JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)

Volume 3, Issue 2, 2025
https://jecir.com/

# LEVERAGING MACHINE LEARNING TECHNIQUES FOR ENHANCING SIGNATURE VERIFICATION TO UNVEILING THE FORGERY

**Shumaila Ejaz**[1]

**Affiliations**

[1]Department: Management Science National College of Business Administration & Economics (NCBAE), Bahawalpur
fusionlake@gmail.com

**Corresponding Author's Email**

[1] fusionlake@gmail.com



**ABSTRACT**

These days, computer vision and machine learning researchers are actively studying handwritten signature verification. It makes sense to define signature verification as a machine-learning task. This is accomplished by figuring out if the signature is real or fake. It is therefore regarded as a two-class classification problem. Given the prevalence of handwritten signatures in legal documents and financial transactions, researchers must carefully consider which machine-learning technique to apply in order to authenticate handwritten signatures and prevent forgeries that could result in significant losses for their clients. Thus far, the application of machine learning algorithms has produced excellent results in terms of equal computation error rates. The research aims to develop a model of classification capable of effectively categorizing forged verified signatures using input data. The primary objective is to explore the creation of a robust signature verification classification model using machine learning and algorithms. The research design involves a step-by-step approach design includes the gathering of data, Preprocessing, classification algorithms, and evaluation of models. The process of verifying the authenticity of a signature by use of machine learning techniques is called signature verification. The present project concentrates on off-line signature verification, however signatures might be of either online or offline form. This project intends to create a methodology that uses writer-independent characteristics to differentiate between authentic and faked signatures. In order to collect signatures from people, execute signature verification, and display the outcomes, we want to develop a whole end-to-end hardware/software system. To achieve this, a number of Machine Learning approaches for off-line signature verification were created and evaluated on benchmark datasets. Our proposed technique outperforms offline signature verification approaches such as support vector machine (SVM), neural network (NN), and logistic regression in terms of accuracy.

**Keywords:** Offline and Online signature, Handwritten Signature Verification, Machine Learning Algorithms, Classification

## INTRODUCTION

"Undoubtedly, more study is required to properly explore and comprehend the possibilities of handwritten signatures, which are still quite unique symbols that clearly show the creativity and complexity of people." (D. Impedovo and G. Pirlo. Automatic signature verification: The state of the art. IEEE Trans. on Systems, Man, and Cybernetics - Part C: Application and Reviews, 38(5):609635, 2008)

### *A. Introduction of Signature Verification*

A signature is a mark or name of someone that can typically be characterized and personalized, showing their identity and integrity. In many economic, authorized, organizational, educational, and other

profitable situations, an individual's handwritten signature is normally recognized as a form of verifying the validity of official papers such as credentials, payments, drafts, letters, agreements, visas, passports, and so on. It is necessary to prevent the forging and forgery of such official papers.

For instance, consider competitive tests such as government and federal exams; in past times, when there were no computerized confirmations, many persons used forged signatures during exam submissions and evaluations, resulting in many people losing their possibilities. For example, a signature is essential in any contract since it identifies the person of interest and demonstrates purpose and learned permission. So, to address this problem, signature verification is established.

*B. Why Automatic Signature Verification?*

There are dual kinds of signature verification: online and offline. Overall, offline verification of signatures is a less effective and longer procedure than online verification while dealing with a large number of records and files to check in fewer periods. Over several decades, numerous scholars have invented numerous techniques for verifying signatures to help persons or groups find whether the name of a specific individual is forged or real [1].

Many security applications involve biometric technologies. Such strategies are designed to identify individuals based on their physical or behavioral features. In the main case, authentication is based on observations of biological traits such as a person's fingerprints, face, or irises. In the final case, behavioral traits such as speech and handwriting cause a problem. Biometric technologies have two main uses: certification and authentication. In the main case, an organization's user provides a biometric example and confirms their identity. The confirmation organization's purpose is to ensure that the customer is who they claim they are. The aim of the credentials case, in which a user provides a biometric sample, is to find the biometric model between the other consumers registered with the technique.

In today's more creative world, a person's signature is an extremely essential element of its identification. The number of false cases is likewise growing rapidly over time.

Thus, the usage of a signature-checked system is asking for the opportunity to strengthen the connection between conformers as well as offer safe techniques for approving official records.

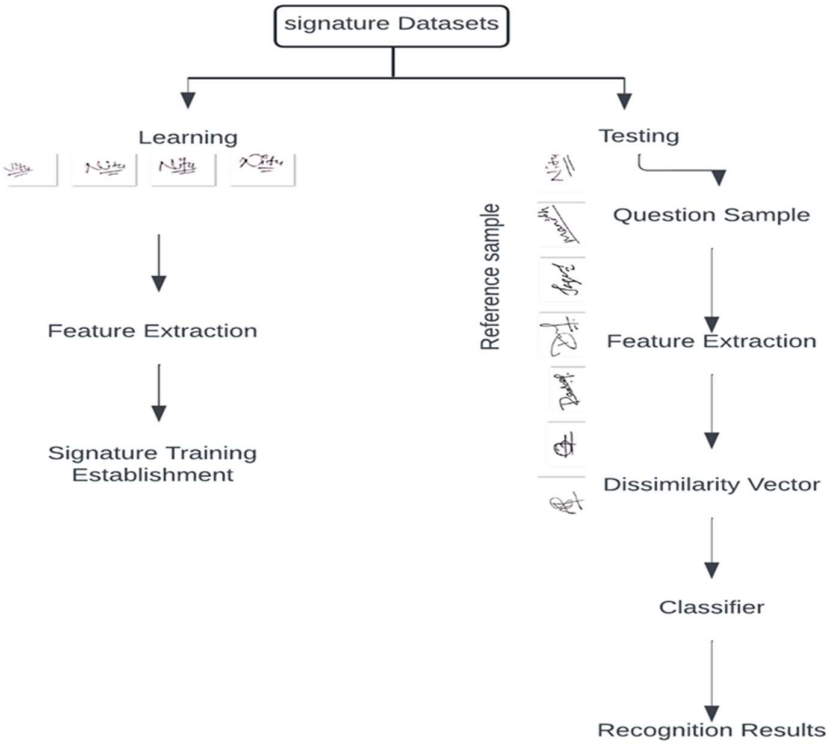


**Fig 1**: Offline signature authentication system model

Use signature verification methods to differentiate between authentic and false signatures. Usually, someone would verify a model sign by matching and verifying the model with duplicates of real name samples they previously acquired, or with the support of witnesses [2].

The existing signature verification systems face difficulties such as limited strength against various types of imitations, vulnerability to skilled forgers, and dependence on physical mediation.

*C. Automatic Signature Verification System*

Imitative signature validation systems frequently struggle with variances in signature types, alterations, and new fraud techniques. These research efforts target these problems by looking into the capacity of machine learning models to memorize and recognize complicated designs, allowing for more precise and computerized signature verification. The application of artificial intelligence and machine learning technologies to analyze and predict the evolution of false signature confirmation has generated a lot of interest in present times.

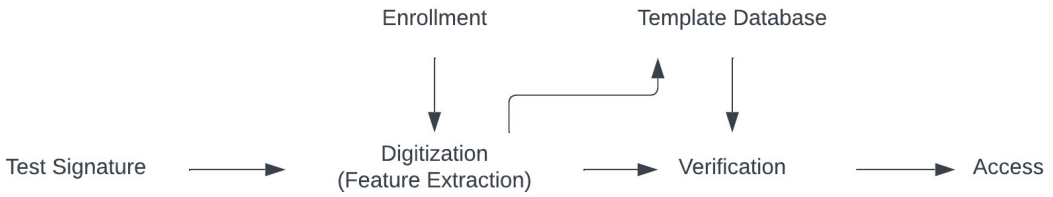


**Fig 2:** Typical signature Verification System

The research aims to develop a model of classification capable of effectively categorizing forged verified signatures using input data. The challenge is to create a strong classification model capable of accurately identifying forged signature verification. Image processing makes sure the model concentrates on the most relevant variables, resulting in increased accuracy and efficiency.

