VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 2, April-June 2024 *pp:231-240*

A Comparative Analysis of Machine Learning Algorithms for Online Signature Recognition

Mehwish Leghari[1], **Asghar Ali Chandio**[2*], **Muhammad Ali Soomro**[3], **Shah Zaman Nizamani**[4], **Muhammad Hanif Soomro**[5]

[1]Department of Data Science, Quaid-e-Awam University of Engineering, Science Technology, Pakistan; [2*]School of Engineering and Information Technology, University of New South Wales, Canberra, Australia; [2*]Department of Artificial Intelligence, Quaid-e-Awam University of Engineering, Science & Technology, Pakistan; [3]Department of Computer Systems Engineering, Quaid-e-Awam University of Engineering, Science & Technology, Pakistan; [4]Department of Information Technology, Quaid-e-Awam University of Engineering, Science & Technology, Pakistan; [5]Department of Information Technology, Sindh University at Mirpur Khas, Pakistan

Keywords: *Online signature identification, dynamic signature recognition, biometric signature verification, signature identification using machine learning.*

Journal Info:
Submitted:
April 27, 2024
Accepted:
May 16, 2022
Published:
June 30, 2024

Abstract

Biometrics recognition plays a vital role in modern human recognition and verification systems. An extensive latest research by the research community has rendered the field of biometrics inevitable for real-life applications. This research study focuses on online signature recognition. The research study is performed to identify if an online signature is genuine or forged. A novel online signature dataset, based on 1000 online signatures, has been collected from 200 participants, wherein every participant provided 5 instances of the online signature. An Android-based mobile application was developed to collect the online signature data. Moreover, a data augmentation technique was used to increase the training samples of the online signature dataset. Some common features such as the width and height of the signature, x and y coordinate values, pressure, pen ups and pen downs, total duration of the signature, etc were extracted. The dataset has been trained and tested using machine-learning techniques. The performance of the five existing classifiers on the newly collected database has been compared. The classifiers used for training and testing included a Support Vector Machine (SVM), a Random Forest Classifier (RFC), a variant of RFC called an Extra Tree Classifier (ETC), a Decision Tree Classifier, and K-Nearest Neighbours. The performance of each classifier was evaluated in terms of precision score, recall score, and f-1 score. The RFC, and ETC classifiers gave an overall classification accuracy of 96%.

***Correspondence author email address:** asghar.ali@quest.edu.pk,z5122075@zmail.unsw.edu.au

DOI: 10.21015/vtse.v12i2.1845

This work is licensed under a Creative Commons Attribution 3.0 License.

1 Introduction

The biometrics can be defined as the technical term for the measurements and calculations of the human body. Research in biometrics recognition has reached various milestones and nowadays, biometrics recognition is part of the daily life of people in most of the developed and developing countries [1]. From attendance systems, Automated Tailored Machines (ATMs), and mobile phones to surveillance systems, forensics, and border control, biometrics are in use everywhere for reliable authentication and identification. A biometrics confirmation system usually works in two steps: one is to register the user in the biometrics system, and the other is to verify the user on the basis of data provided in the registration step [1]. Furthermore, biometrics can broadly be divided into two primary types: Physiological biometrics and behavioural biometrics. The Physiological biometric can be described as the measurement of the physical dimensions of a human body like face, fingerprint, iris and hand geometry. Behavioural biometrics can be defined as the behaviour of the human while accomplishing some tasks like signature, voice, and keystroke dynamics. The physiological biometric systems based mainly on the fingerprints, iris and facial recognition are a part of the daily life systems in many developed countries [2] [3].

The physiological biometrics on the one hand may obtain very high recognition accuracies but on the other hand are more prone to security attacks and spoofing. Keeping in view the security threats to the privacy of a user's biometrics it is very important to not only ensure the security of the databases but it is also essential to search for the other means for the security. Even in today's era sometimes the data inside the databases are stored in unencrypted form. That type of storage is highly vulnerable to security breaches. One of the important breaches in security in 2019 was found by some experts of the security researchers while working on the database named as "BioStar 2" [4]. The database belongs to one of the famous security manufacturer company named "Suprema". The database contained fingerprints, facial recognition data accompanied by personal information, usernames, and passwords. Data belonged to 5700 companies from 83 companies including United States of America, the United Kingdom, Germany, Japan, Turkey, Finland, Belgium, Indonesia, India, Sri Lanka, the United Arab Emirates, and many other countries of the world. The reason is that most of the physiological biometrics are inherently public in nature. Our face, fingerprint, or iris are visible to the public and hence can be captured, re-created, and reused by anyone. However, the behavioural biometrics are more private to the owner and cannot be easily copied or re-created [5] [6].

