Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
JCRES

VOLUME:7, ISSUE:2, PAPER NUMBER:57

Privacy-Preservation in Biometric using Face and Voice Authentication

Kowsalya L[1], Sharan Parasanth V[2], Arunika J[3], Uma Maheshwari G[4]

[1,2,3] Students,and [4] Faculty
Dept. of Computer Science Engineering,
Dr.Mahalingam College of Engineering and Technology, Pollachi-642002, India.
lkowsalyaa0@gmail.com

Abstract: *Biometric recognition systems are increasingly common in various applications, providing reliable user authentication and identification. Using biometric data poses substantial privacy concerns because it's inherently tied to individuals, making it challenging to invalidate or substitute compromised data. Efficient and accurate biometric identification remains a major challenge in the field. Additionally, biometric data is highly sensitive, requiring strong protection measures. This study introduces a solution that utilizes public-key encryption with keyword search to reduce the computational burden of biometric identification systems while maintaining privacy. To ensure the long-term security of biometric data, the study adopts fully homomorphic encryption for template protection. Importantly, the proposed system maintains the recognition accuracy of its unprotected counterpart. The system distinguishes between authorized and unauthorized individuals. Authorized individuals can access the original information, while unauthorized individuals cannot. The system is developed the machine learning algorithm for classifying the person face and voice is authorized or un-authorized by using random forest classifier and CNN. Finally, experimental results demonstrate performance metrics such as accuracy and error rate.*

Keywords: *Biometrics, 2D Convolutional neural network (CNN- 2D), Random forest classifier, RSA, Encryption, Face, Voice, Privacy preserving.*

1. INTRODUCTION:

Automated biometric recognition is now a common feature in our daily lives, ranging from accessing personal devices to using smart border control gates. While biometric authentication offers both convenience and security, it also raises potential privacy concerns. This is because biometric data is categorized as sensitive personal information under the General Data Protection Regulation. This is especially relevant in cases where biometric data is utilized for identification purposes, requiring the central storage of biometric references to aid in searching for an unknown individual. If a malicious actor gains access to the signal representation of a person's biometric trait, it compromises the associated reference, rendering it unreliable for secure authentication. This increases the risk of impersonation and undermines the integrity of the authentication process.

Machine learning techniques are causing a significant shift in pattern recognition, particularly in biometric identification. In this domain, feature extraction methods often rely on training with differentiable loss functions such as the Euclidean distance. As a result, the feature vectors produced are typically represented as fixed- dimensional real-valued vectors. These vectors serve as pivotal biometric templates, contributing to the ongoing evolution of biometric recognition systems. Authentication systems are vital in today's societies, covering personal electronic devices, law enforcement, and airport security. They usually function through two primary methods: knowledge-based and biometric. The knowledge- based method involves a unique code known exclusively to the authorized user, often utilizing passwords and PINs.

2. ENSURING PRIVACY IN BIOMETRIC SYSTEMS WITH FACE AND VOICE AUTHENTICATION:

Our paper, "PRIVACY-PRESERVATION IN BIOMETRIC USING FACE AND VOICE AUTHENTICATION" to develop a robust system capable of accurately distinguishing between authorized and unauthorized individuals using both facial and vocal biometric data. To enhance the system's ability to learn and adapt to different scenarios, thereby improving its overall performance and effectiveness. To develop algorithms for the precise extraction of biometric information from facial images and voice recordings. To prevent unauthorized access and protect the privacy of individuals' biometric data. To achieve higher accuracy and reliability in identifying authorized individuals while minimizing false positives and false negatives. To ensure the confidentiality, integrity, and availability of biometric data stored in the cloud.

3. ARCHITECTURE:

In this system, the FERET images and voice dataset is collected from dataset repository. Then, we can implement the image pre-processing step. We can utilize LBP (Local Binary Pattern) to extract the features from the pre-processed image in this context. After that, we can extract the biometric information for corresponding person. Then, we can implement the machine learning algorithm such as random forest and CNN-2D for classifying or identifying the input person is authorized or un-authorized. After that, we can encrypt the extracted biometric information by using encryption algorithm such as RSA. If the person is authorized, the person can decrypt the biometric information and can view the original data. If the person is un-authorized, the person can't able to see the original biometric information. Finally, the encrypted and decrypted biometric information will be stored in cloud (box cloud or cloudme) for security purpose. Finally, we can estimate the some performance such as accuracy and error rate and visualize the performance in the form of graph. The unwanted noise in the input audio can be eliminated through noise injection and shifting. Following this, the classification algorithm like random forest and CNN must be applied to determine the authorization status of the individual.