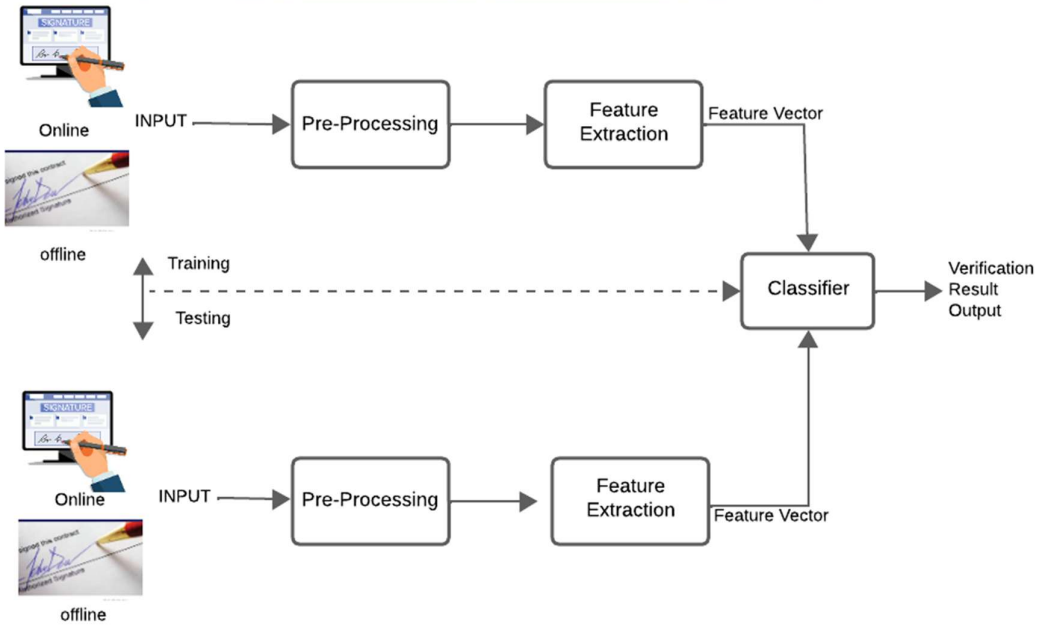


**Fig 3:** Automatic signature verification scheme

In recent years, improvements in artificial intelligence and machine learning techniques have shown great ability in various applications, including Fake signature verification Deep learning, a subgroup of

machine learning, has appeared as a dominant tool for automatically analyzing and deducing complex patterns. Leveraging machine learning algorithms for Fake signature verification could potentially transfigure the field of detective by providing reliable, objective, and proficient diagnostic tools. In recent years, many fake signatures found on different documents in different fields such as in law medical and education departments, etc.

The key purpose of this research is to discover the potential of machine learning procedures in the initial detection and arrangement of Fake signature verification. By binding the power of deep neural networks and large-measure datasets, we seek to develop a strong and accurate Fake signature verification system that can contribute to fake signature detectors in making timely and up-to-date decisions. Our recommended technique outperforms offline sign verification methods such as support vector machine (SVM), neural network (NN), and logistic regression in terms of accuracy.

## PROBLEM STATEMENT

The existing signature verification systems face difficulties such as limited strength against various types of imitations, vulnerability to skilled forgers, and dependence on physical mediation. Imitative signature validation systems frequently struggle with variances in signature types, alterations, and new fraud techniques. These research efforts target these problems by looking into the ability of machine learning models to memorize and recognize complicated designs, allowing for more precise and computerized signature verification. The research aims to develop a model of classification capable of effectively categorizing forged verified signatures using input data.

The challenge is to create a strong classification model capable of accurately identifying forged signature verification. Image processing makes sure the model concentrates on the most relevant variables, resulting in increased accuracy and efficiency.

## OBJECTIVES OF THE STUDY

- To explore the creation of a robust sign verification classification model using machine learning and algorithms.
- To find out the challenges facing signature verification with the development of a reliable classification method using the machine learning method.
- To improve accuracy for signature verification by using machine learning methods.
- To deploy signature verification models for better results.

## RESEARCH QUESTIONS

Research questions related to the classification of signature verification by using machine learning method are as follows:

- What is the impact of using a machine-learning model in signature verification?
- What are the challenges researcher faces in signature verification by using machine learning for signature verification?
- Which machine learning algorithm is more efficient and categorizes an original and fake signature?

## LITERATURE REVIEW

There have been various surveys conducted on handwritten signature verification methods and the methodology utilized. Several approaches were recently developed, and significant studies have been conducted on both the extraction and classification of features. The signature analysis includes several matching algorithms, including holistic matching, regional matching, and multiple regional similarities. Signature verification can be done by using image processing. Feature extraction with the help of Gabor is added to the NN and produces 86.34% accuracy [3].

## BACKGROUND OF THE STUDY

Handwritten signature verification is becoming a key research area in computer vision and machine learning. Signature confirmation is certainly described as a machine learning job. The process is finished by verifying whether the sign is real or fake. Efficient machine-learning approaches can validate handwritten signatures in legal papers and financial trades, preventing costly fraud for clients [4].

Degree certificates have HEI (Higher Education Institutions) provides personalized certificates to recognize individuals' accomplishments. Digital printing as well as scanning technologies is rapidly advancing. The ease of access to important documents, such as degrees and IDs, caused an increase in forgeries. Manually verifying these certificates requires multiple levels of human interaction, making it a complex task. Verifying all graduates from higher education institutions is time-consuming and adds to the load on universities and colleges [5].

Document forgery involves creating forged or copyrighted documents for commercial and official usage. The current manual technique to document authentication has constraints.

1) There is no centralized process to verify each HEI-issued clearing certificate.

2) Fake academic degrees make it easy to avoid procedures for authentication.

3) Manual verification is inefficient in fostering good governance in educational organizations due to a small number of unauthorized certifications being issued.

4) Authenticating academic certificates from various higher education institutions is time-consuming and costly [6].

Signature verification algorithms fail to recognize that the person's signature is a unique drawing that reflects their personality and might consist of numbers, letters, symbols, and forms, rather than a particular form or picture. Signatures are used for verifying one's identity in transactions like banking and legal documents. Copying and counterfeiting a different person's signature can lead to problems. Signature confirmation systems use handwritten signatures to confirm identity and authority. They are a particularly legally as well as socially accepted form of authentication [7].

## RELATED LITERATURE

Scholars from several academies and administrations have been interested in the topic of sign verification due to the importance of handwritten signatures as personal verification in biometric systems. The summation of the huge work accomplished on this topic has been provided in a very thorough evaluation in [8] for the years (1989) and [9] for the periods (1989-1993).

In this segment, we evaluate the innovative signs of progress and rising difficulties in handwritten confirmation systems over the last 12 years, from 2012 to the present. The strategies applied in a study for feature extraction are compared to classifiers in documentation and verification methods.

Hamade'ne et al. introduced an approach using the contourlet convert and co-occurrence matrix. Main, the contour let transform was used to determine the contour section shapes of the handwritten sign. The track number was then computed consuming the co-occurrence matrix. The CEDAR dataset was tested with a support vector machines (SVM) algorithm [10].

Nemours and Chibani observed their relevance to handwritten sign confirmation. The ridgelet transforms and network structures were utilized to remove key attributes. The CEDAR dataset's performance was evaluated in comparison to SVM classifiers [11].

