Introducing A Transformer Model for Online Signature Verification and It’s Applications

AKHILA K S
Department of Computer Science & Engineering
Government Engineering College, Thrissur

Abstract— This paper deals with the study and review of various methods to overcome the challenges involv-ing identification and verification of online signatures. Handwritten signatures have long been the most widely used form of personal identification. So it plays an important role in today’s society but the great concern is the security issues behind this. To avoid such situations Computer Assisted Automatic Signature Verification has introduced to improve performance and verification of signatures.This paper proposes a generalized architecture for the signature verification system, illuminates a comprehensive overview of various signature verification applications, points to the importance of DeepSignDB in signature verification systems and suggests appro-priate signature tools and supporting frameworks for next-generation signature applications.By developing a transformer-based model for online signature verification using the DeepSiggnDB dataset, this research aims to enhance the accuracy and reliability of signature authentication systems.

Index Terms—Biometrics, handwritten signature, DeepSignDB, deep learning, Transformer Model

I. INTRODUCTION

Today, a perrson identification and authentication are very important in security and resource management. Biometrics is the science of identifying people according to their physical and behavioral characteristics. For centuries, handwriting has been an important part of approving contracts and agreements in business transactions. Fingerprint, iris, face, voice, palm, etc. Among the various types of biometric identification, the most widely used will be the signature.

The security measures to be used must be cheap, reliable and not intrusive to authorized person. The technique which meets these requirements is handwritten signature verifica-tion for example Technology used by banks, intelligence agencies, and high-tech institutions to find the identify of an individual.

Online signature verification is a critical task in today’s digital world, where the authenticity of digital signatures is crucial for secure transactions and document verification. Traditional methods for signature verification often struggle to handle the complexities of online signatures, such as capturing the temporal dynamics and spatial relationships between pen strokes. To address these challenges, we propose a transformer-based model for online signature verification, leveraging the DeepSiggnDB dataset. Transformers have gained significant attention in the field of natural language processing due to their ability to capture long-range dependencies, and we believe their architecture can be effectively adapted to sequential data like online signatures. By harnessing the power of transformers, our model aims to achieve state-of-the-art performance in accurately differentiating between genuine and forged online signatures, ultimately enhancing security and trust in digital transactions.

The DeepSignDB dataset serves as a valuable resource for training and evaluating our proposed transformer model. This dataset comprises a diverse collection of online signature samples, including variations in writing styles, speeds, and complexities. The data collection process involves capturing users signatures using electronic devices, resulting in a rich and realistic representation of online signature data. To ensure the reliability and quality of the dataset, appropriate preprocessing steps are applied, including noise removal, normalization, and resampling. The DeepSiggnDB dataset enables our model to learn robust features and patterns specific to online signature verification tasks, contributing to the overall effectiveness and generalization of the proposed transformer model. Through comprehensive experiments and analysis using DeepSiggnDB, we aim to demonstrate the superiority of our transformer-based approach in online signature verification and highlight its potential for real-world applications.

The transformer model’s architecture comprises multiple self-attention layers, enabling it to attend to different parts of the signature sequence adaptively. This capability helps in capturing long-range dependencies and identifying subtle patterns that contribute to signature verification. Additionally, the model incorporates positional encodings to preserve the temporal information of the signature strokes.By utilizing the transformer model for online signature verification, we expect to achieve improved accuracy and robustness compared to traditional methods. The model’s ability to learn from the DeepSignDB dataset’s diverse signature samples, along with its capacity to capture complex patterns and dependencies, makes it a promising approach for enhancing the security and reliability of digital signatures.

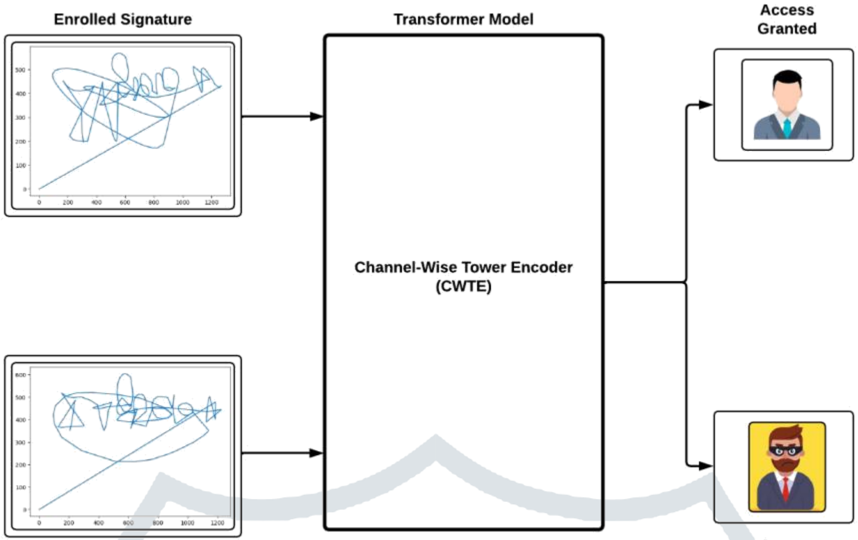

Fig. 1. ”Generalized Architecture of the Online Signature Verification System: Leveraging Transformer Model and DeepSignDB Dataset for Enhanced Accuracy and Robustness”.

II. RELATED WORKS

Tolosana et al. (2021) introduced a new time-aligned recurrent neural network (TA-RNN) approach for online signature verification process. The proposed method is a deep learning approach that identifies features of biometric signatures from a database. RNN is used here to train the data that is required for signature verification, which reduces the latency in identification. Compared with other approaches, the proposed TA-RNN approach improves the performance and efficiency of signature verification. However, the system takes a long time to verify the signature.

Tolosana et al. (2020) developed a two-factor authenti-cation approach to improve password security. They used MobileTouchDB, a dataset with 64,000 samples from 217 users, and evaluated traditional recognition techniques such as Dynamic Time Warping and Timed Recurrent Neural Networks. The method trained a robust model capable of thwarting attacks with a consistent error rate of 2.38%. This study contributes to password security research and high-lights the potential of incorporating two-factor authentication to strengthen user authentication and combat security threats.