To ensure the biometric verification system safe from spoof attacks, it should be considered to use the behavioural biometrics systems [7]. This research uses online signatures as biometric identification. Using an online signature has additional advantages over the offline signature. The online signature preserves much more information, while the offline signature only keeps the overall structure of the signature. It is capable of storing some of the most important attributes like the starting points of the signature, ending point of the signature, distance between the first and last point of the signature, width of the signature, height of the signature, speed of the signature, total time taken by a person to make the signature, pressure applied against the touch screen while making the signature, total number of pen-ups and total duration for the pen-ups.

Several digital devices are available to capture the online signature. Some devices are stylus-based, while others are both the stylus and the fingertip-based [8]. Figure 1 illustrates some devices commonly used for online signature capture.

Thus, keeping in view the importance and efficiency of the online signature, this research study focuses on online signature identification using a newly collected dataset. This research basically compares the performance of five existing machine-learning algorithms on a newly collected dataset. Furthermore, the classification results obtained are compared with the existing research work performed for online signature recognition. The remainder of the paper is arranged as follows: Section II throws light on the review from some

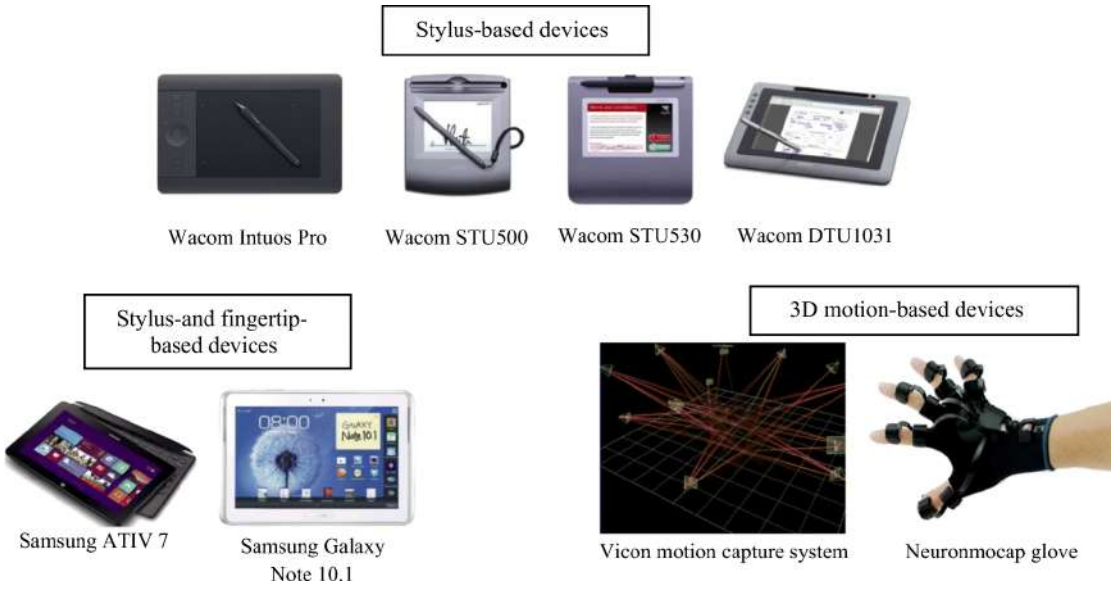

Figure 1. Smart devices used to capture online signature [8].

of the relevant research work, Section III highlights the benchmark dataset collected for this research, the experimental setup and the results achieved by performing different experiments are discussed in section IV, while section V describes the conclusion of the paper with some future research direction discussed in section VI.

