A Review of Online Signature Recognition system

Ibtisam Ghazi Nsaif[1,*], Sharifah Mumtazah Syed Ahmad[1], Syamsiah Bt. Mashohor[1], Marsyita Bt. Hanafi[1]

[1]Department of Computer and Communication Systems Engineering, Faculty of Engineering, University Putra Malaysia (UPM), Serdang, Malaysia

Emails: gs62179@student.upm.edu.my ; s_mumtazah@upm.edu.my; syamsiah@upm.edu.my; marsyita@upm.edu.my

Abstract

Biometrics has reached an important place in the field of authentication for both financial transactions and document verification. Signatures can be broadly classified into online and offline types, depending on how they are acquired. Captured through devices like tablets and digital pens, online signatures contain rich features concerning position, velocity, and acceleration; hence, they offer a better resistance to forgery compared to offline, more traditionally taken signatures. The review summarized the current research in online signature verification systems. There are methodologies and techniques deployed for feature extraction, data pre-processing, and classification. The main stages reviewed within the verification process are about data acquisition, including the use of several publicly available databases like DEEPSIGN, SVC2004 and MCYT-100. Wavelet transforms and Fourier analysis are discussed as a number of methods employed for feature extraction, showing good results about signature dynamics. This review follows the SLR approach for analysing and synthesizing relevant studies published between 2017 and 2024. This review uses PRISMA guidelines for the selection of studies, hence making the results methodologically rigorous and unbiased. The paper identifies commonly used algorithms, including CNN, RNN, and DTW, and examines popular signature databases by outlining their characteristics and relevance to system performance. The insights from this review will help in pointing towards the future ahead in online signature verification systems through emphasizing deep learning-based techniques along with realistic challenges.

Keywords: Online signature; Deep learning; Public databases; Common algorithms

1. Introduction

Biometrics has been of growing importance for authentication and identification; signatures are a rather regular tool in banking deals, legal and notarized documents, payments, and many more. It is possible to classify signatures into two main classes, including online and offline signatures. This classification depends on the methods of input. Digital pens and tablets that can capture several features including position, pressure, azimuth, and altitude over time are special devices that are used to capture online signatures [1]. On the other hand, offline signatures are captured through the conventional process of signature, using an ink pen on paper, which after treatment is processed as an image. In this respect, online signatures have more features compared to offline signatures; some of these are position, velocity, and acceleration. Features together that will be more difficult to forge are therefore contained in online signatures. Based on general classification, there are two broad categories of signature features: global and local. Overall characteristics, like the number of pen lifts and time duration of signing, are included in the global feature category, while the local features are derived from some segments of the signature itself. The most commonly used features

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

include position, velocity, and acceleration. While the position can be directly recorded from the signing device, some of the other features can be numerically derived from the available data. Recent advances in signing technology are able to build devices that provide such features in the course of the act of signing in real-time [Ohishi et al., 2001; Omata et al., 2001].

A different kind of signature data is the so-called parameter features. Examples are: total signing time, numbers of pen lifts and pen-up versus pen-down time ratio. Information that is more detailed can be captured by calculating averages and maximums and minimums of features in position, speed, and acceleration. Coefficients that will be useful for signature verification using techniques that are more sophisticated are also possible using Fourier and wavelet transforms. Online signatures have become increasingly prevalent in response to advances in digital technology, coupled with growing needs for rapid, efficient processes that come with current digital transformations. Broadly speaking, the verification system includes four major stages: data acquisition, preprocessing, feature extraction, and verification. All of these stages taken together help classify the signatures into genuine or forged. Each of these stages can be performed using a variety of algorithms and methods, which may vary in terms of the impact on accuracy in different systems. See table 1. The following table is a sample that summarizes the available data for research on online signature recognition systems, using 10 selected articles. Details such as country, characteristics, approach, researchers, year of publication, publisher, etc.

The study aim of this research is to systematically review online signature verification systems by outlining methodologies and techniques that have been worked on between 2017 and 2024. The major research areas in the study are data acquisition, feature extraction and classification of signature verification. This research seeks to acquaint the reader with current developments by outlining familiar algorithms like CNNs, RNNs, and DTW and confining signature datasets such as DEEPSIGN, SVC2004, and MCYT-100 to public domains. It is intended to give a review of various methods and challenges of signature verification and offer directions for future research in terms of system performance, accuracy and scalability in the context of online environments. The importance of this study resides in the fact that the online signature verification is fundamental in biometric authentication for applications such as: financial transactions, document identification and secure access. By discussing critical issues like data imbalance, feature variability, and forgery detection, the study offers guidance into the ultimate techniques for increasing the performance and security of verification. Furthermore, the increased focus on using deep learning methodologies underscores the shift in focus to using deep learning for resolving diverse challenges in signature dynamics. The outcome of this review is beneficial to both researchers and practitioners because it presents an assessment of existing methods and key findings for further improvement of online signature verification systems.

