International Journal of Innovation Scientific Research and Review
Vol. 08, Issue, 04, pp.9767-9773, April 2026
Available online at http://www.journalijisr.com
SJIF Impact Factor 2025: 7.913

Research Article

ISSN: 2582-6131

MACHINE LEARNING-BASED OFFLINE HANDWRITTEN SIGNATURE VERIFICATION: A SURVEY AND PROPOSED FRAMEWORK

*** Mohammad Awedh**

Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia.

Received 07th February 2026; Accepted 08th March 2026; Published online 25th April 2026

ABSTRACT

Offline handwritten signature verification remains an important biometric authentication problem in applications such as banking, legal documentation, access control, and identity validation. Manual verification is often time-consuming, subjective, and vulnerable to error, particularly in the presence of skilled forgeries. This paper presents a survey of machine learning approaches for offline handwritten signature verification and proposes a general framework for designing such systems. The paper reviews the main stages of the verification pipeline, including image pre-processing, feature extraction, classification, and threshold-based decision making. Both handcrafted and learned feature representations are discussed, with particular attention to convolutional neural networks, support vector machines, deep metric learning, and Siamese architectures. Common benchmark datasets and evaluation measures, including accuracy, precision, recall, F1-score, false acceptance rate, false rejection rate, and equal error rate, are also summarized. Based on the reviewed literature, a modular verification framework is proposed to support future research and practical implementation. The paper further highlights key challenges, including intra-class variation, skilled forgery detection, limited training data, and generalization across writers, and outlines promising directions for future work in secure and scalable signature verification systems.

Index Terms: offline signature verification, handwritten signatures, machine learning, biometric authentication, convolutional neural network, Siamese network, forgery detection.

INTRODUCTION

Handwritten signatures have long been used as a conventional means of personal authentication in financial transactions, legal agreements, institutional records, and administrative procedures [1], [2]. Despite the continued expansion of digital authentication methods, handwritten signatures remain practically and legally important in many environments. Their widespread use, however, creates an ongoing challenge for reliable verification. Manual signature verification is inherently subjective and may vary according to the expertise, attention, and judgment of the examiner. In addition, genuine signatures from the same writer often exhibit natural variation due to differences in writing speed, physical condition, emotional state, or environmental circumstances. At the same time, forged signatures, especially skilled forgeries, may visually resemble authentic samples closely enough to mislead human observers [1], [2]. These limitations have motivated the development of automated systems capable of performing signature verification with greater consistency, objectivity, and efficiency.

Automatic signature verification has therefore become an important area of research within biometric authentication [1], [2]. Signature verification systems are generally divided into online and offline approaches. Online verification captures dynamic information during the signing process, such as pen pressure, writing speed, stroke order, and timing, whereas offline verification relies only on the static image of a completed handwritten signature [1]. Although online methods benefit from richer behavioral information, offline signature verification remains highly relevant because many real-world documents are still created, processed, and archived in paper form. Banking forms, contracts, administrative records, examination documents, and legal paperwork continue to depend on signatures that must be verified from scanned or photographed images [5], [15].

Traditional approaches to offline signature verification relied mainly on handcrafted feature extraction and classical pattern recognition methods [1], [2]. These approaches described signatures using characteristics such as aspect ratio, slant, contour information, stroke thickness, texture, and pixel density, followed by classification using methods such as nearest neighbor techniques, hidden Markov models, or support vector machines [1], [4]. While these methods were useful in many settings, their effectiveness depended strongly on the quality of manually designed features and their ability to capture meaningful differences between genuine and forged signatures. More recent progress in machine learning, especially deep learning, has introduced models capable of learning discriminative representations directly from image data [5], [8]–[10]. Convolutional neural networks, deep metric learning, and Siamese architectures have shown strong potential for modeling signature similarity and improving robustness to natural variation and forgery [8]–[10].

At the same time, the literature shows that offline signature verification remains challenging. Skilled forgeries are difficult to distinguish from genuine signatures when only static image information is available. Performance is also influenced by dataset quality, writer diversity, preprocessing quality, and the limited availability of forged training samples [5], [9], [10], [15]. These observations suggest that effective offline verification requires not only accurate classifiers, but also a well-structured pipeline that accounts for data acquisition, preprocessing, feature extraction, decision thresholds, and evaluation methodology.

