Journal of Cardiovascular Disease Research

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

An Enhanced Biometric Authentication System using Deep Hashing with Modified CNN Model

Dr. B. Subba Reddy[1], B. Smruthi[2], G. Keerthika[2], G. Deepika[2]

[1]Professor & HOD, [2]UG Student, [1,2]Department of Information Technology

[1,2]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 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 fingerprint, and finger-vein.

Keywords: Fingerprint authentication, unimodal biometric system, finger-vein recognition, multimodal biometric system, deep hashing, deep learning model.

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

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

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

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

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.

4. PROPOSED SYSTEM

In this project we are designing Modified Deep Learning Neural Networks (MDNN) algorithms to authenticate persons using couple of biometric features such as fingerprint, and finger-vein. Hence this algorithm is called as Multimodal. To implement this algorithm, we have applied deep hashing for securing and MDNN for feature extraction and then input to MDNN with fusion classifier to train a model to authenticate persons.

4.1 Pre-processing

Data pre-processing is a process of preparing the raw data and making it suitable for a machine learning model. It is the first and crucial step while creating a machine learning model. When creating

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

a project, it is not always a case that we come across the clean and formatted data. And while doing any operation with data, it is mandatory to clean it and put in a formatted way. So, for this, we use data pre-processing task.

Why do we need Data Pre-processing?

A real-world data generally contains noises, missing values, and maybe in an unusable format which cannot be directly used for machine learning models. Data pre-processing is required tasks for cleaning the data and making it suitable for a machine learning model which also increases the accuracy and efficiency of a machine learning model.

4.1.1 Splitting the Dataset into the Training set and Test set

In machine learning data pre-processing, we divide our dataset into a training set and test set. This is one of the crucial steps of data pre-processing as by doing this, we can enhance the performance of our machine learning model. Suppose if we have given training to our machine learning model by a dataset and we test it by a completely different dataset. Then, it will create difficulties for our model to understand the correlations between the models. If we train our model very well and its training accuracy is also very high, but we provide a new dataset to it, then it will decrease the performance. So, we always try to make a machine learning model which performs well with the training set and also with the test dataset. Here, we can define these datasets as:

Training Set: A subset of dataset to train the machine learning model, and we already know the output.

Test set: A subset of dataset to test the machine learning model, and by using the test set, model predicts the output.

4.2 MDNN

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. 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 $F(k_x, k_y, d)$..

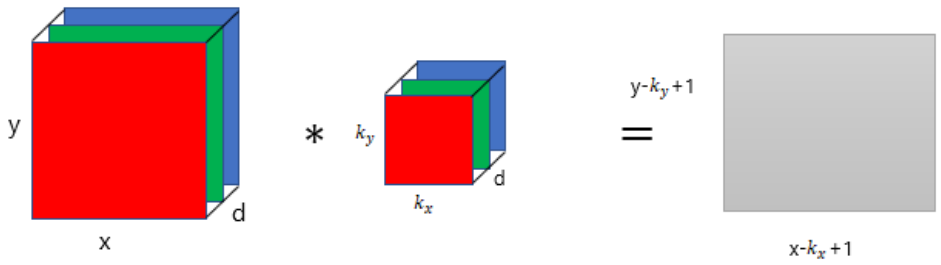
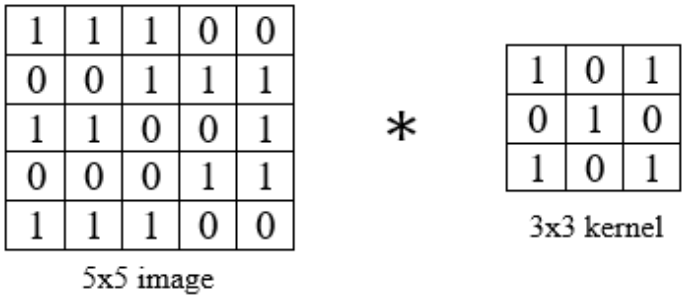


Fig. 1: Representation of convolution layer process.

