WE PRESENT YOU WITH

SIGNATURE FORGERY DETECTION

Under the able guidance of: Dr. Geetha S

DIGITAL IMAGE PROCESSING

01

Team Members:

SHASHANK VINAYAK BURHADE
20MIS1050

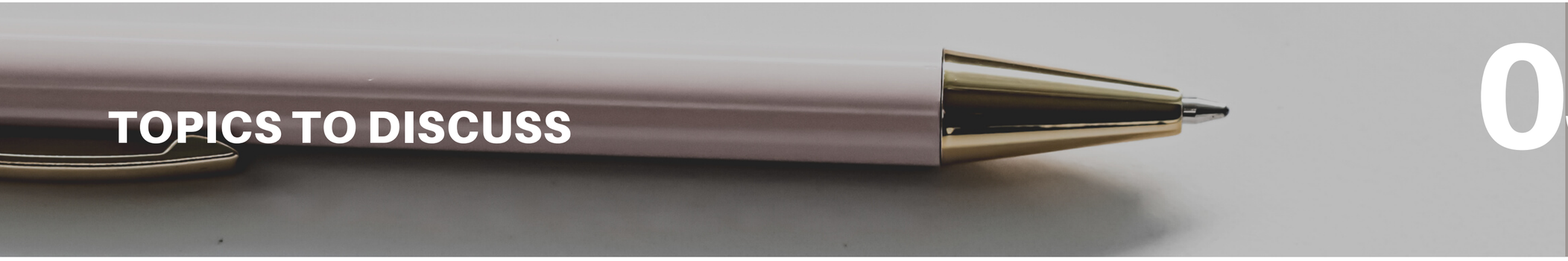
KSHITIJ KIRAN THAKARE
20MIS1136

SONI SINGH
20MIS1136

RAJVEER KALSI
20MIS1161

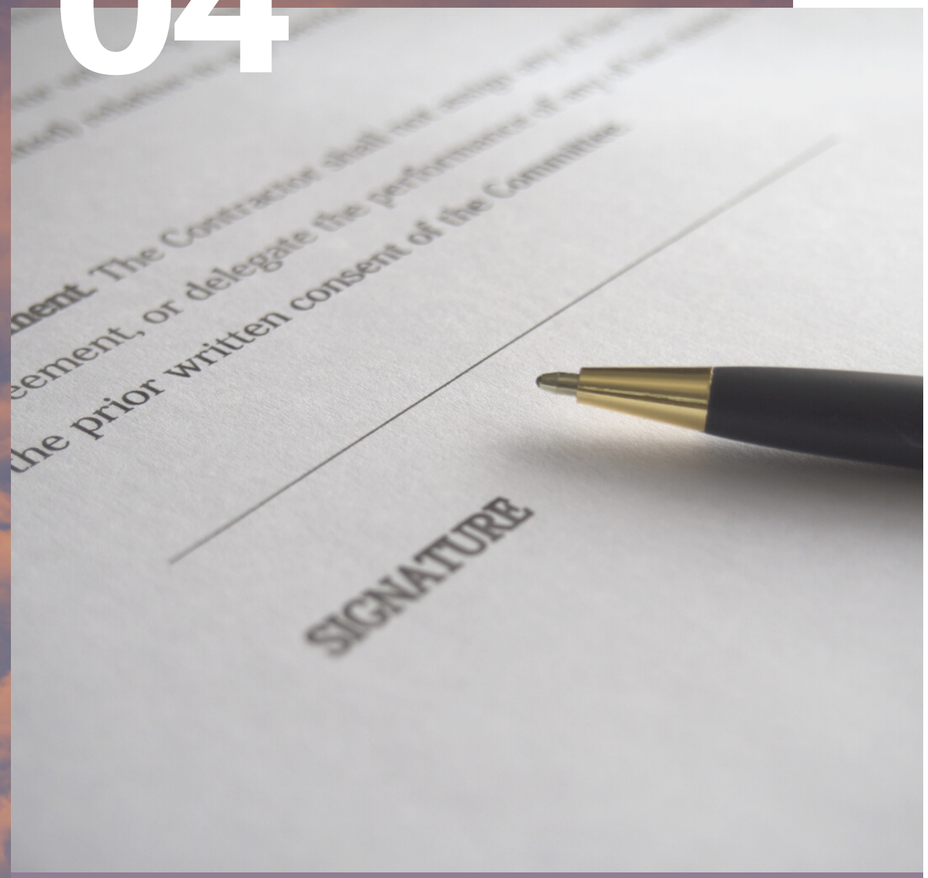
Today's Presentation

- Abstract
- Abstract
- Literature Survey
- Methodology
- DataSet
- Methodolgy
- Future
- Software and hardware used
- Result
- References
- Conclusion
- Contributions



TOPICS TO DISCUSS

04



DIGITAL IMAGE PROCESSING

ABSTRACT

Signature is the most commonly used tool for identification of individuals as personal verification in financial institutions. Even in the digital age, people still use their signatures as a primary form of authentication for a range of transactions. Their signatures authorise checks, new account paperwork, loan documents, and more, and to minimise the risk of fraud, financial institutions need the right solutions to detect forgeries quickly and accurately. Therefore, the need for authentication increases rapidly for various security purposes.

ABSTRACT

In our project, we are planning to implement offline verification of signatures by using different geometric measures. If the absolute difference between the geometric parameters of original signature and the verification signature is greater than a predefined threshold then the signature would be identified as forgery. We aim to develop an efficient system for signature verification and forgery detection based on image processing techniques using python libraries like TensorFlow. A solution is presented where the model is trained with a dataset of signatures, and predictions are made as to whether a provided signature is genuine or forged.

LITERATURE SURVEY

S.no	Paper name and authors	Summary
