OPEN ACCESS
The The Journal of Engineering and Exact Sciences – jCEC, Vol. 10 N. 08 (2024)
journal homepage: https://periodicos.ufv.br/jcec
eISSN: 2527-1075
ISSN: 2446-9416

A Novel Technique for Handwritten Signature Recognition

Article Info:
Article history: Received 2024-09-09 / Accepted 2024-12-12 / Available online 2024-12-12
doi: 10.18540/jcecvl10iss8pp20810

Leila Boucerredj
ORCID: https://orcid.org/0000-0002-8481-7725
Department of Electronics and Automatics, Faculty of Science and Technology, PIMIS, Laboratory, University of 8 Mai 1945, PO Box 401, GUELMA 24000, Algeria
E-mail: l_boucerredj@yahoo.fr
Karima Kechroud
ORCID: https://orcid.org/0000-0003-4833-9022
Department of Electronics and Automatics, Faculty of Science and Technology, PIMIS, Laboratory, University of 8 Mai 1945, PO Box 401, GUELMA 24000, Algeria
E-mail: kechroud21.2001@gmail.com
Bouaziz Noureddine
ORCID: https://orcid.org/0000-0002-2376-1916
Department of Electronics and Automatics, Faculty of Science and Technology, PIMIS, Laboratory, University of 8 Mai 1945, PO Box 401, GUELMA 24000, Algeria
E-mail: noureddine061@gmail.com
Abderrahmane Khechekhouche
ORCID: https://orcid.org/0000-0002-7278-2625
Laboratory (LNTDL), Faculty of Technology, University of El Oued, Algeria
E-mail: khechekhouche-abderrahmane@univ-eloued.dz

Abstract
Handwritten signature recognition (HSR) is a critical component of biometric systems, widely used for securing financial transactions and identity verification. However, the variability of handwritten signatures, influenced by individual writing styles, inconsistencies, and environmental factors, presents significant challenges for recognition systems. Despite these obstacles, signatures remain a reliable and popular biometric trait. This paper introduces a novel deep learning approach utilizing a convolutional neural network (CNN) architecture specifically designed for HSR. The proposed method was validated using two prominent datasets, MCYT-75 and GPDS-300, with detailed descriptions of the CNN structure. Experiments, conducted on a personal computer equipped with an NVIDIA Quadro M1200 GPU, an Intel i7 processor, and 32 GB of RAM, demonstrated the model's exceptional performance, achieving validation accuracies of 99.60% on the MCYT-75 dataset and 99.80% on the GPDS-300 dataset. These results reflect the model's robustness and minimized error rates, outperforming existing techniques and underscoring the effectiveness of deep learning for signature recognition. This study highlights the proposed model's potential for real-world applications and paves the way for further advancements in biometric authentication technologies.

Keywords: Biometric Recognition, Deep Learning (DL), Handwritten Signatures, CNN, MCYT-75 and GPDS-300 database.

1. Introduction

In today's increasingly digital world, where secure identity verification underpins trust and safety, biometric identification has become a cornerstone of modern authentication systems. By leveraging unique physiological or behavioral characteristics, biometrics ensures precise and reliable identification. Among the numerous biometric modalities such as fingerprints, facial recognition, iris patterns, and voice recognition (Albasu *et al.*, 2023; Hezil *et al.*, 2018; Jain *et al.*, 2020), handwritten signatures hold a distinctive position. They represent a unique blend of physiological traits, seen in the individualistic formation of letters and symbols, and behavioral patterns, linked to the act of signing itself (Ferrer *et al.*, 2012; Bhunia *et al.*, 2019).

One of the most complex applications of biometrics in identity verification is signature verification (Diaz *et al.*, 2017; Impedovo et al., 2008). This specialized domain focuses on analyzing signatures to authenticate individuals, playing a vital role in fraud prevention and the verification of critical documents. Signature verification is widely adopted in financial institutions, legal frameworks, and other sectors requiring robust identity confirmation mechanisms (Sharif *et al.*, 2019; Ghosh, 2020; Sadak *et al.*, 2022). The importance of this process cannot be overstated, as it underpins trust and reliability across transactions, agreements, and secure systems.

Handwritten signatures are generally classified into two categories: dynamic (online) and static (offline). Dynamic signature verification captures real-time signing data, analyzing parameters such as speed, pressure, and rhythm to extract behavioral features (Khalil *et al.*, 2009). In contrast, offline signature verification relies on static images of signatures, typically scanned from physical documents, and evaluates their visual characteristics. Effective offline verification requires a well-curated dataset of genuine signatures, which is tested against forgeries to assess the system's accuracy and robustness (Alaei *et al.*, 2017).

A significant body of research has focused on enhancing the accuracy and reliability of offline signature verification using advanced methodologies. For example, one study employed rotation-invariant Local Binary Patterns (LBP) with 8 and 16 neighborhoods, combined with Gray Level Co-occurrence Matrices (GLCM), to distinguish genuine signatures from forgeries (Vargas *et al.*, 2011). By incorporating background removal techniques and a histogram displacement method to mitigate the effects of varying writing instruments, the researchers achieved impressive results. Their approach was tested on the MCYT database and the GPDS-100Gray signature database (Ortega-Garcia *et al.*, 2003; Vargas *et al.*, 2007), yielding Equal Error Rates (EERs) of 12.06% and 9.02% for 5-sample and 10-sample training sets, respectively, when using a Least Squares Support Vector Machine (LS-SVM) classifier (Suykens *et al.*, 2002; Abdoli *et al.*, 2014).

Building on advancements in offline signature verification, (Bharadi *et al.*, 2010) introduced a method utilizing the Walsh transform applied to horizontal and vertical pixel distributions. Their approach achieved a False Acceptance Rate (FAR) of 2.5%, an Equal Error Rate (EER) of 3.29%, and a commendable accuracy of 95.08%. Similarly, (Dubey *et al.*, 2012) employed Support Vector Machine (SVM) methods, achieving a classification rate of 95%. Their technique involved extracting global, directional, and grid features, amounting to 77 distinctive characteristics, and utilizing a one-against-all classification strategy to address the multiclass nature of the signature recognition problem.

Another notable methodology focuses on systems leveraging Hidden Markov Models (HMMs), which have been applied to datasets containing up to 4,000 signatures (Odeh *et al.*, 2011). Enhancements to these models, such as integrating pixel distribution features, have further improved their performance (Shah *et al.*, 2016). Additional studies have explored the potential of HMM-based techniques to strengthen offline signature verification (Benhur, 2021; Kingma *et al.*, 2017).

