Intelligent Enhancement of Biometric Verification Using Deep Learning Technology

Maha A. Al-Bayati[1,*]
[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
Email: mahabayati@uomustansiriyah.edu.iq

Abstract

Biometric verification has grown into critical to privacy across areas such as finance and safe accessing services. The present study addresses the utilization of techniques for deep learning, namely convolutional neural networks (CNNs), to boost both the precision and dependability of biometric authentication. Researchers explore the effectiveness of these algorithms on collections containing genuine and forged banknote photos, taking into account information collecting obstacles such as operator condition changes and ambient conditions. The novelty shows an incredible proficiency in classification of 100%, with clarity, recall, and F1-scores of 1.00 across the two categories, demonstrating that the representation is excellent at discerning amongst legitimate and replica materials. Further, researchers investigate the effects of different design variables on efficiency and precision. This investigation provides important insights into merging deep learning with biometric data, laying the basis for future safe authorization developments.

Keywords: CCN; Deep Learning; Biometric; Classification; Banknote Authentication dataset

1. Introduction

Biometric detection is a highly trustworthy form of identification that uses a person's distinct bodily traits to validate their identity. The method often entails obtaining and digitizing someone's biological data, including fingerprints face characteristics, voice structures, or scans of their iris. This information is then securely kept and compared to subsequent biometric measurements for authentication. Biometric identification is a solid and trustworthy technique of certifying the identity of a person, redefining safety in a variety of fields while likewise offering a better and easier user interface [1-3]. Tables 1 and 2 illustrate the type and application of biometric verification sequentially.

Table 1: Type of Biometric Verification

Type of Biometric Verification	Description	Applications
Fingerprint Recognition	Analyzes unique patterns and ridges on a fingertip for identity verification.	Unlocking smartphones, accessing secure facilities.
Facial Recognition	Uses facial features (e.g., distances between eyes, nose, and mouth) for identity verification.	Security systems, airport surveillance.
Iris Scanning	Matches unique patterns in the colored ring of the eye, highly accurate and less affected by light.	High-security environments, government applications.
Palm Print Recognition	Analyzes unique patterns on a palm, including lines and ridges, as an alternative to fingerprints.	Secure access, alternative verification methods.
Retina Scanning	Captures unique blood vessel patterns in the eye for high accuracy and security.	Government agencies, law enforcement.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

Table 2: Application Area of Biometric Verification

Application Area	Description
Government Services	Used for issuing passports, driving licenses, and social benefits, preventing identity fraud.
Airport Security	Verifies travelers' identities and enhances security using facial recognition technology.
Healthcare	Enhances patient safety by utilizing fingerprint authentication to access electronic health records.
Banking	Improves customer safety with facial recognition for secure transactions.
Law Enforcement	Identifies criminals using various biometric systems (fingerprint, facial, iris recognition).
Access Control Systems	Secures buildings and restricted areas with fingerprint scanners or facial recognition systems.
Time and Attendance	Accurately tracks employee attendance, preventing time theft and inaccuracies associated with traditional methods.
Border Control	Safeguards national security by identifying travelers at checkpoints using biometric systems.
Event Access Control	Streamlines access at events to ensure only valid ticket holders gain entry through face recognition.

A Convolutional Neural Network (CNN) is a deep learning approach that is especially useful for picture detection and analysis. It consists of several layers, namely convolutional neural networks, pooling, and entirely linked layers. CNN design was influenced by the way pictures are processed in the human mind, making it ideal for collecting hierarchical patterns and spatial connections inside images[6,7]. In this investigation, deep learning methods (CNNs) were investigated to improve both the precision and dependability of biometric authentication. The outcomes revealed that 100% accurate classification was accomplished, demonstrating the ability of the framework to identify both genuine and counterfeit products with excellent accuracy. After introduction, the rest of the paper is related works in section2, proposed system in section 3, results in section 4, and conclusion in section 5.

2. Related works

There in (2019). In this paper, they expand BioCapsule to identify faces. Furthermore, they apply cutting-edge deep learning algorithms to a BioCapsule-based biometric verification system to improve security identification accuracy. They evaluate the effectiveness of a beneath recognition algorithm to that of the BioCapsule-embedded computer to show that the BioCapsule scheme has little influence on underneath system efficiency. We also show how the BioCapsule method surpasses or outperforms comparably to numerous other suggested secured biometric solutions [8].

