Adversarial attacks in signature verification: a deep learning approach

Abhisek Hazra[1], Shuvajit Maity[2], Barnali Pal[1], Asok bandyopadhyay[1]
[1]ICT and Services Group, Centre for Development of Advanced Computing-Kolkata, Kolkata India
[2]Department of Information Technology, Government College of Engineering and Ceramic Technology, Kolkata, India

Article Info

Article history:

Received Apr 19, 2024
Revised Jul 16, 2024
Accepted Jul 29, 2024

Keywords:

Adversarial attack
Affine transformation
Convolutional neural network
Forensic document analysis
Image augmentation
Signature verification
Writer authentication

ABSTRACT

Handwritten signature recognition in forensic science is crucial for identity and document authentication. While serving as a legal representation of a person's agreement or consent to the contents of a document, handwritten signatures determine the authenticity of a document, identify forgeries, pinpoint the suspects and support other pieces of evidence like ink or document analysis. This work focuses on developing and evaluating a handwritten signature verification system using a convolutional neural network (CNN) and emphasising the model's efficacy using hand-crafted adversarial attacks. Initially, handwritten signatures have been collected from sixteen volunteers, each contributing ten samples, followed by image normalization and augmentation to boost synthetic data samples and overcome the data scarcity. The proposed model achieved a testing accuracy of 91.35% using an 80:20 train-test split. Additionally, using the five-fold cross-validation, the model achieved a robust validation accuracy of nearly 98%. Finally, the introduction of manually constructed adversarial assaults on the signature images undermines the model's accuracy, bringing the accuracy down to nearly 80%. This highlights the need to consider adversarial resilience while designing deep learning models for classification tasks. Exposing the model to real look-alike fake samples is critical while testing its robustness and refining the model using trial and error methods.

Corresponding Author:

Abhisek Hazra
ICT and Services Group, Centre for Development of Advanced Computing (CDAC) - Kolkata
Plot - E2/1, Block - GP, Sector -V, Salt Lake Electronics Complex, Kolkata - 700091, West Bengal, India
Email: abhisek.hazra@cdac.in

1. INTRODUCTION

Forensic handwritten signature verification is the scientific analysis of handwritten signatures to establish their authenticity. It plays a crucial role in combating fraudulent activities in forged wills and cheques, loan applications, and manipulated legal documents, hence upholding the legal integrity in various legal proceedings, securing persons and organizations from deceptive malpractices [1]-[2]. It also undertakes high reliability in secure business processes, and access controls [3]. Conventional techniques for verifying signatures depend on the skills of forensic investigators who study physical traits, ink properties and handwriting patterns. Nevertheless, these techniques are prone to mistakes during scrutiny and can be exploited by proficient counterfeiters [4]. Some notable developments have been achieved earlier while developing tools like CEDAR-FOX [5], FISH, Wanda Workbench [6] and DIGIDOC [7] for forensic experts, with a few limitations. The effectiveness of such tools [5]-[7] highly depends on certain factors viz. quality and diversity of actual forensic training samples, accuracy and generalization of the tools, expert human intervention and inconclusiveness.

This necessitates the development of more robust and automated verification techniques. Convolutional neural network (CNN), on the other hand, have become a potent tool for automated signature verification because of their capacity to decipher intricate patterns from handwritten signatures. The CNN excels at image classification, making them well-suited for analysing the intricate details of signatures and offering the potential for reliable and efficient automated verification [8]-[9]. In forensic document analysis, particularly for tasks like signature verification using CNN, acquiring a vast and diverse dataset may be challenging, which is addressed using data augmentation, acting as a tool to artificially expand the dataset by creating realistic variations of existing signature images [10]-[11]. After that, k-fold cross-validation is a decisive technique for evaluating the robustness of machine learning models [8]. Finally, the robustness of the CNN model has been tested by introducing hand-crafted adversarial attacks, meticulously designed to deceive the model by producing realistic fake signature samples, posing a severe threat to CNN-based signature verification systems [9].

Many notable works have been done earlier, but the traditional linear and non-linear classifiers suffer from intra-class variations and inter-class similarities [12], which may result in misclassification errors. Misclassifications might result from events during the acquisition of signature images like exhaustion, distraction, or personal interpretation [13]. These mistakes may cause signatures to be mistakenly recognised as authentic or fake, which might have severe repercussions in the legal, financial, and security domains. Apart from these, non-CNN-based models can identify certain forgeries, particularly semi-skilled ones. Unfortunately, these are outperformed by skilled forgeries [14]. In addition, the opinions of forensic examiners are subjective and vulnerable to several influences. Because of their subjectivity, they can make mistakes, and competent forgers can use this weakness to trick them [3]. This demonstrates the potential advantages of adopting CNNs, which can recognise intricate patterns and characteristics in signature data and may provide a more robust defence against forgeries of all types [15].

In this work, ten handwritten signatures at varying speeds and ink colours have been contributed by each signer during a data collection event. Size normalisation has been performed on those signatures to standardise their sizes following their scanning. Next, a range of data augmentation techniques (see section 2.2) have been applied to expand the dataset for deep learning experiments. For 16 signers, 96000 images have been created, with 6000 images from each class. Due to GPU, time and space resource limitations, 10% of the entire dataset (i.e., 9600 samples) has been used for CNN-based experiments with different training and validation data splits. A split that performs the best has been selected for additional examination. However, to obtain a trustworthy performance evaluation, an experiment has been conducted employing 5×2 cross-validation at a 70:30 ratio. A few manually-crafted adversarial samples have been generated to assess the model's resilience. The proposed system's architecture is presented in Figure 1.

