ISSN : 1001-1781

Journal of Clinical Otorhinolaryngology, Head, and Neck Surgery

A COMPLETE PROTOTYPE OF TRI-MODAL BIOMETRIC AUTHENTICATION SYSTEM

B. Ramesh Naidu[1], Ch. Someswara Rao[2], K.V.L. Bhavani[3], Naresh Tangudu[1], M. Jayanthi Rao[4] , Y.Ramesh[1]

[1]Department of Information Technology, Aditya Institute of Technology and Management, Tekkali-532201, India,
ramesshnaiidu5@gmail.com, itsajs@gmail.com, rameshyegireddi@gmail.com

[2]Department of Computer Science and Engineering, SRKR Engineering College, Bhimavaram, AP, India,
chinta.someswararao@gmail.com

[3]Department of Department of Electronics and Communication Engineering, Aditya Institute of Technology and Management, Tekkali-532201, India,
kvlb2003@gmail.com

[4]Department of Computer Science and Engineering, Aditya Institute of Technology and Management, Tekkali-532201, India,
jayanth.mtech@gmail.com

Abstract

In traditional authentication systems, passwords, PINs, and signatures are used as a single source for identification of people. But these can be lost, stolen, or subjected to spoofing attacks. In a biometric authentication system, a person is identified through physical traits or behavioural traits. These traits are fingerprints, palmprints, face, iris, signature, speech, and so on. Biometric authentication systems are more robust, secure, and they do not require you to carry things such as smart cards, which are used in the standard authentication systems. The main advantage of the biometric system is that a person is identified with a trait that cannot be forgotten, misled, guessed, or easily copied. The prime aim of this paper is to develop a biometric authentication system with trimodality by combining physical and behavioural traits and validating them experimentally.

Keywords: Authentication; Biometric; trait

Code metadata

Nr	Code metadata description	Details
C1	Current code version	***v1.1***
C2	Permanent link to code/repository used for this code version	https://github.com/jayanthmadina/Ultrafast-Parallel-Genome-Extractor.git
C3	Permanent link to reproducible capsule	https://codeocean.com/capsule/5081139/tree/v1
C4	Legal code license	*GNU General Public License.*
C5	Code versioning system used	*None*

C6	Software code languages, tools and services used	Java 18
C7	Compilation requirements, operating environments and dependencies	***NA***
C8	If available, link to developer documentation/manual	***NA***

I. Introduction

In the digital world, the authentication of a person's identity whether genuine or imposter is an important and challenging task. Using biometric technique to authenticate a person's identity[1-3] has several advantages over the present practices of Personal Identification Number (PIN), Passwords, ATM, and Smart cards that can be forgotten, lost, stolen or prone to spoofing attacks. In the earlier researches, most of the biometric systems are uni-modal or single trait modal and these are not secure [4-8]. To solve these issues, a new biometric authentication system is proposed with four traits such as fingerprint, face, voice, and pin number. These traits are obtained by using different hardware equipment such as fingerprint device for thumb impression, Webcam for face image, Microphone for voice and pin number is given by Keyboard[5]. The proposed system is much efficient, more secure than any other existing system because of use of multiple traits. The main challenging task in this system is size of the database grows simultaneously, if database has a more number of traits. To overcome this problem, researchers continuously apply the techniques to reduce the storage space[9-10]. To solve these issues a new dynamic biometric authentication system is developed, which reduces the storage complexity, time consumed and improves security. In this work mainly focus is on developing a secure biometric authentication system as well as to reduce the storage space in the trained database[15-17].

Software features

In this section development of a new biometric authentication system by using fingerprint, face, and voice traits is discussed. Features are extracted individually from the pre-processed traits of fingerprint and voice. The individual feature vectors are distributed and then classified using Gaussian mixture model [11-14]. These individual classified vectors are integrated based on maximum score between the traits by using score level fusion technique. Finally, a new fusion vector is created and stored in training database [18-21]. The query image traits are compared with existing training dataset by using correlation method which declares the person as genuine or an imposter. This authentication by this system is more reliable than the single or bi-modal biometric systems[21-27]. The main aim of proposed model is to remove the inconvenience faced in bi-modal biometric recognition of face & voice, fingerprint & voice, and finger print & face. Hence, a new combination is proposed for recognition. The incorporated system offers anti spoofing way, high competence, strong, and more security. The proposed algorithm was shown in Algorithm 1 and framework model is shown in Figure 1.

Proposed Algorithm*:* The proposed algorithm initially uses the three traits fingerprint, face, and voice data and taken as a single input. The input data is compared with the existing dataset and finally displays the result whether individual is genuine or not. This algorithm details are depicted in algorithm 1.

Algorithm 1. Tri-Modal Biometric authentication system

```
Input: The set of traits fingerprint, face and voice.
Output: Matched or Not matched.
correlated-value-1=search(query-face, query-voice);
for each facet and voice from database
Begin
    correlated-value-2=search(fingerprint, face, voice);
    if (correlated-value-1 = = correlated-value-2 ) then
        Display query-data and matched-data
    Else
        Display out of database
    end-if;
end-for;
/* search */
int search(Image fingerprint face, voice)
Begin
    Noise is removed using median filter.
    Compress the data using DCT Transformation.
    Image features are extracted using HOG
    GMM mechanism is applied on Image features
    Probability Density Function values are fused with score level fusion
    return fused value
end search;
```