Dynamic Time Warping (DTW) has emerged as a powerful contender in both online and offline signature verification. In online applications, DTW often surpasses HMM-based methods, utilizing template-matching techniques to great effect (Sanghvirajit, 2021). An enhanced DTW model was proposed by (Kang, 2019), incorporating personalized parameters for individual signers and features such as quantized directions, curvature changes, speed, and pressure. Tested on the SUSIG database, which includes skilled forgeries, this model achieved an area under the Receiver Operating Characteristic (ROC) curve of 99.5% and an EER of 3.48%.

Additional research highlights the use of SVM models for offline signature verification. (Bindal, 2019) compared SVM performance with Multi-Layer Perceptrons (MLP), demonstrating the potential of machine learning techniques in this domain. Another innovative approach converts signature images into time series data through linear scanning, using time series shapelets for feature extraction and the Mahalanobis distance for comparison (Bertolini *et al.*, 2010). This technique was evaluated on a dataset of 1,287 questioned signatures and 646 reference signatures, yielding an EER of 5.8%. Moreover, a system employing an interval symbolic representation and a fuzzy similarity measure was tested on a substantial dataset of 16,200 offline signature images, showing its scalability and effectiveness (Vinushanth, 2020; Manohar, 2017).

Handwritten signature recognition (HSR) plays a crucial role in biometric systems for securing financial transactions and identity verification, yet it remains challenging due to the variability in writing styles, inconsistencies, and environmental factors. This research introduces a novel deep learning (DL) technique based on a convolutional neural network (CNN) architecture specifically designed for offline HSR. By leveraging publicly available datasets, the proposed method demonstrates significant advancements in accuracy and reliability. The approach addresses key challenges in HSR, highlighting its importance and novelty while showcasing its potential for real-world biometric authentication applications.

2. Methodologies

2.1. Deep Learning, Machine Learning, and Artificial Intelligence

Artificial Intelligence (AI) (Wang *et al.*, 2023; Kurani *et al.*, 2023), Machine Learning (ML) (Haug *et al.*, 2023; Yu *et al.*, 2023), and Deep Learning (DL) (Menghani, 2023; Aslani *et al.*, 2023; Liu *et al.*, 2023) are interrelated fields that play pivotal roles in advancing handwritten signature recognition systems. AI serves as the overarching domain focused on designing systems capable of performing tasks that traditionally require human intelligence, such as pattern recognition and decision-making. Within AI, ML represents a subset (illustrated in Figure 1) dedicated to enabling algorithms to learn from data and improve their performance over time without explicit programming. DL, a further subset of ML, employs artificial neural networks with multiple layers to analyze large-scale data, unlocking sophisticated pattern recognition capabilities.

In the context of handwritten signature recognition, these technologies function synergistically. AI provides the foundational framework for designing recognition systems, ML enables adaptive learning and performance optimization from diverse signature samples, and DL excels in capturing intricate and nuanced features of signatures. This combination enhances the system's accuracy and reliability in distinguishing authentic signatures from forgeries, addressing challenges in modern identity verification. Thus, the relationship among these three concepts is hierarchical: AI encompasses ML, which in turn encompasses DL, each representing a more specialized approach to achieving intelligent behavior in machines.

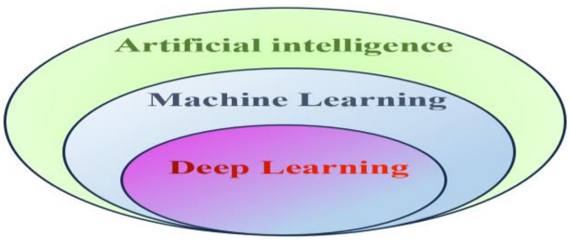

Figure 1 - Relationship between AI, ML, and DL

2.2.Convolution Neural Network (CNN) for handwritten signatures recognition

A Convolutional Neural Network (CNN) is a specialized deep learning architecture designed for a Convolutional Neural Network (CNN) (Akinci *et al.*, 2023; Taşpinar *et al.*, 2023; Cong *et al.*, 2023; Kshatri *et al.*, 2023) is a specialized deep learning architecture designed for processing grid-structured data, such as images. Feature extraction in CNNs (depicted in Figure 2) involves identifying and selecting critical patterns or attributes from input data, such as signature images. CNNs perform this automatically through a series of layers, including convolution, pooling, and activation functions, which transform raw input data into structured representations highlighting relevant characteristics.

Following feature extraction, the classification process (also shown in Figure 2) categorizes the input into predefined classes or labels. In CNN architectures, fully connected layers often succeed the feature extraction layers, interpreting the learned patterns and assigning probabilities to each class. This process ensures accurate categorization based on extracted features. Many CNN architectures follow the standard pattern described by Equation 1 (Sharif *et al.*, 2019), which outlines the relationship between layers and their functionality.

In this framework (equation 1), IN refers to the input layer, CONV signifies the convolution layer, POOL stands for the pooling layer, FC represents the fully connected layer, and OUT indicates the output layer. The variables M and N are integers; the symbol "*" denotes a repetition of elements, while "?" indicates that something is optional.

$$\mathrm{IN} \Rightarrow [\mathrm{CONV} \Rightarrow \mathrm{POOL?}] * \mathrm{M} \Rightarrow [\mathrm{FC}] * \mathrm{N} \Rightarrow \mathrm{OUT} \tag{1}$$

Figure 2 shows CNN architecture for signature recognition. In the realm of signature recognition, feature extraction, and classification work together to effectively identify individuals based on their unique signatures. CNNs automate the extraction of distinctive features from signature images, such as strokes, curves, and angles, which are crucial to differentiating one signature from another. After these features are extracted, the classification phase categorizes the signatures into defined classes, determining whether a signature is genuine or forged. This combination of automated feature extraction and robust classification makes CNNs highly effective in verifying signatures with high accuracy and reliability.