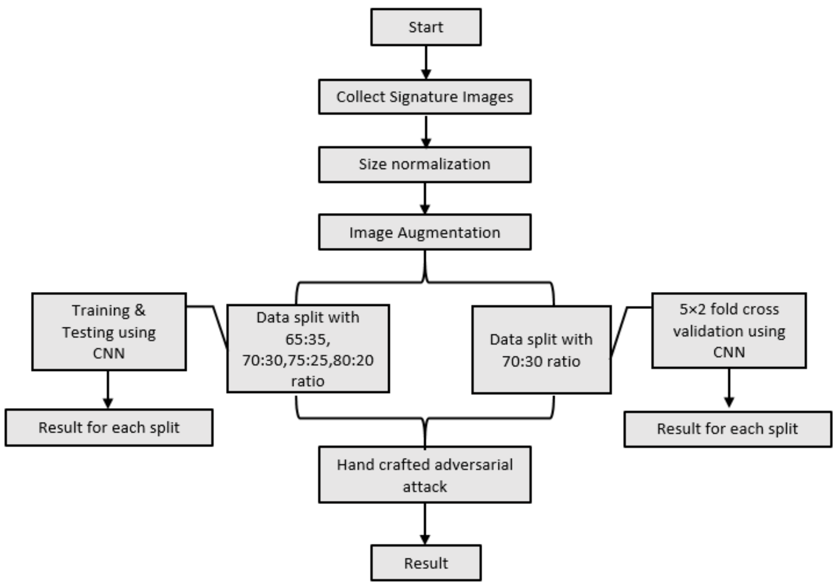


Figure 1. The process flow diagram of the proposed method

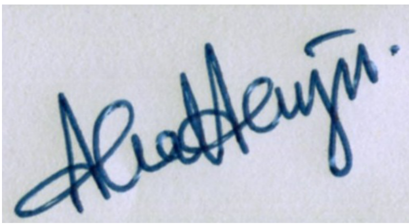
This study presents a novel approach to signature verification through a CNN-based approach. Specifically, it addresses several difficulties related to dataset development, augmentation, model training, and evaluation. One of this work's primary distinctive features is its extensive dataset collection and augmentation with large-scale expansion. Additionally, the study optimises the dataset size for CNN-based experiments by recognising the resource constraints, including GPU and storage limitations. Additionally, the study uses a 5×2 cross-validation scheme for training and validating data to provide a reliable performance evaluation. The work takes one step further by evaluating the model's resistance to adversarial attacks. This includes creating and assessing adversarial samples by hand to gain insight into the model's weaknesses and possible areas for development.

2. RESEARCH METHOD

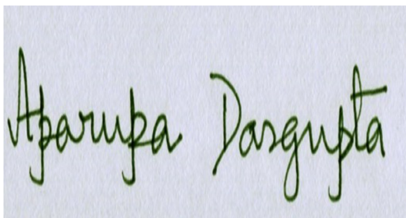
This segment defines the fundamental concepts that drive this research and articulates the current perspectives on establishing and evaluating a CNN-based signature authentication system. It narrates the various processes behind the data collection, pre-processing and data augmentation stages. Using several Python modules for image augmentation, the dataset's quality has methodically improved, confirming its viability for training powerful models. The CNN model has been carefully designed, with a data split ratio optimised for training and validation performance.

2.1. Data acquisition and pre-processing

This study adopts a thorough data collection technique to guarantee the qualitative handwritten signature data collection. This strategy captures the inherent variations in handwritten signatures, including signing speeds (slow vs. fast) and various ink colours [5]. Furthermore, data collection has been conducted in controlled environments with the authors in their normal sitting position and mental state [4]-[7]. This approach aims to maximize the authenticity and consistency of the collected signatures to enhance the classification performance. Sixteen authors of varying ages and sexes have participated in the data collection process in a regulated setting, each contributing ten signature samples [7]. Figure 2 illustrates the signatures of different persons with varying inks and orientations, in which Figure 2(a) features a concise form with quick strokes in a short signature, indicating a more streamlined signing style and Figure 2(b) displays a full-length signature with more extended and detailed pattern. After data collection, an EPSON V39 scanner has been used to scan the handwritten signature data with 120 DPI resolution. After that, size normalisation has been employed to ensure uniformity in the dimensions and properties of the handwritten signatures. The width and height of the signatures have been resized to meet the required specifications of 519× 276 pixels in jpeg format.



(a)



(b)

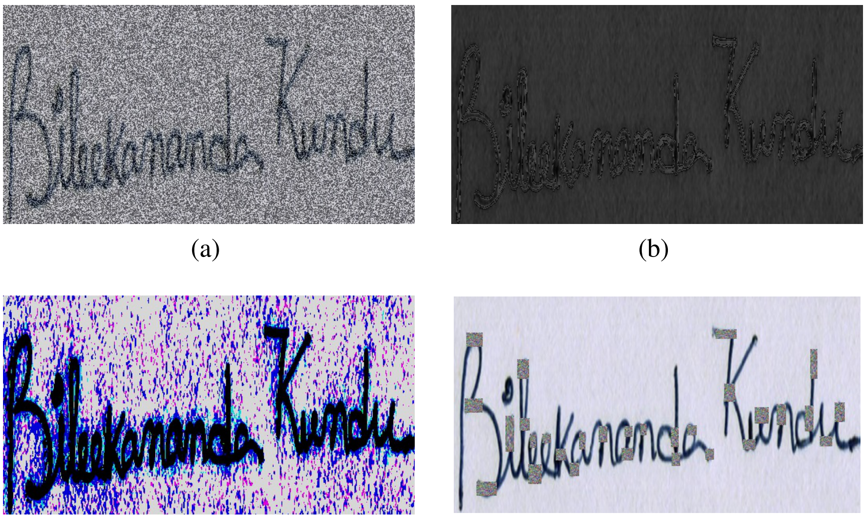
Figure 2. Variations in signing pattern of different signers with different ink combinations (a) short signature and (b) full-length signature

2.2. Data augmentation

Due to its vital role in enhancing the model performance, data augmentation has been employed extensively for the signature images to train and test the CNN model. The dataset of 160 images, comprising 16 classes with 10 samples each, has been expanded to 96,000 data points using a variety of Python libraries, including OpenCV, scikit-image, Matplotlib, Augmentor, Pillow, Keras, Imgaug, and PyTorch. Through the application of diverse transformations such as rotation, translation, scaling, flipping, and brightness adjustments, the dataset is enriched with variations mimicking real-world scenarios [16]-[17]. Figure 3(a) shows the light-grey fog effect, simulating low-contrast conditions by adding a fog-like distortion whereas Figure

3(b) displays the luminance-preserved grayscale conversion simplifying images to grayscale while maintaining original intensity values. Subsequently Figure 3(c) introduces Poisson noise by adding random pixel intensity variations to mimic real-world noise and Figure 3(d) hides the cusp, loop, and bump points with a 20×16 mask to train the model for recognising signatures even with missing details. The following list contains all of the operations used for the signature data augmentation task.

