Jurnal Ilmu Komputer dan Informatika (JIKI) Vol. 6, No. 1, June 2026, Page. 17-32
P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

Hybrid LBP–HOG Feature Extraction with Support Vector Machine and Deep Belief Network for Offline Signature Identification and Verification

Alvian Ardiansyah*[1], Rizal Adi Saputra[2], La Surimi[3]

[1,2,3] Department of Informatics Engineering, Halu Oleo University, Indonesia

Email: [1]alvianarrdiansyah@gmail.com

Received: Apr 22, 2026; Revised: May 28, 2026; Accepted: May 31, 2026; Published: Jul 17, 2026

Abstract

Offline signature verification remains a challenging task due to high intra-writer variability and the presence of skilled forgeries, which can reduce the reliability of biometric authentication systems. This study aims to develop a robust offline signature identification and verification framework by integrating hybrid feature extraction and machine learning-based classification methods. The proposed approach combines Local Binary Pattern (LBP) and Histogram of Oriented Gradients (HOG) to capture complementary texture and shape characteristics from signature images. The extracted features are subsequently classified using Support Vector Machine (SVM) for writer identification and Deep Belief Network (DBN) for signature verification. The experimental dataset consists of signatures collected from 60 individuals, with each participant providing 8 genuine and 8 forged signatures. Prior to feature extraction, preprocessing stages including grayscale conversion, contrast enhancement, and Otsu thresholding were applied to improve image quality and segmentation consistency. Experimental results demonstrate that the proposed framework achieves an identification accuracy of 89.58% using SVM, while the DBN-based verification model attains an accuracy of 87%, an F1-score of 86%, and an AUC value of 0.85. The novelty of this study lies in the integration of hybrid LBP–HOG feature extraction with a dual-classification architecture combining SVM and DBN for offline signature authentication tasks. The combination enables the system to effectively represent both local texture patterns and structural signature characteristics while improving classification robustness against forged signatures. These findings indicate that the proposed framework provides a promising contribution to offline biometric authentication and computer vision-based signature verification research.

Keywords: *Deep Belief Network, Image Processing, Pattern Recognition, Signature, Support Vector Machine*

1. INTRODUCTION

Signatures are a traditional form of authentication that remains widely used in legal documents, banking, business contracts, and administrative transactions. Although handwritten signatures are easy to implement and are legally recognized, manual verification presents several significant limitations, including susceptibility to human error, time inefficiency, and vulnerability to forgery. The growing demand for improved efficiency and security in document authentication has led to the development of automated signature verification systems, particularly in the domain of offline signature verification. Contemporary research emphasizes the integration of advanced feature extraction techniques with machine learning, especially deep learning algorithms, to enhance accuracy and robustness against intra-class variations and skilled forgeries [1].

One of the primary technical challenges in offline signature identification and verification lies in the high degree of intra-writer variability, which refers to natural variations in genuine signatures produced by the same individual, such as differences in pressure, inclination, or writing instruments. In addition, there is often a significant similarity between genuine signatures and skilled forgeries, which are intentionally designed to closely resemble authentic signatures. Furthermore, factors such as image quality including noise, resolution, and contrast along with preprocessing steps such as binarization and normalization, and the size of the dataset, have a substantial impact on system performance. Therefore, the selection of feature extraction techniques that are robust to such variations, as well as classification architectures capable of learning highly discriminative representations, is critically important [2].

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

Due to the legal and financial consequences associated with verification errors, such as false acceptance and false rejection, offline signature verification systems are required to achieve high accuracy while maintaining robustness against skilled forgery and acquisition variability. Consequently, recent studies have increasingly focused on integrating advanced feature extraction and deep learning architectures to improve discriminative capability and generalization performance in biometric authentication systems. Conventional approaches based on handcrafted features such as Local Binary Pattern (LBP), Histogram of Oriented Gradients (HOG), Scale-Invariant Feature Transform (SIFT), and Gray Level Co-occurrence Matrix (GLCM) have demonstrated promising performance in capturing texture and structural characteristics of signatures [3], [4]. However, single-feature extraction methods often exhibit limited robustness when dealing with high intra-writer variability and complex forgery patterns.

Recent advances in deep learning have introduced Convolutional Neural Networks (CNNs), Siamese Networks, Autoencoders, and Vision Transformer (ViT)-based architectures for offline signature verification tasks. CNN-based methods have shown superior capability in automatically learning hierarchical feature representations directly from raw signature images [5]. Siamese Networks are widely adopted for writer-independent verification because they effectively learn similarity metrics between genuine and forged signature pairs [6]. Furthermore, Vision Transformer architectures have recently demonstrated competitive performance in computer vision tasks due to their ability to model long-range dependencies and contextual relationships within image representations [7]. Despite their advantages, these deep learning approaches generally require large-scale datasets and substantial computational resources to achieve stable generalization capability, which limits their applicability in practical offline signature verification scenarios where annotated forged signature datasets are often limited [8].

Several recent studies have therefore explored hybrid frameworks that combine handcrafted feature extraction with machine learning or lightweight deep learning classifiers to balance computational efficiency and verification accuracy [9], [10]. Support Vector Machine (SVM) remains one of the most widely used classifiers because of its strong generalization performance in high-dimensional feature spaces and relatively small datasets [11]. Meanwhile, Deep Belief Network (DBN) provides advantages in learning hierarchical non-linear representations while maintaining lower computational complexity compared to fully end-to-end deep learning architectures [12]. Nevertheless, existing studies still predominantly focus on either single-feature extraction methods or single-classifier frameworks, resulting in limited robustness against intra-class variability and skilled forgery. Therefore, there remains a research gap in developing hybrid offline signature verification frameworks that integrate complementary feature extraction methods with multi-stage classification architectures to improve both identification and verification performance under limited-data conditions.

