Journal of Trends and Challenges in Artificial Intelligence

Vol. 02, No. 03 (2025) 83-88, DOI: 10.61552/JAI.2025.03.003 - http://jai.aspur.rs

MULTI-MODAL BIOMETRIC AUTHENTICATION SYSTEM USING DEEP NEURAL NETWORKS

Vishakha Rawte [1]
Manjusha Khamkar
Harsha Patil
Vikas Mahandule

Received 11.07.2024.
Revised 07.08.2024.
Accepted 19.09.2024.

Keywords:

Artificial intelligence, algorithm fairness, data privacy, data security, education, ethics, management, machine learning, technology, transparency, inclusivity.

Original research

A B S T R A C T

The issue of giving authorized owners of a certain identification process safe and easy access to information and solutions is known as identity management. The primary goal in ascertaining an individual's identity is the implementation of the secured identification feature. Tokens, access cards, PINs, keys, and passwords are a few examples of private identifying components that are used often yet can be lost, stolen, cracked, copied, or posted. It is essential to comprehend biometrics-based identification in order to prevent the drawbacks. Not only can intracategorical changes affect nonuniversality, but they also affect sound and false strikes. Multimodal biometrics are utilized to remove the episodes, which are essentially a collection of countless modalities. Fingerprints and palmprints can be used as sources of authentication. Using this technique, rich neural communities (DNN) were surely projected for fine-grained attribute extraction and item detection. Multimodal biometric solutions are designed to fulfill the rigorous needs of the industry due to the limits of unimodal biometric structures, which lead to high delivery demands, restricted talent splitting, and considerable False Acceptance Rates (FAR) and False Rejection Rates (FRR). In reality, values of Euclidean distance are used for tiny details. The suggested method is highly safe and attains a better recognition speed just while dealing with loud issues.

1. INTRODUCTION

Compared to conventional single-modal systems, Multi-Modal Biometric Authentication Systems offer improved accuracy and resilience, marking a significant advancement in the field of security (Dargan & Kumar, 2020; Samatha & Madhavi, 2024). Through the utilization of several biometric characteristics, including voice, iris patterns, fingerprints, and face recognition, these systems offer a more dependable approach to identity verification (Alsaadi 2015; Bhattacharyya et al., 2009). Combining the strengths and limitations of each biometric modality increases the system's resistance to spoofing efforts and lowers the possibility of false positives or negatives (Wang et al., 2021). The performance of these systems has been further enhanced by the use of Deep Neural Networks (DNNs) (Capra et al., 2020; Galván & Mooney, 2021; Pan et al., 2020). Because DNNs can learn intricate patterns from vast datasets, they are especially well-suited for biometric identification because they allow for more accurate feature extraction and categorization (Dalvi et al., 2021). These networks are capable of managing the high-dimensional, biometric data's noisy character, enhancing the system's overall robustness and accuracy (Rusia & Singh, 2023).

[1] Corresponding author: Vishakha Rawte
Email: rawtevishakha@gmail.com

DNNs improve several elements of multi-modal biometric systems, such as feature extraction, classification precision, and data variability adaptation (Gona & Subramoniam, 2022; Shende et al., 2024). DNNs can automatically extract useful features from biometric data by learning complex patterns, which eliminates the need for human feature engineering (Aizat et al., 2020). In multi-modal systems, where various data kinds necessitate distinct processing methods, this feature is essential (Wang, 2021). Furthermore, because of DNNs' flexibility, these systems may continuously get better when they are exposed to fresh data, which increases their effectiveness in dynamic contexts (Yao et al., 2021). DNNs may be used to fuse numerous biometric modalities at different levels, such as the sensor, feature, score, and decision levels. Every fusion technique has a different set of benefits, ranging from making real-time processing easier to enhancing data richness.

