DOI: 10.6977/IJoSI.202406_8(2).0005
R. Ch, M. Sridevi, et al../Int. J. Systematic Innovation, 8(2), 58-69 (2024)

Enhancing digital security using Signa-Deep for online signature verification and identity authentication

[1]Ravikumar Ch, [2]Mulagundla Sridevi, [3]M Ramchander, [4]Vankudoth Rames,[5]Vadapally Praveen Kumar
[1]Assistant Professor, Department of Artificial Intelligence &Data Science,
Chaitanya Bharathi Institute of Technology, Hyderabad, India-500075.
[2]Associate Professor, Department of Computer Science and Engineering,
CVR College of Engineering, Hyderabad, India-501510
[3]Assistant Professor, Department of Master of Computer Applications,
Chaitanya Bharathi Institute of Technology, Hyderabad, India-500075.
[45]Assistant Professor, Department of Emerging Technologies.
CVR College of Engineering, Hyderabad-500039.
* Corresponding author E-mail: chrk5814@gmail.com
(Received 23 October 2023; Final version received 61 January 2024; Accepted 16 April 2024)

Abstract

In the contemporary digital realm, the utilization of online services has surged, facilitated by the seamless integration of deep learning technology, which is paramount in applications demanding precision and efficiency. A pivotal use case in this context is online handwritten signature verification, where the need for exceptional accuracy is indisputable. This paper introduces 'Signa-Deep,' an innovative approach designed to address the challenge of online signature verification and the determination of an individual's authorization status. The study explores a range of methodologies, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), GoogleNet, and MobileNet, to discern the authenticity of signatures and affirm the identity of the signatory. The results of our proposed method are promising, showcasing its potential to significantly enhance the security of digital transactions and identity verification processes. In summary, 'Signa-Deep' harnesses deep learning technology to bolster the accuracy and reliability of online signature verification, thereby contributing to the overall robustness of digital interactions and identity validation processes.

Keywords: Deep Learning, Online Signature Verification, Authorization Status, Identity Authentication, Digital Transactions Security

1. Introduction

As a biometric feature used for user identification, the human signature makes signature verification a persistent area of study. Online and offline signatures are the two main categories into which signatures fall. Signatures are widely used as a form of authentication. Online signatures, also called dynamic signatures, are digital signatures that are recorded in databases after being digitally taken with electronic equipment. Dynamic characteristics include things like the number and sequence of strokes, the speed at which the signature is made, and the pressure distribution at different points, which make the signature difficult to copy and distinctly unique. After the signature is preprocessed, certain attributes are taken out. User enrollment in an online signature verification system begins with the submission of reference signatures or samples of signatures. Following that, if a user signs a document (called a test signature) to prove who they are, the test signature is compared to the reference signatures linked to that person. The user's request is rejected if the discrepancy is more than a set quantity. Offline signatures, also known as static signatures, originate as ink-on-paper signatures, which are subsequently preserved by scanning to create a digital copy. In practice, it is essential to verify the authenticity of both online and offline signatures. Nevertheless, verifying offline

signatures poses a greater challenge since, unlike their online counterparts, they lack dynamic data (N. Abbas et 2012 & Neha et. 2022).

Numerous sectors, including banks, official documents, and receipts, rely on online signatures to enhance security and establish the identity of the respective individuals. Although each person possesses a unique signature, the challenge lies in consistently reproducing the same signature. The primary objective of signature verification is to reduce intra-individual variations. Online signature verification constitutes the process of confirming the author's identity through a signature verification system (O.Shapran & M. C. Fairhurst 2009). This system can serve as a security measure, facilitating verification for purposes such as access control and password replacement. Utilizing signature verification enables organizations to validate the legitimacy of customer signatures (Y. Ren et 2020.)

Signature verification is a method employed by banks, intelligence agencies, and prestigious organizations to authenticate an individual's identity. This technique is frequently utilized for comparing signatures within bank offices and other branch capture processes. Online signature verification utilizes signatures recorded using pressure-sensitive tablets, which capture not only the signature's shape but also its dynamic properties (C. Y. Low et 2007).

During the verification process, various distance measures are produced by comparing the test signature to every signature in the reference set. Consequently, a methodology for combining these distance values into a single metric that represents the difference between the test signature and the reference set must be implemented. After that, a predetermined threshold is compared to this statistic to make a decision. One can determine the single dissimilarity value by taking the average, maximum, or minimum of all the distance measurements. A verification system usually selects one of these measures and ignores the others.

Determining if a handwritten signature is real or fake is part of the online handwritten signature verification process. It is possible to fake signatures, and these fakes fall into five different categories: self-forgery, random, skilful, basic, and fluent.

a) **Random forgery:** Generated without any prior knowledge of the signature, its shape, or the signer's identity.
b) **Simple forgery:** Produced with only knowledge of the signer's name, lacking any reference to the signer's signature style.
c) **Skilled forgery:** Crafted by observing an authentic signature sample and endeavoring to replicate it as faithfully as possible. This type of forgery involves having access to a sample of the signature to be duplicated. The quality of a skilled forgery relies on factors such as the forger's practice, their skill level, and their meticulous attention to detail in mimicking the original signature. A skilled forgery closely resembles a genuine signature.
d) **Fluent forgery:** The forger aims to imitate the motion of the signature, often resulting in rapid scribbling that overlooks design elements such as the shape of letters.
e) **Self-forgery:** A specific type of forgery in which an individual forges their signature intending to deny it at a later stage."