Kamihira et al. suggested a sign authentication method called "combined segmentation-verification" that uses both offline as well as online characteristics. Three distinct offline article directions were derived from pictures of the Japanese sign (complete name) and photographs of the Japanese sign (major and latest name). For each rancid line article vector, the space was calculated to confirm the sign. Online arrangements apply a dynamic programming similar technique for sign time series records. The final evaluation choice was made by consuming an SVM classifier created on the metric and dynamic encoding [12].

Griechisch et al. offered an online sign-confirmation approach based on simple numerical trials and period parameters. They examined the x, and y directs, force, and velocity features separately before combining them. System efficiency was assessed using the Dutch dataset [13].

Fayyaz et al. described a method that relies on autoencoders to learn sign properties. These qualities were used to demonstrate users' signs. Then, one session classifier was used to classify users' signatures. The suggested method of verification was assessed using the SVC2004 signature database. The outcomes of the experiment revealed a reduction in errors and a gain in accuracy [14].

Radhika and Gopika operated on merging online as well as offline handwritten signature elements to validate them. The online data was collected using a camera, while the offline data was collected using digital signature photos. First, both online and offline data underwent preprocessing phases. Next, both characteristics were saved, with features based on pen tip tracking being used online and gradient and projection-based features being used offline. Ultimately, signs were confirmed using equal procedures individually, and their productions were mixed and fed into the SVM classifier [15].

| Ref | Database | Features | Algorithms | Performance |
|---|---|---|---|---|
| (Alsuhimat & Mohamad, 2023). | UTSig dataset has(8280) | Feature extraction | HOG Algorithm | 92% accuracy |
| (Hashim et al., 2022). | Offline and online datasets | Feature extraction classification techniques | Machine learning approaches | 98% accuracy |
| (Kurowski et al., 2021). | 10,622 signatures | Dynamic analysis, Neural networks | Triplet loss strategy | Improved results |
| (Zhou et al., 2021). | Online combined data of 1200 signatures | Offline and online elements | SVM, Score merging method | Superior results |
| (Saleem & Kovari, 2020). | 5 datasets | Z-standardization,Various attributes | z-normalization | 70%, 92% accuracy |
| (Sharif et al., 2020). | CEDAR, GPDS | Aspect ratio, Sign area, Pure thickness, Centroid, Angle, Direction | SVM classifier | N/A |
| (Foroozandeh et al., 2020). | 3 common datasets | Band transformation, Numerical features | Machine learning approaches | |
| (Sadak et al., 2020). | | Time-sequential points | Dynamic Time Warping (DTW | |
| (Ahmed Salman & Abdul wahab, 2020). | CEDAR | Ridgelet transform, Network structures | SVM classifiers | |
| (Jia et al., 2019). | SVC2004 Task 2 | Shape context, Function feature-based | Interval-valued effusive demonstration | EER 2.39% |
| (Serdouk et al., 2018). | MCYT-75 | Histogram of Template (HOT) | SVM classifier | |
| (Taşkiran & Çam, 2017). | Yildiz Practical Academy | Histograms of Oriented Grades (HOG) | PCA | 97.33% accuracy |
| (Lech & Czyzewski, 2016). | | Fixed structures, Time-domain roles | Dynamic Time Warping (DTW) | 0.82 |

**Table 1**: Accuracy Comparison of ML Algorithms

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)

Volume 3, Issue 2, 2025
https://jecir.com/

An early study on the verification of signatures was carried out. Characteristics taken from signatures that have been divided into sections that are vertical and horizontal were worked on.

IDENTIFICATION AND VERIFICATION

Verifying and identifying signatures is regarded as one kind of biometric system that is applied to person identification. By examining the handwriting style, which varies between and among individuals, one can verify the identity of a person by utilizing their signature. Passports, driver's licenses, immigration, security applications, personal device logins, voter registration, medical records, and smart cards are just a few examples of the papers and activities that use biometric identification and verification.When identifying signatures, the system needs a user's signature to compare it to all the signatures registered in the dataset. It then calculates the results of the similarity between the two signatures. The identified user will be shown by the most similar result, and there are two fundamental methods for signature verification.

Applications for biometric identification and verification can be found in many commonplace papers and activities, including passports, driver's licenses, immigration, applications for voter registration, smart cards, personal device login, security, and health information.

When identifying signatures, the system should be supplied with the user's signature so that it may be compared to the different signatures registered in the dataset. A similarity score will be determined. While there are two fundamental methods for verifying signatures, the most similar result will show who the identified user is. These approaches can be classified as either writer-independent or writer-dependent. The writer-independent method involves training a single paradigm for the entire user base and matching the query signatures in a similarity/dissimilarity space with the reference signatures.

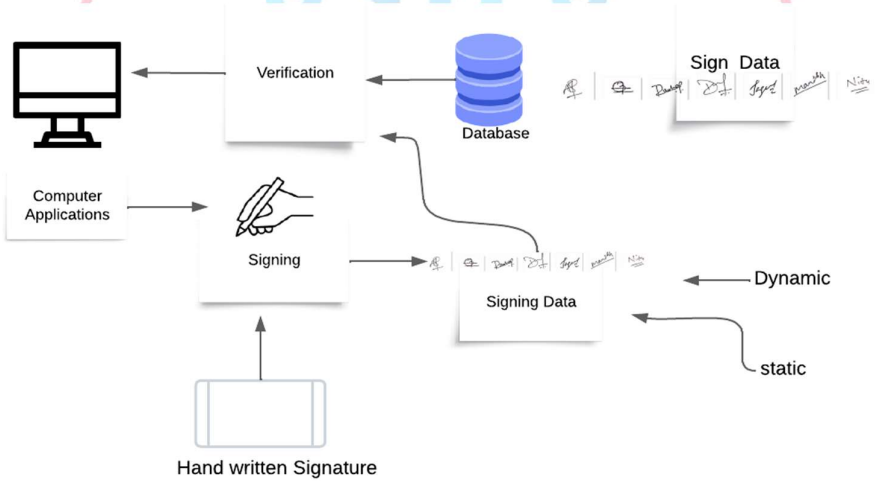


**Fig 4:** A biometric handwritten signature verifier

The two main approaches utilized in the verification process are model-based verification and distance-based verification. To characterize the distribution of data, models like logistic regression models (LR), neural networks (NN), and support vector machines (SVM) are developed in the model-based approach.

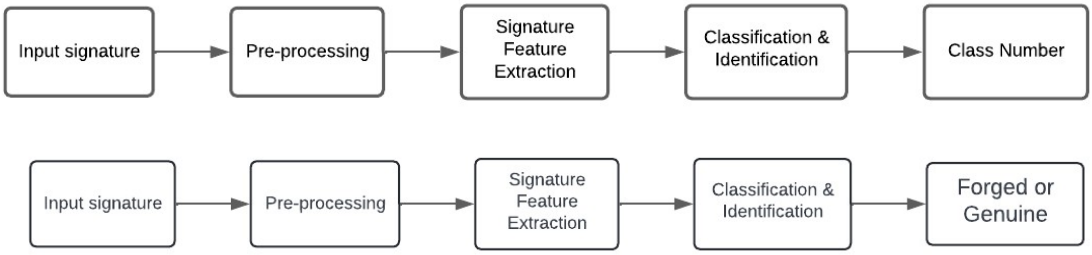


**Fig 5:** Identification System Stages

The term "parameter-based" mostly describes how long the both the signature and the quantity of pen tips on the page. Pressure data and signature trajectories are typically referred to as function-based characteristics. Functional features that are the basis for dynamic features typically yield superior outcomes [16]. The signature is defined as a vector of elements in the context of parameter-based features, where each element represents the value of a single feature. Examples of these characteristics are average speed, height, and width. Each parameter-based feature has an identical signature dimension.