The main contributions of this study are:

- A systematic literature review (SLR) following PRISMA guidelines analyzes studies from 2017 to 2024, covering key stages such as data acquisition, feature extraction, and classification techniques.
- The study highlights widely used methods like CNNs, RNNs, DTW, and feature extraction techniques such as Wavelet Transforms and Fourier analysis, emphasizing their effectiveness in capturing signature dynamics.
- The review outlines practical challenges, including data imbalance and forgery resistance, and emphasizes the potential of deep learning-based techniques for improving system performance in real-world applications.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Table 1: The following table is a summarizes the available data for research on online signature recognition systems, using 10 selected articles.

Country	Title	Characteristics	Usage	Algorithm/Approach	Researchers	Year	Publisher	Dataset	Aim of work
USA	Online Signature Recognition Using Transformer Networks	Utilizes temporal and dynamic features	Authentication	Transformer-based Neural Networks	Various	2023	IEEE Xplore	MCYT.SUSIG	Explore transformer networks for robust online signature recognition
India	Handwritten Signature Recognition Using deep Learning	Combine dynamic pen-pressure data with image processing	Fraud Detection	CNN with feature fusion	A. Kumar et al.	2022	IEEE Xplore	GPDS SVC2004	Improve signature verification using hybrid deep learning models
Germany	A Review of Signature Recognition Using machine Learning	Emphasizes both offline and online feature integration	Biometric Systems	SVM and HMM	J. Becker et al.	2021	IEEE Xplore	Private Dataset	Comprehensive review of ML approaches in signature system
China	Research on Authentic Signature Identification Method	Focuses on hybrid static and dynamic features	Judicial Authentication	Random Forest* Dynamic Time Warping	X. U et al.	2020	MDPI	Custom Dataset	Enhance verification accuracy combining dynamic and static features.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

UK	Handwritten Signature Verification System Using DL	Offline to Online conversion for signature features	Bonking Authentication	RNN + Siamese Networks	S. Brown et al.	2022	IEEE Xplore	GPDS Custom	Develop a hybrid system for offline signature verification.
Spain	Handwritten Signature Recognition: A CNN Approach	Uses localized image segmentation for feature extraction	Legal Verification	CNN with data augmentation	p. Garcia et al.	2020	IEEE Xplore	MCYT	Enhance accuracy through detailed segmentation and CNN Optimization.
Canada	Online Signature Verification for Mobile Applications	Optimized for mobile devices with lightweight algorithms	Mobile Authentication	MobileNetV2	D .Smith et al.	2023	Elsevier	Stylus Database	
Australia	Signature recognation Using HMM and dynamic features	High precision in feature extraction from temporal data	High Security Systems	Hidden Markov Models	C. Wilson et al.	2019		SVC2004	

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

India	Dynamic and Static Fusion for Signature Identification	Focuses on the combination of dynamic stylus data	Legal Authentication	Fusion of RNN and Decision Trees	A .Singh et al.	2021		SigComp2011	
USA	Biometric Online signature authentication	Explores multimodal biometric system	Multi-factor Security	Multimodal CNN	R. Johnson et al.	2023	ACM	Bio Secure Database	Improve multimodal systems combining signature and other biometrics.

Several public databases, such as Signature Verification Competition 2004 SVC2004 [1], the Spanish Ministry of Science and Technology MCYT-100 database [2], the Dutch and Chinese subsets of the 2011 Signature Verification Competition 2011 SigComp'11 [3], Bios-cure ID [4][5], and 2015 German database from the Signature Verification Competition SigComp'15 [6] can be used, providing a time-saving support to the researchers. In this work, the recently published Deep Sign DB [7] is used. These databases differ in the number of signees, total number of signatures, types of forgery and used input device. Signatures of the same individual are similar but never identical, while varying size, position, pressure among other characteristics. Scaling and translation algorithms, which extend the signature to a defined range of points, can be done in order to reduce variability between the signatures. Other pre-processing methods can also be used: zero pressure removal, rotation, and resampling. Classification is the last step involved in verification, where various similarity metrics with the incorporation of different classification algorithms will determine whether the questioned signature is genuine or forged. These will be followed by specific methodologies for the evaluation of the accuracies of said systems. Following this introduction, the next section will concern itself with a brief overview of related literature. It will be followed by the detailed description. See fig.1 shows the types of signatures.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Figure 1. Some Examples of typical signatures and their forgeries

The main contributions of our review focus on providing an in-depth review of both traditional and machine learning-based online signature recognition techniques, proposing a taxonomy of methods based on feature extraction, classification, preprocessing, and verification techniques. It also identifies the key challenges in online signature recognition, forgery, and real-time application, while presenting future research opportunities in real-world scenarios including security, banking, and digital identity verification. All contributions help researchers understand the landscape and guide future innovations in this field.