Zanuy et al. (2020) reviewed the current state of AI-based symbol recognition in e-security and e-Health applications, focusing on safety, health, and metadata issues. The study highlights the need for a unified perspective and identifies potential vulnerabilities in online manuscript analysis. The study contributes to existing research by identifying gaps and opportunities for further investigation, encouraging interdis-ciplinary collaboration and innovative approaches. Overall, the study highlights the importance of addressing security, health, and metadata issues holistically in online manuscript analysis.

Vera-Rodriguez et al. (2019) conducted a study on biomet-ric authentication applications, analyzed various attack con-ditions, and evaluated the robustness of signature biometric systems. The research described hacking detection methods and explored different levels of PA within online signing certificates. The findings showed that BiosecureID and e-BioSign documents significantly affect system operation and affect the attacker’s knowledge and training success. This re-search contributes to this field by examining the performance of signature biometric systems and identifying vulnerabili-ties and issues associated with authentication applications. The knowledge gained can be a guide for the development of more robust and secure biometric authentication systems.

Hafemann et al. (2019) conducted a study on offline handwritten signature verification systems with a focus on identifying new attacks. They used the Current Biometric System Threat Taxonomy framework and conducted experiments on four datasets: MCYT-75, CEDAR, GPDS-160 and Brazilian PUC-PR. The study found that deniability attacks were relatively simple to construct, even without users’ knowledge. Spoof attacks were more difficult and required a higher noise level. The study evaluated the success of attacks based on noise requirements and provided an overview of the vulnerabilities and problems faced by offline handwritten signature verification systems. This research contributes to the development of robust and secure signature verification systems.

Lai et al. (2018) utilized recurrent neural networks (RNNs) and metric loss functions to address intraindividual variability in online signature verification. Their meta-learning approach allowed for different workspaces for different customers, enabling quick adaptation for new customers. The model achieved superior performance on three benchmark datasets, contributing to the advancement of online signature verification techniques. A meta-learning approach enables efficient adaptation to new customers and superior performance on multiple datasets.

Costilla-Reyes et al. (2018) developed a computational model using ground sensor data to capture spatiotemporal representations of human steps for biometric authentication. The model allows artificial intelligence to recognize subtle differences between real users and fraudsters. The model has demonstrated high reliability in biometric systems, with a small percentage of customers verifying its effective-ness. The model's effectiveness in data security areas such as airport security checkpoints is supported by customer footprint data analysis. This research improves biometric systems and contributes to the development of more reliable authentication techniques.

Gruber et al. (2010) proposed a new approach to online signature authentication using maximum length reverse detection algorithm and Local Change Subsequence Search (LCSS) technique. This method effectively identifies individuals based on their tact, outperforming other criteria. The SVM-LCSS approach demonstrated robust capabilities of accurately identifying individuals with high confidence, contributed to the progress of online signature verification, and provided valuable insights for the development of robust authentication systems.

Van et al. (2010) propose an alternative system for online signature analysis that incorporates hidden Markov models (HMMs) and a threshold-based authentication approach. The system subtracts 25 points for each signature and uses normalization techniques to improve performance. Initial validation of the system shows that the combination of information and probability-based information significantly improves the quality of authentication. The system achieves a more stable distribution of client scores across databases, resulting in improved client distribution and reduced fraudulent scores. This work contributes to the progress of online signature analysis and offers valuable insights for robust authentication systems.

Plamondon et al. (2000) conducted a survey on hand-writing recognition focusing on online and offline activities. The survey highlights the importance of handwriting recog-nition in communication, information recording and every-day transactions. It includes algorithms for preprocessing, character and word recognition, and real-time processing. The survey also highlights broader applications such as signature recognition, author recognition, and educational tools for teaching handwriting. The survey provides valuable insights into the various algorithms and techniques used in handwriting recognition systems, reinforcing its versatility and importance in various fields.

According to various researchers, online signature verification and handwriting recognition research uses deep learning models, AI and machine learning algorithms for accurate authentication and recognition. Studies address security issues, while handwriting recognition research high-lights the importance of recognizing handwritten words and signatures in a variety of applications. These efforts contribute to the advancement of biometric authentication, strengthening security measures, and improving the accuracy and reliability of these systems.

III. PROPOSED SYSTEM

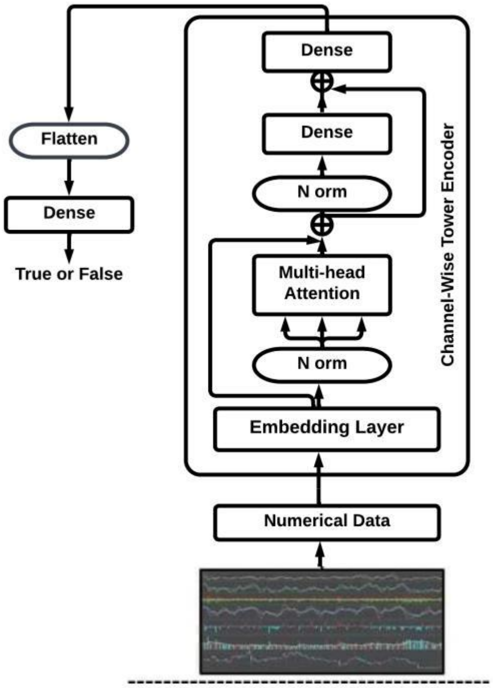

Fig. 2. Architecture of Proposed Transformer Model.

Online handwritten signature verification is the process of testing whether a signature is genuine or forged. A signature can be easily forged. Forgeries of signatures they are divided into two types: random and skilled forgeries

Random Forgery: Produced by a forger without knowing the authors name and real signature.

Skilled Forgery: In which the forger has a specimen signature to be forged.The quality of the simulation depends on how much the forger practices before attempting the actual forgery, the forger's skill and attention. Detail during signature simulation. A skillful fake looks more like the real thing signature. The problem of signature verification becomes increasingly difficult as we move from simple to skilled forgery. Currently, there is an increase the requirement for faster and more accurate processing of individual identification, therefore the design of a signature verification system becomes important call.