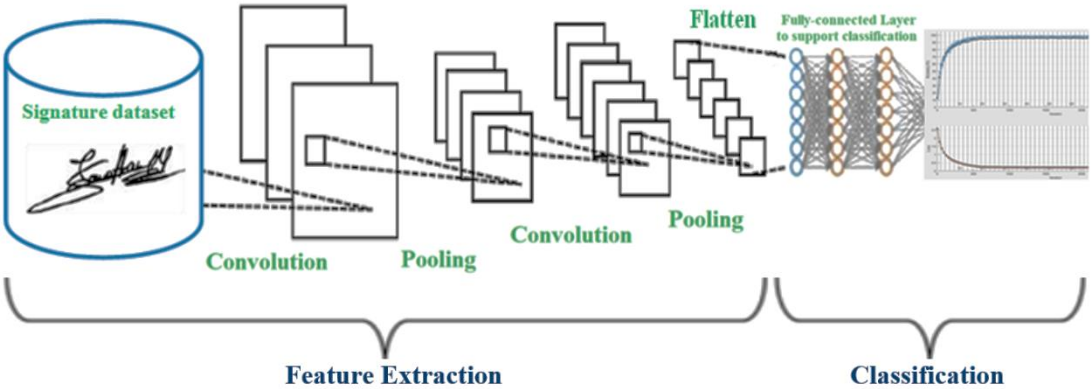

Figure 2 - CNN architecture for signature recognition

The Core Components of CNN for handwritten signatures recognition are:

- Input Layer: The input layer receives the images of handwritten signatures, typically formatted in a consistent resolution suitable for further processing.
- Convolution Layers: These layers apply convolution filters to input images to extract spatial hierarchies of features. Each filter moves across the image and generates feature maps that capture essential patterns, such as edges and textures, which are crucial in distinguishing between different signatures.

- Activation Function: Typically, Rectified Linear Unit (ReLU) (see equation 2) is used after convolutional layers to introduce non-linearity into the model. This allows the CNN to learn complex patterns in the data.

$$\mathrm{ReLU}(x_i) = \max(0, x_i) \tag{2}$$

- Pooling Layers: These layers decrease the spatial dimensions of the feature maps (usually max pooling). Pooling helps in making the representation smaller and more manageable, reduces computation time, and also provides some degree of translation invariance.
- Fully Connected Layers (see equation 3): After multiple convolution and pooling layers, fully connected layers are used to make the final classification. These layers connect every neuron from the previous layer to every neuron in the current layer to learn global features of the signature.

$$x_l = W_l * h_{l-1} \tag{3}$$

- Output Layer: The output layer typically uses a softmax activation function (see equation 4) for multi-class classification, producing probabilities for each class (signature) based on the features extracted from the images. This enables model predictions regarding whether a given signature is genuine or forged.

$$\mathrm{softmax}(x_i) = \frac{e^{x_i}}{\sum_j e^{x_j}} \tag{4}$$

CNNs offer several advantages for the recognition of handwritten signatures:

- Automatic Feature Extraction: CNNs can automatically learn hierarchical features from the input images (signatures) without the need for manual feature extraction. This is particularly useful for capturing the nuances of different handwriting styles.
- Translation Invariance: CNNs are designed to be invariant to translation, which means they can recognize signatures regardless of their position within the input image. This is critical in signature verification where the exact placement can vary.
- Robustness to Distortions: Handwritten signatures may vary due to human writing style, pressure, and speed or different writing instruments. CNNs can effectively generalize and remain robust against these variations by capturing essential patterns in the data.
- Spatial Hierarchy: CNNs effectively capture spatial hierarchies in images by employing multiple layers of convolutions and pooling, allowing them to learn hierarchical representations from edges to complex shapes in signatures.
- Reduced overfitting: Through techniques like pooling and dropout, CNNs can reduce the risk of overfitting, making them more reliable when working with limited datasets.
- 4. Reduced Computational Cost: Through the utilization of weight sharing and local receptive fields, CNNs require fewer parameters than traditional fully connected networks, resulting in lower computational costs and faster training times.
- High Accuracy: Due to their ability to learn complex patterns in the data, CNNs commonly achieve high accuracy.

2.3. Performance evaluation criteria

The evaluation criteria for signature recognition encompass metrics such as validation accuracy, which is derived from true and false positive/negative counts. Alongside accuracy measures for training and validation sets, loss metrics track model performance, while the Equal Error Rate (EER) serves as an indicator of balance between false acceptance and rejection in the system, the system will function better if the error values are lower. These criteria represent essential components for assessing the efficacy of signature recognition models.

- *Validation Accuracy*

A confusion matrix is a performance evaluation tool used in classification problems, including those involving CNNs. It is a two-dimensional matrix (see Figure 3) that summarizes the performance of a classification model by comparing the actual labels with the predicted labels of a dataset.

$$\begin{array}{ll} & \begin{array}{cc} \mathit{Classifier} & \mathit{decision} \\ + & - \end{array} \\ \begin{array}{l} \mathit{label}\ + \\ \mathit{class}\ - \end{array} & \begin{pmatrix} \mathit{TruePositive}(TP) & \mathit{FalseNegative}(FN) \\ \mathit{FalsePositive}(FP) & \mathit{TrueNegative}(TN) \end{pmatrix} \end{array}$$

Figure 3 - Confusion Matrix 2*2

The validation accuracy (equation 5) of a signature recognition model can be defined as:

$$\text{Validation Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \qquad (5)$$

Where:
- TPs are the correctly identified signatures,
- TNs are the correctly rejected non-signatures,
- FPs are the incorrectly accepted non-signatures, and
- FNs are the incorrectly rejected signatures.

- *Equal Error Rate*

The EER is a common performance metric used in biometric systems, defined as the point where the false acceptance rate (FAR) equals the false rejection rate (FRR). The EER can be expressed mathematically as (equation 6):

$$\text{EER} = \text{FAR} = \text{FRR} \qquad (6)$$

Where:
FRR refers to the percentage of legitimate signatures that the system incorrectly identifies as fraudulent (see equation 7).

$$\text{FRR} = \frac{\text{FN}}{\text{TP+FN}} \qquad (7)$$

FAR It gives the percentage of forged signatures that the system accepts as genuine (see equation 8).

$$\text{FAR} = \frac{\text{FP}}{\text{FP+TN}} \qquad (8)$$

2.4. Overview of Datasets

This novel technique aims to create a resilient DL model utilizing CNNs for the HSRs, leveraging two established benchmark datasets: GPDS-300 and MCYT-75 to assess the efficiency of our novel technique.

2.4.1. GPDS-300 Dataset

The GPDS-300 signatures database (see Figure 4) is a specialized dataset designed for research and development in the field of handwriting recognition and signature verification. It comprises 300 genuine and forged handwritten signatures from various individuals (Ferrer *et al.*, 2005; Vargas *et al.*, 2007). Each signature was captured under controlled conditions to ensure quality across multiple samples. This database serves as a benchmark for testing algorithms and systems aimed at distinguishing between authentic and forged signatures, facilitating advancements in biometrics, security, and document verification technologies.