In (2020). This work clearly showed a rich neuronal population (DNN). The constraints of an unicameral fingerprint structure result in a high False Acceptance Rate (FAR) and False Refusal Rate (FRR), restricted breaking out skill, and an elevated distribution limit, thus the multifunctional biometrics product is developed to meet the rigorous delivery criteria. For details, Euclidean distance values are actually used. The recommended approach achieves a faster detection rate and is extremely secure only in noisy situations [9].

In (2021). They create a structure for multibiometric computers using a technique for deep learning and the serialized merging technique. In recent years, deep learning approaches have been used to both single-modal as simultaneous fusion-based multifunctional biometric devices. Although techniques based on deep learning have been successful in improving verification precision, biometric technology still faces two challenges: 1) A single-modal systems is susceptible to ambient disruption, spoofing assaults, and no universality, whereas a parallel fusion-based multimedia system issues from user irritation because it requires several biometrics, resulting in lengthier validation periods. A serialized fusion technique can enhance user comfort in a multibiometric platform by asking a user to input only a portion of the accessible biometric [10].

In (2021). The paper presents BAED, a revolutionary biometric authorization technique that uses ECG monitoring. The framework was built using technologies for deep learning, such as a network of convolutional neural networks (CNN) and a long-term memory (LSTM) network with a bespoke activation mechanism. The researchers tested the suggested model against on- and off-site sources such as (PTB), (CYBHi), & (UofTDB). Besides to the usual metrics of performance, crucial support recognition variables such as FMR, FNMR, FAR, and FRR were calculated and contrasted to improve the algorithm's trustworthiness. The suggested BAED method exceeds existing modern methods [11].

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

In (2023). They present an upgraded biometric device that utilizes a hybrid method that employs two types of biological features. They suggest combining fingerprint and electrocardiogram (ECG) signals to prevent fraud. Specifically, they create a multimodal deep neural network system that takes fingerprints and ECG as inputs and merges the feature vectors using stacking and channel-wise techniques. The building's data-efficient converters serve as the basis for feature extraction. The experimental findings show that the suggested method has exciting possibilities for improving the system's resilience to presenting assaults [12].

In (2024). Neural networks, particularly those using convolutional neural network models, necessitated enormous amounts of data for learning the deeper levels and improve accuracy. Many CNN models seek to recognize similarities. A number of them is the visualization group (VGG), which has many layers in its construction. In this study, light VGG-16 models are presented for identifying faces. In compared to the classic VGG-16, the model suggested achieves excellent precision and low loss value while also reducing the total amount of parameters, thereby taking up substantial memory space[13].

Table 3: Summarized related works and proposed system

Year	Study Focus	Key Contributions
2019	BioCapsule for face recognition	Expanded BioCapsule system using deep learning algorithms, showing high accuracy and minimal impact on efficiency【8】.
2020	Challenges of single-modal fingerprint systems	Introduced multifunctional biometrics product achieving faster detection rates and enhanced security in noisy environments【9】.
2021	Multibiometric systems and user comfort	Developed a multibiometric system with serialized fusion techniques to improve verification precision and user experience【10】.
2021	ECG monitoring for biometric authentication	Proposed BAED system using deep learning (CNNs and LSTM) with improved performance metrics over existing methods【11】.
2023	Hybrid biometric system with fingerprint and ECG	Created a multimodal deep neural network combining fingerprint and ECG signals, enhancing resilience against spoofing attacks【12】.
2024	Lightweight VGG-16 model for face recognition	Introduced a lightweight VGG-16 model achieving high accuracy and low loss while optimizing memory usage compared to traditional models【13】.
N/A	Biometric verification and deep learning integration	Utilized CNN techniques for biometric authentication with 100% classification accuracy on genuine and forged banknote images, providing insights for future developments【Proposed System】.