| Feature Extraction Technique | Advantages | Limitations |
|---|---|---|
| **Statistical features** | (1) Detected more readily than with structural traits.<br>(2) Relative to statistical properties, noise and distortion have less effect. | Suitable only with gray-level and color images |
| **Global features** | (1) Describe the entire image; | Sensitive to clutter and occlusion. |
| **Structural features** | (2) Include the form and texture descriptors in this feature group.<br>(3) Extremely compact image representations are displayed, where each picture is represented by each point in a high-dimensional feature space. capable of encoding some structural information about the items. | Suitable with binary images only |
| **Local features** | (1) The texture in image areas are shown<br>(2) Invariant to scale, rotation, and other transformations | (1) Key-points distinguishing is required<br>(2) Comparing images may be more difficult because of the differing numbers of key-points images.<br>(3) No spatial information |
| **Contourlet transform (CT)** | (1) Suitable for processing two-dimensional pictures.<br>(2) The transformation uses more directions<br>(3) Capable of effectively eliminating noise from the image's borders and smooth sections. | (1) Unsuitable for image coding due to duplicate transformation |

**Table 2:** A comparative analysis of the most popular methods for extracting features

LITERATURE GAP

In the fake signature, verification highlights the critical areas that require more study. It points out the need for systematic investigation of feature extraction and selection methods particular to fake signature verification categorization. It also highlights the lack of detailed testing on a variety of datasets to guarantee the robustness and generalization of classification models. The overview also draws attention to the lack of research on the creation and assessment of interpret able classification models for fake signature verification.[17] Finally, it draws attention to the paucity of research on real-time categorization systems, which are crucial for prompt monitoring and decision-making. Closing these gaps will improve the precision and dependability of co-fake signature verification systems.

ARCHITECTURE

In this study, preprocessed signature photos are divided into training and test sets according to a predetermined split ratio, batch by batch. The image processing tool's orange functions are used for this. These preprocessed signatures are then kept in a file directory structure. Next, the Orange tool is used to develop the LR.SVM,NN in Python utilizing an inspection V3 backend in order to identify the patterns linked to the signatures.

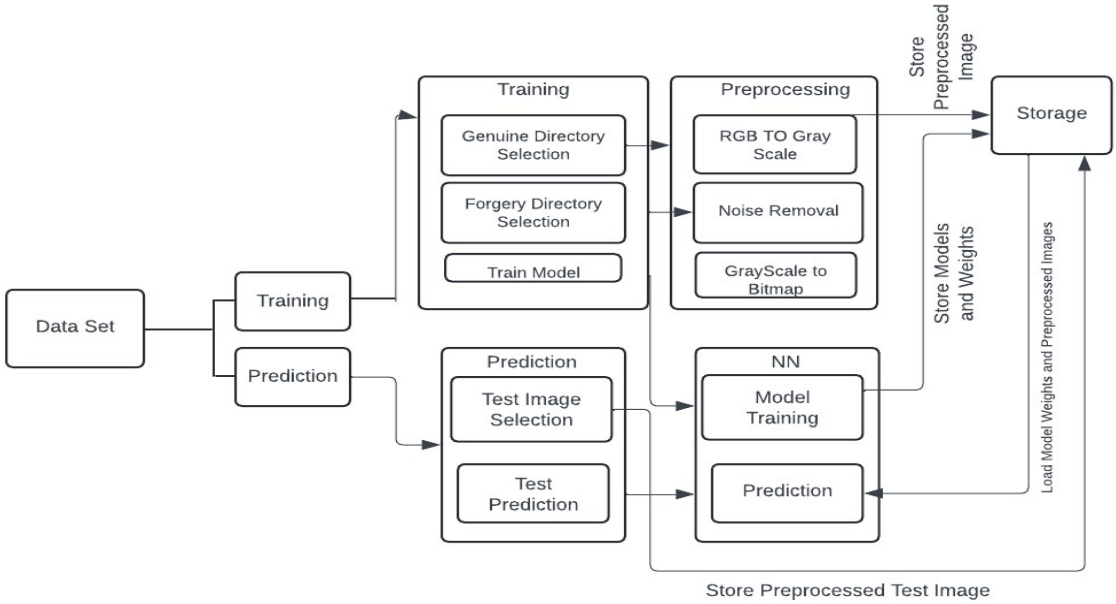


**Fig 6:** Model Architecture

RESEARCH METHODOLOGY

This research aims to develop a powerful computational tool for categorizing forgery signature verification. The proposed methodology involves a step-by-step approach to achieving correct fake signature verification cases based on the available data. The research will focus on classification algorithms to build an effective model. The methodology described here will serve as a guide for researchers interested in fake signature verification tasks.

MACHINE LEARNING IN SIGNATURE VERIFICATION

Since ML techniques and approaches form the foundation of the techniques and approaches used throughout this thesis, we rapidly go over various concepts and steps of a typical ML process in this part. Instead of depending on rigidly written instructions, the discipline of machine learning develops computer algorithms that can complete tasks autonomously.[18] In other terms, machine learning is the process through which computers learn new knowledge. Algorithms for machine learning have been effectively used in a number of disciplines. ML problems fall into two basic categories: supervised machine learning and unsupervised machine learning.

SUPERVISED MACHINE-LEARNING

Accurate classification of data or prediction of events relies on how datasets with labels are used to train algorithms. Based on a training collection of samples that includes accurate targets or replies, the algorithm responds to all possible inputs. This is often referred to as example-based learning.

REGRESSION

Finding the correlations between independent variables or characteristics and dependent variables or outcomes is possible with regression analysis. Forecasting is a method commonly used for, regression algorithms are usually used for population growth prediction, weather forecasting, Market sales forecasting. Polynomial, logistic, and linear regression are examples of regression techniques.

DATA CLASSIFICATION

An algorithm is utilized to properly categorize test results into the various categories. It looks for particular things in the data collection and makes an effort to infer how those objects should be labeled or described. Different categorization algorithms are now available like (SVM,LR,NN) however, it is impossible to tell which one would be better than the others. It is decided by the available tools and the kind of dataset.

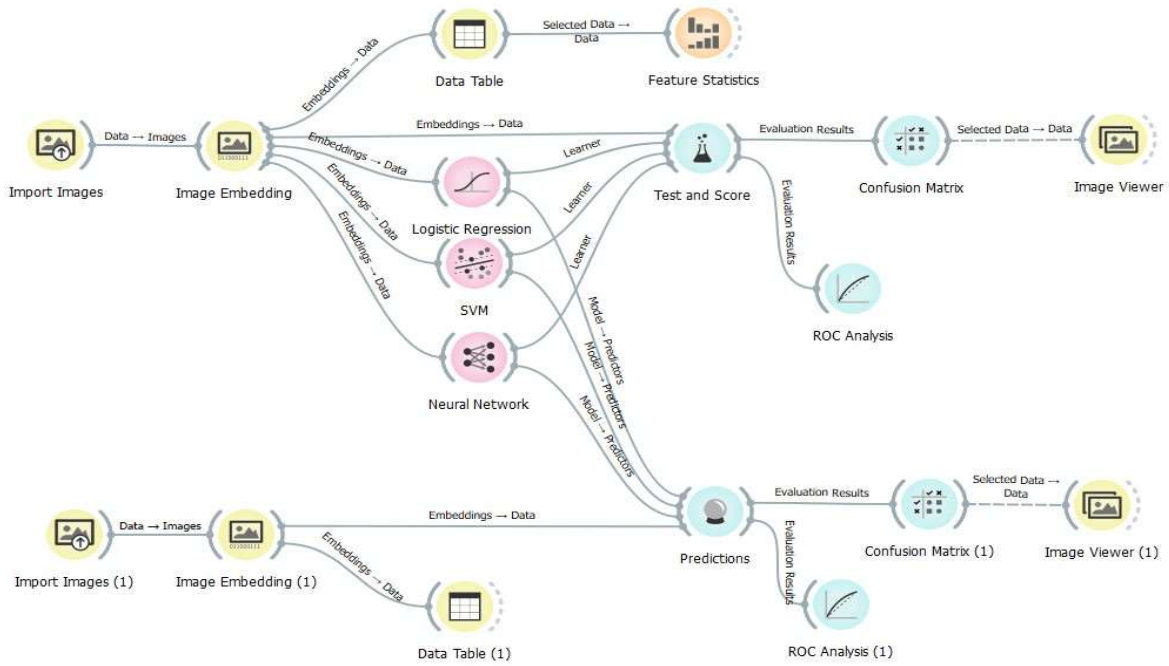


**Fig 7:** Research Model

The objective of this thesis is to create a robust signature verification classification model using a variety of machine-learning methods.

