Grenze International Journal of Engineering and Technology, June Issue

A Survey on Device Heterogeneity and Interoperability in Online Signature Verification

S D Bhavania[1] and R K Bharathib[2]
[1-2]Department of Computer Applications, JSS Science and Technology University, Mysuru, Karnataka, India
Email: bhavani.sd@jssstuniv.in, rkbharathi@ jssstuniv.in

***Abstract*— Automatic Signature Verification is one of the challenging problems that has remained unsolved for over the past forty years of research. A new challenge gets added due to the widespread use of smartphones, tablets, stylus-enabled devices, and dedicated signature pads used for capturing signatures for authentication purposes. This multi-device biometric setting necessitates addressing device interoperability to ensure consistent and reliable verification performance. This survey provides a comprehensive analysis of multi-device signature verification with a focus on device interoperability issues, systematically reviews existing approaches and publicly available multi-device signature datasets. The survey reveals that device-induced intra-class variations severely degrade verification accuracy and that current solutions only partially mitigate these challenges. Finally, we outline open research problems and future directions aimed at developing device-invariant representations and more comprehensive multi-device datasets. This survey serves as a consolidated reference for researchers working toward reliable and interoperable signature verification in real-world multi-device environments.**

***Keywords*— Interoperability issues, intra-class variations, multi-device, research avenues.**

I. INTRODUCTION

Handwritten signature verification has attracted significant research attention due to its practical importance and challenging nature. Based on the acquisition, handwritten signatures are classified into offline and online signatures. Offline signatures are produced by writing on paper with a pen and are transformed into digital images through scanning or camera-based acquisition. The signature acquired using an electronic device such as Tablets, smartphones or dedicated signature pads is known as an online signature, where the signature is saved as a sequence of x-y coordinate values, pen up/down, and pressure information. An online signature is hard to forge as dynamic information is stored, whereas an offline signature contains only static information, which makes the verification process much more challenging [1,7,8,9,10]. Handwritten signature verification is a challenging problem for the research community due to intra-class variations and inter-class similarity. Inter-class similarity occurs when a skilled forger writes a signature similar to the original signature. Intra-class variation occurs when the same individual generates visually dissimilar signatures influenced by factors such as pen and paper type, hand or finger injuries, jewellery, mental state, and writing position. Online signature verification has a wide range of real-time applications. As the technology advances, different devices are used during the enrolment and verification phases. For instance, in recent times, a customer uses a signature pad provided at the bank branch to enrol the signature and later he/she may use a smartphone or tablet for verification.

Grenze ID: 01.GIJET.12.2.10_25

Similarly, in remote document signing, insurance, legal services, and e-governance systems, users often enroll their signatures on laptops or dedicated tablets and later verify them using mobile devices. Healthcare systems also use online signature verification for electronic prescriptions, patient consent forms, and medical record authorization, where signatures captured on hospital devices may later be verified on portable tablets.

Figure 1. Major Phases of Signature Verification

II. ONLINE SIGNATURE VERIFICATION

Signature verification is typically carried out in two phases: enrolment and verification, as depicted in Figure 1. During enrolment, features are extracted from pre-processed genuine signatures and stored in a knowledge base as reference models. In the verification phase, features derived from a query signature are compared with the stored references to decide whether the signature is authentic or forged.
For more than forty years, signature verification has been widely investigated, and its advancements have been systematically reviewed in several comprehensive survey papers [15–18,21]. Recent developments concentrating on both offline and online signatures are reported in [1,7,9,10]. A dedicated survey on online signature verification is found in [8,19,20]. Signature verification begins with signature acquisition, pre-processing, feature extraction, feature selection (optional) and classification. There are several devices available in the market through which signatures can be acquired. Figure 2 depicts the devices through which an online signature can be captured. The various devices like digitising tablets, signature pads, smartphones, Tablets, smart pens, and PDAs are used to capture signatures. Table 1 shows the technical specifications of some of the commonly used COTS devices for signature acquisition.