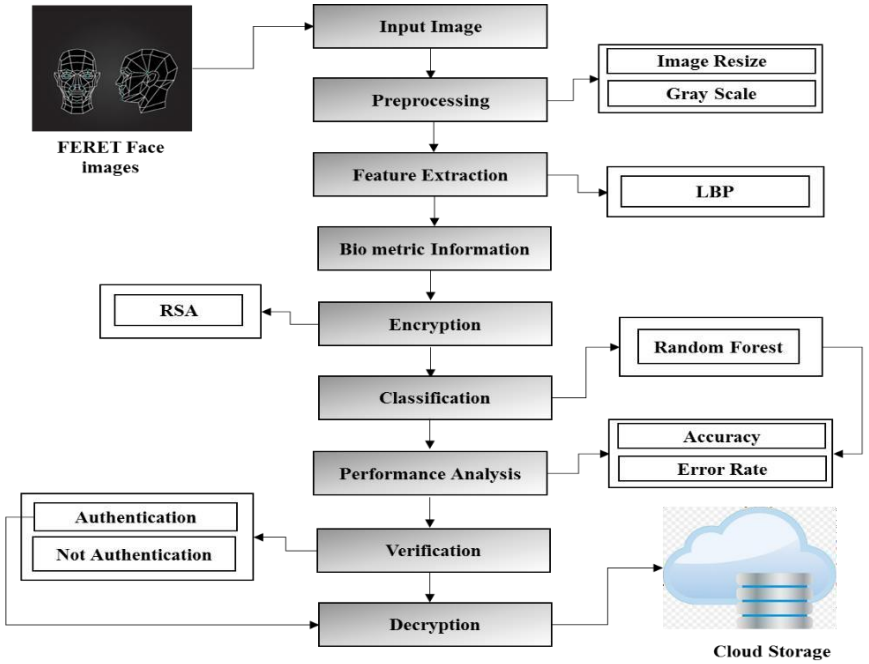

Fig. 1. Architecture diagram for biometric system

4. FLOWCHART:

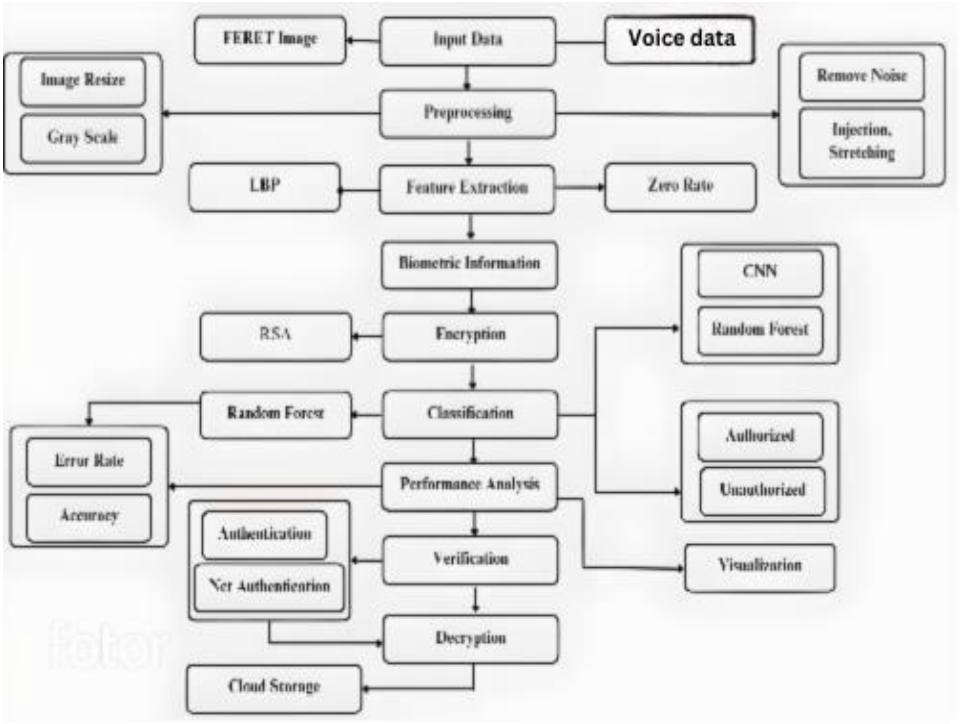

Fig. 2. Flowchart diagram for biometric system

1) First, we have to acquire the FERET images and voice dataset from a reputable dataset repository.
2) Then, applying pre-processing techniques like normalization, resizing, and gray scaling to the images is a common first step in image-based biometric systems.
3) Using Local Binary Patterns (LBP) to extract facial features from the pre-processed images. LBP is a popular texture-based feature descriptor for facial recognition.
4) After feature extraction, we can use the obtained features to extract biometric information for each individual in the dataset.
5) To implement machine learning algorithms like Random Forest and 2D Convolutional Neural Networks (CNN-2D) for classification/identification of authorized vs. unauthorized individuals.
6) Then, encrypting the extracted biometric information with an algorithm like RSA ensures that only authorized individuals can access the original biometric data.
7) Storing the encrypted and decrypted biometric information in a cloud storage service like Box or CloudMe provides an additional layer of security and accessibility.
8) Estimating accuracy, error rate, and visualizing the performance of the system through graphs is an important final step to assess the efficacy of the proposed approach.