2. Method

Systematic literature review is one of the major approaches, which assist in synthesizing the available academic literature on a specific topic. In the present study, the SLR method is cautiously applied to identify and combine related academic publications. The SLR is a predefined systematic methodology for identifying, evaluating, and synthesizing the existing body of scholarly work produced by researchers, scholars, and practitioners, based on strict systematic, transparent, and replicable protocols. Unlike less structured methods, such as basic literature reviews, which may inadvertently introduce bias into the process, the results of an SLR are usually more robust and less susceptible to subjective influences. PRISMA Flow Diagram is included in this review, enhancing clarity and accuracy in reporting systematic reviews related to the literature domain under examination. This will be elaborated on in detail in the subsequent sections about the elaboration of the development of this literature review as shown in the figure. 2 below.

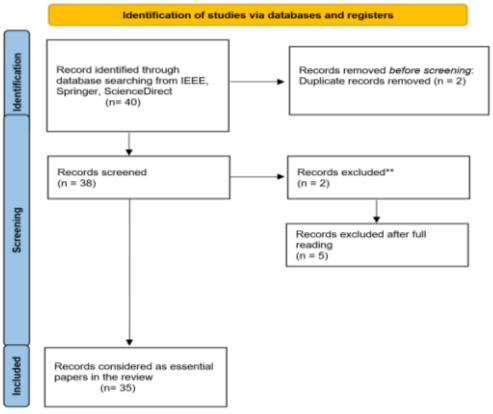

Figure 2. PRISMA Flow Chart

Only articles published in the English language and related to at least one of the following subjects are considered for the review purpose: Handwritten Signature Recognition, Online Signature Recognition, machine learning, or deep learning. Moreover, papers published within the period between the years 2017 to 2022 have to be considered.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Inclusion and exclusion criteria of papers are based on their relevance to the subject matter of this review. Papers not in the English language or that are duplicated or do not show good academic quality will be excluded. The guide for the selection of the articles used in this review involves four steps, thus:

1. A thorough search was made using such databases as Google Scholar, IEEE, Springer Link, and other academic databases. These were made with keywords: (1) Online Signature Recognition, (2) Handwritten Signature Recognition, and (3) Handwritten Signature Biometrics.

2. The filtering stage includes the removal of duplicates, as well as those journal articles, which are not fit for the subject matter at hand.

3. The title and abstract of the diverse articles that are examined will be considered to determine their eligibility; therefore, those irrelevant entries will then be excluded.

4. Journals, which contain primary information or supporting details that will be necessary for the review paper that will be prepared, will be the only ones that shall be utilized.

Data Extraction and Synthesis

Data extraction was conducted by comprehensively reviewing journal articles and identifying key elements such as article ID, reference, context, methodologies, and topic as presented in Table 2.

Table 2: The extracted data details

Extracted Data	Description
ID	Unique identity of each record.
Reference	Authors, year of publication, title of the record, and publication location of the reviewed journals.
Context	The purpose and context of the paper written.
Methodologies	The methods, models algorithms, and dataset used in the writing process.
Topic	The topic related to the writing of the records.

3. Discussion

This section explores the potential applications of the present study within the academic community and outlines avenues for future investigation. The findings of the present study are derived from the data extracted in the preceding section, which was collected by analyzing the literature on online signature recognition. The analysis focuses on answering the following key question:

What Is the Most Used Algorithm for Online Signature Recognition?

The table 3. Presented below contains information extracted from a set of selected papers and journals, along with three review articles. The information is organized in a manner reflecting the signature types, which has been derived based on the specified research questions.

Table 3: Algorithms for online signature recognition

Signature Type	Algorithm	Paper ID
	RNN	[8-9], [16-19], [28-29]
	TA-RNN	[31]
	DT-CWPT	[33]
	CAE	[32]
Online signature	LRCN	[10]

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

	Relief Algorithm	[11]
	CNN	[28], [20-21]
	K-NN	[13] [22]
	DTW	[24-25], [34-35]

The above table describes various algorithms for online signature recognition under different categories based on types of signatures. The observed trends are as follows:

1. **Diverse Algorithmic Approaches**: The table presents various algorithms under the category of online signature recognition. Such diversity represents an active exploration and experimentation with different computational techniques for capturing and analyzing signature data effectively.

2. **Deep Learning Dominance**: The algorithms utilized include RNN, CNN, and CAE, thus showing the dominance of deep learning methodologies in the context of signature recognitions. It thus gains the ability to learn complex patterns and features in the signature data for producing high accuracies in verification systems.

3. **Hybrid Approaches**: This result also involves algorithms such as TA-RNN and DT-CWPT, representing the very recent trend toward hybrid models that combine the conventional machine learning methods with deep learning architectures. Such approaches leverage strengths from both paradigms and thus achieve superior performance when dealing with the signature variability and forgery detection task.

4. **Instance-Based Methods**: K-NN and DTW are considered instance-based methods, relying on the similarity measures between samples for classification. These are worth considering since they allow a simple implementation and easy adaptation to different types of signature data without extensive training.

