Modified Deep Learning Model for Improved Multimodal Authentication System

V. Vaishnavi, Y. Akhila, R. Anusha UG Student,
M. Premchender Assistant Professor,
Department of Information Technology, Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammaguda, Secunderabad, Telangana, India

ABSTARCT
The acceleration of the emergence of modern technological resources in recent years has given rise to a need for accurate user recognition systems to restrict access to the technologies. The biometric recognition systems are the most powerful option to date. Biometrics is the science of establishing the identity of a person through semi or fully automated techniques based on behavioural traits, such as voice or signature, and/or physical traits, such as the iris and the fingerprint. The unique nature of biometrical data gives it many advantages over traditional recognition methods, such as passwords, as it cannot be lost, stolen, or replicated. Biometric traits can be categorized into two groups: extrinsic biometric traits such as iris and fingerprint, and intrinsic biometric traits such as palm. Extrinsic traits are visible and can be affected by external factors, while the intrinsic features cannot be affected by external factors. In general, the biometric recognition system consists of four modules: sensor, feature extraction, matching, and decision-making modules. There are two types of biometric recognition systems, unimodal and multimodal. The unimodal system uses a single biometric trait to recognize the user. While unimodal systems are trustworthy and have proven superior to previously used traditional methods, but they have limitations. These include problems with noise in the sensed data, non-universality problems, vulnerability to spoofing attacks, intra-class, and inter-class similarity. Basically, multimodal biometric systems require more than one trait to recognize users. They have been widely applied in real-world applications due to their ability to overcome the problems encountered by unimodal biometric systems. In multimodal biometric systems, the different traits can be fused using the available information in one of the biometric system's modules. The advantages of multimodal biometric systems over unimodal systems have made them a very attractive secure recognition method. Therefore, with the increasing demand for information security and security regulations all over the world, biometric recognition technology has been widely used in our everyday life. In this regard, multimodal biometrics technology has gained interest and became popular due to its ability to overcome several significant limitations of unimodal biometric systems. In this project, an enhanced multi-modal biometric authentication system is presented using modified deep learning model to authenticate persons using different biometric features such as Face, Iris, Finger, Palm and Ear.
Keywords: biometric authentication, multi-modal system, feature extraction, deep learning.

1. INTRODUCTION
Individual biometric personalities like iris, DNA, Voice recognition, fingerprint, retina, and finger vein can be labeled as unibiometric systems because it relies on a single biometric source for recognition. Unibiometric systems have some disadvantages like erratic biometric basis due to sensor, low quality of specific biometric trait of the authentic user. In addition, high-security applications and large-scale civilian recognition systems place stringent accuracy necessities that cannot be met by obtainable unibiometric systems. To deal with the requirements of such applications, it is necessary to move, beyond the traditional pattern of biometric recognition usually based on a single source of biometric information and consider systems that consolidate evidence from multiple biometric sources for recognition. However, the consolidation of information presented by these multiple cures can result in a more accurate determination or certification of individuality. Hence biometric systems are designed to recognize a person based on information acquired from multiple biometric sources. Such systems are referred as multibiometric systems are expected to be more accurate compared to unibiometric

systems that rely on a particular segment of biometric affirmation. Accuracy enhancement, which is the primary motivation for using multibiometric systems happens due to two reasons. Firstly, the fusion of multiple biometric sources effectively increases the dimensionality of the feature space and reduces the overlap between the feature distributions of dissimilar individuals. In addition to that, a combination of multiple biometrics is more exclusive to an individual than a single biometric trait. Due to noise, imprecision, or inherent drift (caused by factors like ageing) in a subset of the biometric sources can be compensated by the discriminatory information provided by the remaining sources. In addition to accuracy, multimodal biometric systems may also offer the following advantages over unibiometric systems viz., alleviate the non-universality problem and reduce the failure to enrol errors, provide a degree of flexibility in user authentication, enable the search of a large biometric database in a computationally efficient manner and increase the resistance to spoofing attacks. Multimodal biometric implemented based MLCNN. Proposed biometric traits like fingerprint, retina and finger vein were combined.