Notwithstanding the benefits, issues including interoperability, computational complexity, and data privacy still exist. The gathering and storing of biometric data raises privacy issues, hence strong security measures are required to safeguard user data. Real-time applications may be limited by the computational needs of DNNs, particularly in multi-modal systems where substantial processing power is needed. Furthermore, it might be challenging to guarantee smooth integration and compatibility across various biometric modalities and systems. Future work may concentrate on creating DNN architectures that are more effective, improving the interpretability of the system, and investigating novel, less intrusive biometric modalities. Concerns about privacy may also be addressed by developments in federated learning and privacy-preserving methodologies. In the end, Deep Neural Network-Based Multi-Modal Biometric Authentication Systems present a viable method for raising identity verification security and accuracy, with the potential to greatly improve the practicality and dependability of biometric verification techniques.

2. METHODOLOGY

2.1 Data Collection and Preprocessing

Biometric Data Acquisition: To ensure a representative and varied dataset, gather information from a variety of biometric sources, including voice recordings, facial photos, and fingerprints.

Prior to processing: Utilize approaches for alignment, normalization, and noise reduction to guarantee that the biometric data is clear, consistent, and prepared for analysis. This might involve compensating for variances in fingerprint scans, resizing photos, and filtering out background noise from voice recordings.

2.2 Feature Extraction

Modality-Specific Feature Extraction: Use the relevant methods to extract unique features for each biometric modality:

Convolutional Neural Networks (CNNs) may be used for facial recognition in order to extract characteristics from faces, including edges, contours, and textures.

Fingerprint Recognition: To find distinctive patterns in fingerprint data, apply Gabor filters or minutiae extraction techniques.

Voice Recognition: To extract vocal characteristics, use spectrogram analysis or Mel-Frequency Cepstral Coefficients (MFCCs).

2.3 Deep Neural Network Design

Model Architecture: Create and set up distinct DNN models for every biometric modality. From the retrieved characteristics, these models need to be able to learn intricate patterns and representations.

Fusion Layer: Construct a fusion layer by including the modality-specific models' outputs. To provide a cohesive depiction, this layer integrates the characteristics from every modality.

Categorization Layer: Include a last layer of categorization that uses the combined features to identify the person.

2.4 Training and Optimization

Training Procedure: Using labeled biometric data and methods like stochastic gradient descent and backpropagation, train each modality-specific DNN. For a well-generalized model, use a big and varied dataset.

Fusion Model Training: To maximize system performance, train the fusion layer and classification layer using the combined feature set.

Adjusting Hyperparameters: To improve model performance, fine-tune hyperparameters like learning rate, batch size, and number of layers. Use methods like as cross-validation to avoid overfitting.

2.5 Model Evaluation and Testing

Performance measures: Use measures like F1-score, recall, accuracy, and precision to assess the system's performance. Think about measures that are special to biometrics, such as Receiver Operating Characteristic (ROC) curves and Equal Error Rate (EER).

Test the system's robustness against possible spoofing attempts and fluctuations in biometric data, such as shifts in illumination for facial recognition or background noise for voice recognition.

2.6 System Integration and Deployment

Processing in Real-Time: Combine the learned DNN models with a real-time authentication system to effectively handle and verify users' biometric information.

User Interface: Create an intuitive user interface that facilitates smooth communication with the authentication system, guaranteeing usability without sacrificing security.

Security Measures: To safeguard biometric data and stop illegal access, put in place extra security measures like encryption and secure data storage.

2.7 Continuous Monitoring and Improvement

Monitoring: Keep an eye on the system's functionality in real-world situations and collect information on any malfunctions or erroneous acceptances or rejections.

Model Updates: To increase accuracy and adjust to new threats or modifications in biometric patterns, retrain and update the DNN models on a regular basis using fresh data.

User Input: Take into account user input to improve the system's usability and fix any problems with the authentication procedure.

The suggested method is predicated on multimodal biometrics, which leverages fingerprint and palm print biometrics as authentication sources. Figure 1 displays multimodal biometrics with palm prints and fingerprints. They are regarded as some of the most effective, trustworthy, and popular biometrics available.