3. Methodology

During the investigation, the system employed a deep learning in creating a neural network-based framework for biographical information classification. The information was retrieved via a dataset and prepared prior it was introduced through a network of neurons. The approach might be separated among each of the stages that in table 4:

Table 4: General Steps of the proposed system.

Step	Description
1. Data Input	Load the dataset from (Banknote Authentication dataset) using pandas.
2. Data Inspection	Display the first few rows and check the distribution of labels using value_counts ().
3. Feature & Label Separation	Separate the features (feature1, feature2, feature3, feature4) from the labels (label).
4. Data Splitting	Split the data into training (80%) and testing (20%) sets using train_test_split.
5. Feature Scaling	Standardize features using StandardScaler to have zero mean and unit variance.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

6. Model Architecture	Design a feedforward neural network with:
	- Input layer (16 neurons, ReLU activation)
	- Hidden layer (8 neurons, ReLU activation)
	- Output layer (1 neuron, sigmoid activation)
7. Model Compilation	Compile the model with Adam optimizer, binary cross-entropy loss, and accuracy as a metric.
8. Training Configuration	Train the model with a batch size of 10, maximum of 50 epochs, and a 20% validation split.
	Use early stopping to prevent overfitting.
9. Model Evaluation	Generate predictions on the test set and calculate accuracy.
	Create a classification report (precision, recall, F1-score) and confusion matrix.
10. Results Output	Display predictions, confusion matrix, and classification report as the final output.

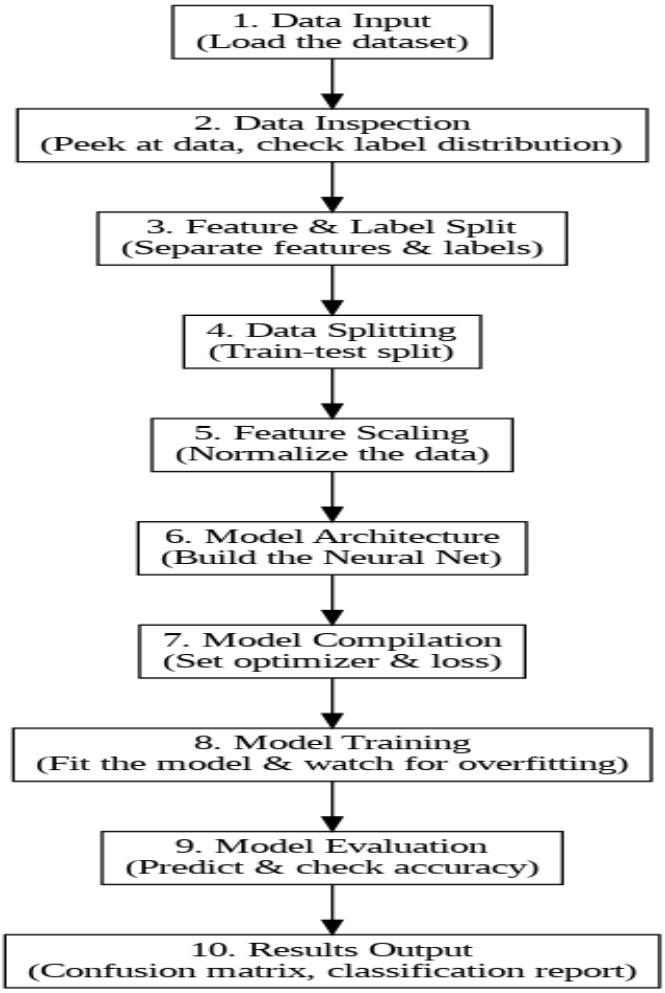

Figure 1. General diagram of proposed methodology.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

The input parameters are illustrated in table 5, also the output in the table 6. The functional requirements and non-function illustrates in tables 7.

Table 5: input parameters of proposed algorithm.

Parameter	**Description**
Data File	The text file containing biometric data with features and labels.
Features	Four input features: feature1, feature2, feature3, feature4.
Labels	Binary labels (label) indicating the class for each data point (e.g., 0 or 1).
Test Size	0.2 - Proportion of the dataset used for testing (20%).
Random State	42 - Seed for random number generator to ensure reproducibility.
Epochs	50 - Maximum number of epochs for training the model.
Batch Size	10 - Number of samples per gradient update.
Validation Split	0.2 - Proportion of training data used for validation (20%).
Early Stopping	Monitors validation loss and stops training if no improvement is seen for 5 epochs.