1)	Handwritten signature forgery detection using convolutional neural networks JeromeGideon,AnuragKandulna,Aron AbhishekKujur,A Diana,Kumudha Raimond	In this paper, a solution based on Convolutional Neural Network (CNN) is presented where the model is trained with a dataset of signatures, and predictions are made as to whether a provided signature is genuine or forged.
2)	Off-line signature verification and forgery detection using fuzzy modeling Madasu Hanmandlua Mohd. ,Hafizuddin Mohd.Yusof,Vamsi KrishnaMadasu	This paper proposes a novel approach to the problem of automatic off-line signature verification and forgery detection. The proposed approach is based on fuzzy modeling that employs the Takagi–Sugeno (TS) model.

LITERATURE SURVEY

3)	Improving the security of arbitrated quantum signature against the forgery attack Ke-Jia Zhang, Wei-Wei Zhang & Dan Li	As a feasible model for signing quantum messages, some cryptanalysis and improvement of arbitrated quantum signature (AQS) have received a great deal of attentions in recent years. However, in this paper we find the previous improvement is not suitable implemented in some typical AQS protocols in the sense that the receiver, Bob, can forge a valid signature under known message attack.

LITERATURE SURVEY

4)	Dynamic signature forgery and signature strength perception assessment S Elloit and A Hunt	Dynamic signature verification has many challenges associated with the creation of the impostor dataset. The literature discusses several ways of determining the impostor signature provider, but this takes a different approach - that of the opportunistic forger and his or her relationship to the genuine signature holder. This examines the accuracy with which an opportunistic forger assesses the various traits of the genuine signature, and whether the genuine signature holder believes that his or her signature is easy to forge.