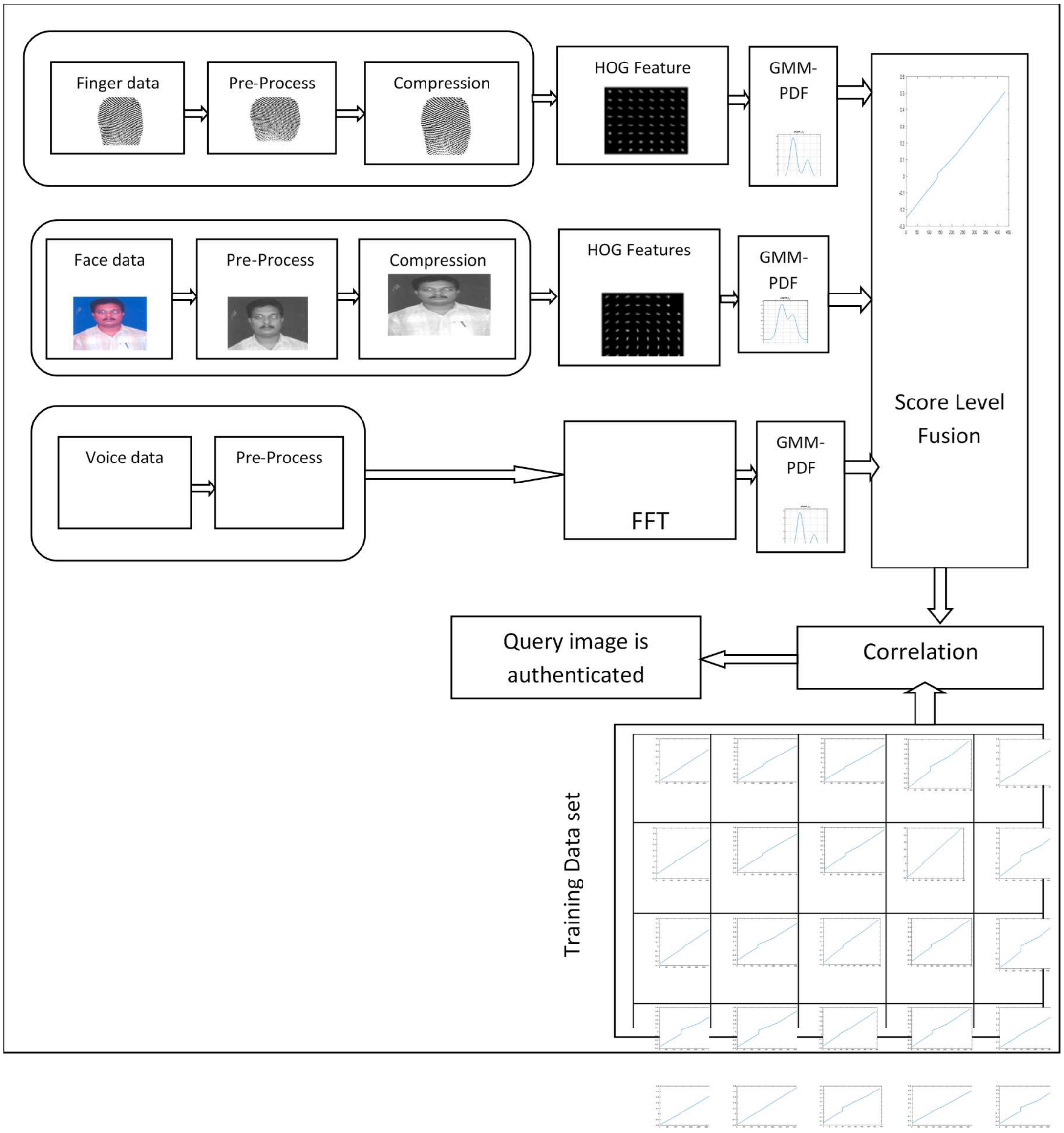


Figure 1 Complete prototype of the tri-modal

Enrollment Phase

The enrollment phase is implemented in two steps. In first step, the system takes the user id, name, and address. After entering the user details, it enters second step for acquiring traits individually. Again, it is a three-stage process like fingerprint collection, face image collection and third one is speech recording. The stage one is fingerprint collection, in this the system reads the thumb with four different poses of a same fingerprint by using thumb scanner device[11]. Once the first level is successful then enter into second level that is, read a face trait by using front camera webcam device. Originally, this image size was lengthy, so to remove unwanted information the face image is cropped from original input image. In third step, capture voice by using microphone and convert this voice into a text grammar format. This format is stored in a training database. The entire process is shown in simulation results.

Simulation Results for Enrollment Phase

In this phase, user details are submitted to enroll in biometric system. Figure 2 is opening page for processing enrolment details like Id number, Name of user, and address. However, id number must be unique. Once given all details of a person then press enroll button for saving all details of a person. After entering the personal details successfully then it shows message like Figure 3, then system is ready to take thumb details.

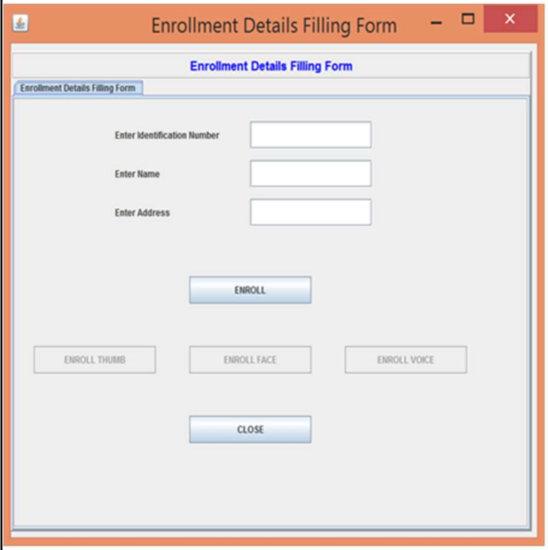
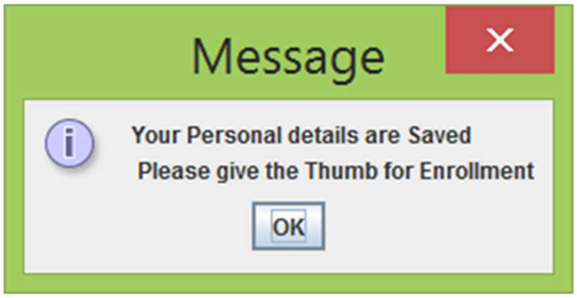
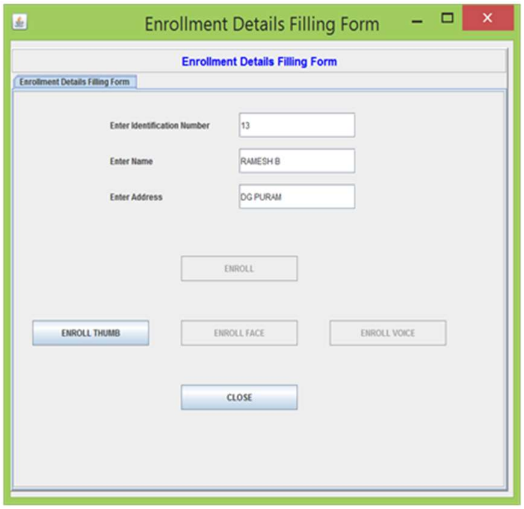