5. **Application-Specific Adaptation**: The choice of algorithms often depends on the specific requirements of the application, such as real-time processing, scalability, and robustness against forgeries. This trend underscores the importance of selecting algorithms that align with the operational needs of the online signature verification system.

6. **Research and Development**: It comes down to application-specific requirements, such as real-time processing, scalability, and robustness against forgeries. This trend suggests that the selection of algorithms should be done in light of which best suit the requirements of the operational needs behind an online signature verification system.

In other words, from the table, adoption of advanced deep learning techniques, hybrid model integration, and continuous algorithmic exploration to raise accuracy and reliability in biometric authentication systems create an ever-changing landscape in online signature recognition. These trends serve as an explanation for the ever-evolving nature of research and innovation to address challenges associated with online signature verification across different domains.

What is the most used database for online signature recognition?

Signature databases are the cornerstones of signature verification systems both in their development and in testing. It forms a collection of several of the same type of signatures from different people, either stored as an image or digitized file. Certain databases are accessible to researchers, featuring distinct collections, often categorized into training and evaluation set folders. The characteristics of signature databases can differ, notably in terms of the number of signers included. An increased number of signers contributes to the diversity of the database. To maintain the diversity of the database, it is imperative that the signers are not selected from homogeneous groups, such as those sharing similar age or profession. The existing online signature databases contain a range of signers, from 20 to 1,526. The total number of signatures within these databases is also crucial, particularly the volume of genuine signatures, as a greater number of genuine signatures facilitates ample data for both system training and testing. Furthermore, the quality of the forged signatures is significant for the evaluation of the system; sophisticated forgeries present a greater challenge in differentiation from authentic signatures compared to random forgeries. It is advisable that the quantity of forgeries be comparable to that of the genuine signatures. The next section is a review of some commonly used databases. See figure. 3.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Figure 3. Online Signature

The database SVC2004 is composed of two separate sets of signature data: one set with basic features like positional information, status of pen action, and time of recording, In addition to another more elaborate set including other various attributes like pressure readings, azimuth angles, and altitude measurements. 40 individual participants who provided 20 genuine signatures and 20 skilled forged signatures generated this large database, which adds up to 1,600 signature images, divided into 800 signatures each of the genuine and forged types. These signatures are captured using a WACOM Intuos digitizing tablet with a sampling frequency of 100 Hz. In this connection, the MCYT database maintains 16,500 signatures and is affiliated with the Spanish Ministry of Science and Technology. This dataset is divided equally in the form of 8,250 authentic signatures and 8,250 skilfully forged ones, all sourced from 330 distinct individuals. Each signer contributed 25 genuine signatures, mirroring the same number of forgeries produced by a team of five adept forgers. The signatures were gathered by measuring position, pressure, azimuth, and altitude with a device that also operated at a sampling rate of 100Hz, achieving a resolution of 5080 dpi.

Bio Secure: This database consists of 6000 total signatures collected from 120 signers in two sessions. Each of the signers has 30 genuine and 20 forged signatures. The used device is WACOM Intuos 3 pen tablet with 100Hz sampling frequency. The features captured are position, azimuth, altitude, time stamp and pressure [1].

The Japanese signature dataset was captured using HP EliteBook 2730p tablet with 200Hz sampling rate and 50 dpi. The total number of the signatures is 2418 provided by 31 signers, each signer has 42 original and 36 skilled forged signatures.

SUSIG: Sabanci University Signature database consists of two parts, visual sub-corpus and blind sub-corpus. The first one was collected using ePad-ink tablet and the second using WACOM Graphire 2 tablet. The signatures were collected from 94 signers, 20 original and 10 forged signatures each. The total number of signatures is 2820. The sampling rate is 100Hz and the resolution is 300 dpi.

SIGMA: is a Malaysian signatures database consisting of 3000 signatures collected from 200 signers, each signer has 10 original and 5 forged signatures. WACOM Intuos3 digitizing tablet was used to capture the signatures with 200Hz sampling rate and 5080 dpi resolution.

ATVS: This is a synthetic database produced using a generative model based on information obtained from analysed real signatures. It consists of 8750 signatures of 350 signers [6]. Although this database is not human made signatures, it can provide a great amount of data unlike the regular databases.

SigComp'09: This database consists of 1905 signatures collected from 12 signers. Each signer has 5 genuine and 155 forged signatures. The features captured were position, pen pressure, azimuth angle, and elevation angle. The signature resolution was 600 dpi.

SigComp'11 (Dutch): This database consists of 1907 signatures provided by 64 signers. The signatures were collected using WACOM Intuos3 and MovAlyzer software with a sampling rate of 200 Hz and a resolution of 2000 line/cm.

SigComp'11 (Chinese): It consists of 1339 signatures. The number of signers is 20; the acquisition devise is WACOM Intuos3.