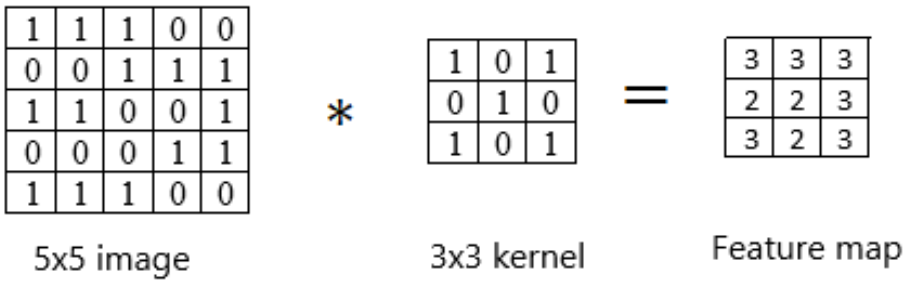
The output obtained from convolution process of input image and filter has a size of $C\left((x - k_x + 1), (y - k_y + 1), 1\right)$, which is referred as feature map. Let us assume an input image with a size of

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

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.



(a)



(b)

Fig. 2: 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.

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

4. RESULTS AND DISCUSSION

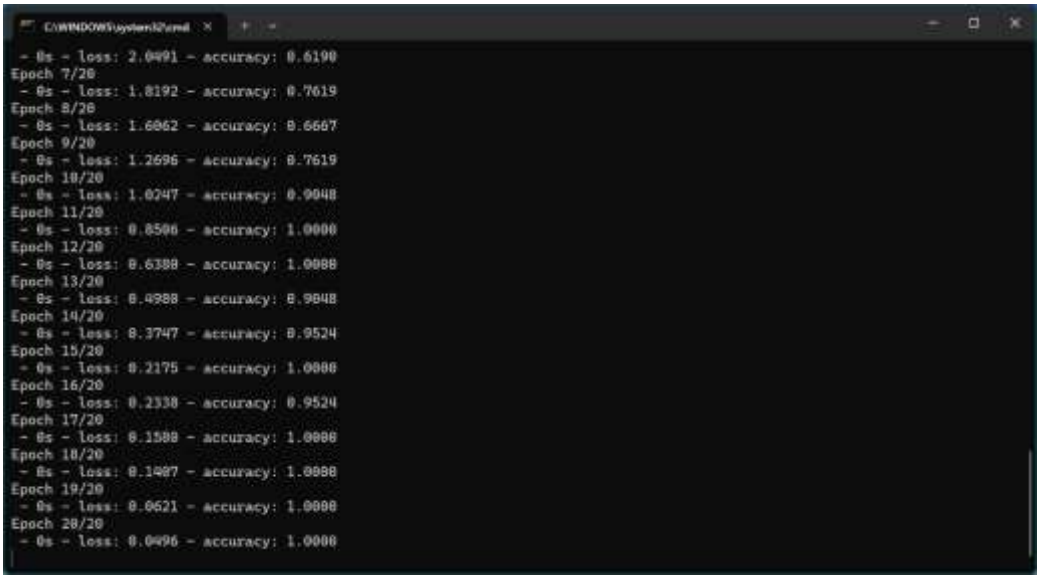
This project employs multimodal images to perform biometric enrolment and authentication to avoid user's privacy leakage. Normal passwords can be easily hacked and to avoid this problem biometric authentication was introduced using IRIS or FINGER but if attacker got access to biometric database, then he easily reconstruct hashing data to identify users and to avoid this problem, this project is using multimodal traits where two biometric input such as fingerprint and finger-vein will be captured from single user and then apply following functions on both images.

1) Upload dataset: this module is used to upload the dataset that consists of both fingerprint and finger vein images.
2) Deep Feature Extraction: this module reads the dataset then extract pixels from both images and then convert those pixels into binary to generate a feature vector. After that, from each image it will select random bits and then these random selected bits will be input to proposed modified CNN model, which will use fusion layer to combine both finger and vein features to generate raw features. Finally, the model gets trained on fusion features and then build a training model. This training model can be applied on test images to authenticate the users.
3) Authentication: using this module application take two images as input (finger and vein) and then extract features from images and then apply proposed modified CNN to predict and authenticate users
4) Performance Graph: it will plot accuracy and loss graph at each epoch/iteration.