5. PICTORIAL REPRESENTATION:

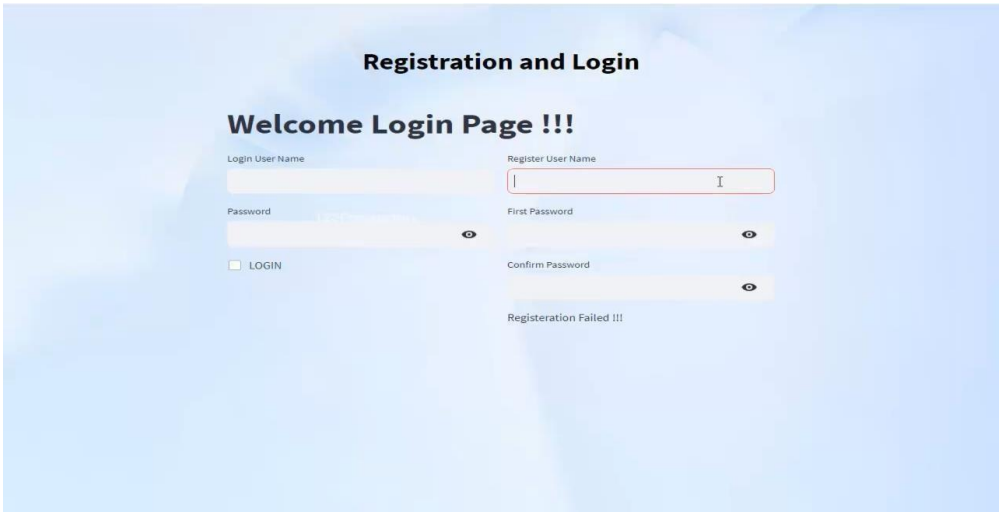

Fig.3.Login page

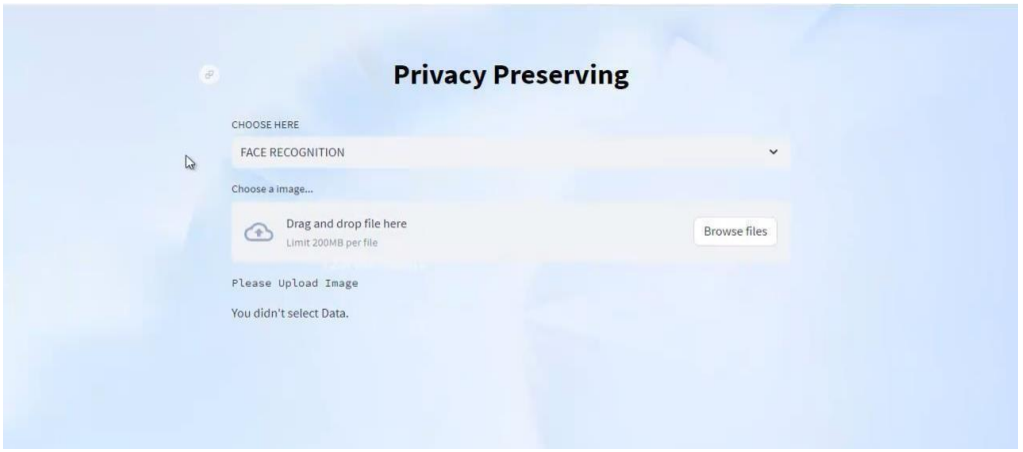

Fig.4.User input image

6. EXPERIMENTAL ANALYSIS:

6.1 Understanding the data:

This dataset contains information about FERET image database and voice dataset were used for evaluation. The FERET dataset, obtained from a dataset repository, serves as the input for this system. The dataset comprises images in the '.png' and '.jpg' formats. To commence the process, the imread() function is employed to read or load the input image. A multimedia audio dataset, with the files in the '.mp3' format. In Python, the librosa package can be utilized to read or load the input dataset from these audio files.

6.2 Preprocessing:

In our workflow, we execute two essential tasks on the image: resizing and converting it to grayscale. Resizing is accomplished by invoking the resize() method with a two- integer tuple specifying the desired width and height. It's crucial to note that this operation leaves the

original image unchanged and returns a new Image object with the updated dimensions. To convert the image to grayscale in Python, we utilize the Conversion Formula and leverage functionalities provided by the matplotlib Library. To applying techniques such as noise removal, noise injection, and shifting to the input audio data in order to eliminate unwanted noise and transform the data into a suitable format for further processing.

6.3 Feature extraction:

During this stage, we have the capability to implement or extract features from the pre-processed image using LBP. LBP, or Local Binary Pattern, is a texture analysis method widely employed in image processing due to its simplicity and effectiveness. This technique involves assigning labels to pixels by comparing their intensities with those of neighboring pixels. Through the application of a threshold, the resulting values are transformed into binary numbers. The LBPH (Local Binary Pattern Histogram) algorithm is specifically designed for face recognition and facilitates the identification of individuals based on their unique facial features. Renowned for its impressive performance, this algorithm is capable of recognizing faces from various angles, including both frontal and side views. The pre-processed audio, including the zero-crossing rate, which is a temporal feature indicating how many times the audio signal crosses the zero amplitude (time axis) within a specific time frame or window. It is a measure of the noisiness or frequency content of the audio signal.

6.4 Biometric information:

We can extract the biometric information for corresponding input person. The biometric information such as person name, age, sex and so on.

6.5 Encryption:

By utilizing the RSA algorithm, we have the capability to encrypt the initial biometric data. This encryption procedure employs a set of interconnected keys: a public key and a private key. The public key is intended for unrestricted distribution, whereas the private key must be safeguarded and kept confidential, shared with no one. The encrypted data will then be securely stored in the cloud.

6.6 Classification:

In our workflow, we aim to integrate machine learning algorithms like Random Forest, a popular choice in Supervised Machine Learning. Random Forest that adoption is supported by various factors: it boasts minimal training time, delivers accurate predictions even with vast datasets, and maintains robustness in the face of missing data. Our workflow incorporates the Convolutional Neural Network 2D (CNN-2D) architecture, a specialized neural network model tailored for processing and analyzing two-dimensional data structures, such as images. These CNN-2D models have demonstrated remarkable performance across a wide range of computer vision applications, including image classification, object recognition, and image segmentation tasks. The strength of this architecture lies in its ability to automatically extract and learn hierarchical representations from raw pixel data, effectively capturing and encoding spatial patterns and correlations present within images. The CNN model predicts the speaker’s identify or performs voice recognition tasks without decrypting the data.

6.7 Performance analysis:

The final result will get generated based on the overall classification and prediction. The performance of this proposed approach is evaluated using some measures like accuracy, error rate. This involves the culmination of various classification and prediction techniques applied to the biometric data collected from the individual's face and voice. A high accuracy rate signifies a reliable authentication process, instilling confidence in the system's ability to accurately verify user identities. The error rate is another important metric evaluated during the result generation process. The error rate provides insights into the frequency of misclassifications or false identifications made by the system.

6.8 Verification:

The user's identity undergoes verification, and upon successful confirmation, access is granted to the system, device, or secure area. In cases where the user's identity cannot be verified, access to the system, device, or secure area is denied.

