Biometric Authentication System Mapping with Real-time Database Workload Using Computational Learning Theory

D.Prabhu*[*], S.Vijay Bhanu[**], S.Suthir[***]

[*] Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India
[**]Research Supervisor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India
[***]Research Co Supervisor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India

Abstract- **In Today's World Biometric Authentication as been rapidly growing in the field of computer science as a form of identification and security purposes among all biometric authentications face recognition mostly used due to its method can be done passively without explicit action are the face image can be obtained from a certain distance using camera the paper is therefore proposed to create an attendance base system using face recognition. In deep learning which includes image steganography has been widely used due to its information hiding technique so we used CNN and Network based method to create this project. The experimental result shows that this system can recognize the face and compare them on the cloud data where multiple student image where uploaded. The storage of data related to students stored in the google firebase**

Index Terms- CNN, HOG, LSB, PVD, CV.

I. Introduction

As technology develops at an extremely rapid pace, the aim is to make people's lives more and more simple, such as biometrics systems which is basically a pattern recognition system, through the use of different biometrics to identify a person, such as fingerprint, retina scanning, iris scanning and face recognition, etc. In this passage, we describe the applications of face recognition systems across different fields, which include financial fields, education fields, transportation fields and public security fields. Face recognition has lately gained a lot of attention as one of the most effective applications of picture analysis and understanding, especially in the last few years. More specifically, facial recognition and other biometric verification systems have developed greatly. A deep learning algorithm does not require manual feature extraction like traditional face recognition techniques. Face detection means capturing or discovering a face in the image. Face recognition is the process of finding a matching face by comparing faces found in a static image or dynamic video.

Deep learning algorithms can automatically extract valuable hierarchical features from training images. Especially, CNN-based algorithms provide state-of-the-art performance in computer vision problems by applying convolution filters accompanied by various nonlinear activation functions. Despite the fact that highly reliable methods of biometric personal identification exist, for example, fingerprint analysis and retinal or iris scans, these methods rely on the cooperation of participants, whereas a personal identification system based on analysis of frontal or profile images is often successful without the participant's cooperation or knowledge. Based on fingerprint identification's high recognition accuracy and uniqueness

A hidden message can be embedded in a cover message according to the ancient art of steganography. Steganography, which is used to hide information in plain sight, allows the use of a wide variety of secret information forms like images, text, audio, video, and files. Image steganography is the process of hiding data in image files. Video is a combination of frames or pictures used to hide text messages. Different methods directly embed data in the cover frame with no changes and of high quality. And it is very imperative to protect our data or information from black-hat hackers or unwanted access. In cryptography, the message has been encrypted, but when communicating with a third party, the encrypted message can be decrypted very easily and destroyed. In steganography, secret information is hidden in cover files; this is the way that the data is also hidden so that while communicating, unwanted access cannot be done easily between two parties. Steganography is capable of combining image, face, and fingerprint datasets into a single file in order to save memory. This allows for data to be stored and retrieved more efficiently.

Google Firebase is a development platform for mobile and online application. It provides a variety of tools and services that can be used to develop high-quality apps quickly and easily. Firebase offers services for authentication, database management, hosting, cloud messaging, and more. It also includes a wide range of tools for testing and monitoring your app's performance, as well as features for user engagement and growth. Firebase can handle the demands of your project. It is designed to automatically scale up or down as needed, ensuring that your app can handle a large number of users without any performance issues. In addition, Firebase is backed by Google's powerful infrastructure and security measures, which means that your app is always secure and reliable. With Firebase, you can rest assured that your app's data is stored securely and that your users' information is protected.

II. PROPOSED SYSTEM

We will propose the project with the extraction of the data stored in the database while saving it in the cloud, which improves the speed and security of the data. This project will save all the records and face and fingerprint biometrics of the person for the attendance system to map into a single entity. Steganography is capable of combining image, face, and fingerprint datasets into a single file in order to save memory. This allows data to be stored and retrieved more efficiently. It helps to consume less data due to a single entity of data, and biometric mapping time and attendance systems can improve security.