Figure 2. Various Acquisition Devices to capture online signatures

TABLE I. TECHNICAL SPECIFICATIONS OF SOME OF THE COMMONLY USED COTS DEVICES FOR SIGNATURE ACQUISITION

Device Name	Device Type	Screen Size	Sensing Technology	Sampling Rate	Pen Pressure Levels	Resolution
Wacom Intuos CTL-472	Pen Tablet	Active area ~6.0 × 3.7 in	Electromagnetic Resonance (EMR)	~133 pps	2048	2540 lpi
Wacom Intuos CTH-680	Pen & Touch Tablet	~8.5 × 5.3 in	EMR + Touch	~133 pps	2048	2540 lpi
Wacom One (CTL-672)	Pen Tablet	~8.5 × 5.3 in	EMR	~133 pps	2048	2540 lpi
Wacom STU-430	Signature Pad	4.5-inch LCD	EMR	~200 pps	1024	2540 lpi
Wacom STU-540	Signature Pad	5-inch LCD	EMR	~200 pps	1024	2540 lpi
Topaz SigLite T-LBK460	Signature Pad	4.4 inch	Electromagnetic	~100–200 pps	1024	410 ppi (approx)
Topaz SigGem LCD 4x3	Signature Pad	4.7 inch	Electromagnetic	~100–200 pps	1024	410 ppi
Huion H610 Pro V2	Pen Tablet	10 × 6.25 in	Battery-free EMR	~233 pps	8192	5080 lpi

XP-Pen Deco 01 V2	Pen Tablet	10 × 6.25 in	EMR	~200 pps	8192	5080 lpi
Apple iPad (with Apple Pencil 2)	Stylus Tablet	10.9–12.9 inch	Capacitive + Active Stylus	~240 Hz (effective)	~4096 (estimated)	~264 ppi
Samsung Galaxy Tab S7 (S Pen)	Stylus Tablet	11 inch	EMR (Wacom)	~240 Hz	4096	~274 ppi
Microsoft Surface Pro + Slim Pen	Stylus Tablet	12.3 inch	Capacitive + Active Stylus	~120–240 Hz	4096	~267 ppi

After acquisition, the signature is subjected to pre-processing steps such as filtering noise[22,23,24], fixed area[25], length equalisation[26,27], and alignments[25,27], to improve the quality of the captured data.
The enhanced signatures are then utilized for extracting discriminative features to determine the authenticity of a query signature. In online signature verification, features can be broadly categorized into functional, global, component-oriented, and pixel-oriented types [1,8]. In recent years, deep learning approaches have been extensively adopted for automatic feature learning and classification. A summary of commonly used features is presented in Figure 3.

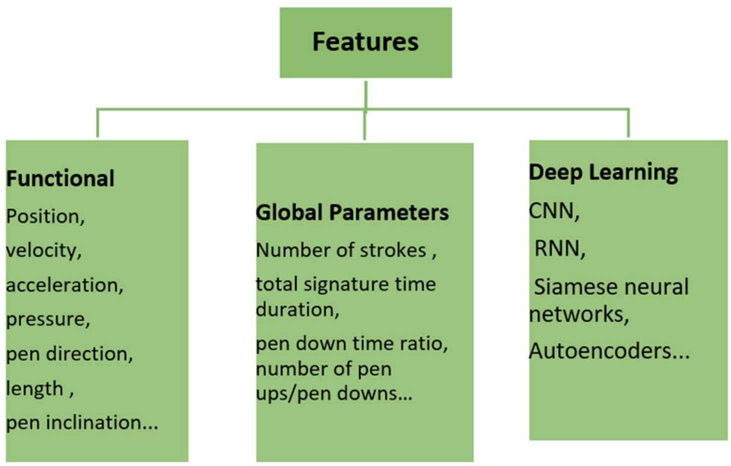

Figure 3. Types of feature extraction techniques

In the verification phase, the features extracted from a query signature are compared with the corresponding reference features stored in the knowledge base to establish whether the signature is genuine or forged. Figure 4 depicts some widely adopted verification techniques.