- Scaling, translation
- Bilateral filter
- Channel shift
- Perspective transform
- Visibility reduction
- Standard Luminance
- Grayscale operations
- NN interpolation
- Random rain
- Brightness, contrast, hue
- Mask cutout, grid erosion
- Elastic transform
- All blurring operations
- Random fog, shadow, snow
- Highlight recovery
- Channel equalization
- Zoom, crop operations
- Padding, shearing
- All artificial noises
- Occlusion, saturation effect
- Luminosity grayscale
- Channel cropout, shuffle
- Equalize, posterize effect
- Rectangular, circular mask



(a) (b) (c) (d)

Figure 3. Different techniques applied during augmentation (a) light-grey fog effect (b) luminance preserved grayscale conversion (c) poisson noise and (d) hiding the cusp, loop, and bump points with a 20×16 mask

2.3. Architecture of the CNN

The core component of this research is a CNN designed for handwritten signature recognition. The model was implemented using the sequential API within the Keras deep learning framework [18]. The architectural diagram is depicted in Figure 4, and detailed specifications are furnished in below sections (2.3.1 - 2.3.5).

2.3.1. Convolutional layers (Conv2D)

Learnable filters are applied to the input image by these layers to accomplish feature extraction. The first Conv2D layer utilizes 16 filters with a kernel size of 3×3, employing "valid" padding and a ReLU activation function. The input shape is defined as (276, 519, 3), corresponding to the height, width, and colour channels of the handwritten signature images.

2.3.2. Pooling layers (MaxPooling2D)

Max-pooling layers reduce the spatial dimensions of the feature maps by selecting the maximum value from each pooling region, which helps to retain essential features while decreasing the computational cost. These layers follow each convolutional layer, progressively downsizing the feature maps to focus on the most prominent information. By reducing the number of parameters, max-pooling also minimises the overfitting and enhances model generalisation.

2.3.3. Subsequent Conv2D layers

The subsequent Conv2D and Max-Pooling layers continue to refine the extracted features by applying more filters and further reducing dimensionality. Each layer builds upon the previous one, learning more complex and abstract patterns in the input image. This iterative process helps the model to develop a comprehensive understanding of the input signatures.

2.3.4. Fully-connected layers (Dense)

The fully connected (Dense) layers combine the extracted features into a one-dimensional vector for final decision-making. In this architecture, the Dense layers consist of 128 neurons each, which integrate features learned by the convolutional layers. The final Dense layer, with 16 nodes, produces the output classification, distinguishing between different signature classes.

2.3.5. Dropout layers

Dropout layers are used to prevent overfitting by randomly deactivating a fraction of neurons during each training step. In this model, a dropout layer follows one of the Dense layers, ensuring that the network does not overly rely on specific neurons. This regularization technique helps the model generalize better to unseen data.

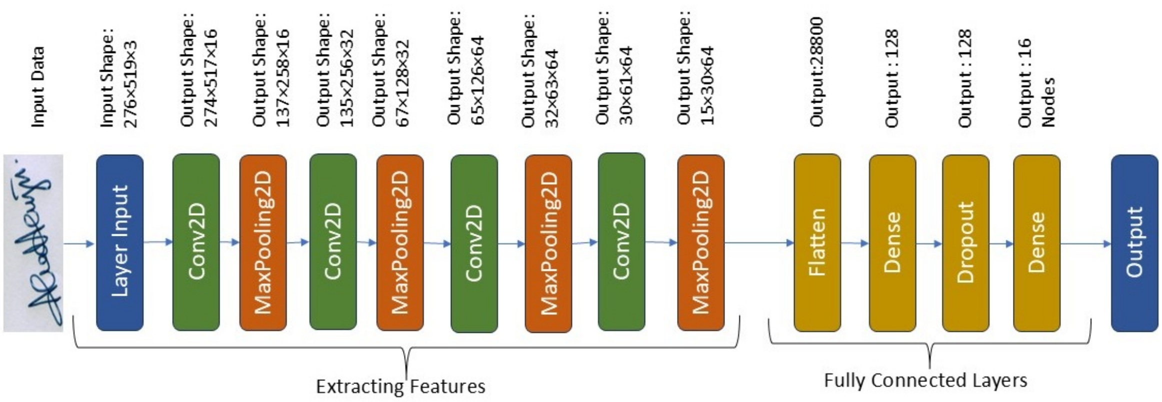


Figure 4. The architectural diagram of the proposed CNN model

3. RESULTS AND DISCUSSION

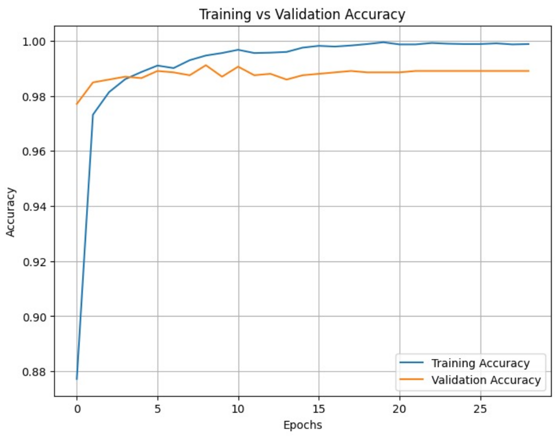
This section explores the influence of training data size on the performance of the CNN, the experimental outcome of the 5×2 cross-validation over the augmented dataset, and the impact of the adversarial attack on the proposed CNN architecture, intended for handwritten signature recognition. The initial experiment utilises a 65:35 split for training and validation data, respectively. While this configuration yields a moderate test accuracy of approximately 86%, subsequent trials aim to make improvement to the model's effectiveness. By incrementally increasing the training data proportion to 70% and 75%, with corresponding reductions in test data, we observe a minor change in the test accuracy viz. 85.89% and 85.83% respectively, demonstrating the positive impact of a more extensive training set. The most significant improvement occurred when the training data was further expanded to 80%, leading to a remarkable test accuracy of 91.35%. Furthermore, the model achieved an impressive training accuracy of 99.87% with minimal loss (0.0032). These findings highlight the crucial role of training data volume in enhancing the model's performance. Table 1 describes the performances of the system in different train vs. test splits with their average validation accuracies.