III. ARCHITECTURE

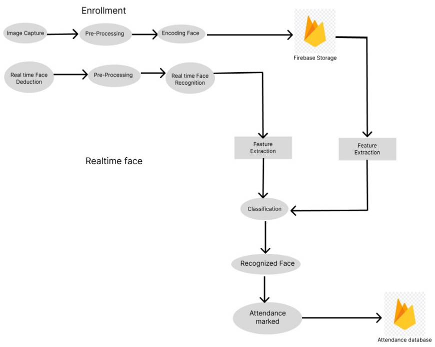


Fig 1: Process of Face Recognition

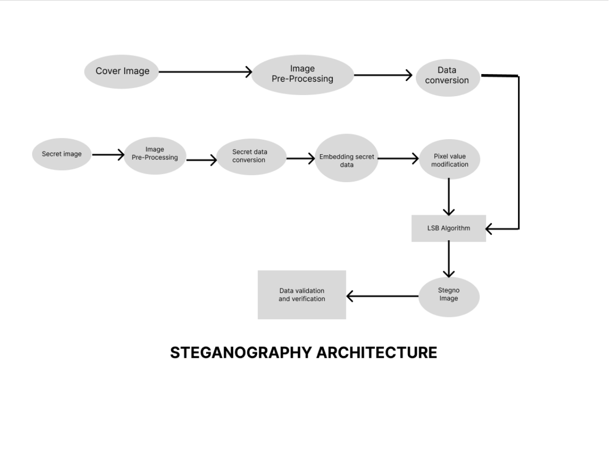


Fig 2: Process of Face Recognition

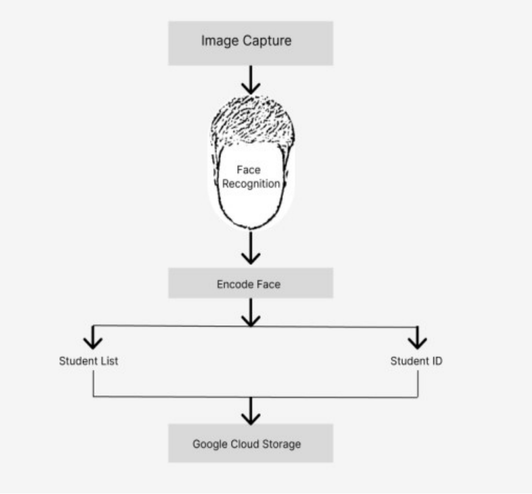


Fig 3: Encode with Real Time Database

IV. EXPERIMENTAL RESULT

1) Face Recognition

Step 1: Using cap.read(), the program reads a frame from the video stream.

Step 2: Using cv2.resize (), the picture is shrunk to a fourth of its original size.

Step 3: cv2.cvtColor () is used to convert the resized image's BGR format to RGB format.

Step 4: Faces are found in the image using face recognition and the face recognition library.face_locations().

Step 5: Faces in the image are encoded with the help of the face recognition library.face_encodings().

Step 6: A mode picture is shown in the corner of the frame, and the original image is superimposed with the current frame.
Step 7: The face recognition library is used to compare each face discovered in the picture with a list of recognized faces.compare_faces().
Step 8: The face recognition library is used to measure the separation between the face and the database of recognized faces.face_distance().
Step 9: Using np.argmin(), the closest match's index is discovered.
Step 10: In general, the algorithm compares faces in a video stream to a list of recognized faces using facial recognition.

