ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

AI-Based Signature Verification and Authentication System

[1]Sampath Boodidha, [2]Mrs. T.Sai Kumari,

[1]M.Tech Scholar , Dept. of CSE (AI&ML), Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India.

Mail id: somepath2003@gmail.com

[2]Assistant Professor, Dept. of CSE(AI & ML), Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India.

Mail id: thakurkumari0318@gmail.com

Abstract:

Signatures are veritably important in our social and legal life for verification and authentication. A hand can be accepted only if it's from the intended person. The probability of two autographs made by the same person being the same is veritably less. Numerous parcels of the hand may vary indeed when two autographs are made by the same person. So, detecting a phony becomes a grueling task. In this paper, a result grounded on Convolutional Neural Network (CNN) is presented where the model is trained with a dataset of autographs, and prognostications are made as to whether a handed hand is genuine or forged. And also we are using Harris technique for the corner detection step to give better input features to the algorithm of convolutional neural network. Using step signature forgery detection is simple.

Introduction:

Automatic signature verification solutions are in high demand due to the importance of signatures in confirming and authorizing transactions. The values of a handwritten signature differ from one person to another and cannot be reproduced, in contrast to passwords, PINs, PKIs, or key cards—identification that is unforgettable, lost, stolen, or shared data. Validation of signatures by simple, obvious means. Rebuilding faith in technology is as simple as defining it. Signatures have already been accepted as a standard method of ownership confirmation, which is the main advantage of signature verification programs that incorporate some kind of technology. There are a couple of ways this issue has been addressed: online signature verification systems and offline methods. In order to verify the authenticity of a file signature, the Internet connection technique employs a tablet computer and a computer-connected pen, collecting robust details such as pressure, speed, typing speed, etc. In addition to using signature photos captured by a camera or scanner, offline verification also makes use of less electronic control. Features extracted from scanned signature images are utilized by the offline signature verification method. Verifying a signature offline is a breeze with the features employed. Here, it's sufficient to verify every pixel in the image. It is challenging to design many desirable aspects for off-line systems due to the lack of information accessible, such as stroke arrangement, speed, and other dynamical details. Only after removing incompetent features from the following picture signatures should the verification process be carried out. For a number of years, researchers have diligently studied handwriting analysis and pattern matching. A new method is being developed and tested locally to replace Handwritten Signature Verification (HSV), particularly offline HSV. We take a look at a few recent articles about HSV offline here. Researchers' methods vary in terms of the characteristics released, training approach, and validation and separation model employed.

Problem statement:

There is currently no independent technology that can detect if a person's hand is fake, which is a major problem in industries like banking where customers place a premium on customer trust. Working in the area of artificial intelligence for some time has given me the knowledge I needed to tackle this problem using what I've learned before. AI is the branch of computer science that focuses on building intelligent systems and teaching computers to make opinions.

Objective:

Using a convolutional neural network and the harris method, the objective of the study is to identify signature forgeries. Banking systems and commercial applications find these useful. Object recognition in images typically begins with noise reduction and other image processing techniques, then moves on to (low-level) feature extraction to find lines, regions, and maybe even places with certain textures. Imagine a road full of

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

automobiles, a conveyor belt full of items, or cancer cells on a microscope slide as individual objects; the clever part is to treat these groups of forms as though they were one. The fact that an object's appearance can change drastically depending on the viewer's perspective and the ambient light makes this an AI problem. The difficulty in distinguishing between object features and those that are just backdrop or shadows is another issue. A machine would need very intelligent programming and a lot of processing capacity to compete with human competence at these tasks, which the human visual system does largely subconsciously. Data manipulation using an image format using a variety of approaches. The patterns seen on photographic prints, slides, television screens, and movie screens often depict a picture as a two-dimensional array of brightness values. Computers can do optical or digital image processing.