To address these challenges, this study proposes a hybrid offline signature identification and verification framework that integrates Local Binary Pattern (LBP) and Histogram of Oriented Gradients (HOG) as complementary feature extraction techniques to capture both local texture information and global geometric structures of signatures. Unlike previous approaches that primarily rely on single-feature extraction or single-classifier methods, which often exhibit limited robustness against intra-writer variability and skilled forgery, the proposed framework combines LBP–HOG features with Support Vector Machine (SVM) and Deep Belief Network (DBN) to improve discriminative capability and generalization performance. SVM is utilized for writer identification due to its effectiveness in high-dimensional feature spaces and limited-data conditions, while DBN is employed for verification tasks to learn hierarchical and non-linear feature representations. Although recent deep learning approaches such as CNNs and Vision Transformers have achieved promising results, they generally require large-scale datasets and high computational resources. Therefore, the novelty of this study lies in the integration of hybrid handcrafted feature extraction with a dual-classification architecture that aims to provide a more computationally efficient yet robust solution for offline signature authentication under limited-data conditions.

Although the dataset used in this study consists of only 60 individuals with 8 genuine and 8 forged signatures per subject, the dataset size remains suitable for evaluating the effectiveness of the proposed framework in limited-data environments, which commonly occur in practical offline signature verification applications due to privacy constraints and the difficulty of collecting forged signature samples. In contrast to computationally intensive deep learning approaches that generally require large-scale datasets, the proposed hybrid framework combining LBP–HOG feature extraction with SVM and DBN is designed to achieve robust performance and better generalization under relatively small training data conditions. Therefore, the objectives of this study are: 1) to develop a hybrid offline signature identification and verification framework integrating LBP and HOG feature extraction; 2) to evaluate the effectiveness of SVM for writer identification and DBN for signature verification; and 3) to analyze the capability of the proposed framework in improving robustness against intra-writer variability and skilled forgery. The scientific contribution of this study lies in the integration of complementary handcrafted feature extraction with a dual-classification architecture to provide a computationally efficient and robust alternative for offline biometric authentication systems.

2. METHOD

The research workflow consists of five main stages: Data Collection, Preprocessing, Feature Extraction, Modelling, and Evaluation. Each stage has specific objectives and interrelated activities, beginning with the identification of research needs and the formulation of the study scope, followed by system design and feature extraction of signature images, model implementation and training for classification tasks, and concluding with system testing and evaluation.

2.1. Data Collection

In the data collection stage, this study utilized a combination of secondary and primary data consisting of genuine and forged offline signature images. The secondary dataset was obtained from a publicly available Kaggle dataset containing signatures from 24 individuals, while the primary dataset was collected directly from 36 Informatics Engineering students and academic staff members. Each participant contributed 8 genuine signatures produced naturally by the original writer and 8 forged signatures created by other participants after visually observing and imitating the target signatures. The forgery process followed a skilled forgery protocol, where imitators were given sufficient opportunity to practice reproducing the signature shape and writing style before generating the forged samples. Consequently, the complete dataset consisted of 60 individuals with 16 signature images per subject, resulting in a total of 960 signature images. The use of combined public and locally collected datasets was intended to increase variability in signature characteristics, including writing style, stroke thickness, inclination, and geometric structure, thereby improving the robustness of the proposed verification framework.

To evaluate model performance, the dataset was divided into training and testing subsets using an 80:20 ratio with randomized stratified sampling to maintain proportional distribution between genuine and forged signatures across all subjects. During the randomization process, data splitting was carefully controlled to prevent duplication and reduce potential bias in the evaluation results. In addition, subject-independent validation was applied to minimize the risk of data leakage between training and testing stages, ensuring that signature samples used for evaluation were not directly reused during model training. This strategy was adopted to obtain a more reliable assessment of the proposed framework's generalization capability under limited-data conditions.

Figure 1. Dataset Signature

2.2. Preprocessing

Vol. 6, No. 1, June 2026, Page. 17-32
https://jiki.jurnal-id.com
DOI: https://doi.org/10.54082/jiki.350

The image preprocessing stage in a signature identification or verification system is critically important, as images obtained from scanning or photography often contain noise, variations in illumination, rotation, scale differences, and unwanted background elements. The purpose of preprocessing is to produce cleaner and more representative images so that subsequent stages, such as feature extraction and classification, can be performed more effectively and accurately. Common steps include binarization to convert images into black-and-white format, noise and artifact removal using filtering techniques, normalization of size and orientation, cropping of the signature region from the background, and adjustment of scale and position to ensure feature consistency [13].

In this study, preprocessing is conducted to standardize the quality and format of signature images prior to feature extraction and classification, particularly because the data originate from two different sources, namely a public dataset from Kaggle and primary data collection, both of which exhibit variations in lighting conditions, background, and image quality. This process aims to reduce irrelevant variations while emphasizing the essential characteristics of the signatures.

The images are read using the cv2.imread function, and if an image fails to load, the system returns a None value to prevent errors in subsequent processing stages. Color images in RGB format are then converted into grayscale using the cv2.cvtColor function. The general formula for RGB to grayscale conversion is as follows:

$$I(x, y) = 0.299R + 0.587G + 0.114B \tag{1}$$

This conversion aims to simplify image information by eliminating color components, thereby focusing the analysis solely on the intensity values of the signature pixels.

To enhance the visibility of signature strokes, contrast enhancement is performed using the Contrast Limited Adaptive Histogram Equalization (CLAHE) method. The formulation of CLAHE with a clip limit is as follows:

$$p'(r) = \min(p(r), T_{clip}) \tag{2}$$

This method enhances local contrast while preventing excessive amplification of noise. In addition, a sharpening process is applied using a kernel filter to emphasize edges and refine the details of the signature strokes.

The subsequent step involves thresholding using Otsu's method with an inverted binary scheme (THRESH_BINARY_INV). The formulation of Otsu's method is based on minimizing intra-class variance, expressed as follows:

$$\sigma_w^2(t) = \omega_0(t)\sigma_0^2(t) + \omega_1(t)\sigma_1^2(t) \tag{3}$$

This process aims to automatically separate the signature from the background based on an optimal threshold value.

After binarization, contour detection is performed using the cv2.findContours function. All detected contours are then combined to determine a bounding box that encompasses the entire signature region. The mathematical formulation of the bounding box is as follows:

$$x_{min} = \min(x_i), y_{min} = \min(y_i) \tag{4}$$

$$w = x_{max} - x_{min}, h = y_{max} - y_{min} \tag{5}$$

The identified region is then cropped by adding a certain margin to ensure that no part of the signature is truncated.

