Received: 24 May 2026 | Revised: 23 July 2026 | Accepted: 11 August 2026 | Published online: 26 August 2026

REVIEW

Smart Wearable Technology
2026, Vol. 00(00) 1–15
DOI: 10.47852/bonviewSWT620210519

BON VIEW PUBLISHING

A Comprehensive Survey of Pattern Recognition, Deep Learning, and Wearable Technology Approaches for Secure Signature Verification Systems

Amal Hameed Khaleel[1,*] **and Suhad Muhajer Kareem**[2]

[1] *Department of Computer Science, University of Basrah, Iraq*

[2] *Department of Cyber Security, University of Basrah, Iraq*

Abstract: Automatic signature verification is a complex biometric authentication problem because signatures involve intent, distinct writing styles, visual texture, and motor dynamics. This review consolidates signature verification work involving offline, online, mobile, contactless, and in-air verification. The reviewed works show a clear shift from traditional classifiers and handcrafted descriptors toward deep metric learning, convolutional feature extractors, capsule models, and recurrent temporal models. Stronger image-level representation does not mean deployment-ready security. There are still many modern cyberattacks and challenges related to skilled forgery, replay attacks, presentation attacks, sensor variability, demographic and cross-linguistic transfer, data scarcity, and privacy-preserving learning. Thus, the paper analyzes those challenges and presents an original, practical taxonomy for over 50 selected works and standards. It also outlines available datasets and measures of performance and suggests a set of best-case solutions in the context of a given operational constraint, an expanded wearable-technology analysis, and a trustworthiness framework for explainable and auditable biometric decision-making. The future works for secure biometric services are the integration of advanced computer vision, calibrated and reliable security thresholds, a range of methods for detection of presentation attacks, assurance of cancellability, continuous post-deployment assessment, and privacy are some key components.

Keywords: signature verification, computer vision, cybersecurity, wearable technologies, explainable AI

1. Introduction

Even though many processes have gone digital, handwritten signatures are still legally and socially recognized as identity verification. These include processes in banking, contracts, dealings with government records, health administration, the field of document forensics, and others. Given this context, automatic signature verification demands an interesting mix of handwriting pattern identification required by the field of computer vision alongside the protection of a high-value process in which cyberspace identities may be imitated or forged, while stored biometric templates may also be compromised [1, 2].

The field is typically defined in terms of offline and online verification. Offline systems deal with static images created through scanners, cameras, or document workflows, thus relying on the visual representation of the signature such as stroke shapes, contours, textures, spacing, and local structures. On the other hand, online systems deal with dynamic traces of signature creation, which include the x-y coordinates and the pressure, velocity, and acceleration of the signing action, pen-up versus pen-down events, and in some situations, motion of the signing device. Optimal signature verification is tied to the quality of the sensors and the protocols employed [3–6].

The benchmark for this field has changed with time. Old systems employed handcrafted features and relied on traditional classifiers. Today's systems, on the other hand, employ various methods including convolutional neural networks (CNNs), Siamese networks, triplet loss, capsule networks, Recurrent Neural Network (RNN)/Long Short-Term Memory (LSTM) models, spatial transformer networks, hybrid graph structures, and attention modules. These methods, as well as hybrid designs of ResNet and transformers, among others, have the advantage of flexibility to build new types of systems employing raw images or dynamic traces but have the disadvantage of being tied to a training protocol, diversity of the dataset, and secure deployment practice [7–12].

A review paper becomes important in the presence of a fragmented literature spread across document analysis, biometrics, pattern recognition, deep learning, mobile authentication, cybersecurity, and their forensic applications. While many papers

***Corresponding author:** Amal Hameed Khaleel, Department of Computer Science, University of Basrah, Iraq. Email: amal.khaleel@uobasrah.edu.iq

claim high accuracy on specific datasets, comparisons are difficult since papers operate under different writer-dependent or writer-independent protocols, various forgery types, different amounts of reference signatures, and different metrics such as accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR) [2, 13–15]. This review offers a consolidated taxonomy, a comparative analysis of model families, a cybersecurity-centric system perspective, and a deployment-oriented research agenda.

2. Review Scope and Selection Strategy

This review emphasizes studies that consist of techniques and models concerning offline, online, mobile, and in-air signature verification, deep metric learning, transformers, template protection, learning with privacy, biometric authentication, and multi-factor authentication [15–21].

Studies were categorized by acquisition mode, feature representation, architecture of learning, dimension of evaluation, security contribution, and relevance of use [7, 17, 22].

The corpus formed exceeds 50 papers and standards, where the focus was on practical signature verification services. Rather than papers being assessed by single accuracy, the review was based on methodologies, reproducibility, threat coverage, scalability, and suitability for practical services. This is of high relevance, as methods may be good at random forgeries, but they fail at skilled forgeries or cross-device deployment [2, 13]. The review questions and synthesis dimensions are shown in Table 1.

2.1. Structured search strategy and reproducible screening protocol

This survey is a structured, task-oriented review. The aim is to build a reproducible evidence map for signature verification across offline, online, mobile, contactless, wearable-assisted, and security-aware settings. The structured search, screening, and synthesis protocol added to improve reproducibility is shown in Table 2.

Searches were organized around six concept blocks: (i) signature verification and forgery detection; (ii) offline image-based and computer vision approaches; (iii) online/mobile dynamic signatures; (iv) Siamese, triplet, CNN, transformer, recurrent, and generative models; (v) wearable, in-air, inertial measurement unit (IMU), smart pen, smartwatch, and sensor-fusion data; and (vi) cybersecurity, template protection, presentation attack detection (PAD), explainable AI, and trustworthy biometric auditing. The search string combined terms such as "offline signature verification," "online signature verification," "writer-independent verification," "skilled forgery," "deep metric learning," "Siamese network," "transformer," "wearable sensor," "IMU," "smart pen," "presentation attack detection," "cancellable biometrics," and "explainable biometrics."

The screened sources were taken from major scholarly databases and publisher platforms, including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Wiley, MDPI, PubMed/PMC, and Google Scholar for backward/forward snowballing. The primary time window was 2020–2026, while older landmark works were retained only when they defined a

Table 1
Review questions and synthesis dimensions

Dimension	Review question	Why it matters
Acquisition mode	Is the system offline, online, mobile, contactless, or in-air?	Determines available features and attack surface
Representation	Are features handcrafted, CNN-based, temporal, metric learning, or transformer-based?	Controls generalization and interpretability
Security	Does the work handle skilled forgery, replay, presentation attacks, or template privacy?	Separates academic accuracy from deployable authentication
Evaluation	Which metrics and protocols are used?	Enables fair comparison across datasets and thresholds

Table 2
Structured search, screening, and synthesis protocol added to improve reproducibility

Method item	Specification added in the revised manuscript
Databases/platforms	*IEEE Xplore; ACM Digital Library; ScienceDirect; SpringerLink; Wiley; MDPI; PubMed/PMC; Google Scholar; ISO/IEC* and *NIST* standards pages
Period covered	Main focus: 2020–2026; older landmark sources retained only for datasets, protocols, standards, or foundational template-protection concepts
Inclusion criteria	Peer-reviewed journal/conference papers, recognized standards, benchmark/dataset papers, and studies reporting acquisition mode, method, protocol, and evaluation metric
Exclusion criteria	Opinion-only papers, inaccessible full text, duplicated reports, unclear acquisition protocol, missing evaluation metric, and papers unrelated to signature/handwriting biometrics
Screening log	186 candidate records were considered; 38 duplicates were removed; 148 titles/abstracts were screened; 64 full texts were assessed; 52 sources were retained in the final cited corpus
Synthesis method	Narrative and comparative synthesis by modality, model family, evaluation protocol, security risk, explainability, and deployment constraints

dataset, protocol, terminology, or template-protection concept that remains necessary for interpretation.

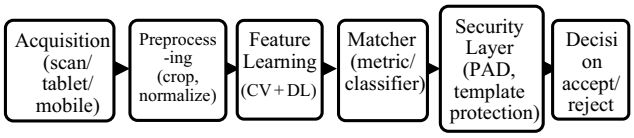
3. Technical Background

Pattern recognition for signature verification involves the following stages: acquisition, preprocessing, feature extraction/learning, matching/classification, thresholding, and decision reporting. In traditional pipelines, these stages are distinct and separate, while in deep learning pipelines, feature extraction and similarity learning are integrated into a trainable end-to-end model [1, 3, 9]. Offline verification of signatures is a unique case in computer vision. Signature images tend to be sparse, extremely writer-specific, and subject to signature scanning artifacts. Signatures are usually defined by thin strokes rather than object-like areas, so preprocessing (binarization, skeletonization, cropping, scaling, denoising, slant, background removal, etc.) is disproportionately significant [2, 10, 23].

