Signature fraud detection using Deep Learning

First Author: Mr. Raja Bhargava, Assistant Professor, Department Of Computer Science & Engineering, Visvodaya Engineering College, Kavali, Nellore District, A.P.

Second Author:

Sk.P.Firoze, Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali.
G.Venkatesh Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali.
V.Sai Nikitha Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali.
Sk.Rehan Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali.

ABSTRACT

Online attacks have advanced significantly in recent years. Two-factor authentication, which is used to protect online banking users, has not evolved at the same pace, meaning that users are not sufficiently protected against these new and advanced attacks. This raises an important question: is it possible to make online activities more secure for the user? More specifically, we want to understand whether it is possible to prevent online attacks by involving the user? Signature verification as compared to traditional handcrafted system, where a forger has access and also attempt to imitate it which is used in commercial scenarios, like bank check payment, business organizations, educational institutions, government sectors, health care industry etc. so the signature verification process is used for human examination of a single known sample. As Signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased. The captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate.

1. INTRODUCTION

Signature verification is the process of using a digital signature algorithm and a public key to verify a digital signature on data. It is a form of identity verification. Banks, intelligence services, and other prestigious institutions employ signature verification to confirm a person's identification. In bank branches and other branch capture, signature comparison is frequently employed. The signature verification software compares a direct signature or a picture of a signature to the recorded signature image. The signature serves as the authority for all legal transactions. Thus, the necessity for signature verification grows. It is distinct for the handwritten signatures to individuals and that cannot be duplicated. In addition to being a well-liked area of research in the fields of pattern recognition and image processing, signature verification also plays a significant role in numerous applications, including access control, security, and privacy. The process of certifying someone based on their handwritten signature is known as signature verification. Systems for verifying signatures come in two varieties [1].

Online Signature Verification System, which records details like pressure, speed, direction, etc. using an electronic device like a tablet. Offline Signature Verification System, in which the

signature is written offline and verified using the image of the signature that has previously been stored. Two distinct methods can be used to verify offline signatures. One involves building models of real and fake signatures for each writer in a process known as writer dependent signature verification. Next, a writer's test signature sample is contrasted with its own training sample. This method's downside is that each new writer must have a model created in order to be confirmed.

Before features are recovered from each of the original scanned signatures, size normalization, binarization, and thinning are used as pre-processing steps. These qualities make up the knowledge base that is later used for authenticating signatures and spotting forgeries. We now provide a quick explanation of the system's several processes for signature verification.

Based on their distinguishing characteristics, handwritten signature forgeries have been divided into different categories [f2]. The following forms of signature forgeries can be generally categorized:

1. Random Forgery - The signer creates a forgery known as "the simple forgery" or "random forgery" by using the victim's name in his own unique manner.

2. Unskilled Forgery - The signer imitates the signature in his own manner without prior experience or knowledge of the spelling.

3. Expert Forgery - Without a doubt, the most challenging forgeries are produced by experienced forgers or professional impostors. Ammar et.al [I0] worked on the detection of competent forgeries in the 1980s. They analyzed the statistics of dark pixels and used them to spot shifts in the writing's overall flow.

2. LITERATURE SURVEY

Comparative research was done by Hansheng Lei and Venu Govindaraju on aspects that are often used. A consistency model is created to measure the distances-based measure by generalizing the already-existing feature-based measure. It was discovered that uniformly re-sampling the sequences does not always improve verification performance and that the simple features, such as X- and Y-coordinates, writing speed, and angle with the X-axis, are among the most consistent and the rate for identifying original signal is 93%.[3]

Dr. Maged and M. M. Fahmy introduced a system for online handwritten signature verification that is based on discrete wavelet transforms (DWT) feature extraction and classification using feed-forward back error neural networks [7]. The signature is validated in the DWT domain to

increase the distinction between a real signature and a fake.A multi-matcher, which matches for the same input biometric signal using several representations and six neural networks, is used to validate signatures. A discussion and comparison of the recognition rates for each of these neural network recognizers is conducted. Twenty authentic signatures and twenty expertly forged signatures are tested on five users of the signature database. The success rate for identifying genuine signatures is 95%.[5]

Christian Gruber et al. put a novel approach to online signature verification using support vector machines that is based on the LCSS kernel function [8]. Here, the length of an LCSS is calculated using a kernel function to compare the two time series. It has been demonstrated that the SVM LCSS can reliably authenticate people with just six real signatures. The similarity assessment of online signature data based on LCSS turned out to be even better than DTW-based methods [9].To validate online signatures, Abhishek Sharma and Suresh Sundaram have introduced a novel model-based

technique called GMM within the DTW framework [10].