***Corresponding Author: Mohammad Awedh,**
Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia.

This paper is intended as a survey-informed framework paper rather than a report of a newly benchmarked verification model. Its main contributions are threefold. First, it provides a concise survey of major machine learning approaches for offline handwritten signature verification, covering handcrafted feature-based methods, classical classifiers, convolutional neural networks, deep metric learning, and Siamese architectures. Second, it organizes and analyzes the main components of the verification pipeline, including preprocessing strategies, feature extraction methods, classification approaches, commonly used datasets, and evaluation metrics. Third, based on this analysis, it proposes a modular framework for offline signature verification that can serve as reference architecture for future implementation, comparison, and application in real-world authentication settings.

SURVEY OF RELATED WORK

A. Handcrafted Feature-Based Approaches

Automatic signature verification has been studied for decades as a biometric recognition problem [1], [2]. Early offline systems relied heavily on handcrafted features that described the visual characteristics of a signature through explicitly defined measurements. Common examples included aspect ratio, height-to-width ratio, slant angle, projection histograms, contour descriptors, pixel density, connected components, and texture-related statistics [1], [2]. These features were attractive because they were interpretable and computationally efficient.

Traditional methods often represented signatures using both global and local descriptors. Global features described overall shape and geometry, whereas local features captured detailed stroke patterns, curvature, intersections, and texture characteristics [1], [5]. Such approaches offered useful baselines for offline verification and could perform reasonably well when signatures were captured under controlled conditions. However, their success depended strongly on whether manually designed features could capture authentic writing traits while remaining robust to natural variability.

B. Classical Machine Learning Classifiers

After handcrafted features were extracted, classifiers were used to separate genuine signatures from forgeries. Techniques such as nearest neighbor classification, hidden Markov models, and support vector machines were commonly used in earlier research [1], [4]. Among these, support vector machines became especially popular because of their strong performance in high-dimensional feature spaces and their suitability for relatively limited training data [4], [6]. In many offline signature verification systems, SVMs served as a strong baseline when combined with carefully selected geometric and structural descriptors.

Despite their usefulness, classical classifiers were only as strong as the handcrafted descriptors supplied to them. In practice, this made SVM-based pipelines attractive when data were scarce and interpretability mattered, but less effective when the verification task required modeling subtle intra-writer variation or skilled forgery patterns. Compared with later deep models, these approaches were usually easier to train and deploy, yet they offered less representational flexibility.

C. Deep Learning for Feature Representation

Recent advances in machine learning have increasingly focused on learned feature representations for offline handwritten signature verification [5], [7], [15]. Convolutional neural networks have become particularly important because they can learn hierarchical image features directly from preprocessed signature images [3], [7], [8]. Through layers of convolution, pooling, and nonlinear activation, CNNs can model structural, spatial, and textural information that may be difficult to represent using handcrafted descriptors alone.

Hafemann *et al.,* demonstrated the value of writer-independent feature learning using deep convolutional neural networks, showing that learned representations can generalize across different writers [8]. Relative to handcrafted pipelines, CNN-based methods reduce dependence on manual feature engineering and generally scale better to writer-independent settings, but they also demand more data, tuning, and computational resources. Their advantage is therefore most visible when sufficient training diversity is available and evaluation protocols are carefully controlled.

D. Siamese Networks and Metric-Learning Methods

Another important development in the literature is the use of deep metric learning and Siamese architectures for signature verification [9], [10]. Rather than treating the task only as conventional classification, these methods learn and embedding or similarity function in which genuine signatures from the same writer are placed closer together than forged signatures. This formulation is particularly suitable for verification problems, where the goal is often to compare a questioned signature with one or more reference samples rather than assign it to a broad class label.

Rantzsch *et al.,* proposed deep metric learning for writer-independent offline signature verification, while Dey *et al.,* introduced SigNet, a convolutional Siamese network for writer-independent verification [9], [10]. These approaches have received attention because they align naturally with verification settings and can be effective in low-sample or writer-independent scenarios.

E. Sparse Representation and Hybrid Approaches

Beyond CNNs and Siamese models, other methods have also contributed to the field. Sparse representation techniques have shown promising performance for offline signature verification, especially in writer-dependent settings [14]. Hybrid methods that combine conventional descriptors with learned features have also been explored as a way to balance interpretability, data efficiency, and representational power. Similarly, bag-of-visual-words approaches using local descriptors such as KAZE features have been used to capture local image structure in signatures [13].