LITERATURE SURVEY

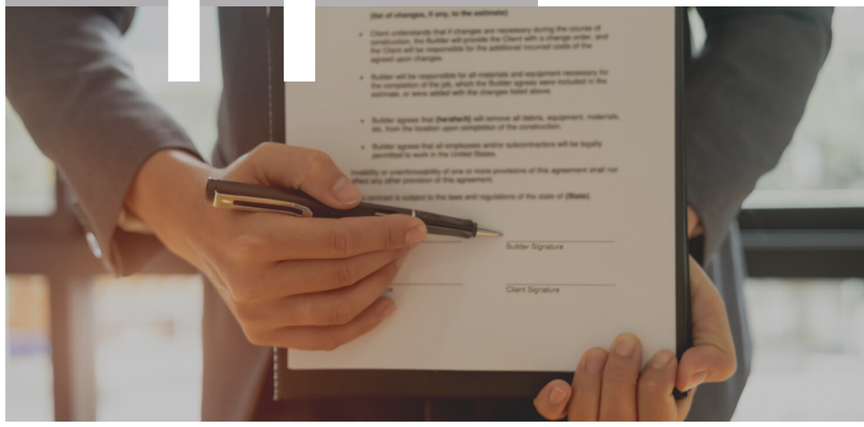
5)	Forgery I—Simulation JFSOAD	The study shows that the simulators concentrate on the more eye-catching characteristics, neglecting the inconspicuous—and very often fundamental and therefore more useful—diagnostic features of handwriting. The experiment confirms the empirical information contained in authoritative texts of handwriting examination.
6)	Parameterization of a forgery handwritten signature verification system using SVM L.E. Martinez; C.M. Travieso; J.B. Alonso; M.A. Ferrer	A new method for off-line handwritten signature verification is described in this paper. It is compared with four different parameterization techniques using support vector machines (SVM) as a classification system. The results show which one is the most suitable parameterization technique for this system.

LITERATURE SURVEY

7)	An Automatic Off-Line Signature Verification and Forgery Detection System Vamsi Krishna Madasu, Brian C. Lovell	This paper presents an off-line signature verification and forgery detection system based on fuzzy modeling. The various handwritten signature characteristics and features are first studied and encapsulated to devise a robust verification system. The verification of genuine signatures and detection of forgeries is achieved via angle features extracted using a grid method. The derived features are fuzzified by an exponential membership
		function, which is modified to include two structural parameters.The structural parameters are devised to take account of possible variations due to handwriting styles and to reflect other factors affecting the scripting of a signature.