2. LITERATURE SURVEY

Ryu et al. provided a systematic survey of existing literature on CMBA systems, followed by analysis to identify, and discuss current research and future trends. The study has found that many diverse biometric characteristics are used for multimodal biometric authentication systems. Many of the studies in the literature reviewed apply supervised learning approaches as a classification technique, and score level fusion is predominantly used as a fusion model. The review has determined however that there is a lack of comparative analysis on CMBA design in terms of combinations of biometric types (behavioural only, physiological only, or both), machine learning algorithms (unsupervised learning and semi-supervised learning), and fusion models.
Hammad et al. proposed a secure multimodal biometric system that uses convolution neural network (CNN) and Q-Gaussian multi support vector machine (QG-MSVM) based on a different level fusion. This framework developed two authentication systems with two different level fusion algorithms: a feature level fusion and a decision level fusion. The feature extraction for individual modalities is performed using CNN. systems were tested on several publicly available databases for ECG and fingerprint.
Sengar et al. projected rich neural community (DNN). The confinements of unimodal biometric structure lead to substantial False Acceptance Rate (FAR) along with False Rejection Rate (FRR), limited splitting up skill, top bound within delivery therefore the multimodal biometric product is designed to satisfy the strict delivery demands. For minutiae corresponding, values of Euclidean distance are used. The better identification pace is attained throughout the suggested procedure & it's extremely safe only in loud problem.
Joseph et al. proposed a multimodal authentication system by fusing the feature points of fingerprint, iris, and palm print traits. Each trait has undergone the following procedures of image processing techniques such as pre-processing, normalization and feature extraction. From the extracted features, a unique secret key is generated by fusing the traits in two stages. False Acceptance Rate (FAR) and False Rejection Rate (FRR) metrics are used to measure the robustness of the system. This performance of the model is evaluated using three standard symmetric cryptographic algorithms such as AES, DES, and Blowfish. This proposed model provides better security and access control over data in cloud environment.
Choudhary et al. given an overview of multiple biometrics used for authentication. Focusing on challenges in multimodal biometrics practiced through various fusion levels and different algorithms, this paper discussed scope of further research in this field. Majorly, the template security issue of multimodal biometrics is emphasized with various techniques to protect the crucial asset of human identity.
Wu et al. proposed and implemented LVID, a multimodal biometrics authentication system on smartphones, which resolved the defects of the original systems by combining the advantages of lip

movements and voice. LVID simultaneously captures these two biometrics with the built-in audio devices on smartphones and fuses them at the data level. The reliable and effective features are then extracted from the fused data for authentication. LVID is practical as it requires neither cumbersome operations nor additional hardware's but only a speaker and a microphone that are commonly available on smartphones.
Zhang et al. implemented DeepKey with a live deployment in the university and conduct extensive empirical experiments to study its technical feasibility in practice. DeepKey achieved the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) of 0 and 1.0%, respectively. The preliminary results demonstrated that DeepKey is feasible, showed consistent superior performance compared to a set of methods, and has the potential to be applied to the authentication deployment in real-world settings.
Rahiem et al. adopted Multi-Canonical Correlation Analysis (MCCA). This framework combined the two biometric systems based on ECG and finger vein into a single multimodal biometric system using feature and score fusion. The performance of the proposed system is tested on two finger vein (TW finger vein and VeinPolyU finger vein) databases and two ECG (MWM-HIT and ECG-ID) databases. Experimental results revealed the improvement in terms of authentication performance with Equal Error Rates (EERs) of 0.12% and 1.40% using feature fusion and score fusion, respectively. Therefore, the proposed biometric system is effective in performing secure authentication and assisting the stakeholders in making accurate authentication of users.
Zhang et al. designed and developed an efficient Android-based multimodal biometric authentication system with face and voice. Considering the hardware performance restriction of the smart terminal, including the random-access memory (RAM), central processing unit (CPU) and graphics processor unit (GPU), etc., which cannot efficiently accomplish the tasks of storing and quickly processing the large amount of data, a face detection method is introduced to efficiently discard the redundant background of the image and reduce the unnecessary information. Furthermore, an improved local binary pattern (LBP) coding method is presented to improve the robustness of the extracted face feature. We also improve the conventional endpoint detection technology, i.e., the voice activity detection (VAD) method, which can efficiently increase the detection accuracy of the voice mute and transition information and boost the voice matching effectiveness.
Ahmed et al. proposed an AI-based multimodal biometric authentication model for single and group-based users' device-level authentication that increases protection against the traditional single modal approach. To test the efficacy of the proposed model, a series of AI models are trained and tested using physiological biometric features such as ECG (Electrocardiogram) and PPG (Photoplethysmography) signals from five public datasets available in Physionet and Mendeley data repositories. The multimodal fusion authentication model showed promising results with 99.8% accuracy and an Equal Error Rate (EER) of 0.16.