In above screen click on 'Upload Dataset' button to upload all 20 user's datasets of fingerprint, and finger-vein. By selecting and uploading entire 'Dataset' folder and then click on 'Select Folder' button to load dataset and to get below screen

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

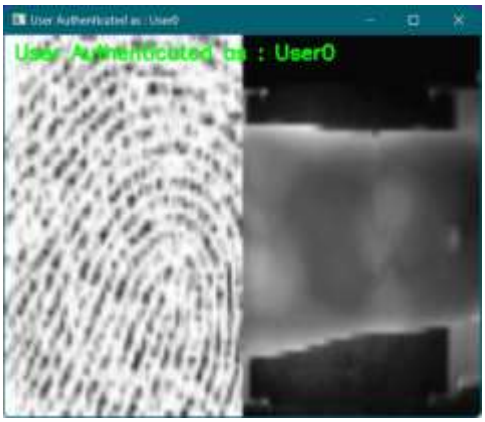
In above screen dataset loaded and now click on 'Deep feature extraction' button to extract features and then train CNN.

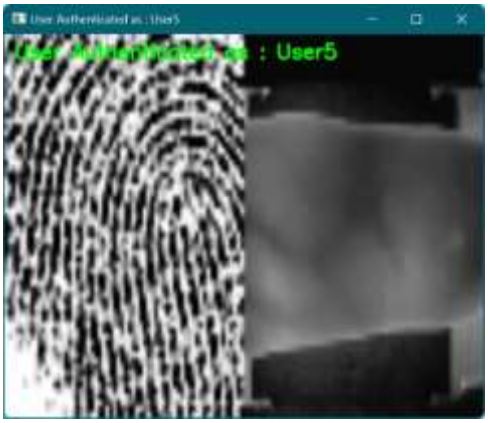


In above screen proposed modified CNN model start generating and at each increasing epoch, we can see the accuracy is getting increased and loss is getting decreased. In above screen at final epoch, proposed modified CNN has obtained an accuracy of 100% and now see main application output in below screen.

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

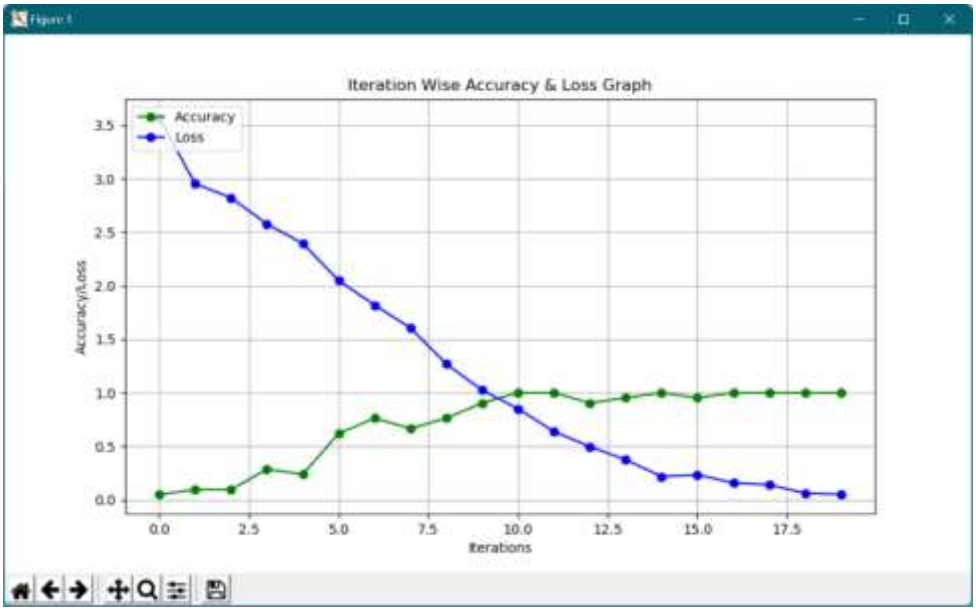
In above screen CNN got 21 users and after training all 21 users CNN got accuracy as 100%. Now click on 'Authentication' button to upload test images and then CNN will identify or authenticate users. Test images you can find inside 'testImages' folder. by selecting and uploading 'sample1' folder and then click on 'Select Folder' button to get below result





In above screen uploaded sample images are identified as 'User0' and 'User5'.

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023



In above graph x-axis represents EPOCH and y-axis represents accuracy and loss values and in above graph blue line represents loss and green line represents accuracy and in above graph we can see with each increasing epoch accuracy get increased and loss get decreased.

5. 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 MDNN training and testing model to authenticate persons using different biometric features such as fingerprint, and finger-vein. 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.

ISSN: 0975-3583, 0976-2833 VOL 14, ISSUE 01, 2023

[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.