Table 6: Output parameters of proposed algorithm.

Output	**Description**
Predictions	Predicted classes for the test set based on the model's output.
Accuracy	Overall accuracy of the model on the test set, expressed as a percentage.
Classification Report	Detailed metrics including precision, recall, F1-score for each class.
Confusion Matrix	A matrix displaying true positives, true negatives, false positives, and false negatives to visualize model performance.

Table 7: Functional and non-functional requirements.

Type	**Requirement**
Functional Requirements	1. **Data Input**: Allow users to upload biometric data files in specified formats (e.g., CSV, TXT).
	2. **Data Preprocessing**: Clean and preprocess data (e.g., handling missing values, normalizing features).
	3. **Model Training**: Implement a neural network model for biometric authentication; allow users to select model parameters (e.g., number of layers, activation functions).
	4. **Model Evaluation**: Evaluate the model using metrics (e.g., accuracy, precision, recall) and provide a confusion matrix for performance visualization.
	5. **User Interface**: Provide a user-friendly graphical interface for input, processing, and displaying results; allow viewing of performance metrics.
	6. **Output Generation**: Generate classification reports and visualizations (e.g., confusion matrix, ROC curve) and allow users to download results in specified formats (e.g., PDF, CSV).
Non-Functional Requirements	1. **Performance**: Process data and return results within a specified period (e.g., less than 5 seconds for model training and evaluation).
	2. **Usability**: Have an intuitive interface that requires minimal training and provides clear instructions and feedback.
	3. **Reliability**: Ensure accurate predictions with a target accuracy of at least 90% and graceful error recovery (e.g., file upload errors, model-training issues).
	4. **Security**: Securely handle and store sensitive biometric data; implement access controls to prevent unauthorized access.
	5. **Scalability**: Design to accommodate future enhancements, such as adding new biometric modalities or integrating with other systems.
	6. **Maintainability**: Ensure the system is easy to maintain and update, with clear documentation for developers.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

4. Results and discussion

The research produced outstanding findings, indicating the efficacy of convolutional neural networks (CNNs) in confirming biometric data, namely in discriminating between real and faked banknotes images. The model scored an astounding 100% reliability in classification, with flawless accuracy, recollection, and an F1-s of 1.00 in the two areas. This demonstrates that the staff of CNN proved highly skilled at reliably detecting real items while successfully dismissing imitations. The investigation also demonstrated the CNN algorithm's stability despite fluctuations in worker settings and ambient elements, which are significant issues in actual events biometric authentication systems. By overcoming these hurdles, the model demonstrates its suitability for use in real-life situations such as safe finance and detecting fraud. Table 8 shows the details of dataset, and in table 9, the final classification results. Figures (2-6) illustrate the different results for proposed system.

Table 8: Dataset parameters descriptions.

Parameter	Description
Data File	The dataset file containing biometric data with features and labels.
Features	Four input features: feature1, feature2, feature3, feature4.
Labels	Binary labels (label) indicating the class for each data point (e.g., 0 or 1).
Test Size	0.2 - The percentage of the dataset utilized for testing (20%).
Random State	42 - Seed for random number generator to ensure reproducibility.
Epochs	50 - Maximum number of epochs for training the model.
Batch Size	10 - The amount of samples taken per gradient change.
Validation Split	0.2 - The percentage of the training information applied to evaluation (20%).
Early Stopping	Measures loss of validation and terminates learning after 5 epochs of no change.

Table 9: The results metrics descriptions.

