Signature verification using image processing

U Sai Kiran Reddy, Pamanji thanooj,prof:DR P.Nirmala
ECE, Vellore Institute of technology, Chennai

***Abstract*-** Signature verification is a crucial aspect of various applications, including authentication and personal identification. The primary goal of this project is to use a number of image processing techniques to construct a signature verification system in MATLAB. The project includes the following techniques: setting up a database, specifying a scanner, filtering, binarization, turning a grayscale image into a binary image, cropping, thinning, skeletonizing, rotating for skew correction, resizing, and examining the aspect ratio, horizontal center, and vertical center of the signature. In a variety of applications, including banking, legal documents, and personal identification, the developed system provides a useful tool for automating the process of signature verification, boosting security, and guaranteeing trustworthy authentication.

I. INTRODUCTION

A specific case of pattern reorganization is offline signature verification. A person's identity is frequently verified using biometric technology for legal and administrative purposes. They are frequently designed as Pattern Recognition systems, where biometric information about a person is collected, stored, and used as a "template" for comparisons in the future or to train a classifier that can determine whether new samples belong to this user. They can be used to automatically verify the signature on bank cheques and other documents. The goal of the offline signature verification system is to determine whether a given signature is valid or invalid and whether it is related to the user or not. The verification of a person's signature is a biometric verification, which is a significant area of research aimed at automatic identification verification in settings including law, finance, and high security. Online and offline signature verification can be categorized into two groups. An electronic tablet and pen are used in an online method. The phrase "digital image" describes how a digital computer transforms a two-dimensional image. It denotes digital processing of any two-dimensional data in a larger context. An array of real or complex integers represented by a finite number of bits makes up a digital image. An image that has been provided as a transparency, slide, photograph, or X-ray is first digitized and stored in computer memory as a matrix of binary numbers. A high-definition television monitor can then be used to process and/or display this digitized image. To provide a visually continuous display, the image is kept in a rapid-access buffer memory for display, which refreshes the monitor at a rate of 25 frames per second.

[II] LITERATURE REVIEW:

1.HANDWRITTEN SIGNATURE IDENTIFICATION USING BASIC CONCEPTS OF GRAPH THEORY

The purpose of this study is to outline a novel promising technique in handwritten signature identification based on certain fundamental ideas of graph theory and to discuss past work in the field of signature and writer identification to highlight the historical development of the notion. Both online and offline handwritten signature recognition systems can use this idea.

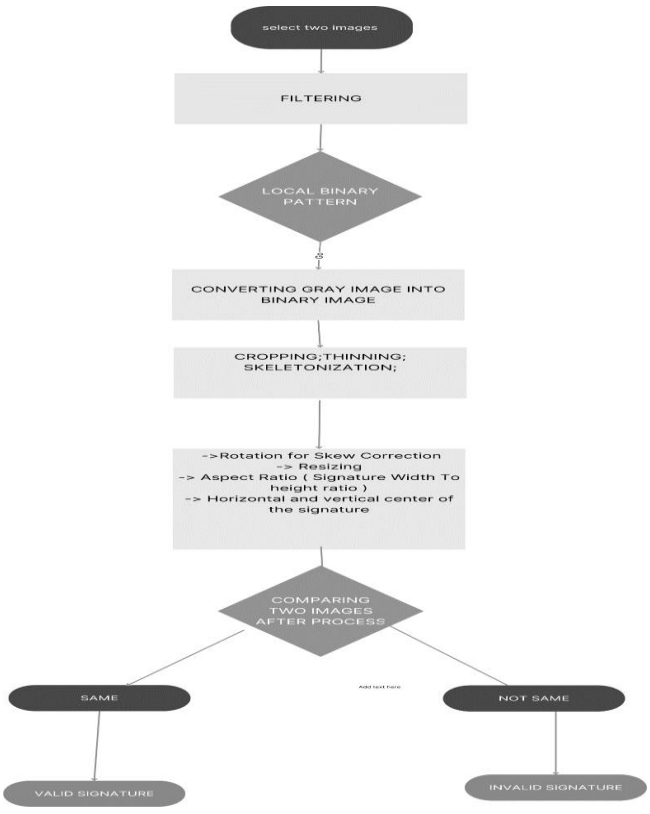
2.OFFLINE SIGNATURE VERIFICATION USING LOCAL INTEREST POINTS AND DESCRIPTORS

This paper proposes a novel method for offline signature verification based on a large baseline general-purpose matching mechanism. The proposed approach detects local interest points in the signature images rather than matching geometric, signature-dependent features as is typically done. Next, local descriptors are computed in the vicinity of these points, and finally, these descriptors are compared using local and global matching procedures.