The complexity of the signature verification task increases notably when transitioning from simple to skilled forgery. Consequently, crafting an effective signature verification system poses a significant and critical challenge (Chang et.2023).

The vital and complex field of signature verification, which is essential for user identification using the biometric characteristic of a human signature, is the subject of this study. Differentiating between offline and online signatures, the study emphasizes how online signatures are more dynamic and difficult to duplicate. Reference signatures are submitted as part of the registration procedure, and these signatures serve as the foundation for identity verification utilizing comparison with test signatures that are later submitted. Because they are not dynamic, offline signatures which started as ink on paper and were subsequently digitized present a unique set of challenges. Despite these difficulties, online and offline signatures are essential for improving security and verifying personal identity in a variety of industries, such as banking, intelligence services, and elite institutions. The main objective of the work is to tackle the crucial problem of intra-individual differences in signatures, which is necessary for the creation of efficient signature verification systems with security, access control, and

password replacement applications in mind.

Additionally, the study explores how difficult it is to verify the veracity of handwritten signatures, classifying fakes into various categories. Verifying a signature becomes more difficult when moving from simple to professional forgeries. This investigation clarifies the constantly changing field of biometric authentication and offers insightful information about the enduring difficulties encountered by industries that depend on signature validation for identity authentication. The study's importance originates from its thorough examination of signature verification, which provides a sophisticated grasp of the complexities involved and advances the development of efficient identification validation systems.

1.2 Major Contributions of the Study

a) **Static vs. Dynamic Signatures:** The study highlights the difficulties in validating static signatures in the absence of dynamic data and elucidates the distinctions between dynamic (online) and static (offline) signatures.
b) **Applications and Difficulties by Sector:** It highlights how commonplace online signatures are in industries like banking and documents, but it also notes how hard it is to reliably replicate original signatures, particularly when offline verification is involved.
c) **Minimizing Intra-Individual Variation:** The study acknowledges that the primary objective of signature verification is to minimize variances within a single signature. This knowledge is essential for creating secure, access-control, and password-replacement systems that work.
d) **Forgery Categories and Complexity:** The study clearly illustrates the complexity involved, especially when dealing with sophisticated forgeries, by classifying signature forgeries into five categories.

Crafting an effective system to address the complexity of skilled forgeries entails recognizing the substantial challenge inherent in developing signature verification systems capable of discerning sophisticated attempts to replicate genuine signatures. This understanding serves as the cornerstone for the advancement of future biometric authentication systems.

The subsequent sections of this article are structured as outlined below: In Section II, prior research in signature verification through deep learning is outlined. Section III provides comprehensive insights into our proposed algorithms: CNN, LSTM, GoogleNet, and MobileNet. Section IV presents a comparative analysis of the algorithms, focusing on accuracy scores. Finally, in Section V, we draw our ultimate conclusions.

2. Related Work

(Ata Larijani et.al) the authors address the critical issue of safeguarding data collected by smart meters to protect consumer privacy. Emphasizing the potential threats posed by data disclosure, the paper focuses on developing a platform for dynamic pricing to enhance the efficiency of electricity facilities. Unlike previous research, this study prioritizes user authentication, aiming to provide an efficient and comprehensive privacy-preserving solution for smart electricity networks. The proposed method, involving mutual authentication and key agreement between entities, significantly reduces computational complexity and communication overhead while maintaining resistance to various attacks.

(Ata Larijani et.al 2024) present an in-depth exploration of an enhanced intrusion detection method for multiclass classification. The paper introduces a novel approach employing the modified teaching–learning-based optimization (MTLBO) and modified JAYA (MJAYA) algorithms in conjunction with a support vector machine (SVM). MTLBO aids in feature subset selection, optimizing feature subsets for improved intrusion detection accuracy. The study demonstrates the effectiveness of the proposed MTLBO-MJAYA-SVM algorithm, surpassing the performance of original TLBO and JAYA algorithms on a well-established intrusion detection dataset. This research contributes to advancing optimization techniques in the domain of intrusion detection systems.

(R. Choupanzadeh et al 2023) focus centers on the development of a deep neural network (DNN) modeling methodology to predict radiated emissions from a shielding enclosure. The authors investigate the impact of aperture attributes, such as shape, size, pitch, and quantity, on the radar cross section (RCS) of a 3D enclosure resembling a desktop PC. The study employs the modified equivalent current approximation

(MECA) method to generate training data for machine learning, comparing its validity against analytical methods and a commercial field-solver. Through an exploration of various DNN models, the authors identify optimal configurations based on accuracy, computation time, and memory usage. The results demonstrate strong agreement between MECA and DNN predictions for previously unseen cases, highlighting the potential of this approach for efficient electromagnetic compatibility (EMC) assessment in electronic devices.