These methods highlight the methodological diversity of the field. Hybrid and sparse approaches are often attractive when datasets are moderate and interpretability or data efficiency matters. Pure deep models, by contrast, tend to perform best when larger training sets support richer representation learning. This trade-off between data efficiency and representation power remains central to method selection in offline handwritten signature verification.

F. Challenges Identified in the Literature

The reviewed literature consistently identifies several important challenges. First, offline verification lacks dynamic writing information such as pen pressure, velocity, and stroke order, which are often helpful in distinguishing skilled forgeries [1], [2]. Second, natural intra-class variation among genuine signatures can be large, complicating the learning of stable writer-specific patterns [5], [15]. Third, forged samples are often limited, especially in practical applications, making robust training and generalization difficult [5], [9], [15]. Finally,

reproducibility and fair comparison remain important concerns, since different studies use varying datasets, preprocessing pipelines, evaluation protocols, and performance measures [15].

Overall, the literature shows a clear progression from handcrafted descriptors and shallow classifiers toward learned representations and similarity-based deep architectures. Handcrafted and shallow models remain useful as efficient baselines. CNNs provide stronger feature learning for complex visual variability, and Siamese or metric-learning methods are especially well matched to verification-by-comparison. However, gains reported in one setting do not always transfer to another, especially across writer-dependent and writer-independent protocols. These observations motivate the need for a structured framework that organizes the main stages of offline handwritten signature verification in a coherent and modular manner. Table I summarizes representative studies frequently cited in the offline handwritten signature verification literature.

Table I. Representative studies in offline handwritten signature verification

Study	Core approach	Key contribution / limitation
Impedovo & Pirlo [1]	Classical survey	Foundational overview, but limited to the pre-deep-learning era.
Hafemann et al. [8]	Writer-independent CNN	Learns transferable deep features; usually needs substantial training data.
Rantzsch et al. [9]	Deep metric learning	Verification-oriented embedding; depends on careful pair or triplet design.
Dey et al. [10]	SigNet Siamese CNN	Strong similarity modeling; tuning can be more complex than shallow baselines.
Okawa [13]	BoVW + KAZE features	Captures local structure, but is less expressive than modern deep models.
Zois et al. [14]	Sparse representation	Competitive with limited references; performance can be scenario sensitive.
Hameed et al. [15]	Systematic review	Summarizes datasets, methods, metrics, and open issues in the literature.

PROBLEM STATEMENT

The problem addressed in offline handwritten signature verification is the automatic determination of whether a given scanned signature image is genuine or forged [1], [5]. In a typical scenario, the system receives a questioned signature along with one or more reference samples associated with a claimed identity. Based on the visual evidence available in the images, it must decide whether to accept the signature as genuine or reject it as forged.

An effective verification framework must address several challenges simultaneously. It must distinguish genuine signatures from random and skilled forgeries while accounting for the natural variability present among authentic signatures produced by the same writer. It must also remain robust to noise introduced during image acquisition, including lighting inconsistencies, scanning artifacts, background interference, and variations in scale or alignment. In addition, the framework should support reasonable computational efficiency and practical use in security-sensitive domains such as banking, legal documentation, institutional record management, and access control.

The central objective, therefore, is to organize a reliable, scalable, and modular verification pipeline that can guide future implementation and evaluation using machine learning techniques.

PROPOSED VERIFICATION FRAMEWORK

Based on the reviewed literature, a modular framework for offline handwritten signature verification is proposed. The framework is intended as a general reference architecture rather than a claim of a newly benchmarked model. It consists of five major components: data acquisition, preprocessing, feature extraction, classification or similarity analysis, and decision making.

A. Data Acquisition

The framework begins with the collection of signature samples in scanned grayscale or color image form [1], [5]. These samples may come from real-world document workflows or from public benchmark datasets such as GPDS-960 and MCYT [11], [12]. For training and evaluation, multiple genuine signatures should ideally be available for each writer, and forged signatures should be included where possible to support realistic verification analysis. Input samples are typically stored in common image formats such as PNG, JPEG, or TIFF.

B. Preprocessing

Preprocessing aims to improve the quality and consistency of input signature images before feature extraction [1], [5], [15]. In line with common practice in the literature, preprocessing may include grayscale conversion, noise removal through median or Gaussian filtering, binarization, cropping using the signature's bounding box, resizing to a fixed resolution, and normalization of pixel intensity values. Optional operations such as thinning or skeletonization may also be applied when structural analysis is emphasized [1], [14].