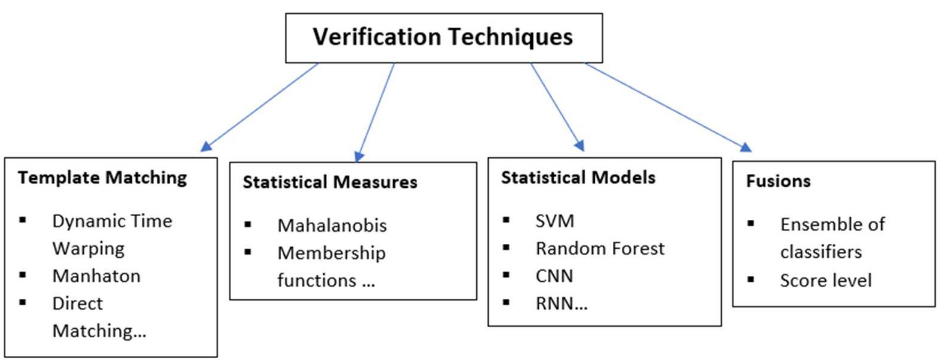

Figure 4. Types of Verification Techniques

III. Issues and Challenges

Nowadays, with the advent of technology, online signatures have become a de facto option in the modern world for most transactions, including various registration processes, internet banking, business contracts and the education sector. There are various devices through which signatures can be acquired, as depicted in Figure 2. These devices have different configurations, such as screen size, sensing technology, sampling frequency, spatial pixel density, etc. This difference in configuration has led to a new challenge, i.e. device interoperability issues. Device interoperability refers to the capability of a signature verification system to maintain consistent recognition performance across samples acquired from heterogeneous devices with varying sensor technologies, resolutions, sampling rates, and writing interfaces. Poor interoperability leads to increased intra-class variations and lower accuracy when signatures are captured using different devices or writing tools (stylus or finger) [2].

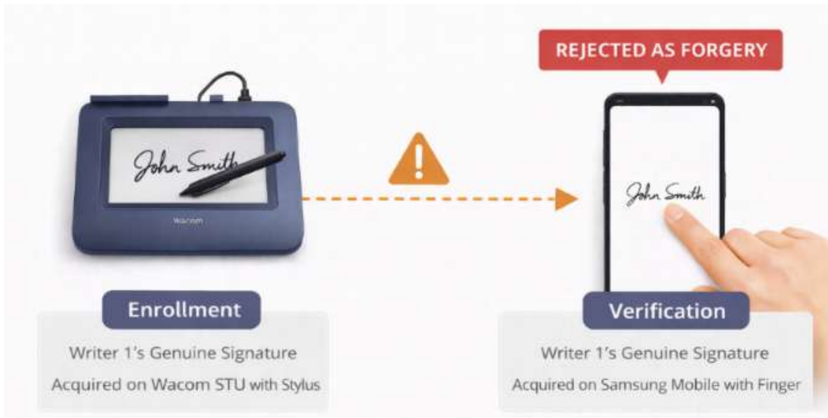

Figure 5. Illustration of an interoperability issue

Figure 5 illustrates the issue of device interoperability. In this scenario, during the enrolment phase genuine signature is acquired using a tablet with a stylus as a writing tool. Later, during the verification phase, the same signer's genuine signature is acquired using a different device with a finger as a writing tool. In this case, the trained model classifies the query signature as forged, even though the query signature is genuine. This happens due to a device interoperability issue, where different devices are used during the enrolment and verification phase.

Device interoperability issues occur due to the usage of various advanced devices for capturing signatures in diverse real-world applications. This problem has not been exploited much in the literature. Very few researchers have explored it in various dimensions. Pirlo et al. [3] analysed the effect of writing area on geometric features of online signatures. Since there were no benchmark datasets, the authors created a custom dataset to study the effect of writing area, and the study revealed that the writing area significantly influences the geometric features of signatures. Likewise, Tolosana et al. [4] aimed at attaining adaptability between signatures captured using diverse devices. Their method encompassed deriving global and temporal characteristics from online signatures, and the suggested method was examined on the BioSecure DS2 and DS3 datasets. The suggested model revealed that there is a significant improvement in the performance of the model. To resolve the issue of device interoperability, a new dataset named e-BioSign was created for online signatures and handwriting recognition [6]. This dataset constitutes signatures captured using five modern devices, including three devices specifically designed for signature and handwriting capture (Wacom tablets) and two general-purpose tablets (Samsung devices) well-suited for collecting data using both a stylus and a finger. Tolosana et al. [5] empirically assessed the implications of device interoperability using the multi-device e-BioSign dataset, which constitutes signatures acquired using five varieties of modern devices and two writing tools.

The authors benchmarked device interoperability under three contexts: inter-device, intra-device, and hybrid, to systematically examine interoperability challenges. The experimental results revealed that both device configuration and the writing instrument strongly influence the performance of classification systems. In [7], Impedovo et al. suggested a method in which signatures were first normalised using a transformation mapping, later succeeded by deploying a genetic algorithm to strengthen the similarity among signature samples. The efficacy of the suggested method was experimented on the e-BioSign dataset, yielding in an improvement of approximately 26%.

IV. DATASETS

This paper addresses the device interoperability challenge that has emerged due to the widespread use of electronic devices in commercial applications. This section discusses the datasets required to study device interoperability. The multi-device datasets considered are summarised in Table 2.