The high-performance computing resources in this work are accessed through Google Colab. These tasks are specifically carried out with the help of two virtual CPUs for general computing tasks, 52 GB of RAM for data processing and model storage, and 100 GB of cloud storage for storing augmented images, training and testing datasets, and the trained model. Additionally, various high-performance NVIDIA GPUs are used for hardware acceleration during model training. This setup guaranteed the availability of solid hardware resources required for deep learning model training, such as the CNN architecture used in this study.

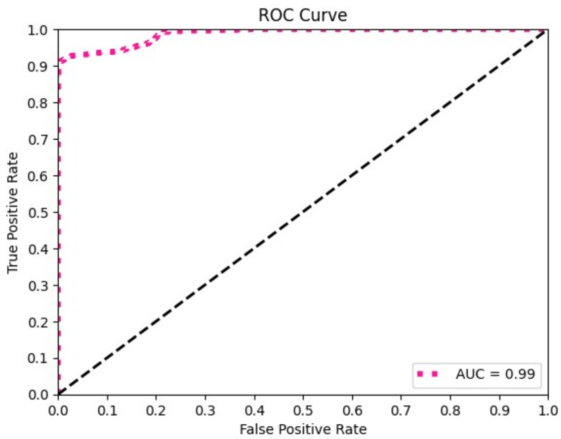
Table 1. The performance of the CNN with various train-test ratio

Train-test split	Testing accuracy(Avg.)
65:35	86.09%
70:30	85.89%
75:25	85.83%
80:20	91.35%

It is imperative to recognise that choosing a 9600 sample dataset is contingent upon hardware constraints, such as RAM capacity, GPU capabilities, and computational units on Google Colab. Despite these constraints, the model achieves promising results, showcasing the chosen CNN architecture's efficacy and the training data's quality. It may be observed from Figure 5(a) that the validation accuracy reaches a peak between the 8^{th} and 10^{th} epoch, showcasing that the model is performing well on unseen data whereas the ROC curve and high AUC (0.99) in Figure 5(b) demonstrating the efficacy of the model at distinguishing between positive and negative cases. An interesting observation may be found if the model complexity is reduced and more augmented data may be used for training and validation.



(a)



(b)

Figure 5. Results obtained with 80:20 split (a) Training vs. validation accuracy and (b) ROC Curve for Testing

The proposed technique is compared with other recent CNN-based techniques such as Triplet-CNN, ResNet-50, VGG-16, DenseNet and Attention-based CNN. From the comparison (Table 2), DenseNet emerges as the top-performing model in offline signature verification, achieving the highest scores across all metrics. VGG-16 and Attention-Based CNN also demonstrate strong performance, while the proposed method outperforms ResNet-50 and Triplet-CNN. The findings emphasise the balancing between model complexity and dataset augmentation when optimising performance under hardware restrictions. Despite restrictions, the chosen CNN architecture is effective, as proven by promising outcomes. Notably, the observed validation accuracy curve and subsequent increase in validation loss indicate the possibility of limiting the overfitting problem through model simplification and higher data augmentation. Further exploration into these pathways may provide insights into how to improve the robustness and generalisation capabilities of the signature recognition system.

3.1. k-fold cross validation

A 5×2 cross-validation approach is adopted in this work which not only ensures comprehensive use of the dataset but also allows for better generalization of the CNN model's performance across unseen data. By repeatedly alternating between training and testing on different folds, the technique reduces the likelihood of overfitting and ensures that the model remains robust. The split between training and validation within each cycle further enables the fine-tuning of hyperparameters, optimizing model performance before final testing. Such a method is especially valuable in domains like signature verification, where variations in handwritten samples can be significant, and robust validation is essential to guarantee the reliability of the model in practical applications. The final model selected through this rigorous process can then be used for advanced studies or real-world implementations, providing a reliable benchmark for future comparative research. Algorithm 1 portrays a 5×2 fold cross-validation scheme to conduct experiments on the signature dataset. It divides the dataset into 5 folds, uses each as the test set, and trains the model on the remaining folds. For model selection, the training data is divided into a training set (70%) and a validation set (30%) in each cycle [19]. This process is repeated five times, ensuring that all data points participate in training and evaluation. Finally, the best model has been adopted for futuristic work [20]-[21].

Table 2. Comparison of test accuracies for CNN models in offline signature verification

Model	Accuracy(%)	Precision(%)	Recall(%)	F1–Score(%)
Proposed method	91.35	88.48	91.35	89.50
Triplet-CNN (2018)	84.32	83.91	84.32	81.99
ResNet-50 (2019)	73.02	70.95	73.02	70.90
VGG-16 (2018)	93.39	93.63	93.39	93.27
DenseNet (2020)	95.26	95.51	95.26	95.21
Attention-Based CNN (2020)	92.24	94.50	92.24	91.51

Algorithm 1 Handwritten signature recognition with 5-fold cross validation

Input: Dataset D, Number of folds 5
Output: Model M
Split D into 5 folds $D_1, D_2, ..., D_5$
for $i \leftarrow 1$ **to** 5 **do**
    $D_{test} \leftarrow D_i$
    $D_{train} \leftarrow D \setminus D_i$
    Split D_{train} into a training set D_{train_train} (70%) and validation set D_{train_val} (30%)
    Train model M_i on D_{train_train}
    Validate model M_i on D_{train_val}
    Calculate validation accuracy Acc_i
end for
$best\_model \leftarrow M_i$ with highest validation accuracy Acc_i
return $best\_model$

Five-fold cross-validation yields consistent performance metrics across the folds. Training loss ranged from 0.0476 to 0.0545 (average: 0.0466), while training accuracy varied between 0.9843 and 0.9873 (average: 0.9863). Validation loss values fell within the range of 0.0573 to 0.0956 (average: 0.0743), and validation accuracy achieved values between 0.9795 and 0.9868 (average: 0.9830). These results demonstrate the model's effectiveness in learning from the data during validation. It is evident from Figure 6 that the training accuracy is highest in the 2^{nd} fold, whereas in the 4^{th} fold, the validation accuracy is at its peak.