Online verification is considered similar to time-based biometric authentication. Here, the signature is represented as a multivariate temporal signal for modeling. It enables the use of various elements such as order, pressure, velocity, acceleration, pauses, and rhythm. However, it makes verification less effective due to static image copying and introduces various limitations such as sensor dependence, mobile-device variability, and privacy concerns, as explaining dynamic behavior may lead to the user revealing some of their stable personal traits [4, 6, 17].

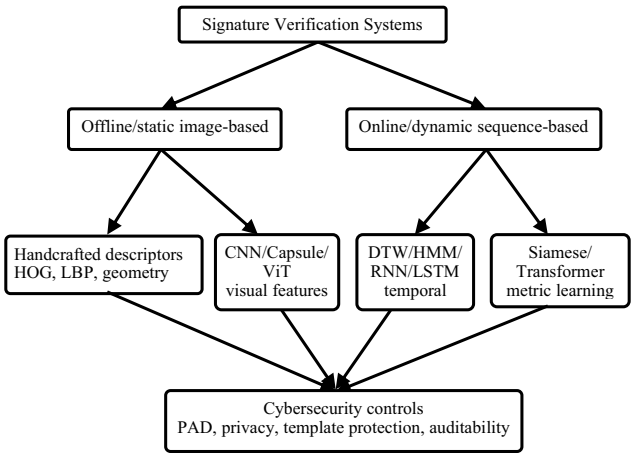
From a cybersecurity standpoint, signature verification cannot be equated to a password check. Passwords are easily changeable, but biometric traits are not. Consequently, leaked signature templates provide a basis for forgery and impersonation. Therefore, modern systems must implement template protection, revocability, and encryption, as well as access controls, presentation attack detection, and retention policies [16, 19, 20, 24, 25]. Figure 1 is used as an analytical map. The left side represents data acquisition and representation learning, while the right side identifies the security control points where PAD, template protection, threshold calibration, logging, and human escalation must be applied. This clarifies that high recognition accuracy alone is insufficient unless the pipeline also protects the acquisition channel, stored template, decision threshold, and post-deployment audit trail.

Figure 1
Generic signature verification pipeline integrating computer vision, matching, and cybersecurity controls



Offline/static image-based systems use handcrafted descriptors, CNN/CapsNet/ViT visual features, and Siamese or Transformer metric learning. Online/dynamic sequence-based systems use Dynamic Time Warping (DTW), Hidden Markov Model (HMM), RNN, LSTM, pressure, velocity, acceleration, rhythm, and pen-up/down evidence. Both branches require security controls: PAD/liveness, template protection, privacy, calibrated thresholds, and auditability. Figure 2 is interpreted as a taxonomy of evidence availability. Offline methods operate mainly on visual stroke morphology; online methods add temporal dynamics; wearable-assisted and in-air methods add inertial, pressure, and motion streams. The taxonomy therefore explains why performance comparisons must be stratified by acquisition mode instead of pooling all signature verification studies into a single accuracy leaderboard.

Figure 2
Taxonomy of signature verification approaches



4. Offline, Online, Mobile, and Contactless Signatures

Offline signature verification is the most common situation studied because a signature is the most common feature of checks, forms, contracts, and archival documents. The limitation of offline signature verification systems is the absence of indicators of dynamic evidence. Therefore, systems must work on inferring the signature's authenticity from its visual shape. Offline systems are particularly vulnerable to forgeries and to dataset biases due to the writing instrument, the paper, the image resolution, and the acquisition [2, 7, 10, 26].

The verification of online signatures utilizes dynamic evidence, and therefore, systems can work on modeling the dynamic behavior of signers rather than on the final state of the ink. Recent online systems such as Deep Sign and others show that the use of recurrent and synchronized modeling improves the systems' effectiveness against forgeries if consistent dynamic evidence is provided. Still, online datasets vary in the number and type of signing devices, number of participants, number of reference signatures, and number of impostor signers [4, 13, 14, 27].

The use of mobile devices for signature verification has become a necessity due to the ability of mobile devices to collect both coordinate and pressure traces. Existing lighter models of mobile-signature verification using CNNs are capable of signature verification based on the collected coordinate and pressure traces, but main issues persist in the balance between the shape of the models and the efficiency in signature verification [6, 28].

5. Pattern Recognition and Machine Learning Foundations

Description, plus geometrical, structural, statistical, and textural descriptors, such as aspect ratio, stroke density, projection profile, contour features, local binary patterns, histograms of oriented gradients, and keypoint descriptors. While they remain useful for small datasets because they are interpretable, computationally inexpensive, and easier to audit, they often remain

ineffective for large intra-writer variations and skilled imitations [2, 9, 23].

Classic classifiers, such as K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Random Forests (RFs), HMMs, and DTWs, remain important baselines. While the limited accuracy of such methods provides the ability to draw a calibrated line of the decision boundary, the limited representation learning of such methods remains an important limitation [3, 4, 13].

Hybrid systems process the data, use handcrafted descriptors, and integrate optimization and machine learning. Recent work, similar to Sign Guard, shows that optimization-driven data preprocessing and selection of descriptors can remain competitive, especially in a controlled offline verification pipeline that has explainable components. These systems become more appealing in institutional settings, even with marginal accuracy gains [8, 29].

6. Deep Learning Approaches

CNNs are the primary deep learning method on the market for offline signature verification, as they learn and identify local patterns and fragments in image-based signatures. CNNs also require fewer manual inputs when compared to traditional algorithms, but they are limited by the number of available samples. Furthermore, CNNs are prone to learning the signature capture artifacts and not the signatures themselves [30].

To improve upon CNNs, more complex network architectures have been used to model the spatial relationships that exist between components of a signature. One such model is CBCapsNet, which employs a combination of CNNs and capsule networks to model the spatial components of signatures. Capturing the spatial relationships of signature verification is an important property; however, more traditional architectures (CNNs and Siamese networks) have received more extensive evaluation than capsule networks, and as a result, analytical performance in signature verification may be lacking [31].

The use of Siamese and triplet networks is prevalent in signature verification networks, as the task of signature verification is also inherently a similarity task. Unlike traditional classification models where a writer is assigned to a static class, within the context of a signature verification network, it is up to the model to determine the spatial distributions of the samples (i.e., signatures) in the learned space. Overall, the ability of the models to perform writer-independent signature verification and also to allow for few-shot integration is defined by the way paired (or triplet) samples are selected, as well as the network loss function [32, 33].

Current state-of-the-art Siamese models, such as the two-stage Siamese-STN model for signature verification, implement the use of a focal loss component in combination with a spatial transformer to focus the network's attention on the more informative parts of a signature sample and to better address class imbalance.

Models working with sequential data, particularly recurrent and temporal models, should be adopted for online signature verification due to the sequential nature of signing. RNNs, LSTMs, and time-aligned recurrent networks can learn patterns of speed, rhythm, and pressure and handle temporal warping. Although these models are preferred over static features for online data, they still need to be tested under conditions of behavioral changes and long-term transfer between devices [4, 13, 34, 35].

Transformers and hybrid ResNet-transformer models are likely to improve the boundary features of both offline and online signatures due to attention mechanisms that learn long-range dependencies and multi-scale structures. Signatures can be verified within their correct context. ResT-type systems and graph-attention transformers are likely to improve the boundary features of both online and offline signatures. For signature verification, they may serve better in the highest security scenarios [3, 15, 36].

Hong et al. [21] also describe generative models in terms of augmentation, augmentation attacks, and liveness tests. Diffusion-based synthetic signature generation can help address the concern of signature rarity and can serve to stress-test signature verification systems. However, generative models can be used by attackers to create convincing forgeries. For this reason, stick to provenance controls, attack simulations, and clear evaluation of skilled forgeries [21, 37–39]. Table 3 shows a simplified comparison between major model families and deployment trade-offs, while Table 4 shows a comparison from another perspective between major signature verification model families.