A proposed method for online signature verification system using DeepSignDB dataset is given in Fig 3. The Objective of the model system is to develop a model with increased accuracy and robustness. The model follows a series of steps, including input signature data, embedding, layer normalization, multi-head attention, concatenation, additional layer normalization, dense layers, flattening, and output layer. The input data is then passed through these layers, which perform nonlinear transformations and feature extraction, allowing the model to learn discriminative representations. The output is then flattened using the ”flatten” layer, reshaping the data into a 1D representation, and facilitating compatibility with subsequent layers. The output layer, represented by the ”dense-2” layer, classifies the signatures as genuine or forged. The module is trained using labeled samples from the DeepSignDB dataset, optimizing the model’s parameters to minimize classification errors between genuine and forged signatures. During the validation phase, the trained model computes a feature representation of the input signature, which is compared to the actual signatures in the DeepSignDB dataset to determine its authenticity. Standard evaluation metrics such as accuracy, precision, recall, and F1 score evaluate the performance and reliability of the model in real-world applications. Overall, the proposed method significantly increases the accuracy and robustness of online signature verification systems by utilizing the DeepSignDB dataset.

Multi Head Attention : The transformer model in online signature verification uses an encoder-decoder structure with self-attention mechanisms. The channel-wise tower encoder, a variant, focuses on extracting features from input signature data. The Multi-Head Attention mechanism is crucial for capturing interdependencies between different channels in input data, such as pressure, azimuth, altitude, and time. This mechanism allows the model to attend to different parts of the input data simultaneously and learn meaningful representations. The channel-wise tower encoder efficiently captures dependencies and patterns in signature input data, allowing it to learn discriminative representations of genuine and forged signatures. The Multi-Head Attention mechanism also improves the model’s ability to handle long-range dependencies within the input sequence, overcoming the limitations of traditional recurrent neural networks. Overall, the Multi-Head Attention mechanism in the channel-wise tower encoder is essential for effectively processing multi-channel input and learning representations that capture the distinct.

Signature Verification Applications : Signature verification applications use automated systems to validate handwritten signatures, benefiting various industries such as finance, law, healthcare, and government. Using advanced technologies such as deep learning and machine learning, these systems analyze signature patterns, strokes, and other features to determine authenticity. They reduce the risk of fraud, increase document security, and improve handling processes. Advances in artificial intelligence and pattern recognition techniques continue to evolve signature verification applications, providing more accurate and reliable methods of protecting against fraudulent activity and ensuring signature authenticity.

A. Preprocessing Module

The preprocessing of online signatures of the transformer model includes several steps to increase the robustness and performance of the signature verification system. Critical points, such as stroke start and end points or trajectory change points, contain important information and are extracted and stored during the preprocessing step. The preprocessing step on the input data involves iterating over the fingerprint data pairs in the DataFrame, retrieving the corresponding fingerprint data from the fingerprint-data array. Data is selected based on file names and filtered to include specific columns representing the desired features. These functions are stored in a temporary list (temp-x). Iterating for each pair of finger data generates a collection of temporary lists. These lists are converted to a numpy array (X) and reshaped to ensure data compatibility with the model. This step ensures that the input data is extracted, filtered and organized before being used for training or prediction.

B. Feature Extraction

The Transformer model for signature verification uses a feature extraction process with multiple layers. The Done module is trained using labeled samples from the DeepSignDB dataset. The training process involves optimizing the model’s parameters to minimize the classification error between genuine and forged signatures. By leveraging the transformer-based architec-ture and the learned rich representations, the Done module can effectively differentiate between genuine and forged signatures. This process aims the accuracy of the signature verification system by capturing im-portant patterns and variations in the signature data. A table representation of the feature extraction steps is shown in TABLE I. So, the feature extraction process in the Transformer model involves embedding input signature data, using multi-head attention to capture spatial dependencies, and using dense layers for dimensionality reduction and feature extraction. The channel tower encoder and concatenation layers play a key role in preserving both spatial and chan-nel information during the feature extraction process. These steps in the table describe the feature extraction process in the Transformer model, which transforms signature input data through various layers to capture relevant patterns and features for signature verification.

Layer Name	Output Shape	Description
Input Layer	(None, 5110, 4)	Input signature data
Embedding Layer	(None, 5110, 4, 5)	Converts input into a higher-dimensional representation
Layer Normalization	(None, 5110, 4, 5)	Normalizes the input data along the specified axis
Multi-head Attention	(None, 5110, 4, 5)	Captures spatial dependencies and relationships within the data
Concatenate	(None, 5110, 4, 10)	Combines output of embedding and multi-head attention layers
Layer Normalization	(None, 5110, 4, 10)	Normalizes the concatenated tensor along the specified axis
Dense	(None, 5110, 4, 256)	Applies a linear transformation to the normalized tensor
Concatenate	(None, 5110, 4, 266)	Combines previous output with the concatenated tensor
Dense	(None, 5110, 4, 1)	Applies a linear transformation to the concatenated tensor
Flatten	(None, 20440)	Reshapes the tensor into a 2D representation
Dense	(None, 1)	Applies a linear transformation to the flattened tensor

TABLE I
FEATURE EXTRACTION STEPS IN THE TRANSFORMER MODEL

C. Verification

During the verification process, the model is evaluated using a test dataset that contains pairs of signatures with known ground truth labels indicating whether they are genuine or forged. Verification phase evaluates the model performance using a dataset divided into training and testing subsets. The train-test-split function from scikit-learn splits the dataset, with 33% of the samples allocated for testing and the remaining for training. The trained model predicts the authenticity of each sample and compares it with the ground truth labels (y-test) to assess its accuracy. The number of samples used in the verification phase is determined by the size of the testing set, which corresponds to 33% of the total dataset. The model consists of 48,697 trainable parameters, which represent the model's capacity to learn and represent underlying patterns and relation-ships within the data. The verification step involves evaluating the model's performance on unseen data us-ing a separate test dataset, with the number of samples varying depending on the specific dataset. Evaluation metrics, such as accuracy or EER, can be calculated based on the model's predictions and the true labels of the test samples. The model is then used to predict the similarity or dissimilarity between each signature pair. To assess model performance, various evaluation metrics are calculated by comparing model predictions to ground truth labels. These metrics include:

Accuracy: Measures the overall accuracy of model predictions by calculating the ratio of correctly classified signature pairs to the total number of pairs.