Advantages:

- Forgery detection of signatures are easy.
- Trained by better algorithm

Applications:

- Forensic applications
- Banking applications
- Business applications

Literature Survey:

The purpose of the study was stated by Kshitij Swapnil Jain et al. (2021) to determine whether a signature is genuine or fake, to learn about signature traits, and to develop a method to identify fake signatures. Although trained eyes may spot forgeries in signatures, there is no foolproof method because forgers use a wide range of handwriting styles and levels of expertise. When it comes to accurately authenticating signatures and distinguishing between real and fake ones, automatic recognition systems can be a huge help. The suggested approach employs a NN in dual roles: feature extractor and classifier. Using down sampling and convolution filtering, the feature extractor pulls features out of the incoming data. The authors make the assumption that a trained NN can distinguish between fake and real signatures and identify forgery by its behavior traits, such as sketching the intricate parts of a signature slowly or hesitantly. Even while deep networks are capable of learning features at many levels of abstraction and representing complex functions, they run into trouble when the gradient drops exponentially and hits 0 as backpropagation goes from the last to the first layer. The authors circumvent this problem by employing ResNet, which cuts out unnecessary connections or stages, allowing the gradient to backpropagate directly and preventing it from rapidly dropping to a very small value. Improved efficiency, accuracy, and the capacity to detect sophisticated forgeries were all achieved during offline signature verification using the authors' suggested method. Python and its libraries, in conjunction with a Neural Network (NN) based approach, allowed the authors to successfully detect signature forgeries.

Architecture and explanation:-

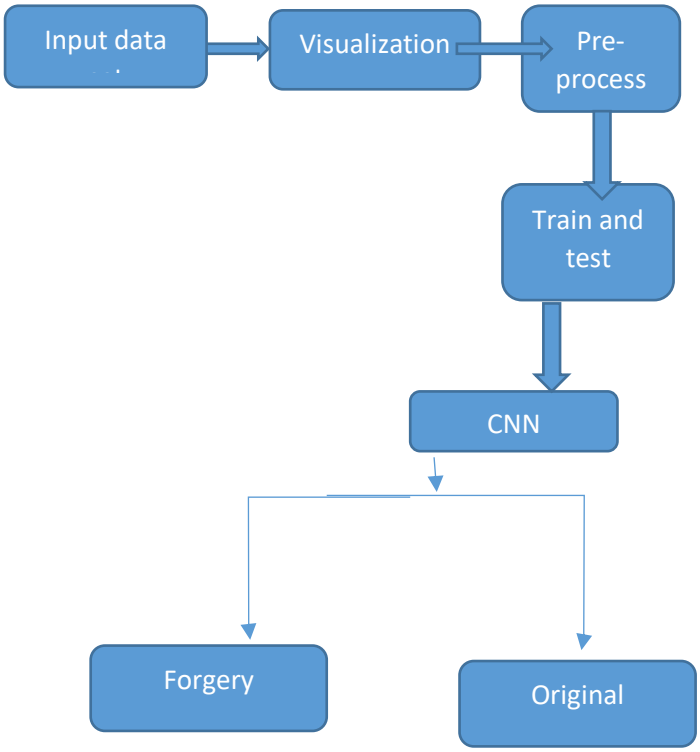


Fig: System Architecture

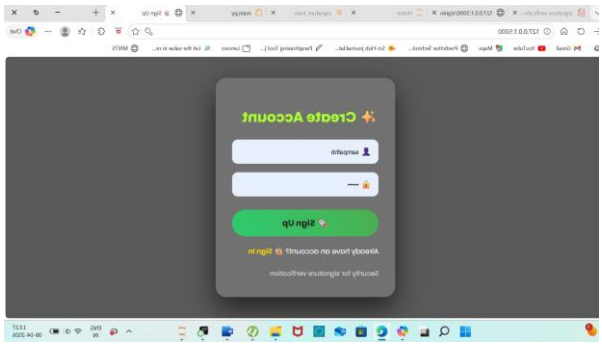
Online datasets available for the model. The idea was to have a number of samples of every person/ client including genuine as well as forged autographs to make a person dependent system. Luckily, I plant colorful online datasets of the same manner online. I used Dutch as well as English autographs so as to increase the dataset.