WEEKS	NO OF STUDENTS RECOGNIZED	ACCURACY (%)	NO OF STAFF RECOGNIZED	ACCURACY (%)
1	250	95	100	93
2	250	94	100	96
3	250	98	100	96
4	250	96	100	97
5	250	97	100	98
6	250	96	100	97
7	250	97	100	97
8	250	100	100	100

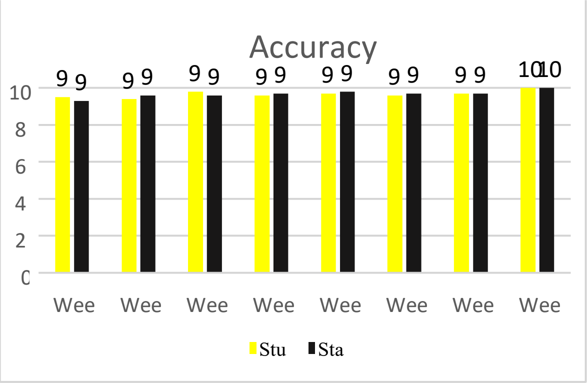
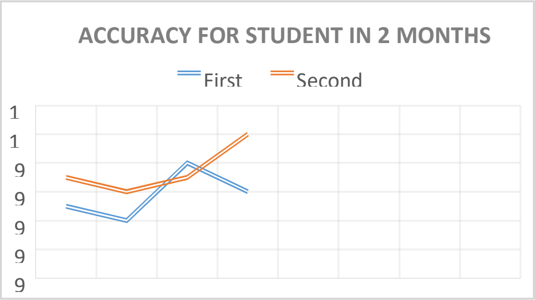


Fig 4 : Accuracy for student and staff per weeks
Bar Graph represents the accuracy of the student & staff from Table to analyze the accuracy recorded in week.

Comparision For First And Second Month Accuracy

For face recognition best understating we take sample accuracy recorded for two months for both teacher & student encoded face. Graph represents the accuracy of the students and Graph represents the accuracy of the Staff recorded in the past two month. These graph are compared by month 1 and month 2 to identify the improvement of the accuracy.



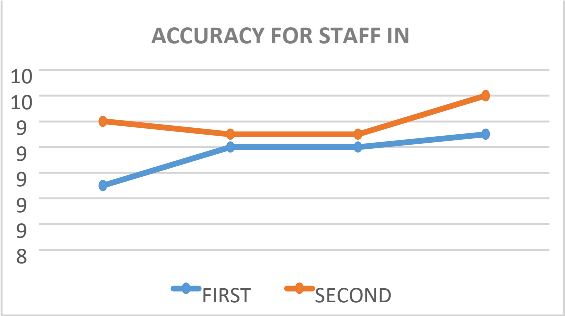


Fig 6: Accuracy for students in 2 months.

2) Steganography Steps

Step 1: The function loads both the cover picture and the secret image before scaling the secret image to fit the dimensions of the cover image.

Step 2: It iterates through each pixel in the cover picture, extracting the red, green and blue (RGB) values from both the cover image and the secret image for each pixel.It also extracts the alpha value from the hidden picture if it contains an alpha channel (that is, if it is in RGBA mode).

Step 3: It performs a bitwise OR operation to merge the red, green, and blue values from the cover and secret pictures before storing the outcome in the new variables new_r, new_g, and new_b.The RGB values of each pixel in the cover picture are then changed to the new values (new_r, new_g, and new_b).

Step 4: The binary representation of the RGB values is combined using the bitwise OR operator. The most significant bit (MSB) of each color component in the cover picture is moved to its equivalent place in the hidden image's least significant bit (LSB).

Step 5: the cover images other color components are still present. As a result, the cover picture's visual look isn't drastically altered but the secret image data may be concealed within the cover image data.

3) Steganography

Graph represents the comparison of the Existing technology vs proposed technology for the steganography algorithm. This will help to easily identify the difference and improvement in Quality of the Stegno-image obtained by the proposed model.

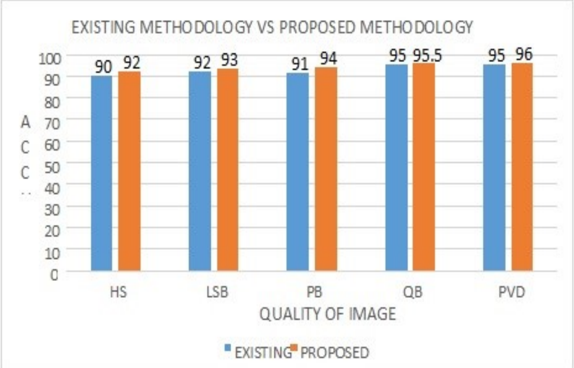


Fig 7: Existing Methodology Vs Proposed Methodology.