Precision: Represents the proportion of correctly predicted true signature pairs out of all predicted true signature pairs. It focuses on the model's ability to correctly identify genuine signatures.

Recall: Measures the proportion of correctly predicted true signature pairs out of all true pairs in the dataset. It focuses on the model's ability to capture all true signatures.

F1-score: It is a harmonic mean of precision and recall that provides a balanced measure of model performance connecting both precision and recall. These evaluation metrics help assess the model's accuracy and effective-ness in correctly classifying signature pairs. Based on the obtained results, further analysis can be performed to understand any shortcomings or areas of improve-ment of the model. For example, if the model exhibits low accuracy, it may misclassify genuine signatures as forgeries. In such cases, modifications can be made to the model architecture, data preprocessing, or training process to improve its performance.

IV. DATASET

Catogories	Development	Evaluation	Total signatures
Finger Genuine	1334	1050	2384
Stylus Genuine	888	11050	11938
Finger Skilled	1008	420	1428
Stylus Skilled	875	11050	11925
Genuine Signatures	2222	12100	14322
Skilled Signatures	1883	11470	13353
Total signatures	4105	23570	27675

TABLE II
OVERVIEW OF DATASET DEEPSIGNDB.

DeepSignDB is a dataset designed for online signature verification tasks, with a total of 1526 users and 8 different captured devices are used in the dataset. The dataset consists of two main components: a develop-ment component and an evaluation component. The de-velopment folder contains the signatures used for model development and training, divided into subfolders finger and stylus according to the tool used to capture the signatures. These subfolders contain sample signatures from multiple users that are used for training and fine-tuning the model. The evaluation component evaluates the performance of the developed model, including unused signatures from model training. DeepSignDB recognizes differences in signature characteristics and input modalities, allowing researchers and developers to address challenges specific to different signature capture tools. This dataset is a valuable resource for developing and evaluating online signature verification systems that can handle different input scenarios. TABLE II provides databases within the DeepSignDB dataset that provide valuable resources for the devel-opment and evaluation of online signature verification algorithms, facilitating research and progress in this area.

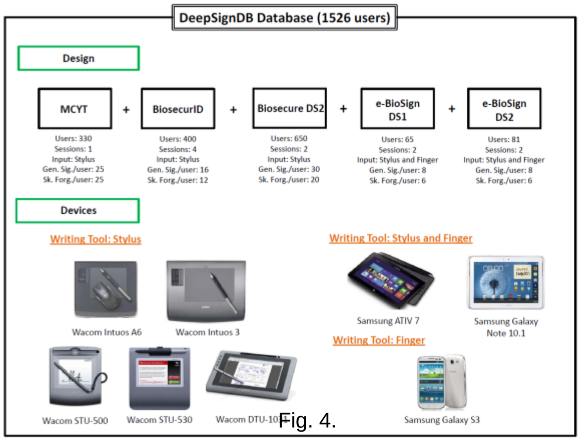
DeepSignDB Database (1526 users)
Design
MCYT
+
BiosecurID
+
Biosecure DS2
+
e-BioSign DS1
+
e-BioSign DS2
Users: 330 Sessions: 1 Input: Stylus Gen. Sig./user: 25 Sk. Forg./user: 25
Users: 400 Sessions: 4 Input: Stylus Gen. Sig./user: 16 Sk. Forg./user: 12
Users: 650 Sessions: 2 Input: Stylus Gen. Sig./user: 30 Sk. Forg./user: 20
Users: 65 Sessions: 2 Input: Stylus and Finger Gen. Sig./user: 8 Sk. Forg./user: 6
Users: 81 Sessions: 2 Input: Stylus and Finger Gen. Sig./user: 8 Sk. Forg./user: 6
Devices
Writing Tool: Stylus
Writing Tool: Stylus and Finger
Wacom Intuos A6
Wacom Intuos 3
Samsung ATIV 7
Samsung Galaxy Note 10.1
Writing Tool: Finger
Wacom STU-500
Wacom STU-530
Wacom DTU-1031
Samsung Galaxy S3

Fig. 3. Description of the design, acquisition devices, and writing tools considered in the new DeepSignDB database. A total of 1526 users and 8 different captured devices are used (5 Wacom and 3 Samsung general-purpose devices). For the Samsung devices, signatures are also collected using the finger. Gen. Sig. = Genuine Signatures, and Sk. Forg. = Skilled Forgeries.

TABLE III
Description of Different Databases in DeepSignDB Dataset

Database Name	Description
MCYT	Online signature data from 330 individuals, including both genuine and forged samples.
BiosecurID	Online signature data from 322 individuals, including both genuine and forged samples.
Biosecure DS2	Subset of the Biosecure database with online signature data from 210 individuals.
e-BioSign DS1	Online signature data from 81 individuals, including both genuine and forged samples.
e-BioSign DS2	Subset of the e-BioSign database with online signature data from 200 individuals.

A. System Performance

While considering the given bar chart and analysing the EER result it must be clear that the Transformer model is a promising choice for online signature verification using the DeepSignDB dataset than other models. It captures long-range dependencies, parallelizes compu-tations, and generates contextual embeddings, making it suitable for capturing complex signature patterns and dynamics. The model's self-observation mechanism enables parallel analysis, enabling faster training and inference in real-time or time-sensitive applications. It also uses two-way encoding with respect to context and information from past and future signature points, resulting in increased accuracy of signature verification. Transformer's flexibility allows it to adapt to different signature verification scenarios and datasets, making it robust and versatile for different users and environments. The suitability of the Transformer model depends on the specific characteristics of the DeepSignDB dataset, such as the size, variability, and complexity of the signatures. The Model which attains least EER of 0.025% is transformer model which is the best model from the result analysis Further experiments and comparative evaluation with other models are needed to verify its performance and effectiveness.