The cropped image is subsequently resized to a fixed dimension of 128 × 128 pixels while preserving the aspect ratio to avoid distortion. Padding with a value of 0 is applied when necessary to obtain a uniform square shape. To further reduce residual noise, morphological operations, specifically opening and closing with an elliptical kernel, are applied to smooth the signature structure without removing its essential characteristics. Finally, pixel values are normalized to the range [0, 1] by dividing the intensity values by 255 to ensure computational stability. The resulting preprocessed images are then utilized in the Hybrid LBP–HOG feature extraction stage prior to classification using SVM and DBN.

2.3. Feature Extraction

P-ISSN: 2807-6664
https://jiki.jurnal-id.com
E-ISSN: 2807-6591
DOI: https://doi.org/10.54082/jiki.350

Feature extraction can be understood as the process of transforming raw data into a simplified representation in the form of specific characteristics that capture the essential information. In image processing, this technique is particularly important as it helps reduce data dimensionality and improves classification accuracy by utilizing only the most significant features. Color feature extraction in images is a crucial technique for representing visual information in a more compact and informative form. Various methods, such as color histograms and feature descriptors, are employed to capture the primary characteristics of an image. These features are subsequently utilized in applications such as content-based image retrieval (CBIR) and other forms of visual analysis [14].

The feature extraction stage aims to obtain a set of representative features that effectively capture the unique characteristics of signature images. In this study, a hybrid feature extraction approach is employed, combining Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG). LBP is utilized to capture local texture information based on pixel intensity differences, while HOG is applied to extract shape and structural information through the distribution of gradient orientations. The combination of these two methods is expected to complement each other in representing both the texture and contour of signatures more comprehensively, thereby enhancing the system's ability to distinguish between genuine and forged signatures during the classification stage [15].

2.3.1 Local Binary Pattern

Local Binary Patterns (LBP) is one of the most widely used feature extraction techniques in digital image analysis, particularly for capturing local texture at the pixel level. The fundamental principle of LBP is to compare the intensity value of a central pixel with those of its neighbouring pixels, and then generate a binary code based on whether each neighbour has a higher or lower intensity than the center. The result is a local binary pattern, which is subsequently transformed into a histogram to serve as a texture feature descriptor [16]. The LBP operator has been proven to be a robust texture descriptor. The process involves labelling image pixels using a thresholding technique within a 3×3 neighbourhood, where each pixel is treated as the center value and the comparison results are converted into binary form. The resulting LBP values are then aggregated into a histogram with 256 bins, which is utilized as the texture descriptor [17].

The following are some of the fundamental LBP formulations used in this system:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} s(g_p - g_c) \cdot 2^p \tag{6}$$

Description:
g_c= intensity value of the central pixel
g_p= intensity value of the p-th neighboring pixel
P= number of neighbors (in this case, P= 8)
$s(x)$= threshold function

The threshold function is defined as:

$$s(x) = \begin{cases} 1, & \text{jika } x \geq 0 \\ 0, & \text{jika } x < 0 \end{cases} \tag{7}$$

This means:
If the neighboring pixel ≥ central pixel → value 1
If the neighboring pixel < central pixel → value 0
The resulting binary pattern is then converted into a decimal number.

After all pixels have been assigned their respective LBP values, a histogram distribution is constructed as follows:

$$H_i = \frac{n_i}{N} \tag{8}$$

Description:

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

n_i= number of occurrences of the i-th LBP pattern
N= total number of pixels
H_i= normalized histogram value

In the uniform LBP method, only binary patterns with at most two bitwise transitions (for example, 00011100) are considered dominant patterns. Other patterns are grouped into an additional bin, thereby reducing the total number of bins (in this implementation, 10 bins are used).

2.3.2 Histogram Oriented of Gradient

HOG is a feature extraction method that utilizes gradient information to describe the characteristics of objects within an image. This approach is performed by computing the distribution of gradient orientations within localized regions. The process begins by dividing the image into smaller cells, followed by calculating the gradient histogram for each cell based on changes in pixel intensity values, which indicate the presence of object edges [18].

For each pixel in the grayscale image, the gradient is computed using differential operators, commonly Sobel or Prewitt operators.

Horizontal Gradient (X-direction gradient):

$$G_x = I(x+1, y) - I(x-1, y) \tag{9}$$

Vertical Gradient (Y-direction gradient):

$$G_y = I(x, y+1) - I(x, y-1) \tag{10}$$

Description:
I (x, y): intensity value of the pixel at coordinate (x, y)
G_x, G_y: horizontal and vertical gradient components

The gradient magnitude represents the rate of intensity change. A higher value indicates a stronger edge or texture within the image.

$$M(x, y) = \sqrt{G_x^2 + G_y^2} \tag{11}$$

Description:
M (x, y): gradient magnitude at pixel (x, y)

The gradient direction represents the orientation of edges at each pixel and is mapped into specific bins for histogram construction.

$$\theta(x, y) = \arctan\left(\frac{G_y}{G_x}\right) \tag{12}$$

Description:
θ (x, y): gradient orientation at pixel (x, y) typically expressed in degrees within the range (0° – 180° or 0° – 360°)

2.4. Modeling

Before initiating the model development process, a data splitting procedure is first performed. In data processing, the dataset must be divided into training data and testing data. This technique, commonly referred to as data splitting, can be implemented using the scikit-learn library in Python. The training data is used to train the model to recognize patterns within the dataset, while the testing data is utilized to evaluate the model's performance, as it is not involved in the training process [19].

Jurnal Ilmu Komputer dan Informatika (JIKI) Vol. 6, No. 1, June 2026, Page. 17-32
P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

2.4.1 Identification Model (SVM)

SVM is a classification method that operates by determining an optimal hyperplane within a feature space to maximally separate two classes of data. This hyperplane is selected in such a way that the distance (margin) between the two classes is maximized, enabling the model to distinguish data with minimal classification error. This approach makes SVM particularly effective in handling high-dimensional data and provides strong generalization capability to unseen data when the training process is properly conducted [20]. In image processing, SVM is often combined with feature extraction techniques such as LBP and HOG to obtain more informative data representations prior to classification [21].

