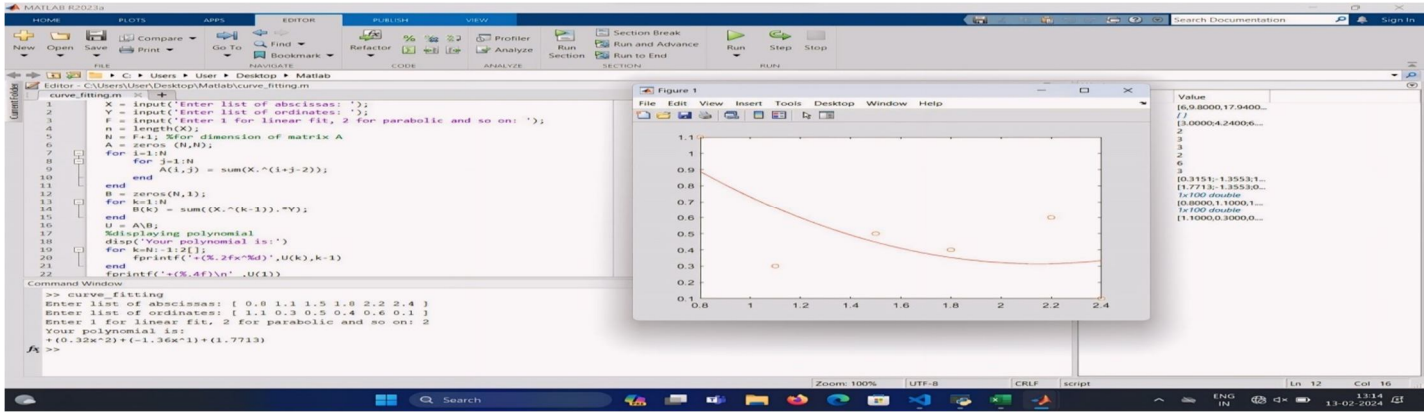


Fig. 1: Matlab code with graph. It describes the curve fitting curve and the command window that provides the results of the code when the data points are added.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Source code for mean value of signature image is –

```
clc;
clear;
close all;
warning('off','all')
%%%%%%%% READ THE INPUT IMAGES FROM THE DATASET %%%%%%%
[f,d]=uigetfile('*.jpeg');
image=imread([d f]);
figure,imshow(image),title('INPUT IMAGE');
%%%%%%%% TO CONVERT THE IMAGE TO GRAYSCALE %%%%%%%%%
gray=rgb2gray(image);
meanimag1=mean(gray(:))
figure,imshow(gray),title('GRAY CONVERTED IMAGE');
```

Step 1 - Save the above given source code in the new script.
Step 2 – Run the code.
Step 3 – Enter the original image of the signature sample.
Step 4 – The mean value of the signature will be shown.
Step 5 – Repeat the same for the questioned sample.