2 Related Work

The literature presents a rich work in the field of signature recognition. The accuracy of a signature recognition system has been improved up to a level of satisfaction, on the reliability of a signature recognition system. Recently, Dhieb et. al., [9] achieved an Equal Error Rate (EER) of as low as 0.9% on the MCYT-100 dataset, while Wei, et al., [10] achieved an ERR of 0.05%. Similarly, Okawa proposed a single template by applying the mean template and the weighted DTW for online signature verification [11]. Carlos Alonso-Martinez and Marcos Faundez-Zanuy fused the online signature with handwriting recognition to increase the accuracy even more [12]. For handwriting recognition, an accuracy of 86.11% has been achieved and for online signature, the accuracy of 96.9% has been achieved. After fusing the handwriting with an online signature, an accuracy of 99.7% was achieved. Singhal and Shinghal [13] combined the online signature and face feature for a multimodal biometrics authentication system. They used the x and y coordinate values, azimuth, pressure, time stamp, and altitude information for the online signature, while for the face image, a modified context-aware technique where the mouth, nose, eyes, and the texture areas of the face were considered for the feature extraction. In 2019 Jia et. al [14] proposed a new technique based on dynamic time warping for online signature matching. Their proposed technique works on the shape of the signature and they named the technique as shape context-dynamic time warping (SC-DTW). They tested the technique on SVC2004 database and achieved an EER of up to 2.39%. The researchers are also working on the feature selection process for online signatures. Shekhar et. al [15] proposed the feature selection for online signatures that are specific to the writer of the signature. They achieved the lowest EER in different categories (a detailed discussion of the categories and various EER obtained is beyond the scope of this research.), while they performed the experiments on the four most common state-of-the-art datasets of the online signatures. The research community is also working on deep neural networks to train the classifiers on online signatures. Mohammad Hajizadeh

Saffar tested a deep neural network on the publicly available dataset and obtained an Equal Error Rate (EER) of as low as 0.77%. Some of the researchers also suggest that human intervention has an important role in improving the efficiency of online signature recognition [16] [17], [18], [19]. These systems suggest the importance of the role of the human being in signature recognition systems.

In contrast with offline signatures, there are comparably a few databases available for research in online signatures. Different databases are already available like "eBioSignDS1signature" database [20]. This database is from "Biometrics Research Group ATVS Universidad Autonoma de Madrid, Spain". It contains a total of 490 online signatures from 35 subjects. Each subject contributed 14 signatures. Similarly "sigComp2011-trainingSet" is also publicly available [21] for the research purpose. This dataset is from a well-known forum "ICDAR 2011 Signature Verification Competition (SigComp2011)". It comprises 240 online signatures in total from 10 subjects. Each subject contributed 24 signatures. A hybrid dataset of online signatures and fingerprints was collected in [22] and [23] for multimodal biometric recognition. Furthermore, the recent advancements in the field of biometrics systems particularly focusing on signature verification have been described in [24]. Keeping in view of scarcity of online signature databases available for research, a novel dataset has been collected for this research.

3 Benchmark Dataset

An online signature dataset was collected for this research. The dataset samples were collected from undergraduate students of three different Universities in the Sindh including Quaid-e-Awam University of Engineering, Science and Technology located at Nawabshah, Sindh Agriculture University located at Tandojam, Campus of Sindh University located at Mirpurkhas and the campus of Sindh University located at Dadu city. The students who participated in the data collection ranged in age from 19 to 23 years.The dataset consists of 1000 online signatures from 200 subjects in total. Each subject contributed 5 samples of their online signature.

An Android based application has been developed to collect the online signatures from various persons. That application has been used to collect the online signatures using Samsung Galaxy Note 3 with S-Pen. Figure 2 depicts the application developed for the data collection of the online signature. The subjects were requested to make 5 signatures on the surface of the Samsung Galaxy Note 3 with the S-Pen. The developed application was able to store the 'x' and 'y' coordinates, pressure and time for each of the pixels of the signature drawn on the screen. Each of the participants provided 5 samples of their signature. Part of a sample from online signature template collected for this research is presented in Figure 3.