3. EXISTING SYSTEM

ML falls under the larger canvas of Artificial Intelligence. ML seeks to build intelligent systems or machines that can automatically learn and train themselves through experience, without being explicitly programmed or requiring any human intervention. In this sense, ML is a continuously evolving activity. It aims to understand the data structure of the dataset at hand and accommodate the data into ML models that can be used by companies and organizations. Following are the benefits of ML.

- Enhanced decision-making: ML uses advanced algorithms to improve the decision-making process capacity. It facilitates innovative models and business services simultaneously. It provides a deep understanding of the variations and types of data patterns. You can determine which step to take next based on the variations and data patterns.

- Increases business productivity: It improves the business process and productivity, contributing to business growth. It helps you to adapt to the changing situations at workplaces quickly. The data continue to be updated daily. So, the work environment, too, keeps on changing quickly. ML reduces the chances of error occurrence by half. Hence, it boosts business productivity. This aspect is important to consider when carrying out deep learning vs neural network.
- Removes manual data entry: One of the most common concerns in many organizations is the usage of duplicate records. ML algorithms use predictive models that significantly avoid any errors caused by manual data entry. The corresponding programs use the discovered data to enhance these processes. Hence, the employees can save time to focus on other important business tasks.
- Guarantees customer satisfaction: The ML algorithms are uniquely designed to continue attaining experience with time. They are accurate and efficient. These algorithms improve the machines' decision-making skills. ML can anyhow find a way to make accurate decisions or predictions, although the data is overwhelming and ever-increasing. It benefits businesses with the latest market opportunities related to revenue. As a result, it can satisfy the customers' expectations and boost your business' sales in less time. Moreover, it can quickly recognize threats in the market. You can compare deep learning vs neural networks based on this aspect to have a clear judgment.
- Provides product recommendation: Unsupervised research assists in the development of suggestion systems depending on goods. Currently, most e-commerce platforms use ML to provide product recommendations. ML algorithms use the consumers' purchasing experience to balance it with the assets' huge inventory. This helps in detecting secret trends and connects identical products. Finally, these goods are recommended to the consumers.
- Detects spam: ML is widely used for spam detection. It uses spam filters to identify spam and phishing communications.
- Improves network security: ML improves an organization's security. It helps organizations to develop new systems capable of quickly and efficiently recognizing unknown threats. It can track abnormalities present in network activity and automatically execute relevant actions. When the ML algorithm is used for self-training, it removes manual research and analysis. So, it enhances the organization's network security. Many deep learning neural networks are also used for this purpose.
- Simplifies business analysis: ML is used in business analysis that involves huge volumes of precise and quantitative historical data. It is widely used for algorithmic trading, portfolio management, fraud detection, and lending in finance. The future ML applications for finance will entail Chatbots and a few other interfaces for improving customer service, security, and sentiment analysis. Many neural networks and deep learning algorithms are also used to streamline finance analysis.

3.1 Disadvantages

- ML Model makes decisions based on what it has learnt from the data. As a result, while ML models may learn from data, they may need some human interaction in the early stages.
- Moreover, its performance is poor with large dataset.