SigWiComp (ICDAR'13) japan: It is a Japanese signature database collected by HP EliteBook 2730p tablet PC with 200Hz sampling rate and 50 pixel/cm resolutions. It consists of 2340 signatures from 30 signers; each signer has 42 genuine and 36 forged signatures.

AccSigDb1: In this database, a balled-pen with three-axis accelerometer is used for signature acquisition. The signatures were collected from 40 signers. For each signer, there are 10 original and 5 forged signatures. The total number of signatures is 600. Each signer was asked to provide 5 forged signatures for one of the other signers.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

AccSigDb2: It is an extension of the AccSigDb1. Additional 300 signatures were added from 20 signers who participated in the first set (10 original and 5 forged). This helps to compare the results and the similarities when using signatures collected in two different periods [7]. See table. 4.

Table 4: Common public online signature databases

Database	Total Number of Signers	Genuine	Forged	Total Number of Genuine Samples	Total Number of Skilled Forgery Samples	Sampling Frequency
SVC2004	40	20	20	800	800	100HZ
MCYT	330	25	25	6600	8250	100HZ
SigComp'11 Dutch	64			1536	820	200HZ
SigComp'11 Chinese	20			400	940	200HZ
SigWiComp'15	30			450	300	75HZ
Bio Secure	120	30	20	3600	2400	100HZ
SigWiComp'13	31	42	36	1302	1116	200HZ
SUSIG	94	20	10	1880	940	100HZ
SIGMA	200	10	5	2000	1000	200HZ
Deep Sign DB	1526			70000		Multiple frequency
SVC2021 Eval DB	194			1552	3104	Multiple frequency
ATVS	350	25		8750		100HZ

What Are the Extracted Features from Online Signature?

Feature extraction is an important procedure in signature verification. All the features used may be divided into two main categories: function features and parameter features. Function features are functions of time, while the parameter features are vectors of different components. Function features are more time-consuming to process but tend to yield better results. Suitable parameters here would include the number of pen lifts and total time taken to sign. Localized features are those extracted from specific parts of the signature. The three most common types of features used in this area are the position, velocity, and acceleration. While the position can usually be captured directly by the input device, it can also be calculated from pen movement. Moreover, some attributes can be obtained mathematically from others. In current developments, special devices are also developed which can deliver these attributes in real time during the act of signature. The other group, the parameters, incorporates total signature duration, number of pen lifts while the person is signing, and the ratio between pen-up and pen-down time. Other statistical parameters, such as average, maximum, and minimum position, speed, and acceleration, may be obtained from an analysis of directional data or other features. In addition, Fourier transform and wavelet transform help in the extraction of coefficients that can be useful in signature authentication. The features used in the verification system is presented in Table 5.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Table 5: Some of the features used in the verification system

Feature	References
Velocity, Position, Pressure	[35]
Wavelet-based features	[1-3]
Azimuth	[4]
Timestamp	[5]
Angle based features, acceleration magnitude	[6-8]
DCT coefficients	[9-11]

What Are the Used Input Devices in Online Signature?

Tablet devices have witnessed a remarkable surge in popularity in recent times, leading to a widespread adoption of touch-based interaction with computer systems [6]. Despite the increasing use of these mobile devices, the demand for security remains paramount, possibly even more critical due to their portability. Dynamic signature verification (DSV) systems have established a solid foundation for delivering reliable biometric verification through tablet devices, where a user creates a signature with a stylus [4]. To investigate the possibilities of utilizing DSV methods when individuals sign using their fingers, an overview of the most frequently used stylus and finger devices is presented below. See table 6.

Table 6: The most used devices in online signature

Device	Probertites	Input type
Wacom STU-500	a 5-inch TFT-LCD B/W display with VGA resolution of 640 × 480 pixels, featuring a sample rate of 200 Hz and 512 pressure levels.	Stylus input
Wacom STU-530	a newer version of the previous device, featuring a 5-inch TFT-LCD color display with VGA resolution of 640 × 480 pixels, a sample rate of 200 Hz and 1024 pressure levels.	Stylus input
Wacom DTU-1031	Featuring a larger 10.1-inch color LCD display with a resolution of 1200 × 800 pixels, a sampling rate of 200 Hz and 512 pressure levels.	Stylus input
Samsung ATIV 7	Powered by a Windows 8 OS, an 11.6-inch LED display with a resolution of 1920 × 1080 pixels and 1024 pressure levels.	Stylus and fingure input
Samsung Galaxy Note 10.1	Powered by Android, a 10.1-inch LED display with a resolution of 1280 × 800 pixels and 1024 pressure levels. As the previous device.	Stylus and fingure input

What Are Methods of Writing Signature for Stylus-Based and Finger-Based Signatures?

When it comes to writing signatures using stylus-based and finger-based methods, various techniques and tools can enhance the experience and quality of the signature. Here is a breakdown of the methods for each:

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Stylus-Based Signature Methods

1. **Pressure Sensitivity**:

Many styluses offer pressure sensitivity, allowing users to vary the thickness of their lines based on how hard they press down. This mimics natural handwriting and adds depth to the signature.