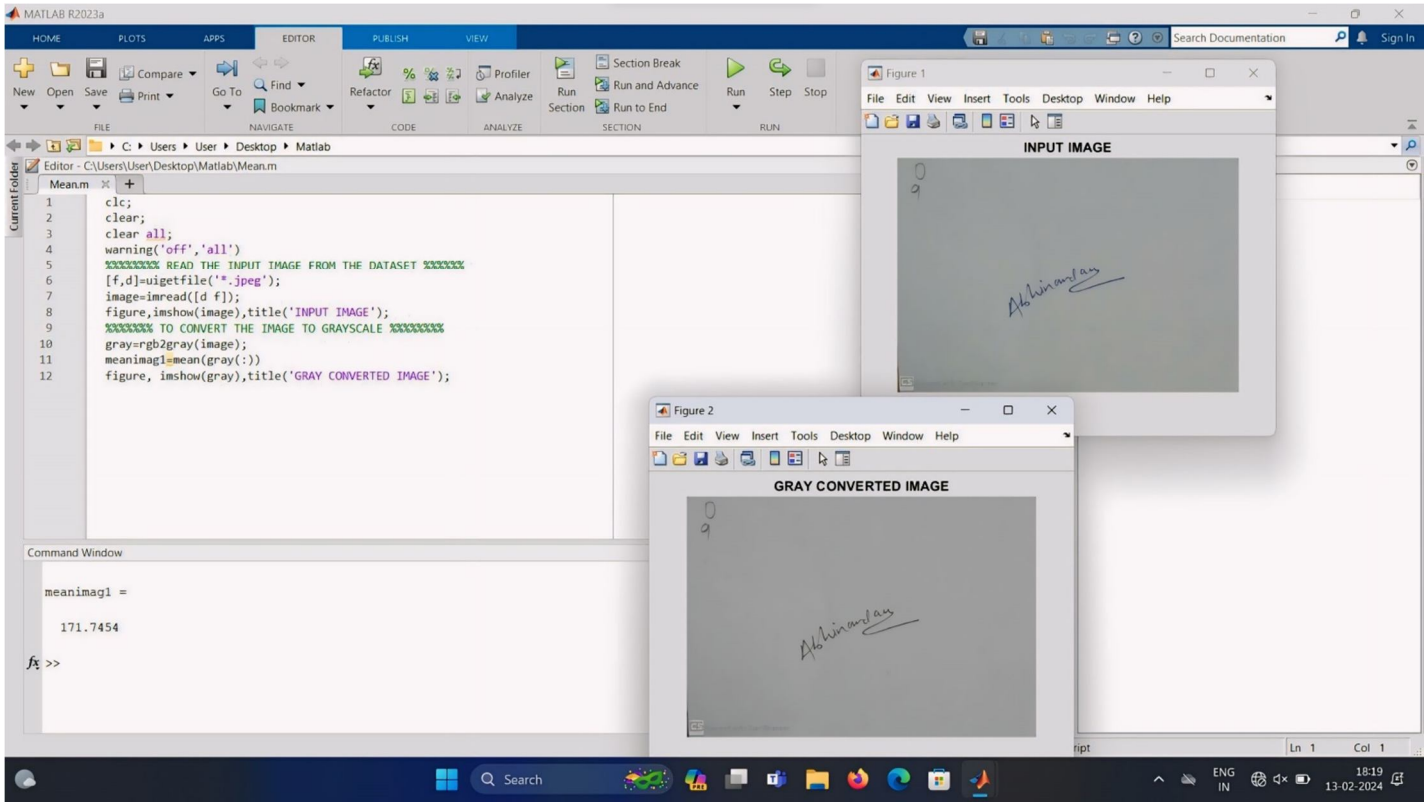


Fig. 2: Matlab mean code. It describes the editor window with code, the input image, and the gray-converted image of the signature. The results are shown in the command window.

b) PYTHON software: Python is a complex, translated software design speech for ease and legibility. It is a versatile and powerful language suitable for a wide range of applications, and its popularity continues to grow across various fields. It features dynamic typing and provisions to numerous encoding patterns, comprising practical, target concerned, and useable software.

Features of PYTHON:

- Large standard library – It contains a comprehensive criterion collection that stipulates components and sets for a broad variety of tasks.

- Community support – It has a large and active community, contributing to a wealth of resources, libraries and frameworks.
- Object-oriented – It encourages code organization and reusability.
- Platform Independence – Code written in Python can run on diverse running structures without modification.
- Extensibility – It can be extended through C/C++ integration, allowing for performance-critical sections to be written.
- Ease of learning – For beginners it is a great language due to its simplicity.
- While making this code we had kept the threshold value 90 which means if the signatures match more than 90% they will be considered as the original signature. Difference of 10% is kept because of natural variations present in the writing. The application finds differences based on the structural features of the signatures.

Source code for signature verification in python [2] -

```
import tkinter as tk
from tkinter.filedialog import askopenfilename
from tkinter import messagebox
import os
import cv2
from numpy import result_type
from signature import match, showimage1,showimage2

# Mach Threshold
THRESHOLD = 90

def browsefunc(ent,functionName):
        filename = askopenfilename(filetypes=([
        ("image", ".jpeg"),
        ("image", ".png"),
        ("image", ".jpg"),
        ]))
        ent.delete(0, tk.END)
        ent.insert(tk.END, filename)  # add this
        if functionName == "showimage1":
        showimage1(ent.get())
        else:
        showimage2(ent.get())

def capture_image_from_cam_into_temp(sign=1):
        cam = cv2.VideoCapture(0, cv2.CAP_DSHOW)

    cv2.namedWindow("test")

        # img_counter = 0

        while True:
        ret, frame = cam.read()
        if not ret:
        print("failed to grab frame")
        break
      cv2.imshow("test", frame)

        k = cv2.waitKey(1)
        if k % 256 == 27:
```

```
            # ESC pressed
            print("Escape hit, closing...")
            break
            elif k % 256 == 32:
            # SPACE pressed
            if not os.path.isdir('temp'):
            os.mkdir('temp', mode=0o777)  # make sure the directory exists
            # img_name = "./temp/opencv_frame_{}.png".format(img_counter)
            if(sign == 1):