4. PROPOSED SYSTEM

In this project we are designing Modified Deep Learning Neural Networks (MLDNN) algorithms to authenticate persons using different biometric features such as Face, Iris, Finger, Palm and Ear. Hence this algorithm is called as Multimodal. To implement this algorithm, we have applied KLDA features reduction algorithm to reduce biometric image features and then input to MLDNN algorithm to train a model to authenticate persons. MLDNN algorithm will further extract FSL features while training itself.

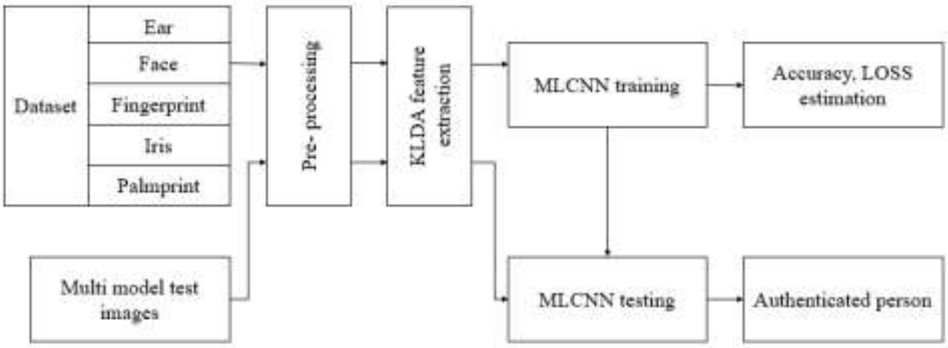


Fig. 1: Block diagram of proposed system.

4.1 KLDA

The principle of KLDA can be illustrated in below Fig.2. Owing to the severe non-linearity, it is difficult to directly compute the discriminating features between the two classes of patterns in the original input space (left). By defining a non-linear mapping from the input space to a high-dimensional feature space (right), we (expect to) obtain a linearly separable distribution in the feature space. Then LDA, the linear technique, can be performed in the feature space to extract the most significant discriminating features. However, the computation may be problematic or even impossible in the feature space owing to the high dimensionality. By introducing a kernel function which corresponds to the non-linear mapping, all the computation can conveniently be carried out in the input space. The problem can be finally solved as an eigen-decomposition problem like PCA, LDA and KPCA.

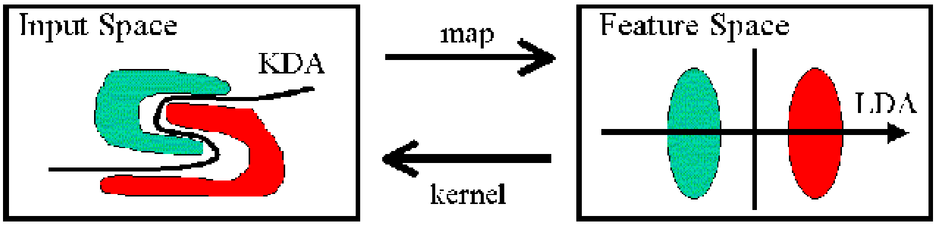


Fig. 2: Kernel discriminant analysis.

4.2 MLCNN

According to the facts, training and testing of CNN involves in allowing every source data via a succession of convolution layers by a kernel or filter, rectified linear unit (ReLU), max pooling, fully connected layer and utilize SoftMax layer with classification layer to categorize the objects with probabilistic values ranging from.

Layer description

Convolution layer is the primary layer to extract the features from a source image and maintains the relationship between pixels by learning the features of image by employing tiny blocks of source data. It's a mathematical function which considers two inputs like source image $I(x, y, d)$ where x and y denotes the spatial coordinates i.e., number of rows and columns. d is denoted as dimension of an image (here d=3 since the source image is RGB) and a filter or kernel with similar size of input image and can be denoted as $F(k_x, k_y, d)$..

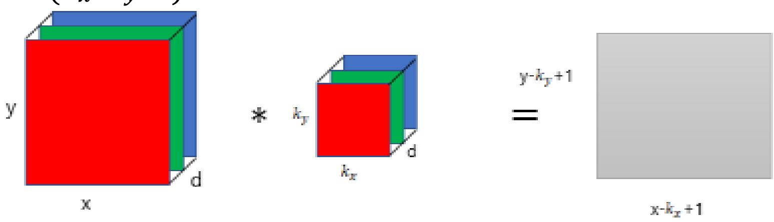


Fig. 3: Representation of convolution layer process.