SVM can be applied in both linear and non-linear forms, depending on the characteristics of the data. In practice, the selection of an appropriate kernel function is crucial for obtaining optimal support vectors. Through this approach, the model identifies the best hyperplane by determining the maximum margin and optimal separation within the feature space [22].

During the SVM model training stage, the Grid Search method is employed to determine the optimal combination of parameters that yields the best performance. The parameters evaluated include the regularization parameter C, the kernel parameter γ, and the type of kernel function used, namely linear and radial basis function (RBF). This process aims to identify the most suitable parameter configuration that aligns with the characteristics of the features extracted using LBP and HOG.

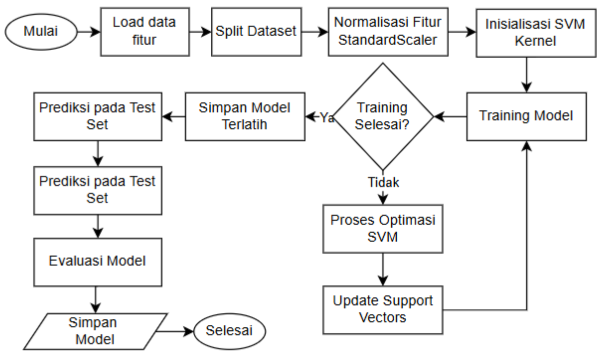

Figure 2. Flowchart of the Identification Model Development

Figure 2 illustrates that the Grid Search process evaluates 24 parameter combinations using 5-fold cross-validation, resulting in a total of 120 training iterations. The optimization process explored several SVM hyperparameters, including the regularization parameter C, kernel type, and gamma value, to determine the most suitable configuration for the dataset. The optimal parameters obtained from the Grid Search were $C = 0.1$, kernel = linear, and gamma = scale. The use of a relatively small Cvalue improves model generalization by reducing sensitivity to noise and preventing overfitting, while the linear kernel was selected because it provided the best classification performance for the extracted feature space. The 5-fold cross-validation strategy was employed to ensure a more objective evaluation and to improve the robustness of the model performance estimation.

2.4.2 Verification Model (DBN)

DBN is a deep learning architecture capable of progressively learning increasingly abstract feature representations from input data through a layer-wise training process, typically utilizing Restricted Boltzmann Machines (RBMs) as its fundamental building blocks. DBN possesses the ability to perform unsupervised pretraining and supervised fine-tuning, where the initial layers learn dominant patterns in unlabeled data, followed by the adjustment of the entire network for classification tasks using labeled data. This hierarchical structure enables DBN to capture complex patterns and non-linear relationships within images that are often beyond the capability of shallower models, thereby enhancing class discrimination in pattern recognition tasks. The application of DBN in image classification has been explored across various domains of image processing, including hyperspectral image classification, where DBN has demonstrated the ability to extract more robust features and achieve superior classification performance compared to traditional methods [23].

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

During the DBN model training stage, a deep neural architecture is employed, consisting of multiple Dense layers with a gradually decreasing number of neurons. This structure is designed to extract high-level feature representations from the feature vectors obtained through the hybrid LBP and HOG extraction process. The initial layer, which contains a larger number of neurons, functions to capture comprehensive feature information, while the subsequent layers progressively simplify the representation in a hierarchical manner.

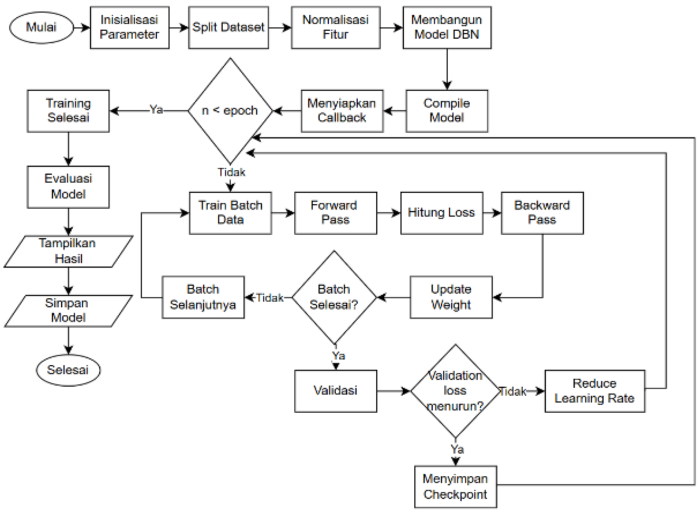

Figure 3. Flowchart of the Verification Model Development

Figure 3 illustrates the architecture of the optimized Deep Belief Network (DBN) model used in this study. The model consists of four fully connected Dense layers containing 256, 128, 64, and 32 neurons, respectively. Each Dense layer uses He Normal initialization and is followed by Batch Normalization and a ReLU activation function to improve training stability and accelerate convergence. To reduce overfitting, L2 regularization with a coefficient of 0.001 was applied to each Dense layer, while Dropout layers with rates of 0.4, 0.4, 0.3, and 0.2 were inserted after each hidden layer to randomly deactivate neurons during training. The output layer consists of a single Dense neuron with a sigmoid activation function for binary classification in both identification and signature verification tasks.

The DBN model was trained using mini-batch learning with an optimized training configuration to improve convergence and generalization performance. The use of progressively smaller hidden layers enables the model to learn hierarchical feature representations more effectively. In total, the network contains 1,086,721 trainable parameters, providing sufficient capacity to learn complex signature patterns and effectively distinguish between genuine and forged signatures while maintaining stable generalization performance.

2.5. Evaluation

Evaluation is conducted to measure the performance of the proposed system in distinguishing between genuine and forged signatures based on classification results obtained using the SVM and DBN algorithms. The evaluation process employs several performance metrics derived from the confusion matrix, including accuracy, precision, recall, F1-score, and Area Under the Curve (AUC). In addition, Receiver Operating Characteristic (ROC) curve analysis is utilized to evaluate the classification capability of the model across different decision thresholds and to assess the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR).