            img_name = "./temp/test_img1.png"
            else:
            img_name = "./temp/test_img2.png"
            print('imwrite=', cv2.imwrite(filename=img_name, img=frame))
            print("{} written!".format(img_name))
            # img_counter += 1
            cam.release()
            cv2.destroyAllWindows()
            return True

def captureImage(ent, sign=1):
            if(sign == 1):
            filename = os.getcwd()+'\\temp\\test_img1.png'
            else:
            filename = os.getcwd()+'\\temp\\test_img2.png'
            # messagebox.showinfo(
            #           'SUCCESS!!!', 'Press Space Bar to click picture and ESC to exit')
            res = None
            res = messagebox.askquestion(
            'Click Picture', 'Press Space Bar to click picture and ESC to exit')
            if res == 'yes':
      capture_image_from_cam_into_temp(sign=sign)
            ent.delete(0, tk.END)
            ent.insert(tk.END, filename)
            return True

def checkSimilarity(path1, path2):
            result = match(path1=path1, path2=path2)
            if(result <= THRESHOLD):
      messagebox.showerror("Failure: Signatures Do Not Match",
                        "Signatures are "+str(result)+f" % similar!!")
            pass
            else:
      messagebox.showinfo("Success: Signatures Match",
                        "Signatures are "+str(result)+f" % similar!!")
            return True

root = tk.Tk()
root.title("Signature Matching")
root.geometry("500x700")  # 300x200
uname_label = tk.Label(root, text="Compare Two Signatures:", font=10)
```

```
uname_label.place(x=90, y=50)

img1_message = tk.Label(root, text="Signature 1", font=10)
img1_message.place(x=10, y=120)

image1_path_entry = tk.Entry(root, font=10)
image1_path_entry.place(x=150, y=120)

img1_capture_button = tk.Button(
        root, text="Capture", font=10, command=lambda: captureImage(ent=image1_path_entry, sign=1))
img1_capture_button.place(x=400, y=90)

img1_browse_button = tk.Button(
        root, text="Browse", font=10, command=lambda: browsefunc(ent=image1_path_entry, functionName="showimage1"))
img1_browse_button.place(x=400, y=140)

image2_path_entry = tk.Entry(root, font=10)
image2_path_entry.place(x=150, y=240)

img2_message = tk.Label(root, text="Signature 2", font=10)
img2_message.place(x=10, y=250)

img2_capture_button = tk.Button(
        root, text="Capture", font=10, command=lambda: captureImage(ent=image2_path_entry, sign=2))
img2_capture_button.place(x=400, y=210)

img2_browse_button = tk.Button(
        root, text="Browse", font=10, command=lambda: browsefunc(ent=image2_path_entry,functionName="showimage2"))
img2_browse_button.place(x=400, y=260)

compare_button = tk.Button(
        root, text="Compare", font=10, command=lambda: checkSimilarity(
                                        path1=image1_path_entry.get(),
                                        path2=image2_path_entry.get(),))

compare_button.place(x=200, y=320)
root.mainloop()
```