6.9 Decryption:

If the biometric data (face and voice) presented during the decryption process matches the biometric templates securely bound to the encryption key (or the key protecting the RSA private key), then the system can successfully derive the correct key and decrypt the encrypted biometric data or templates. This allows authorized users to access and use their biometric data for authentication and decryption purposes. If an unauthorized user attempts to decrypt the biometric data, their biometric data will not match the securely bound biometric templates.

6.10 Cloud storage:

The biometric information (features extracted from face images and voice data) that has been encrypted using the RSA algorithm can be stored in a cloud storage service.

7. PERFORMANCE ANALYSIS:

The eventual outcome is a result of the complete classification and prediction process. The efficacy of the suggested approach is assessed using various metrics such as

- **Accuracy:** The accuracy of a classifier indicates its effectiveness in correctly predicting class labels, whereas predictor accuracy evaluates how accurately a predictor can anticipate the values of predicted attributes for new data points.

$$AC = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

- **Error rate:** It denotes a metric quantifying the extent of prediction inaccuracy of a model concerning the genuine model.

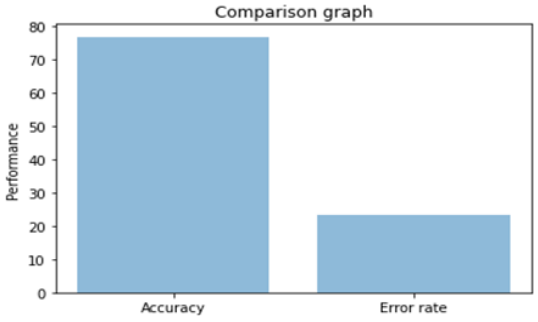

Fig.5.Comparison graph

8. EVALUATION AND RESULTS:

The ultimate outcome, whether a person is categorized as authorized or unauthorized, is determined by the collective classification and prediction results of the system. To evaluate the performance and efficacy of this proposed multimodal biometric authentication approach, several measures and metrics are employed. These performance measures provide a comprehensive evaluation of the system's capabilities, including its accuracy, error rates, and ability to distinguish between authorized and unauthorized individuals effectively.