The output obtained from convolution process of input image and filter has a size of $C\left((x-k_x+1),(y-k_y+1),1\right)$, which is referred as feature map. Let us assume an input image with a size of 5×5 and the filter having the size of 3×3. The feature map of input image is obtained by multiplying the input image values with the filter values.

$$\underset{\text{5x5 image}}{\begin{bmatrix}1&1&1&0&0\\0&0&1&1&1\\1&1&0&0&1\\0&0&0&1&1\\1&1&1&0&0\end{bmatrix}} * \underset{\text{3x3 kernel}}{\begin{bmatrix}1&0&1\\0&1&0\\1&0&1\end{bmatrix}}$$

(a)

$$\underset{\text{5x5 image}}{\begin{bmatrix}1&1&1&0&0\\0&0&1&1&1\\1&1&0&0&1\\0&0&0&1&1\\1&1&1&0&0\end{bmatrix}} * \underset{\text{3x3 kernel}}{\begin{bmatrix}1&0&1\\0&1&0\\1&0&1\end{bmatrix}} = \underset{\text{Feature map}}{\begin{bmatrix}3&3&3\\2&2&3\\3&2&3\end{bmatrix}}$$

(b)

Fig. 4: Example of convolution layer process (a) an image with size 5×5 is convolving with 3×3 kernel (b) Convolved feature map.

ReLU layer

Networks those utilizes the rectifier operation for the hidden layers are cited as rectified linear unit (ReLU). This ReLU function $\mathcal{G}(\cdot)$ is a simple computation that returns the value given as input directly if the value of input is greater than zero else returns zero. This can be represented as mathematically using the function $max(\cdot)$ over the set of 0 and the input x as follows:

$$\mathcal{G}(x) = \max\{0, x\}$$

Max pooing layer

This layer mitigates the number of parameters when there are larger size images. This can be called as subsampling or down sampling that mitigates the dimensionality of every feature map by preserving the important information. Max pooling considers the maximum element form the rectified feature map.

Advantages of proposed system

- CNNs do not require human supervision for the task of identifying important features.
- They are very accurate at image recognition and classification.
- Weight sharing is another major advantage of CNNs.
- Convolutional neural networks also minimize computation in comparison with a regular neural network.
- CNNs make use of the same knowledge across all image locations.

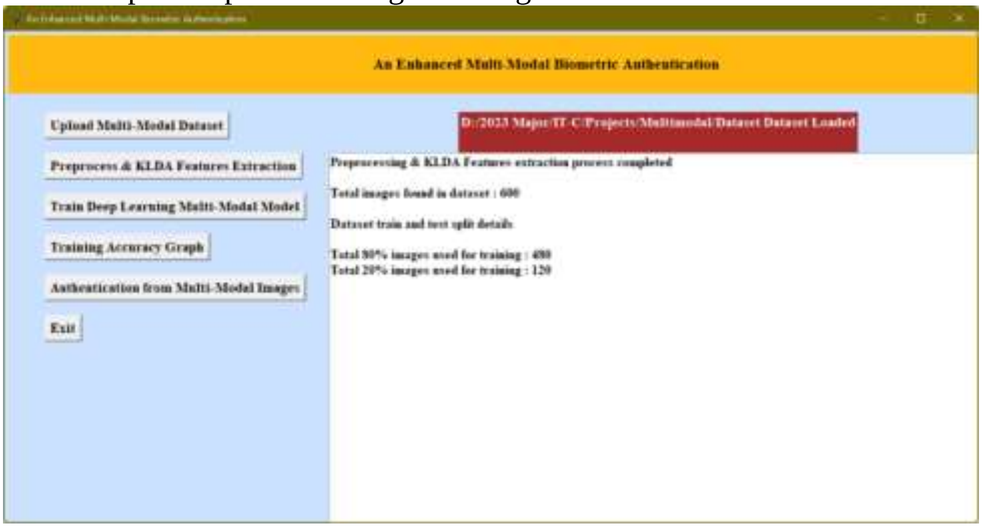
5. RESULTS AND DISCUSSION

To implement this project, we have designed following modules.