Enrollment Details Filling Form
Enrollment Details Filling Form
Enrollment Details Filling Form
Enter Identification Number
Enter Name
Enter Address
ENROLL
ENROLL THUMB
ENROLL FACE
ENROLL VOICE
CLOSE

Figure 2 Enrollment of a person's details



Your Personal details are Saved
Please give the Thumb for Enrollment

Figure 3 Successful enrollment message



Enrollment Details Filling Form

Enrollment Details Filling Form

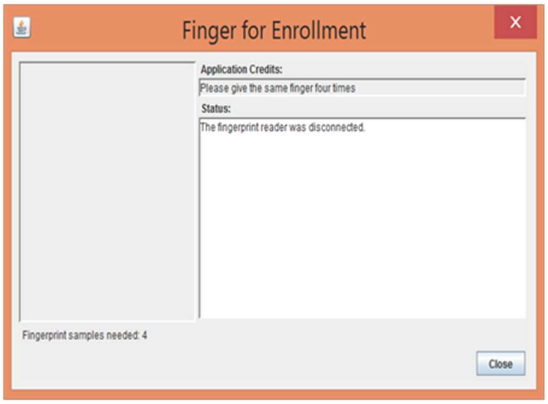
Enter Identification Number: 13

Enter Name: RAMESH B

Enter Address: DG PURAM

Figure 4(a) Collection of thumb details

After entering into thumb enrollment phase where four different fingerprint poses are taken one by one of same thumb. Collection of thumb details are shown in Figure 4(a), Enrollment of fingerprint is shown in Figure 4(b), reading fingerprint is shown in Figure 4(c) and successful enrollment message is shown in Figure 4(d). After successfully completing, then data is stored into thumb database.



Finger for Enrollment

Application Credits:

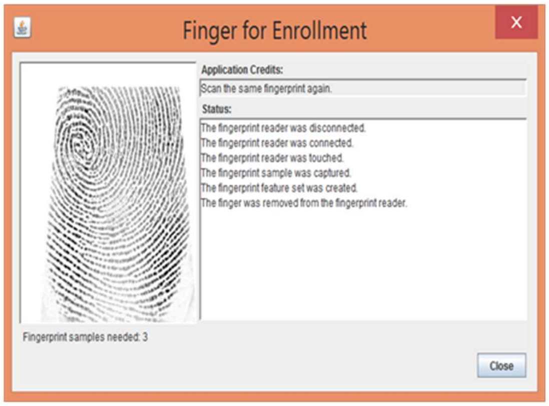
Please give the same finger four times

Status:

The fingerprint reader was disconnected.

Fingerprint samples needed: 4

Figure 4(b) Thumb enrollment



Finger for Enrollment

Application Credits:

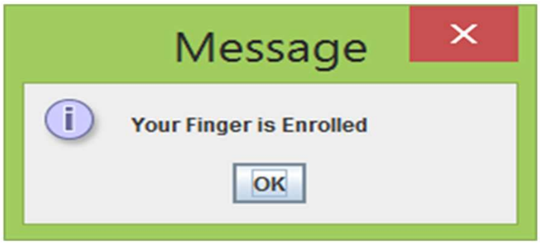
Scan the same fingerprint again.

Status:

The fingerprint reader was disconnected.
The fingerprint reader was connected.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.

Fingerprint samples needed: 3

Figure 4(c) Fingerprint collection with different poses

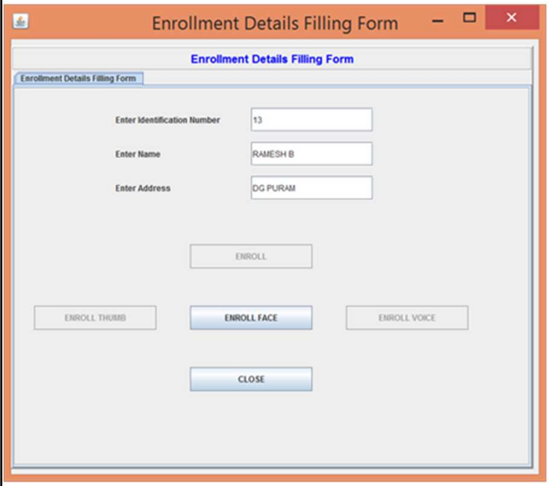


Message

Your Finger is Enrolled

Figure 4(d) Successful enrollment message

Similarly after giving the details of fingerprint, it enters into next phase, face enrollment is shown in Figure5(a). In this, select enroll face button and capturing face image by using webcam. Originally, this image size is huge and clearly shown in Figure5(b). From this image crop only frontal face for better performance result as shown in Figure 5(c). After this message is displayed on the screen successfully enrolled is shown in Figure 5(d).