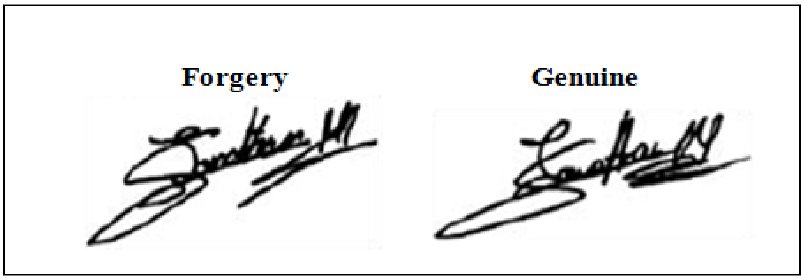

Figure 4 - Example of GPDS-300 signature database

2.4.2. MCYT-75 Dataset

The MCYT-75 database (see Figure 5) is a comprehensive dataset used primarily for the research and development of handwriting recognition and verification systems (Ortega-Garcia *et al.*, 2003). It contains 75 different handwriting samples collected from different writers each class contains 15 genuine signatures and 15 forgeries.

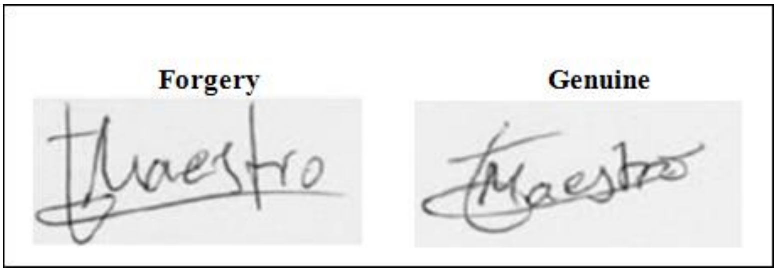

Figure 5 - Example of MCYT-75signature database

These datasets serve as benchmarks for assessing the reliability and effectiveness of signature recognition algorithms.

2.5. CNN Architecture for Signature Recognition

The steps of the CNN architecture are detailed below:

2.5.1. Data Preprocessing:

Figure 6 illustrates that data preprocessing involves several essential steps to ensure the development of a reliable handwritten signature recognition system:

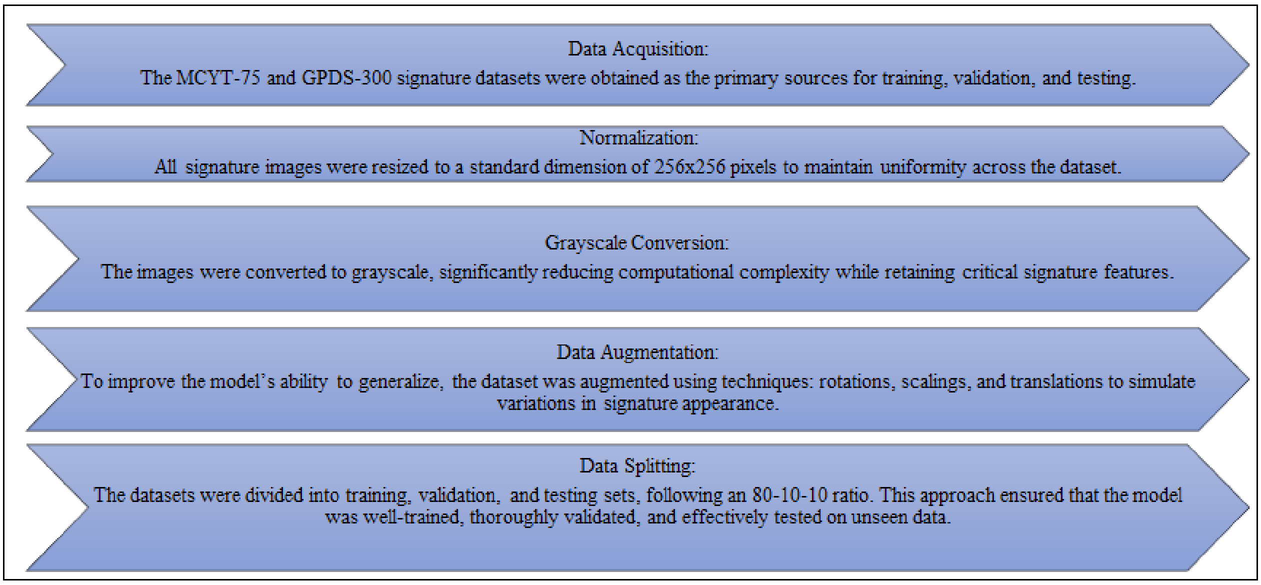

Figure 6 - Data Preprocessing for Enhanced Handwritten Signature Recognition

2.5.2. Model Architecture

This CNN architecture is designed for multi-class classification, extracting features through four convolutional layers with max-pooling for dimensionality reduction. Flattened outputs are processed by fully connected layers, with dropout layers minimizing overfitting. A softmax output layer ensures precise class probability assignments, ideal for tasks like handwritten signature recognition as shown in Table 1.

Table 1 – CNN architecture

1. Convolutional Layer 1 (conv1): - Number of filters: 32 - Filter size: 3x3 - Activation function: ReLU - Output size: 254 x 254 - Maxpooling Layer 1 (pool1): ▪ Pooling size: 3x3 ▪ Stride: 1 ▪ Output size: 84 x 84	2. Convolutional Layer 2 (conv2): - Number of filters: 64 - Filter size: 3x3 - Activation function: ReLU - Output size: 82 x 82 - Maxpooling Layer 2 (pool2): ▪ Pooling size: 2x2 ▪ Output size: 41 x 41
3. Convolutional Layer 3 (conv3): - Number of filters: 128 - Filter size: 3x3 - Activation function: ReLU - Output size: 39 x 39 - Maxpooling Layer 3 (pool3): ▪ Pooling size: 2x2 ▪ Output size: 19 x 19	4. Convolutional Layer 4 (conv4): - Number of filters: 256 - Filter size: 3x3 - Activation function: ReLU - Output size: 17 x 17 - Maxpooling Layer 4 (pool4): ▪ Pooling size: 2x2 ▪ Output size: 8 x 8
5. Flattening Layer: - Converts the output from the last pooling layer into a 1D vector of size 2048.	6. Fully Connected Layer 1 (FC1): - Number of neurons: 512 - Activation function: ReLU
7. Dropout Layer 1 (dropout1): - Dropout rate: 0.5 (to reduce overfitting)	8. Fully Connected Layer 2 (FC2): - Number of neurons: 128 - Activation function: ReLU
9. Dropout Layer 2 (dropout2): - Dropout rate: 0.5	10. Output Layer: - Number of neurons: Matches the total number of individual signatures or author identities in the dataset.