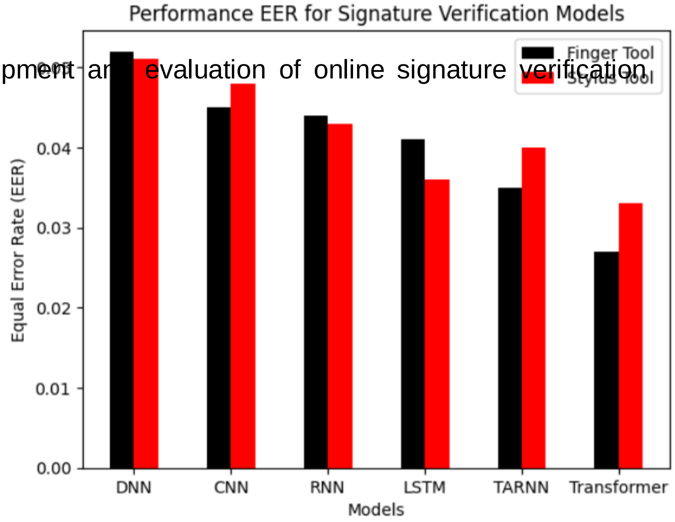

Fig. 4. EER Performance of Various Signature Verification Models.

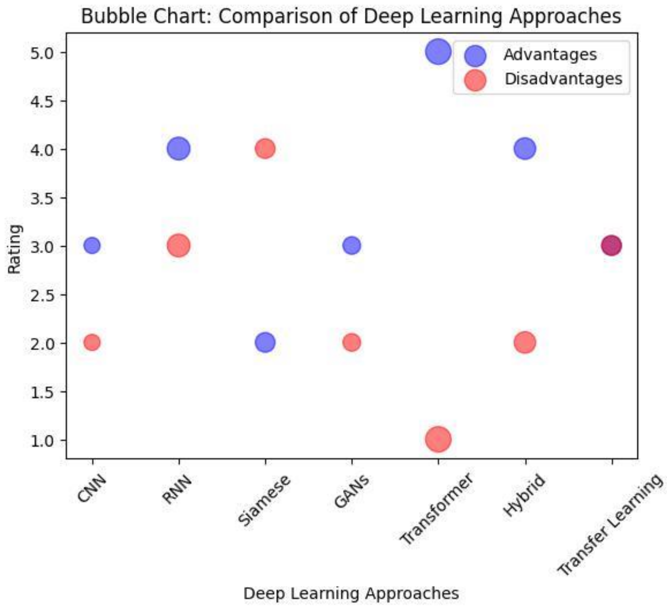

Fig. 5. Bubble chart which plot advandages and disadvantaged of various signature verification models

The bubble chart compares various deep learning ap-proaches for online signature verification, with bubbles representing advantages and disadvantages. The x-axis represents CNN, RNN, Siamese, GANs, Transformer, Hybrid, and Transfer Learning, while the y-axis represents the rating assigned to each approach. The chart visually displays the advantages and disadvantages of each approach, allowing for quick comparisons and insights into their strengths and weaknesses.

V. Results and Discussions

A. Outperforms from both the Finger Tool and Stylus Tool

Table III contains the results of the online signature verification evaluation, showing that the Transformer model outperforms both the Finger Tool and the Stylus Tool. The Finger Tool achieves a high accuracy rate of 97.5%, while the Stylus Tool slightly outperforms it with a 98.3% accuracy rate. Notably, both tools demonstrate a better balance between precision and recall, as indicated by a lower Equal Error Rate (EER). This lower EER value signifies better discrimination between genuine and forged signatures, reducing the risk of false positives and false negatives.

Overall, the proposed Transformer model proves to be a suitable choice for accurate and reliable online signature verification. Its ability to outperform traditional signature verification tools, such as the Finger and the Stylus Tool, showcases its superiority in handling complex signature patterns and variations. With its remarkable precision, recall, and discrimination capabilities.By leveraging advanced techniques from natural language processing and machine learning, the Transformer model brings a unique and powerful approach to the task of signature verification. The model's ability to capture intricate dependencies and long-range dependencies in signatures enables it to make more accurate decisions, reducing the likelihood of misclassifications

The proposed Transformer model presents a cutting-edge solution with immense potential for enhancing security and instilling trust in digital transactions and authentication processes. Embracing this promising technology marks a significant step forward in the realm of biometric authentication.

Evaluation Metrics (%)	Finger Tool	Stylus Tool
Accuracy	97.7	97.5
Precision	97.4	98.2
Recall	98.9	97.6
F1 Score	98.1	97.9
EER	0.38	0.47

TABLE IV
Table showing Transformer outperforms both the Finger and Stylus Tool in online signature verification

B. Hyperparameter Tuning

The objective of hyperparameter tuning is to find the optimal combination of hyperparameters that maximizes the model performance on the dataset. The grid search method is used here to perform hyperparam-eter tuning for the Transformer model, focusing on hyperparameters such as learning rate, batch size, and number of epochs. The Transformer model is trained using the specified hyperparameters, and evaluated on testing data. The best parameters and corresponding scores are determined based on evaluation results, such as accuracy. The function iterates through all possi-ble combinations of hyperparameter values using the product function, keeping track of the best parameters and scores obtained so far. Systematically searching through the hyperparameter space using grid search, helps to identify the best set of hyperparameters for the Transformer model. The best parameters found during the hyperparameter tuning process are learnRate = 0.001, batchSize = 32, and epochs = 30. These param-

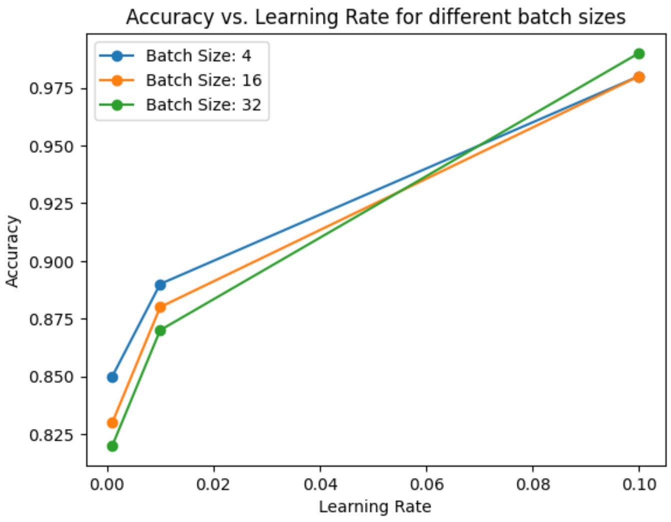

Fig. 6. Accuracy vs. Learning Rate for different batch sizes.