Enrollment Details Filling Form

Enrollment Details Filling Form

Enrollment Details Filling Form

Enter Identification Number 13

Enter Name RAMESH B

Enter Address DG PURAM

Figure 5(a) Face image enrollment

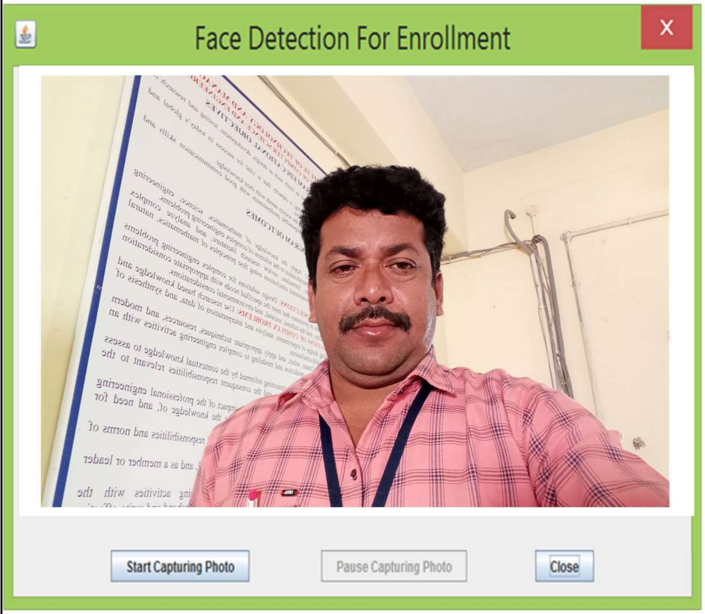


Figure 5(b) Capturing face image

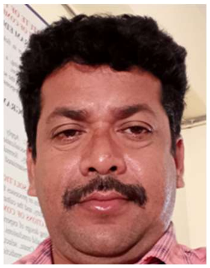
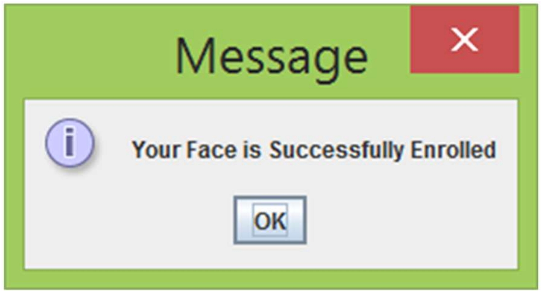


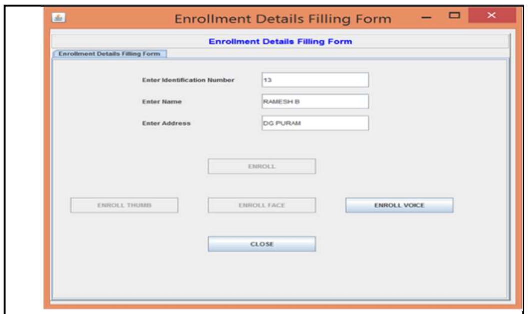
Figure 5(c) Result after crop face image



Your Face is Successfully Enrolled

Figure 5(d) Successful enrollment message

After giving details of face enrollment, system enters into voice enrollment phase. In this, select "enroll voice" button for reading voice data which is shown in Figure 6(a). After clicking button, the system is ready to capture the voice data using microphone as shown in Figure 6(b). After capturing voice, click next button "store voice in database" for storing speech in voice dataset shown in Figure 6(c). Once successfully enrolled, then system shows a message voice is stored in database shown in Figure 6(d). After completion of three traits enrollment, the traits successfully enrolled message is received which is shown in Figure 7.


Enrollment Details Filling Form
Enrollment Details Filling Form
Enrollment Details Filling Form
ENROLL
ENROLL THUMB
ENROLL FACE
ENROLL VOICE
CLOSE

Enter Identification Number 13

Enter Name RAMESH B

Enter Address DG PURAM

Figure 6(a) Voice Enrollment

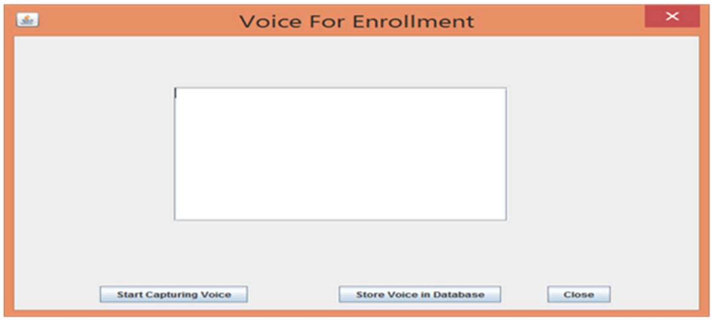
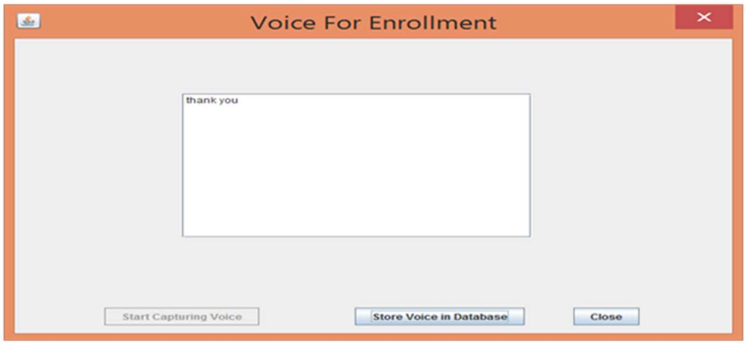
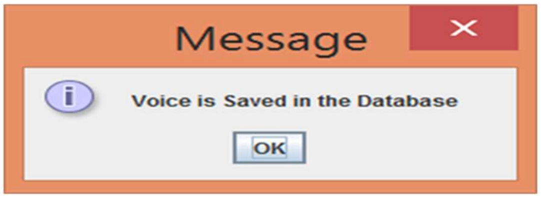


Figure 6(b) Capturing voice



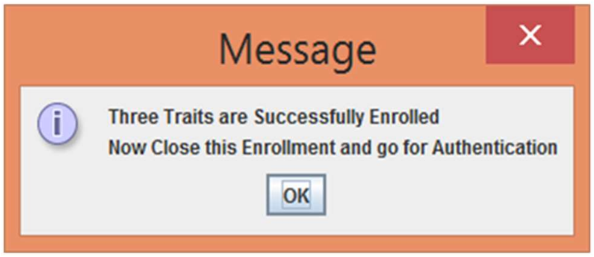
thank you

Figure 6(c) Voice is stored in database



Voice is Saved in the Database

Figure 6 (d) successfully stored



Three Traits are Successfully Enrolled
Now Close this Enrollment and go for Authentication