| Classifier | Advantages | Limitations |
|---|---|---|
| **Support vector machine (SVM)** | (1) Ideal for tidy, tiny datasets<br>(2) Operational in spaces with high dimensions | (1) Less effective on noisy datasets;<br>(2) Not appropriate for large datasets<br>(3) Selecting an appropriate kernel function that is reliable to interpret might be challenging. |
| **Dynamic time warping (DTW)** | (1) Time series averaging is responsible for the classification's increased speed and accuracy.<br>(2) Fit for a limited selection of templates | (1) The number of templates is restricted<br>(2) Actual training samples is required |
| **Deep Learning** | (1) Processing power has no bearing on it.<br>(2) High dimensionality<br>(3) Autonomous data adaptation<br>(4) Faster in obtaining results<br>(5) Capable of handling large and intricate datasets | (1) Difficult to comprehend<br>(2) Requires a lot of data for training<br>(3) Requires a lot of memory and processing power<br>(4) Expensive<br>(5) Excessive prevalence of failures |
| **Nearest Neighbor (KNN)** | (1) The complete dataset is covered for finding Knearest neighbors<br>(2) Cannot handle the missing value issue regression problems | (1) Alert to anomalies<br>(2) Adequate for categorizing several classes and<br>(3) Expensive in terms of math |

| | | |
|---|---|---|
| | | (4) A large amount of RAM is needed.<br>(5) There must be homogeneous traits. |
| **Probabilistic neural network (PNN)** | (1) Quicker and more accurate than MLPs<br>(2) Insensitive to outliers<br>(3) Representative training set is required | (1) More memory space is needed<br>(2) When it compared to MLP it is slower in case of new classification samples |
| **Euclidean distance** | (1) Extremely well-liked technique;<br>(2) Simple computation;<br>(3) Effective with compact or isolated clusters; (4) Capable of handling variable-length inputs; | 1) More memory and time it requirement<br>2) Sensitive to outliers<br>3) Sensitive to the outliers |

**Table 3:** Compression between most used classifier

UNSUPERVISED LEARNING

Unlabeled datasets are examined and clustered using ML techniques in unsupervised ML. These algorithms operate independently of humans to identify hidden data clusters or patterns. The algorithm looks for similarities between the input data instead of giving appropriate or correct responses, therefore the input data are classified continuously. This is also known as a density estimate [19].

DIMENSIONALITY REDUCTION

Although having more data typically results in more accurate findings, it can also affect how well ML algorithms work (e.g., by causing over fitting) and making it more difficult to envision datasets. When a dataset has an extreme number of attributes or dimensions, the dimensionality reduction (DR) technique is utilized. While reducing the amount of data inputs to a manageable amount, the integrity of the dataset is maintained as much as feasible. It is frequently employed throughout the data preparation procedure [20].

CLUSTERING

Unlabeled data are classified using the data mining method of clustering according to their differences or similarities. The process of grouping raw, unlabeled data items into groups that can be seen as patterns or structures in the data is known as clustering. There are various clustering algorithms, such as overlapping, hierarchical, exclusive, & probabilistic ones.

REINFORCEMENT LEARNING

This learning falls in between supervised and unsupervised learning. The study of decision-making is called reinforcement learning. It requires understanding how to respond in a situation in order to achieve the rewards. This ideal conduct is learned through interactions with the environment and watching how it reacts. The algorithm is informed when the response is incorrect, but it is not provided any instructions on how to make it right. It must research and evaluate several options before deciding how to reach the best conclusion. Because the check looks at the response or answer but doesn't demand perfection.

RESEARCH DESIGN/ STUDY MODEL

This research design outlines the approach and methodology for developing model forgery signature verification. The research design includes the gathering of data, preprocessing, classification algorithms, and evaluation of models. The primary objective is to create accurate and efficient forgery signature verification characteristics for cases using machine learning techniques. Our proposed technique outperforms offline signature verification approaches such as K-nearest neighbor, support vector machine (SVM), neural network (NN), and logistic regression in terms of accuracy.

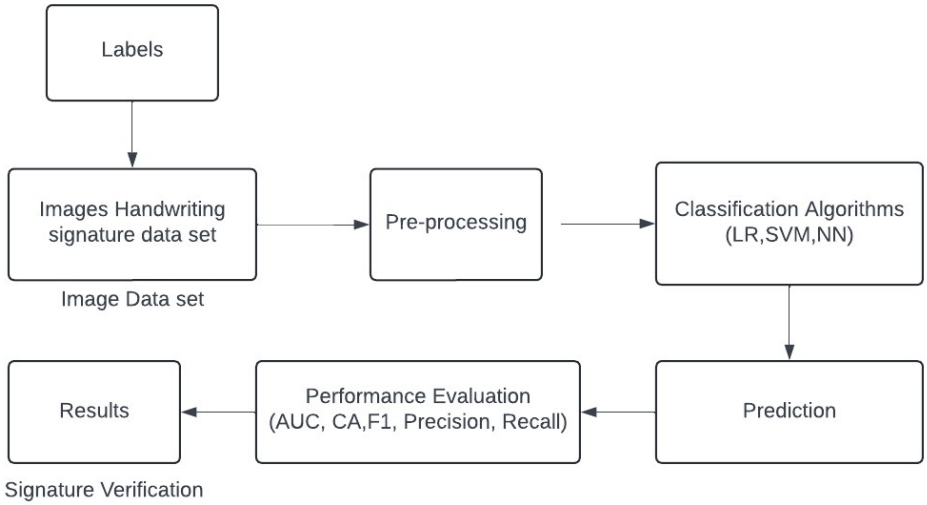


**Fig 8:** Model Diagram

RESULTS AND DISCUSSIONS

The objective of the fake signature verification project was to employ machine learning techniques to develop an accurate and efficient system for identifying and classifying. The project utilized neural networks (NNs), a powerful deep learning architecture, to analyze fake signature verification. In this segment, we present the results gained from the project and discuss their effects.

EXPERIMENTAL SETUP

The experiment consequences show the ability of the proposed method, especially for our main task our method not only correctly distinguishes the genuine and forger.

The investigative results demonstrate the usefulness of the proposed strategy, particularly in accomplishing our core aim. Our technique not only identifies between actual and faked signatures during the training and validation stages, but it also achieves astonishing results of approximately 97.10%, 98.40%, 98.10%, and 98.90% accuracy on the testing dataset, respectively.

EVALUATION

After putting a model into practice in everyday life, how well will it function on data that has never been seen before to ascertain its overall performance? Selecting the measure is dependent on the type of model under discussion rather than the type of model itself.

