Handwritten Signature Verification

N. Ganitha Aarthi[1], Mrs. Parvathi R[2]

Assistant Professor, Department of Computer Science and Design, SNS College of Engineering(Autonomous), Coimbatore, India. arthi.ganitha@gmail.com

Karishma S [3], Bhackya bharathi M[4], Keerthana S[5], Narayanan C P [6]

UG Students - Department of Computer Science and Design, SNS College of Engineering(Autonomous), Coimbatore, India.

Abstract Handwritten signatures have been a traditional method for personal authentication and authorization in various fields. With the increasing reliance on digital transactions and the prevalence of electronic documents, there is a growing need for robust and secure methods to verify handwritten signatures. This research explores the application of deep learning techniques for the automatic verification of handwritten signatures. The proposed system leverages convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to extract and learn distinctive features from handwritten signature images. The model is trained on a diverse dataset of genuine and forged signatures to develop a robust and accurate signature verification system. The deep learning model adapts to the unique characteristics of each individual's signature, providing a personalized and secure authentication process. The evaluation of the system involves testing its performance on various datasets, considering factors such as signature variability, different writing styles, and potential adversarial attacks. The results demonstrate the effectiveness and reliability of the proposed deep learning approach in accurately verifying handwritten signatures, outperforming traditional signature verification methods. The implementation of this research has the potential to enhance security in digital transactions, document authentication, and access control systems. The utilization of deep learning for handwritten signature verification not only improves accuracy but also offers a scalable and adaptable solution to meet the evolving demands of a technologically advancing society.

Keyword- convolutional neural networks, signature, adversarial attacks, handwritten signatures, authentication, demands.

I. INTRODUCTION

Nowadays, with everyone's life moving so quickly, nobody has time to stand in line for lengthy banking procedures. For this reason, a large number of people use ATMs. An ATM is now the central component of the banking system because to its 24/7 self-banking service. An ATM can be used to pay for a variety of household bills, such as those related to energy, water, and phone use, as well as to withdraw cash, pay with a credit or debit card, and transfer money between accounts. We may now complete all of our banking duties quickly and easily with the help of ATMs (Automatic Teller Machines). The number of fraudulent assaults against ATM has been rising daily in tandem with the growing use of these machines. The current ATM paradigm involves an ATM/debit card, credit card, or both, together with a PIN. This leads to a growth in assaults via stolen cards, PINs that are statically assigned, card duplication, and other risks. After the card number, expiration date, owner name, and PIN are verified, an ATM or debit card can be used to authenticate a person. But what happens if the card is lost or stolen, or if someone not authorized knows the PIN? We need a better level of security for this, which is why the idea to incorporate biometric and one-time password (OTP) into the current technology was developed. Biometric authentication methods include facial recognition, fingerprint recognition, retinal recognition, iris recognition, and more. Although they may also incorporate additional features like iris or face recognition, palm or finger vein print biometrics are the most commonly utilized biometric measurements. However, the technique that we are recommending here is based on the fingerprint recognition mechanism. Authentication with biometric technologies is safe and unchallengeable. People's fingerprints are initially recorded in the database using their mobile fingerprints here. There are four switches that we employ to record each person's fingerprint. It is shown on the 16x2 LCD display whether or not a person is permitted. The fingerprint module will identify each person's fingerprint and communicate this

 DOI : 10.35291/2454-9150.2024.0077

information to the Arduino, which will then send a signal to the GSM module. when a user inserts their finger into the fingerprint scanner and the fingerprint is compared to the database. The user will receive an OTP in his or her predetermined or registered number through the GSM module if the fingerprint detection matches the user's pre-saved fingerprint database. The OTP will be typed by the user on the keypad. Only the user will be able to access the transaction if their fingerprint and OTP match those in the database. Access won't be allowed and the transaction will fail if the user's fingerprint and OTP don't match. Additionally, an alert buzzer will sound, and an LCD message indicating that the person is not permitted will appear.

II. EXISTING SYSTEM

The existing handwritten signature verification systems face limitations in terms of reliability and security. These systems often struggle with forgeries or attempts to replicate signatures, as they may not effectively distinguish between genuine and fraudulent signatures. Additionally, variations in an individual's signature over time can pose challenges for consistency in verification. The reliance on static signature samples may not adequately capture the dynamic nature of a person's signing behavior, making the system susceptible to false positives or negatives. Furthermore, these systems may lack robustness against sophisticated techniques employed by malicious actors to manipulate or deceive the verification process, highlighting the need for more advanced and adaptive authentication methods.