Step 1 – Save the above given code in python. Naming it main.py
Step 2 – Now type python main.py in command window.
Step 3 – Signature matching box will open.
Step 4 – Enter the original signature or capture it.
Step 5 – Enter the questioned signature or capture it.
Step 6 – Compare both the signatures.
Step 7 – The results will be shown on the screen in percentage.

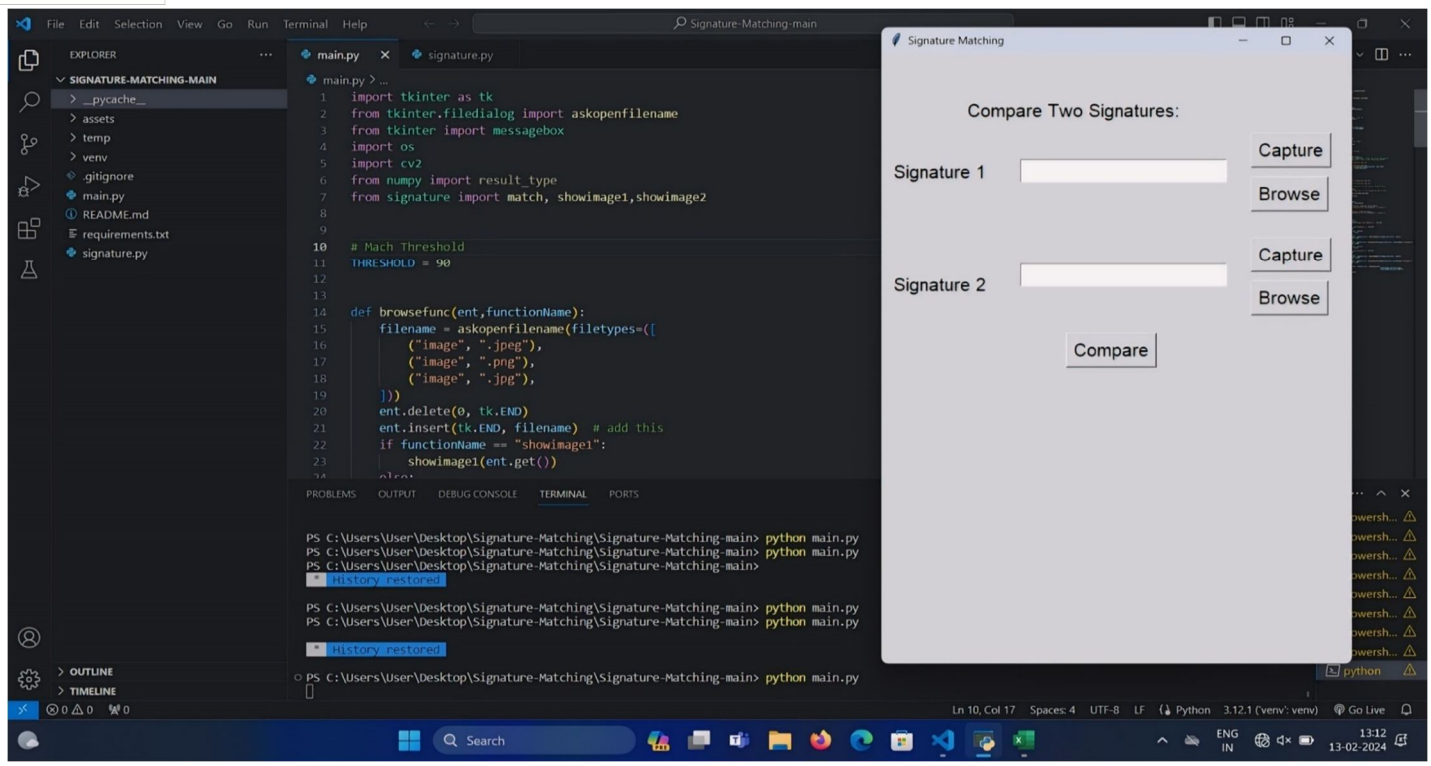


Fig 3: Python code and signature matching box

III. OBSERVATIONS AND RESULTS

In the traditional method, as a result, to complete one set of signatures, 10 minutes were needed. So, approximately 34 hours were needed for 200 sets of signatures. According to the observations made through the traditional method, it was said that all 200 questioned samples were forged. Whereas in digital methods, MATLAB software has taken approx. 3 minutes for each set of signatures. The results were calculated based on the difference between the two graphs. If the difference in the graph is more than 5cm, it will be considered a forged signature, as shown in Fig. 5, and if it is less than 5 cm, it will be considered an original signature, as shown in Fig. 4. If the mean value of the signature has shown the difference more than 10 then they are considered forged signature. After comparing the signatures with both the criteria the application was able to detect forgery in 190 sets of signatures. In 10 sets of signatures, the application has shown that the forged signature is original. Python software has taken approx. 2 minutes for each set of signatures. The threshold used was 90; 10% was kept for natural variations. So, if the system shows 76% similarity, it will be considered forged, as shown in Fig. 6, and if 92% similarity is shown, it will be considered the original signature, as shown in Fig. 7.