TABLE II: DESCRIPTION OF MULTIDEVICE DATASETS

Dataset	Writers	Device /writing tool	Genuine/ signer	Skilled forgeries	Sessions
e-BioSign DS1[6]	65	Wacom STU – 500(Stylus) Wacom STU – 530(Stylus) Wacom DTU – 1031(Stylus) Samsung Galaxy Note (Stylus /Finger) Samsung ATIV7(Stylus/Finger)	56	42	2
e-BioSign DS2[14]	81	Wacom STU-530 (Stylus) Samsung Galaxy Note 10.1(Stylus/Finger) Samsung Galaxy S3(Stylus/Finger)	40	30	2
SVC2021_EvalDB Office scenario Mobile scenario [13]	 75 119	 Wacom STU-530(Stylus) 94 different smartphones (Stylus/Finger)	 8 8	 16 16	 2 4
SUSIG [11]	100	WacomGraphire2 (stylus) ePad-nk(stylus)	20 (visual subcorpus) 810 (blind subcorpus)	10	2
SVC2004[12]	100	Wacom Intuos (stylus) PDA (stylus)	20	20	2

V. RESEARCH AVENUES IN ONLINE SIGNATURE VERIFICATION

This section provides research avenues related to online signature verification, specifically in a multi-device scenario.

A. Cross-device Signature verification

Since many devices, such as tablets, smartphones, and digital pens, are used to capture signatures that have different pressure sensitivities, sampling rates and resolutions. This leads to a major research direction to develop a model that can accurately verify signatures captured from heterogeneous devices.

B. Device – independent feature extraction

The feature extracted from pre-processed signatures plays a significant role in discriminating between authentic and fake signatures. Hence, extracting device invariant features that are not affected by the acquisition devices is required to develop an efficient verification system.

C. Low – cost device adaptation

The high-end dedicated devices that can accurately capture signatures' dynamic information are expensive and less accessible to all domains. But the alternative low-cost handheld devices fail to capture accurate dynamic information. However, researchers need to focus on improving the efficacy of verification models in this direction.

D. Signature Verification on Mobile Devices

Mobile devices are more commonly used for digital transactions as it is more convenient to carry anywhere. However, the use of mobile devices comes with many challenges such as varying screen size, limited sensing capability and inconsistent touch sampling, which demands more research in this area.

E. Real-Time Verification Systems

In real-time applications, there is a need for developing fast and lightweight algorithms, which is an important research direction. Here, the goal is to attain high accuracy with less computational cost.

F. Multimodal Device Integration

With the development in technology, recent devices can capture additional biometric information such as finger touch area, tilt angle, acceleration, and gyroscope data. Researchers are investigating how merging these signals might enhance the effectiveness of authentication.

VI. DISCUSSION AND CONCLUSION

The research on online signature verification began in the 1980s [16]. In those days, the devices available for signature acquisition were limited. Hence, the devices used for enrolment and verification were nearly the same configuration. However, in the era of growing technology, there are an ample number of devices available in the market for signature acquisition with a variety of configurations such as sampling rate, sensing technology, resolution, writing tools (Stylus/Finger) and screen size. This difference in specification creates interoperability issues, leading to intra-class variations. Due to intra-class variation, even the genuine signature acquired during the verification phase gets classified as a forged signature. Therefore, device interoperability issues lead to a large number of false rejections. Even, there are possibilities of inter-class similarity due to a device interoperability issue leading to false acceptance. This issue has been discussed in the literature [2], and needs to be addressed in order to develop a reliable verification system.

In this paper, a comprehensive survey is conducted to highlight the cause of the device interoperability issue. A detailed description of the consequences of the issue and the reason for addressing the issue is provided in the paper. This survey reveals the configuration of popular devices used for signature acquisition and also describes how differences in configuration lead to intra-subject variation and inter-subject similarity that result in false rejection and false acceptance. The multi-device datasets that are available for addressing this issue are discussed in the paper.

REFERENCES

[1] Diaz, M., Ferrer, M. A., Impedovo, D., Malik, M. I., Pirlo, G., & Plamondon, R. (2019). A perspective analysis of handwritten signature technology. Acm Computing Surveys (Csur), 51(6), 1-39.

[2] Impedovo, D., & Pirlo, G. (2018). Automatic signature verification in the mobile cloud scenario: survey and way ahead. IEEE Transactions on Emerging Topics in Computing, 9(1), 554-568.

[3] Pirlo, G., Rizzi, F., Vacca, A., & Impedovo, D. (2015, August). Interoperability of biometric systems: Analysis of geometric characteristics of handwritten signatures. In International Conference on Image Analysis and Processing (pp. 242-249). Cham: Springer International Publishing.

[4] Tolosana R, Vera-Rodriguez R, Ortega-Garcia J, Fierrez J (2015) Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification. IEEE Access 3:478–489 115.