III. PROPOSED IDEA

In ideating a handwritten signature verification system, various methods are considered. Image processing techniques, such as preprocessing for quality enhancement and feature extraction for capturing stroke patterns, play a crucial role. Graph metric analysis focuses on dynamic aspects like signing speed and trajectory, contributing to a behavioral biometric profile. Machine learning and pattern recognition involve supervised and unsupervised learning, while deep learning approaches like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) extract hierarchical and sequential information from signature images. The fusion of static and dynamic features, along with exploring behavioral biometrics like keystroke dynamics, enhances the system's accuracy. Continuous authentication and liveness detection, incorporating real-time monitoring and anti-spoofing measures, contribute to robust security. Additionally, user-centric design, involving feedback mechanisms and adaptive interfaces, aims to optimize the user experience and address usability concerns, ensuring a comprehensive and effective handwritten signature verification solution.

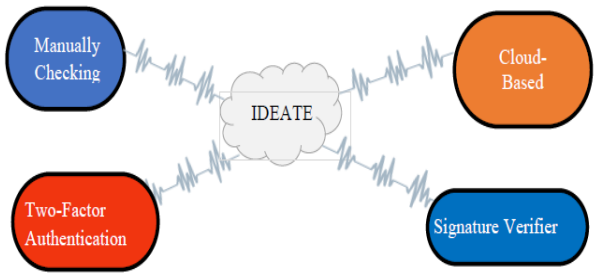

Fig 1; Proposed idea block diagram

This project involves using a machine learning model, specifically a Convolutional Neural Network (CNN), to learn and distinguish between genuine and forged signatures. The model is trained on a dataset of labeled signature images, and the features extracted from these images contribute to the learning process. The trained model is then used for real-time signature verification by comparing the input signature against the learned patterns. Please note that the actual implementation details, such as the architecture of the CNN, specific preprocessing techniques, and the choice of feature extraction methods, would depend on the characteristics of your dataset and the complexity of the signature verification task.

The Structural Similarity Index (SSIM) is a metric commonly used for image quality assessment, including image comparison in the context of signature verification. It measures the similarity between two images, considering luminance, contrast, and structure. SSIM values range from -1 to with 1 indicating perfect similarity.

IV. METHODOLOGY

Definition of SSIM:

SSIM measures the structural similarity between two images by comparing luminance, contrast, and structure. It produces a value between -1 and 1, where 1 indicates perfect similarity.

Reference Signature and Test Signature:

Assume you have a reference signature (genuine) and a test signature (to be verified).

Preprocessing:

Preprocess the signature images. This may include converting them to grayscale, resizing, and normalizing pixel values.

SSIM Calculation:

Apply the SSIM algorithm to calculate the similarity index between the reference and test Signatures. The SSIM algorithm compares local patterns of pixel intensities in the images and computes the similarity index based on luminance, contrast, and structure.

Thresholding:

Establish a threshold for the SSIM value. Signatures with SSIM values above the threshold are considered genuine,

 DOI : 10.35291/2454-9150.2024.0077

while those below are classified as forgeries. The threshold can be adjusted based on the desired balance between false positives and false negatives.

Integration with the Verification System:

Integrate the SSIM calculation into the larger signature verification system. This can be part of a decision-making process where the SSIM value contributes to the overall decision on the authenticity of the signature.

In this signature verification project, the initial phase involves training a Convolutional Neural Network (CNN) using a dataset of both genuine and forged signatures. The trained and tested images are organized into separate training and testing folders. When a user provides the input image path and name for verification, the system initiates a step-by-step process using the trained CNN. The first stage is image pre-processing, involving binarization and segmentation to simplify and isolate the signature from the background. The resulting extracted image is then utilized to train the classifier. to determine the authenticity of provided signatures