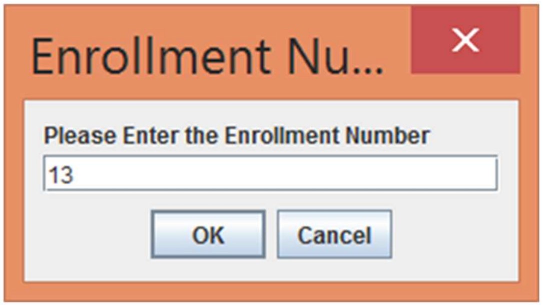
Figure 7 Successful enrollment message

Design and Development of User Authentication Phase

The authentication phase is implemented in two steps. In first step, the system asks the details like user id, name, and address of a person. Once these values are genuine then the system enters into next level. In second step, verification process is done in three stages like fingerprint verification, face verification, and voice verification. In first stage, acquire fingerprint data for verification process. In second stage, acquire face data for verification process. In third stage acquire voice for verification process. Finally, authentication process is completed successfully then the biometric authentication system shows result that whether user is genuine or imposter.

Simulation results for authentication phase

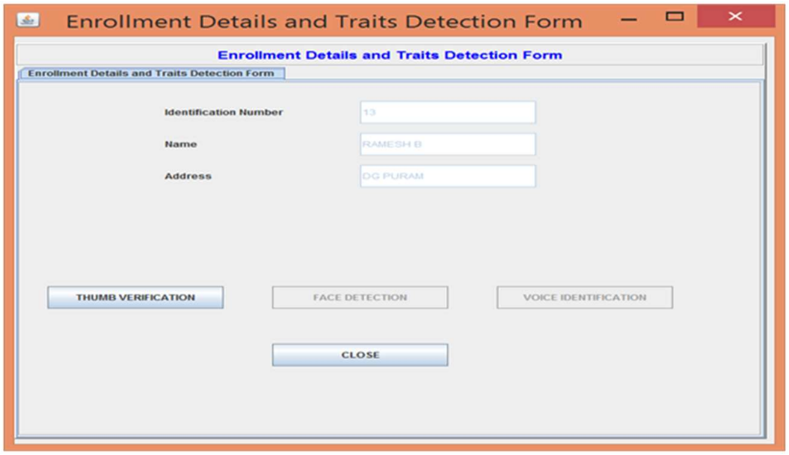
In biometric authentication system, second phase is authentication phase and this is used to identify a person or user whether "genuine" or "imposter". This is achieved by comparing testing dataset with training dataset. In the following figures process of verification of a person is explained. In verification phase first enter "roll number id" shown in Figure 8. If id number is correct then system enters into verification phase shown in Figure 9. In this, first system takes fingerprint through device.



Please Enter the Enrollment Number

13

Figure 8 Enrollment verification


Enrollment Details and Traits Detection Form
Enrollment Details and Traits Detection Form
Enrollment Details and Traits Detection Form
THUMB VERIFICATION
FACE DETECTION
VOICE IDENTIFICATION
CLOSE

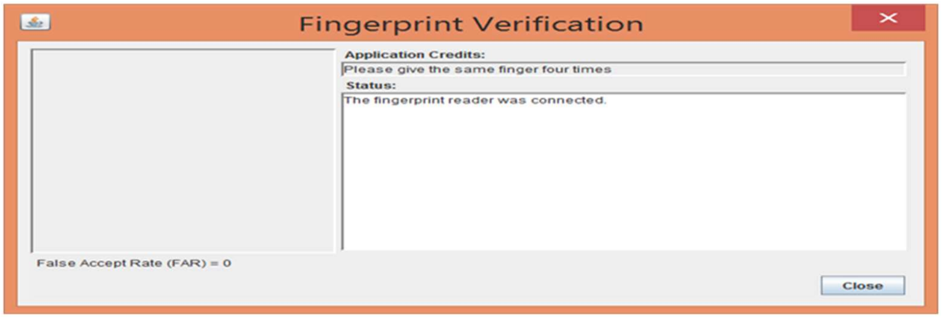
Identification Number 13

Name RAMESH B

Address DG PURAM

Figure 9 Identification process

In first phase, thumb verification process is done as shown in Figure 10(a) and Figure 10(b). After verification is successfully completed, then it shows "VERIFIED" message shown in Figure 10(c).

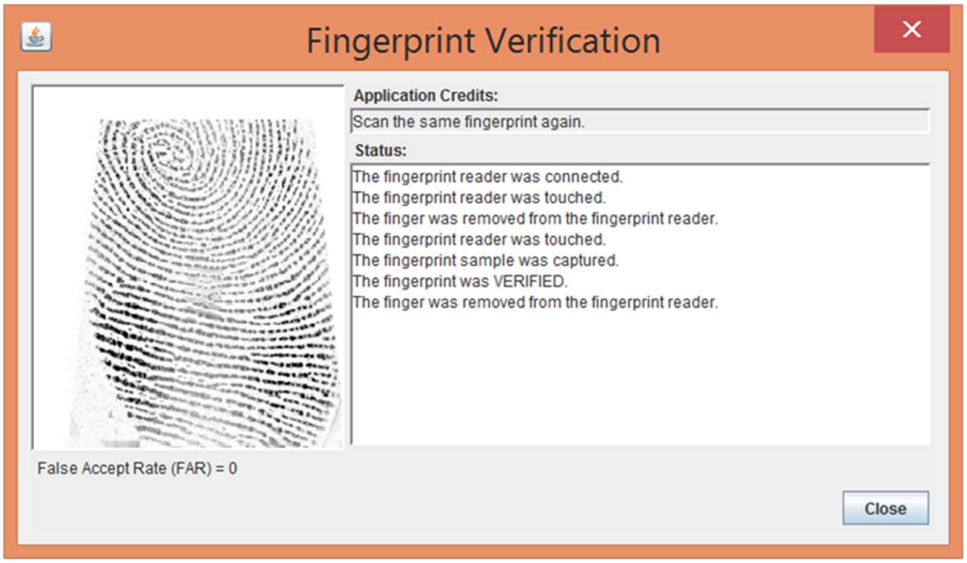


Application Credits:
Please give the same finger four times

Status:
The fingerprint reader was connected.