These steps help reduce irrelevant background variation and improve the visibility of signature structure. Effective preprocessing is particularly important because downstream feature learning and classification depend strongly on the quality of the input representation.

C. Feature Extraction

Feature extraction transforms the preprocessed signature image into a representation suitable for learning or comparison.

Handcrafted feature extraction may use geometric, structural, statistical, or textural descriptors such as signature width, height, aspect ratio, center of mass, black pixel density, projection profiles, contour properties, connected components, or local image statistics [1], [2]. These descriptors are relatively interpretable and may be useful when computational simplicity is a priority.

Learned feature extraction may instead use convolutional neural networks to automatically derive hierarchical representations from the image [3], [5], [8]. In such cases, convolutional layers, pooling layers, nonlinear activation functions, and dense layers work together to encode increasingly abstract visual properties of the signature. This approach is attractive because it reduces reliance on manual feature engineering and can capture subtle structural patterns.

An alternative strategy is similarity-based feature learning through Siamese or metric-learning architectures [9], [10]. These models learn and embedding space in which genuine signatures are closer to one another than to forgeries. Such methods are especially well suited to verification settings that emphasize pair wise or reference-based comparison.

D. Classification or Similarity Analysis

After features are extracted, the system must determine whether the questioned signature should be accepted or rejected. When handcrafted or CNN-derived feature vectors are available, classifiers

such as support vector machines may be used to distinguish genuine and forged samples [4], [6]. In end-to-end deep learning systems, the network may directly produce a verification output. In similarity-based approaches, Euclidean distance, cosine similarity, or learned metric functions may be used to compare the questioned signature against enrolled references [9], [10].

This stage may operate in writer-dependent or writer-independent modes. Writer-dependent models are trained specifically for each individual writer, whereas writer-independent models attempt to learn verification-relevant characteristics that generalize across multiple writers [5], [8]–[10]. Each setting has practical trade-offs related to scalability, personalization, and data requirements.

E. Decision Making

The final stage of the framework applies a decision threshold to the classifier output or similarity score. This threshold determines whether the signature is accepted as genuine or rejected as forged [5], [15]. Threshold selection is important because it directly affects false acceptance and false rejection behavior. In applications where security is the primary concern, the threshold may be adjusted to reduce false acceptance. In applications where convenience and accessibility are more important, the system may tolerate slightly higher acceptance rates while reducing false rejections.

This threshold-based design makes the framework adaptable across different operational requirements and application domains.

SYSTEM ARCHITECTURE

The proposed verification framework can be expressed as a modular system architecture consisting of interconnected functional modules for input handling, preprocessing, feature extraction, classification or similarity analysis, decision making, and reference signature storage. This architecture is intended to support flexible implementation and comparative evaluation rather than prescribe a single fixed model design.

The architecture includes the following modules. The input module receives the scanned signature image. The preprocessing module performs grayscale conversion, filtering, binarization, cropping, resizing, and normalization [1], [5], [15]. The feature extraction module derives either handcrafted descriptors, CNN-based representations, or similarity-oriented embeddings [1], [8], [13], [14]. The classification or similarity module applies SVM-based classification, end-to-end neural prediction, or pair wise similarity analysis [4], [8]–[10]. The decision module generates the final output as genuine or forged based on a threshold or decision rule. The database module stores enrolled reference signatures and related metadata for use during comparison and verification.

The modular design makes it possible to substitute or extend individual components according to application needs. For example, a lightweight implementation may use handcrafted features and SVM classification, whereas a more advanced implementation may incorporate writer-independent CNN embeddings or Siamese similarity learning. This flexibility makes the framework suitable both for research comparison and for practical system design.

Figure 1 presents the proposed modular framework and summarizes the main flow from input signature image to final verification outcome.