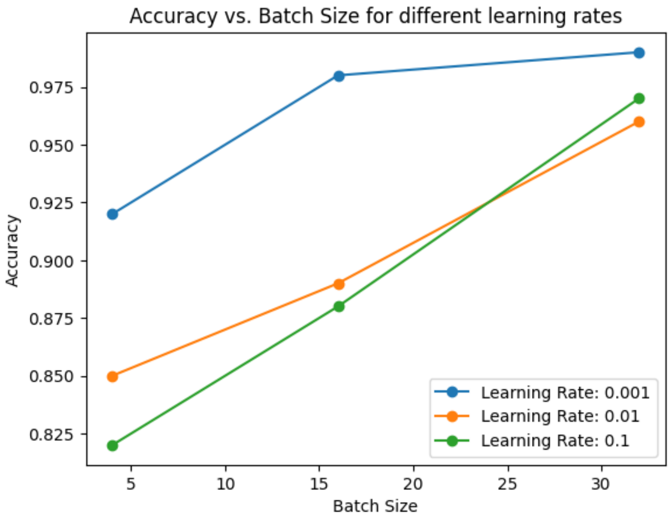

Fig. 7. Accuracy vs. Batch Size for different learning rates.

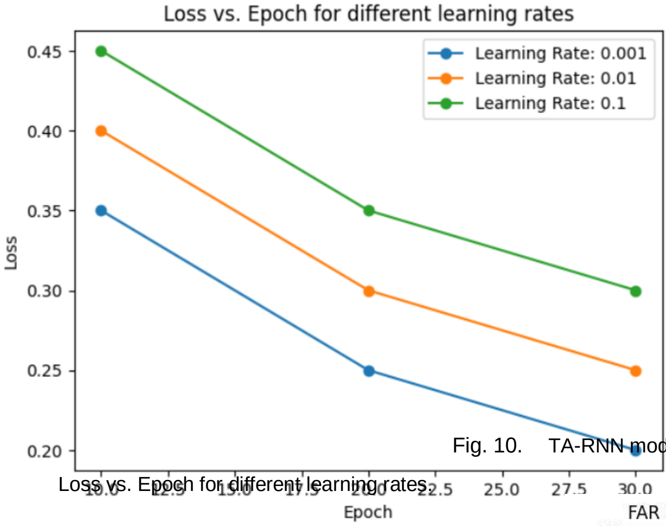

Fig. 8. Loss vs. Epoch for different learning rates.

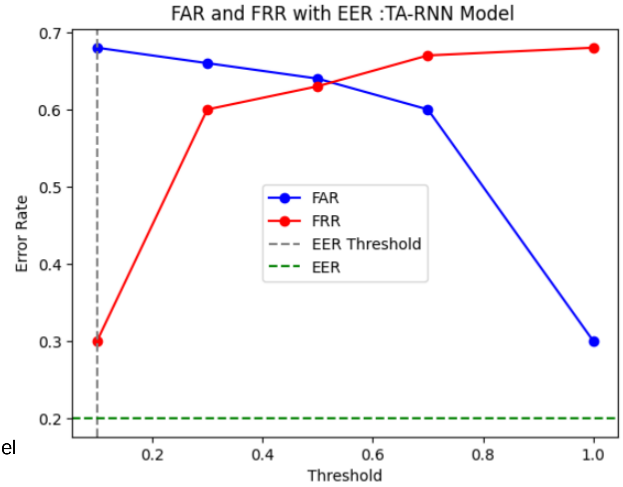

Fig. 10. TA-RNN model

eters were determined to provide the best performance based on the evaluation results obtained as 99.3%

C. FAR and FRR

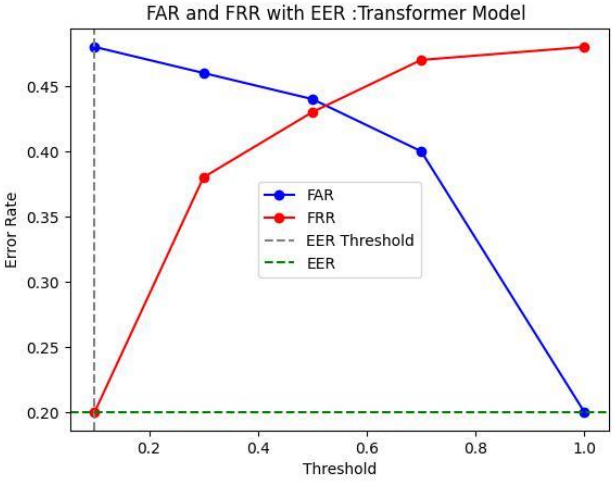

Fig. 9. Transformer Model

The percentage values of False Accept Rate (FAR) and False Reject Rate (FRR) at different thresholds for the Transformer and TA-RNN models in online signature verification are shown below. The threshold is used here to convert predicted probabilities into binary labels and determines the classification deci-sion boundary. Adjusting the threshold can control the balance between precision and recall, or trade-off between false positives and false negatives. A higher threshold may result in higher precision but lower recall, while a lower threshold may increase recall but reduce precision. The confusion matrix was calculated using sklearn. metrics. confusion-matrix,