V. RESULT AND DISCUSSIONS

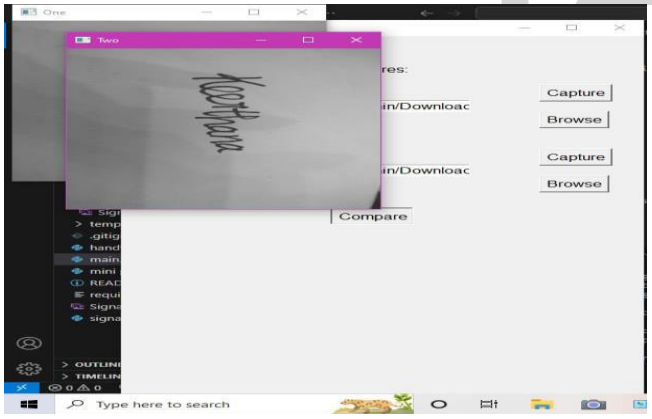

Fig 2 ; Screenshot test1

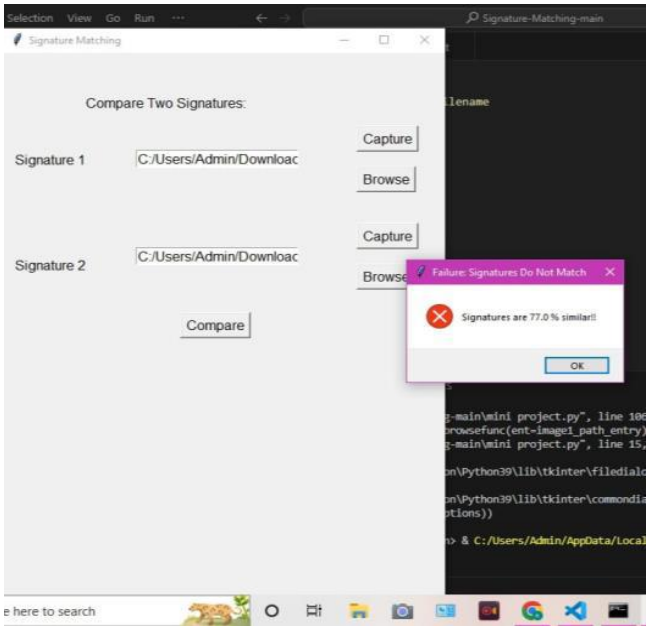

Fig 3; Screenshot test 2

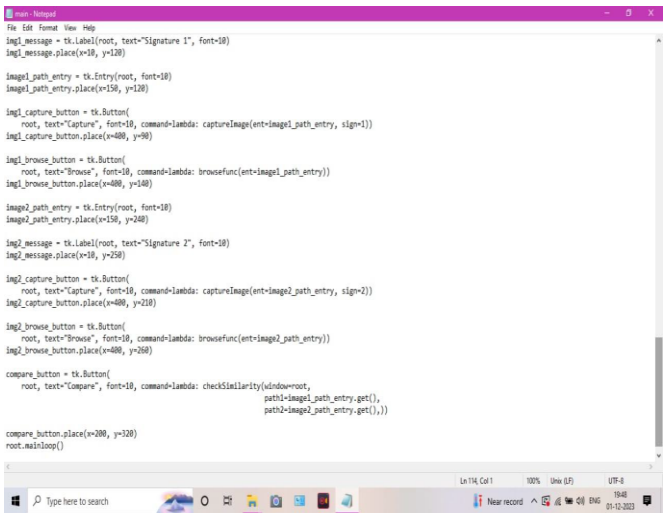

Fig 4; Screen shot (Real-Time Detection code)

Data Testing

In the signature verification project, testing is performed by using a separate dataset not seen during training. Images in this test set undergo the same pre-processing steps, such as binarization and segmentation. The trained Convolutional Neural Network (CNN) then predicts whether each signature is genuine or fraudulent. Performance metrics, including accuracy and precision, assess the model's ability to generalize to new data. If needed, adjustments are made to improve the model's performance through iterative refinement. In real-world scenarios, users can input their own signatures for verification, subject to the same pre-processing and testing steps to determine authenticity.