False Accept Rate (FAR) = 0

Figure 10(a) Fingerprint verification



Fingerprint Verification

Application Credits:

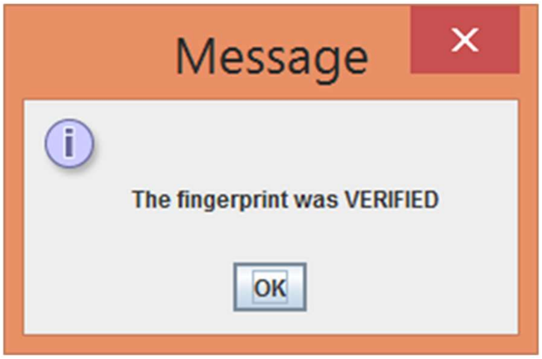
Scan the same fingerprint again.

Status:

The fingerprint reader was connected.
The fingerprint reader was touched.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint was VERIFIED.
The finger was removed from the fingerprint reader.

False Accept Rate (FAR) = 0

Figure 10(b) Sample retrieving of fingerprint



Message

The fingerprint was VERIFIED

Figure 10 (c) Successful verification

Face image capturing is second phase in verification process. Here apply same process of enrollment stage. In this, image is captured using webcam, processed, and compared with existing training dataset. It is clearly shown in Figure 11(a), Figure 11(b) for capturing face image, Figure 11(c) for extracting only useful information from original image. Finally, Figure 11(d) shows successful message.

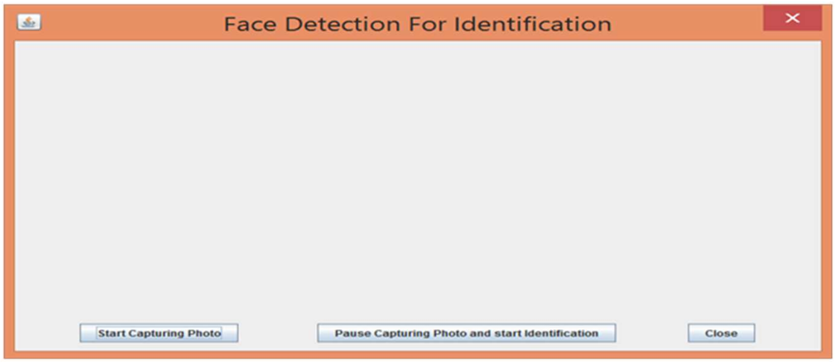

Face Detection For Identification
Start Capturing Photo
Pause Capturing Photo and start Identification
Close

Figure 11(a) Starting page of face detection

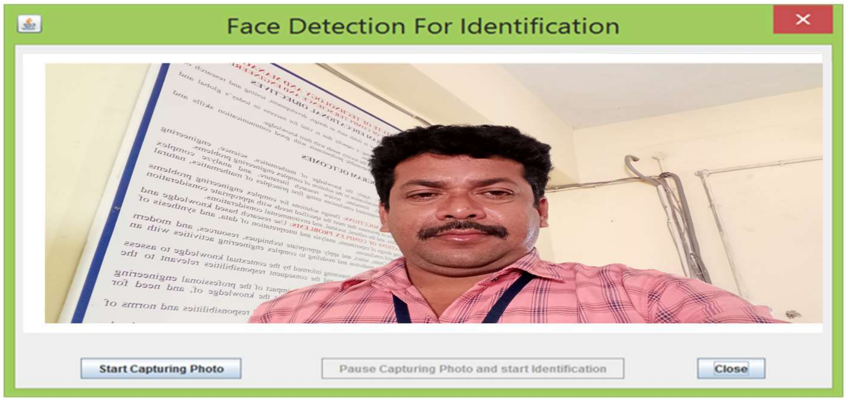
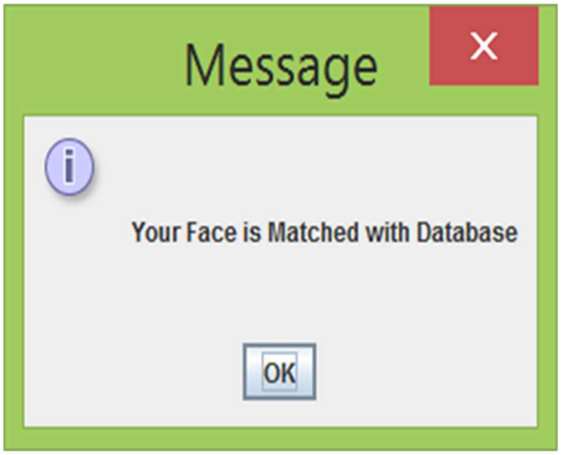

Face Detection For Identification
Start Capturing Photo
Pause Capturing Photo and start Identification
Close

Figure 11(b) Sample face image capturing through webcam

Figure 11 (c) Cropping face portion



Your Face is Matched with Database

Figure 11(d) Successful verification message

After reading face successfully then enter into next phase voice recognition. In this stage read voice from microphone and compare with existing voice dataset. Figure 12(a) is starting page for voice capturing. Figure 12(b) is reading voice data and Figure 12(c) shows the successful message. Finally, Figure 13displays the final output result of entire system whether it is “genuine" or "imposter".