Table 3
Friendly comparison of major model families and deployment trade-offs

Model family	Strength	Main risk	Best use
Handcrafted + SVM	Interpretable, small data	Weak skilled-forgery model	Legacy/low-resource
CNN/CapsNet	Strong visual features	Domain shift, overfitting	Offline images
Siamese/Triplet	Few-shot similarity	Pair sampling sensitivity	Writer-independent Offline Signature Verification (OSV)
RNN/LSTM	Temporal structure	Sensor dependence	Online signatures
Transformer/Hybrid	Long-range structure	Data and compute demand	High-value deployments

Table 4
Comparative synthesis of major signature verification model families

Family	Main strength	Main limitation	Recommended use	Key refs.
Handcrafted descriptors + SVM/KNN	Low data requirement, interpretable, fast	Limited robustness to skilled forgeries and domain shift	Small institutional systems, baseline experiments	[2, 9, 23]
CNN feature learning	Strong visual representation and end-to-end training	Overfitting and acquisition-artifact learning	Offline scanned signatures and cheque images	[10, 37–40]

(*Continued*)

Table 4
(*Continued*)

Family	Main strength	Main limitation	Recommended use	Key refs.
Capsule networks	Better spatial relationship modeling	Less standardized benchmarking	Writer-independent offline verification	[11, 41]
Siamese/triplet metric learning	Few-shot enrollment and writer-independent matching	Sensitive to pair/triplet sampling and thresholds	Banking, document verification, low-reference users	[7, 12, 42]
RNN/LSTM/Temporal Attention-Recurrent Neural Network (TA-RNN)	Models signing rhythm and dynamics	Requires online sensors and stable protocols	Tablet/mobile online signatures	[4, 13, 33]
Transformer/hybrid attention	Long-range and multi-scale modeling	High compute and data demand	High-value secure verification	[3, 15, 35]
Federated/privacy-preserving learning	Keeps training data distributed	Communication, heterogeneity, audit complexity	Cross-institutional banking and e-health	[18, 43]
Template protection/cancellable biometrics	Reduces damage from template compromise	Possible accuracy loss and implementation complexity	Regulated authentication services	[19, 24, 44]

6.1. Critical synthesis of model behavior, trade-offs, and failure cases

A critical interpretation of the reviewed studies shows that higher accuracy is usually not attributable to a single architectural label but to the interaction among feature granularity, training protocol, forgery difficulty, and sensor consistency. CNNs and capsule-based systems are effective under stable visual acquisition conditions because they learn local stroke texture, contour shape, and spatial arrangement. However, they can overfit scanner noise, background texture, pen thickness, or dataset-specific preprocessing. Siamese and triplet networks are more suitable for writer-independent verification because the task is fundamentally a similarity decision, but their performance depends strongly on pair/triplet mining, positive-negative imbalance, and calibrated operating thresholds [7, 10, 12, 32, 45].

Deep models may fail in four recurring situations: (1) skilled forgeries that closely reproduce the global outline while differing only in line quality or microstructure; (2) cross-dataset deployment where the scanner, camera, tablet, stylus, or smartphone changes; (3) low-reference enrollment, where the model has too few genuine samples to estimate intra-writer variability; and (4) adversarial or operational attacks, such as replayed online traces, synthetic-image injection, template compromise, and preprocessing manipulation. Therefore, reported accuracy should be interpreted together with FAR/FRR/EER curves, operating thresholds, calibration plots, latency, and a description of random, simple, and skilled-forgery protocols [6, 13, 16, 19, 20].

The review therefore distinguishes performance-oriented gains from deployment-oriented trust. Handcrafted descriptors remain weaker against skilled forgery but are easier to explain, audit, and reproduce. CNNs provide strong visual features but require dataset diversity. Temporal RNN/LSTM models capture pressure, velocity, and rhythm but are sensor-dependent. Transformers and hybrid attention models can model long-range dependencies, but their data and computational requirements make them less suitable for low-power or legally auditable settings unless accompanied by calibration, uncertainty reporting, and human-review workflows.

Dataset limitations are not merely a matter of sample size. Many public datasets are collected in controlled sessions with limited device diversity, limited time gaps between sessions, and a limited number of skilled forgers. This weakens ecological validity for banking, government, and legal-document workflows in which signatures may be captured across years, devices, languages, stress levels, health states, paper conditions, and acquisition channels. For this reason, a more robust benchmarking protocol should include at least three levels: intra-dataset testing, cross-dataset testing, and stress testing under adverse acquisition or attack conditions. For offline signatures, stress tests should include scanner/camera variation, compression, blur, background artifacts, and pen-type variation. For online and wearable signatures, stress tests should include sampling-rate changes, pressure quantization, device substitution, delayed or missing sensor streams, and replayed traces. These conditions directly connect dataset design to the security and reliability claims made by the system.

7. Datasets, Protocols, and Evaluation Metrics

Signature verification relies heavily on systems and devices and forgery protocols. As a result, public datasets are important, such as BHSig260, DeepSignDB, CEDAR, GPDS, MCYT, BioSecure, SigComp, SVC2021_EvalDB, and various other datasets. Although many researchers use these datasets, this does not ensure their practical implementations, as many datasets differ in size compared to each other and compared to real-world systems like eGovernment or banking [4, 13, 14, 28, 46]. The common datasets and evaluation concerns in recent signature verification studies are shown in Table 5.

For signatures, FAR is defined as the percentage of forgeries that are accepted as genuine, and on the other hand, FRR is the percentage of genuine signatures that are rejected, while the EER represents the point where FAR and FRR converge. These data should be reported as signatures are threshold-sensitive and not as a number that states the overall correctness of the algorithm. Additionally, the precision, recall, F1-score, and receiver operating characteristic curve should be reported [2, 13, 14].

Table 5
Common datasets and evaluation concerns in recent signature verification studies

Dataset/setting	Typical modality	Strength	Evaluation concern
CEDAR/GPDS/BHSig260	Offline images	Common baselines for scanned signatures	Protocols vary; not always deployment-like
MCYT/BioSecure	Online and multimodal traces	Dynamic temporal and pressure information	Device dependence and older acquisition conditions
SigComp/4NSigComp	Offline and online tasks	Competition-style evaluation	Limited scale and language-specific effects
DeepSignDB/SVC2021_EvalDB	Online signatures	Large-scale benchmark and ongoing competition	Requires consistent protocol reporting
Mobile signatures	Online/mobile traces	Closer to modern smartphones and tablets	Device, posture, and touch/stylus variability
In-air/contactless signatures	Trajectory or vision-based dynamics	Useful for touchless authentication	Replay, camera, and reconstruction risks

Finally, providing FAR, FRR, and EER is not enough if the comparison of testers is not reported, if the testing was conducted under a proven (controlled) or random environment, what the thresholds were, and in what way confidence intervals were interpreted. The accuracy and generalization of the tested models would be provided relative to very different tasks, since the same results can indicate very different measurements [7, 10, 13].

7.1. Quantitative performance ranges and cross-dataset interpretation

The survey presents an evidence map in Table 6 that reports representative performance ranges from the reviewed literature. The quantitative pattern supports a central conclusion: strong numbers in offline image datasets do not automatically transfer to online, mobile, wearable, or in-air deployment. As the acquisition channel becomes richer, the model gains behavioral evidence, but the attack surface also expands to replay, injection, device substitution, synchronization errors, and template privacy risks. Therefore, the discussion now connects accuracy, EER, FAR, FRR, computational cost, and sensor conditions, rather than relying on accuracy alone.

8. Cybersecurity and Computer Vision Considerations

Signature verification systems can be deceived by simple and advanced forgeries, replaying captured traces, image injections, synthetic signatures, and templates. Additionally, templates can

Table 6
Quantitative evidence map across representative datasets and model families

Model family/setting	Dataset or protocol	Representative reported performance	Interpretation for this review	Refs.
Triplet/Siamese similarity model	4NSigComp2010, SigComp2011, 4NSigComp2012, BHSig260, CEDAR	Accuracy around 86.1–93.5%; FAR about 3.7–6.8%; FRR about 3.1–4.5 in the reported tSSN experiments	Metric learning improves writer-independent matching, but CEDAR and cross-validation results show that generalization can fall when datasets are smaller or more heterogeneous	[12]
Hybrid handcrafted + ML optimization	CEDAR, SID, BHSig260, DeepSignVault	Reported accuracy reached 98.77% with Orthogonal Combination of Centre Symmetric Local Binary Patterns (OC-CSLBP) and 97.46% with Centre Symmetric Local Binary Pattern (CSLBP) in SignGuard experiments	Optimized handcrafted descriptors remain competitive when protocols are controlled and features are well aligned with stroke texture	[8]
Online sequence-to-image/temporal fusion	MCYT-100 and SVC-2004 task 2	2D-MFFnet + Temporal Convolutional Network (TCN) reported 93.74% accuracy/6.45% EER on MCYT-100 and 89.55% accuracy/10.57% EER on SVC-2004 task 2	Online systems benefit from dynamic information, but EER increases on more difficult cross-device or low-sample protocols	[14]