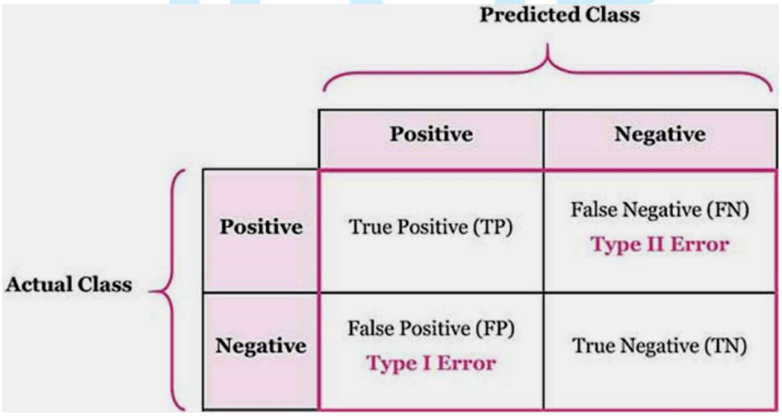


**Fig 9:** Confusion Matrix for classification of signature Verification

Calculating accuracy, sensitivity, specificity, precision, and F1 score is aided by the confusion matrix.

ACCURACY

A model's total correctness is measured by its accuracy. It is computed as the ratio of all test cases to the number of accurate predictions (true positives and true negatives).

Accuracy=(Number of Turly Classified Samples)/(Total Sample)

…….. (1)

Accuracy=(TP+TN)/(TP+TN+FP+PN).....

SENSITIVITY

The test model's actual positive rate is known as sensitivity. It assesses the degree to which a test can identify individuals who actually have the illness. It is calculated as the percentage of true positives (incorrectly identified as positive) out of all actual positives.

Sensitivity=(Trure Positive )/(True Positive+False Negative

)……. (2)

Sensitivity=TP/(TP+FN)……

SPECIFICITY

Specificity is the actual negative test case rate for the model. It evaluates how well a test can identify those who do not have the illness. It is calculated as the percentage of true negatives among all real negatives that were mistakenly labeled as negative.

Specificity=(True negative )/(True Negative+False Positive )..... (3)

Specificity=TN/(TN+FP)……..

PRECISION

The prediction value is positive. The percentage of actual positive outcomes among all positive forecasts is computed. It highlights how dependable a good prognosis is.

Precision =(True Positive)/(True Positive +False Positive

)…… (4)

Precision=TP/(TP+FP)…….

F1 Score

It offers a balanced measurement of both precision and sensitivity because it is the harmonic mean of both. When you are concerned about avoiding false positives as well as false negatives, it is helpful.

F1 Score=2×(Precision×sensitivity

)/(Precision+sensitivity)…… (5)

DISCUSSION

The classification model was trained and validated using signature image data. Images of 27 distinct people's signature specimens were taken throughout the data collection phase. Was gathered, with each class receiving 100 signatures. Of the 100 signatures—85 of which are used as a training set and 15 of which are utilized as the test dataset. The hard copy data was transformed into a photograph file taken using a smartphone camera and scanned into the computer.

CLASSIFICATION

Classification results of models LR,SVM and NN training for different cases are as below. For Signature verification the LR model classification accuracy is 100%, Area Under Curve (AUC) 100%, F1 score 98.8%, Precision 98.8%, and recall 98.8%. For SVM the classification accuracy is 100%, , F1 score 98.5%, Precision 99.5, and Recall 99.5%. For Neural Network the classification accuracy is 100%, AUC 99.2%, F1 score 99.2%, Precision 99.2%, and Recall 99.2%. Overall model training results are shown in Table.

**Fig 10:** Classification Results

| Model | AUC | CA | F1 | Prec | Recall | MCC |
|---|---|---|---|---|---|---|
| Logistic Regression | 1.000 | 0.988 | 0.988 | 0.988 | 0.988 | 0.988 |
| SVM | 1.000 | 0.984 | 0.984 | 0.984 | 0.984 | 0.983 |
| Neural Network | 1.000 | 0.992 | 0.992 | 0.992 | 0.992 | 0.992 |

| Results/ validation | AUC(Area Under ROC Curve) (%) | CA (Classification Accuracy) (%) | F1 Score (%) | Precision (%) | Recall (%) |
|---|---|---|---|---|---|
| **CV1** | 100 | 99.9 | 99.9 | 100 | 99.8 |
| **CV2** | 100 | 100 | 100 | 100 | 100 |
| **CV3** | 100 | 99.6 | 99.6 | 99.6 | 99.6 |
| **CV4** | 100 | 100 | 100 | 100 | 100 |
| **CV5** | 100 | 100 | 100 | 100 | 100 |
| **CV6** | 100 | 99.7 | 99.7 | 99.6 | 99.8 |
| **CV7** | 100 | 99.6 | 99.6 | 99.6 | 99.6 |
| **CV8** | 100 | 99.6 | 99.6 | 99.4 | 99.8 |
| **CV9** | 100 | 99.6 | 99.6 | 99.6 | 99.6 |
| **CV10** | 100 | 99.9 | 99.9 | 99.8 | 100 |
| **Average** | 100 | 99.7 | 99.7 | 99.7 | 99.8 |

**Table 4**: Signature Verification Classification Accuracy Summary

RECEIVER OPERATING CHARACTERISTICS (ROC) CURVE ANALYSIS
CLASSIFICATION ROC ANALYSIS

In this proposed model, Receiver operating characteristics curve is used for evaluation of results. ROC curve is used to calculate performance of classification model and display result in graphical form. This curve plots two paramters, one is True positive rate and false positive rate. ROC with 0.575 threshold are generated in this study model. Signature verification classification accuracy result as 0.600 as shown in Figure 4.4.

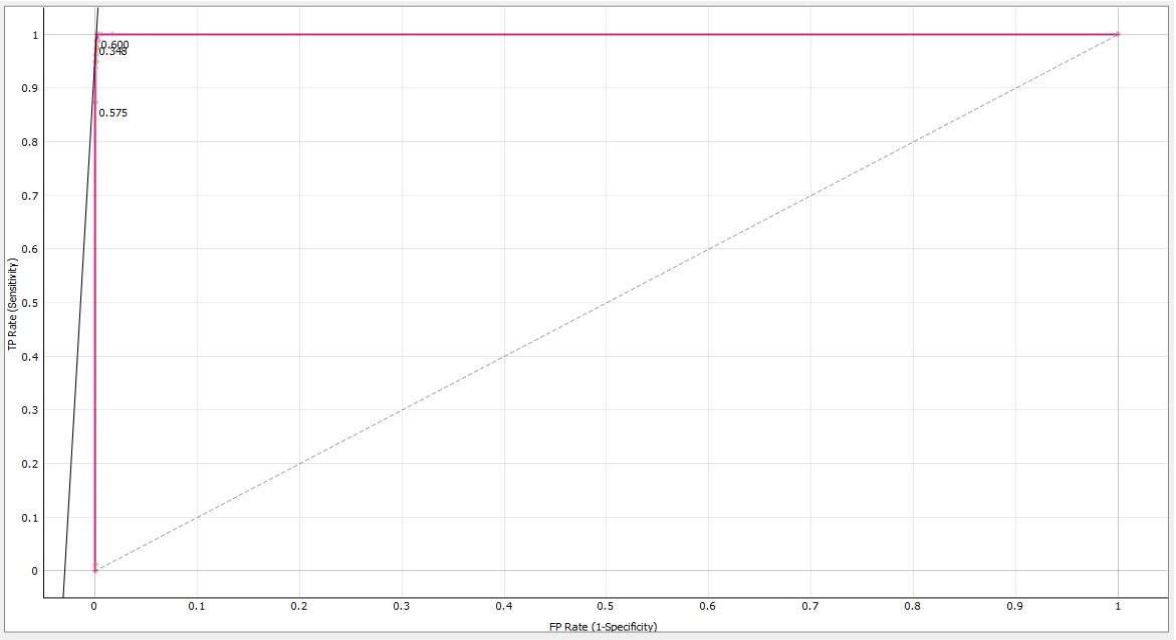


**Fig 11**: Classification ROC

| Category | AUC (Area Under ROC Curve) (%) | CA (Classification Accuracy) (%) | F1 Score (%) | Precision (%) | Recall (%) |
|---|---|---|---|---|---|
| Handwritten | 100 | 99.5 | 97.8 | 96.8 | 98.9 |
| Online | 100 | 100 | 100 | 100 | 100 |
| Offline | 100 | 99.5 | 99.3 | 99.7 | 99.0 |
| Overall | 100 | 99.5 | 99.5 | 99.5 | 99.5 |