For signature matching, they first retrieved the writer dependent statistical characteristics. Then, using a derivation in a warping path-based feature that is useful for verification, the properties of a warping path are studied.A novel approach to online signature verification using support vector machines that is based on the LCSS kernel function was put forth by Christian Gruber, Thiemo Gruber et.al. Here, the length of an LCSS is calculated using a kernel function to compare the two-time series.The kind of characteristics retrieved, the training process, and the classification and verification models employed vary amongst research methods.[8]

Hidden Markov Model (HMM) was presented by J. K. Guoetal.Each point in a handwritten signature's journey was represented by a series of vectors of values. An effective signature verification system might be created using the HMM's specified set of feature vectors. These models were stochastic ones that could take into account both the differences and similarities across patterns. Stochastic matching of the model and the signature was used in HMM. The process of matching was carried out through steps of the probability distribution of the features used in the signatures or the probability used to generate the original signature.[1]

3. PROPOSED SYSTEM

Proposed system suggests a prototype for Handwritten Signature Verification using Machine Learning and Deep Learning and a model which can learn from signatures and make predictions as to whether the signature in question is a forgery or not. This model can be deployed at various government offices where handwritten signatures are used as a means of approval or authentication. Our results demonstrated that the MLP model is an effective and robust method for handwritten signature verification. The proposed model showed superior performance compared to existing models and was robust to variations in input signature features. This suggests that MLP models have great potential in signature verification applications.

MODULES

CAPTURE MODULE

This module designed to load live signature images.

When the module selected, the camera off our device will be activated to capture the image, and read as dataset or test image.

BROWSE MODULE

This module allow the user to browse the images from external sources, ie.., from our device. It will considered as test image or dataset image.

COMPARE MODULE

This module activates the algorithms in system to compare both signature images, and provide the result.

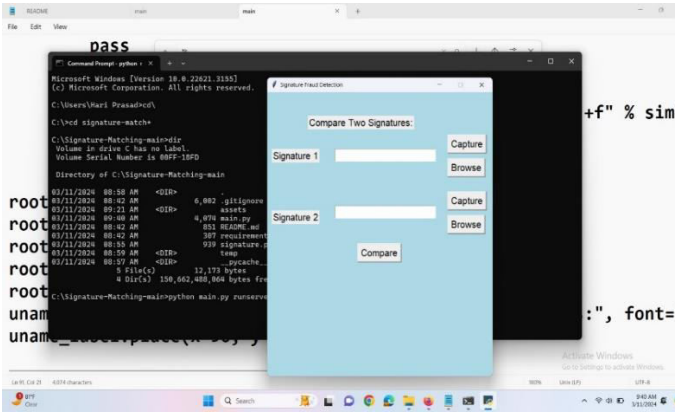
4. CONCLUSION

This method can be implemented in places that require signature authentication and verification, it can be used faster hence processing a large number of signatures and can help save resources and time while detecting forged signatures.

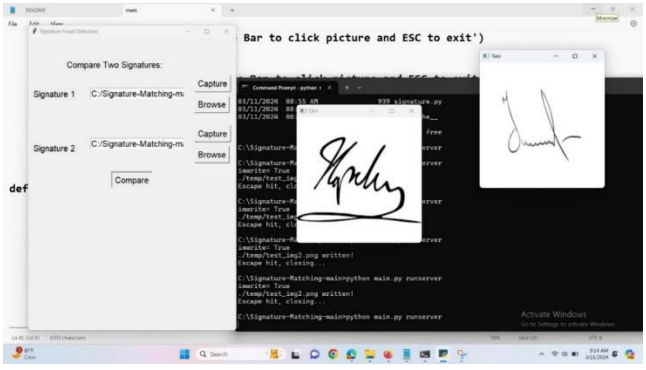
We can detect forged signatures using the mentioned method.