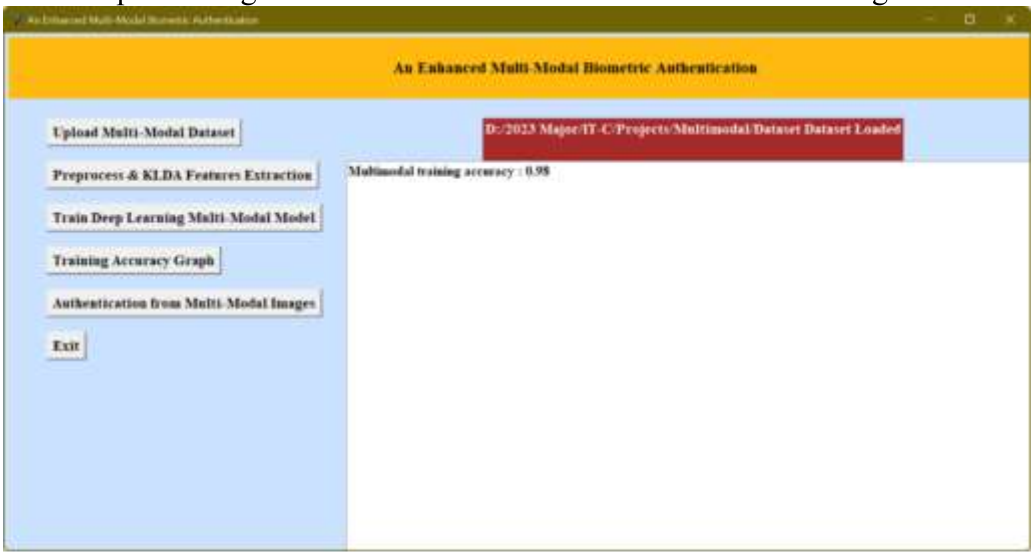
1) Upload Multi-Modal Dataset: using this module we will upload dataset to application.
2) Preprocess & KLDA Features Extraction: using this module we will read all images from dataset and then apply preprocessing technique such as resizing image, normalize pixels and then apply KLDA algorithm to extract features.
3) Train Deep Learning Multi-Modal Model: we will input extracted features to MLDNN algorithm to train authentication model.
4) Training Accuracy Graph: using this module we will plot MLDNN training and loss graph.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

5) Authentication from Multi-Modal Images: using this module we will upload folder with 5 different images such as ear, face, finger, iris and palm and then Multimodal MLDNN algorithm will predict person from given images.