Figure 1. Finger and palm print

The methods used by the Automated Fingerprint Identification System (AFIS) are frequently predicated on the amounts of particular chemicals.

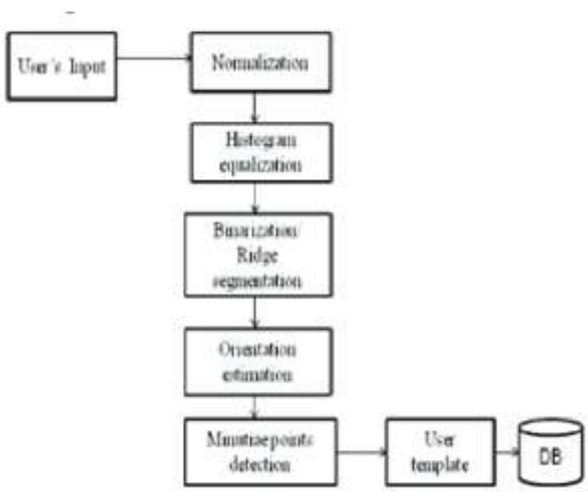

Figure 2. Flow Sequence of Image Acquisition

Marginalia, core lines, wrinkles, and other features of a fingerprint vary depending on what particular information can be recovered. Fingerprints and palm prints are considered to be two of the most wonderful ways to identify a property because of the abundance of floor information they provide. Artificial Neural Networks (ANN) are one of several Soft Computing methods for multimodal biometric identification.

An 8-bit dim scope image is directly converted into a two-fold image with one share for valleys and zero share for tips using binaryization. Advantage segmentation is completed in order to determine advantage finishing, edge department, and differentiate return on original capital expenditure. In reality, the launch procedure is used during such time to split the parallel image into w * w squares. Figure 2 shows the picture security information stream chart.

The Features Are Removed Identifying the appropriate trait to extract from the brother QL is without a doubt the most crucial endeavor. In reality, DNN is used to extract elements (Figure 3). This algorithm is unique in that it is made up of many neurons, or units, connected in tiers. There is just one way that information is shared, and it lacks even sectors and cycles. The information concentrations are really divided by DNN, which comes from the edges, valleys, and wrinkles, as shown in Fig. 3. Deep learning networks and rule lines are really realized by deeper hidden level neural networks, that is, the number of hub levels where information must pass within a multistep instance acknowledgment process. The initial Perceptrons and other neural network iterations were crude, deriving up to one veiled level in the center, one yield level, and one piece of information. "Deep" learning consists of two stages: yield and counting information. Therefore, "deeply" is more than simply a gimmick to make computations seem as though they run into Tune and Sartre in environments that you haven't yet seen. It's a phrase selected with care that expresses something more profound than a person's shadow.

Minor Interactions the Multilayer Perceptron (MLP) method is used to differentiate between the details, whether they are on edge finishing or advantage department. It consists of several levels, including covered levels like feedback and yield levels. The networking is split using the Back propagation method, often referred to as the cooking or mastering process. The picture is isolated into a 3 by 3 windowpane square measurement as part of a community procedure; if the windowpane is on specifications, the self-esteem is actually one or even a different zero. If there is one and only one neighbor with self-esteem within a pixel worth, the details component will undoubtedly be on the winning side. In the distant scenario when the center pixel's value is if a person is genuinely one and only has three self-esteem neighbors, then the advantage department is the details component. Euclidean splitting up with long final is really found between certain concentrations and stored in a repository.