[5] Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2017) Benchmarking desk top and mobile handwriting across COTS devices: The e-BioSign biometric database. PLoS ONE 12(5):e0176792

[6] Vera-Rodriguez, R., Tolosana, R., Ortega-Garcia, J., & Fierrez, J. (2015, March). e-BioSign: Stylus-and finger-input multi-device database for dynamic signature recognition. In 3rd International Workshop on Biometrics and Forensics (IWBF 2015) (pp. 1-6). IEEE.

[7] Bhavani, S. D., & Bharathi, R. K. (2024). A multi-dimensional review on handwritten signature verification: strengths and gaps. Multimedia Tools and Applications, 83(1), 2853-2894.

[8] Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: The state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(5), 609-635.

[9] Bibi, K., Naz, S., & Rehman, A. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79(1), 289-340.

[10] Kaur, H., & Kumar, M. (2023). Signature identification and verification techniques: state-of-the-art work. Journal of Ambient Intelligence and Humanized Computing, 14(2), 1027-1045.

[11] Kholmatov, A., & Yanikoglu, B. (2009). SUSIG: an on-line signature database, associated protocols and benchmark results. Pattern Analysis and Applications, 12(3), 227-236.

[12] Yeung, D. Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., & Rigoll, G. (2004, July). SVC2004: First international signature verification competition. In International conference on biometric authentication (pp. 16-22). Berlin, Heidelberg: Springer Berlin Heidelberg.

[13] Tolosana, R., Vera-Rodriguez, R., Gonzalez-Garcia, C., Fierrez, J., Rengifo, S., Morales, A., ... & Jabin, S. (2021, September). ICDAR 2021 competition on on-line signature verification. In International Conference on Document Analysis and Recognition (pp. 723-737). Cham: Springer International Publishing.

[14] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2021). DeepSign: Deep on-line signature verification. IEEE Transactions on Biometrics, Behavior, and Identity Science, 3(2), 229-239.

[15] Leclerc, F., & Plamondon, R. (1994). Automatic signature verification: The state of the art—1989–1993. International journal of pattern recognition and artificial intelligence, 8(03), 643-660.

[16] Plamondon, R., & Lorette, G. (1989). Automatic signature verification and writer identification—the state of the art. Pattern recognition, 22(2), 107-131.

[17] Sabourin, R., Plamondon, R., & Lorette, G. (1992). Off-line identification with handwritten signature images: Survey and perspectives. In Structured document image analysis (pp. 219-234). Berlin, Heidelberg: Springer Berlin Heidelberg.

[18] Singla, A., & Mittal, A. (2025). Exploring offline signature verification techniques: A survey based on methods and future directions. Multimedia Tools and Applications, 84(6), 2835-2875.

[19] Linden, J., Marquis, R., Bozza, S., & Taroni, F. (2018). Dynamic signatures: A review of dynamic feature variation and forensic methodology. Forensic science international, 291, 216-229.

[20] Saleem, M., & Kovari, B. (2020, June). Survey of preprocessing techniques and classification approaches in online signature verification. In International Conference on Image Analysis and Recognition (pp. 253-266). Cham: Springer International Publishing.

[21] Stauffer, M., Maergner, P., Fischer, A., & Riesen, K. (2020). A survey of state of the art methods employed in the offline signature verification process. New trends in business information systems and technology: digital innovation and digital business transformation, 17-30.
[22] Diaz, M., Fischer, A., Ferrer, M. A., & Plamondon, R. (2016). Dynamic signature verification system based on one real signature. IEEE transactions on cybernetics, 48(1), 228-239.
[23] Diaz-Cabrera, M., Ferrer, M. A., & Morales, A. (2015). Modeling the lexical morphology of western handwritten signatures. PloS one, 10(4), e0123254.
[24] Fischer, A., & Plamondon, R. (2016). Signature verification based on the kinematic theory of rapid human movements. IEEE Transactions on Human-Machine Systems, 47(2), 169-180.
[25] Tolosana, R., Vera-Rodriguez, R., Ortega-Garcia, J., & Fierrez, J. (2015). Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification. Ieee Access, 3, 478-489.
[26] Pirlo, G., Cuccovillo, V., Diaz-Cabrera, M., Impedovo, D., & Mignone, P. (2015). Multidomain verification of dynamic signatures using local stability analysis. IEEE Transactions on Human-Machine Systems, 45(6), 805-810.
[27] Yahyatabar, M. E., Baleghi, Y., & Karami, M. R. (2013, May). Online signature verification: A Persian-language specific approach. In 2013 21st Iranian Conference on Electrical Engineering (ICEE) (pp. 1-6). IEEE.