(Raveen Wijewickrama et.al 2023) address emerging security concerns associated with the integration of sensors in headphones. Traditional audio playback devices, now equipped with high-definition microphones and accelerometers, may inadvertently pose eavesdropping vulnerabilities. This work introduces OverHear, a framework leveraging acoustic and accelerometer data to infer keystrokes, emphasizing clustering by hand position and individual keystroke distinction through Mel Frequency Cepstral Coefficients (MFCC) analysis. Machine learning models and dictionary-based word prediction refine the results. Experimental tests demonstrate top-tier accuracy, around 80% for mechanical and 60% for membrane keyboards, with over 70% accuracy in top-100-word predictions across all keyboard types. The study highlights both the effectiveness and limitations of the proposed approach in real-world scenarios.

Kamran et.al addresses the critical role of short-term load forecasts (STLF) in power system operation and planning. Their proposed hybrid method combines artificial neural network (ANN) and artificial bee colony (ABC) algorithms, utilizing ABC to optimize ANN's learning procedure. Incorporating new load modeling based on historical and weather data, the method considers bad data elimination and calendar effects, enhancing STLF accuracy. Verified by forecasting Bushehr province demand, the results demonstrate significant improvements, underscoring the efficacy of the proposed hybrid approach in STLF precision enhancement.

(J. Vajpai et al. 2013) introduce an innovative approach to dynamic signature verification for safeguarding classified online information. Given the accessibility of sensitive data on e-commerce websites, the authors advocate a method that combines a password or PIN with a digital signature to ensure user authentication.(H. Shekar et al. 2011) introduce a robust online signature verification model that operates in stages. During the initial stage, signature preprocessing is carried out, followed by the construction of an Eigen signature from the preprocessed signature data. This model has been applied to offline Kannada signatures.

According to (D. Falahati et al. 2011), signature verification holds significant importance in financial management. The authors have introduced an approach that utilizes Discrete Time Warping for signature matching. As per the research conducted by (M. Fayyaz et al. 2015), feature extraction and feature selection are pivotal elements in the field of signature verification. The author introduces a novel approach centred on feature learning through a sparse autoencoder. These learned features serve as representations for user signatures. The study leverages the SVC2004 signature database for verification, which includes both authentic and forged signatures, enabling robust training and testing to enhance the model's accuracy. (R. C. Sonawane et al. 2012), delineated the diverse attributes of a dynamic signature captured using a digital tablet and a dedicated pen linked to the computer's USB port. The authors examined both spatial and temporal characteristics to authenticate legitimate signatures.

3. Methodology

3.1 Data collection and preprocessing

We present an extended overview of the methodological framework employed in our study.

a) **Dataset Description:** The real-time dataset used in our experiment encompasses a total of 1,000 signatures collected from 500 distinct participants. This dataset is evenly divided, consisting of 500 real signatures and 500 fake signatures. To ensure a robust evaluation, we implemented an 80-20 data split strategy. This involved allocating 80% of the dataset for the training phase, allowing the model to learn from the majority of the data, while the remaining 20% was earmarked for rigorous testing, ensuring a comprehensive assessment of the model's performance.

b) **Data Preprocessing Significance:** Recognizing the paramount importance of data preparation in guaranteeing the dependability and

efficiency of deep learning models, our methodology places a strong emphasis on this critical stage. The primary goal of data preprocessing is to transform raw, unprocessed data into a format conducive to the utilization of deep learning models. Particular attention is given to noise reduction, a key component in preparing signature images. During the data collection phase, inadvertent noise artifacts may find their way into signature scans, and meticulous treatment of these artifacts is undertaken to enhance the accuracy and resilience of the model.

c) **Deep Learning Algorithm and Feature Extraction:** Following data preprocessing, our study employs a deep learning algorithm to extract intricate features from the signatures. This process plays a pivotal role in assessing the authenticity of signatures, focusing on the model's ability to distinguish between genuine and forged signatures. This task is of paramount importance in the domain of signature verification, contributing significantly to the overall success of our approach.

d) **Experimental Process:** Illustrated in Figure 1, the experimental process provides a visual representation of the successful application of our deep learning model. This showcases the model's capability to achieve the crucial distinction between genuine and forged signatures. The demonstrated success of our approach holds promising implications for the enhancement of digital security and identity verification processes.

In conclusion, the extended methodology not only addresses the reviewer's valuable comments but also provides a more detailed and comprehensive insight into the robustness of our experimental framework. We believe that these refinements contribute significantly to the transparency, reproducibility, and overall quality of our study