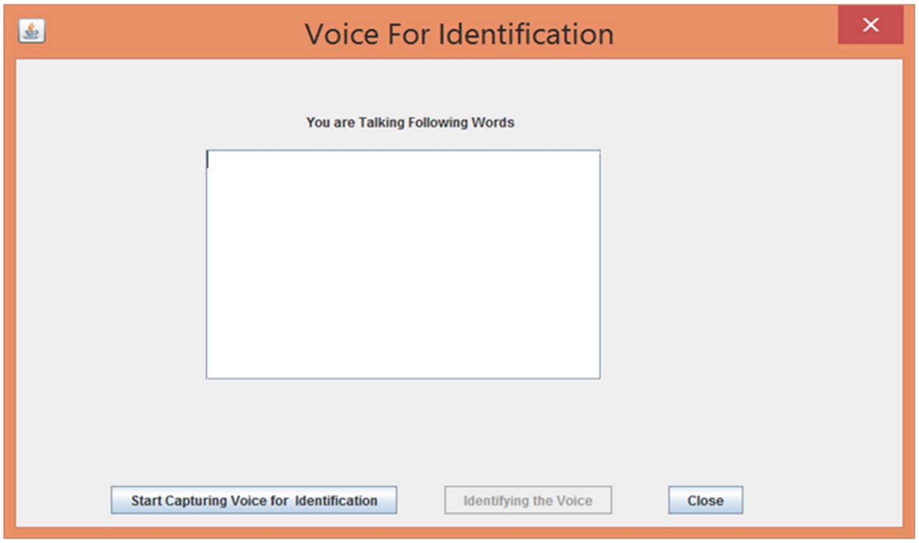
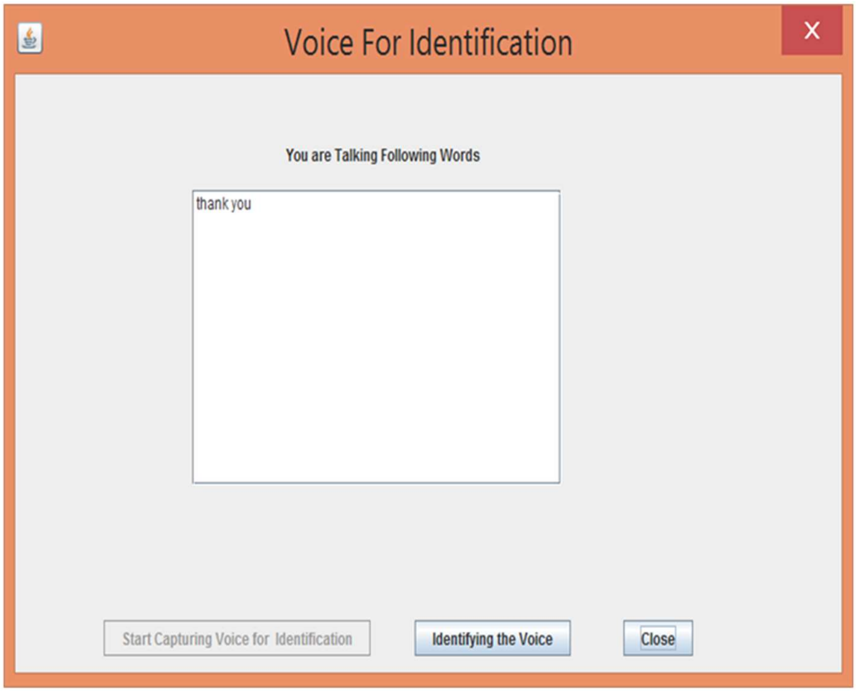

Voice For Identification
×
You are Talking Following Words
Start Capturing Voice for Identification
Identifying the Voice
Close

Figure 12(a) Starting page of voice capture

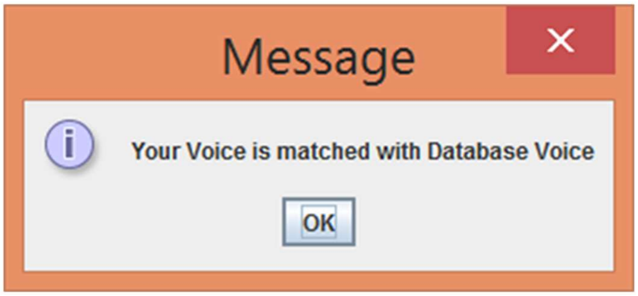


Voice For Identification

You are Talking Following Words

thank you

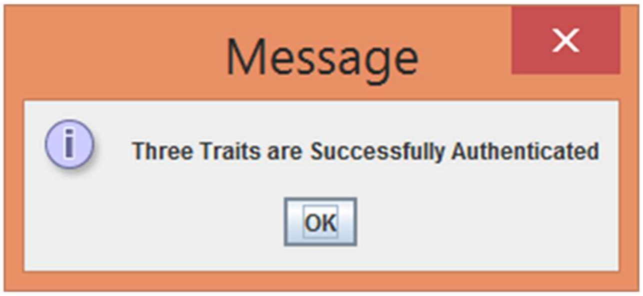
Figure 12(b) Sample voice capturing



Message

Your Voice is matched with Database Voice

Figure 12(c) Result of successful voice recognition



Message

Three Traits are Successfully Authenticated

Figure 13 Final report of authentication

Impact overview

A Biometric authentication system has to be developed to notice human being's available physiological or behavioral attributes such as face, fingerprint, signature, iris, voice, palmprint, and so on. Since none of the single trait identification techniques are much effective as they are subjected to difficulties in user authentication, data storage, and data transfer in the communication networks. They all need plenty of data to ensure reliable authentication. The inactive decision rate with them is because of processing methods which leads to shortage of productivity, long queue, and chafe on the part of the public being validation. Also, there is a need to implement extensive database to store this data. We can completement this biometric authentication system further using deep learning state of art results and IoT[15-17].

In order to solve these problems, this paper work took up the problem to experimentally investigate and implement multimodal systems with enhanced image compression algorithms as they reduce storage size, decrease the transfer time and effectively utilized network bandwidth in our proposed biometric authentication model under following objectives.

Conclusions

In this paper, a novel biometric authentication system is proposed, for verification of individual traits such as fingerprint, face, voice, and pin-number. In this, hardware devices used for enrollment and verification for checking personal details. To improve the performance, by taking dynamic inputs from hardware devices like fingerprint recognition device, webcam and speech recorder. This system is supported by low cost embedded application solution when compared to existing works.