(*Continued*)

Table 6
(*Continued*)

Model family/setting	Dataset or protocol	Representative reported performance	Interpretation for this review	Refs.
Open online benchmark competition	SVC-onGoing tasks	Best reported EER values included 3.33%, 7.41%, and 6.04% across the benchmark tasks	Common benchmarks help reveal scenario difficulty; mobile/finger tasks can be harder than stylus/office tasks	[13]
Mobile online signatures	MobiBits subset/mobile devices	Reported EER values included approximately 0.63% for random forgeries and 6.66% for skilled forgeries	Pressure and coordinate traces support mobile verification, but skilled forgeries remain harder and cross-device calibration matters	[6]
Wearable/sensor-fusion handwriting biometrics	60-participant sensor-fusion handwriting dataset	Reported recognition accuracy was 0.982 for signatures, 0.927 for words, 0.884 for short sentences, and 0.661 for letters	Sensor fusion can be strong for signature-level motor patterns, but ablation and modality reporting are required to avoid redundant or noisy sensors	[47]
In-air contactless signatures	25 participants; 200 positive/negative pairs; 300 LTSO splits	Average accuracy 85%, F1-score 85%, and recall 91%	Contactless signatures are feasible but still below mature offline/online benchmarks; larger public datasets and replay/PAD testing are needed	[17]

be stolen, and threshold-level probing and inputs can be modified. A computer vision model that performs well on a closed benchmark may be ineffective unless integrated into a strong authentication system [16, 19, 24, 37].

PAD is essential when capture channels are vulnerable to being spoofed. Presentation attacks occurring during offline document workflows may consist of signed documents being printed, copied, and pasted, while online document workflows may be attacked via trace replay or sensor injections. Presentation attacks occurring during in-air document workflows may consist of documents undergoing video replay or motion reconstruction. When it comes to signature verification services, ISO/IEC 30107 provides a terminology and evaluation framework for biometric PAD, which can be easily tailored to support signature verification [16, 20].

Template protection is one of the most important cybersecurity needs due to the fact that biometric templates are often considered sensitive and nearly impossible to revoke. Various non-invertible transformations; cancellable, sealed, or trusted templates; secure settings; and secure, sealed, or trusted execution environments and risk-optimized federated learning may help to reduce the risk, but it is important that all of the above are carefully assessed from perspectives of performance of recognition and irreversibility. An added value of a secure setting design is the safe separation of raw acquisition information from templates and limiting the use of deep, long-term deposits [18, 19, 24, 48].

The guidance NIST SP 800-63B-4 provides is critical for authenticator assurance and risk management for secure authentication life cycle management. For signature verification, this probably means signatures will rarely be the sole isolating factor for high-risk access and will probably be most often coupled with device binding, document verification, liveness or PAD, context of the transaction, and human escalation for unclear decision situations [24, 49].

Security is affected by many factors when it comes to computer vision. Overly aggressive or heavy noise reduction may remove signs of forgery. Uncontrolled background noise and artifacts coupled with strong preprocessing may help minimize background artifacts and scanning noise. Possibly the best safe approach is to determine the overall quality of the scan by considering visual quality as well as FAR, FRR, EER, and the effect of forgery quality on the results [2, 7, 10].

The importance of explainability and auditability cannot be overstated because signature verification may impact legal or financial outcomes. Systems cannot replace expert forensic judgment. They provide confidence scores, evidence maps, and uncertainty flags, among other outputs, for reviewable, mutually agreeable decisions and automation. They help reduce the risk of unchallengeable black box rejection [8, 15, 32, 50].

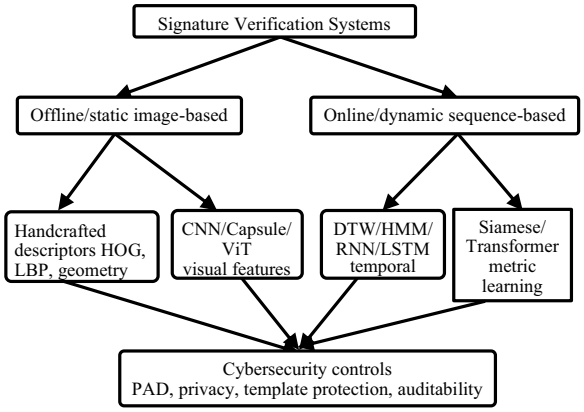
8.1. Explainability, trustworthiness, and audit requirements

Because signature verification may influence financial authorization, contractual validity, and forensic screening, explainability should be treated as part of the security case rather than as an optional visualization. A trustworthy system should report (i) local evidence maps showing which strokes, regions, or temporal segments influenced the decision; (ii) calibrated similarity scores with uncertainty intervals; (iii) threshold rationale for low-risk and high-risk use cases; (iv) audit logs documenting acquisition device, preprocessing, model version, template version, and reviewer override; and (v) periodic error analysis for false accepts, false rejects, and demographic or script-related bias [24, 45, 51].

Trustworthiness also requires lifecycle governance. ISO/IEC 23894 frames AI risk management as an organizational process, while ISO/IEC 24745 focuses on confidentiality, integrity,

renewability/revocability, and privacy of biometric information. In a signature verification service, these principles translate into model-version control, template revocation, risk-based access control, post-deployment drift monitoring, fairness testing across scripts and user groups, and incident response when a template or capture device is compromised [51, 52]. The cybersecurity threat model for signature verification as a biometric authentication service is shown in Figure 3.

Figure 3
Cybersecurity threat model for signature verification as a biometric authentication service



Explanations must also be validated. Saliency maps or attention weights can be misleading if they highlight background artifacts or scanner noise rather than signature evidence. Therefore, an explainability protocol should combine quantitative checks, such as deletion/insertion sensitivity, with expert review of disputed cases. For legal or high-value financial settings, the model output should be considered decision support: the system should provide a confidence score, an uncertainty warning, and a reason code, while borderline cases should be escalated to a human expert instead of being automatically accepted or rejected.

8.2. Consolidated cybersecurity and deployment interpretation

The cybersecurity argument is consolidated into three non-overlapping layers. First, the acquisition layer addresses presentation attacks, replay, sensor injection, and document-image manipulation. Second, the template and model layer addresses non-invertibility, cancellability, encryption, model extraction, adversarial probing, and threshold manipulation. Third, the service layer addresses audit logging, retention, human escalation, bias monitoring, and periodic recalibration. Later sections now refer back to these layers and discuss only modality-specific risks, especially those introduced by wearables and contactless capture.

The practical trade-off is that high-security deployments should not select the highest-accuracy model if that model lacks calibrated decision scores, a documented threshold policy, failure-case analysis, template protection, and PAD testing. Conversely, low-resource deployments may reasonably choose an interpretable handcrafted or compact CNN baseline when the system is explicitly positioned as decision support and when borderline cases are escalated to human review.

9. Representative Literature from Recent Years

This section presents studies and recent literature, along with their associated standards. Table 7 shows what each study or paper contributes to the secure design of signature verification systems through computer vision. It does not intend to say which method is superior, as results depend on the protocols.

10. Wearable Technologies in Secure Signature Verification

Wearable technology significantly enhances signature verification processes by capturing motor behaviors of the signer.

Table 7
Studies in the secure design of signature verification systems

Study	Mode	Main approach	Contribution
Tolosana et al. [4]	Online	TA-RNN, DeepSignDB, benchmark protocol	Strong online dynamic baseline
Liu et al. [10]	Offline	Region-based deep metric learning	Local region features for skilled forgery
Parcham et al. [11]	Offline	CNN + Capsule network	Spatial relationship modeling
Tolosana et al. [13]	Online	SVC-onGoing benchmark	Open benchmarking and protocols
Xamxidin et al. [23]	Offline	Multilingual verification network	Cross-language verification issue
Fatihia et al. [38]	Offline	CNN with batch normalization	Training stability and optimization
Ishfaq et al. [3]	Offline	Hybrid vision transformer	Attention-based visual verification
Tehsin et al. [12]	Offline	Triplet Siamese similarity network	Metric learning across datasets
Roszczewska et al. [6]	Online/mobile	Light CNN using coordinates and pressure	Mobile-device feasibility
Luan et al. [14]	Online	Relative position matrix + 2D-MFFnet	Temporal-to-image conversion
Hong et al. [21]	Offline/generative	Denoising Diffusion Probabilistic Model (DDPM) signature generation	Augmentation and synthetic-risk discussion

(*Continued*)

Table 7
(*Continued*)