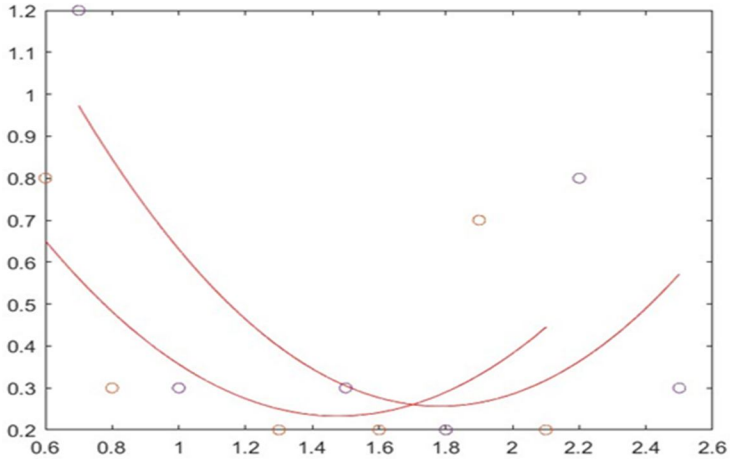


Fig 4: Matlab graph – Original signature

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

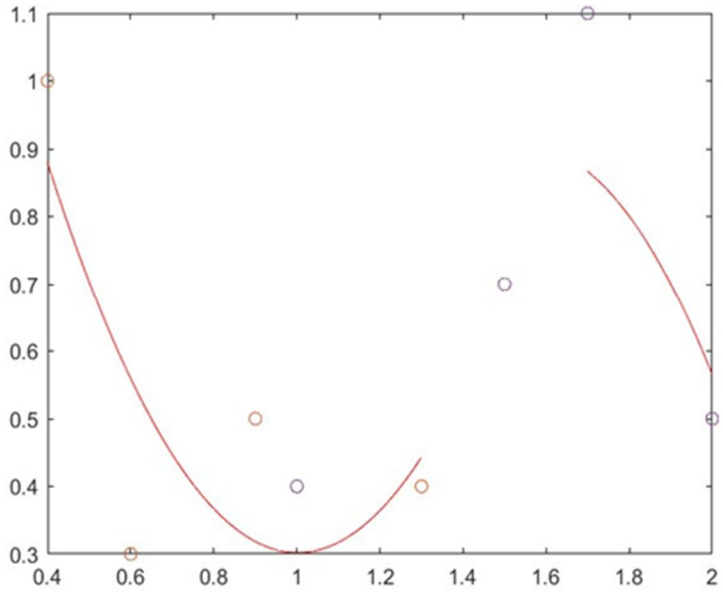


Fig 5: Matlab graph – Forged signature

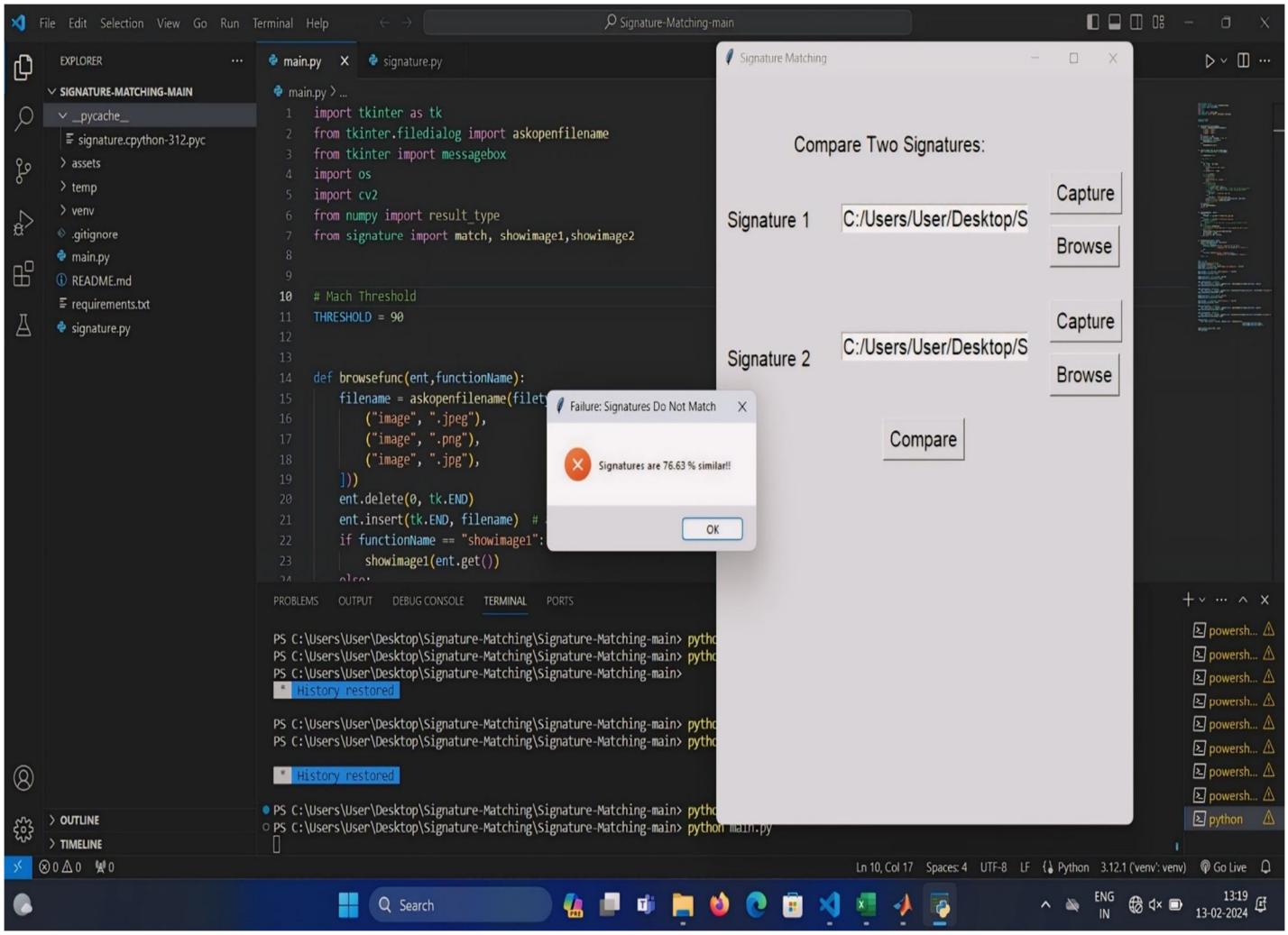


Fig 6: Python detecting forged signatures.