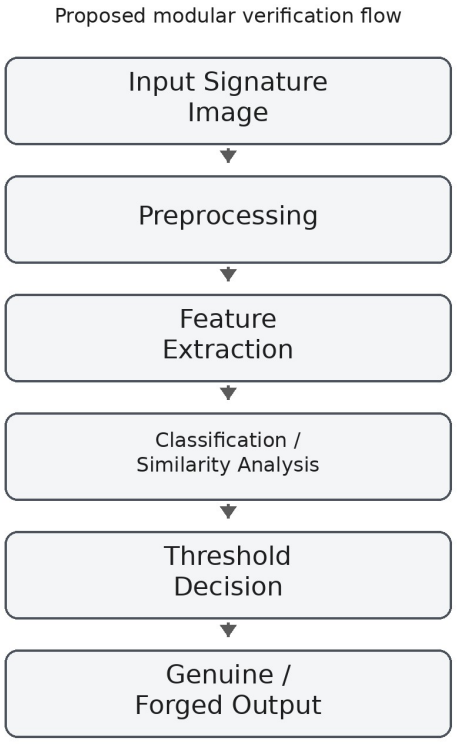

Fig.1: Proposed modular framework for offline handwritten signature verification.

EVALUATION CONSIDERATIONS FOR FUTURE IMPLEMENTATION

Although this paper does not present a newly benchmarked experimental model, the literature suggests several important considerations for evaluating offline handwritten signature verification systems. These considerations are useful for guiding future implementation and comparative study.

A. Benchmark Datasets

Public benchmark datasets play an essential role in offline handwritten signature verification because they provide a common basis for comparison and reproducibility. Datasets such as GPDS-960 and MCYT are widely used in the literature because they include signature samples from multiple writers and support evaluation under realistic verification conditions [11], [12]. Benchmark datasets are especially valuable for comparing writer-dependent and writer-independent approaches under clearly defined protocols.

B. Preprocessing Protocols

Evaluation should account for the influence of preprocessing on verification performance. Differences in grayscale conversion, filtering, binarization, cropping, normalization, and image resizing can substantially affect the quality of extracted features and the behavior of downstream classifiers [5], [15]. For this reason, preprocessing protocols should be described clearly and applied consistently across compared methods.

C. Training and Validation Considerations

Training and validation strategies depend on the selected model. Classical machine learning methods require careful feature design and classifier tuning, whereas deep learning methods require

architectural decisions, optimization settings, regularization, and augmentation strategies [6], [7]. In future implementations, datasets should be divided into separate training, validation, and test subsets so that hyper parameter tuning and final evaluation remain properly separated. Techniques such as augmentation, transfer learning, and early stopping may be particularly important when reference signatures are limited.

D. Evaluation Metrics

Offline handwritten signature verification is a biometric security task, so evaluation should not rely on accuracy alone. Common measures include precision, recall, F1-score, false acceptance rate, false rejection rate, and equal error rate [5], [8], [9], [15]. False acceptance rate reflects the proportion of forgeries incorrectly accepted as genuine, while false rejection rate reflects the proportion of genuine signatures incorrectly rejected. Equal error rate is especially useful because it summarizes the trade-off between these two types of error at the operating point where they are equal.

E. Baseline Comparison and Reproducibility

Meaningful evaluation should compare advanced methods against suitable baselines, such as handcrafted feature extraction combined with support vector machine classification [4]. Reproducibility also requires clear reporting of dataset composition, train-test splits, preprocessing steps, hyper parameters, and threshold selection. Since the literature includes both writer-dependent and writer-independent settings, future studies should specify the evaluation scenario clearly and avoid comparing results across incompatible protocols.

LITERATURE-BASED DISCUSSION

The literature on offline handwritten signature verification shows that machine learning has significantly improved the ability of automated systems to distinguish genuine signatures from forged ones. Across prior studies, preprocessing is consistently identified as a critical stage because scanned signature images often contain noise, background artifacts, inconsistent contrast, and variations in scale or alignment. Techniques such as grayscale conversion, filtering, binarization, cropping, and normalization help reduce irrelevant variation and provide a more stable representation for subsequent analysis. Consequently, effective preprocessing contributes directly to more reliable feature extraction and improved verification consistency.

The reviewed studies also indicate that handcrafted feature-based approaches remain important as baseline methods because they are computationally light and can perform competitively when training data are limited or acquisition conditions are controlled. Features such as contour descriptors, geometric ratios, pixel density, and projection profiles are interpretable and easy to deploy with classifiers such as support vector machines [1], [4]. Their main weakness is dependence on predefined descriptors. As a result, they often under represent the subtle local distortions that characterize skilled forgeries. Learned representations become more advantageous as task complexity and data diversity increase.