Study	Mode	Main approach	Contribution
Salkanovic et al. [28]	Hybrid sensing	Sensor-fusion apparatus	Multimodal data acquisition
Xiao and Wu [7]	Offline	Siamese + spatial transformer + focal loss	Attention to imbalance and local features
Yilmaz and Öztürk [26]	Offline	Vanilla CNN analysis	Simplicity versus complexity argument
Salkanovic et al. [47]	Hybrid sensing	Contextual handwriting with sensor fusion	Sensor fusion for dynamic traits
Hayat et al. [19]	Online/security	Non-invertible template protection	Cybersecurity and template privacy
Kakade and Raut [1]	Biometric security	Biometric authentication trends	System-level biometric security context
Wang et al. [15]	Offline	ResNet + Transformer (ResT)	Multi-scale visual feature extraction
Rathore et al. [8]	Offline	SignGuard hybrid ML + Grey Wolf Optimization (GWO)	Optimized preprocessing and hybrid ML
Salturk et al. [17]	In-air	Deep Siamese contactless verification	Touchless dynamic biometric direction
Veraros et al. [18]	Offline/privacy	Federated learning for signature verification	Privacy-preserving cross-site learning
Huang et al. [34]	Online	Hybrid online multi-class verification	Modern online classifier comparison

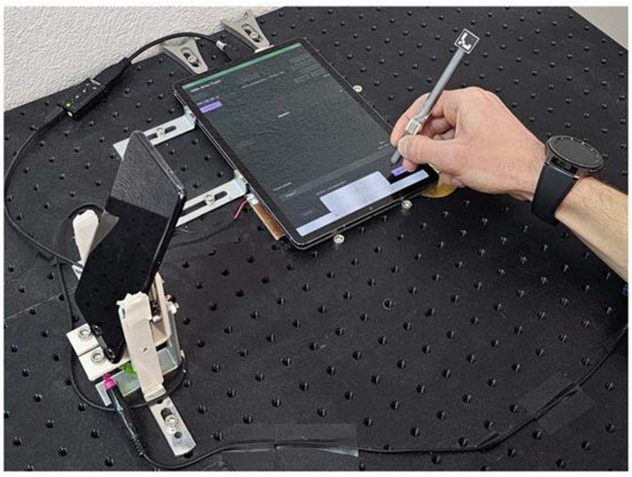
Offline verification focuses mainly on the signature's visual end state. Systems that integrate wearables can capture a signer's signatures along with the data of time, consistency, and variations of acceleration, tilt, pressure, angular velocity, and grip. In online, in-air, and mobile signatures, distinguishing a signer's natural movements from those of a forger can be done thanks to these additional data [6, 17, 28, 47].

Smart pens and styluses, smartwatches, wristbands, smart rings, and IMUs remain the most readily available sources of wearables. Smart pens and styluses capture data for pen-up/pen-down events, tilt, pressure, and detailed traces. Wristbands and smartwatches capture wrist movements in signing through rotational and linear accelerations. Rings and finger sensors capture movement and tremors in a more detailed way. In contactless scenarios, these data can be used to support in-air signature verification in combination with camera-based models and trajectory-based models [17, 22, 28]. From the standpoint of modeling, data from wearables should be treated as a time-series stream that is synchronized and continuous. A sophisticated wearable system for signature verification should integrate many features and address many aspects, such as the calibration of the sensors, time syncing of the wearable to the signature trace, filtering noise, fusing features, and establishing a threshold for score levels. LSTM, temporal CNN, and attention-based transformers are capable of capturing the variations of movement and motor behaviors of signers within the context of the system [6, 14, 34].

Figure 4 provides a hardware-level example from wearable-assisted sensor fusion. The setup combines wrist-worn inertial sensing with tablet/stylus dynamics, smartphone-based visual tracking, and piezoelectric signals, illustrating how wearable motion evidence can be synchronized with handwriting acquisition. A participant signs on a tablet while wearing a smartwatch; the setup also incorporates smartphone/camera and external piezoelectric sensing [28, 47].

Beyond the configuration shown in Figure 4 [47], wearable-assisted acquisition may also include smart rings, finger-mounted IMUs, and instrumented gloves. These devices can capture finger micro-motions, tremor, grip-related movement, and joint dynamics that are not directly available from the final signature image. Tablet or smartphone surfaces complement these streams with touch position, pressure, and timing, enabling synchronized multimodal analysis [17, 28, 47].

Figure 4
Wearable-assisted sensor-fusion handwriting acquisition setup



The main risks in the deployment of these technologies are pressure-profile replay, substitution of devices, synchronization drift, exposure of privacy, variation of sensor placement, high cost, and bias caused by movements of the user. There is also a risk of theft of biometric templates. From a cybersecurity perspective, incorporating wearable technologies into signature verification is useful, but they should not be relied upon. An example of a secure service may include wearable technologies, document-image analysis, and online trace capture, combined with tools such as detection of presentation attacks, device binding, pressure-friendly attack plots, and automated systems, with human review in the borderline cases. This design greatly reduces

the chances that a trace, image, or template can be reused to authenticate a secure transaction [18, 19, 24].

In conclusion, when integrating wearable technologies with signature images and online trace capture via a fusion strategy that is cognizant of risk, the full potential of these technologies is realized.

10.1. Wearable datasets, sensor reporting, and fusion strategies

Available dynamic-signature resources include online signature databases and competitions such as MCYT, BioSecure/BiosecurID, DeepSignDB, SVC2021_EvalDB, and mobile-signature datasets, while recent sensor-fusion work extends the acquisition channel using touchscreen input, accelerometers, gyroscopes, magnetometers, camera-based tracking, and piezoelectric sensors [4, 6, 13, 47]. Recent contactless work also shows the feasibility of in-air signature verification with a webcam and Siamese BiLSTM modeling, but with small participant numbers and strict protocol dependence [17].

A complete wearable protocol should report the device model, sensor axes, units, sampling frequency, timestamp precision, pressure/tilt availability, filtering method, synchronization method, and battery/thermal state. For example, sensor-fusion studies emphasize that readings from accelerometer, gyroscope, magnetometer, touchscreen, camera, and piezoelectric sensors must be synchronized with the touch or writing event; otherwise, the model may learn timing artifacts rather than stable signing behavior [47].

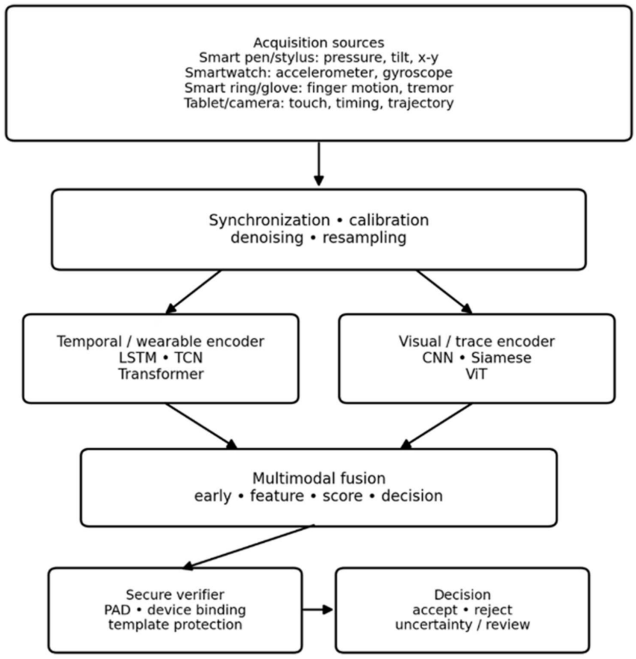
Fusion can be organized at four levels. Early fusion concatenates synchronized raw streams after resampling, but it is sensitive to missing channels and synchronization drift. Feature-level fusion learns separate embeddings for image, online trace, and wearable streams and then combines them using concatenation, attention, or cross-modal transformers. Score-level fusion combines independent match scores, which is easier to audit in regulated environments. Decision-level fusion is conservative and useful when one channel is unavailable or untrusted. For high-security use, score-level or feature-level fusion with ablation testing is preferable because it can show which sensor contributed to a correct or incorrect decision.

Figure 5 provides an original synthesis of the wearable-assisted verification pipeline linking smart pens, wrist-worn and finger-worn inertial sensors, and tablet/camera streams to synchronization, modality-specific encoding, multimodal fusion, secure verification, and final decision reporting [6, 17, 28, 47].