	- Activation function: Softmax (suitable for multi-class classification).

2.5.3. Training configuration

- The hardware used for this study is a single GPU for facilitated efficient processing of the training data.
- Loss function: For multi-class classification tasks, we utilize the Categorical Cross-Entropy loss function.
- Optimizer: SGD (Stochastic Gradient Descent) optimizer chosen for efficient convergence with an initial learning rate of 0.01.
- Batch Size: Use a batch 64 size suitable for the hardware.
- Epochs and Iterations: The model trained for 100 epochs, with 30 iterations per epoch, for a total of 3000 iterations.

2.5.4. Validation

- Evaluate the model using validation datasets to determine accuracy and to ensure the model's ability to generalize.
- Validation frequency: Validation of the model is performed every 30 iterations during training to continuously monitor performance.
- Monitor performance metrics: validation accuracy throughout the training process and error rate.

2.5.5. Results evaluation metrics

- Accuracy: The percentage of correctly identified signatures.
- Error Rate (EER): The proportion of incorrectly identified signatures.

The flowchart resumed our approach is shown below (see Figure 7):

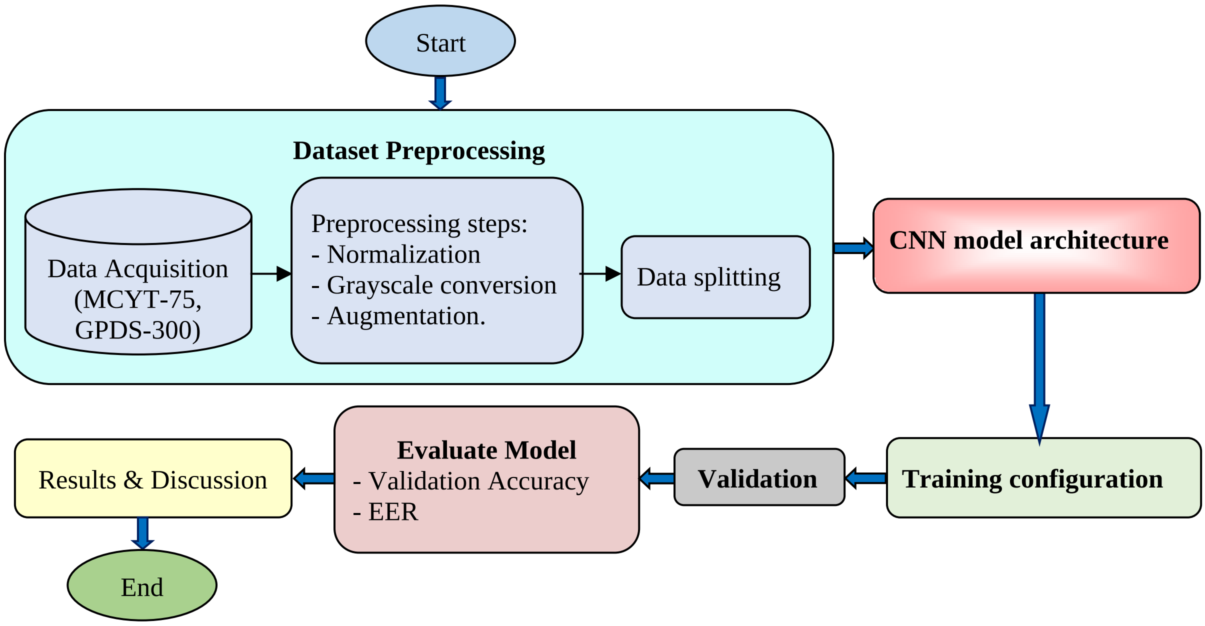

Figure 7 - Flowchart of the proposed approach.

3. Experiments results and discussion

A personal PC with an i7 processor and 32 GB of RAM is used to conduct this experiment in MATLAB software. The configuration characteristics of our experimental platform are shown in Table 2.

Table 2 - Hardware specifications of our experimental platform configuration

Configuration	Version
System	64-bit operating system, x64 processor
GPU	NVIDIA Quadro M1200
RAM	32,0 GB
CPU	Intel R Core TM i7-7700HQ @ 2.80GHz

In our deep learning approach to handwritten signature recognition, we utilized a Convolutional Neural Network (CNN) and evaluated its performance on the GPDS-300 and MCYT-75 datasets. The training process was conducted with a fixed learning rate of 0.01 over 100 epochs, encompassing 3000 iterations. Validation checks were performed every 30 iterations, ensuring consistent monitoring of the model's performance throughout the training phase.

The training and validation accuracies achieved were remarkable, as depicted in Figures 8 and 9, highlighting the effectiveness of the proposed method. For the GPDS-300 dataset, the model achieved an exceptional validation accuracy of 99.80%, effectively distinguishing genuine signatures from forgeries. Similarly, the MCYT-75 dataset recorded an impressive validation accuracy of 99.60%, showcasing the robustness of the model across different datasets.