3.OFFLINE SIGNATURE VERIFICATION USING DTW

In this research, they suggest a Dynamic Time Warping (DTW)-based signature verification system. The technique compares reference and probe feature templates using elastic matching after extracting the vertical projection feature from signature images. The fundamental DTW method is modified to consider the stability of the different parts of a signature.

[III] PROPOSED TECHNIQUE:
(SYSTEM ARCHITECHTURE)



[IV] METHODOLOGY: The rapid advancement in technology has led to the increased demand for secure and reliable authentication systems. Signature verification is one such area where automated methods can play a vital role in ensuring document integrity and personal identification. In this project, we propose a comprehensive approach for signature verification using MATLAB, encompassing various methods for accurate and efficient analysis.

[1] The project begins with **database preparation,** where a diverse collection of signature samples is acquired and organized for training and testing purposes.

[2] The **scanner specification** is crucial for capturing high quality signature images, and parameters such as resolution, colour depth, and sampling rate are considered to ensure optimal results.

[3] filtering techniques to enhance the quality of signature images, are employed to remove noise and improve clarity.

[4] Binarization, is then performed to convert grayscale images into binary images, simplifying subsequent processing steps. The conversion process considers the thresholding technique best suited for signature analysis. **LOCAL BINARY PATTERN,** LBP features compute co-occurrence of pixel values in predetermined neighbourhoods. LBP method is commonly used in object recognition with good success, and we expected it also to be useful in offline signature verification.

[5] Cropping techniques are applied to isolate the signature region of interest, ensuring precise analysis and minimizing computational complexity.

[6] Thinning and **skeletonization** algorithms are employed to reduce the signature stroke width and extract the skeleton structure, respectively. These steps help in capturing the essential features of the signature while reducing computational overhead

[7] To compensate for skew, **rotation techniques** are applied to correct any angular misalignment present in the signature images.

[8] Resizing operations are then carried out to standardize the signature dimensions for consistent analysis.
Finally,

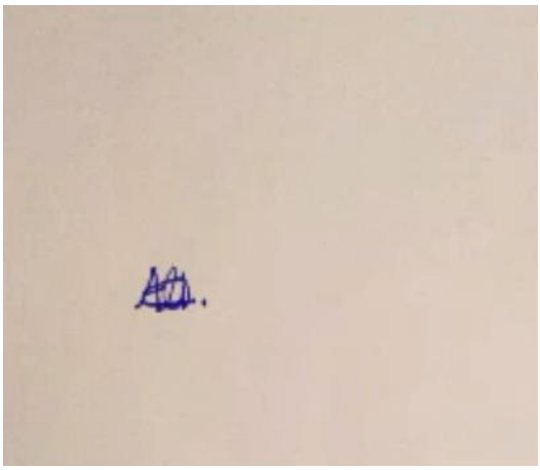
[**9] the horizontal and vertical** centres of the signature are determined to evaluate the position and balance of the signature within the image. These measures aid in distinguishing genuine signatures from forgeries based on their spatial distribution
The proposed approach combines these methods into a robust and efficient system for signature verification. Extensive experimentation and analysis demonstrate the effectiveness and accuracy of the approach, showcasing its potential for real world applications in document verification, financial transactions, and personal identification systems.

[v] EXPERIMENTAL RESULTS AND ANALYSIS:

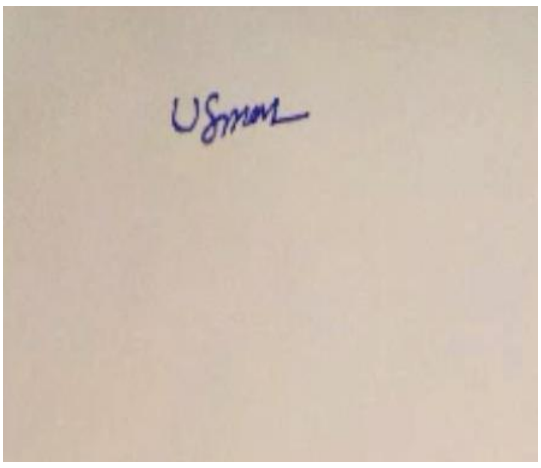
So first we will take data which is of two different images for verifying so when we give input image one and input image 2 , it will perform all these methods which is proposed and then it gives result if both the signatures are same then it tells valid for signature verification if we give two different images it says invalid for signature verification.