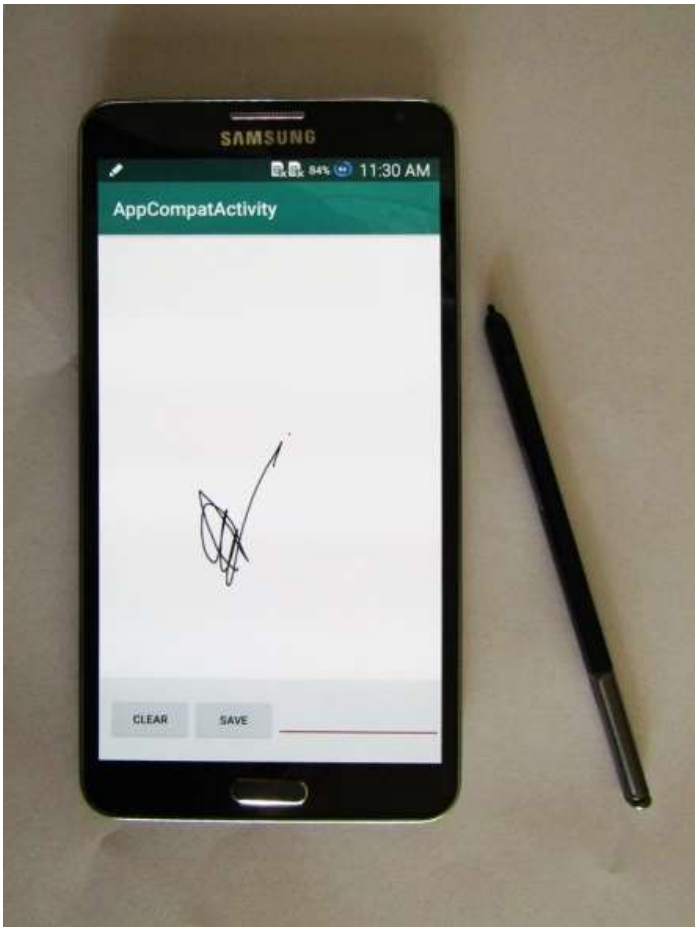

Figure 2. An interface of the mobile app developed for the collection of online signature data

To train a classifier, the data from different partici-

pants is kept in different classes. It is important to increase the number of samples in a class as the number of samples increases the classification accuracy. In this research, the number of participants is 200 and the number of samples in a class is 5. Learning from 5 samples of signatures for a class was also very difficult for any classifier, hence it was inevitable to perform the data augmentation for online signatures. As an online signature sample consists of a text file containing numerical features of the signature, hence the augmentation needed for the text file was also different in nature from the image file. From each original text file of an online signature, 2 augmented text files of the online signatures have been created. The text file for the online signature consists of x-coordinates, y-coordinates, pressure data, and time for the signature. Data augmentation has been performed using a simple code of python to read a file of online signature and changing the values of pressure, time, x and y coordinates to create new files. For each augmented file, the values of the x-coordinate and y-coordinate have been increased and decreased slightly to change the location and angles of the signature. Similarly, time has also been increased to make a new augmented file different from the original one. However, the pressure has been very slightly changed from the original pressure. In this way, 10 augmented files have been created from 5 original files for each class, making the number of samples 15 for each of the 200 classes. The dataset after applying the augmentation has become the 3000 online signatures.

4 EXPERIMENTS AND RESULTS

Experiments for this research have been performed in Python programming language on the Anaconda 3 platform using Scikit-learn open source machine learning library. The dataset is divided into two parts. 80% of the data is used for the training and 20% of the data is used for the testing purpose. The basic methodology of the online signature and verification system is depicted in Figure 4. It is clear from Figure 4 that an online signature recognition system may be divided into two basic steps named as signature registration or enrolment part and signature identification

173	840	0.18768328	20190806_11212467
173	840	0.18768328	20190806_11212467
171	840	0.19159335	20190806_11212469
171	840	0.19159335	20190806_11212470
171	840	0.19159335	20190806_11212470
171	840	0.19159335	20190806_11212470
171	840	0.19159335	20190806_11212470
171	844	0.19745846	20190806_11212471
171	844	0.19745846	20190806_11212471
176	854	0.24437928	20190806_11212473
176	854	0.24437928	20190806_11212473
185	870	0.28152493	20190806_11212474
185	870	0.28152493	20190806_11212475
196	891	0.3030303	20190806_11212476
196	891	0.3030303	20190806_11212476
209	914	0.31867057	20190806_11212478
209	914	0.31867057	20190806_11212478
223	935	0.32355815	20190806_11212479
223	935	0.32355815	20190806_11212479
223	935	0.32355815	20190806_11212480
239	962	0.32844573	20190806_11212481
239	962	0.32844573	20190806_11212481
248	975	0.34017596	20190806_11212483

Figure 3. Part of a text file representing a sample from the online signature database. Four columns represent the values for the x-coordinate, y-coordinate, pressure, and time respectively.