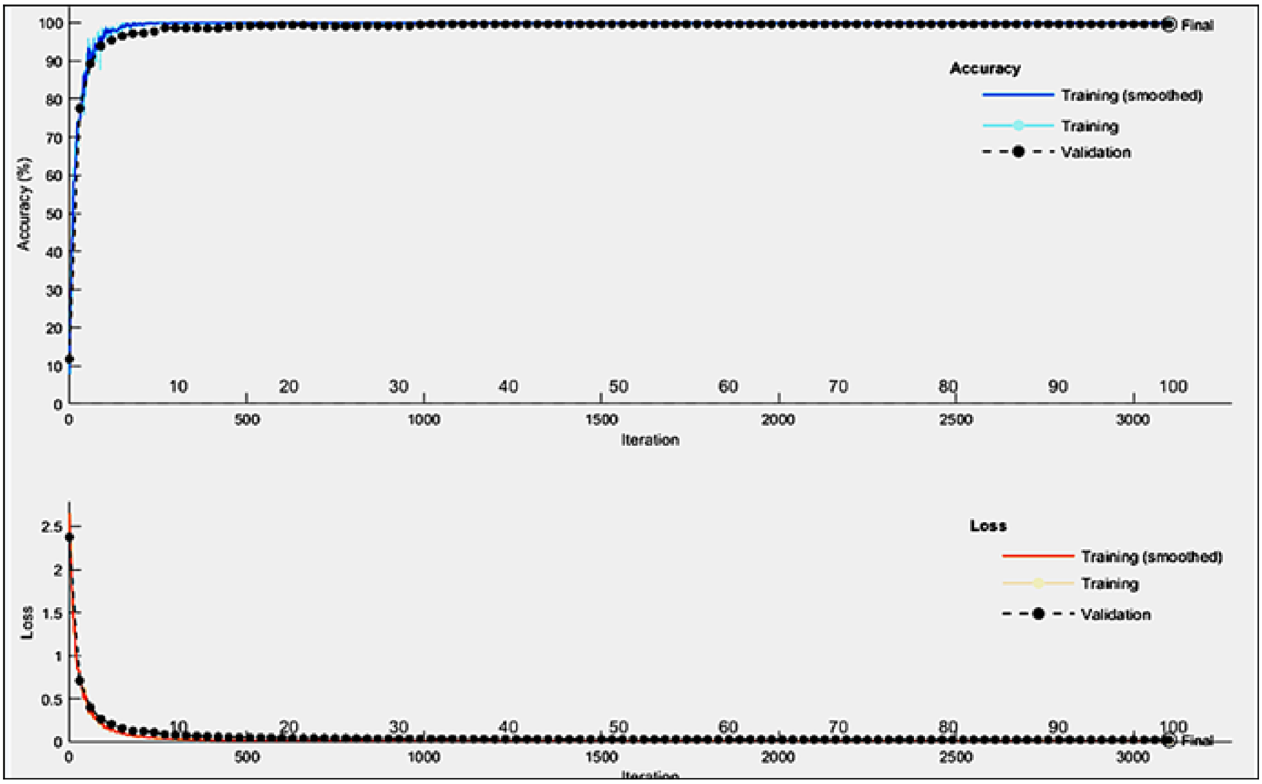

Figure 8 - Accuracy and loss curve of signature (MCYT-75 datasets).

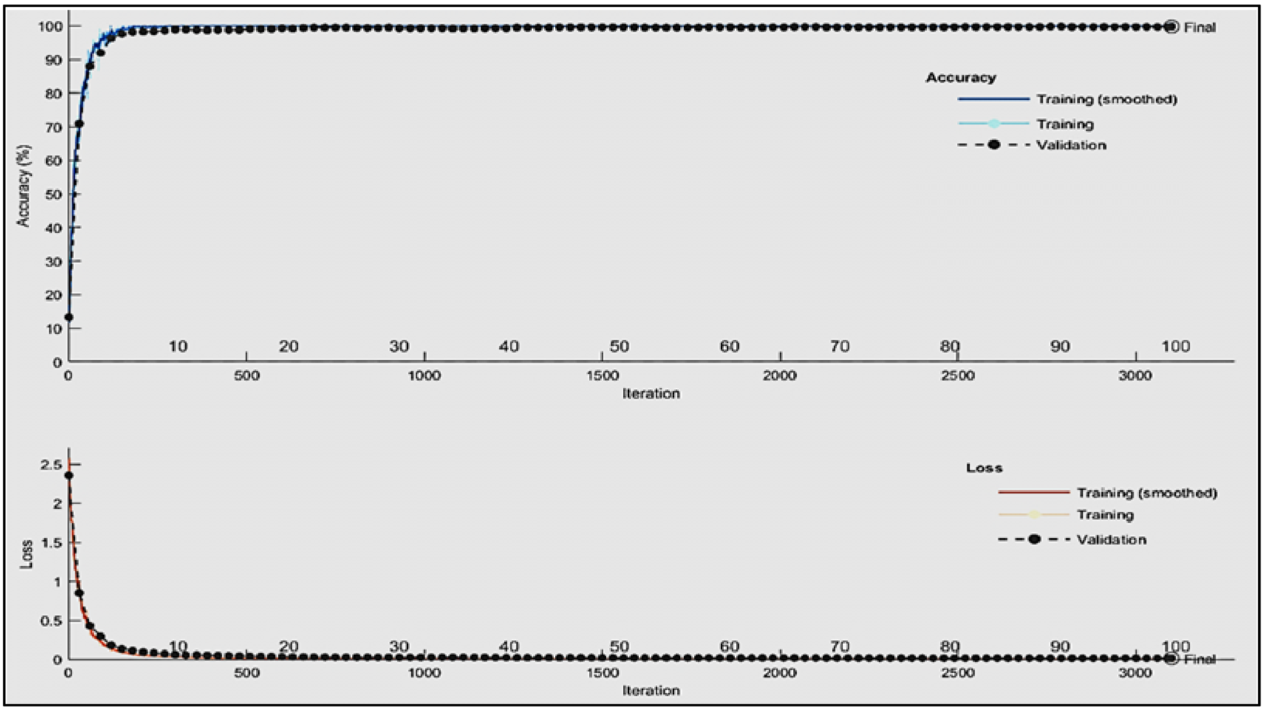

Figure 9 - Accuracy and loss curve of signature (GPDS-300 datasets)

The high recognition rates achieved on both datasets underscore the robustness of the CNN model in identifying complex patterns characteristic of handwritten signatures. The slight difference in accuracy between the GPDS-300 and MCYT-75 datasets can be attributed to variations in their size and diversity. The larger GPDS-300 dataset likely provides a more comprehensive training set, enhancing the CNN model's learning capabilities. The error rates (ERR) for both datasets, as illustrated in Figure 10, further demonstrate the model's effectiveness in handwritten signature recognition. The consistently low error rates indicate the exceptional performance and reliability of the trained CNN model. Overall, these results validate the proposed deep learning approach, showcasing its efficacy and minimal error rates across both datasets.