Security vulnerabilities specific to wearable sensors include pressure-profile replay, device substitution, sensor-stream injection, synchronization manipulation, wearable malware, side-channel leakage, and template reconstruction. Therefore, wearable signals should be bound to a trusted device identity, protected by secure storage, and evaluated with PAD/liveness tests. In addition, models should be tested against cross-device transfer and longitudinal drift because a signer's motion can change with fatigue, injury, aging, posture, or stress.

Minimum wearable reporting checklist: report the sensor type and axes, device model, sampling frequency, timestamp precision, synchronization method, preprocessing/filtering, fusion level, missing-channel handling, latency, energy use, calibration time, privacy/consent policy, and cross-device validation. These items directly affect whether a wearable-assisted signature model is reproducible and deployable outside a controlled laboratory.

Figure 5
Wearable-assisted multimodal signature verification and sensor-fusion architecture



10.2. Quantitative and practical evidence for wearable-assisted verification

There are three quantitative and practical types. First, mobile-device studies show that coordinate-plus-pressure traces can reach very low EER for random forgeries, but skilled forgeries remain more difficult. Second, sensor-fusion handwriting studies report strong signature recognition accuracy, yet the gains depend on the input modality, sensor subset, and training size. Third, in-air signature studies demonstrate contactless feasibility, but their reported accuracy remains lower than mature offline and online benchmarks, which indicates that larger datasets, replay simulation, and liveness evaluation are still needed before high-risk deployment.

For wearable-assisted systems, the manuscript now recommends reporting the following deployment variables with every result: device model, sensor channels, sampling frequency or timestamp resolution, synchronization method between handwriting trace and wearable stream, calibration procedure, sensor placement, battery or energy cost, latency on target hardware, and whether the attacker is assumed to know the sensor configuration. Without these details, performance results cannot be fairly reproduced or transferred to another smartwatch, stylus, ring, glove, or smartphone. These wearable-specific evidence, vulnerabilities, and deployment reporting requirements are shown in Table 8.

11. Scenario Models: Security Priority Comparative Discussion

The practical guidelines for selecting system designers based on scenario, model, family, and security priority are illustrated in Table 9.

In low-resource offline systems, using handcrafted features or compact CNNs remains justifiable. Although the systems are faster, the weaknesses and fewer resources to combat skilled

Table 8
Wearable-specific evidence, vulnerabilities, and deployment reporting requirements

Wearable source	Useful signal	Quantitative evidence to report	Specific vulnerability	Practical constraint
Smartphone/tablet	x-y coordinates, pressure, timing, touch dynamics	EER/FAR/FRR by device and by random vs skilled forgery	Trace replay, screen injection, pressure-profile spoofing	Device diversity, posture, screen size, pressure-sensor precision
Smartwatch/wristband	Accelerometer, gyroscope, wrist rhythm	Accuracy/EER with and without wrist stream; synchronization error	Device substitution, replayed IMU stream, loose strap or changed wrist position	Battery, comfort, user compliance, privacy of behavioral dynamics
Smart ring/finger IMU	Finger micromotions, tremor, grip-related movement	Ablation by sensor channel and input modality	Ring sharing, sensor drift, hand dominance mismatch	Fit, calibration, cost, limited public datasets
Smart pen/stylus	Pressure, tilt, pen-up/down, coordinate trace	EER under stylus vs finger input and cross-device settings	Stylus substitution, pressure replay, firmware tampering	Availability, calibration, and device-binding requirements
Camera + wearable fusion	Trajectory, pose, inertial and visual synchrony	PAD metrics plus accuracy/F1/recall under replay conditions	Video replay, trajectory reconstruction, sensor injection	Lighting, occlusion, latency, and secure synchronization

Table 9
Practical selection guidance for system designers

Scenario	Recommended model family	Security priority	Evaluation evidence
Scanned cheques/forms	Siamese CNN or region-based metric learning	Skilled forgery and image injection	EER, FAR at fixed FRR, cross-dataset tests
Legal document archive	Handcrafted + CNN hybrid	Auditability and human review	Explainable features, false-case analysis
Tablet-based signing	RNN/LSTM or temporal transformer	Replay and sensor spoofing	Online skilled-forgery protocol and replay tests
Smartphone signing	Light CNN or temporal compact model	Device variability and privacy	Cross-device validation and latency reporting
Banking/high-value access	Multifactor + protected template + PAD	Template theft and account takeover	Threat model, PAD metrics, access-control design
Wearable-assisted signing	Temporal Siamese, LSTM, or compact transformer with sensor fusion	Replay, device substitution, and behavioral-template privacy	EER/FAR/FRR with latency, sampling rate, energy use, and cross-device validation
In-air wearable signatures	Deep Siamese or attention-based sequence model using IMU/camera fusion	Video replay, trajectory reconstruction, and sensor injection	PAD/liveness metrics, synchronized sensor tests, and attacker-knowledge protocol

forgeries mean that the systems should be treated as decision-support systems or be used with manual review for user-value documents.

Siamese and triplet networks are the strongest options when offline verification systems are used without writer restrictions, as they are naturally aligned with enrollment-based authentication. Furthermore, they are able to compare query signatures while employing genuine signatures, meaning they are suited to situations with a large number of users. However, operational thresholds should be set based on application risks and should not be decided only based on validation accomplishments.

In high-security scenarios, the benefits offered by deep metric learning models and hybrid attention systems are greater than the added complexity. These models are not designed to capture long-range dependencies or multi-scale structures. High-security deployments should not select complex models merely because they are newer. They should select them only when the additional representation power is justified by stronger evidence against skilled forgery, replay, and cross-device attacks. Hybrid attention models are useful precisely because they can capture long-range and multi-scale structure, but this advantage must be balanced against compute cost, explainability burden, and the need for larger, more diverse training data.

Large neural networks with strong validation protocols should be coupled with bias and model monitoring, as well as privacy and adversarial testing, to overcome the obfuscation of failure modes.

In applications sensitive to cybersecurity, a layered architecture is recommended. A layered architecture approach entails combining signature verification with integrity checks of documents, device or channel authentication, liveness controls or PAD, protected templates with role-based access, logging, and human

escalation. This layered approach reduces the risk that a single instance of a forged or replayed signature leads to a system-wide authentication failure [16, 19, 24, 49].

12. Open Challenges and Future Directions

The first open challenge is skilled forgery realism. While many datasets include skilled forgeries, the skill, number of attempts, and forgers' information vary. Studies should focus on attacker knowledge, forgery conditions, and failure cases instead of relying solely on aggregate accuracy.

The second challenge is cross-domain generalization. Language, culture, writing tools, signing surfaces, devices, age, health, and stress all result in different signature appearances and dynamics. Streamlined cross-domain and longitudinal validations should become standard to ensure robustness of models.

The third challenge is privacy-preserving deployment. As signature data are sensitive and hard to uncollect, prioritizing cancellable templates, non-invertible transforms, and secure storage, along with federated learning and differential privacy, will reduce raw biometric retention.

The fourth challenge is trustworthy integration with cybersecurity operations. Modern digital-identity guidance advocates treating authentication as a lifecycle, and verification systems must support periodic threshold reviews.

The fifth problem is about the standardization of wearable devices. For wearable-assisted signature verification to work, placement of sensors needs to be communicated clearly, along with sampling, calibration, and posture sync methods, battery status, and what device was used. In the absence of this information, a model developed using one smartwatch or smart pen and an inertial sensor may be useless with a different data collection protocol. Datasets of the future must include time-synchronized signature images, online traces, and wearable sensor streams with a privacy-preserving release policy.

The sixth challenge is the responsible use of generative AI. The use of generative AI should be ethically regulated, as improved synthetic signatures could make forgery detection more effective but could also be used for attacks. Future studies should be more progressive and less reactive to this challenge of AI within a controlled system.

To strengthen the linkage between challenges and future work, the following agenda is recommended. First, benchmark protocols should explicitly model attacker knowledge: random forgery, simple imitation, skilled forgery with training, replay, synthetic signature generation, and sensor injection should be reported separately. Second, cross-domain evaluation should move beyond one-time dataset splits and include cross-device, cross-language, and longitudinal sessions. Third, wearable-assisted studies should release privacy-preserving metadata about sensor sampling, synchronization, missing data, and placement so that results can be reproduced without exposing raw biometric traces. Fourth, explainable and auditable models should become a required component in legal and financial scenarios, using calibrated thresholds, local evidence maps, model cards, human override logs, and post-deployment drift monitoring. Fifth, template protection must be evaluated not only by recognition accuracy but also by irreversibility, unlinkability, renewability, and revocation procedures in line with biometric-information protection principles.