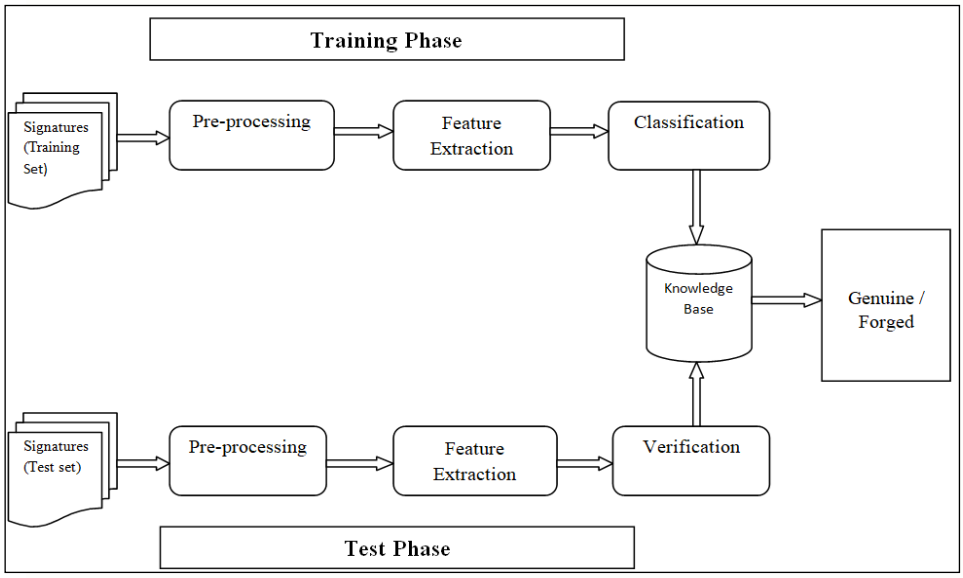

Figure 1. Architecture of Signature verification

3.2 Models

We employed four distinct models on the signature dataset for comparative analysis. Subsequently, the best-performing model was employed for real-time signature verification. The models employed include CNN, LSTM, GoogleNet, and MobileNet.

3.2.1 CNN

A Convolutional Neural Network (CNN) is a deep learning algorithm employed with image datasets for tasks such as classification, verification, recognition, or detection (K. Anatska et al. 2022 & B.H. Shekar et al. 2022).

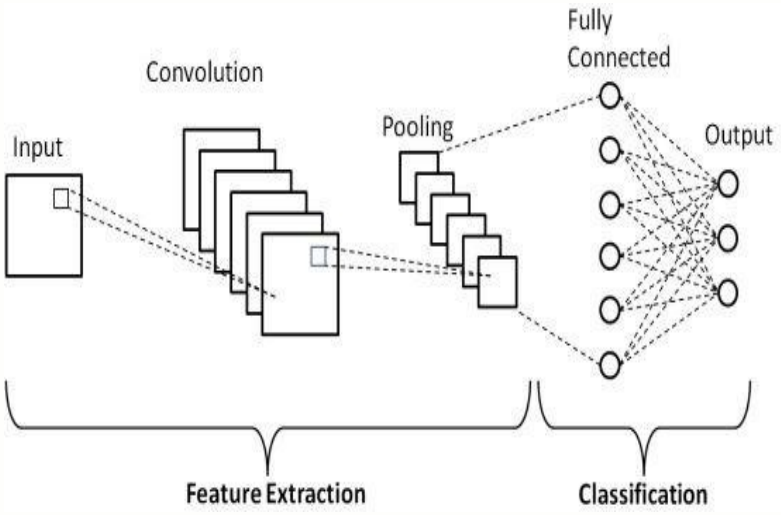

Figure 2. CNN architecture

The CNN architecture comprises several key layers (R. C. Suganthe et al. 2022) as shown in Figure 2:

a) **Convolutional Layer:** This layer operates on the input image to extract meaningful features.
b) **Pooling Layer:** Responsible for downsampling the image, common pooling methods include max pooling, min pooling, and average pooling (M. Mutlu et al. 2018).
c) **Fully Connected Layer:** The final layer of the CNN is primarily utilized for classification tasks.

Additionally, activation functions like ReLU are applied to introduce non-linearity into the network, enhancing its capacity to capture complex patterns.

3.2.2 LSTM

LSTM, an acronym for Long Short-Term Memory, belongs to the category of recurrent neural networks (RNNs). LSTM networks have been designed to overcome the limitations inherent in traditional RNNs (J. Vajpai et.2013). They prove highly effective in addressing tasks involving sequential data, such as speech recognition, analysis of time series data, and more. The LSTM model is depicted in Figure.

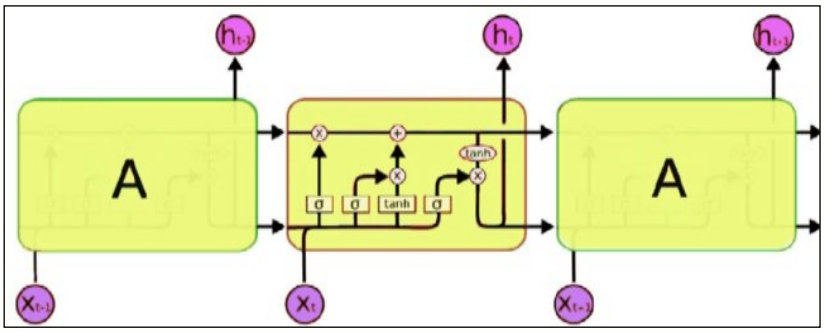

Figure 3. LSTM architecture

a) The principal components within LSTM architecture encompass:

1. Memory Cells: These specialized units serve the critical role of storing information across extended sequences, making them indispensable when dealing with long-term dependencies.