part. Each step is further divided into sub-steps. In the registration part, first, the signature is obtained by an input device. In this case online signature is acquired by a Samsung Galaxy Note 3 with S pen using an Android application developed especially for this research. The signature is stored in a text file that stores x-coordinates, y-coordinates, pressure, and time for each point of the signature. Once the signature is acquired, it is ready for preprocessing step. The preprocessing is performed on the online signature to make it usable for feature extraction. Preprocessing is performed by eliminating the repetition of the data. The data that is the same in all 4 columns of the online signature file has been eliminated by applying the built-in functions of Pandas library. Also, the zeros are appended (if applicable) at the end of the text file to make all files of the same size to feed those to the feature extraction algorithm. Once online

signatures are preprocessed, they are ready to be used for feature extraction. In this research, a simple feature extraction technique that is commonly used in computer vision problems is used. The technique is called Histogram of Oriented Gradients (HOG). A Histogram of Oriented Gradients (HOG) is basically for image data and the image is segmented into cells and the orientation of the pixel is computed for each cell. In this research, the best values were achieved for the orientation, blocks, and cells, after performing the experiments on different values for these attributes of HOG for the online signature file.

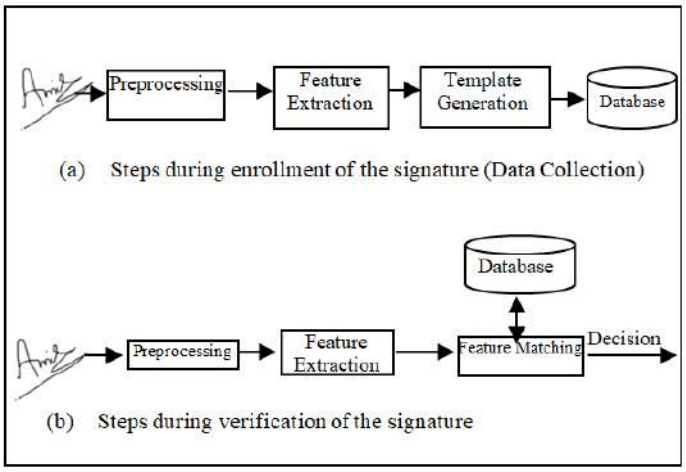

Figure 4. steps and sub-steps during (a) Enrolment Phase and (b) Verification Phase of online signature recognition system.

Feature extraction is the most important part of biometrics recognition, and it takes place during both the registration phase as well as the recognition phase. For that reason, the feature extraction part has been paid special attention during this research study. Different extracted features had noticeable variances among their values. For example on one hand the pressure for each pixel of the signature is represented by a fractional value between 0 and 1 while on the other hand x and y coordinates for the same pixel are represented by a three-digit value. To address the issue of variance between different features, the features scaling technique has been used to avoid the biasing of some of the features. It is ensured by feature scaling that all the features have been represented by the same scale so that all the features can play their role in training a classifier efficiently.

After the features from the online signature samples, the classifier has been trained with the 80% data from the data set. The remaining 20% of the data has been used for testing. Five different classifiers have been trained and tested for this research. The names of the classifiers are Support Vector Machine (SVM), Random Forest Classifier (RFC), Extra Tree Classifier (ETC), Decision Trees (DT), and the K-Nearest Neighbour (KNN). The classifiers were trained on the default hyperparameters as well as fine-tuned hyperparameters. The best results were achieved with the fine-tuned hyperparameters. Some of the potential limitations of this research are described as follows. This research study is limited to analysing five already existing machine learning algorithms on a newly collected dataset for online signature. The results of each of the classifiers are represented in terms of precision, recall f1-score, and accuracy. Table 1 depicts the results of each classifier in terms of precision, recall, f1 scores, and accuracy.

Table 1. Online Signature Identification Results for Different Machine Learning Classifiers

Classifier	Precision	Recall	F-Score	Accuracy
SVM	0.85	0.81	0.80	0.81
RFC	0.98	0.96	0.96	0.96
ETC	0.98	0.96	0.96	0.96
DT	0.94	0.92	0.93	0.93
KNN	0.90	0.88	0.88	0.88

The precision value achieved by RFC and ETC classifiers is 0.98 while it is 0.94, 0.90 and 0.85 with the DT, KNN, and SVM classifiers. The recall achieved by RFC and ETC is 0.96 while the DT, KNN, and SVM classifier yielded a recall value of 0.92, 0.88, and 0.81, respectively. Similarly, the RFC and the ETC achieved the f1-score of 0.96 while the DT, KNN, and SVM classifier achieved the f1-score of 0.93, 0.88, and 0.80, respectively. The overall testing accuracy for the classification of online signature achieved by DT, KNN, and SVM is 93%, 88%, and 81% while by the other two classifiers is 96%, respectively as illustrated in Figure 5. The con-

fusion matrix using RFC classifier for all 200 classes is presented in Figure 6 for this research.