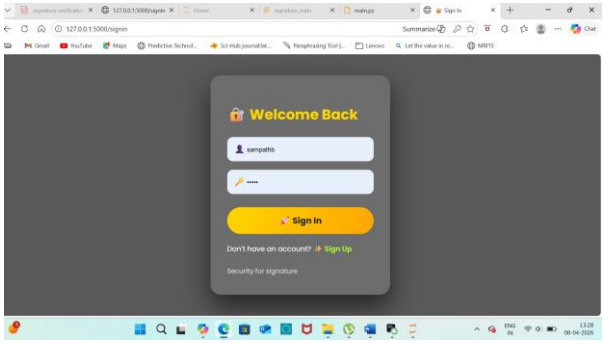
Results

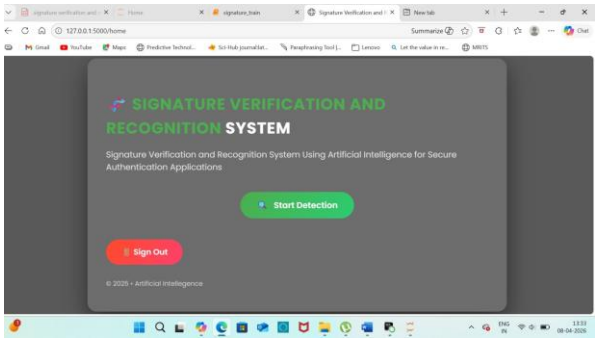
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