LITERATURE SURVEY

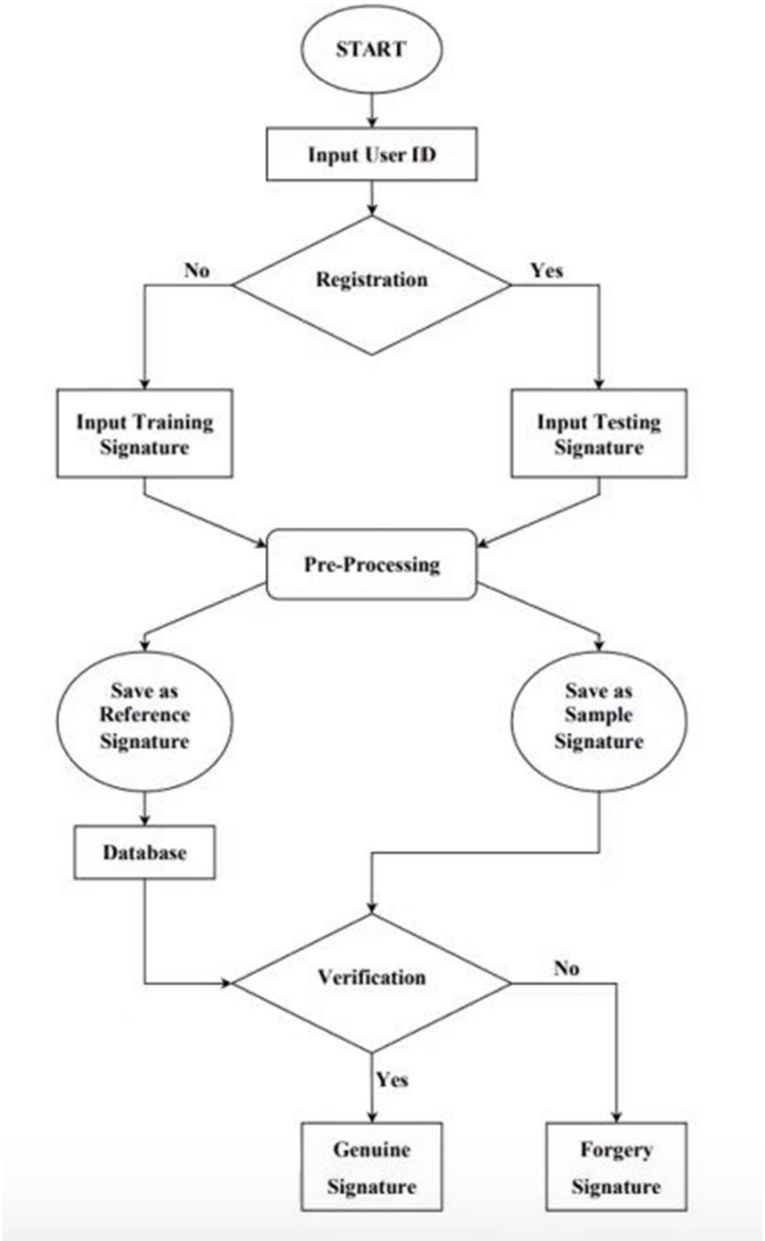
8)	An Online Signature Verification System for Forgery and Disguise Detection Abdelâali HassaïneSomaya Al-Maadeed	In this paper, they have proposed a new system for online signature verification for both forgeries and disguised signatures. This system extract features from both the questioned and the reference signature. The combination of the features is performed using several classifiers and achieves high performances on several signature databases.
9)	Offline Signature Verification using Artificial Neural Network Dhvani Patel, Nehal Ghosalkar, Aruna Pavate	This report focuses on offline signature verification, characterized by the usage of static images of signatures and an artificial neural network based Back-propagation Algorithm. It decides whether the signature is forged or not, and it allow the signature verification persons to take part in the deciding Process. The only drawback of this method is that it is time Consuming.



LITERATURE SURVEY

10)	Signature Forgery Recognition Using CNN Amit Chaurasia,Harsh Agarwal,Ankur Vishwakarma,Ashish Dwivedi,Arpit Sharma	This paper presents the recognition of handwritten signatures. A methodology for offline signature authentication actually utilizes a number of simple geometric highlights based on form. The highlights that are considered are area, eccentricity, center of gravity, pressure, pen up/down, and inclination. Before extricating the highlights, preprocessing of a filtered picture is important to detach the marked part and to expel any fake commotion present.