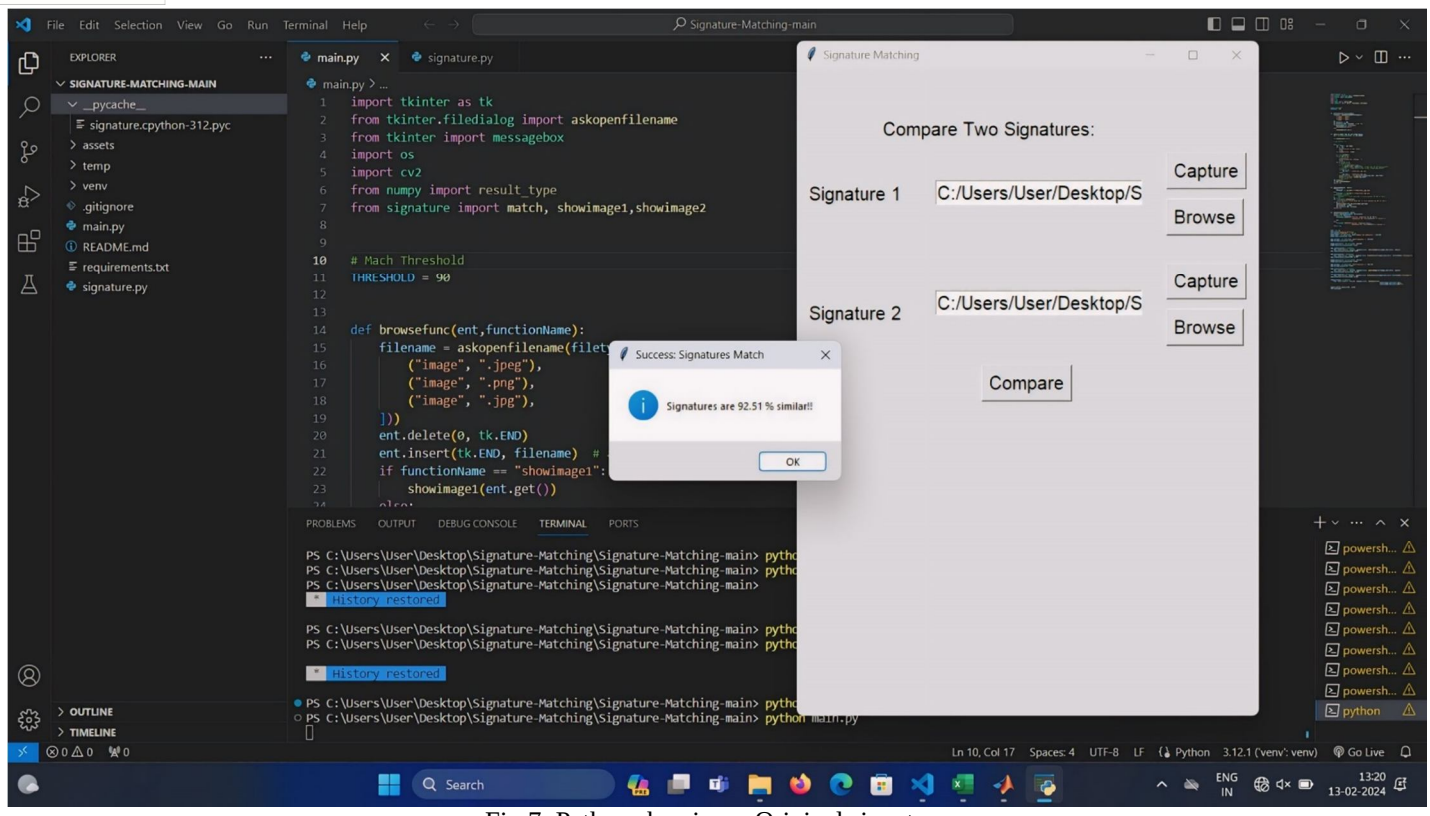


Fig 7: Python showing – Original signature

According to the results, MATLAB has a false acceptance rate (FAR) of 5%, and Python has a FAR of 4%. The accuracy of both digital methods is approximately 95%–96%, which is also explained below:

		Recognized	Not recognized	Total
Matlab	No.	190	10	200
	%	95	5	100
Python	No.	192	8	200
	%	96	4	100

IV. CONCLUSION AND FUTURE WORK

In this paper, we have demonstrated that our digital-based system outperforms most human verifiers. Therefore, as a substitute for human verification, our digital system is a viable option. It is clear from the above-shown table that one human verifier, with a FAR of 4%–5%, performed significantly. The accuracy of our systems is 95%–96%. In order to ascertain whether these results were significant or coincidental, the experiment has to be performed several times. Also, more features should be added to the system. Due to time constraints, it is now no longer carried out. In future works, the software should be updated with more features, as of now, only limited features are used. The data points of the signature image was collected manually in matlab software in future work can be done on this for digitally collecting the data points.

V. ACKNOWLEDGMENT

My dissertation would not have been possible and completed without the support and guidance of my colleagues and the faculty members. On acknowledgement of my dissertation, I would first like to thank the whole Department of Forensic Science.
I am very much thankful to my parents, for their care, affection, and support.

I would like to extend my thanks to honourable Dr. Trilok B. Akhani (Dean/Principal, Parul Institute of Applied Science, Parul University), Dr. Pallavi Khedkar (Academic Director of Parul University), and Mr. Karan J. Mehta (Head, Department of Forensic Science, PIAS, Parul University), whose valuable guidance and suggestions have played a major role in accomplishment of my training.

I would like to extend my gratitude to my guide, Ms. Devyani Parkhe who helped and supported me in pursuing my dissertation her continuous support and encouragement that helped me overcome the obstacles that I encountered during the realization of this project. Without her valuable feedback and instructions, it would be impossible to complete this project, which constitutes a significant attempt to present the empirical work of forensic document examiners. I also have to thank Ms. Yachna Modi (Faculty of Mathematics Department) for her help and very beneficial talking in regards to my project, which helped me solve the problems of coding in the software in general. In addition, I would like to thank the staff, students, and colleagues who always offered their help with professionalism and immediacy without a second thought or hesitation. Also, thanks to all of them who provided me with a sample of signatures.

On a personal level, I want to express my sincere love and thanks to my friends who have supported me from the first moment and helped me to not lose hope and faith during the most difficult moments of this project, to stay focused on my goal, and to give the full range of my abilities for the successful completion of my dissertation.

Finally, I would like to thank everyone who supported me to complete my training successfully.