2. Gates: LSTM incorporates distinct gates, including the input gate, forget gate, and output gate. These gate mechanisms control the flow of information in and out of the memory cell, enabling the selective retention, removal, or access to information.

- Input Gate: Regulates the input information that gets stored within the memory cell.

- Forget Gate: Determines the relevance of information and facilitates its removal from the memory cell.

- Output Gate: Dictates which information should be read from the memory cell to generate the final output.

3. Cell State: LSTM networks maintain a cell state, effectively functioning as a conduit for information transfer across various time steps, adhering to the specific requirements of the task at hand.

3.2.3 Google Net

GoogleNet also referred to as Inception-v1, was developed by Google's research team and is primarily employed for tasks related to image classification. The inception module of GoogleNet is shown in Fig4.

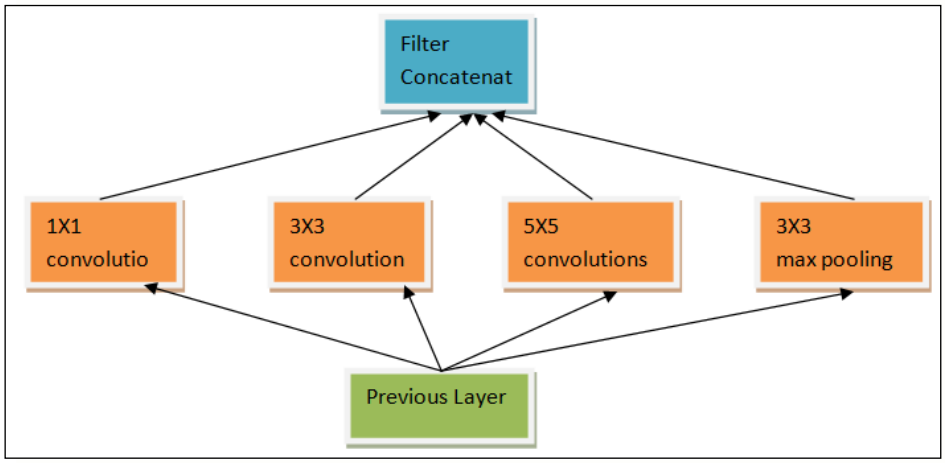

Figure 4. Inception module of GoogleNet

b) Key elements within the GoogleNet architecture include:

1. **Inception Module:** The hallmark of GoogleNet, the inception module, incorporates multiple filters of varying kernel sizes within the same layer. This design facilitates the simultaneous extraction of features at diverse scales, leading to enhanced model performance. The inception module features parallel paths and pooling layers for dimensionality reduction.
2. **Global Average Pooling:** GoogleNet adopts global average pooling as an approach to reduce the spatial dimensions of feature maps, aiding in the generation of predictions. This technique helps mitigate the risk of overfitting.
3. **Auxiliary Classifiers:** In GoogleNet, auxiliary classifiers are strategically placed at intermediate layers of the network. These auxiliary classifiers provide additional supervision during the training process, serving as a countermeasure against the vanishing gradient problem.

GoogleNet stands as a significant achievement in deep learning (B. H. Shekar et.2011), showcasing the potential for deep neural networks to achieve both high accuracy and computational efficiency. Its architectural innovations have influenced subsequent models and found applications in various computer vision tasks, including image classification and object detection.

3.2.4 MobileNet

"Developed by Google researchers, MobileNet is specifically tailored for mobile and embedded devices, demonstrating remarkable efficiency in image classification and object detection tasks, all the while conserving memory and computational resources (D.Falahati et al. 2011).

a) MobileNet encompasses the following components as depicted in Figure.5:

1. **Depth-wise Separable Convolution:** MobileNet employs depth-wise separable convolutions, which segregate spatial and depth-wise convolutions. This approach substantially diminishes both the parameter count and computational load.
2. **Point-wise convolution** often referred to as 1x1 Convolution, utilizes a compact kernel size to conduct convolution on the input data. This operation spans all channels and consolidates information from various channels at each spatial position. It plays a crucial role in adjusting the model's width, influencing its computational intensity. Typically, it is employed in conjunction with depth-wise convolution to enhance the efficacy of feature capture.
3. **Width Multiplier (Alpha):** Among the hyperparameters available, the width multiplier denoted as 'alpha' allows precise control over the number of channels in each layer. This strategic adjustment enhances model compactness.
4. **Resolution Multiplier (Rho):** Another valuable hyperparameter, the resolution multiplier ('rho'), empowers users to downscale the input image resolution. This, in turn, leads to reductions in both memory consumption and computational demands.