**Table 5:** Classification Results Summary

Signature verification classification accuracy is 1(100%) as shown in figure 4.5

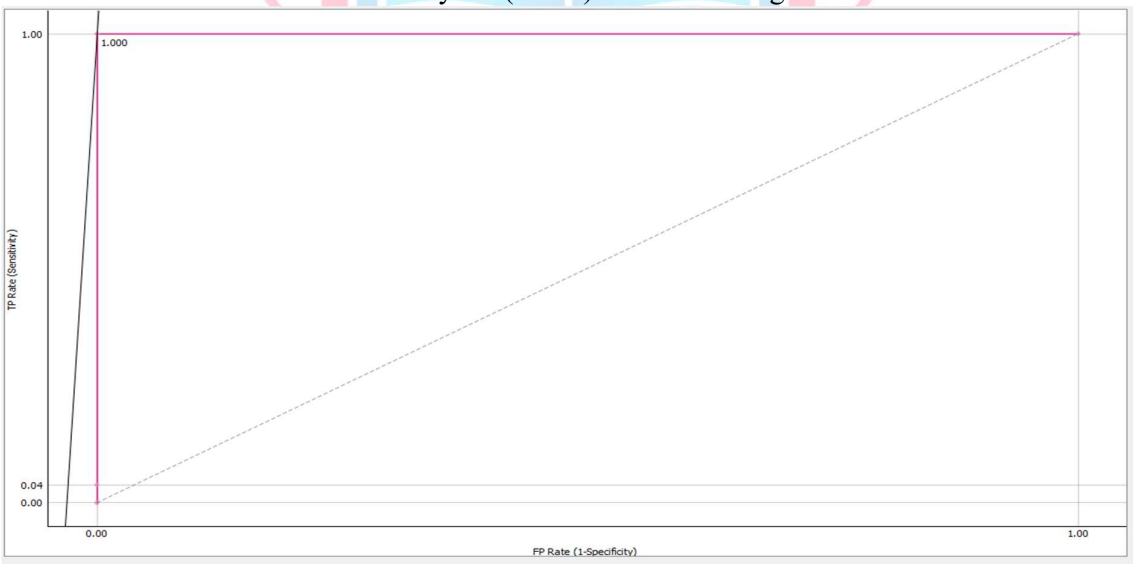


**Fig 12**: Prediction ROC

| Category | AUC (Area Under ROC Curve) (%) | CA (Classification Accuracy) (%) | F1 Score (%) | Precision (%) | Recall (%) |
|---|---|---|---|---|---|
| Handwritten | 100 | 99.7 | 98.6 | 100 | 97.2 |
| Online | 100 | 99.7 | 100 | 100 | 100 |
| Offline | 100 | 99.7 | 99.6 | 99.6 | 100 |
| Overall | 100 | 99.7 | 99.7 | 99.7 | 99.7 |

**Table 6:** Prediction Results Summary

COMPARATIVE ANALYSIS

Based on experimental findings, it is possible to verify handwritten signatures effectively by combining static and dynamic features using SF-A. Through examination of the experimental outcomes for every feature, it is discovered that for offline images, LR works better than SVM when the number of samples is 3 or 5, while SVM works better than NN when the number of samples is 8 or 10. Overall, texture features outperform geometric features, which could have something to do with feature vector dimensions. Geometric features have a reduced feature vector dimension. Nonetheless, the outcome of merging texture and geometric features typically enhances verification accuracy. Because the geometric feature reflects the image's global information and the texture feature represents the offline image's local texture information, it also lowers the FAR and FRR. More representativeness and dependability should be seen in the composite feature vector. The experimental results of both SF-L and SF-A are better than those of static or dynamic features alone, from the standpoint of score fusion, that is, combining static and dynamic features. This suggests that the two fusion methods can enhance the complementary performance between the two classifiers. In terms of SF-L and SF-A (score fusion method based on accuracy), the SF-A suggested in this work has weighted the classifier's verification accuracy to obtain the best results under various training samples. Specifically, the FAR (false acceptance rate) index's improvement. More specifically, the FAR index has improved more significantly, and there are frequently greater FAR standards in some situations [21]. As a result, we may say that the suggested SF-A can significantly raise the effectiveness of handwritten signature verification.

LIMITATION

Signature verification has two main limitations: First, there is a high intra-class and inter-class variability; second, in real-life scenarios, only a small number of real signatures can be obtained for training; and third, there is insufficient data, which is also a problem that needs to be resolved. The person's original signature will change due to many factors, such as time and age; the imposter will also try to copy the signature with a lot of training beforehand.

Researchers discover two restrictions in offline signature verification. Initially, a large portion of the dynamic data contained in the signature is deleted. There is a discrepancy between the quantity of extracted characteristics and the available signature samples.

Following is a summary of the challenges associated with online and offline signature verification:

- The process of choosing a signer's best attributes;
- Assessing the performance of signature verifiers;
- Classifying forgeries;
- Analyzing signature variability and constancy;
- Updating reference sets and building big databases
- And comparing results using accepted and sensible guidelines.

CONCLUSION

This project used the most recent and potent LR, SVM, and NN that are currently available to experiment with and implement the signature verification job. In addition to experimenting with the classification or verification of offline signatures, this study also suggested a unique application program for experimenting with fresh signature datasets and training on them for subsequent novel verification challenges. The project's final results are incredibly encouraging and actually motivate us to conduct more study and development in this area [22]. Despite the developed software's optimistic performance, the lack of an online

verification technique is apparent due to the absence of dynamic features such as pen speed, pressure, azimuth angle, etc. would have significantly improved the verification performance and in coming future we are very eager to work on that. After the conclusion of this project we are very optimistic that will immerge many wonderful outcomes and possibilities in this field in the coming future.

FUTURE WORK

With the use of C++ wrappers for Python and its libraries in conjunction with logistic regression, support vector machines, and neural networks as the basis for our solution networks, we were able to detect the signature cheats with success. The model will be enhanced in the future by lowering CNN's error rejection rate.

Combining offline and online signature verification technologies is an intriguing concept that will fortify the system by necessitating both validity and speed of execution. Combining offline and online signature verification systems would be a promising endeavor as well. This would increase the system's robustness by increasing its execution speed and authentic appearance signature, which would make it more challenging to manufacture signatures. A single language was used to implement this project.

For better user engagement, many more languages can be added to the digital signature upload process via a graphical user interface (GUI) built on the Flask platform. The proposed system is very cost-effective in terms of real-time counterfeit detection and tracking, so it can be made more responsive by storing the extracted features and training them on artificial neural networks.

More sophisticated methods, including online verification, would have produced better application results if dynamic data characteristics, like pressure, speed, pen position, azimuth/altitude angle, etc., had not been incorporated into the system. Online signature verification is more reliable, saves time, and may be added in the future. The quantity of the data we gathered was restricted, and the data contradicted each other because human signatures vary so much. Higher precision may have been achieved if the data had been appropriately and widely collected. The dataset may not have undergone enough pretreatment; more data cleaning and preprocessing operations will guarantee improved results.

Data collection with enhanced technique, such as with an electronic signature capturing device, can facilitate big number of sample collection in relatively little time. Previously, training data was gathered in hard copy format, which limited the potential of collecting large number of training data. In further work, we can additionally concentrate on improving the system's accuracy by experimenting with new and improved parameter coefficients that lengthen the time interval between authentic and fake signatures.