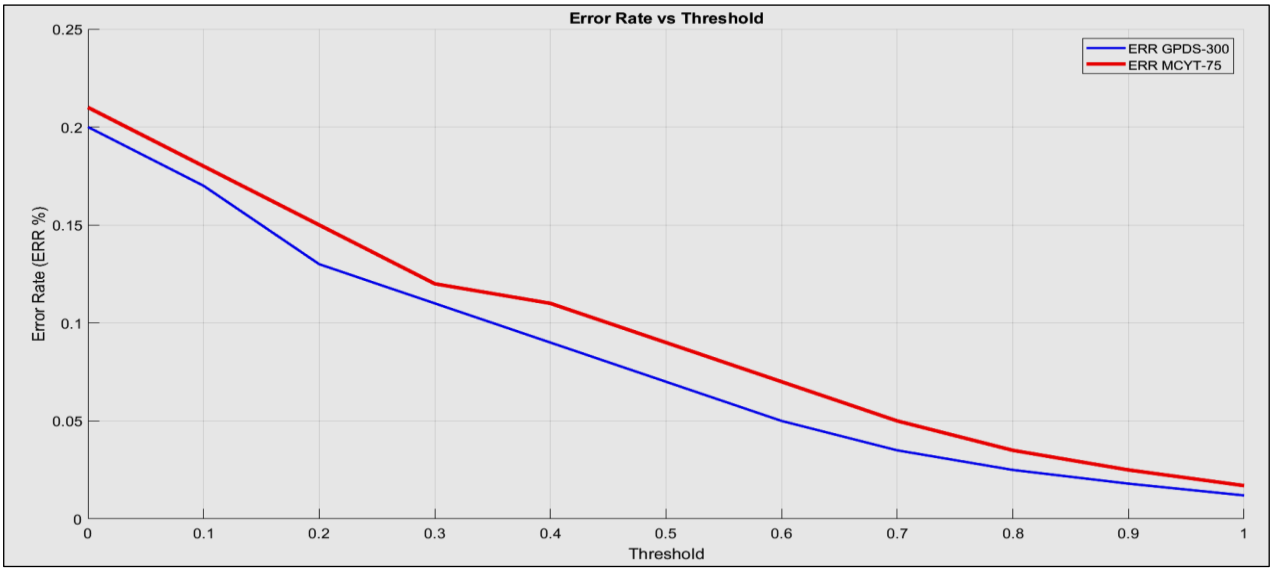

Figure 10 - Error rate for handwritten signatures recognition

Table 3 presents a comparison with existing techniques, revealing that our method enhances performance relative to other works in the literature. Our deep learning approach significantly outperforms previous signature recognition methods, underscoring the superior capabilities of the CNN architecture in biometric recognition tasks. The validation accuracy achieved illustrates the model's effectiveness in learning and extracting relevant features from handwritten signatures in the GPDS-300 and MCYT-75 datasets. This outstanding performance is particularly impressive considering the inherent challenges of signature recognition, such as variations in signature styles and writing conditions. The results highlight the robustness and adaptability of the proposed deep learning method, setting a new benchmark for accuracy in signature recognition.

Table 3 - Comparison with other approach

Authors	Approach	Accuracy (%)
(Albasu *et al.*, 2023)	Convolutional Siamese Neural Networks	97.5
(Anamika *et al.*, 2021)	ANN	Hindi : 95.29, Bengali : 97.79
(Alajrami *et al.*, 2020)	ANN	in an 80-20 ratio: 99.7, in an 60-40 ratio: 99.7, in an 70-30 ratio: 98
Our work	CNN	MCYT 75: 99.96 GPDS 300: 99.98

4. Conclusion

This study introduces a robust approach for offline handwritten signature recognition (HSR) in biometric systems, achieving exceptional accuracy and demonstrating the efficacy of deep learning techniques. To evaluate the proposed CNN-based model, experiments were conducted on the MCYT-75 and GPDS-300 datasets. The model, trained over 100 epochs with optimal parameters selected based on validation loss, achieved remarkable validation accuracies of 99.80% on GPDS-300 and 99.60% on MCYT-75. The training process, executed efficiently on a single GPU with a constant learning rate of 0.01, minimized error rates and highlighted the model's robustness for signature recognition tasks.

These findings underscore the effectiveness of CNN architectures in addressing the challenges associated with handwritten signature variability, making the proposed approach highly suitable for real-world biometric authentication systems. Furthermore, the research provides valuable insights into leveraging deep learning for complex pattern recognition in HSR applications.

Future work will focus on further enhancing the model's performance through advanced techniques such as data augmentation and transfer learning. Additionally, expanding the dataset to include a wider range of environmental conditions will be prioritized to improve the model's generalizability and robustness in diverse real-world scenarios.

Reference

Abdoli, S., & Hajati, F. (2014). Offline signature verification using geodesic derivative pattern. In *22nd Iranian Conference on Electrical Engineering (ICEE 2014)*, 1018–1023.

Akinci, T., Antonoli, D., et al. (2023). Development and evaluation of deep learning models for automated estimation of myelin maturation using pediatric brain MRI scans. *Radiology Artificial Intelligence*, *5*(5), e220292.

Alaei, A., et al. (2017). An efficient signature verification method based on an interval symbolic representation and a fuzzy similarity measure. *IEEE Transactions on Information Forensics and Security*, *12*(10), 2360–2372. https://doi.org/10.1109/TIFS.2017.2707332

Alajrami, E., et al. (2020). Handwritten signature verification using deep learning. *International Journal of Academic Multidisciplinary Research*, *3*(12), 39–44.

Albasu, F. B., & Al Akkad, M. A. (2023). Exploiting deep learning techniques for the verification of handwritten signatures. *Intellektual'nye Sistemy v Proizvodstve*, *21*(3), 27–39. https://doi.org/10.22213/2410-9304-2023-3-27-39

Anamika, J., et al. (2021). Signature verification using geometrical features and artificial neural network classifier. *Neural Computing and Applications, 33*(12), 6999–7010. https://doi.org/10.1007/s00521-020-05473-7

Aslani, S., et al. (2023). Utilisation of deep learning for COVID-19 diagnosis. *Clinical Radiology, 78*(2), 150–157.

Benhur, S. J. (2021). A friendly introduction to Siamese networks. *Medium*. https://towardsdatascience.com/a-friendly-introduction-to-siamese-networks-85ab17522942

Bertolini, D., et al. (2010). Reducing forgeries in writer-independent offline signature verification through ensemble of classifiers. *Pattern Recognition, 43*(1), 387–396. https://doi.org/10.1016/j.patcog.2009.05.009

Bharadi, V. A., & Kekre, H. B. (2010). Off-line signature recognition systems. *International Journal of Computer Applications*, *1*(27), 48–56.