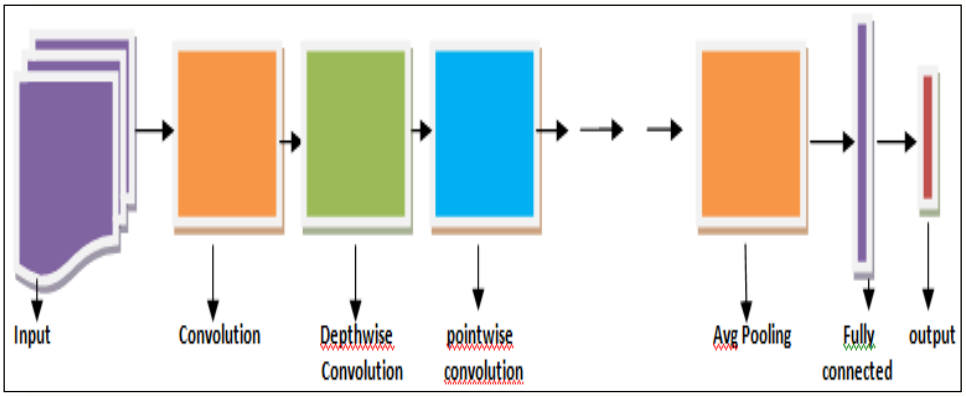

Figure 5. Architecture of MobileNet

4. Results

In this paper, we have also developed a dashboard capable of receiving signature images as input and providing feedback on their authenticity as illustrated in **Figure 6**. We employed four distinct algorithms to assess their performance in distinguishing between genuine and forged signatures. The evaluation was conducted on a consistent dataset, allocating 80% for training and 20% for testing.

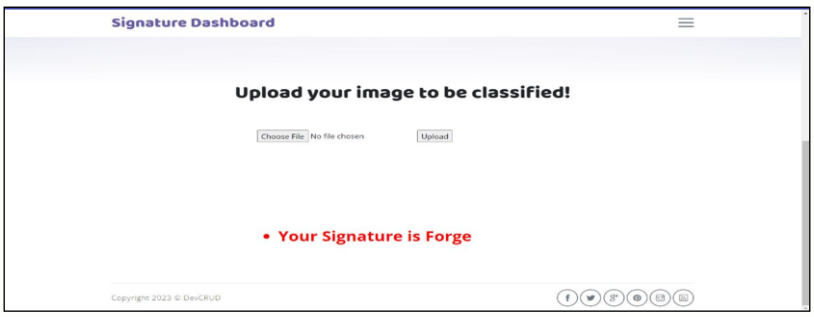

Figure 6. Dashboard showing signature is forged

Table 1. Results summary table

S.No	Algorithm	Accuracy (%)
1	CNN	98
2	MobileNet	93
3	LSTM	50
4	GoogleNet	50

The findings of our study are now presented in a clear and organized manner, including accuracy scores and relevant performance metrics. Table 1 serves as a results summary, outlining the accuracy percentages achieved by four distinct algorithms in distinguishing between genuine and forged signatures during both the training and testing phases.

During the training phase, CNN emerged as the standout performer, achieving an impressive accuracy rate of 98%. This exceptional performance underscores the robustness of the Convolutional Neural Network in the context of signature verification. MobileNet also exhibited noteworthy accuracy at 93%, showcasing its potential for reliable results in both phases. In contrast, LSTM and GoogleNet both displayed similar accuracy levels of 50% during the training phase, suggesting that they might require further refinement to match the performance of CNN and MobileNet.

The consistency of these results between the training and testing phases is remarkable. CNN and MobileNet maintained their high accuracy levels, reinforcing their reliability in both phases. Meanwhile, LSTM and GoogleNet, while not as accurate as CNN and MobileNet, demonstrated stable performance across the different data subsets. These findings highlight CNN's superiority in signature verification and its potential to enhance the security of digital transactions and identity verification processes.

Figure 8 has been incorporated to enhance the understanding and comparison of the results. This accuracy comparison chart visually illustrates the performance of CNN, LSTM, GoogleNet, and MobileNet algorithms. The graphical representation provides a concise overview of the relative accuracies of these models.

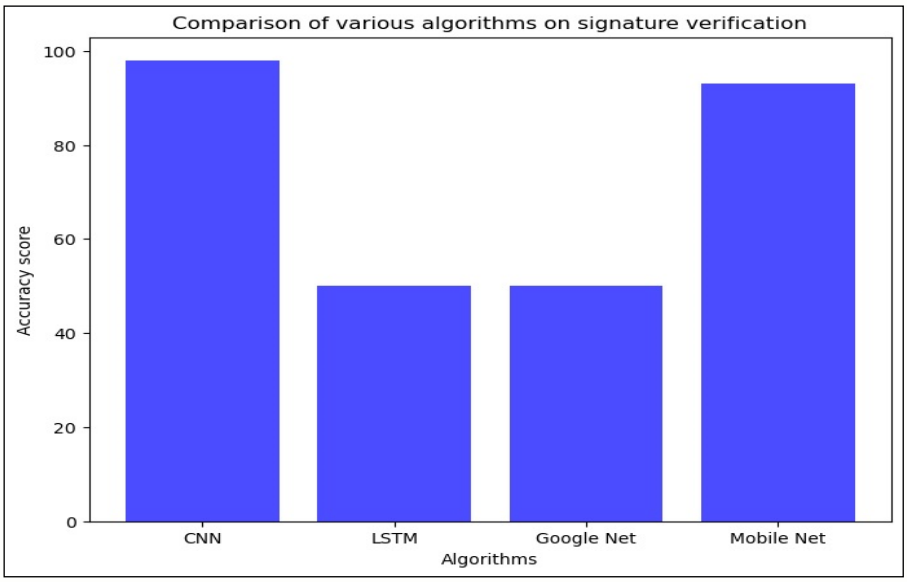

Figure 8. An accuracy comparison chart of CNN, LSTM, GoogleNet, and MobileNet algorithms