Finally, future generative-AI research should be framed as controlled security testing rather than unrestricted data augmentation. Synthetic signatures can help evaluate robustness against advanced forgeries, but generated samples should be watermarked or provenance-controlled, separated from enrollment templates, and used under an attacker-model protocol. Otherwise, the same technology that improves augmentation could lower the cost of producing convincing forgeries.

12.1. Problem-linked future directions and actionable solutions

There are many future directions linked to current problems; each proposed direction in Table 10 is linked to a measurable weakness in this review and to a practical solution that can be implemented in future experiments, benchmark designs, or secure biometric service deployments.

Table 10
Future directions linked to current problems and measurable solutions

Current problem	Concrete future direction	Required evidence	Expected deployment value
Superficial cross-paper comparison	Build a shared protocol matrix for offline, online, mobile, wearable, and in-air modes	Same train/test split description, same forgery type, FAR/FRR/EER, confidence intervals, and latency	Allows fair comparison rather than accuracy-only ranking
Limited skilled-forgery realism	Create attacker-knowledge levels: random, casual imitation, trained skilled imitation, replay, and sensor injection	Report FAR at fixed FRR for each attacker level and include failure-case examples	Improves risk-based threshold setting in banking and legal applications
Weak wearable reproducibility	Release synchronized multimodal datasets combining image, online trace, IMU, pressure, and device metadata	Sampling rate, timestamp drift, calibration, placement, energy, and hardware latency	Enables robust cross-device wearable-assisted verification
Black-box decisions	Develop explainable evidence reports using saliency maps, stroke-level contribution, uncertainty flags, and audit logs	Agreement with forensic expert review and calibrated score reliability	Supports legal defensibility and user challenge procedures

(*Continued*)

Table 10
(*Continued*)

Current problem	Concrete future direction	Required evidence	Expected deployment value
Template compromise	Evaluate cancellable, non-invertible, encrypted, and federated templates under accuracy-security trade-offs	Recognition loss after protection, irreversibility tests, revocability, and attack simulations	Reduces impact of biometric leakage and supports regulated deployment
Generative-AI forgery risk	Use diffusion/Generative Adversarial Network (GAN) signatures only inside controlled red-team evaluation pipelines	Provenance records, synthetic-vs-human detection, PAD metrics, and model robustness under generated attacks	Turns generative AI into a stress-testing tool rather than an uncontrolled forgery source
Deployment drift	Add post-deployment monitoring for threshold drift, demographic/language bias, device aging, and sensor replacements	Periodic EER/FAR/FRR audits, drift dashboards, and human escalation rate	Keeps biometric performance stable after real-world deployment

13. Conclusion

This review suggests many advancements in signature verification, including approaches employing intricate pattern recognition, deep learning, and privacy-focused frameworks. Signature verification remains a key design principle prioritizing biometric service systems, computer vision integrated with temporal modeling, and cybersecurity.

Signature verification combines balanced metrics with multiple deep learning technologies, capsule, and region-based deep learning methodologies to identify offline signatures. Signature verification prioritizes modeling technologies to capture signing behaviors. Furthermore, the verification system must be designed to be integrated into the entire service ecosystem, combining multiple controls. Continuous evaluation and real-world testing of emerging signature verification systems and tools, particularly those incorporating federated security, confidence assessment, and adaptive verification techniques, show promising benefits for enhancing reliability and security. Moreover, integrating user-specific requirements into the design and deployment of verification and signature systems is a critical aspect of achieving robust and practical biometric solutions.

Finally, the future directions link each recommendation to a concrete technical challenge identified in this review and propose a practical solution that can be implemented in future experiments.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Amal Hameed Khaleel: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Suhad Muhajer Kareem:** Conceptualization, Methodology, Validation, Resources, Writing – review & editing.

References

[1] Kakade, S., & Raut, U. (2026). Biometric authentication systems: Trends, challenges, and future prospects–A comprehensive review. *MethodsX*, *16*, 103908. https://doi.org/10.1016/j.mex.2026.103908

[2] Nori, J. M., & Murshid, A. M. (2025). A survey of offline handwriting signature verification. *Al-Kitab Journal for Pure Sciences*, *9*(01), 117–128. https://doi.org/10.32441/kjps.09.01.p8

[3] Ishfaq, M., Saadia, A., Alserhani, F. M., & Gul, A. (2024). Enhancing security: Infused hybrid vision transformer for signature verification. *IEEE Access*, *12*, 137504–137521. https://doi.org/10.1109/ACCESS.2024.3447083

[4] 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. https://doi.org/10.1109/TBIOM.2021.3054533

[5] Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers and Electrical Engineering*, *119*(Part A), 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

[6] Roszczewska, K., & Niewiadomska-Szynkiewicz, E. (2024). Online signature biometrics for mobile devices. *Sensors*, *24*(11), 3524. https://doi.org/10.3390/s24113524

[7] Xiao, W., & Wu, H. (2025). Learning features for offline handwritten signature verification using spatial transformer network. *Scientific Reports*, *15*(1), 9453. https://doi.org/10.1038/s41598-025-92704-3

[8] Rathore, N. C., Juneja, A., Kumar, N., Kumar, V., & Dhaka, A. (2026). A hybrid machine learning framework for offline signature verification using gray wolf optimization. *Scientific Reports*, *16*(1), 7124. https://doi.org/10.1038/s41598-026-36163-4

[9] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Offline handwritten signature verification—Literature review. In *2017 Seventh International Conference on Image Processing Theory, Tools and Applications*, 1–8. https://doi.org/10.1109/IPTA.2017.8310112

[10] Liu, L., Huang, L., Yin, F., & Chen, Y. (2021). Offline signature verification using a region based deep metric learning network. *Pattern Recognition*, *118*, 108009. https://doi.org/10.1016/j.patcog.2021.108009

[11] Parcham, E., Ilbeygi, M., & Amini, M. (2021). CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks. *Expert Systems with Applications*, *185*, 115649. https://doi.org/10.1016/j.eswa.2021.115649

[12] Tehsin, S., Hassan, A., Riaz, F., Nasir, I. M., Fitriyani, N. L., & Syafrudin, M. (2024). Enhancing signature verification using triplet Siamese similarity networks in digital documents. *Mathematics*, *12*(17), 2757. https://doi.org/10.3390/math12172757

[13] Tolosana, R., Vera-Rodriguez, R., Gonzalez-Garcia, C., Fierrez, J., Morales, A., Ortega-Garcia, J., …, & Jabin, S. (2022). SVC-onGoing: Signature verification competition. *Pattern Recognition*, *127*, 108609. https://doi.org/10.1016/j.patcog.2022.108609

[14] Luan, F., Cao, W., & Yuan, S. (2024). Relative position matrix and multi-scale feature fusion for writer-independent online signature verification. *Heliyon*, *10*(18), e37655. https://doi.org/10.1016/j.heliyon.2024.e37655

[15] Wang, H., He, X., Wei, Z., Lv, Z., Mu, Z., Zhang, L., & Gao, Y. (2026). Writer-independent offline signature verification using local and global feature fusion. *Symmetry*, *18*(1), 149. https://doi.org/10.3390/sym18010149

[16] Pooshideh, M., Beheshti, A., Qi, Y., Farhood, H., Simpson, M., Gatland, N., & Soltany, M. (2024). Presentation attack detection: A systematic literature review. *ACM Computing Surveys*, *57*(1), 1–32. https://doi.org/10.1145/3687264

[17] Salturk, S., Pamukcu, T. E., & Kahraman, N. (2026). Contactless biometric verification from in-air signatures using deep Siamese networks. *Scientific Reports*, *16*(1), 130. https://doi.org/10.1038/s41598-025-29100-4

[18] Veraros, H., Zantalis, F., Katsoulis, S., Zois, E. N., & Koulouras, G. (2026). A federated learning approach for privacy-preserving automated signature verification. *Engineering Proceedings*, *124*(1), 100. https://doi.org/10.3390/engproc2026124100

[19] Hayat, A., Ali, S. S., Kumar, V., & Bhateja, A. K. (2025). SigTem: A non-invertible technique for online signature template protection. *Expert Systems with Applications*, *283*, 127646. https://doi.org/10.1016/j.eswa.2025.127646

[20] Haasnoot, E., Spreeuwers, L. J., & Veldhuis, R. N. J. (2022). Presentation attack detection and biometric recognition in a challenge-response formalism. *EURASIP Journal on Information Security*, *2022*(1), 5. https://doi.org/10.1186/s13635-022-00131-y