Bhunia, A. K., Alaei, A., & Roy, P. P. (2019). Signature verification approach using fusion of hybrid texture features. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-019-04220-x

Bindal, A. (2019). Normalization techniques in deep neural networks. *Techspace*. https://medium.com/techspace-usict/normalization-techniques-in-deep-neural-networks-9121bf100d8

Cong, S., et al. (2023). A review of convolutional neural network architectures and their optimizations. *Artificial Intelligence Review, 56*(3), 1905–1969.

Diaz, M., Ferrer, M. A., Eskander, G. S., & Sabourin, R. (2017). Generation of duplicated off-line signature images for verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 39*(5), 951–964. https://doi.org/10.1109/TPAMI.2016.2560810

Dubey, R., & Agrawal, D. K. (2012). Comparative analysis of off-line signature recognition. In *Proceedings – 2012 International Conference on Communication, Information, and Computing Technology (ICCICT)*, 1–6.

Ferrer, M. A., Vargas, J. F., Morales, A., & Ordonez, A. (2012). Robustness of offline signature verification based on gray level features. *IEEE Transactions on Information Forensics and Security*, *7*(3), 966–977. https://doi.org/10.1109/TIFS.2012.2190281

Ferrer, M., Alonso, J., & Travieso, C. (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 27*(6), 993–997.

Ghosh, R. (2020). A recurrent neural network based deep learning model for offline signature verification and recognition system. *Expert Systems with Applications*, *114*, 114249. https://doi.org/10.1016/j.eswa.2020.114249

Haug, C. J., et al. (2023). Artificial intelligence and machine learning in clinical medicine, 2023. *New England Journal of Medicine*, *388*(13), 1201–1208.

Hezil, H., Djemili, R., & Bourouba, H. (2018). Signature recognition using binary features and KNN. *International Journal of Biometrics, 10*(1), 1. https://doi.org/10.1504/ijbm.2018.090121

Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: The state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38*(5), 609–635. https://doi.org/10.1109/TSMCC.2008.923866

Jain, A., Singh, S. K., & Singh, K. P. (2020). Signature verification using geometrical features and artificial neural network classifier. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-020-05473-7

Kang, N. (2019). Introducing deep learning and neural networks – Deep learning for rookies (1). *Medium*. https://towardsdatascience.com/introducing-deep-learning-and-neural-networks-deep-learning-for-rookies-1-bd68f9cf5883

Khalil, M. I., et al. (2009). Enhanced DTW-based on-line signature verification. In *16th IEEE International Conference on Image Processing (ICIP)* (pp. 2713–2716). IEEE. https://doi.org/10.1109/ICIP.2009.5414166

Kingma, D. P., & Ba, J. (2017). Adam: A method for stochastic optimization. *arXiv:1412.6980*. http://arxiv.org/abs/1412.6980

Kshatri, S. S., et al. (2023). Convolutional neural network in medical image analysis: A review. *Archives of Computational Methods in Engineering, 30*(4), 2793–2810.

Kurani, A., et al. (2023). A comprehensive comparative study of artificial neural network (ANN) and support vector machines (SVM) on stock forecasting. *Annals of Data Science, 10*(1), 183–208.

Liu, Z., et al. (2023). Deep learning-based brain tumor segmentation: A survey. *Complex & Intelligent Systems, 9*(1), 1001–1026.

Manohar, S. (2017). *Mastering machine learning with Python in six steps: A practical implementation guide to predictive data analytics using Python*. Apress.

Menghani, G. (2023). Efficient deep learning: A survey on making deep learning models smaller, faster, and better. *ACM Computing Surveys, 55*(12), 1–37.

Odeh, S., & Khalil, M. (2011). Apply Multi-Layer Perceptrons Neural Network for Off-Line Signature Verification and Recognition. *International Journal of Computer Science Issues (IJCSI), 8*(6), 261–266.

Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., & et al. (2003). MCYT baseline corpus: A bimodal biometric database. *Vision, Image and Signal Processing, IEE Proceedings, 150(6)*, 395–401. doi:10.1049/ip-vis:20031078

Sadak, M. S., Kahraman, N., & Uludağ, U. (2022). Dynamic and static feature fusion for increased accuracy in signature verification. *Signal Processing: Image Communication, 108*, 116823. https://doi.org/10.1016/j.image.2022.116823

Sanghvirajit. (2021). A complete guide to Adam and RMSprop optimizer. *Analytics Vidhya*. https://medium.com/analytics-vidhya/a-complete-guide-to-adam-and-rmsprop-optimizer-75f4502d83be

Shah, A., et al. (2016). An offline signature verification technique using pixels intensity levels. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 9*(8), 205–222. https://doi.org/10.14257/ijsip.2016.9.8.18

Sharif, M., Raza, M., Shah, J. H., Yasmin, M., & Fernandes, S. L. (2019). An overview of biometrics methods. In *Handbook of Multimedia Information Security: Techniques and Applications* (pp. 15–35).

Suykens, J. A. K., Van Gestel, T., De Brabanter, J., De Moor, B., & Vandewalle, J. (2002). *Least squares support vector machines*. World Scientific Publishing Co., Pte, Ltd.

Taşpinar, G., et al. (2023). 3D CNN-based automatic diagnosis of ADHD using fMRI volumes. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi, 25*(73), 1–8.

Vargas, F., Ferrer, M. A., Travieso, C. M, & Alonso, J. B. (2007). Off-line handwritten signature GPDS-960 corpus. In *Proceedings of the 9th International Conference on Document Analysis and Recognition*, pp. 764–768. doi:10.1109/icdar.2007.4377018

Vargas, J.F.; Ferrer, M.A.; Travieso, C. M.; Alonso, J. B.; (2011). Off-line signature verification based on grey level information using texture features. *Pattern Recognition, 44*(2), 375–385. https://doi.org/10.1016/j.patcog.2010.08.010

Vinushanth, C. V. (2020). Markov and hidden Markov models. *Medium*. https://towardsdatascience.com/markov-and-hidden-markov-model-3eec42298d75

Wang, J., Wang, J., Wang, S., & Zhang, Y. (2023). Deep learning in pediatric neuroimaging. *Displays, 80*, 102583. https://doi.org/10.1016/j.displa.2023.102583

Yu, T., et al. (2023). Machine learning-enabled retrobiosynthesis of molecules. *Nature Catalysis, 6*(2), 137–151.