5. Conclusion and future scope

This work explores the field of signature verification for behavioral authentication, which is a commonly used technique for user authentication. Utilizing a real-time dataset including 500 unique users and equal distribution of 500 authentic and 500 fraudulent signatures, we conducted a detailed examination of four distinct algorithms – CNN, LSTM, GoogleNet, and MobileNet. With an astounding accuracy of 98%, CNN stood out as a particularly strong performer, demonstrating its resilience in signature verification. Additionally, MobileNet showed dependability with a respectable 93% accuracy rate. By comparison, the accuracy rates of LSTM and GoogleNet were 50%, suggesting areas that could benefit from further development. The study also presents an easy-to-use dashboard that is intended to facilitate effective signature verification, offering a useful instrument for identity authentication procedures.

Future scope: To improve identity authentication systems, this research will broaden the incorporation of biometric elements like fingerprint or face recognition. The goal of additional research and architecture optimization for GoogleNet and LSTM is to improve overall performance and accuracy. The emergence of real-time online signature verification capabilities creates opportunities for instantaneous authentication in digital transactions, necessitating additional research into these models' computing efficiency. Future research endeavors will further enhance and modify signature verification methods in response to technological advancements, guaranteeing improved precision, safety, and usability in the ever-changing identity authentication field.

References

Larijani, A., & Dehghani, F. (2024). Computationally Efficient Method for Increasing Confidentiality in Smart Electricity Networks. Electronics, vol. 13, no. 1, 2024, p. 170. https://doi.org/10.3390/electronics13010170.

Shekar, B. H.& Bharathi, R. K. (2011). Eigen-signature: A Robust and an Efficient Offline Signature Verification Algorithm. 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2011, pp. 134-138. doi: 10.1109/ICRTIT.2011.5972461.

Shekar, B. H., Abraham, W. & Pilar, B. (2022) Offline Signature Verification Using CNN and SVM Classifier. 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Mangalore, India, 2022, pp. 304-307. doi: 10.1109/ICRAIE56454.2022.10054336.

Low, C. Y., Teoh, A. B. J. & Tee, C. (2007) A Preliminary Study on Biometric Watermarking for Offline Handwritten Signature. 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia, 2007, pp. 691-696. doi: 10.1109/ICTMICC.2007.4448568.

Chang, S. J., & Wu, T. R. (2023). Development of a Signature Verification Model Based on a Small Number of Samples. Signal, Image and Video Processing, 2023, pp. 1-10.

Falahati, D., Helfrush, M. , Danyali, H. & Rashidpour, M. (2011). Static Signature Verification for Farsi and Arabic Signatures Using Dynamic Time Warping. 2011 19th Iranian Conference on Electrical Engineering, Tehran, Iran, 2011, pp. 1-1.

Vajpai, J., Arun, JB, & Vajpai, I. (2013). Dynamic Signature Verification for Secure Retrieval of Classified Information. 2013 Fourth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), Jodhpur, India, 2013, pp. 1-4. doi: 10.1109/NCVPRIPG.2013.6776170.

Anatska, K., & Shekaramiz, M. (2022). Offline Signature Verification: A Study on Total Variation versus CNN. 2022 Intermountain Engineering, Technology and Computing (IETC), Orem, UT, USA, 2022, pp. 1-6. doi: 10.1109/IETC54973.2022.9796924.

Larijani, A., & Dehghani, F. (2024). An Efficient Optimization Approach for Designing Machine Models Based on Combined Algorithm. FinTech, vol. 3, no. 1, 2024, pp. 40-54. https://doi.org/10.3390/fintech3010003.

Fayyaz, M., Saffar, M. H., Sabokrou M., Hoseini, M. & Fathy, M. (2015). Online Signature Verification Based on Feature Representation. 2015 The International Symposium on Artificial Intelligence

and Signal Processing (AISP), Mashhad, Iran, 2015, pp. 211-216. doi: 10.1109/AISP.2015.7123528.

Yapici, Mutlu, Tekerek, M. A.& Topaloglu, N. (2018). Convolutional Neural Network Based Offline Signature Verification Application. 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 2018, pp. 30-34. doi: 10.1109/IBIGDELFT.2018.8625290.

Abbas, N., & Chibani, Y. (2012). SVM-DSmT Combination for Off-Line Signature Verification. 2012 International Conference on Computer, Information and Telecommunication Systems (CITS), Amman, Jordan, 2012, pp. 1-5. doi: 10.1109/CITS.2012.6220365.

Sharma, Neha, Gupta, Sheifali, Mehta, Puneet , Cheng, Xiaochun, Shankar, Achyut, Singh, Prabhishek & Nayak, Soumya Ranjan. (2022). Offline Signature Verification Using a Deep Neural Network with Application to Computer Vision. Journal of Electronic Imaging, vol. 31, no. 4, 2022, p. 041210. doi: 10.1117/1.JEI.31.4.041210.