5. RESULT

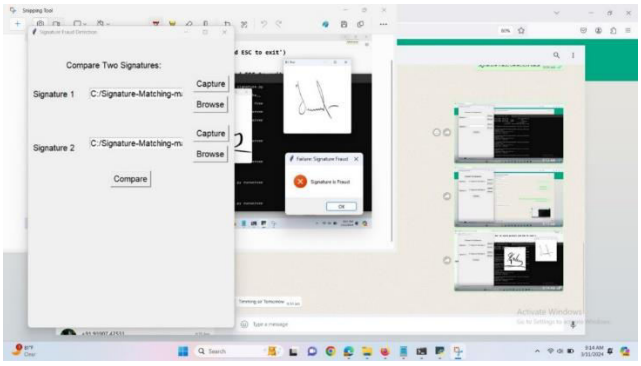
HOME PAGE



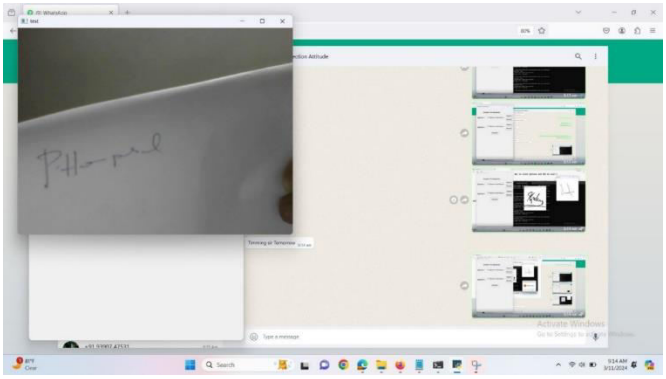
BROWSE TWO SIGNATURES



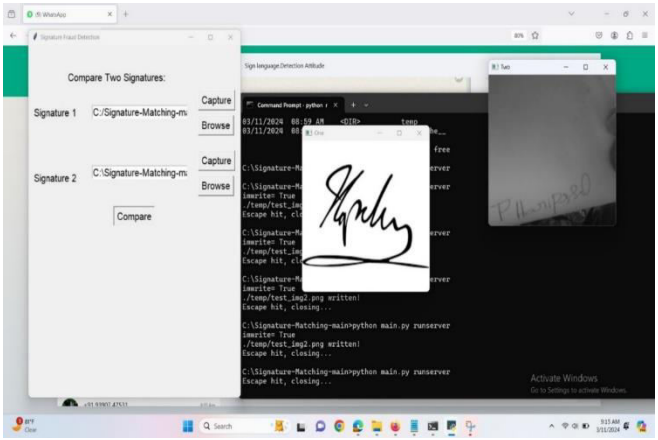
COMPARISION RESULTS



LIVE CAPTURE OF SIGNATURE



MPARING SIGNATURE WITH LIVE CAPTURED SIGNATURE



6. REFERENCES

[1] M. A. Taha and H. M. Ahmed, “Iris features extraction and recognition based on the local binary pattern technique,” in Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA), pp. 16–21, Maysan, Iraq, July 2021.

[2] M. A. Taha and H. M. Ahmed, “A fuzzy vault development based on iris images,” Eureka: Physics and Engineering, no. 5, pp. 3–12, 2021.

[3] V. Iranmanesh, S. M. S. Ahmad, W. A. W. Adnan, S. Yussof, O. A. Arigbabu, and F. L. Malallah, “Online handwritten signature verification using neural network classifier based on principal component analysis,” The Scientific World Journal, vol. 20148 pages, Article ID 381469, 2014.

[4] K. Radhika and S B. Gopika, “Online and offline signature verification: a combined approach,” Procedia Computer Sci- ence, vol. 46, pp. 1593–1600, 2015.