REFERENCES

[1] H. A. Salman and H. Abdul wahab, “Anti-screenshot keyboard for web-based application using cloaking,” in *Proc. Int. Conf. Adv. Intell. Syst. Inform.*, 2020, pp. 473–478, doi: 10.1007/978-3-030-21005-2_45.

[2] F. M. Alsuhimat and F. S. Mohamad, “Offline signature verification using long short-term memory and histogram orientation gradient,” *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 10–19, Feb. 2023, doi: 10.11591/eei.v12i1.4024.

[3] A. Hamadene and Y. Chibani, “One-class writer-independent offline signature verification using feature dissimilarity thresholding,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1226–1238, Jun. 2016, doi: 10.1109/TIFS.2016.2521611.

[4] Z. Hashim, H. M. Ahmed, and A. H. Alkhayyat, “A comparative study among handwritten signature verification methods using machine learning techniques,” *Sci. Program.*, vol. 2022, p. 8170424, Jan. 2022, doi: 10.1155/2022/8170424.

[5] Sam et al., “Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet Inception-v1 and Inception-v3,” *Procedia Comput. Sci.*, vol. 161, pp. 475–483, 2019, doi: 10.1016/j.procs.2019.11.147.

[6] M. Kurowski, A. Sroczyński, G. Bogdanis, and A. Czyżewski, “An automated method for biometric handwritten signature authentication employing neural networks,” *Electronics*, vol. 10, no. 4, p. 456, Feb. 2021, doi: 10.3390/electronics10040456.

[7] I. Alim, N. Imtiaz, A. Al Prince, and M. A. Hasan, "AI and blockchain integration: Driving strategic business advancements in the intelligent era," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 2, pp. 38–50, 2025.
[8] M. Z. Afshar and M. H. Shah, "A narrative review for revisiting BCG matrix application in performance evaluation of public sector entities," *J. Res. Rev.*, vol. 2, no. 02, pp. 325–337, 2025.
[9] F. Leclerc and R. Plamondon, "Automatic signature verification: The state of the art - 1989-1993," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 8, no. 3, pp. 643–660, Sep. 1994, doi: 10.1142/S0218001494000346.
[10] F. S. Mohamad, F. M. Alsuhimat, M. A. Mohamed, M. Mohamad, and A. A. Jamal, "Detection and feature extraction for images signatures," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 44–48, 2018.
[11] 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, doi: 10.1016/0031-3203(89)90059-9.
[12] D. Ali and T. Ahmed, "Computational analysis of geothermal-enhanced heavy oil production," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 2, pp. 10–20, 2024.
[13] M. Z. Afshar and M. H. Shah, "Leveraging Porter's Diamond Model: Public Sector Insights," *Crit. Rev. Soc. Sci. Stud.*, vol. 3, no. 2, pp. 2255–2271, 2025.
[14] K. S. Radhika and S. Gopika, "Online and offline signature verification: A combined approach," *Procedia Comput. Sci.*, vol. 46, pp. 1593–1600, 2015, doi: 10.1016/j.procs.2015.02.089.
[15] R. Amin and A. A. Kazmi, "Smart grids: A comprehensive review of technologies, challenges, and future directions," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 2, pp. 45–70, 2024.
[16] T. A. Shiva, J. G. Brown, A. A. McField, R. E. Osborne, and C. D. Oberle, "Cultural associations with prosocial behaviors and attitudes among Asian Americans," *Asian Am. J. Psychol.*, 2025, early access.
[17] M. Sharif, M. A. Khan, M. Faisal, M. Yasmin, and S. L. Fernandes, "A framework for offline signature verification system: Best features selection approach," *Pattern Recognit. Lett.*, vol. 139, pp. 50–59, Nov. 2020, doi: 10.1016/j.patrec.2018.01.021.
[18] D. Suryani, E. Irwansyah, and R. Chindra, "Offline signature recognition and verification system using efficient fuzzy kohonen clustering network (EFKCN) algorithm," *Procedia Comput. Sci.*, vol. 116, pp. 621–628, 2017, doi: 10.1016/j.procs.2017.10.025.
[19] M. A. Saputra and I. Nurhaida, "Signature originality verification using a deep learning approach," *Electron. J. Educ. Soc. Econ. Technol.*, vol. 5, no. 1, pp. 19–29, 2024.
[20] N. Patel, P. J. Patel, and A. Changa, "Exploring the effectiveness of machine learning algorithms in image forgery detection," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 1, pp. 45–54, 2024.
[21] M. Asif, "Contingent effect of conflict management towards psychological capital and employees' engagement in financial sector of Islamabad," Ph.D. dissertation, Preston Univ., Kohat, Islamabad Campus, Pakistan, 2021.
[22] M. Asif and A. Shaheen, "Creating a high-performance workplace by the determination of importance of job satisfaction, employee engagement, and leadership," *Journal of Business Insight and Innovation*, vol. 1, no. 2, pp. 9-15, 2022.
[23] M. Asif, "Mediating role of trust between emotional intelligence and project team performance in telecommunication sector," *Journal of Business Insight and Innovation*, vol. 1, no. 2, pp. 9-15, 2022. *(Note: Assumed journal based on context; please verify if this is correct.)*
[24] Aurangzeb, M. Asif, and M. K. Amin, "Resources management and SME's performance," *Humanities & Social Sciences Reviews*, 2021, doi: 10.18510/hssr.2021.
[25] M. A. Pasha, M. Ramzan, and M. Asif, "Impact of economic value added dynamics on stock prices fact or fallacy: New evidence from nested panel analysis," *Global Social Sciences Review*, vol. 4, no. 3, pp. 135-147, 2019.
[26] S. H. Alizai, M. Asif, and Z. K. Rind, "Relevance of motivational theories and firm health," *International Journal of Management (IJM)*, vol. 12, no. 3, pp. 1130-1137, 2021.
[27] Aurangzeb, T. Mushtaque, M. N. Tunio, Zia-ur-Rehman, and M. Asif, "Influence of administrative expertise of human resource practitioners on the job performance: Mediating role of achievement motivation," *International Journal of Management (IJM)*, vol. 12, no. 4, pp. 408-421, 2021.

[28] M. Asif, M. A. Pasha, and A. Shahid, "Energy scarcity and economic stagnation in Pakistan," *Bahria University Journal of Management & Technology*, vol. 8, no. 1, pp. 141-157, 2025.
[29] A. Mumtaz, N. Munir, R. Mumtaz, M. Farooq, and M. Asif, "Impact of psychological & economic factors on investment decision-making in Pakistan Stock Exchange," *Journal of Positive School Psychology*, vol. 7, no. 4, pp. 130-135, 2023.
[30] M. Asif, H. Shah, and H. A. H. Asim, "Cybersecurity and audit resilience in digital finance: Global insights and the Pakistani context," *Journal of Asian Development Studies*, vol. 14, no. 3, pp. 560-573, 2025.
[31] M. Asif, "The complexities of bioterrorism: Challenges and considerations," *International Journal of Contemporary Issues in Social Sciences*, vol. 3, no. 3, pp. 2175–2184, 2024.
[32] Dr. Aurangzeb and M. Asif, "Role of leadership in digital transformation: A case of Pakistani SMEs," in *2021 Fourth International Conference on Emerging Trends in Engineering, Management and Sciences (ICETEMS)*, Oct. 13-14, 2021, vol. 4, no. 1, pp. 219-229.
[33] H. A. Usama, M. Riaz, A. Khan, N. Begum, M. Asif, and M. Hamza, "Prohibition of alcohol in Quran and Bible (A research and analytical review)," *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 19, no. 4, pp. 1202-1211, 2022.