- Tanuja Bhadarge

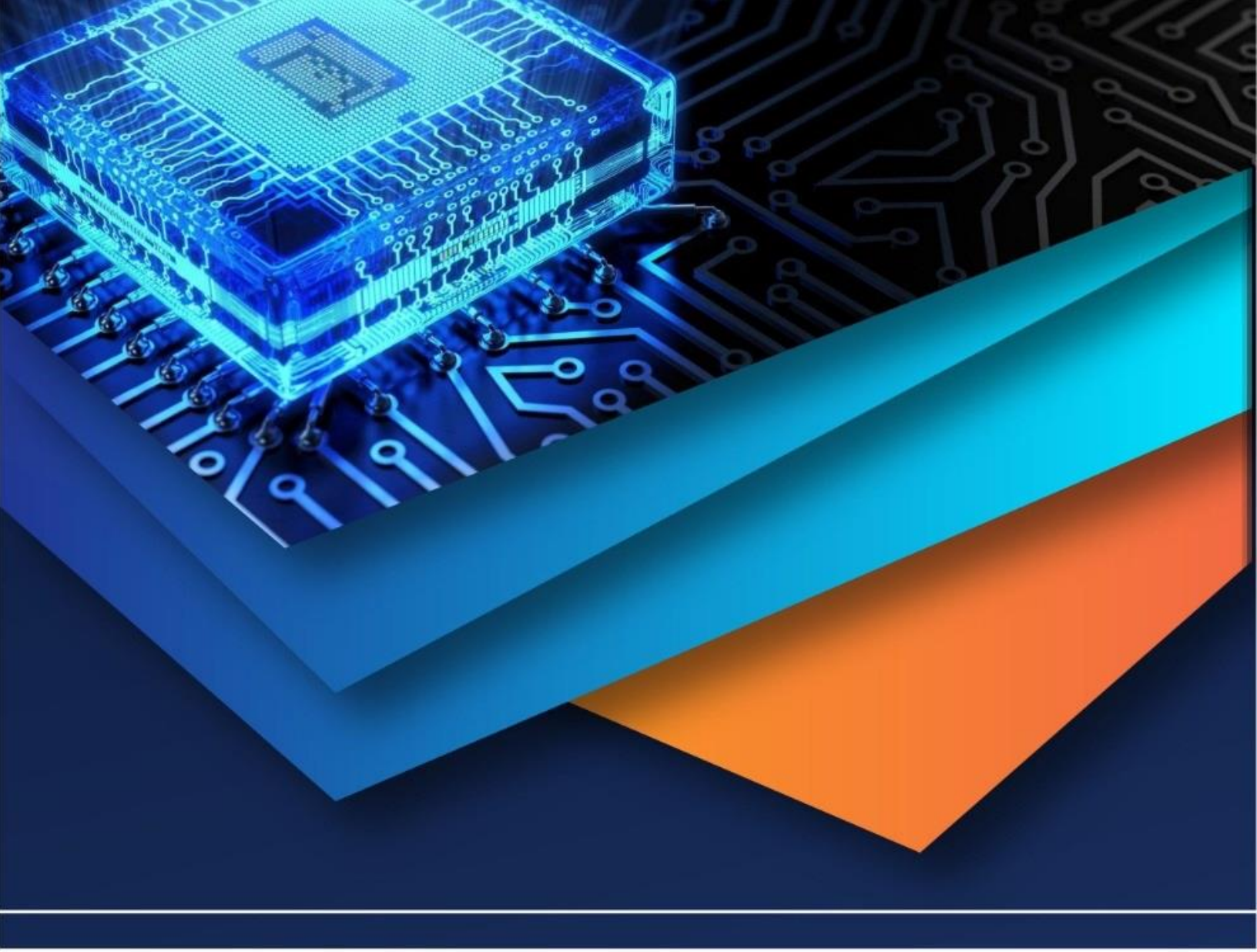
REFERENCES

[1] Chatzisterkotis, T. (2015). An examination of quantitative methods for Forensic Signature Analysis and the admissibility of signature verification system as legal evidence (Doctoral dissertation, University of Kent (United Kingdom)).
[2] Franke, K. Y., Schomaker, L. R. B., Veenhuis, C., Vuurpijl, L. G., Erp, M. V., & Guyon, I. (2004). WANDA: A common ground for forensic handwriting examination and writer identification
[3] Krasiuk, I. P. (2022). Problems of forensic handwriting examination in the analysis of signatures and short notes. НАУКОВИЙ ВІСНИК, 27(1), 72.
[4] Huber, R. A., & Headrick, A. M. (1999). Handwriting identification: facts and fundamentals. CRC press.
[5] Black, D. A. (1962). Forged signatures more skillfully written than the true signatures. J. Crim. L. Criminology & Police Sci., 53, 109.
[6] Hassaïne, A., & Al-Maadeed, S. (2012). An online signature verification system for forgery and disguise detection. In Neural Information Processing: 19th International Conference, ICONIP 2012, Doha, Qatar, November 12-15, 2012, Proceedings, Part IV 19 (pp. 552-559). Springer Berlin Heidelberg.
[7] Anagha, R., & Kumar, C. (2023). SIGNATURE RECOGNITION AND FORGERY DETECTION. Authorea Preprints.
[8] Franke, K., & Köppen, M. (2001). A computer-based system to support forensic studies on handwritten documents. International Journal on Document Analysis and Recognition, 3, 218-231.
[9] Leedham, S. S. G., & Srihari, S. (2003, November). A survey of computer methods in forensic handwritten document examination. In Proceeding the Eleventh International Graphonomics Society Conference, Sccottsdale Arazona (pp. 278-281)
[10] Spagnolo, G. S., Simonetti, C., & Cozzella, L. (2004). Superposed strokes analysis by conoscopic holography as an aid for a handwriting expert. Journal of Optics A: Pure and Applied Optics, 6(9), 869.
[11] Alonso-Fernandez, F., Fairhurst, M. C., Fierrez, J., & Ortega-Garcia, J. (2007, September). Impact of signature legibility and signature type in off-line signature verification. In 2007 Biometrics Symposium (pp. 1-6). IEEE.
[12] Sita, J., Found, B., & Rogers, D. K. (2002). Forensic handwriting examiners' expertise for signature comparison. Journal of Forensic Sciences, 47(5), 1117-1124.
[13] Manning, K. A., & Srihari, S. N. (2009, August). Computer-assisted handwriting analysis: Interaction with legal issues in US courts. In International Workshop on Computational Forensics (pp. 137-149). Berlin, Heidelberg: Springer Berlin Heidelberg.
[14] Jain, A. K., Griess, F. D., & Connell, S. D. (2002). On-line signature verification. Pattern recognition, 35(12), 2963-2972.
[15] Bertolini, D., Oliveira, L. S., Justino, E., & Sabourin, R. (2010). Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition, 43(1), 387-396.
[16] Baltzakis, H., & Papamarkos, N. (2001). A new signature verification technique based on a two-stage neural network classifier. Engineering applications of Artificial intelligence, 14(1), 95-103.
[17] Dimauro, G., Impedovo, S., Lucchese, M. G., Modugno, R., & Pirlo, G. (2004, October). Recent advancements in automatic signature verification. In Ninth International Workshop on Frontiers in Handwriting Recognition (pp. 179-184). IEEE.
[18] Fairhurst, M. C., Kaplani, E., & Guest, R. M. (2001). Complexity measures in handwritten signature verification. In HCI (pp. 305-309).
[19] Morales, A., Morocho, D., Fierrez, J., & Vera-Rodriguez, R. (2017). Signature authentication based on human intervention: performance and complementarity with automatic systems. IET Biometrics, 6(4), 307-315.