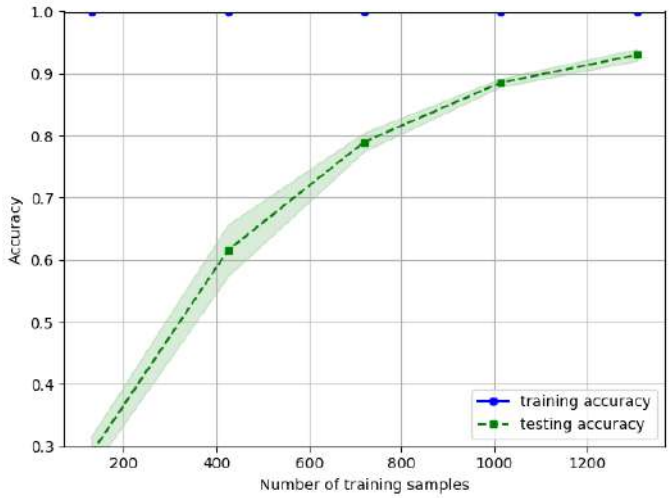

Figure 5. ROC curve representing training and testing accuracy for online signature identification.

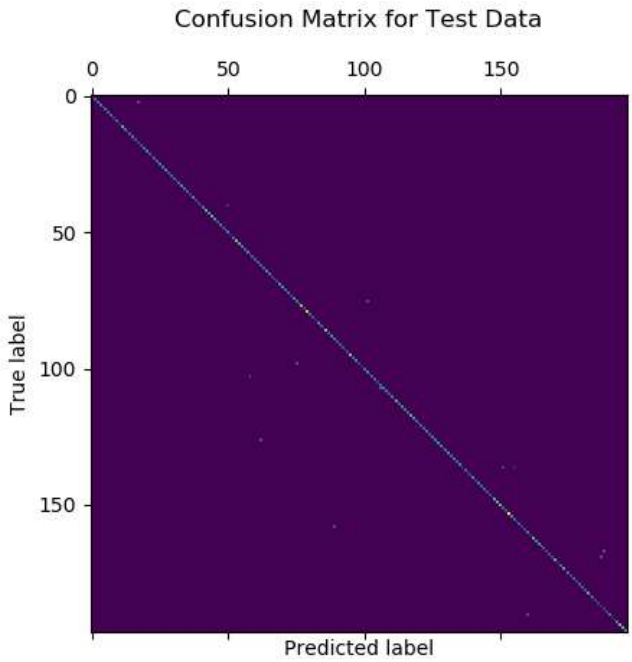

Figure 6. Confusion matrix for online signature identification.

4.1 Comparison with Online Signature Recognition

The performance of the machine learning classifiers on the collected online signature dataset has been compared with the existing machine learning-based online signature recognition systems. The performance has been compared in terms of precision, recall, f1-score, and accuracy. Table 2 compares the machine learning classifiers applied to the proposed dataset of online signatures with existing machine learning-based methods.

Khoh et al., [25] collected an on-air dataset of online signatures and applied an SVM to recognise the signatures. The dataset was collected from the 100 users who participated voluntarily. The overall accuracy reported in the results is 0.97, however, the precision, recall, and f-Scores are 0.94, 0.93, and 0.93, respectively. Compared to [25], the proposed online signature recognition method gives an overall accuracy of 0.96, however, the precision, recall, and f-score values are higher than [25].

Chang et al., [26] modified the AlexNet and obtained an accuracy of 0.96. After applying the transfer learning approach, the accuracy of the model was improved to 0.97. A dataset of 640 samples was used to train and test the model. Foroozandeh et al., [27] proposed a technique based on Dual-Tree Complex Wavelet Packet Transform to recognise and verify online signatures. The vertical, horizontal, and pressure signals were calculated and used as the features. The SVM and KNN were applied for signature recognition. The overall accuracy of the model reported is 0.83.

Ahrabian et al., [28] applied the autoencoder and the immense network to classify the signatures as genuine or forged. An attention-based method along with down-sampling was applied to further improve the classification accuracy. The model was evaluated on two different publicly available datasets and an average accuracy of 0.95 is reported in the results. Lupu et al., [29] extracted different feature matrices from three datasets and combined them for online signature verification and identification. Weka and LibSVM were used to perform the signature verification and identification task. An average accuracy of 0.95 is reported in the results.