Accuracy measures the proportion of correct predictions out of the total number of predictions made. It can be calculated using the following equation:

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} * 100 \quad (13)$$

Precision measures the proportion of correctly predicted positive instances out of all positive predictions made by the model. It is defined as:

P-ISSN: 2807-6664
E-ISSN: 2807-6591
Vol. 6, No. 1, June 2026, Page. 17-32
https://jiki.jurnal-id.com
DOI: https://doi.org/10.54082/jiki.350

$$Precision\ = \frac{TP}{TP+FP} * 100 \tag{14}$$

Recall measures the proportion of correctly predicted positive instances out of all actual positive instances. It is calculated as:

$$Recall\ = \frac{TP}{TP+FN} * 100 \tag{15}$$

The F-measure (F1-score) represents the harmonic mean of precision and recall, and is computed using the following equation:

$$F1 = 2 \times \frac{Precission \times Recall}{Precission + Recall} \tag{16}$$

The confusion matrix is an evaluation tool that presents a summary of the model's prediction results by comparing them with the actual labels, including the number of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). It provides a detailed insight into classification performance, not only indicating how many predictions are correct but also identifying the types of errors made. Consequently, it serves as the basis for calculating other evaluation metrics such as accuracy, precision, recall, and F1-score, and is widely used in classification studies to assess model effectiveness [24].

In addition to classification performance evaluation, computational complexity analysis was also conducted to assess the feasibility of implementing the proposed framework in real-world authentication systems. The analysis includes training time, inference time, and computational cost associated with the hybrid feature extraction and deep learning classification processes. Hardware specifications used during experimentation are also reported to provide a clearer understanding of the computational resources required by the proposed method. This evaluation is important because practical authentication systems require not only high accuracy but also efficient execution and reasonable computational requirements.

To improve the robustness of the evaluation strategy, the proposed method was further analyzed using ROC curve visualization and AUC measurements to evaluate the discriminative capability of the classifier under varying thresholds. Furthermore, the performance of the proposed hybrid SVM–DBN framework was compared with baseline classification approaches to demonstrate its effectiveness relative to conventional methods. These additional evaluations provide a more comprehensive assessment of the proposed system in terms of classification performance, reliability, and deployment feasibility [25].

3. RESULT

3.1. Implementation of Local Binary Pattern (LBP)

After performing feature extraction using LBP, the results obtained are presented as follows.

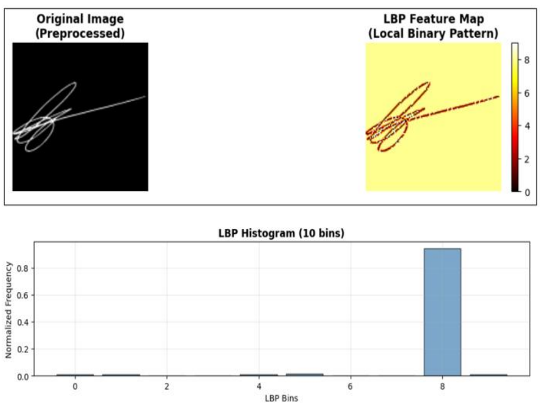

Figure 4. LBP Feature Extraction

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

Figure 4 illustrates the feature extraction process using the LBP method on signature images that have undergone preprocessing, with the aim of capturing local texture patterns from the signature strokes. This process is performed by comparing the intensity of the central pixel with its neighboring pixels and encoding the results into binary form, thereby generating an LBP feature map that represents texture characteristics such as writing style, pressure, and distinctive stroke patterns of each individual. From this feature map, an LBP histogram is computed to describe the global frequency distribution of the patterns. The histogram is then normalized and used as a numerical feature vector for the signature identification and verification process before being combined with HOG features in the subsequent hybrid feature extraction stage.

The experimental results demonstrate that the LBP method is effective in capturing fine-grained texture information from signature images, particularly in representing local stroke variations and writing pressure characteristics. These local texture patterns play an important role in distinguishing genuine signatures from forged signatures, as forged signatures often fail to reproduce subtle texture consistency and natural stroke transitions. The robustness of LBP against illumination variation and minor noise also contributes to the stability of the extracted features, enabling the system to preserve discriminative information during the classification process. Consequently, the extracted LBP features provide meaningful local descriptors that strengthen the overall representation capability of the hybrid feature extraction framework.

3.2. Implementation of Histogram of Oriented Gradient (HOG)

After performing feature extraction using HOG, the results obtained are presented as follows.

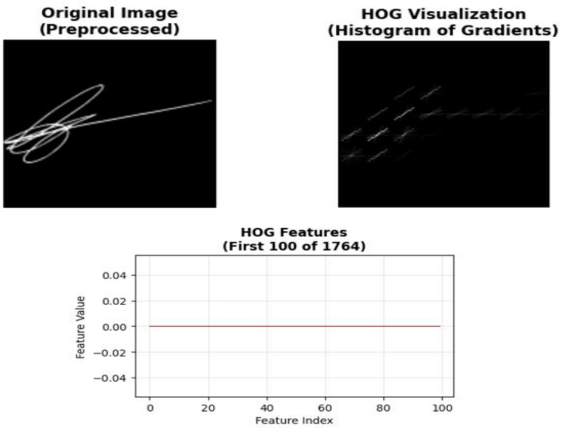

Figure 5. HOG Feature Extraction

Figure 5 illustrates the results of feature extraction using the HOG method on preprocessed signature images, with the objective of capturing shape information and stroke orientation through the distribution of pixel intensity gradients. The process involves dividing the image into several small cells, computing the gradient magnitude and orientation within each cell, and representing these values in the form of histograms that reflect the global structure and distinctive contours of the signature. The normalized gradient histograms form a numerical feature vector, as shown in the HOG visualization and feature graph. These features are subsequently used as input for the classification stage in signature identification and verification and are combined with LBP features within a hybrid scheme, resulting in a feature shape of (480, 1777), with a total of 1,777 features per image.

The HOG method contributes significantly to capturing global structural characteristics of signatures, including stroke direction, curvature, and contour distribution. Unlike LBP, which focuses on local texture information, HOG emphasizes spatial and geometric properties that are highly relevant for distinguishing signature shapes between individuals. The combination of gradient orientation information and local normalization improves robustness against small variations in writing position and scale. The resulting feature representation enables the model to identify structural inconsistencies commonly found in forged signatures, particularly in stroke alignment and writing dynamics. Therefore, the integration of HOG with LBP creates a complementary hybrid feature representation that combines

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

both local texture characteristics and global structural information, leading to improved discriminative performance.