These findings demonstrate the model's stable performance across data partitions, with a narrow range of training and validation losses indicating efficient learning without overfitting. Minimal fluctuations in accuracy metrics further highlight the robustness of the model's architecture and training process. This consistency is crucial for signature verification, where small variations can significantly affect the results.

3.2. Hand-crafted adversarial attack

Unfortunately, there are some inherent weaknesses in CNN-based handwritten signature verification, so it is imperative to conduct adversarial attack experiments to measure the robustness of the proposed scheme.

Despite its strength in image recognition, CNNs are not auto-immune to adversarial instances, which are malicious changes made to an input image that may lead to a false positive or false negative case [22]-[23]. This might fool the system into accepting a fake signature or rejecting an authentic one regarding forensic signature verification. In this context, hand-crafted adversarial attacks were opted for several compelling reasons. First, these attacks are beneficial for evaluating security since they enable practitioners to evaluate the security and robustness of the machine learning models in depth [24]. By purposefully altering the input data in many ways, researchers may determine if models are prone to manipulation and misclassification, identifying vulnerabilities that require further investigation, thus creating more robust algorithms and strategies for classification [25]. Moreover, the significance of adversarial attacks extends to real-world applications, where adversaries may exploit the weaknesses in machine learning systems for malicious purposes [9]. By studying adversarial attacks, researchers can craft defences to safeguard against such threats in practical domains such as cybersecurity, autonomous vehicles, and healthcare systems. Finally, adversarial attacks prompt crucial ethical considerations surrounding the utilization of AI and machine learning. By comprehending the manipulative potential of models, researchers and practitioners can devise strategies to uphold principles of fairness, transparency, and accountability in AI systems, ensuring their responsible deployment and use [26].

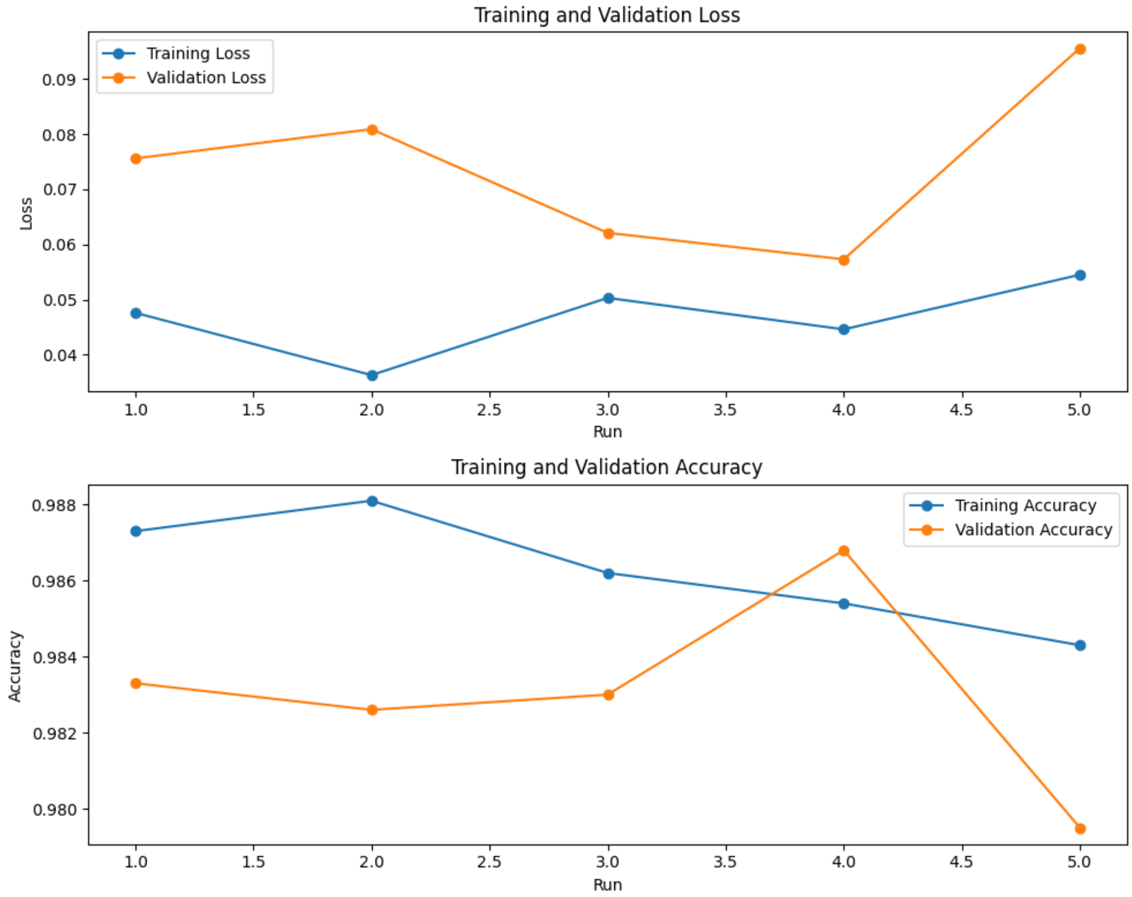


Figure 6. The result of the 5×2 fold cross-validation technique

In this study, some hand-crafted perturbations have been produced on original handwritten signatures to fool the CNN model, in order to produce misclassification. The process involves replicating a part of a signature to another part (copy-move forgery), adding coffee or tea stains on the signature images, simulating penmanship errors by striking out the signatures, mimicking insect damage by placing bug impressions on the signatures, hiding the crucial points (loop, cusp and bump) using a 22×14 pixel mask and erasing the same points of the signatures, as shown in Figure 7.