Rasheed et al., [30] applied different feature de-

scriptors such as SIFT, SURF, FREAK, ORB, and others to detect the key-frames from the signature data. Furthermore, a CNN was applied to automatically extract the useful features from the signature data. An average accuracy of 0.95 and a precision score of 0.85 is obtained. Zeng et al., [31] proposed different models of deep learning including CNN, RNN, and CNN-RNN for signature verification. A temporal information technique was applied to enhance the features of the path signature. The precision, recall, f-score, and average accuracy reported are 0.93, 0. 97, 0.90, and 0.90, respectively.

Table 2. Comparison of Machine Learning Classifiers on the Proposed Online Signature Dataset with Existing Machine Learning Methods

Model	Precision	Recall	F-Score	Accuracy
Khoh [25]	0.94	0.93	0.93	0.97
Chang [26]	0.95	0.91	0.93	0.96
Foroozandeh [27]	–	–	–	0.83
Ahrabian [28]	–	–	–	0.95
Lupu [29]	–	–	–	0.91
Rasheed [30]	0.85	–	–	0.95
Zeng [31]	0.93	0.87	0.90	0.90
Proposed	0.98	0.96	0.96	0.96

5 Discussion and Conclusions

This research study presented a detailed study of the nature of online signature recognition. A novel dataset was collected for this research study. The collected dataset comprises of 1000 samples of the online signatures collected from 200 participants. Each participant gave 5 samples of their signature using an app of Android custom developed for the collection of the data samples. The dataset collected was split into train and test sets and given to five classifiers namely SVM, RFC, ETC, DT, and KNN for the training and evaluation. The maximum testing accuracy of 96% was achieved from the RFC and ETC. The results in terms of precision, recall, and f1 score have been presented in table form and graphically in the form of a confusion matrix.

In the future, this research can be extended in various directions. The online signatures collected for this research may be combined with one of the physiological biometrics traits to be used in a multimodal biometrics system. Such a multimodal biometrics system will not only ensure user privacy but also promise high accuracy and reliability. Online signatures may be combined with offline signatures to create more accurate biometrics signature recognition systems. Additionally, more samples may be collected and tested on the classifiers to analyze their effects. Deep learning and transformer techniques can also be applied to make online signature recognition systems more accurate and robust.

Author Contributions

Mehwish Legahri: Conceptualisation, data collection, methodology, experiments and Writing the original draft **Asghar Ali Chandio**: Data collection, experimental work and writing the original draft. **Muhammad Ali Soomro**: Data labelling, proofreading. **Shah Zaman Nizamani**: Algorithm testing, review original draft.: **Muhammad Hanif Soomro**: Data collection, validation, supervision and editing

Compliance with Ethical Standards

The authors declare no conflict of interest. This research required human participation for online signature data collection. However, informed consent was obtained from all individual participants included in the study.

Funding Information

This research has not received funds from any institution.

References

[1] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern recognition letters*, vol. 79, pp. 80–105, 2016.

[2] B. Alsellami, P. D. Deshmukh, Z. A. Ahmed, *et al.*, “Overview of biometric traits,” in *2021 Third IEEE International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 807–813, September 2021.

[3] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, 2020.

[4] T. Burlee, "Breach of biometrics database exposes 28 million records containing fingerprint and facial recognition data." https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records/-containing-fingerprint-and-facial-recognition-data/. [Retrieved on: 18-05-2024].

[5] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics continuous user authentication on mobile devices: A survey," *Information Fusion*, vol. 66, pp. 76–99, 2021.

[6] S. A. Abdulrahman and B. Alhayani, "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics," *Materials Today: Proceedings*, vol. 80, pp. 2642–2646, 2023.

[7] T. Gernot and C. Rosenberger, "Robust biometric scheme against replay attacks using one-time biometric templates," *Computers Security*, vol. 137, p. 103586, 2024.

[8] M. Faundez-Zanuy, J. Fierrez, M. A. Ferrer, *et al.*, "Handwriting biometrics: Applications and future trends in e-security and e-health," *Cognitive Computation*, vol. 12, pp. 940–953, 2020.

[9] T. Dhieb, H. Boubaker, S. Njah, M. B. Ayed, and A. M. Alimi, "A novel biometric system for signature verification based on score level fusion approach," *Multimedia Tools and Applications*, vol. 81, no. 6, pp. 7817–7845, 2022.

[10] Z. Wei, S. Yang, Y. Xie, F. Li, and B. Zhao, "Svsv: Online handwritten signature verification based on sound and vibration," *Information Sciences*, vol. 572, pp. 109–125, 2021.