3.3. Implementation of the Identification Model (SVM)

The features extracted using LBP and HOG are then classified using the SVM algorithm, yielding the following results.

Table 1. Evaluation Results of the Identification Model

Category	Parameter	Score
Model Accuracy	Training Accuracy	1.00
	Test Accuracy	0.89
	Gap (Overfitting)	0,10
Testing Metrics	Precision	0.92
	Recall	0.89
	F1-Score	0.89

The model achieved a training accuracy of 100% and a testing accuracy of 89.58%, indicating excellent learning capability with relatively strong generalization performance despite the presence of mild overfitting of approximately 10.42%. The high training accuracy demonstrates that the hybrid LBP–HOG features contain sufficiently discriminative information for separating signature classes. Meanwhile, the testing accuracy indicates that the model is capable of maintaining stable performance on unseen data, suggesting that the extracted features successfully preserve both texture and structural characteristics of the signatures.

The obtained Precision value of 91.67% indicates that the model produces a relatively low false positive rate, meaning that most predicted signatures are correctly classified. In addition, the Recall value of 89.58% demonstrates that the model can successfully recognize the majority of genuine signatures within the testing data. The balanced F1-Score of 88.75% further confirms that the model achieves stable performance between prediction accuracy and completeness. These results suggest that the hybrid feature extraction framework significantly contributes to improving classification quality by combining complementary information from LBP and HOG descriptors.

The relatively small performance gap between training and testing results indicates that the selected SVM hyperparameters successfully control model complexity and improve generalization capability. The use of a linear kernel with an optimized regularization parameter enables the classifier to construct effective decision boundaries within the extracted feature space while avoiding excessive sensitivity to noise. Nevertheless, several misclassifications still occur due to the high similarity between genuine and skilled forged signatures, especially when forged signatures successfully imitate the global structure and writing style of the original signatures. This finding indicates that signature verification remains a challenging classification problem because of substantial intra-class variability and inter-class similarity.

3.4. Implementation of the Verification Model (DBN)

The features extracted using the hybrid LBP and HOG methods were subsequently classified using the DBN algorithm, yielding the following results.

Table 2. Evaluation Results of the Verification Model

Metrics	Score
Accuracy	0.87
Loss	1.0
Precision	0. 91
Recall	0. 81
F1-Score	0. 86
AUC	0.85
Total Test Data	192

P-ISSN: 2807-6664 https://jiki.jurnal-id.com
E-ISSN: 2807-6591 DOI: https://doi.org/10.54082/jiki.350

Based on testing conducted on 192 test samples, the verification model achieved an accuracy of 0.87, with a precision of 0.91, recall of 0.81, F1-score of 0.86, and an AUC of 0.85. These results indicate that the DBN model possesses strong discriminative capability in distinguishing genuine signatures from forged signatures. The high Precision value demonstrates that the model produces relatively few false positive predictions, which is particularly important in authentication systems because incorrectly accepting forged signatures can lead to security risks.

The Recall value of 0.81 indicates that the model is capable of correctly identifying most genuine signatures, although several genuine samples are still misclassified as forgeries. This condition may occur because natural variations in handwriting, writing pressure, stroke thickness, and signing speed can produce significant differences even among genuine signatures from the same individual. Consequently, some genuine signatures may exhibit characteristics that overlap with forged samples, making the classification task more difficult.

The AUC value of 0.85 further confirms that the model has good capability in separating positive and negative classes across multiple decision thresholds. This result demonstrates that the proposed hybrid feature extraction combined with DBN classification can effectively learn complex nonlinear relationships within signature patterns. The layered architecture of the DBN enables the model to capture hierarchical representations from the extracted features, allowing deeper analysis of subtle differences between genuine and forged signatures.

Although the model achieved good overall performance, the loss value of 1.0 indicates that prediction errors still occur during classification. This result suggests that several feature patterns remain difficult to separate perfectly, especially in cases involving skilled forgery attempts. However, the use of Batch Normalization, Dropout, and L2 regularization contributes significantly to improving training stability and reducing overfitting, enabling the DBN model to maintain relatively consistent performance on unseen data.

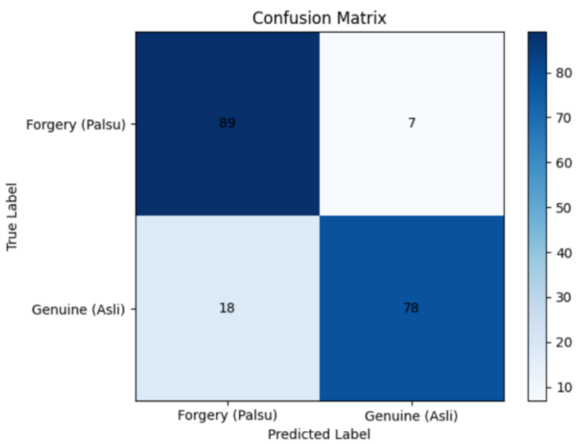

Figure 6. Confusion Matrix of the Verification Model

Figure 6 shows that the model correctly classified 89 forged signature samples while misclassifying 7 samples. For genuine signatures, the model correctly identified 78 samples but incorrectly classified 18 samples as forgeries. Overall, the model demonstrates reasonably strong verification capability because the number of correct predictions substantially exceeds the number of errors. However, the higher number of false negative cases indicates that the model still encounters difficulties in distinguishing several genuine signatures from forged signatures. This condition is primarily influenced by intra-writer variability, where signatures produced by the same individual may naturally vary in stroke thickness, writing pressure, slant angle, writing speed, and character spacing. These variations can alter the extracted texture and structural features, causing some genuine signatures to appear visually different from other samples belonging to the same writer.

In addition, overlapping feature distributions between genuine and forged signatures also contribute to the misclassification problem. Skilled forged signatures often imitate the global structure and stroke orientation of genuine signatures with high similarity, making the extracted LBP and HOG features partially overlap within the feature space and reducing the clarity of the classification boundary.