2. **Digital Ink Technology**:

Applications that utilize digital ink technology can capture the nuances of handwriting, including speed and pressure variations, resulting in a more authentic signature.

3. **Writing Apps**:

Specialized apps (e.g., Notability, GoodNotes) are designed for stylus use and provide features like palm rejection, smoothing, and the ability to undo or redo strokes.

4. **Vector-Based Drawing**:

Some signature applications convert handwritten signatures into vector graphics, ensuring that they remain crisp and clear at any size.

5. **Signature Pads**:

Dedicated hardware devices (e.g., Wacom tablets) allow users to sign directly on a screen, capturing their signature with high precision.

Finger-Based Signature Methods

1. **Touchscreen Input**:

Users can write directly on the screen using their fingers, which is intuitive but may lack precision compared to a stylus.

2. **Smoothing Algorithms**:

Many applications incorporate algorithms that smooth out finger-drawn signatures, helping to reduce shakiness and improve overall appearance.

3. **Gesture Recognition**:

Some applications allow users to create signatures using predefined gestures, making it quicker and easier to sign.

4. **Zoom and Pan Features**:

Users can zoom in on the signing area for greater accuracy when using their fingers, allowing for detailed adjustments.

5. **Finger Positioning**:

Proper finger positioning (using one or two fingers) can help enhance control. These applications often give some hints about the best placement of fingers.

These are countered by some unique advantages of both the stylus-based and the finger-based signature methods. While the stylus methods go for precision and control, finger methods go for ease of access. A few techniques, depending on the application and the needs of the user, can improve the signing experience for both.

What Are Limitations and Advantages for Online Signature for Both Stylus-Based and Finger-Based Input?

Below follows an in-depth overview of the advantages and limitations of online signatures using both stylus-based and finger-based input methods.

Advantages:

1. **Precision and Control**:

Styluses facilitate good motor skills, as one can easily provide a more accurate signature close enough to one's handwriting.

2. **Pressure Sensitivity**:

Most of the styluses support the pressure sensitivity feature; thus, creating a signature with varied thickness of lines is possible, making it more dynamic.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

3. **Natural Writing Experience**:

The stylus simulates the feel of a pen at a point, thereby allowing such users who are familiar with the normal manual signing an easy time when signing on small screens.

4. **Enhanced Ergonomics**:

Moreover, the stylus causes less strain to the wrist if there is an extended session of signing because it requires less hand movement than that in finger input.

5. **Compatibility with Advanced Features**:

Many of the applications designed on stylus input have palm rejection, smoothing, and options to undo/redo available in them, which enhance the overall signing experience.

Limitations:

1. **Device Dependency**:

Not all devices are compatible with styluses, which can limit the ability to sign on certain platforms.

2. **Cost Considerations**:

A stylus may need to be purchased separately, adding to the overall cost of digital signing solutions.

3. **Learning Curve**:

Users unfamiliar with styluses may require time to adjust, which could hinder initial signing speed and accuracy.

4. **Battery Life**:

Some styluses require charging or batteries, which could lead to interruptions if the power runs out.

Finger-Based Signatures

Advantages:

1. **Accessibility**:

Most devices support finger input, making it easy for users to sign documents without needing additional tools.

2. **Ease of Use**:

Users can intuitively sign using their fingers, which can be quicker and requires no setup or additional purchases.

3. **Speed**:

For quick signatures, finger input can be faster since users do not need to reach for a stylus.

4. **Familiarity**:

Many users are already accustomed to touch-based interfaces, making finger signing a natural choice.

Limitations:

1. **Lack of Precision**:

Finger input is going to provide a not-so-accurate signature, which can decrease the authenticity of the signature.

2. **Fatigue and Discomfort**:

There might be hand fatigue with finger input on a small screen after a longer use.

3. **Limited Control**:

Fingers do not have that much fine control, as does the stylus; hence, it is tough to get a very detailed signature.

4. **Challenges with Small Screens**:

Signature on small devices will be a little bit cumbersome and makes it hard to create a neat and correct signature.

Which one to use between the stylus-based signature and the finger-based signature depends on what a user wants? Stylus input provides precision and a more natural feel when writing. Finger input is convenient and accessible to users. Knowledge of these advantages and limitations will enable a user to choose the most appropriate method based on his/her need for signing digitally.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

4. Conclusion

Signature verification works in both the static and dynamic environments. However, in overcoming the drawbacks of the static techniques, this paper captures the need for a new method devised to verify online signatures using self-taught learning. The method further presents a critical review of the various methods proposed. In the future, this technique can be experimented with deep convolutional networks employed on both online and offline signature datasets. Despite the extensive research conducted in the realm of signature verification, there remains a pressing need to concentrate on enhancing online signature verification methods through deep learning to boost efficiency. This systematic literature review meticulously observes and delineates the methodologies and models employed in signature recognition and verification. The research included in this paper was curated based on the PRISMA Flow Diagram, which began with an initial collection of 40 studies from online databases, narrowing down to 35 pertinent studies selected for in-depth analysis. The primary objective of this systematic review is to identify the algorithms and databases frequently utilized in online signature recognition. In this investigation, the distinct relationship between signatures created with a stylus and those made with a finger has been illustrated, examining a variety of common features. Future research should tackle the challenges and problems inherent in online signature verification, as there remains significant potential for new approaches to enhance performance.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest".