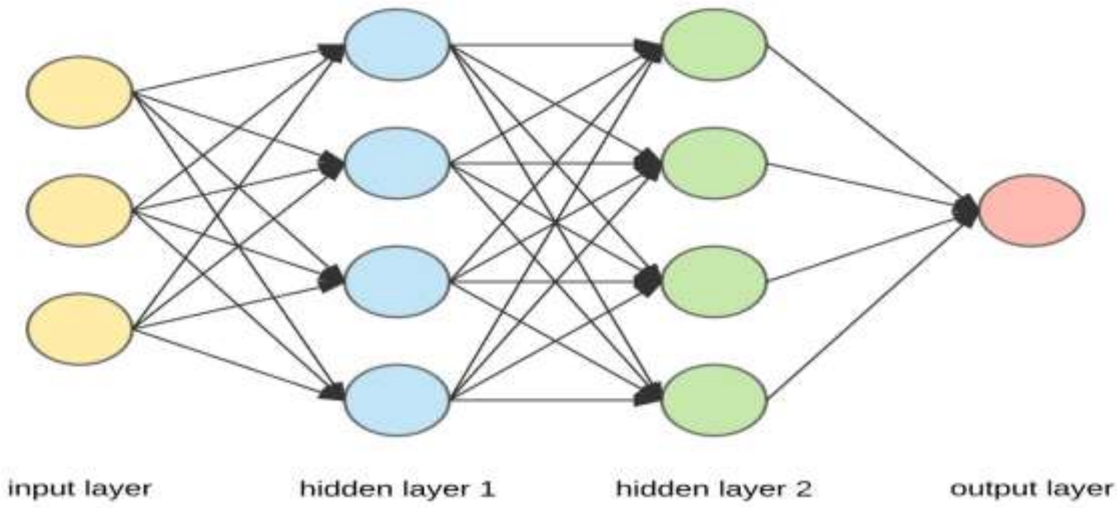

Figure 3. A Sample DNN

3. DISCUSSSION

The structure consists of two phase forms: Identification and Enlistment (Figure 4). The system design for the Particulars Coordinating Based Individual Identification System is displayed in throughout the hiring procedure, the candidate enlists both their fingerprint and palm print. The characteristics that are retrieved from the particular concentrations that are collected include peaks, troughs, primary clusters, wrinkles, and furrows. Using details recognition, the information focuses are divided into end and bifurcation (edge endings) concentrates. Right now step, the information concentrations and the Euclidean splitting up esteems are calculated and saved within the repository simultaneously. During the identification procedure, a fingerprint and a palm print are really taken. This kind of process keeps on until details are identified. The details identified in the supplied data and the camera kept inside the repository are evaluated to determine the coordination Score esteems when details are coordinated. The way the decision is carried out is influenced by the coordinating score. Should the prospect's coordination score surpass their advantage value—an unusual scenario—they will be recognized and verified. Furthermore, the prospect receives both rejection and unapproval.

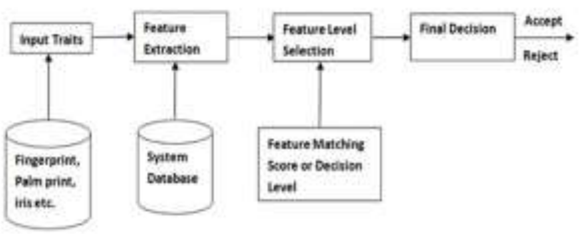

Figure 4. System Architecture

Matlab is used to select and store all fingerprint and palmprint images, which are then stored in an MS Access repository. At this stage of the identification process, the images are packed for image enhancement, which includes the execution of advantage launch, standardization, and histogram adaptation. The details focus are truly separated in the superior images. The community procedure is used to carry out the bifurcation and advantage ends within the first coat level. In reality, euclidean breaking up calculation is carried out. By calculating the scores and examining the validation, the information esteems coordination are finished. Gabor channel switches are offered for both actual components and Imaginary component, as well as FAR and FRR, are impacted by the quantity of evaluations. It has been noted that there are several limitations to the delivery of the suggested techniques, Tar, including limitations on the fake accept and fake refuse speeds. Consequently, the suggested strategy is predicated on techniques to enhance the accuracy of distinction with respect to fraudulent as well as authentic consumers, using the FAR and FRR estimates.