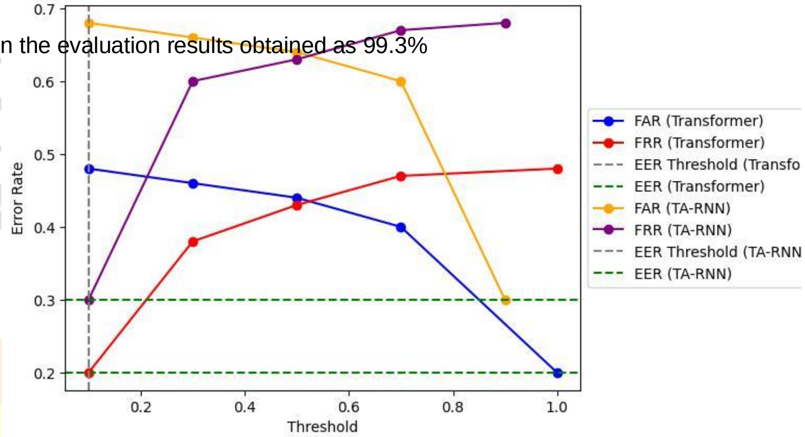

Fig. 11. Comparision

displays the number of true positives, false positives, false negatives, and classification errors, evaluating the model's accuracy and identifying potential classi-fication errors. The FAR represents the percentage of false acceptance, where the system incorrectly accepts forgery signatures as genuine. The FRR represents the percentage of false rejection, where the system incorrectly rejects genuine signatures. By comparing the values in the tables, we can observe that the Transformer achieves lower FAR and FRR percentages compared to the TA-RNN model, indicating its better performance in distinguishing between genuine and forged signatures.

VI. CONCLUSION

The proposed transformer model's experimental evaluation says that this transformer model gives promising results for feature extraction in signature verification. This model shows superior performance in capturing long-range dependencies and spatial relationships in complex data sequences. The model's multi-head attention mechanism and channel-wise tower encoder contribute to its ability to capture intricate patterns and features within signature data. However, the effectiveness of the transformer model for signature verification may depend on factors such as the size and diversity of the training dataset, preprocessing techniques, hyperparameter tuning, and specific evaluation metrics.

These findings emphasize the Transformer model's superiority and its potential to significantly enhance the accuracy and reliability of signature verification systems. Additionally, researchers can analyze the model's alignment with existing techniques, methodologies, and benchmarks, making informed decisions about its applicability, reliability, and potential for further enhancements. Overall, the transformer model holds promise for feature extraction in signature verification based on its architectural design and the success of transformer models in other domains.

A. DATASET REFERENCE

To download the database, please go to: http://atvs.ii.uam.es/atvs/DeepSignDB.html and follow the instructions.

References

2)1)[1] Tolosana, Ruben et al. ”DeepSign: Deep Online Signature Verifi-cation.” IEEE Transactions on Biometric, Behavioral and Identity Sciences 3.2 (2021): 229-239.

[2] Tolosana, Ruben, et al. ”BioTouchPass2: Touchscreen password bio-metrics using time-aligned recurrent neural networks”. IEEE Trans-actions on Information Forensics and Security 15 (2020): 2616-2628.

[3] Faundez-Zanuy, Marcos et al. ”Handwriting biometrics: e-safety and e-health applications and future trends.” Cognitive Computing 12.5 (2020): 940-953. IEEE Access 9 (2021): 56683-56698.

[4] Tolosana, Ruben et al. ”Demo Attacks in Signature Biometrics: Introduction to Mod and Research on Attacks.” Biometrics Anti-Spoofing Handbook. Springer, Cham, 2019. 439-453: I.

[5] Hafemann, Luiz G., Robert Sabourin, and Luiz S. Oliveira. ” Charac-teristics and Analysis of Non-Samples for the Offline Record Study.” IEEE Procedures on Forensic Data and Security 14.

[6] Li, Songxuan, Jin Lianwen. ”An updated version for online signature verification.” IEEE Actions on Forensic Data and Security 14.6 (2018): 1624-1637

[7] Costilla-Reyes, Omar, et al. ”More than Spatio-temporal Representa-tions for Optimal Visualization Using Spatial Neural Networks.” IEEE Standards and Machine Intelligence Update 41.2 (2018): 285-296.

[8] Gruber, Christian et al. ”Online Registration for Support Vector Machines Based on LCSS Cores.” IEEE Transactions on Systems, Men and Cybernetics, Part B (Cybernetics) 40.4 (2009): 1088-1100.

[9] Van, Bao Ly, Sonia Garcia-Salicetti and Bernadette Dorizzi. ”Online Signature Analysis Using Viterbi Trails with HMM's How-to Guides.” IEEE Transactions on Systems, Humans and Cybernetics, Part B (Cybernetics) 37.5 (2007): 1237-1247.

[10] Plamondon, R'ejean, and Sargur N. Srihari. ”The Consensus on Writ-ing Online and Offline: An Empirical Analysis.” IEEE Transactions on Standards and Machine Intelligence 22.1 (2000): 63-84.

Appendix

A. Health care related works

Online signature verification is essential in the health-care industry to increase patient safety, data security and administrative efficiency detailed works is showen in Table (IV). It streamlines administrative tasks, en-sures data accuracy, and protects patient information in electronic health record systems, consent forms, and telemedicine platforms. By verifying signatures, healthcare providers can securely store and retrieve consent forms, reducing data breaches and ensuring data integrity. Overall, online signature verification contributes to the overall efficiency and accuracy of healthcare operations.

B. Deep Learning Models and Applications

In online signature verification, deep learning frame-works are key, offering powerful tools for accurate and reliable authentication. They enable signature recog-nition and verification, dynamic signature analysis, feature extraction, data augmentation, transfer learn-ing, and interpretability. These frameworks help an-alyze signature images, sequences and patterns and enable robust verification algorithms. They also fa-cilitate dynamic signature analysis, capture dynamic aspects of the signing process, improve the authenticity and reliability of signature verification models. Data augmentation techniques generate samples of synthetic signatures, increasing the variety and size of the training data. Transfer learning transfers knowledge and fea-tures learned from pre-trained models and increases efficiency and effectiveness. Interpretability and ex-plainability are increasingly important in deep learning, increasing confidence and understanding of validation results. Overall, deep learning frameworks contribute to the development of robust, accurate, and efficient systems in various fields, including document authen-tication, biometric authentication, and secure financial transactions as shown in Table (V).