References

1. B.R. Naidu and P.V.G.D.P. Reddy, Fusion of face and voice for a multimodal biometric recognition system, international journal of engineering and advanced technology, 2019, 8(3), 506-515.
2. B.R. Naidu and P.V.G.D.P. Reddy, Biometric authentication data with three traits using compression technique, HOG, GMM and Fusion technique, Data in Brief, 18, 1976–1986, 2018.
3. B.R. Naidu and M.S.P. Babu, A novel biometric authentication system with score level fusion, Annals of Data Science, 4, 383-404, 2017.
4. Heidari, Hadis, and Abdolah Chalechale. Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. Expert Systems with Applications 2022, 191,116278.
5. El-Rahiem, B.A., El-Samie, F.E.A. and Amin, M., Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. Multimedia Systems, 2022, 28(4), 1325-1337.
6. Ryu, Riseul, Soonja Yeom, David Herbert, and Julian Dermoudy. An Adaptive Biometric Authentication System for Online Learning Environments Across Multiple Devices. In International Conference on Artificial Intelligence in Education, pp. 375-378. Springer, Cham, 2022.

7. Yang, W., Wang, S., Shahzad, M. and Zhou, W., A cancelable biometric authentication system based on feature-adaptive random projection. Journal of Information Security and Applications, 2021, 58, p.102704.

8. Borade SN, Deshmukh RR, Ramu S., Face recognition using fusion of PCA and LDA: Borda count approach, Mediterranean Conference on Control and Automation (MED), pp. 1164-1167, 2016.

9. Gawande U, Golhar Y, Hajari K., Biometric-based security system: issues and challenges, Intelligent Techniques in Signal Processing for Multimedia Security, pp. 151-176, 2017.

10. M. Jayanthi Rao, R. Kiran Kumar, Follicle Detection in Digital Ultrasound Images Using BEMD and Adaptive Clustering Algorithms, Lecture Notes in Mechanical Engineering, 651-659, 2020.

11. M. Jayanthi Rao, R. Kiran Kumar., J. Harikiran, Method for follicle detection and ovarian classification in digital ultrasound images using geometrical features, Journal of Advanced Research in Dynamical and Control Systems, 11(2), 1249–1258, 2019.

12. M. Balakrishna, M. Ramanaiah, B. Ramakrishna, M. Jayanthi Rao and R. Neeraja, Inductively Coupled Plasma-Mass Spectroscopy: Machine Learning Screening Technique for Trace Elemental Concentrations in Hemidesmus Indicus. Annals of Forest Research, 65(1), 4431-4445, 2022.

13. M. Jayanthi Rao, P. Prasanthi, P. Suresh Patnaik, M. Divya, J. Sureshkumar and M. Ramanaiah, forecasting systems for heart disease using advanced machine learning algorithms. Int. J. Food and Nut. Sci., 11(7), 1257-1268, 2022.

14. Yuanrong Xu, Guangming Lu, Yao Lu, David Zhang, High resolution fingerprint recognition using pore and edge descriptors, Pattern Recognition Letters, 2019, 125, 773-779.

15. Tangudu, N., & Raju, O. N. (2021). Segmentation of Nuclei in Histopathological Images Using Fully Convolutional Neural Architecture. *Design Engineering*, 4962-4971.

16. Tangudu, n., & raju, o. N. Computer aided diagnosis of breast cancer from histopathological images using deep learning techniques. Turkish journal of physiotherapy and rehabilitation, 32, 2.

17. B. E. Manjunath Swamy. "Personalized Ranking Mechanism Using Yandex Dataset on Machine Learning Approaches." Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 1. Singapore: Springer Nature Singapore, 2022.

18. Burada, Sreedhar,"Computer-Aided Diagnosis Mechanism for Melanoma Skin Cancer Detection Using Radial Basis Function Network." Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 1. Singapore: Springer Nature Singapore, 2022.

19. Kumar, M. S, et al. "Deep Convolution Neural Network Based solution for Detecting Plant Diseases." Journal of Pharmaceutical Negative Results (2022): 464-471.

20. Prasad, Tvs Gowtham, et al. "Cnn Based Pathway Control To Prevent Covid Spread Using Face Mask And Body Temperature Detection." Journal of Pharmaceutical Negative Results (2022): 1374-1381.

21. Natarajan, V. A., Kumar, M. S., Tamizhazhagan, V., & Chevdumoi, R. M. (2022). Prediction Of Soil Ph From Remote Sensing Data Using Gradient Boosted Regression Analysis. Journal of Pharmaceutical Negative Results, 29-36.

22. Kumar, M. Sunil, et al. "Deep Convolution Neural Network Based solution for Detecting Plant Diseases." Journal of Pharmaceutical Negative Results (2022): 464-471.

23. Sreedhar, B., BE, M.S. and Kumar, M.S., 2020, October. A comparative study of melanoma skin cancer detection in traditional and current image processing techniques. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 654-658). IEEE.

24. P. Sai Kiran, and M. S Kumar. "Resource aware virtual machine placement in IaaS cloud using bio-inspired firefly algorithm." Journal of Green Engineering 10 (2020): 9315-9327.

25. Balaji, K., P. Sai Kiran, and M. Sunil Kumar. "Power aware virtual machine placement in IaaS cloud using discrete firefly algorithm." Applied Nanoscience (2022): 1-9.

26. Ananthanatarajan, V., Kumar, M. S., & Tamizhazhagan, V. (2020). Forecasting of wind power using lstm recurrent neural network. Journal of Green Engineering, 10.

27. Ramesh Yegireddi, Jagadeesh Kumar G, Naresh Tangudu, Nagaraju Rayapti, Kavitha K, & G V L Narayana. (2022). Recent advancements and challenges of Internet of Things in Healthcare. *Journal of Pharmaceutical Negative Results*, 44–57. https://doi.org/10.47750/pnr.2022.13.S06.007