More recent research has increasingly favored learned feature representations through convolutional neural networks [5], [8]. Compared with handcrafted pipelines, CNN-based approaches are better at capturing distributed stroke patterns and textural cues, especially in writer-independent settings where fixed descriptors may generalize poorly. Their trade-off is that they require more data and are more sensitive to training protocol. Reported gains therefore depend strongly on dataset scale, preprocessing consistency, and validation design.

Siamese networks and deep metric-learning methods represent another important development in the field [9], [10]. Compared with standard classifiers that decide from a single feature vector, similarity-based models map more naturally to the verification problem because they optimize pairwise or relative relationships between questioned and reference signatures. This can make them more flexible when only a few reference signatures are available. However, performance depends heavily on pair or triplet sampling strategy, threshold calibration, and the quality of the learned embedding space.

At the same time, the surveyed literature consistently identifies skilled forgery detection as one of the most difficult challenges in offline signature verification. Because offline systems rely only on static images, they cannot use dynamic signing cues such as pressure, timing, and stroke order [1], [2]. This limitation makes it harder to identify subtle differences between genuine signatures and carefully imitated forgeries. As a result, even advanced learning-based models must depend heavily on high-quality preprocessing, robust feature representations, and carefully tuned decision thresholds.

Another recurring theme in the literature is the importance of dataset quality and diversity. Deep learning methods generally benefit from larger and more varied datasets, since broader exposure to genuine variation and forgery patterns improves generalization [7], [8], [15]. In comparative terms, shallow models often degrade more gracefully in small-data regimes. Deep architectures, by contrast, usually gain more from dataset scale, augmentation, and transfer learning. Method choice should therefore be matched to the expected operating regime rather than treated as universally optimal.

Taken together, the reviewed works indicate a clear transition in the field: from handcrafted descriptors and shallow classifiers toward learned representations and similarity-based deep architectures. The literature suggests that no single method dominates across all settings. Instead, performance depends on the interaction among data availability, verification protocol, feature representation, and threshold design. In this context, the proposed framework presented in this paper serves as a structured reference model that reflects current research directions and may guide future implementation and comparison.

ADVANTAGES OF THE PROPOSED FRAMEWORK

The proposed framework offers several practical and conceptual advantages. First, it organizes the offline handwritten signature verification problem into distinct modules, making the verification pipeline easier to understand, implement, and evaluate. Second, its modular structure supports flexibility, since different preprocessing methods, feature extractors, and decision models can be substituted according to application needs. Third, it accommodates both traditional and deep learning approaches, allowing it to serve as a bridge between classical feature-based systems and more recent learned-representation methods.

The framework is also useful from a research perspective. Because it separates acquisition, preprocessing, feature extraction, classification, and decision stages, it supports more systematic comparison of alternative methods. In addition, its threshold-based design is well suited to application-specific tuning, where different operational settings may prioritize low false acceptance or low false

rejection. Finally, the framework has relevance for practical domains such as banking, legal documentation, institutional verification, and secure identity validation, where signature authentication remains important.

LIMITATIONS

The proposed framework also has several limitations that reflect broader challenges in offline handwritten signature verification. Most importantly, offline systems do not capture dynamic writing information such as pen pressure, signing speed, and stroke order, which are often valuable for distinguishing skilled forgeries [1], [2]. This means that even a well-designed framework remains constrained by the information available in static images. In addition, verification quality depends strongly on data availability and image quality. Poor scanning conditions, low contrast, distortion, and background noise may reduce preprocessing effectiveness and weaken downstream learning. Finally, the framework presented in this paper is conceptual rather than experimentally validated in this manuscript, so future work is needed to benchmark specific implementations under standardized protocols.

FUTURE RESEARCH DIRECTIONS

Future research in offline handwritten signature verification may proceed in several directions. One promising area is the continued development of similarity-based models such as Siamese networks, triplet-learning architectures, and other deep metric-learning methods [9], [10]. These approaches align naturally with verification tasks and may provide stronger robustness in writer-independent settings.

Another important direction is the integration of transfer learning, data augmentation, and hybrid feature extraction strategies to improve generalization when training data are limited [5], [14], [15]. Explainable artificial intelligence techniques may also help make deep verification models more interpretable, which is especially valuable in legal or institutional applications where transparency is important.