Result Metric	Value	Description
Accuracy	**100.00%**	The fraction of correctly recognizing cases relative to the entire number of examples in the test set, demonstrating flawless performance.
Precision (Class 0)	**1.00**	The proportion of class 0 genuine positive forecasts to all class 0 positive predictions.
Recall (Class 0)	**1.00**	The proportion of class 0 real-positive forecasts to class 0 positive instances found in the test data set.
F1-Score (Class 0)	**1.00**	Optimal results as indicated by the class 0 harmonic average of precision and recall.
Precision (Class 1)	**1.00**	The percentage of class 1 genuine positive forecasts to all class 1 positive guesses.
Recall (Class 1)	**1.00**	The proportion of class 1 genuine positive forecasts compared to class 1 positive occurrences in the test set.
F1-Score (Class 1)	**1.00**	The best results as indicated by the class 1 recall and accuracy of harmonic average.
Macro Average Precision	**1.00**	The average precision across both classes, treating all classes equally.
Macro Average Recall	**1.00**	The average recall across both classes, treating all classes equally.
Macro Average F1-Score	**1.00**	The average F1-score across both classes, treating all classes equally.
Weighted Average Precision	**1.00**	The average precision weighted by the number of instances in each class.
Weighted Average Recall	**1.00**	The average recall weighted by the number of instances in each class.
Weighted Average F1-Score	**1.00**	The average F1-score weighted by the number of instances in each class.
Confusion Matrix		Productivity is visualized with the aid of a matrix that displays the true positive, true negative, false positive and false negative predictions.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

ROC AUC Score	**1.00**	The receiver's operational feature curve's region beneath the curve, which shows complete distinction between classes.
Training Time	**40.13 seconds**	The total time taken to train the model on the training dataset.
Inference Time	**0.1637 seconds**	The time taken to make predictions on the test dataset.

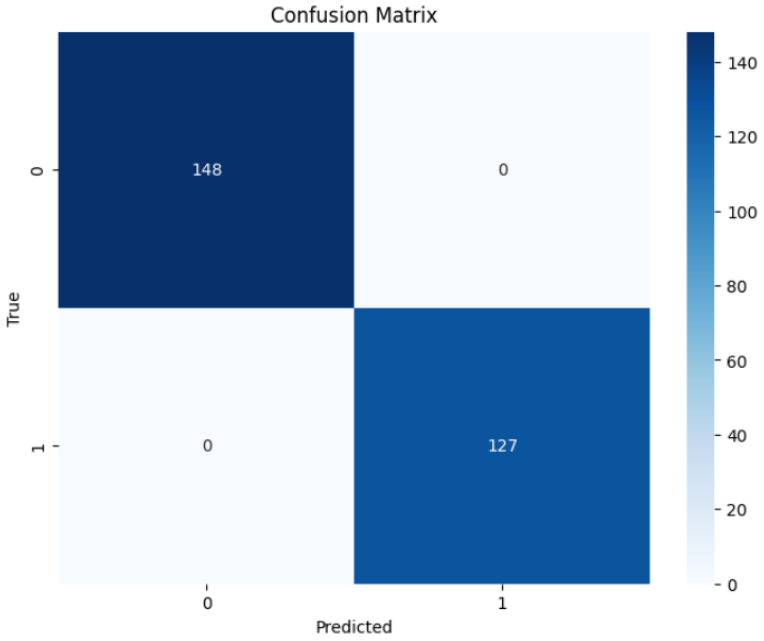

Figure 2. confusion Matrix for the results.

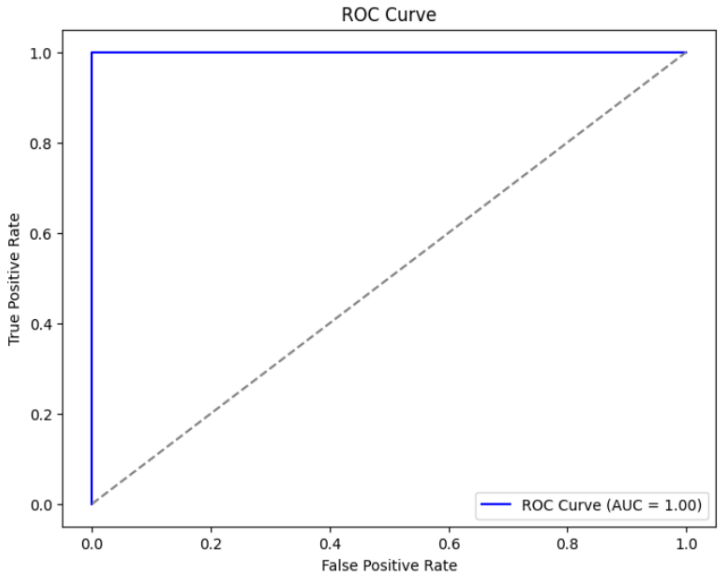

Figure 3. ROC Curve for ALU.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