[20] Oliveira, L. S., Justino, E., Freitas, C., & Sabourin, R. (2005, June). The graphology applied to signature verification. In 12th conference of the international graphonomics society (pp. 286-290).
[21] Bhattacharya, I., Ghosh, P., & Biswas, S. (2013). Offline signature verification using pixel matching technique. Procedia Technology, 10, 970-977.
[22] Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: The state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(5), 609-635.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[23] Qi, Y., & Hunt, B. R. (1995). A multiresolution approach to computer verification of handwritten signatures. IEEE Transactions on Image Processing, 4(6), 870-874.
[24] Araujo, R. S. A., Cavalcanti, G. D., & Carvalho Filho, E. C. D. B. (2006, October). On-line verification for signatures of different sizes. In Tenth international workshop on frontiers in handwriting recognition. Suvisoft.
[25] Bovino, L., Impedovo, S., Pirlo, G., & Sarcinella, L. (2003, August). Multi-Expert Verification of Hand-Written Signatures. In ICDAR (Vol. 3, pp. 932-936).
[26] Chalechale, A., Naghdy, G., Premaratne, P., & Mertins, A. (2004, June). Document image analysis and verification using cursive signature. In 2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763) (Vol. 2, pp. 887-890). IEEE.
[27] Bulacu, M., & Schomaker, L. (2007). Text-independent writer identification and verification using textural and allographic features. IEEE transactions on pattern analysis and machine intelligence, 29(4), 701-717.
[28] Coetzer, J., Herbst, B. M., & Du Preez, J. A. (2006, October). Off-line signature verification: A comparison between human and machine performance. In Tenth International Workshop on Frontiers in Handwriting Recognition. Suvisoft.
[29] El-Yacoubi, A., Justino, E. J. R., Sabourin, R., & Bortolozzi, F. (2000, December). Off-line signature verification using HMMs and cross-validation. In Neural Networks for Signal Processing X. Proceedings of the 2000 IEEE Signal Processing Society Workshop (Cat. No. 00TH8501) (Vol. 2, pp. 859-868). IEEE.
[30] Freire-Santos, M., Fierrez-Aguilar, J., & Ortega-Garcia, J. (2006, April). Cryptographic key generation using handwritten signature. In Biometric technology for human identification III (Vol. 6202, pp. 225-231). SPIE.
[31] Fierrez, J., Ortega-Garcia, J., Ramos, D., & Gonzalez-Rodriguez, J. (2007). HMM-based on-line signature verification: Feature extraction and signature modeling. Pattern recognition letters, 28(16), 2325-2334.
[32] Gonzalez-Rodriguez, J., Fierrez-Aguilar, J., Ramos-Castro, D., & Ortega-Garcia, J. (2005). Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems. Forensic science international, 155(2-3), 126-140.
[33] Jayasekara, B., Jayasiri, A., & Udawatta, L. (2006, August). An evolving signature recognition system. In First international conference on industrial and information systems (pp. 529-534). IEEE.
[34] Ismail, I. A., Ramadan, M. A., El-Danaf, T. S., & Samak, A. H. (2010). An efficient off line signature identification method based on fourier descriptor and chain codes. International Journal of Computer Science and Network Security, 10(5), 29-35.
[35] Majhi, B., Reddy, Y. S., & Babu, D. P. (2006). Novel features for off-line signature verification. International Journal of Computers Communications & Control, 1(1), 17-24.

YOUTUBE REFERENCES
[1] Curve fitting with matlab code - ATTIQ IQBAL https://youtu.be/0pqSL3ezwVo?si=SGYXkVjz-4Sfg2fm
[2] Signature matching code walkthrough - Code2project https://youtu.be/SfCab_QAwgY?si=eVXqHfYUuKmLwarU



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)