V. ALGORITHM

1) *Viola-Jones algorithm*

This approach is centered on teaching a model to distinguish between faces and other objects. Although the framework is still widely used for face recognition in real-time applications, it struggles to recognize faces that are hidden or not facing in the right direction.

2) *Convolutional neural network-based*

A deep learning ANN called a convolutional neural network (CNN) is used to analyze pixel data in image recognition and processing. An R-CNN, or region-based CNN, offers suggestions using a CNN framework that locates and categorizes objects in pictures. These suggestions concentrate on sections or regions in a photograph that resemble other locations, such the pixelated area of an eye. The R-CNN knows it has discovered a match when this region of the eye aligns with other parts of the eye. However, CNNs may become too complicated to the point that they "over fit," matching noise-filled areas.

3) *Least Significant Bit*

This code's algorithm is a straightforward instance of LSB (Least Significant Bit) steganography. When using LSB steganography, the secret data is concealed within the cover image's pixel values' least significant bits, where altering the least significant bit does not significantly alter the cover image's visual appearance. The secret picture is concealed within the cover image using this code, which substitutes the least significant bits of the cover image's pixel values with the most significant bits of the hidden image's pixel values.The cover picture and the secret image are loaded specifically in this function, and the secret image is then scaled to the cover image's specifications. The pixel information for both photos is then acquired. The least significant bits of the red, green, and blue values for each pixel in the cover picture are swapped out for the most significant bits of the corresponding values in the secret image. The output picture is the resultant changed cover image.

VI. LITERATURE SURVEY

The research of several video steganography techniques is additions of image-based steno techniques. The research founds the various works from different authors.

In[1] D. Prabhu, S. Vijay Bhanu, S. Suthir: To achieve security and privacy in the cloud computing (CC) environment, biometric authentication is critical. Several types of biometrics are utilized in the authentication process, with the fingerprint being a popular choice for optimal security. However, it is readily taken, inadvertently divulged, and difficult to recall. As a result, biometric authentication techniques are required, as is an encryption mechanism to strengthen the security of the authentication process. In this regard, this work presents a multiple share creation for the cloud environment using an optimum signcryption-based biometric authentication system (MSCOS-BAS- FLNN-PeSeOA).

In[2] Manohar N and Peetla Vijay Kumar: Secure communication is processed via video steganography. When we look at the history of steganography, we see that it was concealed in a variety of ways, including tablets covered in wax and writing on rabbit stomachs. The approaches for doing secure steganography communication using videos are taken into consideration in this study.

In[3] Shahid Rahman , Jamal Uddin , Muhammad Zakarya , (Senior Member, Ieee), Hameed Hussain , Ayaz Ali Khan , Aftab Ahmed , And Muhammad Haleem : The best method for protecting data from potential dangers is steganography. The need for effective information concealing strategies in the new digital sphere has long been a sticking point for academics and researchers.

In[4] Lingyu Zhang , Qingxiao Guan , And Hongfei Yu: The Important Picture (IM) may be many times larger than the cover image thanks to a revolutionary image concealing approach that is shown in this research. It also has an enhanced block matching mechanism and high embedding capacity.

In[5] Nandhini Subramanian , (Member, IEEE), Omar Elharrouss , Somaya Al-Maadeed , (Senior Member, IEEE), And Ahmed Bouridane , (Senior Member, IEEE): The method of hiding information, such as text, images, or videos, under a cover picture is known as image steganography. The secret information is concealed so that human eyes cannot see it. Recent years have seen an surge in interest in deep learning technology, which has shown to be a potent tool in a number of applications, including picture steganography.