Classifier	Accuracy	Error rate
Random forest	76.66	23.33
CNN-2D	94.10	6.56

Table.1.Accuracy and error rate table

9. SAMPLE OUTPUT

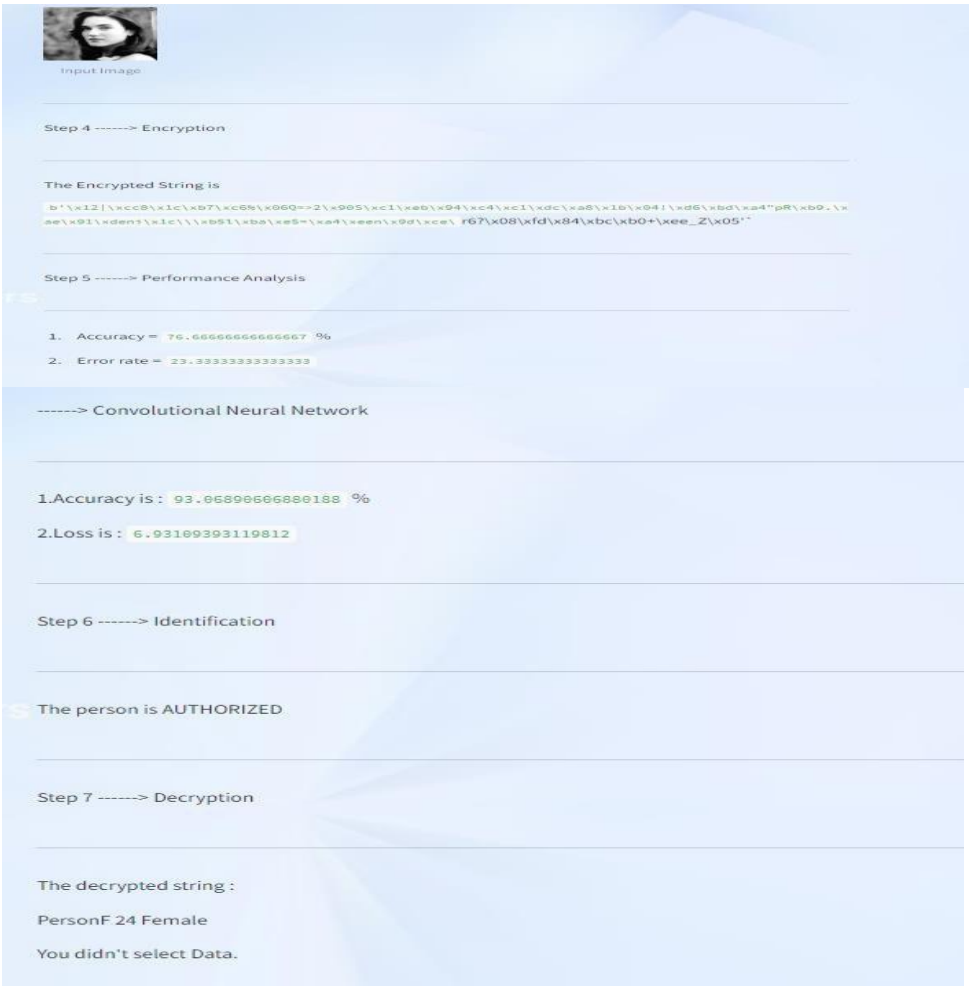

Fig.6.Face authentication

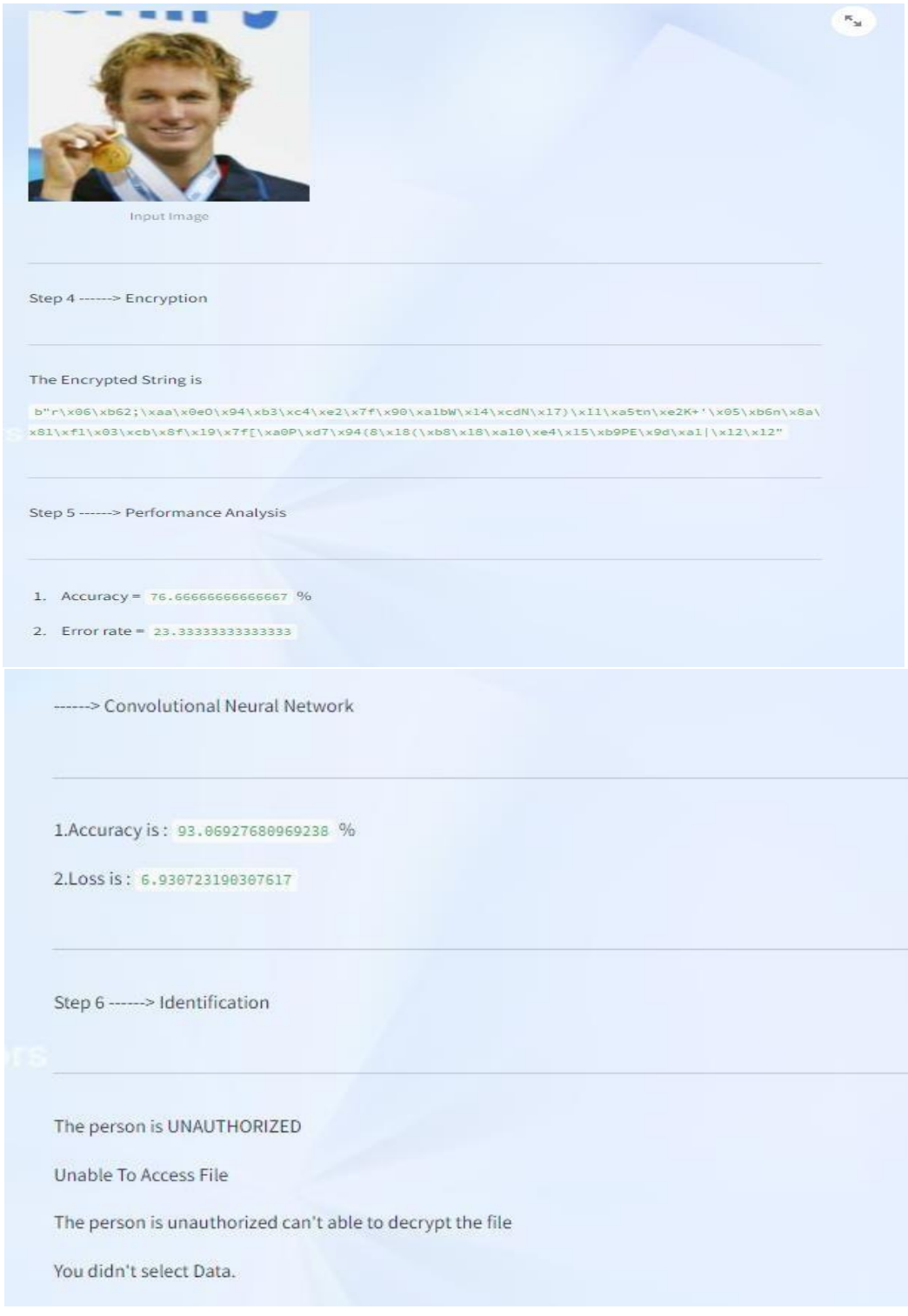

Fig.7.Face un-authentication

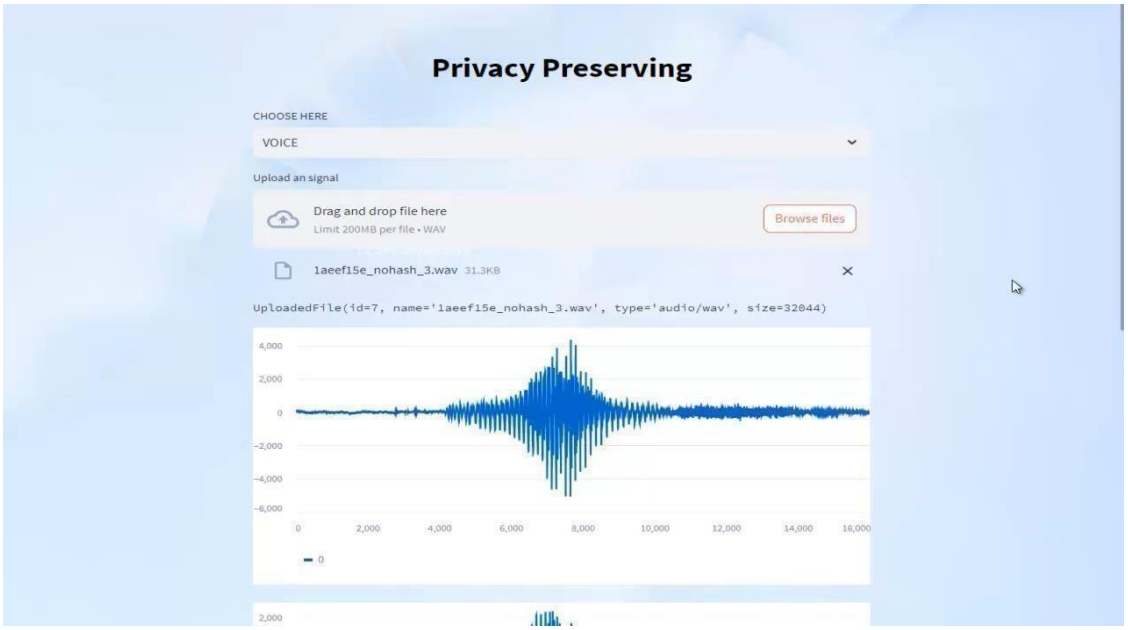

Fig.8.Audio preprocessing

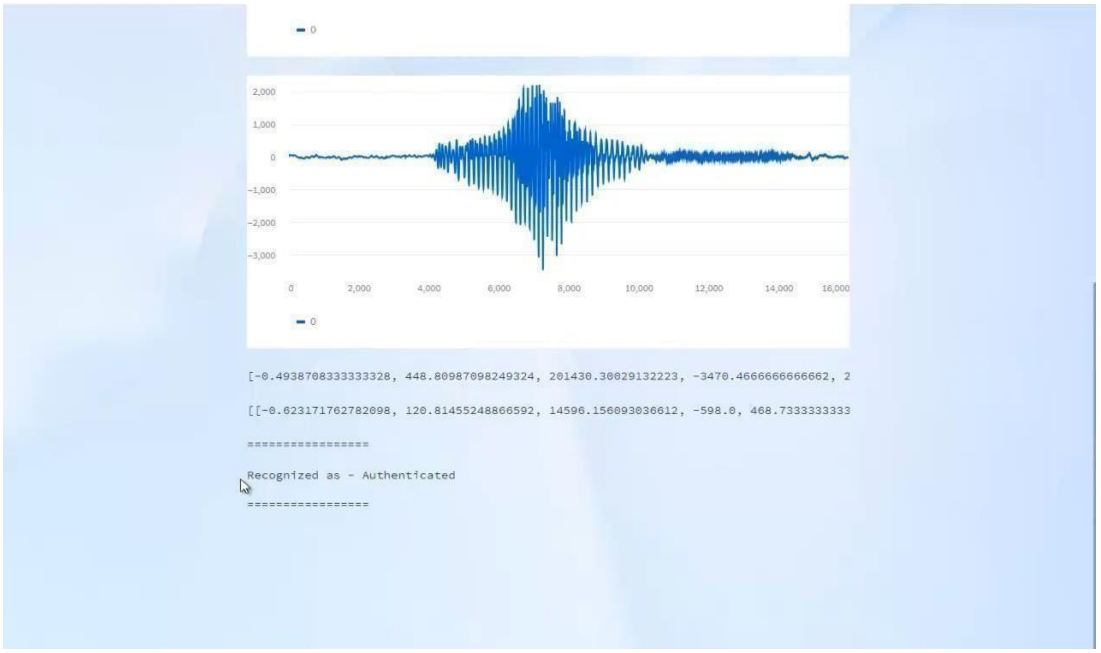

Fig.9.Vocal authentication

10. CONCLUSION:

Our analysis indicates that the FERET image and voice dataset were sourced from a dataset repository. Subsequently, we extracted the features utilizing the local binary pattern method. Then, we are extracted the biometric information for corresponding input image. Then, encrypt the biometric information by using RSA algorithm. Then, we are developed the classification algorithm such as random forest and CNN- 2D. Then, the encrypted and decrypted data are stored in cloud. Upon successful authentication, the encrypted biometric information was decrypted, allowing authorized users to access the original data securely. As an additional security measure, both the encrypted and decrypted biometric