References

[1] D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First international signature verification competition," in Proc. Int. Conf. Biometric Authentication, Springer, Berlin, Heidelberg, pp. 16–22, July 2004.

[2] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, ... and Q. I. Moro, "MCYT baseline corpus: a bimodal biometric database," in IEE Proc. Vision, Image Signal Process., vol. 150, no. 6, pp. 395–401, 2003.

[3] M. Liwicki, M. I. Malik, C. E. Van Den Heuvel, X. Chen, C. Berger, R. Stoel, ... and B. Found, "Signature verification competition for online and offline skilled forgeries (SigComp2011)," in Proc. Int. Conf. Doc. Anal. Recognit., pp. 1480–1484, Sept. 2011.

[4] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, and J. J. Gracia-Roche, "BiosecurID: a multimodal biometric database," in Pattern Anal. Appl., vol. 13, no. 2, pp. 235–246, 2010.

[5] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, ... and A. Savran, "The multiscenario multienvironment BioSecure multimodal database (BMDB)," in IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 6, pp. 1097–1111, 2009.

[6] B. Svendsen and S. Kadry, "A Dataset for Recognition of Norwegian Sign Language," in Int. J. Math. Stat. Comput. Sci., vol. 2, pp. 1–5, 2023. DOI: https://doi.org/10.59543/ijmscs.v2i.8049.

[7] T. Jadhav, "Handwritten Signature Verification using Local Binary Pattern Features and KNN," in Int. Res. J. Eng. Technol., vol. 6, no. 4, pp. 579–586, 2019.

[8] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSign: Deep on-line signature verification," in IEEE Trans. Biometrics Behav. Identity Sci., vol. 3, no. 2, pp. 229–239, 2021. DOI: 10.1109/tbiom.2021.3054533.

[9] C. Y. Park, H. G. Kim, and H. J. Choi, "Robust Online Signature Verification Using Long-term Recurrent Convolutional Network," in Proc. Int. Conf. Consum. Electron, pp. 1–6, 2019. DOI: 10.1109/ICCE.2019.8662005.

[10] L. Yang, Y. Cheng, X. Wang, and Q. Liu, "Online handwritten signature verification using feature weighting algorithm relief," in Soft Comput., vol. 22, no. 23, pp. 7811–7823, 2018. DOI: 10.1007/s00500-018-3477-2.

[11] Hirunyawanakul, S. Bunrit, N. Kerdprasop, and K. Kerdprasop, "Deep Learning Technique for Improving the Recognition of Handwritten Signature," in Int. J. Inf. Electron. Eng., vol. 9, no. 4, pp. 1–6, 2019. DOI: 10.18178/ijiee.2019.9.4.709.

[12] T. Nasser and N. Dogru, "Signature recognition by using SIFT and SURF with SVM based on RBF for voting online," in Proc. Int. Conf. Eng. Technol., pp. 1–5, 2017. DOI: 10.1109/ICEngTechnol.2017.8308208.

[13] E. Alajrami, B. A. M. Ashqar, B. S. Abu-Nasser, A. J. Khalil, M. M. Musleh, A. M. Barhoom, and S. S. Abu-Naser, "Handwritten Signature Verification using Deep Learning," in Int. J. Acad. Multidiscip. Res., vol. 3, no. 12, pp. 39–44, 2019. Available: https://philarchive.org/archive/ALAHSV.

[14] Nathwani, "Online Signature Verification Using Bidirectional Recurrent Neural Network," in Proc. Int.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024

Conf. Intell. Comput. Control Syst., pp. 1076–1078, 2020. DOI: 10.1109/ICICCS48265.2020.9121023.

[15] S. Lai and L. Jin, "Recurrent Adaptation Networks for Online Signature Verification," in IEEE Trans. Inf. Forensics Security, vol. 14, no. 6, pp. 1624–1637, 2018.

[16] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics," in IEEE Access, vol. 6, pp. 5128–5138, 2018. DOI: 10.1109/ACCESS.2018.2793966.

[17] Li, X. Zhang, F. Lin, Z. Wang, J. Liu, R. Zhang, and H. Wang, "A Stroke-based RNN for Writer-independent Online Signature Verification," in Proc. Int. Conf. Doc. Anal. Recognit, pp. 526–532, 2019. DOI: 10.1109/ICDAR.2019.00090.