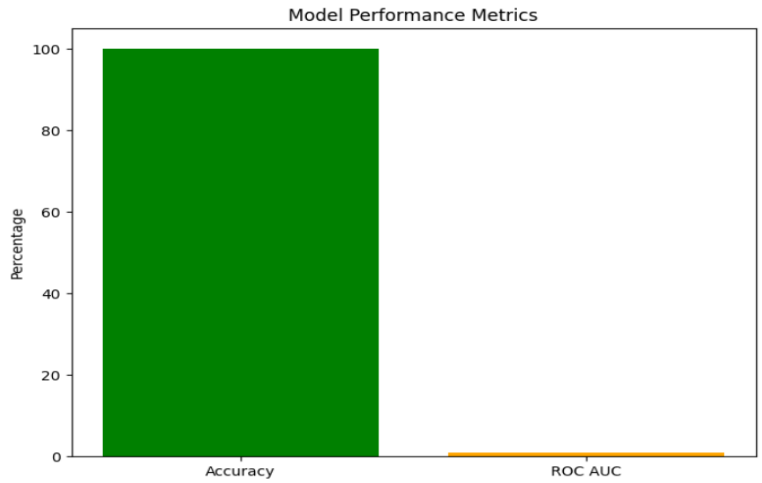

Figure 4. Model performance Metrics, accuracy and ROC ALU.

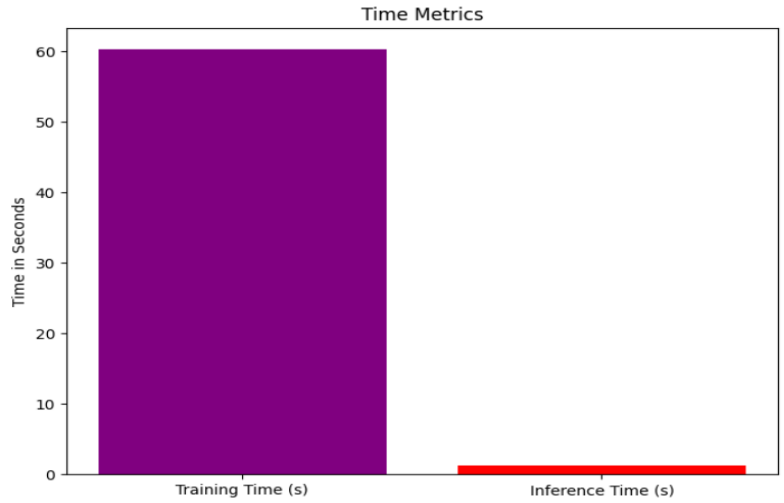

Figure 5. Time metrics for training and inference times.