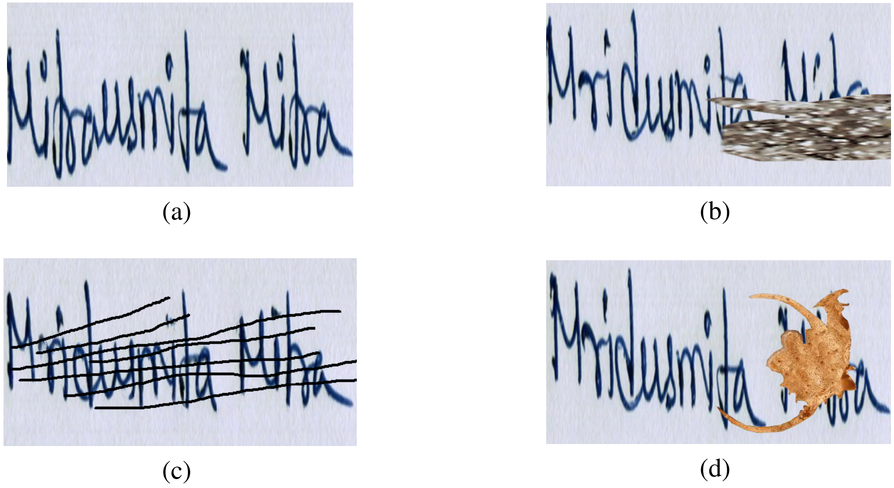


Figure 7. Images obtained from the handcrafted adversarial attacks executed on the handwritten signature data using (a) Copy-move forgery (b) Insect damage impression (c) Pen strike out and (d) Coffee or tea stain

Ten samples have been produced for each of the sixteen signers, yielding 160 altered signatures. Out of 160 samples, 129 signatures are properly categorised when the accuracy is tested using the same CNN model, revealing that the accurate positive prediction drops to 80.62% (Figure 8), indicating the need to train the CNN with more realistic altered data samples. Real-world signatures may undergo alterations, either intentional (e.g. through software like Photoshop) or unintentional (such as stains or impressions). By training on these realistic manipulated images, a CNN can learn to identify the underlying item or scene despite these alterations. As a result, the system performs more accurately in real-world situations. The attack success rate is 19.37% (Figure 8), indicating that the CNN gains strength by using altered signatures while training, making it difficult to deceive the system with adversarial noises.

To conclude, each author's signature sample tests each of the hand-constructed assaults separately. The primary goal is to determine the individual effects of these attacks on the dataset. From this experiment, it is observed (Figure 9) that the overlapping effect, caused by making a 50% cut-move operation on each signature, yields 37.5% false positive predictions. In contrast, the shadow effect has the most minor influence on the CNN model. On the other hand, the impacts of copy-move forgeries, deleting significant portions of the signatures, the coffee or tea stain effect, and the bug imprint effect on the signatures have a comparable 25% ASR impact on the CNN model (Figure 9). These results emphasize the CNN model's varying susceptibility to different types of hand-crafted adversarial attacks. Understanding these vulnerabilities can guide the development of more robust models, capable of accurately distinguishing between authentic and forged signatures, even under challenging conditions.

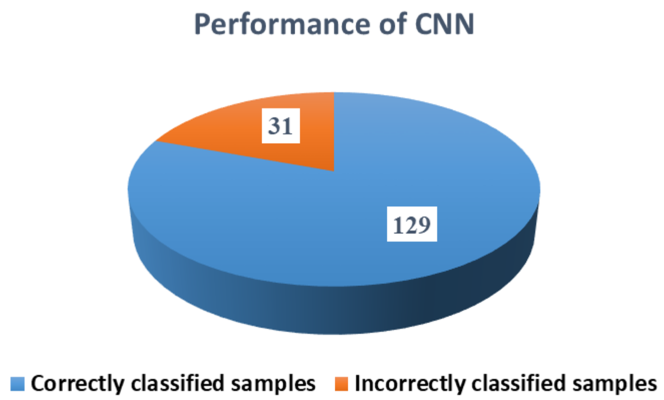


Figure 8. Overall performance of the CNN during handcrafted adversarial attacks

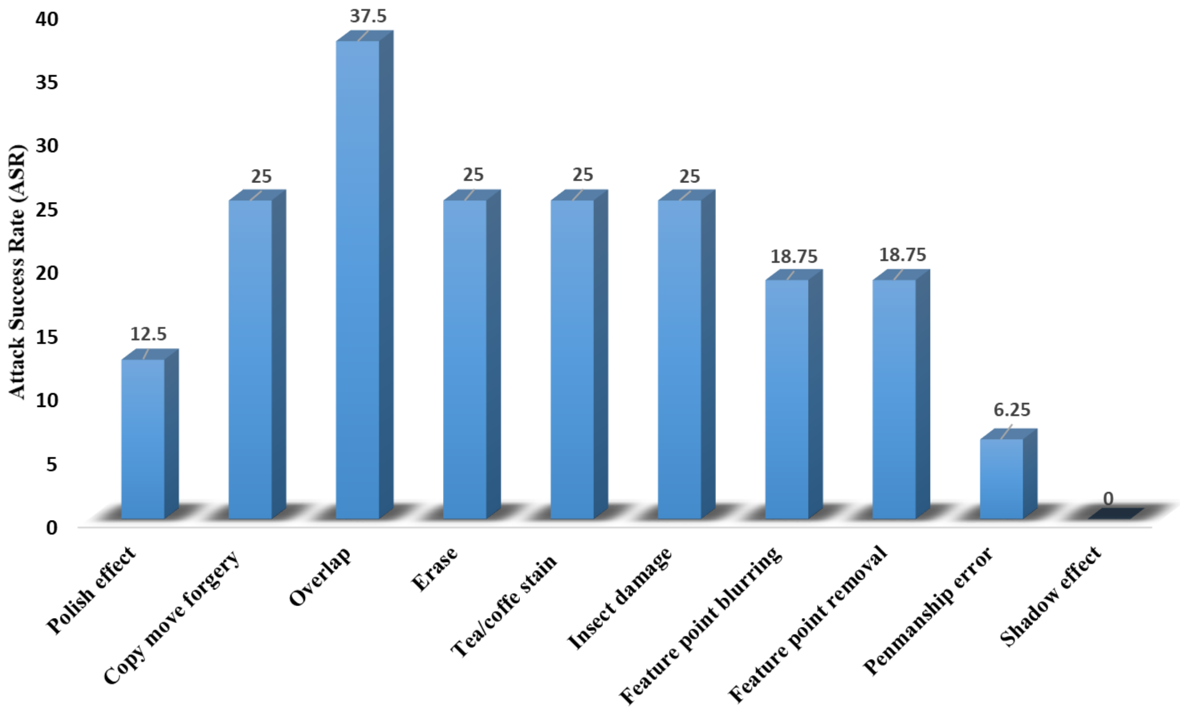


Figure 9. Effect of adversarial assaults on CNN using various hand-crafted mechanisms