4. CONCLUSION

By merging many biometric modalities, such as voice, facial, and fingerprint identification, a Multi-Modal Biometric Authentication System employing Deep Neural Networks (DNNs) provides a reliable and safe method of identity verification. By using DNNs, the system may improve accuracy and resilience against spoofing attempts by learning intricate patterns and characteristics from a variety of biometric data. The system enhances overall security and user experience by lowering the possibility of false positives and negatives through the integration of several modalities. This cutting-edge method is especially well-suited for uses where maximum security and dependability are critical.

A Deep Learning-Based Multi-Modal Biometric Authentication System The usage of biometrics is essential for house identification. The implementation of multimodal biometrics techniques consistently meets the goal of creating a secure unique identifying device. Fingerprints and palm prints with extensive floor information yield the highest accuracy. DNN-based differentiation becomes an improved identification cost. The proposed technique enhances the remarkable delivery and distinction accuracy in terms of new elements when coupled with the collections. The results yield far higher accuracy for your proposed method.

References:

Aizat, K., Mohamed, O., Orken, M., Ainur, A., & Zhumazhanov, B. (2020). Identification and authentication of user voice using DNN features and i-vector. *Cogent Engineering*, *7*(1), 1751557.

Alsaadi, I. M. (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: A review. *International Journal of Scientific & Technology Research*, *4*(12), 285-289.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, *2*(3), 13-28.

Capra, M., Bussolino, B., Marchisio, A., Masera, G., Martina, M., & Shafique, M. (2020). Hardware and software optimizations for accelerating deep neural networks: Survey of current trends, challenges, and the road ahead. *IEEE Access*, *8*, 225134-225180.

Dalvi, C., Rathod, M., Patil, S., Gite, S., & Kotecha, K. (2021). A survey of ai-based facial emotion recognition: Features, ml & dl techniques, age-wise datasets and future directions. *Ieee Access*, *9*, 165806-165840.

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*, 113114.

Galván, E., & Mooney, P. (2021). Neuroevolution in deep neural networks: Current trends and future challenges. *IEEE Transactions on Artificial Intelligence*, *2*(6), 476-493.

Gona, A., & Subramoniam, M. (2022). Convolutional neural network with improved feature ranking for robust multi-modal biometric system. *Computers and Electrical Engineering*, *101*, 108096.

Pan, Y., Fu, M., Cheng, B., Tao, X., & Guo, J. (2020). Enhanced deep learning assisted convolutional neural network for heart disease prediction on the internet of medical things platform. *IEEE Access*, *8*, 189503-189512.

Rusia, M. K., & Singh, D. K. (2023). A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. *Multimedia Tools and Applications*, *82*(2), 1669-1748.

Samatha, J., & Madhavi, G. (2024). Securesense: Enhancing person verification through multimodal biometrics for robust authentication. *Scalable Computing: Practice and Experience*, *25*(2), 1040-1054.

Shende, S. W., Tembhurne, J. V., & Ansari, N. A. (2024). Deep learning based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions. *Multimedia Tools and Applications*, 1-43.

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, *188*, 103080.

Wang, Y. (2021). Survey on deep multi-modal data analytics: Collaboration, rivalry, and fusion. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *17*(1s), 1-25.

Yao, D., Xiang, L., Wang, Z., Xu, J., Li, C., & Wang, X. (2021). Context-aware compilation of dnn training pipelines across edge and cloud. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *5*(4), 1-27.

Vishakha Rawte
Mit Acsc Alandi Pune,
India.
rawtevishakha@gmail.com

Harsha Patil
Mit Acsc Alandi Pune
India.
hvpatil@mitacsc.ac.in
ORCID: 0000-0001-6519-9987

Manjusha Khamkar
Mit Acsc Alandi Pune,
India.
manjushakhamkar02@gmail.com

Vikas Mahandule
Mit acsc Alandi Pune
India.
vnmahandule@mitacsc.ac.in
ORCID: 0009-0007-5415-9227