E-signature Mobile Scanner for Signature Verification

Alleckzer Querido
College of Computer Studies Engineering
Computer Engineering Department
Jose Rizal University
Mandaluyong City, Philippines
alleckzer.querido@my.jru.edu

Ameenah Guro
College of Computer Studies Engineering
Computer Engineering Department
Jose Rizal University
Pateros, Philippines
ameenah.guro@my.jru.edu

Elizher James Ursabia
College of Computer Studies Engineering
Computer Engineering Department
Jose Rizal University
Mandaluyong City, Philippines
elizherjames.ursabia@my.jru.edu

Michael Dennis Paragas
College of Computer Studies Engineering
Computer Engineering Department
Jose Rizal University
San Juan City, Philippines
michaeldennis.paragas@my.jru.edu

***Abstract*— This study introduces an E-signature mobile scanner designed for signature verification purposes. The research presents a potent convolutional neural network (CNN) architecture designed for image classification tasks. The CNN model exhibits outstanding performance, achieving an impressive accuracy of approximately 96.13% on a test dataset, with an optimal training accuracy of 99.55%. Utilizing an Adam optimizer with a learning rate of 0.000001 and Sparse Categorical Crossentropy loss function, the model successfully minimized training and validation losses to around 0.0425 and 0.0965 as well. These results underscore the potential application of the mobile scanner in accurate signature verification tasks. Future research may focus on enhancing the model's generalizability and interpretability, possibly through transfer learning, data augmentation and model interpretability approaches, for more reliable real-world applications.**

Keywords—verification, mobile-based, signature, CNN model, accuracy, architecture

I. INTRODUCTION

It is evident that technology runs through every aspect of our lives in this age of technological domination. Technology has advanced significantly even in the area of paperwork and documentation, where signatures verify the authenticity of documents. Since the introduction of digital notebooks and tablets, electronic signatures have gained widespread use and are recognized as legitimate endorsements in the digital world. The most important job is to confirm that these signatures are authentic. While visual inspection is a part of traditional methods, this manual approach is difficult and prone to human error. Applying an Artificial Intelligence (AI) becomes an essential tool in this case.

Automation of the verification process is possible due to AI's ability to examine minute of details of a signature, such as writing style, strokes, and general patterns. This automated system replaces the visual inspection method, which improves accuracy and speeds up the validation process. Beyond efficiency, the suggested mobile application seeks to solve the digital age's critical need for security. By utilizing Artificial Intelligence (AI) capabilities, the system protects sensitive data and acts as a deterrent against fraud in addition to verifying signatures.

This research aims to pioneer a novel approach, building on the foundation laid by previous studies of Dias et al. (2016), which highlighted the difficulties of signature verification systems requiring multiple samples [1]. The goal of the study is to create a mobile application that verifies signatures using Convolutional Neural Network (CNN) algorithm. Our method streamlines the verification process by training the model with different samples of signatures, in contrast to existing systems that uses different algorithm. This paper explores the study's methodology, objectives, and expected results with the ultimate goal of designing and creating an advanced mobile application for safe and easy signature verification.

II. RELATED WORKS

Verification of e-signature is still an essential component of biometric authentication, especially when it comes to offline handwritten signatures. Verification processes encounter challenges considering signatures are complex variable data [1]. In the realm of offline signatures, the distinction between dynamic and static signatures is vital, where dynamic signatures involve active signing and static ones denote non-active signing states. Notably, the intra-personal variability in offline signatures complicates consistent authentication even among skilled signers [2].

Progress in signature verification in recent times has mainly relied on deep learning (DL) methods, specifically Deep Convolutional Neural networks (CNN). The writer-dependent (WD) and writer-independent (WI) models used in CNN frameworks are interesting approaches [3]. These models are essential for improving offline signature verification algorithms' accuracy.

The use of Artificial Neural Networks (ANN) in conjunction with novel methodologies like Histogram Oriented Swerve Angle (HOSA) has surfaced as a promising strategy for offline signature verification [4]. This approach heavily emphasized feature extraction through skeletonization techniques and HOSA-based signature image feature extraction methods. Also, promising outcomes have been observed in the comparative analysis of optimization methods such as Stochastic Gradient Descent (SGD) and Levenberg-Marquardt (LM) [4].