data were stored in a cloud environment, leveraging robust cloud storage solutions for enhanced data protection and accessibility. The noise injection and shifting can remove the unwanted noise from input audio. Then, we have to implement the classification algorithm to predict the person authorized or unauthorized.

11. References:

[1] J. Kolberg, P. Bauspieß, M. Gomez-Barrero, C.Rathgeb, M. Durmuth, ¨ and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in Intl. Workshop on Information Forensics and Security (WIFS), pp. 1–6, IEEE, 2019.

[2] J. J. Engelsma, A. K. Jain, and V. N. Boddeti, "HERS: Homomorphically encrypted representation search," IEEE Trans. on Biometrics, Behavior, and Identity Science (T-BIOM), 2022.

[3] R. Behnia, A. A. Yavuz, and M. O. Ozmen, "High-speedhigh-security public key encryption with keyword search," in IFIP Conf. on Data and Applications Security and Privacy, pp. 365–385, Springer, 2017.

[4] D. Osorio-Roig, C. Rathgeb, P. Drozdowski, and C. Busch, "Stable hash generation for efficient privacy-preserving face identification," Trans. on Biometrics, Behavior, and Identity Science (TBIOM), 2021.

[5] P. Bauspieß, J. Olafsson, J. Kolberg, P. Drozdowski, C. Rathgeb, and C. Busch, "Improved homomorphically encrypted biometric identification using coefficient packing," in Proc. Intl. Workshop on Biometrics and Forensics (IWBF), 2022.

[6] L. Lai, S.-W. Ho, and H. V. Poor, ''Privacy–security trade-offs in biometric security systems—Part II: Multiple use case,'' IEEE Trans. Inf. Forensics Security,vol. 6, no. 1, pp. 140–151, Mar. 2011.

[7] T. Scheidat, C. Vielhauer, and J. Dittmann, ''An iris- based interval mapping scheme for biometric key generation,'' in Proc. 6th Int. Symp. Image Signal Process. Anal., 2009, pp. 511–516.

[8] P. Mihăilescu, A. Munk, and B. Tams, ''The fuzzy vault for fingerprints is vulnerable to brute force attack,'' in Proc. BIOSIG, vol. 155. 2009, pp. 43– 54.

[9] Drozdowski, C. Rathgeb, and C. Busch, "Computational workload in biometric identification systems: An overview," IET Biometrics, vol. 8, no. 6, pp. 351–368, 2019.

[10] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS), Data and Applications Security and Privacy for face recognition system pp. 1-10 IEEE 2018.