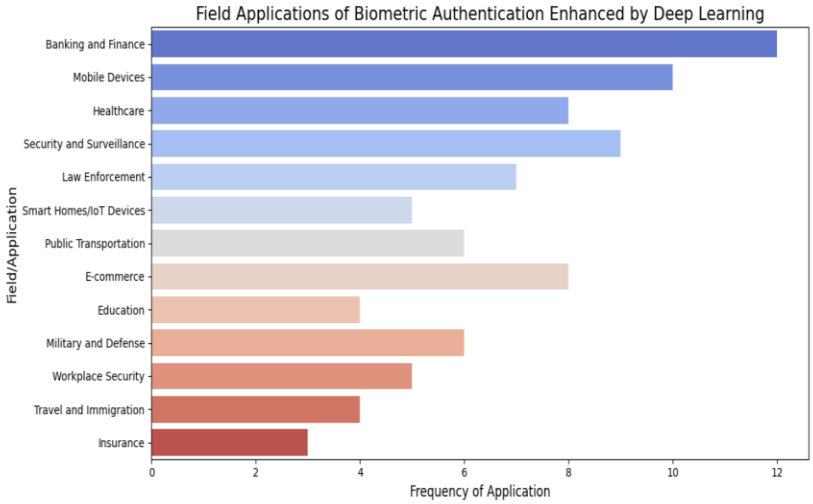

Figure 6. Results of biometric authentication enhancement by deep learning

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024

5. Conclusion

The One kind of machine learning technique called "deep learning" makes use of artificial neural networks to extract knowledge from sources. Neural networks, which draw inspiration from the brains of humans, can be applied to a wide range of applications, such as recognition of speech, identification of images, and NLP. .In this system applied deep learning to collections containing genuine and forged banknote photos, taking into account information-collecting obstacles such as operator condition changes and ambient conditions. The results are 100% classification, with clarity and recall, and F1 scores of 1.00 across both categories, indicating that the representation is excellent at distinguishing between legitimate and counterfeit materials. Because of its exceptionally precise results, capacity to generate predictions on unstructured information, and capacity to offer valuable insights into the datasets, deep learning is still becoming more and more popular. Numerous sectors are already being transformed by it. Deep learning is probably going to keep developing and have a big influence on our civilization in the future.

Acknowledgment

The author would like to expose her thanks to the Computer Science Department / College of Science / Mustansiriyah University /Baghdad-Iraq for the continuous enhancement and supporting to accomplish this research.

References

[1] S. Sett and H. Gupta, "A Biometric Security Model for the Enhancement of Data Security," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2024, pp. 1-5, IEEE.

[2] K. P. Kumar, P. K. Prasad, Y. Suresh, M. R. Babu, and M. J. Kumar, "Ensemble recognition model with optimal training for multimodal biometric authentication," *Multimedia Tools and Applications*, pp. 1-25, 2024.

[3] A. Iskandar, M. Alfonse, M. Roushdy, and E. S. M. El-Horbaty, "Biometric systems for identification and verification scenarios using spatial footsteps components," *Neural Computing and Applications*, vol. 36, no. 7, pp. 3817-3836, 2024.

[4] M. Lim, A. B. J. Teoh, and J. Kim, "Biometric feature-type transformation: Making templates compatible for secret protection," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 77-87, 2015.

[5] M. Al Rousan and B. Intrigila, "A comparative analysis of biometrics types: literature review," *Journal of Computer Science*, vol. 16, no. 12, pp. 1778-1788, 2020.

[6] T. Kattenborn, J. Leitloff, F. Schiefer, and S. Hinz, "Review on Convolutional Neural Networks (CNN) in vegetation remote sensing," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 173, pp. 24-49, 2021.

[7] L. Alzubaidi et al., "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, pp. 1-74, 2021.

[8] T. Phillips, X. Zou, F. Li, and N. Li, "Enhancing biometric-capsule-based authentication and facial recognition via deep learning," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, May 2019, pp. 141-146.

[9] S. S. Sengar, U. Hariharan, and K. Rajkumar, "Multimodal biometric authentication system using deep learning method," in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Mar. 2020, pp. 309-312, IEEE.

[10] T. Edwards and M. S. Hossain, "Effectiveness of deep learning on serial fusion based biometric systems," *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 1, pp. 28-41, 2021.

[11] A. J. Prakash, K. K. Patro, M. Hammad, R. Tadeusiewicz, and P. Pławiak, "BAED: A secured biometric authentication system using ECG signal based on deep learning techniques," *Biocybernetics and Biomedical Engineering*, vol. 42, no. 4, pp. 1081-1093, 2022.

[12] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal approach for enhancing biometric authentication," *Journal of Imaging*, vol. 9, no. 9, p. 168, 2023.

[13] R. Sharma, "Biometric Authentication using lightweight Convolutional Neural Network," in *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Feb. 2024, pp. 1-6, IEEE.

[14] S. Hendi, H. B. Taher, and K. Q. Hussein, "Advanced facial recognition with LBP-URIGL hybrid descriptors," *Pollack Periodica*, 2024.

DOI: https://doi.org/10.54216/FPA.180116
Received: July 08, 2024 Revised: October 07, 2024 Accepted: December 30, 2024