[21] Hong, D.-J., Chang, W.-D., & Cha, E.-Y. (2024). Handwritten signature generation using denoising diffusion probabilistic models with auxiliary classification processes. *Applied Sciences*, *14*(22), 10233. https://doi.org/10.3390/app142210233

[22] Guo, Y., Zhou, Y., Ge, Y., Yu, J., Li, G., & Sato, H. (2025). New online in-air signature recognition dataset and embodied cognition inspired feature selection. *Scientific Reports*, *15*(1), 19314. https://doi.org/10.1038/s41598-025-03917-5

[23] Xamxidin, N., Mahpirat, Yao, Z., Aysa, A., & Ubul, K. (2022). Multilingual offline signature verification based on improved inverse discriminator network. *Information*, *13*(6), 293. https://doi.org/10.3390/info13060293

[24] Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*(37–38), 27721–27776. https://doi.org/10.1007/s11042-020-09197-7

[25] Abduljaleel, I. Q., & Khaleel, A. H. (2021). Speech signal compression and encryption based on sudoku, fuzzy C-means and threefish cipher. *International Journal of Electrical and Computer Engineering*, *11*(6), 5049–5059. https://doi.org/10.11591/ijece.v11i6.pp5049-5059

[26] Yilmaz, M. B., & Öztürk, K. (2025). Vanilla convolutional neural network is all you need for online and offline signature verification. *International Journal of Applied Mathematics and Computer Science*, *35*(2), 357–370. https://doi.org/10.61822/amcs-2025-0025

[27] Tolosana, R., Vera-Rodriguez, R., Gonzalez-Garcia, C., Fierrez, J., Rengifo, S., Morales, A., …, & Jabin, S. (2021). ICDAR 2021 competition on on-line signature verification. In *Document Analysis and Recognition – ICDAR 2021: 16th International Conference*, 723–737. https://doi.org/10.1007/978-3-030-86337-1_48

[28] Salkanovic, A., Bačnar, D., Sušanj, D., & Ljubic, S. (2024). A sensor-fusion-based experimental apparatus for collecting touchscreen handwriting biometric features. *Applied Sciences*, *14*(23), 11234. https://doi.org/10.3390/app142311234

[29] Ozkan, Y., & Erdogmus, P. (2024). Evaluation of classification performance of new layered convolutional neural network architecture on offline handwritten signature images. *Symmetry*, *16*(6), 649. https://doi.org/10.3390/sym16060649

[30] Singhal, M., & Shinghal, K. (2024). An efficient, fast and accurate online signature verification using blended feature vector and deep learning. *IETE Journal of Research*, *70*(9), 7354–7364. https://doi.org/10.1080/03772063.2024.2351567

[31] Kumar, K. S., Venugopal, B., Reddy, G. A., & Reddy, S. P. (2026). SigVerify: A deep learning framework for signature authentication and computerised forgery detection. *International Journal of Scientific Research in Engineering and Management*, *10*(04), 1–5. https://doi.org/10.55041/IJSREM60386

[32] Sevinc, O., Mehrubeoglu, M., Yılmaz, A. A., & Derrick, S. (2025). Forensic identification using Siamese, transfer learning and custom deep learning models. *Scientific Reports*, *16*(1), 890. https://doi.org/10.1038/s41598-025-30703-0

[33] Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline signature recognition and forgery detection using deep learning. *Procedia Computer Science*, *170*, 610–617. https://doi.org/10.1016/j.procs.2020.03.133

[34] Huang, L., Ruan, Y., Li, W., Xu, N., & Zheng, P. (2026). Multi-class online signature verification based on hybrid statistical moments and UMAP-based nonlinear dimensionality reduction. *Technologies*, *14*(2), 89. https://doi.org/10.3390/technologies14020089

[35] Luan, F., Qin, J., & Yuan, S. (2025). Online signature verification based on Siamese networks and LSTM. *Seventeenth International Conference on Digital Image Processing: Proceedings of SPIE*, *13709*, 1370908. https://doi.org/10.1117/12.3073358

[36] Yang, Z., Wang, D., Liu, J., Zeng, Q., & Liu, X. (2025). A statistical learning theory framework for multi-scale attention transformers in signature verification. In *Proceedings of the 2025 International Symposium on Artificial Intelligence and Computational Social Sciences*, 658–666. https://doi.org/10.1145/3776759.3776862

[37] Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., . . . , & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of Systems Architecture*, *162*, 103402. https://doi.org/10.1016/j.sysarc.2025.103402

[38] Fatihia, W. M., Fariza, A., & Karlita, T. (2023). CNN with Batch Normalization adjustment for offline hand-written signature genuine verification. *JOIV: International Journal on Informatics Visualization*, *7*(1), 200–207. https://dx.doi.org/10.30630/joiv.7.1.1443

[39] Chaitanyaswami, H., Dobariya, A., Iyer, S., Chen, C.-L., Liu, L.-C., Uddin, M., & Hussain, S. (2025). Multi-stage deep learning framework for robust recognition of overlapping and faded handwritten text in bank cheques. *Scientific Reports*, *15*(1), 43099. https://doi.org/10.1038/s41598-025-28764-2

[40] Tuteja, D., Dhand, R., Reineu, M., Israni, J., Singh, D., & Dhal, K. (2024). Automated signature verification in bank cheque processing using Siamese and convolutional neural networks. In *2024 First International Conference on Electronics, Communication and Signal Processing*, 1–6. https://doi.org/10.1109/ICECSP61809.2024.10698370

[41] Agrawal, P., Chaudhary, D., Madaan, V., Zabrovskiy, A., Prodan, R., Kimovski, D., & Timmerer, C. (2021). Automated bank cheque verification using image processing and deep learning methods. *Multimedia Tools and Applications*, *80*(4), 5319–5350. https://doi.org/10.1007/s11042-020-09818-1

[42] Rantzsch, H., Yang, H., & Meinel, C. (2016). Signature embedding: Writer independent offline signature verification with deep metric learning. In *International Symposium on Visual Computing*, 616–625. https://doi.org/10.1007/978-3-319-50832-0_60

[43] Guo, J., Mu, H., Liu, X., Ren, H., & Han, C. (2024). Federated learning for biometric recognition: A survey. *Artificial Intelligence Review*, *57*(8), 208. https://doi.org/10.1007/s10462-024-10847-7

[44] Dash, P., Samanta, D., Sarma, M., Das, A. K., & Vasilakos, A. V. (2025). Privacy preserving unique robust and revocable passcode generation from fingerprint data. *Computers & Security*, *159*, 104698. https://doi.org/10.1016/j.cose.2025.104698

[45] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., . . . , & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*(n71). https://doi.org/10.1136/bmj.n71

[46] Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., . . . , & Moro, Q.-I. (2003). MCYT baseline corpus: A bimodal biometric database. *IEE Proceedings-Vision, Image and Signal Processing*, *150*(6), 395–401.

[47] Salkanovic, A., Sušanj, D., Batistić, L., & Ljubic, S. (2025). Beyond signatures: Leveraging sensor fusion for contextual handwriting recognition. *Sensors*, *25*(7), 2290. https://doi.org/10.3390/s25072290

[48] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. https://doi.org/10.1147/sj.403.0614

[49] Temoshok, D., Galluzzo, R., LaSalle, C., Lefkovitz, N., Regenscheid, A., Choong, Y.-Y., . . . , & Gupta, S. (2025). *Digital identity guidelines. (Report No. NIST SP 800-63-4)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

[50] Vasilakis, N., Chorianopoulos, C., & Zois, E. N. (2025). A Riemannian dichotomizer approach on symmetric positive definite manifolds for offline, writer-independent signature verification. *Applied Sciences*, *15*(13), 7015. https://doi.org/10.3390/app15137015

[51] Tucci, C., Della Greca, A., Tortora, G., & Francese, R. (2024). Explainable biometrics: A systematic literature review. *Journal of Ambient Intelligence and Humanized Computing*, 1–20. https://doi.org/10.1007/s12652-024-04856-1

[52] Otroshi Shahreza, H., Melzi, P., Osorio-Roig, D., Rathgeb, C., Busch, C., Marcel, S., . . . , & Vera-Rodriguez, R. (2026). Benchmarking of cancelable biometrics for deep templates. *Journal on Image and Video Processing*, *2026*(1), 4. https://doi.org/10.1186/s13640-025-00679-y

How to Cite: Khaleel, A. H., & Kareem, S. M. (2026). A Comprehensive Survey of Pattern Recognition, Deep Learning, and Wearable Technology Approaches for Secure Signature Verification Systems. *Smart Wearable Technology*. https://doi.org/10.47852/bonviewSWT620210519