Our data signatures of two persons:

Signature:



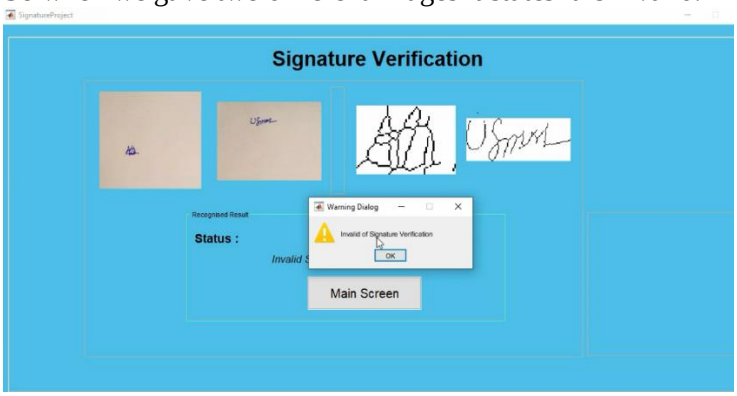
Signature:



Then we will give the data from our folder

Then we click on the result it will automatically do all analysis and give final outputs and gives correct statement.

So when we gave two different images it states it is invalid.



And when we gave same it states valid

IV. CONCLUSION

In conclusion, the research paper on "Signature Verification by Image Processing using MATLAB" explores various methods and techniques to authenticate signatures through image processing. The paper focuses on the following steps: Database Preparation, Scanner Specification, Filtering, Binarization, Conversion of Gray level image into binary image, Cropping, Thinning, Skeletonization, Rotation for Skew Correction, Resizing, Aspect Ratio (Signature Width to Height Ratio), and Horizontal and Vertical Center of the Signature. Overall, this research paper demonstrates the effectiveness of image processing techniques in signature verification. The combination of these methods allows for accurate and reliable authentication of signatures, making it a valuable contribution to the field of biometric identification and security.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” Circuits and Systems for Video Technology

[2] B. Biggio, g. fumera, P. Russu, L. Didaci, and F. Roli, “Adversarial Biometric Recognition A review on biometric system security from the adversarial machine- learning perspective,”

[3] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and Harnessing Adversarial Examples,” in International Conference on Learning Representations, 2015.

[4] F. Tram`er, A. Kurakin, N. Papernot, D. Boneh, and P. McDaniel, “Ensemble Adversarial Training: Attacks and Defenses,” in International Conference on Learning Representations, 2018.

[5] “Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods,” in Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, 2017.

[6] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, “Can machine learning be secure?” in Proceedings of the 2006 ACM Symposium on Information, computer and communications security.

[7] B. Biggio, G. Fumera, and F. Roli, “Security evaluation of pattern classifiers under attack, 2014.

[8] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” EURASIP J. Adv. Signal Process, 2008.

[9] N. K. Ratha, J. H. Connell, and R. M. Bolle, “An analysis of minutiae matching strength,” in International Conference on Audio-and Video- Based Biometric Person Authentication. Springer, 2001.

[10] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” in International Conference on Learning Representations, 2014.

[11] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, “Distillation as a defense to adversarial perturbations against deep neural networks,” in Security and Privacy, IEEE Symposium on. IEEE, 2016.

[12] N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017.

[13] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, “Towards Deep Learning Models Resistant to Adversarial Attacks,” International Conference on Learning Representations, 2018.

[14] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, “The security of machine learning,” 2010.

[15] B. Biggio and F. Roli, “Wild patterns: Ten years after the rise of adversarial machine learning,” 2018.

AUTHORS

First Author – Pamanji Thamooj, BTECH,3RD YEAR, ECE, VIT CHENNAI,thanoojpamanji@gmail.com

Second Author –U.SAI KIRAN REDDY, BTECH,3RD YEAR, ECE, VIT CHENNAI,saikiranreddy@gmail.com