Real-time testing

In real-time testing for the signature verification project, user-inputted signatures undergo immediate pre-processing and are assessed by the trained Convolutional Neural Network (CNN) for authenticity. This process ensures swift and accurate verification, offering users real-time feedback on the genuineness of their provided

VI. CONCLUSION

In this project, we provide a straightforward method for offline signature verification, in which the signature is written on paper and converted to an image format or taken using a tablet or mobile device. Pre-processing on input, one of the main goals of Mat-lab toolboxes, is successfully accomplished to obtain the final, updated input. The second is based on deep learning and uses soft max layer and auto encoders. The application\'s GUI is set up for simple understanding. Through the use of a convolutional neural network (CNN), offline signature verification has been carried out in this study. We can extract more accurate representations of the image content using a neural network model called CNN. For improved categorization, CNN uses the image\'s raw pixel data to train a model before automatically extracting features. The biggest benefit In

 DOI : 10.35291/2454-9150.2024.0077

comparison to its forerunners, it automatically recognizes the crucial details without human supervision and has the best level of image prediction accuracy. The GUI application is used for the uploading, training, and testing of the code using previously submitted data. Offline signature verification is made simple, quick, and clear using this method.

For future enhancements, the signature verification project could benefit from several potential improvements. Incorporating advanced feature extraction techniques, such as deep learning architectures specifically designed for signature analysis, may enhance the model's ability to capture intricate patterns. Additionally, exploring ensemble methods or transfer learning approaches could contribute to increased robustness across diverse signature styles. Continuous expansion of the dataset with a focus on diverse signatures can improve the model's generalization capabilities. Furthermore, integrating user feedback mechanisms and adaptive learning can contribute to a more dynamic and responsive verification system. Embracing emerging technologies and advancements in the field of computer vision could also open avenues for further innovation, ultimately refining the project's accuracy and real-world applicability.

REFERENCES

[1] A.Aditya Shankar, P.R.K.Sastry, A.L.Vishnu ram.A.Vamsidhar Fingerprint Based Door Locking System International Journal of Engineering and Computer Sciences ISSN:2319-7242, Volume 4 Issue 3 March 2015.

[2] Kanak Chopra, garvit Jain Door Opening System Based on Fingerprint Scanning International Journal of Engineering Research Management Technology, March 2015, Volume 2, Issue-2.

[3] Pavithra.B.C, Myna.B.C, Kavyashree.M Fingerprint Based Bank Locker System Using Microcontroller Proceedings of IRF International Conference, 5 April-2014, Pondicherry, India, ISBN: 978-93-82702-71-9.

[4]M.Gayathri, P.Selvakumari, R.Brindha Fingerprint and GSM based Security System International Journal of Engineering Sciences Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[5] Sagar S. Palsodkar, Prof S.B Patil Biometric and GSM Based Security for lockers International Journal of Engineering Research and Application ISSN: 2248-9622, Vol.4, December 2014.

[6] Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM International Journal of Emerging Trends Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March April 2013.

[7] R.Ramani,S.Valarmathy, S. Selvaraju, P.Niranjan Bank Locker Security System based on RFID and GSM Technology International Journal of Computer Applications (09758887) Volume 57 No.18, November 2012 .

[8] Pramila D Kamble and Dr. Bharti W. Gawali Fingerprint Verification of ATM Security System by Using Biometric and Hybridization International Journal of Science and Research Publications, Volume 2, Issue 11, November 2012.

[9] Gyanendra K Verma, Pawan Tripathi, A Digital Security System with Door Lock System Using RFID Technology, International Journal of Computer Applications (IJCA) (0975 8887), Volume 5 No.11, August 2010.

[10] Mary Lourde R and Dushyant Khosla Fingerprint Identi_cation in Biometric Security Systems International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October,2010.

[11] Sagar S. Palsodkar*, Prof S.B. Patil , “Review: Biometric and GSM Security for Lockers” Int. Journal of Engineering Research and Applications , Vol. 4, Issue 12(Part 6), December 2014.

[12] R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan , “Bank Locker Security System based on RFID and GSM Technology ’’, International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012.

[13] Vaijanath R. Shintre, Mukesh D. Patil, “Banking Security System Using PSoC”. International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 7, July 2015.

[14] Tarief.M. F. Elshafiey, "Design and Implementation of a museum and bank security system using antenna as IR proximity sensor and PSoC Technology", IEEE symposium on wireless technology and applications, September 25-28 Malaysia 2011.

[15] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., “Online Ration card System by using RFID and Biometrics”, International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

 DOI : 10.35291/2454-9150.2024.0077