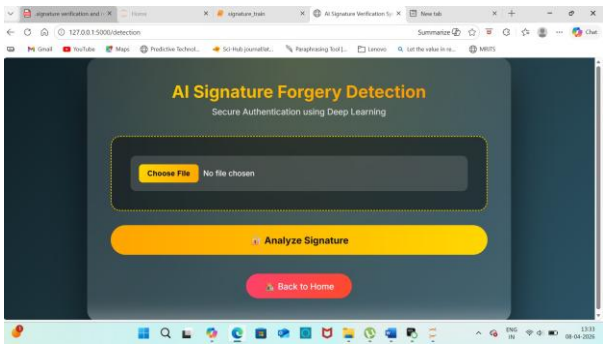
ISSN: 2454-9940 www.ijasem.org

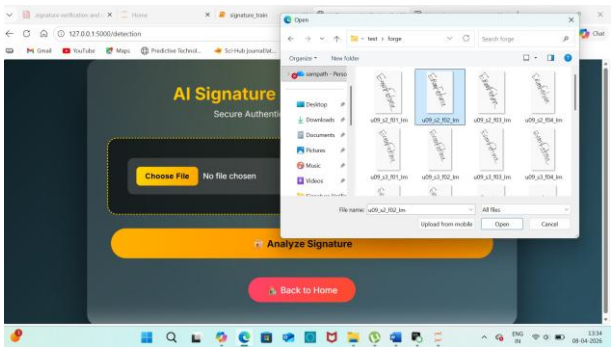
Vol 20, Issuse.2 April 2026

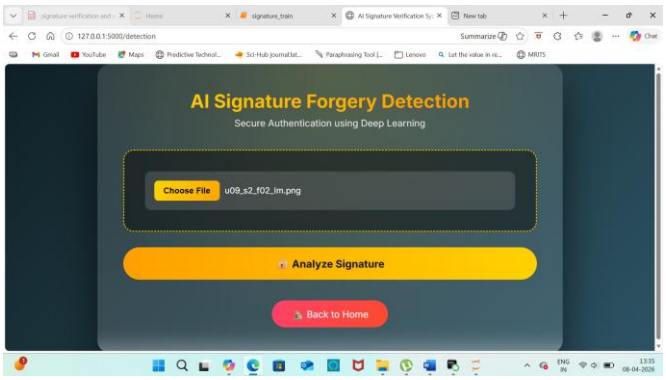


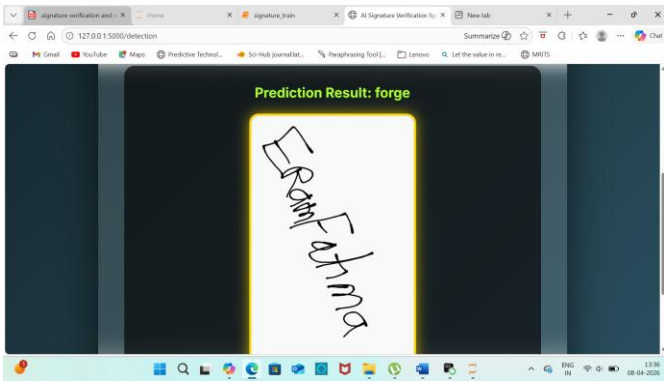


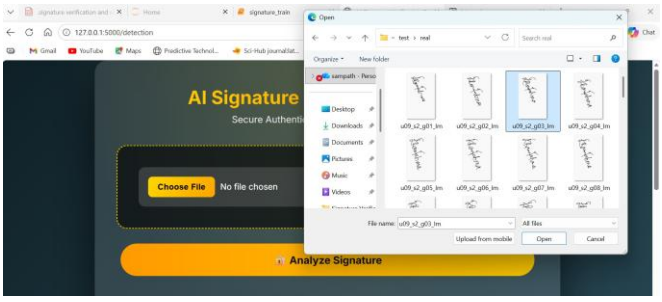


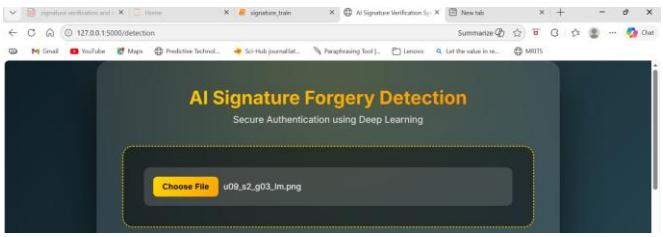


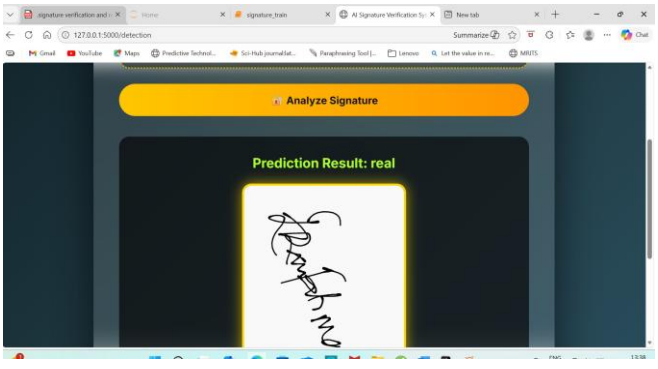












Conclusion:

On the test set, the network provided data that is delicate, which is probably quite significant. I apologize for any spelling or grammar mistakes that may have been present in this blog; I worked on it for an online competition, and while I didn't win, I learned a lot.
In the future, we can use the same method with even greater precision when analyzing videos.

Future Scope:

The future development of the Signature Verification and Recognition System focuses on enhancing accuracy, security, and usability. Advanced AI techniques like deep learning can improve verification performance, while real-time signature capture (including dynamic features such as speed and pressure) will strengthen authentication. Integration with multi-modal biometrics (face, fingerprint) can provide higher security through multi-factor authentication

References:

[1] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Characterizing and Transferring the Signature Verification Problem," IEEE Trans. Inf. Forensics Security, vol. 16, pp. 4093-4108, 2021. doi: 10.1109/TIFS.2021.3101912

[2] L. Chen, X. Wang, and J. Zhang, "Siamese Neural Networks for One-Shot Signature Verification with Attention Mechanisms," Pattern Recognit. Lett., vol. 158, pp. 45-52, Jun. 2022. doi: 10.1016/j.patrec.2022.04.009

[3] C. S. Vorugunti, V. Pulabaigari, P. Mukherjee, and S. C. Dass, "OSVFNet: Online Signature Verification Using Fused Deep Networks," Neurocomputing, vol. 461, pp. 203-217, Oct. 2021. doi: 10.1016/j.neucom.2021.07.044

[4] A. Soleimani, K. Fouladi, and B. N. Araabi, "UTSig: A Persian Offline Signature Dataset with Detailed Annotations for Machine Learning Research," IET Biometrics, vol. 9, no. 6, pp. 297-308, Nov. 2020. doi: 10.1049/iet-bmt.2020.0025

[5] S. Lai, L. Jin, and W. Yang, "SynSig2Vec: Learning Representations from Synthetic Dynamic Signatures for Real-World Verification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, no. 7, pp. 2339-2353, Jul. 2021. doi: 10.1109/TPAMI.2020.2974320