In addition, multimodal systems that combine signature verification with other biometric or contextual signals may improve security and reliability [12]. Research into mobile capture, real-time verification, and low-resource deployment is also relevant for expanding practical use. Finally, future studies should place greater emphasis on reproducible evaluation protocols, dataset diversity, and fair comparison across writer-dependent and writer-independent settings, since methodological clarity remains essential to progress in the field.

CONCLUSION

This paper presented a survey of machine learning approaches for offline handwritten signature verification and proposed a modular framework for the design of such systems. The discussion focused on the principal stages of the verification pipeline, including preprocessing, feature extraction, classification, and decision making, while also reviewing commonly used datasets, learning strategies, and evaluation measures. By bringing these elements together, the paper aimed to provide both a concise overview of the field and a structured foundation for future system development.

The reviewed literature indicates that offline handwritten signature verification remains an important and challenging problem in biometric authentication. Traditional handcrafted feature-based methods continue to offer useful baselines because of their interpretability and computational efficiency, while more recent deep learning approaches, including convolutional neural networks, Siamese networks, and metric-learning models, show strong promise in capturing complex signature characteristics and improving verification robustness. At the same time, the literature makes clear that issues such as intra-class variation, limited training data, writer independence, and especially skilled forgery detection remain open research challenges.

Based on this literature, the proposed framework is not intended as a claim of a newly benchmarked state-of-the-art model, but rather as reference architecture that organizes the key components required for effective offline handwritten signature verification. As such, it may support future implementation, comparative evaluation, and adaptation in practical domains such as banking, legal documentation, administrative verification, and secure identity validation.

In conclusion, machine learning provides a strong and evolving foundation for offline handwritten signature verification. Continued progress will likely depend on improved datasets, more robust similarity-learning methods, reproducible evaluation protocols, and hybrid frameworks that balance accuracy, interpretability, and deployment practicality. The survey and proposed framework presented in this paper are intended to contribute to that continuing development by offering a coherent view of the field and a useful basis for future research and application.

REFERENCES

[1] D. Impedovo and G. Pirlo, “Automatic signature verification: The state of the art,” IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 38, no. 5, pp. 609–635, 2008.

[2] R. Plamondon and G. Lorette, “Automatic signature verification and writer identification—The state of the art,” Pattern Recognit., vol. 22, no. 2, pp. 107–131, 1989.

[3] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proc. IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[4] C. Cortes and V. Vapnik, “Support-vector networks,” Mach. Learn., vol. 20, pp. 273–297, 1995.

[5] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification—Literature review,” in Proc. Int. Joint Conf. Neural Netw. (IJCNN), 2017, pp. 1–8.

[6] C. M. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006.

[7] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[8] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Writer-independent feature learning for offline signature verification using deep convolutional neural networks,” in 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 2016, pp. 2576–2583.

[9] H. Rantzsch, H. Yang, and C. Meinel, “Signature embedding: Writer independent offline signature verification with deep metric learning,” in Advances in Visual Computing, Lecture Notes in Computer Science, vol. 10073, 2016, pp. 616–625.

[10] S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Lladós, and U. Pal, “SigNet: Convolutional Siamese network for writer independent offline signature verification,” arXiv:1707.02131, 2017.

[11] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, “Off-line handwritten signature GPDS-960 corpus,” in Proc. 9th Int. Conf. Document Analysis and Recognition (ICDAR 2007), Curitiba, Brazil, 2007, pp. 764–768.

[12] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. Igarza, C. Vivaracho, D. Escudero, Q. Moro, and N. Cardeñoso-Payo, "MCYT baseline corpus: A bimodal biometric database," IEE Proc.-Vis. Image Signal Process., vol. 150, no. 6, pp. 395–401, 2003.

[13] M. Okawa, "Offline signature verification based on bag-of-visual words model using KAZE features and weighting schemes," in Proc. IEEE Conf. Computer Vision and Pattern Recognition Workshops (CVPRW), Las Vegas, NV, USA, 2016, pp. 183–190.

[14] E. N. Zois, D. Tsourounis, I. Theodorakopoulos, A. L. Kesidis, and G. Economou, "A comprehensive study of sparse representation techniques for offline signature verification," IEEE Trans. Biometrics, Behavior, Identity Sci., vol. 1, no. 2, pp. 68–81, 2019.

[15] M. M. Hameed, R. Ahmad, M. L. M. Kiah, and G. Murtaza, "Machine learning-based offline signature verification systems: A systematic review," Signal Process.: Image Commun., vol. 93, p. 116139, 2021.

****