4. CONCLUSION

This work investigates the effectiveness of a Convolutional Neural Network for handwritten signature verification. The proposed system achieves a testing accuracy of 91.35% with an 80:20 train-test split, surpassing an earlier study by the authors with an average validation accuracy of 90%. The model demonstrates robustness to variations in the training vs. testing data split, achieving accuracies of 86.09%, 85.89%, 85.83% for 65:35, 70:30, and 75:25 split, respectively. Additionally, 5×2 fold cross-validation produces an average validation accuracy of 98.30%, further solidifying the model's performance. Furthermore, the system underwent testing against various hand-crafted attacks, with the overlapping effect demonstrating the highest attack success rate (37.5%). It highlights the importance of considering potential forgeries and incorporating methods to improve attack detection in future iterations. However, investigating through adversarial attacks revealed potential vulnerabilities, emphasizing the need for adversarial robustness in CNN-based future developments. Though the proposed scheme demonstrates promising outcomes, there are ample avenues for further exploration. There is a strong need to increase the number of realistically manipulated samples and expand the author pool with variations in age, sex, orientation, and pen colour, thereby increasing the generalisability of the model. Additionally, incorporating a controlled number of forged signatures would further strengthen the framework. Finally, more realistic augmentation techniques may be introduced so that the model learns from newer variations.

ACKNOWLEDGEMENTS

The authors wish to sincerely thank Ms Sourima Nath, Intern at CDAC Kolkata, for her technical contribution in this work and Ms Mridusmita Mitra, Linguist at CDAC Kolkata, for proofreading the article and sharing her insights. They also acknowledge Dr. Ch.A.S. Murty (Centre Head) and Shri Aditya Sinha (former Centre Head) of CDAC-Kolkata for their kind support and encouragement. The financial support for this study was provided by a project grant titled "Work-based Learning Program" funded by the Ministry of Electronics and Information Technology (MeitY), Government of India.

REFERENCES

[1] M. I. Malik, S. Ahmed, M. Liwicki and A. Dengel, "FREAK for Real-Time Forensic Signature Verification" in *12th International Conference on Document Analysis and Recognition*, Washington DC, USA, 2013, pp. 971-975, doi: 10.1109/ICDAR.2013.196.

[2] Z. J. Barad and M. M. Goswami, "Image Forgery Detection using Deep Learning: A Survey" in *6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2020, pp. 571-576, doi: 10.1109/ICACCS48705.2020.9074408.

[3] S.D. Bhavani, and R.K. Bharathi, "A multi-dimensional review on handwritten signature verification: strengths and gaps" *Multimedia Tools and Applications*, vol. 83, pp. 2853–2894, May 2023, doi: https://doi.org/10.1007/s11042-023-15357-2.

[4] S. Kulik and D. Nikonets, "Forensic handwriting examination and human factors: Improving the practice through automation and expert training" in *Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, Moscow, Russia, 20216, pp. 221-226, doi: 10.1109/DIPDMWC.2016.7529393.

[5] S. N. Srihari, S.H. Cha, H. Arora and S. Lee, "Individuality of handwriting" *Journal of Forensic Sciences*, vol. 47, no. 4, pp. 856-872, July 2002, PubMed: https://pubmed.ncbi.nlm.nih.gov/12136998.

[6] K. Franke, L. Schomaker, C. Veenhuis, C. Taubenheim, I. Guyon, L. Vuurpijl, M. Van Erp and G. Zwarts, "WANDA: A common ground for forensic handwriting examination and writer identification" in *Third International Conference on Hybrid Intelligent Systems(HIS-2003)*, Melbourne, Australia, 2003, pp. 927–938, IOS Press.

[7] A. Hazra, D. Pal,, B. Pal, and A. Bandyopadhyay, "DIGIDOC: A Handwritten Document Analysis Tool for Forensic Application", In: Smys, S., Tavares, J.M.R.S., Shi, F. (eds) in *Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing*, vol. 1439, Springer, Singapore, 2023, pp. 379–397, doi: 10.1007/978-981-19-9819-5_29.

[8] Y. Muhtar, W. Kang, A. Rexit, Mahpirat and K. Ubul, "A Survey of Offline Handwritten Signature Verification Based on Deep Learning" in *3rd International Conference on Pattern Recognition and Machine Learning (PRML)*, Chengdu, China, 2022, pp. 391-397, doi: 10.1109/PRML56267.2022.9882188.

[9] S. Rokade, S. K. Singh, S. Bansod and P. Pal, "An Offline Signature Verification Using Deep Convolutional Neural Networks" in *Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*,Bhilai, India, 2023, pp. 1-4, doi: 10.1109/ICAECT57570.2023.10117669.

[10] K. Nanthini, D. Sivabalaselvamani, K. Chitra, P. Gokul, S. KavinKumar and S. Kishore, "A Survey on Data Augmentation Techniques" in *7th International Conference on Computing Methodologies and Communication (ICCMC)*,Erode, India, 2023, pp. 913-920, doi: 10.1109/ICCMC56507.2023.10084010.

[11] J. F. Ramirez Rochac, N. Zhang, J. Xiong, J. Zhong and T. Oladunni, "Data Augmentation for Mixed Spectral Signatures Coupled with Convolutional Neural Networks" in *9th International Conference on Information Science and Technology (ICIST)*,Hulunbuir, China, 2019, pp. 402-407, doi: 10.1109/ICIST.2019.8836868.

[12] A. Hazra, A. Chaudhuri, and A. Bandyopadhyay, "Development of a System with Online Signature Biometric for Access Control Application" in *2nd International Conference on Informatics, Control and Automation (ICA2019)*, Hangzhou, China, 2019, doi: 10.12783/dtcse/ica2019/30720.