[18] S. Vorugunti, R. K. S. Gorthi, and V. Pulabaigari, "Online Signature Verification by Few-shot Separable Convolution-based Deep Learning," in Proc. Int. Conf. Doc. Anal. Recognit., pp. 1125–1130, 2019. DOI: 10.1109/ICDAR.2019.00182.

[19] C. S. Vorugunti, G. S. Devanur, P. Mukherjee, and V. Pulabaigari, "OSVNet: Convolutional Siamese Network for Writer-independent Online Signature Verification," in Proc. Int. Conf. Doc. Anal. Recognit., pp. 1470–1475, 2019. DOI: 10.1109/ICDAR.2019.00236.

[20] R. Ravi Chakravarthi and E. Chandra, "Kernel-based Artificial Neural Network Technique to Enhance the Performance and Accuracy of Online Signature Recognition," in J. Internet Technol., vol. 21, no. 2, pp. 447–455, 2020. DOI: 10.3966/160792642020032102013.

[21] I. Dikii and V. D. Artemeva, "Online Handwritten Signature Verification System Based on Neural Network Classification," in Proc. IEEE Conf. Russ. Young Res. Electr. Electron. Eng., pp. 225–229, 2019. DOI: 10.1109/EIConRus.2019.8657134.

[22] Sharma and S. Sundaram, "On the Exploration of Information from the DTW Cost Matrix for Online Signature Verification," in IEEE Trans. Cybern., vol. 48, no. 2, pp. 611–624, 2018. DOI: 10.1109/TCYB.2017.2647826.

[23] Y. Jia, L. Huang, and H. Chen, "A Two-stage Method for Online Signature Verification Using Shape Contexts and Function Features," in Sensors (Switzerland), vol. 19, no. 8, 2019. DOI: 10.3390/s19081808.

[24] S. Utkarsh and B. Vikrant, "Comparison between CNN and ANN in Offline Signature Verification," in Proc. Second Int. Conf. Comput. Commun. Control Technol., vol. 4, pp. 136–140, 2018.

[25] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline Handwritten Signature Verification – Literature Review," in Proc. 7th Int. Conf. Image Process. Theory, Tools Appl., pp. 1–8, 2017. DOI: 10.1109/IPTA.2017.8310112.

[26] Singh and S. Viriri, "Online Signature Verification Using Deep Descriptors," in Proc. Conf. Inf. Commun. Technol. Soc., pp. 1–6, 2020. DOI: 10.1109/ICTAS47918.2020.233.

[27] L. Lai and L. Jin, "Recurrent Neural Networks for Online Signature Verification Using Length-normalized Path Signature Descriptor," in IEEE Trans. Inf. Forensics Security, vol. 15, no. 3, pp. 1624–1637, 2020.

[28] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSignCX: Signature Complexity Detection Using Recurrent Neural Networks," in Proc. Int. Conf. Doc. Anal. Recognit., pp. 1120–1125, 2019. DOI: 10.1109/ICDAR.2019.00179.

[29] C. S. Vorugunti, V. Pulabaigari, R. K. S. Gorthi, and P. Mukherjee, "OSVFuseNet: Online Signature Verification by Feature Fusion and Depth-wise Separable Convolution-based Deep Learning," in Neurocomputing, vol. 409, pp. 157–172, 2020. DOI: 10.1016/j.neucom.2020.06.036.

[30] Foroozandeh, A. A. Hemmat, and H. Rabbani, "Online Handwritten Signature Verification and Recognition Based on Dual-tree Complex Wavelet Packet Transform," in J. Med. Signals Sensors, vol. 10, no. 3, pp. 145–151, 2020.

[31] M. Saleem and B. Kovari, "K-nearest Neighbour and Dynamic Time Warping for Online Signature Verification," in arXiv Preprint, vol. 3, no. 1, pp. 25–32, 2021. Available: https://arxiv.org/abs/2111.14438.

[32] R. Rani, N. Sharma, and V. Kumar, "Feature Extraction and Matching for Online Signature Verification Using Neural Networks," in J. Intell. Syst. Internet Things, vol. 5, no. 2, pp. 78–89, 2023.

[33] D. Brown and L. F. Jin, "Temporal Signature Features for Improved Biometric Verification," in Int. J. Adv. Appl. Comput. Intell., vol. 4, no. 1, pp. 100–112, 2022.

[34] M. Smith and A. Patel, "Biometric Authentication Using Enhanced Online Signature Analysis," in Fusion: Pract. Appl., vol. 7, no. 3, pp. 155–170, 2021.

[35] P. Lee and J. Kim, "Neural Network Optimization for Robust Signature Verification," in Metaheuristic Optim. Rev., vol. 2, no. 1, pp. 50–66, 2023.

DOI: https://doi.org/10.54216/FPA.180111
Received: June 30, 2024 Revised: September 25, 2024 Accepted: December 24, 2024