METHODOLOGY



14

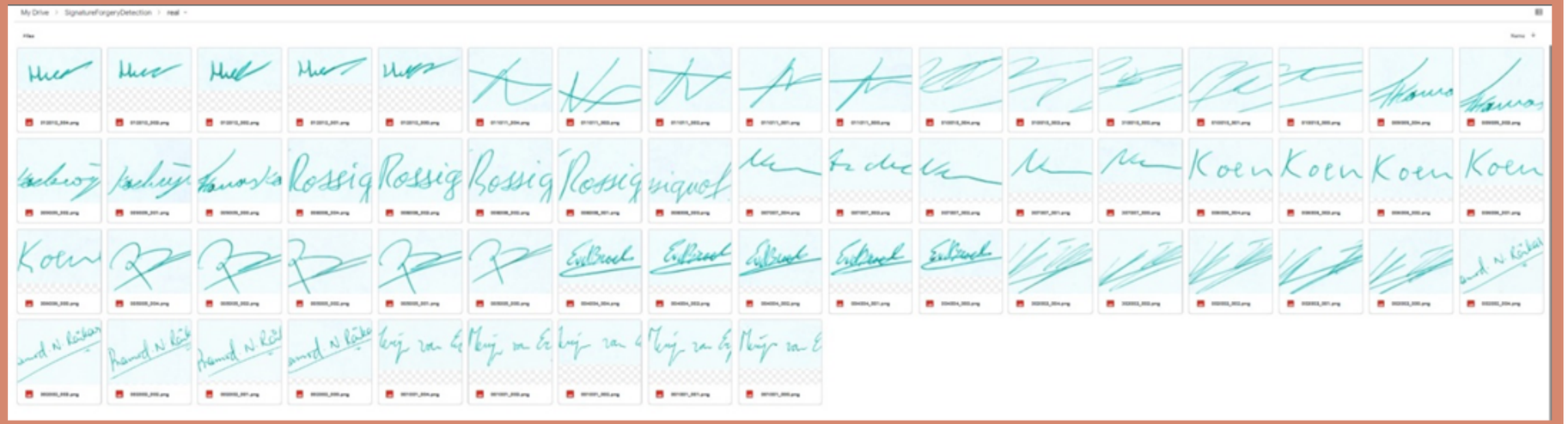
METHODOLOGY

- This signature verification system is started with the input of the User ID.
- The user is required to key in his/her ID to the system. Here, the system will decide whether the user ID is registered or not. If the user ID is not registered, the user has to drop down 5 sets of signatures for training purposes. The signature will then proceed to pre processing and feature extraction stage.
- After this stage, the input training signature will be saved as reference signature in the database.
- If the user ID is registered, the user will then be asked to sign for testing. Then, the input testing signature will proceed to the Pre-processing stage.

METHODOLOGY

- After this stage, the input testing signature will be saved as sample signature and proceed to the verification stage.
- In the Verification stage, the sample signature will be compared with the reference signature which is stored in the database.
- If the difference between two signatures does not exceed the Threshold value, the sample signature will be accepted as genuine signature and vice versa.

DATASET



ORIGINAL SIGNATURE

The user will import 5 signatures of his original signature to train the system.

DATASET

FORGED SIGNATURE

The incorrect Signature

SOFTWARE AND HARDWARE USED

SOFTWARE IS USED-GOOGLE COLLABORATORY

Colaboratory, or “Colab” for short, is a product from Google Research. Colab allows anybody to write and execute arbitrary python code through the browser, and is especially well suited to machine learning, data analysis and education. More technically, Colab is a hosted Jupyter notebook service that requires no setup to use, while providing access free of charge to computing resources including GPUs.

SOFTWARE AND HARDWARE USED

HARDWARE USED:

Parameter	Google Colab	Kaggle Kernel
CPU Model Name	Intel(R) Xeon(R)	Intel(R) Xeon(R)
CPU Freq.	2.30GHz	2.30GHz
No. CPU Cores	2	4
CPU Family	Haswell	Haswell
Available RAM	12GB (upgradable to 26.75GB)	16GB
Disk Space	25GB	5GB

RESULT

INPUT 1: (REAL SIGNATURE)

OUTPUT:
(DISPLAYS RESULT AS GENUINE IMAGE)

```
        print("Training average-", train_avg/n)
        print("Testing average-", test_avg/n)
        print("Time taken-", time()-start)
    return train_avg/n, test_avg/n, (time()-start)/n


evaluate(train_path, test_path, type2=True)
```

```
Enter person's id : 002
Enter path of signature image : /content/012012_002.png
Genuine Image
True
```


RESULT

INPUT 2: (FORGED SIGNATURE)

```
[28]            test_avg += test_score
            if display:
        #         print("Number of neurons in Hidden layer-", n_hidden_1)
                print("Training average-", train_avg/n)
                print("Testing average-", test_avg/n)
                print("Time taken-", time()-start)
            return train_avg/n, test_avg/n, (time()-start)/n



        evaluate(train_path, test_path, type2=True)
```

```
Enter person's id : 002
Enter path of signature image : /content/021012_002.png
Forged Image
False
```


CONCLUSION

In this project we implemented offline verification of signatures by using different geometric measures. We developed an efficient system for signature verification and forgery detection based on image processing techniques using python libraries like TensorFlow. A solution is presented where the model is trained with a dataset of signatures, and predictions are made as to whether a provided signature is genuine or forged. As a result, we were able to distinguish between genuine and forged handwritten documents using pre-processing, feature extraction, and training the model with genuine and forged image datasets.