[11] M. Okawa, "Online signature verification using single-template matching with time-series averaging and gradient boosting," *Pattern Recognition*, vol. 102, p. 107227, 2020.

[12] C. Alonso-Martinez and M. Faundez-Zanuy, "Online handwriting and signature normalization and fusion in a biometric security application," in *Springer Neural Approaches to Dynamics of Signal Exchanges*, (Singapore), pp. 453–463, 2019.

[13] M. Singhal and K. Shinghal, "Secure deep multimodal biometric authentication using online signature and face features fusion," *Multimedia Tools and Applications*, vol. 83, pp. 30981–31000, 2024.

[14] Y. Jia, L. Huang, and H. Chen, "A two-stage method for online signature verification using shape contexts and function features," *Sensors*, vol. 19, no. 8, p. 1808, 2019.

[15] V. Sekhar, P. Mukherjee, D. D. Guru, and V. Pulabaigari, "Online signature verification based on writer specific feature selection and fuzzy similarity measure," *arXiv preprint arXiv:1905.08574*, 2019.

[16] R. Tolosana, R. Vera-Rodriguez, C. Gonzalez-Garcia, *et al.*, "Svc-ongoing: Signature verification competition," *Pattern Recognition*, vol. 127, p. 108609, 2022.

[17] D. Morocho, A. Morales, J. Fierrez, and R. Vera-Rodriguez, "Human-assisted signature recognition based on comparative attributes," in *2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*, vol. 8, pp. 5–9, January 29 2018.

[18] M. Hnatiuc, O. Geman, A. G. Avram, D. Gupta, and K. Shankar, "Human signature identification using iot technology and gait recognition," *Electronics*, vol. 10, no. 7, p. 852, 2021.

[19] M. Kutyłowski and P. Błaśkiewicz, "Advanced electronic signatures and eidas–analysis of the concept," *Computer Standards Interfaces*, vol. 83, p. 103644, 2023.

[20] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Benchmarking desktop and mobile handwriting across cots devices: The e-biosign biometric database," *PloS one*, vol. 12, no. 5, 2017.

[21] M. Liwicki, M. I. Malik, C. E. van den Heuvel, *et al.*, "Signature verification competition for online and offline skilled forgeries (sigcomp2011)," in *2011 IEEE International Conference on Document Analysis and Recognition (ICDAR)*, pp. 1480–1484, 2011.

[22] M. Leghari, S. Memon, L. D. Dhomeja, *et al.*, "Deep feature fusion of fingerprint and online signature for multimodal biometrics," *Computers*, vol. 10, no. 2, p. 21, 2021.

[23] M. Leghari, S. Memon, and A. A. Chandio, "Feature-level fusion of fingerprint and online signature for multimodal biometrics," in *2018 IEEE International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–4, 2018.

[24] H. Kaur and M. Kumar, "Signature identification and verification techniques: state-of-the-art work," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 2, pp. 1027–1045, 2023.

[25] W. H. Khoh, Y. H. Pang, and H. Y. Yap, "In-air hand gesture signature recognition: An ihgs database acquisition protocol," *F1000Research*, vol. 11, 2022.

[26] S. J. Chang and T. R. Wu, "Development of a signature verification model based on a small number of samples," *Signal, Image and Video Processing*, vol. 18, no. 1, pp. 285–294, 2024.

[27] A. Foroozandeh, A. A. Hemmat, and H. Rabbani, "Online handwritten signature verification and recognition based on dual-tree complex wavelet packet transform," *Journal of Medical Signals & Sensors*, vol. 10, no. 3, pp. 145–157, 2020.

[28] K. Ahrabian and B. BabaAli, "Usage of autoencoders and siamese networks for online handwritten signature verification," *Neural Computing and Applications*, vol. 31, pp. 9321–9334, 2019.

[29] E. Lupu, S. Emerich, and F. Beaufort, "On-line signature recognition using a global features fusion approach," *Acta Tehnica Napocensis Electronics and Telecommunications*, vol. 50, no. 3, pp. 13–20, 2009.

[30] A. F. Rasheed and A. M. Alkababji, "A novel method for signature verification using deep learning," *Webology*, vol. 19, no. 1, pp. 1561–1572, 2022.

[31] Z. Zeng and J. Tian, "Deep learning methods for signature verification," *arXiv preprint arXiv:1912.05435*, 2019.