[6] X. Zhu, X. Li, and H. Zhang, "Transformer-Based Signature Verification with Global Context Modeling," Expert Syst. Appl., vol. 203, p. 117429, Oct. 2022. doi: 10.1016/j.eswa.2022.117429

[7] J. Guo, Y. Qian, and C. Li, "Graph Neural Networks for Signature Topology Modeling and Verification," IEEE Signal Process. Lett., vol. 30, pp. 445-449, 2023. doi: 10.1109/LSP.2023.3261789

[8] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSign: Deep On-Line Signature Verification," IEEE Trans. Biometrics Behav. Identity Sci., vol. 3, no. 2, pp. 229-239, Apr. 2021. doi: 10.1109/TBIOM.2021.3059224

[9] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, and J. Fierrez, "BioTouchPass2: Touchscreen Password Biometrics Using Time-Aligned Recurrent Neural Networks," IEEE Trans. Inf. Forensics Security, vol. 17, pp. 2817-2832, 2022. doi: 10.1109/TIFS.2022.3175519

[10] H. Liu, J. Sun, and B. Zhang, "Adversarial Attack and Defense for Handwritten Signature Verification Systems," Neural Netw., vol. 162, pp. 228-242, Jun. 2023. doi: 10.1016/j.neunet.2023.02.025

[11] M. Diaz, A. Fischer, R. Plamondon, and M. A. Ferrer, "Perspective Analysis of Handwriting Generation with Generative Adversarial Networks," Pattern Recognit., vol. 114, p. 107830, Jun. 2021. doi: 10.1016/j.patcog.2021.107830

[12] C. S. Vorugunti and P. Mukherjee, "Explainable Signature Verification Using SHAP-Based Feature Attribution," Comput. Security, vol. 119, p. 102782, Aug. 2022. doi: 10.1016/j.cose.2022.102782

[13] E. Maiorana and P. Campisi, "Increasing Privacy and Security of Biometric Data in Signature Recognition Systems Using Cancelable Biometrics," IEEE Trans. Dependable Secure Comput., vol. 18, no. 2, pp. 887-900, Mar. 2021. doi: 10.1109/TDSC.2019.2907568

[14] H. Rantzsch, S. Uchida, and A. Dengel, "Signature Embedding: Writer Independent Offline Signature Verification with Deep Metric Learning," in Proc. 17th Int. Conf. Frontiers Handwriting Recognit. (ICFHR), 2020, pp. 173-178. doi: 10.1109/ICFHR2020.2020.00040

[15] V. L. F. Souza, A. L. I. Oliveira, and R. Sabourin, "A Writer-Independent Approach for Offline Signature Verification Using Deep Convolutional Neural Networks Features," Appl. Soft Comput., vol. 111, p. 107647, Nov. 2021. doi: 10.1016/j.asoc.2021.107647

[16] Das P, Bhaumik S, Nath S (2022) Signature recognition and detection of skilled forgeries using image transformation and multistream cnn. In: 2022 IEEE VLSI device circuit and system (VLSI DCS), IEEE, pp 225–229

[17] Reyes RC, Polinar MJ, Dasalla RM, Zapanta GS, Melegrito MP, Maaliw RR (2022) Computer vision-based signature forgery detection system using deep learning: a supervised learning approach. In: 2022 IEEE international conference on electronics, computing and communication technologies (CONECCT). IEEE, pp 1–6

[18] Gowri P, Sivapriya G, Kamaleshwar N, Kesavaraj N et al (2022) Real time signature forgery detection using machine learning. In: 2022 second international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT). IEEE, pp 1–5

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

[19] Summra S, Usman MG, Muhammad A et al (2021) Supervised neural network for offline forgery detection of handwritten signature. In: 2021 18th international conference on electrical engineering, computing science and automatic control (CCE). IEEE, pp 1–6

[20] Jain S, Khanna M, Singh A (2021) Comparison among different cnn architectures for signature forgery detection using siamese neural network. In: 2021 international conference on computing, communication, and intelligent systems (ICCCIS). IEEE, pp 481–486