Vol. 6, No. 1, June 2026, Page. 17-32
P-ISSN: 2807-6664
https://jiki.jurnal-id.com
E-ISSN: 2807-6591
DOI: https://doi.org/10.54082/jiki.350

Several errors may also be influenced by preprocessing limitations and insufficient dataset diversity, which can reduce the model's generalization capability when encountering complex handwriting variations. Nevertheless, the model tends to behave conservatively by classifying uncertain signatures as forgeries rather than accepting them as genuine signatures, which is preferable in authentication systems because rejecting suspicious signatures is generally less risky than incorrectly accepting forged signatures.

3.5. Comparative Analysis of Classification Algorithms

To further validate the effectiveness of the proposed framework, comparative evaluation was conducted using several classification algorithms. The results are presented in Table 3.

Table 3. Comparative Evaluation

Classifier	Accuracy	Precision	Recall	F1-Score	AUC
KNN	0.79	0.82	0.77	0.79	0.76
Random Forest	0.83	0.86	0.81	0.83	0.81
ANN	0.84	0.88	0.80	0.84	0.82
SVM	0.89	0.92	0.89	0.89	0.87
DBN	0.87	0.91	0.81	0.86	0.85

Based on Table 3, the SVM and DBN models achieved superior performance compared to conventional machine learning and shallow neural network approaches. The SVM classifier produced the highest identification accuracy because it effectively constructs optimal decision boundaries within the extracted hybrid feature space. In addition, SVM demonstrates strong robustness in handling high-dimensional feature vectors generated from the hybrid LBP–HOG descriptors.

The DBN model also demonstrated strong performance due to its deep layered architecture, which enables hierarchical learning of complex nonlinear relationships among signature features. Compared with ANN, the DBN architecture provides deeper feature representation learning capability, allowing the model to capture subtle differences between genuine and forged signatures more effectively.

In contrast, KNN and Random Forest produced lower performance because these models are relatively less effective in handling highly complex feature distributions and subtle intra-class variations within signature datasets. KNN is sensitive to local neighbourhood distribution and noisy samples, while Random Forest may experience limitations in learning highly detailed nonlinear feature relationships. Overall, the comparative analysis confirms that the proposed hybrid feature extraction combined with SVM and DBN classification provides the most stable and discriminative performance for signature identification and verification tasks.

4. DISCUSSIONS

The experimental results demonstrate that the combination of Local Binary Pattern (LBP) and Histogram of Oriented Gradient (HOG) features provides a complementary and highly discriminative representation of signature characteristics. LBP effectively captures local texture information such as stroke pressure, micro-patterns, and writing style consistency, while HOG emphasizes global structural properties including stroke orientation, contour distribution, and writing direction. Comparative experiments showed that the hybrid LBP–HOG method achieved higher accuracy (0.89) than LBP-only (0.81) and HOG-only (0.84) approaches, confirming that the integration of local texture and global structural information improves the separability between genuine and forged signatures. These findings indicate that handcrafted hybrid feature extraction remains highly effective for biometric authentication tasks involving limited and complex datasets.

The SVM identification model achieved a training accuracy of 1.00 and testing accuracy of 0.89, outperforming several conventional classifiers such as KNN (0.79), Random Forest (0.83), and ANN (0.84). Meanwhile, the DBN verification model achieved an accuracy of 0.87, precision of 0.91, F1-score of 0.86, and AUC of 0.85, demonstrating competitive performance compared to similar offline signature verification studies reported in recent literature. The strong performance of SVM is influenced by its ability to construct optimal decision boundaries within high-dimensional hybrid feature spaces, while the DBN architecture enables hierarchical learning of complex nonlinear feature representations.

Vol. 6, No. 1, June 2026, Page. 17-32
P-ISSN: 2807-6664
https://jiki.jurnal-id.com
E-ISSN: 2807-6591
DOI: https://doi.org/10.54082/jiki.350

Nevertheless, the lower recall value indicates that several genuine signatures were still misclassified as forgeries due to intra-writer variability, overlapping feature distributions, and similarities between genuine and skilled forged signatures.

The findings of this study also provide important implications for current research trends in biometric authentication and machine learning. Although end-to-end Convolutional Neural Network (CNN) approaches have become increasingly popular, the results demonstrate that hybrid handcrafted feature extraction combined with deep learning classifiers can still achieve competitive performance, particularly in scenarios with limited datasets and constrained computational resources. Compared to CNN-based methods that generally require large-scale datasets and high computational cost, the proposed LBP–HOG with SVM and DBN framework offers a more efficient and interpretable approach while maintaining strong classification capability. Furthermore, the confusion matrix analysis revealed that the model tends to classify uncertain signatures as forgeries rather than accepting them as genuine signatures, which is preferable in authentication systems because rejecting suspicious signatures generally presents lower security risk than falsely accepting forged signatures.

5. CONCLUSION

This study proposed an offline signature identification and verification framework based on hybrid Local Binary Pattern (LBP) and Histogram of Oriented Gradient (HOG) feature extraction combined with Support Vector Machine (SVM) and Deep Belief Network (DBN) classification models. The experimental results demonstrate that the integration of LBP and HOG features provides complementary local texture and global structural information, enabling the system to achieve strong discriminative capability in distinguishing genuine and forged signatures. The proposed framework achieved an identification accuracy of 89% using SVM and a verification accuracy of 87% using DBN, indicating that hybrid handcrafted feature extraction combined with deep learning classification remains competitive for biometric authentication tasks, particularly in environments with limited datasets and computational resources.

Nevertheless, several limitations remain within the proposed framework. Misclassification errors still occurred due to intra-writer variability, overlapping feature distributions, and similarities between genuine and skilled forged signatures. In addition, the evaluation was conducted on a limited dataset and has not yet included broader cross-dataset validation or real-world deployment testing. Therefore, future research should focus on increasing dataset diversity, improving preprocessing robustness, optimizing deep learning architectures, and conducting broader comparative evaluations to further improve generalization capability and verification reliability in practical biometric authentication systems.