[13] G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo and P. Mignone, "Multidomain Verification of Dynamic Signatures Using Local Stability Analysis" *IEEE Transactions on Human-Machine Systems*, vol. 45, no. 6, pp. 805-810, December 2015, doi: 10.1109/THMS.2015.2443050.

[14] 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, doi: 10.1109/TSMCC.2008.923866.

[15] M. Hanmandlu, Md.H.Md. Yusof, and V.K. Madasu, "Off-line signature verification and forgery detection using fuzzy modeling" *Pattern Recognition*, vol. 38, no. 3, pp. 341-356, Dec. 2015, doi: 10.1109/THMS.2015.2443050.

[16] Y. Gupta, Ankit, S. Kulkarni, and P. Jain, "Handwritten Signature Verification Using Transfer Learning and Data Augmentation", In: Agarwal, B., Rahman, A., Patnaik, S., Poonia, R.C. (eds) in *Proceedings of International Conference on Intelligent Cyber-Physical Systems. Algorithms for Intelligent Systems*, Springer, Singapore, 2022, pp. 233–245, doi: 10.1007/978-981-16-7136-4_19.

[17] C. Wigington, S. Stewart, B. Davis, B. Barrett, B. Price, and S. Cohen, "Data Augmentation for Recognition of Handwritten Words and Lines Using a CNN-LSTM Network" in *14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*, IEEE, Kyoto, Japan, 2017, vol. 1, pp. 639-645, doi: 10.1109/ICDAR.2017.110.

[18] F. Chollet, *Deep Learning with Python.* New York: Manning Publications Co., 2017.

[19] I. Nti, O. Nyarko-Boateng, and J. Aning, "Performance of Machine Learning Algorithms with Different K Values in K-fold Cross-Validation" *International Journal of Information Technology and Computer Science*, vol. 6, pp. 61-71, Dec. 2021, doi: 10.5815/ijitcs.2021.06.05.

[20] E. Kee, J.J. Chong, Z.J. Choong, and L. Michael, "A Comparative Analysis of Cross-Validation Techniques for a Smart and Lean Pick-and-Place Solution with Deep Learning" *Electronics*, vol. 12, no. 11, 2023, doi: 10.3390/electronics12112371.

[21] Y. Nie, L. De Santis, M. Carratù, M. O'Nils, P. Sommella, J. Lundgren, "Deep Melanoma classification with K-Fold Cross-Validation for Process optimization" in *IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, Bari, Italy, 2020, pp. 1-6, doi: 10.1109/MeMeA49120.2020.9137222.

[22] K. N. Kumar, C. K. Mohan,and L. R. Cenkeramaddi, "The Impact of Adversarial Attacks on Federated Learning: A Survey" *IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, vol. 46, no. 5, pp. 2672-2691, May 2024, doi: 10.1109/TPAMI.2023.3322785.

[23] B. Biggio, and F. Roli, "Adversarial Attacks and Defences: A Survey" *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, issue 4, pp. 974-994, 2021, doi: 10.1109/TNNLS.2020.2985318.

[24] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z.B. Celik, and A. Swami, "The Limitations of Deep Learning in Adversarial Settings" in *IEEE European Symposium on Security and Privacy (EuroS&P)*, Saarbruecken, Germany, 2016, pp. 372-387, doi: 10.1109/EuroSP.2016.36.

[25] S. -M. Moosavi-Dezfooli, A. Fawzi and P. Frossard, "DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks" in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 2574-2582, doi: 10.1109/CVPR.2016.282.

[26] L.G. Hafemann, R. Sabourin, and L. Oliveira, "Characterizing and Evaluating Adversarial Examples for Offline Handwrit-

ten Signature Verification" *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2153-2166, doi: 10.1109/TIFS.2019.2894031.

BIOGRAPHIES OF AUTHORS

Abhisek Hazra is working as an R&D engineer in the Centre for Development of Advanced Computing (CDAC), Kolkata for the last 13 years. He completed his M.Tech in Computer Science & Engg. from Jadavpur University, India 2012. He received B. Tech in Computer Science & Engg. from Government College of Engineering & Ceramic Technology, India in 2008. He has prior industry and academic experiences. He received several awards and authored research articles in prestigious conferences and journals. His research interests include biometrics, forensic document analysis, human-computer interaction, perception engineering and artificial reality. He can be contacted at email: abhisek.hazra@cdac.in.

Shuvajit Maity is a software development intern at the Centre for Development of Advanced Computing(CDAC), Kolkata. He completed his B.Tech in Information Technology from Maulana Abul Kalam Azad University of Technology (MAKAUT), India in 2023. Currently, he is pursuing an M.Tech in Information Technology from the Government College of Engineering & Ceramic Technology, India. His research interests are artificial intelligence applications and questioned document analysis. He can be contacted at email: shuvajitmaity99@gmail.com.

Barnali Pal is serving as a Scientist-E and section head in ICT & Services Group at Centre for Development of Advanced Computing (CDAC), Kolkata with more than 23 years of working experience in Digital Signal Processing, Speech Processing, Language Technology, Cyber Forensics etc. Her academic qualification is B.Tech in Radio Physics and Electronics, from the Institute of Radio Physics and Electronics and a B.SC. Physics (Hons.) from the University of Calcutta. She has executed national and international projects as a CI and published papers on these areas. Her current research focus includes natural language processing, machine translation, digital signal processing, artificial reality, cyber security and education technology. She can be contacted at barnali.pal@cdac.in.

Asok Bandyopadhyay is the Group Head and designated as Scientist-F of the ICT & Services Group in the Centre for Development of Advanced Computing (CDAC), Kolkata. His academic qualifications are an M.Tech and B.Tech in Radio Physics and Electronics from the Institute of Radio Physics and Electronics and a B.SC. Physics (Hons.) from the University of Calcutta. He has over 31 years of experience in R&D activities in microprocessor and microcontroller-based industrial systems, DSP-based control systems, speech processing, soft computing, biometric-based access control, infrared imaging etc. He led several GOI projects in this area, with more than 30 national and international research articles. His current research interests are cyber security and forensics, infrared image processing, questioned document analysis and artificial reality. He can be contacted at email: asok.bandyopadhyay@cdac.in.