[5] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification — literature review,” in Proceedings of the 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 1–8, Montreal, QC, Canada, November 2017.

[6] H. Nemmour and Y. Chibani, “Off-line signature verification using artificial immune recognition system,” in Proceedings of the 2013 International Conference on Electronics, Computer and Computation (ICECCO), pp. 164–167, Ankara, Turkey, November 2013.

[7] S. Mushtaq and A. Mir, “Signature verification: a study,” in Proceedings of the 4th IEEE International Conference on Computer and Communication Technology, ICCCT, pp. 258– 263, Allahabad, India, September 2013.

[8] A. Kumar and K. Bhatia, “A survey on offline handwritten signature verification system using writer dependent and independent approaches,” in Proceedings of the 2016 2nd International Conference on Advances in Computing, Com- munication, & Automation (ICACCA) (Fall), pp. 1–6, Bareilly, India, September 2016.

[9] R. A. Mohammed, R. M. Nabi, S. M.-R. Mahmood, and

R. M. Nabi, “State-of-the-Art in handwritten signature ver- ification system,” in Proceedings of the 2015 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 519–525, Las Vegas, NV, USA, De- cember 2015.

[10] N. Sharma, S. Gupta, and P. Mehta, “A comprehensive study on offline signature verification,” Journal of Physics: Confer- ence Series, vol. 1969, no. 1, Article ID 012044, 2021.

[11] H A B. Nehal and M. Heba, “signature identification and verification systems: a comparative study on the online and offline techniques,” Future Computing and Informatics Journal, vol. 5, no. 1, 2020.

[12] H. Kaur and M. Kumar, “Signature identifcation and ver- ifcation techniques: state-of-the-art work,” Journal of Ambient Intelligence and Humanized Computing, 2021.

[13] M A S. Hanaa and H. Shrooq, “Eye Detection Using Helmholtz Principle,” Baghdad Sci.J, vol. 16, p. 18, 2019.

[14] H. M. Ahmed and R. T. Rasheed, “A raspberry PI real-time identification system on face recognition,” in Proceedings of the 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA, pp. 89–93, Baghdad, Iraq, July 2020.

[15] H. Mohsin and S. H. Abdullah, “Pupil detection algorithm based on feature extraction for eye gaze,” in Proceedings of the 2017 6th International Conference on Information and Communication Technology and Accessibility (ICTA), pp. 1–4, Muscat, Oman, December 2017.

[16] H. Mohsin and H. Bahjat, “Anti-screenshot keyboard for web-based application using cloaking,” Edited by M. Bouhlel and

S. Rovetta, Eds., in Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Infor- mation and Telecommunications (SETIT’18), vol. vol 146, July 2020.

[17] Y. Zhou, J. Zheng, H. Hu, and Y. Wang, “Handwritten sig-nature verification method based on improved combined features,” Applied Sciences, vol. 11, p. 5867, 2021.

[18] D. Impedovo and G. Pirlo, "Automatic signature verification: the state of the art," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 609–635, Sept. 2008.

[19] M. Saleem and B. Kovari, "Online signature verification based on signer dependent sampling frequency and dynamic time warping," in Proceedings of the 2020 7th International Con- ference on Soft Computing & Machine Intelligence (ISCMI), pp. 182–186, Stockholm, Sweden, November 2020.

[20] M. Fayyaz, M. H. Saffar, M. Sabokrou, M. Hoseini, and

M. Fathy, "Online signature verification based on feature representation," in Proceedings of the 2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP), pp. 211–216, Mashhad, Iran, March 2015.2020.

First Author:

Mr. Raja Bhargava, Assistant Professor, Department Of Computer Science & Engineering, Visvodaya Engineering College, Kavali, Nellore District, A.P.

Second Author:

Sk.P.Firoze, Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali. Nellore District, A.P.

G.Venkatesh Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali. Nellore District, A.P.

V.Sai Nikitha Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali. Nellore District, A.P.

Sk.Rehan Pursuing B.Tech(CSE) from Visvodaya Engineering College, Kavali. Nellore District, A.P.