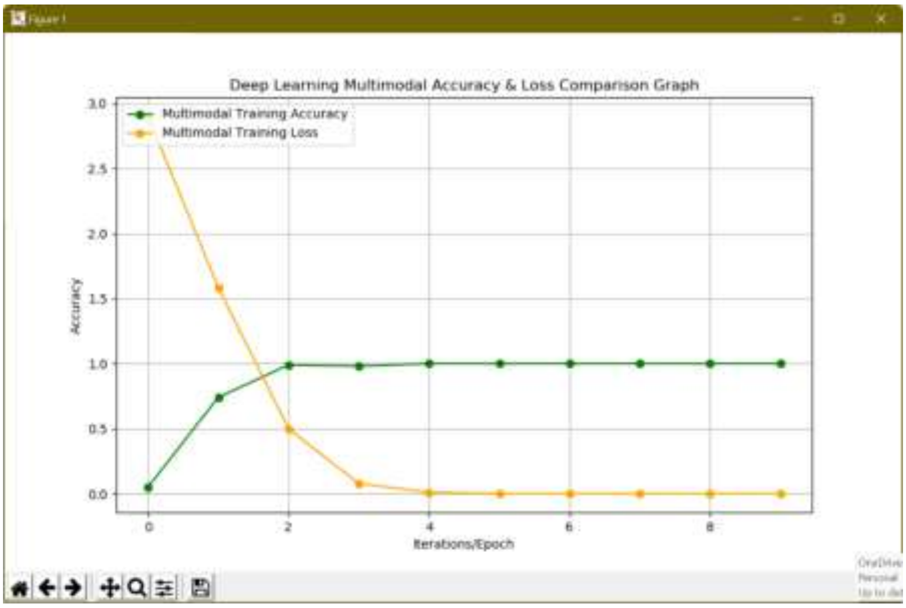


In above screen application processed all 600 images and then split dataset into train and test and now click on 'Train Deep Learning Multi-Modal Model' button to train model and get below output



In above screen model is trained and we got model accuracy as 98% and now click on 'Training Accuracy Graph' button to get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023



In above graph x-axis represents epoch number and y-axis represents accuracy and loss values and green line represents accuracy and yellow line represents LOSS value and in above graph we can see with each increasing epoch accuracy got increase and loss got decrease. Now click on 'Authentication from Multi-Modal Images' button to upload folder with face, finger, iris, palm and ear and get below output.

In above screen uploaded multimodal images are authenticated as person ID 4 and similarly you can upload other images and test.

In above screen multi modal images authenticated as person ID 6.

6. CONCLUSION AND FUTURE WORK

With the increasing demand for information security and security regulations all over the world, biometric recognition technology has been widely used in our everyday life. In this regard, multimodal biometrics technology has gained interest and became popular due to its ability to overcome several significant limitations of unimodal biometric systems. In this project, an enhanced multi-modal biometric authentication system is presented using MLCNN training and testing model to authenticate persons using different biometric features such as Face, Iris, Finger, Palm and Ear. Future work can be further extended by accurately modeling feature extraction techniques and managing the database more effectively and evaluating the matching methodology and its performance of biometric system using different level of fusion.

REFERENCES

[1] R. Ryu, S. Yeom, S. -H. Kim and D. Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," in IEEE Access, vol. 9, pp. 34541-34557, 2021, doi: 10.1109/ACCESS.2021.3061589.

[2] M. Hammad, Y. Liu and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint," in IEEE Access, vol. 7, pp. 26527-26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[3] S. S. Sengar, U. Hariharan and K. Rajkumar, "Multimodal Biometric Authentication System using Deep Learning Method," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 309-312, doi: 10.1109/ESCI48226.2020.9167512.

[4] Joseph, T., Kalaiselvan, S.A., Aswathy, S.U. et al. RETRACTED ARTICLE: A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. J Ambient Intell Human Comput 12, 6141–6149 (2021). https://doi.org/10.1007/s12652-020-02184-8

[5] S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1062-1069, doi: 10.1109/ICOEI.2019.8862563.

[6] L. Wu, J. Yang, M. Zhou, Y. Chen and Q. Wang, "LVID: A Multimodal Biometrics Authentication System on Smartphones," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1572-1585, 2020, doi: 10.1109/TIFS.2019.2944058.

[7] X. Zhang, L. Yao, C. Huang, T. Gu, Z. Yang, and Y. Liu. 2020. DeepKey: A Multimodal Biometric Authentication System via Deep Decoding Gaits and Brainwaves. ACM Trans. Intell. Syst. Technol. 11, 4, Article 49 (August 2020), 24 pages. https://doi.org/10.1145/3393619

[8] Rahiem, B.A., El-Samie, F.E.A. & Amin, M. Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. Multimedia Systems 28, 1325–1337 (2022). https://doi.org/10.1007/s00530-021-00810-9

[9] X. Zhang, D. Cheng, P. Jia, Y. Dai and X. Xu, "An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice," in IEEE Access, vol. 8, pp. 102757-102772, 2020, doi: 10.1109/ACCESS.2020.2999115.

[10] Ahamed F, Farid F, Suleiman B, Jan Z, Wahsheh LA, Shahrestani S. An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services. Future Internet. 2022; 14(8):222. https://doi.org/10.3390/fi14080222.