Shape-based preprocessing techniques, coupled with Eigen-signature construction, offer an efficient avenue for feature extraction in offline signature verification [5]. The proposed model showcases its robustness through experimental validation, exhibiting notable performance when compared to texture-based verification systems.

In parallel, the intersection of dynamic signature verification with secure information retrieval is gaining traction [6]. This approach integrates digital signatures with traditional authentication measures like passwords or PINs to safeguard classified information against unauthorized access.

The proposal of a hybrid digital signature verification algorithm combining secure hash code generation, DNA encryption/decryption, and EIGamal encryption/decryption techniques aims to enhance data security in online services [7]. This algorithm seeks to mitigate security challenges within communication networks, catering to user authentication, data confidentiality, and integrity.

The use of Convolutional Neural Network (CNN)-based offline signature verification introduces a novel approach for distinguishing between Writer Dependent (WD) and Writer Independent (WI) signatures [8]. Experimental findings indicate a 62.5% success rate for WI and 75% WD, demonstrating the potential of CNN when coupled with additional feature extraction methods.

III. METHODOLOGY

A. Data Collection Techniques

The dataset consists of 672 images for both training and testing, each resized to uniform size of 64x64 pixels. Each team member contributed 24 authentic and 24 forged signatures, resulting in a total of 96 images per member. Additionally, online signature samples were integrated, adding diversity to the dataset.

Utilizing Android Studio and Java, this prototype layout seamlessly combines robust backend functionality with user-friendly interface. User interact with the app to capture or select a signature image. Before verification, the selected signature image undergoes preprocessing steps within the app. These steps involve resizing and normalization to prepare the image for verification. The app initiates the verification process, passing the preprocessed signature image through the integrated CNN model. The mode's classification outcome is crucial in determining the signature's validity. The app the verification result on the result screen, users are presented with a clear indication whether the signature is original or forged.

B. Data Preprocessing

The quality of input data has a significant impact on model outcomes in the field of deep learning, where Convolutional Neural Networks (CNNs) are frequently utilized for image analysis. The *ImageDataGenerator* class from Keras is employed to implement essential image preprocessing techniques. To ensure consistent data for the model, this includes *normalization*, which involves scaling pixel values to a standard range between 0 and 1. In order to improve the training dataset and the model's generalization to a variety of inputs, random transformations like rotations, zooming, and horizontal flipping are also applied as part of *data augmentation*. Ensuring uniformity in the input dimensions is achieved by *resizing images* to predefined dimension. In order to promote stable and effective training, *batch normalization* is used to normalize activations in intermediate layers. By randomly deactivating neurons during training, *dropout* is used as a regularization technique to prevent overfitting. All of these preprocessing methods work together to improve the deep learning model's resilience and capacity for generalization when used with research data.

- Normalization

```
x_train = np.array(x_train) / 255
x_val = np.array(x_val) / 255
```

- Data Augmentation

```
datagen = ImageDataGenerator(
    rotation_range=30,
    zoom_range=0.2,
    width_shift_range=0.1,
    height_shift_range=0.1,
    horizontal_flip=True,
    vertical_flip=False
)
datagen.fit(x_train)
```

- Resizing Images

  img_arr = cv2.imread(os.path.join(path, img))[...,::-1]
  resized_arr = cv2.resize(img_arr, (img_size, img_size))

- Batch Normalization

  model.add(BatchNormalization())

- Dropout

  model.add(Dropout(0.3))

C. Model Classification

This section details the architecture, training process, evaluation metrics, and overall significance of the CNN-based model designed for mobile-based signature verification application. Its efficacy in accurately classifying signatures as authentic or forged forms the foundation of its utility in real-world applications.

The CNN architecture's effectiveness in signature verification arises from the cooperative interaction among its components. From the initial feature extraction in the convolutional layers to the synthesis of acquired insights within the fully connected layers, each element contributes distinctly to the model's precision in identifying between authentic and forged signatures.

The training initiates with image preprocessing, wherein images undergo resizing to a standardized 64x64 pixel dimension and normalization, optimizing data consistency for model utilization. Leveraging the Adam optimizer, the model refines its weights during training, while the SparseCategoricalCrossentropy as the loss function streamlines the multi-class classification task. Conducting training over a specified number of epochs facilitates the model's evolution fine tuning its capacity to verify between genuine and forged signatures.