FUTURE

This project will help provide financial institutions the right solutions to detect forgeries quickly and accurately. The planned system is highly economical in recognizing and sleuthing the forgeries at runtime and therefore the responsibility of the system can be magnified by training the extracted features on the Artificial Neural Networks by storing the extracted features. Negligible misclassification or error is required in such sensitive applications although it’s at the cost of a High Recognition Rate (HRR). Different aim is that the probability chance of forgery signature as if it’s a real one is zero. As a future work, we may also aim at increasing the resultant system accuracy by trying new and better parameter coefficients that increases the deviation between real and forged signatures.

REFERENCES

1.S Jerome Gideon, Anurag Kandulna, Aron Abhishek Kujur, A Diana, Kumudha Raimond,Handwritten Signature Forgery Detection using Convolutional Neural Networks,Procedia Computer Science,Volume 143,2018,Pages 978-987,ISSN 1877-0509.

2.Madasu Hanmandlu, Mohd. Hafizuddin Mohd. Yusof, Vamsi Krishna Madasu,Off-line signature verification and forgery detection using fuzzy modeling,Pattern Recognition,Volume 38, Issue 3,2005,Pages 341-356,ISSN 0031-3203,

3.Zhang, KJ., Zhang, WW. & Li, D. Improving the security of arbitrated quantum signature against the forgery attack. *Quantum Inf Process* 12, 2655–2669 (2013).

4.S. Elliott and A. Hunt, "Dynamic signature forgery and signature strength perception assessment," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 6, pp. 13-18, June 2008, doi: 10.1109/MAES.2008.4558003.

5.Journal of Forensic Sciences, Vol. , No. , 1993, pp. -, https://doi.org/. ISSN

REFERENCES

6.L. E. Martinez, C. M. Travieso, J. B. Alonso and M. A. Ferrer, "Parameterization of a forgery handwritten signature verification system using SVM," *38th Annual 2004 International Carnahan Conference on Security Technology, 2004.*, 2004, pp. 193-196, doi: 10.1109/CCST.2004.1405391.

7.Vamsi Krishna Madasu (Queensland University of Technology, Australia) and Brian C. Lovell (NICTA Limited (Queensland Laboratory) and University of Queensland, Australia

8.Hassaïne A., Al-Maadeed S. (2012) An Online Signature Verification System for Forgery and Disguise Detection. In: Huang T., Zeng Z., Li C., Leung C.S. (eds) Neural Information Processing. ICONIP 2012. Lecture Notes in Computer Science, vol 7666. Springer, Berlin, Heidelberg.

REFERENCES

9. Dhvani Patel, Nehal Ghosalkar, Aruna Pavate, 2017, Offline Signature Verification using Artificial Neural Network, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICIATE – 2017 (Volume 5 – Issue 01),

10. Chaurasia A., Agarwal H., Vishwakarma A., Dwivedi A., Sharma A. (2021) Signature Forgery Recognition Using CNN. In: Ranganathan G., Chen J., Rocha Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 145. Springer, Singapore.

Contribution

SHASHANK VINAYAK BURHADE
Coding and Implementation

KSHITIJ KIRAN THAKARE
Data Set Collection

SONI SINGH
Data Set Collection

RAJVEER KALSI
Coding and Implementation

Something to Think About

“Uniqueness is like a signature, nobody can forge it's exact copy.”

THANK YOU