REFERENCES

[1] Deepali Narwade and Vaishali Kolhe, “A Survey: Deep Learning Approaches for Signature Verification,” *Int. J. Sci. Res. Sci. Eng. Technol.*, pp. 291–312, Aug. 2023, doi: 10.32628/ijsrset23103216.
[2] S. D. Bhavani and R. K. Bharathi, “A multi-dimensional review on handwritten signature verification: strengths and gaps,” *Multimed. Tools Appl.*, vol. 83, no. 1, pp. 2853–2894, Jan. 2024, doi: 10.1007/s11042-023-15357-2.
[3] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks,” May 2017. doi: 10.1016/j.patcog.2017.05.012.
[4] D. singh, A. Mittal, N. Aggarwal, and R. Kumar, “Offline Signature verification : A Systematic Review,” Jun. 09, 2022. doi: 10.21203/rs.3.rs-1723015/v1.
[5] S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Llados, and U. Pal, “SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification,” *Pattern Recognit. Lett.*, pp. 1–7, Sep. 2017, [Online]. Available: http://arxiv.org/abs/1707.02131
[6] J. Bromlane, J. W. Bentz, and L. Bottou, “Signature Verification using a Siamese Time Delay Neural Network,” *Intern. J. Pattern Recognit. Artif. Intell.*, vol. 07, no. 04, pp. 669–688, 1993.
[7] A. Dosovitskiy *et al.*, “An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale,” *ICLR*, pp. 1–22, Jun. 2021, [Online]. Available: http://arxiv.org/abs/2010.11929

[8] M. Hanmandlu, A. B. Sronothara, and S. Vasikarla, "Deep Learning based Offline Signature Verification," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2018, pp. 732–737. doi: 10.1109/UEMCON.2018.8796678.

[9] R. R. Upadhyay and K. K. Singh, "Handwritten signature verification system using hybrid transfer learning approach," *Evolving Systems*, vol. 15, no. 6, pp. 2313–2322, 2024, doi: 10.1007/s12530-024-09617-1.

[10] M. L. Shuwandy *et al.*, "A Robust Behavioral Biometrics Framework for Smartphone Authentication via Hybrid Machine Learning and TOPSIS," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Jun. 2025, doi: 10.3390/jcp5020020.

[11] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Off-line signature verification based on grey level information using texture features," *Pattern Recognit.*, vol. 44, no. 2, pp. 375–385, 2011, doi: https://doi.org/10.1016/j.patcog.2010.07.028.

[12] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A Fast Learning Algorithm for Deep Belief Nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, Jul. 2006, doi: 10.1162/neco.2006.18.7.1527.

[13] U. Yu. Akhundjanov and V. V. Starovoitov, "Pre-processing of handwritten signature images for following recognition," *Analisis Sistem dan Informatika Terapkan*, vol. 2, pp. 4–9, Jun. 2022, doi: 10.21122/2309-4923-2022-2-4-9.

[14] S. Ashillah, S. A. Gulo, Y. Rahmi, D. Yandra Niska, and S. Adventino Gulo, "Implementasi Algoritma Pengolahan Citra Digital untuk Perbaikan Kualitas Gambar," *Jurnal Sistem Komputer dan Kecerdasan Buatan*, vol. 8, no. 3, pp. 274–280, 2025.

[15] Y. Zhou, J. Zheng, H. Hu, and Y. Wang, "Handwritten signature verification method based on improved combined features," *Applied Sciences (Switzerland)*, vol. 11, no. 13, Jul. 2021, doi: 10.3390/app11135867.

[16] M. T. Kanugroho, M. A. Rahman, and R. C. Wihandika, "Klasifikasi Batik dengan Ekstraksi Fitur Tekstur Local Binary Pattern dan Metode K-Nearest Neighbor," 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[17] R. A. Sutiani, N. Made, S. Ulandari, and R. A. Saputra, "Klasifikasi Kesegaran Ikan Menggunakan Citra Mata dengan Convolutional Neural Network Arsitektur VGG-16," *Jointer-Journal of Informatics Engineering*, vol. 05, no. 02, pp. 30–35, 2024.

[18] S. Ibrahim and N. A. N. Samlan, "Histogram of oriented gradient (HOG) for off-line handwritten signature authentication," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 1 1.1 Special Issue, pp. 102–107, 2020, doi: 10.30534/ijeter/2020/1681.12020.

[19] K. G. Ramadhan *et al.*, "Komparasi Deteksi Penyakit Ginjal Kronis Menggunakan Algoritma Support Vector Machine dan Random Forest," *Jurnal Informatika & Rekayasa Elektronika)*, vol. 8, no. 1, pp. 13–22, 2025, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[20] G. Isnansyah and R. Adi Saputra, "Analisis Perbandingan Algoritma Klasifikasi Email Spam Menggunakan Long Short-Term Memory, Naïve Bayes Dan Support Vector Machine," *ANIMATOR*, vol. 2, no. 1, pp. 1–8, 2024.

[21] E. F. Laili, Z. Alawi, R. Rohmah, and A. Barata, "Komparasi Algoritma Decision Tree dan Support Vector Machine (SVM) dalam Klasifikasi Serangan Jantung," *Jurnal Sistem Informasi dan Informatika (Simika)*, vol. 8, no. 1, pp. 67–76, 2025, [Online]. Available: https://www.kaggle.com/datasets/thxogg/heart-

[22] A. Setiawan, R. Febrio Waleska, M. Adji Purnama, and L. Efrizoni, "Komparasi Algoritma K-Nearest Neighbor (Knn), Support Vector Machine (SVM), Dan Decision Tree Dalam Klasifikasi Penyakit Stroke," *Jurnal Informatika & Rekayasa Elektronika)*, vol. 7, no. 1, pp. 107–115, 2024, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[23] C. Li, Y. Wang, X. Zhang, H. Gao, Y. Yang, and J. Wang, "Deep belief network for spectral–spatial classification of hyperspectral remote sensor data," *Sensors (Switzerland)*, vol. 19, no. 1, pp. 1–13, Jan. 2019, doi: 10.3390/s19010204.

[24] S. Kurnia, A. Khaidar, and P. Studi Magister, "Perbandingan Metode Machine Learning Menggunakan Metode Support Vector Machine dan Artificial Neural Network Dalam

Memprediksi Serangan Jantung," *Jurnal Informatika Kaputama (JIK)*, vol. 9, no. 2, pp. 87–94, 2025.

[25] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Inf. Process. Manag.*, vol. 45, no. 4, pp. 427–437, 2009, doi: https://doi.org/10.1016/j.ipm.2009.03.002.