Shapran, O., & Fairhurst, M. C. (2009). Enhancing Signature Verification Using Alternative Handwriting Semantics. 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP 2009), London, 2009, pp. 1-6. doi: 10.1049/ic.2009.0242.

Sonawane, R. C., & Patil, M. E. (2012). An Effective Stroke Feature Selection Method for Online Signature Verification. 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, India, 2012, pp. 1-6. doi: 10.1109/ICCCNT.2012.6395926.

Suganthe, R. C., Geetha, M., Sreekanth, G. R., Manjunath, R., Krishna, S. M. & Balaji, P. M. (2022). Performance Evaluation of Convolutional Neural Network Based Models on Signature Verification System. 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2022, pp. 1-6. doi: 10.1109/ICCCI54379.2022.9741030.

Choupanzadeh, R., & Zadehgol, A. (2023). A Deep Neural Network Modeling Methodology for Efficient EMC Assessment of Shielding Enclosures Using MECA-Generated RCS Training Data. IEEE Transactions on Electromagnetic Compatibility, vol. 65, no. 6, 2023, pp. 1782-1792. doi: 10.1109/TEMC.2023.3316916.

Wijewickrama, R., Abbasihafshejani, M., Maiti, A. & Jadliwala, M.. (2023). OverHear: Headphone-Based Multi-Sensor Keystroke Inference. arXiv preprint arXiv:2311.02288, 2023.

Ren, Y., Wang, C. Chen, Y. , Chuah, M. C. & Yang, J. (2020). Signature Verification Using Critical Segments for Securing Mobile Transactions. IEEE Transactions on Mobile Computing, vol. 19, no. 3, 2020, pp. 724-739. doi: 10.1109/TMC.2019.2897657.

DOI: 10.6977/IJoSI.202406_8(2).0005
R. Ch, M. Sridevi, et al../Int. J. Systematic Innovation, 8(2), 58-69 (2024)

AUTHOR BIOGRAPHIES

Ravikumar Ch is an accomplished professional in the field of Computer Science & Engineering. He obtained his B.Tech. Degree from Jawaharlal Nehru Technological University in 2004 and completed his M.Tech in 2011. Currently, he is pursuing a PhD in Computer Science & Engineering at Lovely Professional University. He holds the position of Assistant Professor at Chaitanya Bharathi Institute of Technology (AI & DS), which is affiliated with Osmania University. In his role, Ravikumar imparts knowledge and mentors students in the field of computer science. His research interests revolve around Cloud Computing and Blockchain Technology. For any inquiries or further communication, he can be contacted at chrk5814@gmail.com.

Dr.Mulagundla Sridevi received Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad in 2020. She has 23 years of teaching and research experience. Currently, working as an Associate Professor at the Department of CSE, CVR College of Engineering, Ibrahimpatnam, RR District, and Telangana, India. She is a Life Member for ISTE and a Member of CSI. Her research areas of interest are Security in databases and Web Applications, Machine Learning, data science, Data mining, and Artificial Intelligence. She has published more than 30 research papers in National and International Journals, SCI and published a book chapter in Springer, and attended several National and International conferences. She can be contact at sreetech99@gmail.com.

Dr. M. Ramchander is an accomplished professional in the field of Computer Science and engineering. He obtained M.Tech (CSE) from Osmania University in 2005 and completed his Ph.D.(CSE) from Osmania University in 2023. He holds the position of an Assistant Professor at Chaitanya Bharathi Institute of Technology (Dept. of MCA), which is affiliated with Osmania University. In his role, Dr. M. Ramchander imparts knowledge and mentors students in the field of computer science. His research interests revolve around Databases, Data Mining, Big Data and Machine Learning. For any inquiries or further communication, he can be contacted at go2ramchander@gmail.com.

Vakudoth Ramesh is an accomplished professional in the field of Computer Science & Engineering. He obtained his B.Tech. Degree from Jawaharlal Nehru Technological University Hyderabad in 2010 and completed his M.Tech in 2012. Currently, he is pursuing a Ph.D. in Computer Science & Engineering at Jawaharlal Nehru Technological University Anantapur. He holds the position of Assistant Professor at CVR College of Engineering (DS), which is affiliated with Jawaharlal Nehru Technological University Hyderabad. In his role,

Vankudoth Ramesh imparts knowledge and mentors students in the field of computer science. His research interests revolve around Blockchain Technology and Network Security. For any inquiries or further communication, he can be contacted at v.ramesh406@gmail.com.

Vadapally Praveen Kumar is an accomplished professional in the field of Computer Science & Engineering. He obtained his M.Tech. Degree from Jawaharlal Nehru Technological University in 2014 and currently, he is pursuing a PhD in Computer Science & Engineering at SR University, Warangal. He holds the position of Assistant Professor at CVR College of Engineering in the department of Data Science, which is affiliated with JNTUH. In his role, Praveen Kumar imparts knowledge and mentors students in the field of computer science. His research interests revolve around Internet of things and Cloud Computing. For any inquiries or further communication, he can be contacted at micro091983@gmail.com