IV. EXPERIMENTAL RESULTS

Model Architecture

During the training phase, the model was optimized using the Adam optimizer with a low learning rate set at 0.00001. To compute the loss, the Sparse Categorical Crossentropy function was utilized, interpreting the model's output as logarithms. Throughout the training, the primary metric monitored was accuracy, over the training iterations, the model exhibited significant learning, achieving an impressive training accuracy of around 99355%. On the validation set, the model demonstrated commendable performance, attaining an accuracy of approximately 96.13%. Regarding the loss, the model succeeded in minimizing it substantially. The training loss reached a minimal value of approximately 0.0425, while the validation loss was minimized to about 0.0965. Collectively, these findings demonstrate the model's capacity to extract complex patterns from the data, attaining high accuracy while reducing the corresponding loss, indicating potent learning and generalization abilities.

Model: “sequential_2”

Layer (type)	Output Shape	Param#
conv2d_4 (Conv2D)	(None, 64, 64, 32)	896
…		
Dense_4 (Dense)	(None, 2)	258
Total params: 1112162 Trainable params: 1111394 Non-trainable params: 768		

Model Training Progress

The Model was trained 100 epochs using a dataset comprising 672 signature images. The training progress was as follows. The table 1 presents the outcomes of the model training process over 100 epochs. The training accuracy consistently improved, reaching approximately 99.7& indicating the model's increasing capability to learn from the dataset. The training loss steadily decreased to 0.0156, showcasing the model's enhanced ability to minimize errors during training.

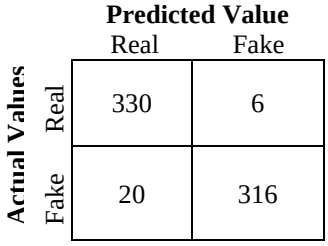
TABLE I. Model Training Progress

Epoch	**Loss**	**Accuracy**
1	0.4487	0.7976
25	0.0590	0.9762
50	0.0489	0.9836
75	0.0270	0.9896
100	0.0156	0.9970

Confusion Matrix

The confusion matrix illustrates how effectively the model differentiates between real and fake samples. The model's predictive accuracy is demonstrated by the 330 true positives for real samples and 316 true positives for fake samples, along with only a few misclassifications.

Real & Fake Confusion Matrix



Classification Report

The precision, recall, and F1-score metrics provide a detailed assessment of the model's performance. High precision and recall scores around 0.96 indicate the model's effectiveness in identifying both real and fake samples. The model's balanced performance across classes is further supported by the weighted average F1-score of 0.96.

	Precision	**Recall**	**F1-Score**	**Support**
real	0.98	0.94	0.96	350
fake	0.94	0.98	0.96	322
accuracy			0.96	672
macro avg	0.96	0.96	0.96	672
weighted avg	0.96	0.96	0.96	672

V. CONCLUSIONS AND FUTURE WORKS

The experimental results are notable given the model achieves an impressive accuracy of about 96.13% on the test dataset. This result demonstrates the model's effectiveness in precise classification, which is supported by an excellent 99.55% training accuracy. The model's capacity to reduce errors during learning is demonstrated by the simultaneous decrease in losses during training and validation, with approximately 0.0425 and 0.0965, respectively. These findings provide compelling evidence for the model's ability to perform effectively in image classification tasks.

Despite these encouraging results, the study acknowledges some limitations and possible areas for improvement. The model performs differently when exposed to different or more diverse datasets, even though it shows resilience within the dataset it was trained on. Future research may focus on improving the generalization ability of the model by exploring strategies like ensemble methods, data augmentation, and transfer learning to address this. Lastly, continual model evaluation and retraining using updated datasets are recommended to ensure adaptability to evolving signature patterns and potential security threats.

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

[2] S. Soisang and S. Poomrittigul, "Artificial Neural Network with Histogram Oriented Swerve Angle for Signature Verification," 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Phuket, Thailand, 2022, pp. 419-422.

[3] B. H. Shekar and R. K. Bharathi, "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.

[4] J. Vajpai, Arun JB and I. Vajpai, "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.

[5] B. H. Shekar and R. K. Bharathi, "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.

[6] J. Vajpai, Arun JB and I. Vajpai, "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.

[7] R. Kasodhan and N. Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 10-15.

[8] M. Mutlu Yapici, A. Tekerek and N. Topaloglu, "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.