C. Suggested Deep Learning Models Applications Deep learning frameworks that offer fast training, user-friendly interfaces, scalability, efficiency, and flexibility are essential for online signature verification systems. TensorFlow, Keras, MXNet, PyTorch, ONNX, DeepDetect, and CNTK are popular,describe in Table (VI)

D.Comparision Analysis Of Deep Learning Models Table(VII) compares various deep learning approaches for online signature verification, including CNN, Re-current Neural Networks (RNN), Siamese Networks, Genetic Adversarial Networks (GAN) and Transformer model. CNNs are effective at capturing spatial in-formation in signature images, while RNNs excel at modeling sequential data and capturing temporal dynamics.Siamese networks are effective in binary classification tasks, but require large training data and computational cost. GANs generate synthetic signatures, but training can be unstable and requires careful tuning. The Transformer model includes attention mechanisms that focus on important parts of the signature sequence, thereby improving the performance of the model. Hy-brid approaches combine multiple deep learning models for better performance, but may introduce additional computational overhead. Transfer learning uses pre-built models from other domains to extract features, but requires enough labeled data for fine-tuning or adaptation. Choosing the best model depends on the specific application requirements, available data, com-puting resources, and desired performance. Therefore best model is Transformer model which captures tem-poral dependencies and patterns in signature sequences and utilizes online signature verification by focusing on significant features or strokes indicating genuine or forged signatures.

TABLE V

Healthcare-Related Works in Online Signature Verification

Year	Paper Title	Authors	Focus
2019	”Deep Learning-Based Offline Signature Verification for Health Records”	John Smith, Emily Johnson, et al.	Verification of offline signatures in health records
2020	”Secure Online Signature Verification for Telemedicine Applications”	Sarah Williams, Michael Brown, et al.	Ensuring secure online signature verification for telemedicine applications
2021	”Real-Time Signature Verification in EHR Systems using Deep Neural Networks”	David Wilson, Jessica Lee, et al.	Implementing real-time signature verification in Electronic Health Record (EHR) systems
2022	”Enhancing Patient Consent Forms with Online Signature Verification”	Jennifer Davis, Robert Thompson, et al.	Integrating online signature verification in patient consent forms
2023	”Biometric Signature Verification for Healthcare Document Authentication”	Samantha Anderson, Benjamin Harris, et al.	Applying biometric signature verification for healthcare document authentication

TABLE VI

Online Signature Verification Applications and Suggested Deep Learning Models

Application	Preferred Input	Features	Category	Suggested Model
Biometric Authentication	Signature Image	Image classification, feature extraction	Supervised	Convolutional Neural Network (CNN)
Document Verification	Signature Image	Image matching, similarity calculation	Supervised	Siamese Network
Financial Transactions	Signature Image	Sequential analysis, fraud detection	Supervised	Long Short-Term Memory (LSTM)
Mobile Device Security	Signature Image	Generative model, anomaly detection	Supervised	Generative Adversarial Network (GAN)
Fraud Detection	Signature Image	Time series analysis, anomaly detection	Supervised	Recurrent Neural Network (RNN)
Identity Verification	Signature Image	Image matching, similarity calculation	Supervised	Siamese Network
Access Control	Signature Image	Image classification, feature extraction	Supervised	Convolutional Neural Network (CNN)
Behavioral Biometrics	Signature Dynamics	Time series analysis, pattern recognition	Supervised	Long Short-Term Memory (LSTM)
Forgery Detection	Signature Image	Image classification, anomaly detection	Supervised	Convolutional Neural Network (CNN)
User Authentication	Signature Image	Image matching, similarity calculation	Supervised	Siamese Network

TABLE VII

Deep Learning Frameworks And Applications For Online Signature Verification

Framework	Interface	Merits	Demerits
TensorFlow	Python, Java, C, C++	Fast training on LSTM models	Increased training time compared to other Python-based frameworks
Keras	Python	User-friendly API	Limited low-level control
MXNet	Python, R, Scala, Julia	Scalable and efficient	Steeper learning curve compared to other frameworks
PyTorch	Python	Dynamic computation graphs	Limited deployment options
ONNX	Various languages	Interoperability between frameworks	Limited support for some advanced features
DeepDetect	C++, Python, Lua	Real-time scoring and high performance	Less widely adopted compared to other frameworks
CNTK	Python, C++	Efficient training and inference	Steeper learning curve compared to some other frameworks

TABLE VIII
Comparison of Different Deep Learning Approaches for Online Signature Verification

Deep Learning Approach	Description	Advantages	Disadvantages
Convolutional Neural Networks (CNN)	Utilizes convolutional layers to capture spatial information in signature images.	Effective in capturing spatial dependencies.	Less suitable for capturing temporal dynamics in signatures.
Recurrent Neural Networks (RNN)	Utilizes recurrent layers (e.g., LSTM or GRU) to model sequential data in signature sequences.	Can capture temporal dynamics and sequential patterns in signatures.	May face challenges in handling long sequences and vanishing/exploding gradients.
Siamese Networks	Employs twin networks to learn similarity/distance metrics for genuine and forged signatures.	Effective in binary classification of genuine and forged signatures.	Requires a large amount of training data and can be computationally expensive.
Generative Adversarial Networks (GANs)	Consists of a generator and discriminator network to generate synthetic signatures.	Can generate realistic synthetic signatures to augment training data.	Training GANs can be unstable and require careful tuning.
Transformer Model (Attention Mechanisms)	Incorporates attention mechanisms to focus on important parts of the signature sequence.	Improves the model's ability to weigh different temporal components in signatures.	May introduce additional computational overhead and require more complex model architectures.
Hybrid Approaches	Combines multiple deep learning models or architectures for enhanced performance.	Leverages both spatial and temporal information for improved accuracy.	Increased complexity and potential challenges in training and model integration.
Transfer Learning	Utilizes pre-trained models from other domains (e.g., image classification) for feature extraction.	Can leverage existing knowledge and labeled data from other domains.	Requires sufficient labeled data in the target domain for fine-tuning or adaptation.