In[6]: Mohammed Aloraini , (Member, IEEE), Mehdi Sharifzadeh , (Member, IEEE), And Dan Schonfeld , (Senior Member, IEEE): The major method used by algorithms for compressed picture steganography to incorporate concealed message at the moment is to reduce distortion or statistical detectability. However, there are no closed-form solutions for JPEG steganography due to purely heuristic distortion definitions and numerically solvable equations in statistical models.

In[7]: Sai Wang: Information security is crucial given the internet's and computers' fast growth. Identification has traditionally been accomplished mostly through passwords or ID cards, however these methods are easily lost or stolen. Face recognition systems, however, can swiftly and easily resolve the issue, therefore it is presently starting to be widely employed in a variety of fields.

In[8]: Busra Kocacinar , Bilal Tas , Fatma Patlar Akbulut , (Member, IEEE), Cagatay Catal , And Deepti Mishra , (Senior Member, IEEE): The Covid-19 virus and its variations have spread around the world, causing new requirements and issues that have a significant impact on our daily life. The use of masks as the most efficient method of stopping the virus's propagation and transmission has introduced a number of security flaws. It is crucial to detect those who break this rule since wearing a mask is a common occurrence in the world we live in today.

In[9]: Harshit Nigam , Mohammad Nabigh Abbas , Mohneesh Tiwari , Himanshu Mali Shalaj , Ms. Nida Hasib: The largest advancement in biometric identification and security since fingerprints is facial recognition, which utilizes a person's face traits to identify and recognize them. Smartphones put a futuristic technology that appears too far-fetched straight out of a science fiction book in our hands. Whether it's mobile phones, sophisticated security systems, ID verification, or something as basic as logging into a website, facial recognition has become popular as the primary way of identification.

VII. CONCLUSION

The suggested technique may be used to cellphones, security cameras, and other gadgets during the worldwide epidemic. This essay explores the definition of human recognition face recognition, which is a biometric identification method based on a person's facial traits that uses a camera to photograph a person's face and a set of algorithms to identify them. The final and most crucial step is to describe how biometrics are used in four different fields. It is a reliable way to identify someone immediately. For entries needing biometric verification, this technology ensures a new orientation toward an accurate face recognition solution without human interaction. It can combine a facial image with a fingerprint image to create a single entity

VIII. REFERENCES

[1] D. Prabhu, S. Vijay Bhanu, S. Suthir.”Design of Multiple Share Creation with Optimal Signcryption based Secure Biometric Authentication System for Cloud Environment”. Accepted 17 Jul 2022, Published online: 08 Aug 2022.

[2] Manohar N and Peetle Vijay Kumar (2020).” Data Encryption & Decryption Using Steganography”Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020).

[3] Shahid Rahman , Jamal Uddin , Muhammad Zakarya , (Senior Member, Ieee), Hameed Hussain , Ayaz Ali Khan , Aftab Ahmed , And Muhammad Haleem(2023).” A Comprehensive Study of Digital Image Steganographic Techniques”. Date of publication 16 January 2023 in IEEE Access.

[4] Lingyu Zhang , Qingxiao Guan , And Hongfei Yu.” An Image Hiding Method of Block Matching Way with Improved Texture Fusion Feature and High Embedding Capacity Product Code Over Z4”. Date of publication 21 July 2022 in IEEE Access.

[5] Nandhini Subramanian, (Member, IEEE), Omar Elharrouss , Somaya Al-Maadeed , (Senior Member, IEEE), And Ahmed Bouridane , (Senior Member, IEEE).” Image Steganography: A Review of the Recent Advances”. Date of publication January 25, 2021 in IEEE Access.

[6] Mohammed Aloraini , (Member, IEEE), Mehdi Sharifzadeh , (Member, IEEE), And Dan Schonfeld , (Senior Member, IEEE).” Quantized Gaussian JPEG Steganography and Pool Steganalysis”. Date of publication April 5, 2022 in IEEE Access.

[7] Sai Wang.” The Application of Face Recognition System”. Proceedings of the 2021 International Conference on Social Development and Media Communication (SDMC 2021).

[8] Busra Kocacinar , Bilal Tas , Fatma Patlar Akbulut , (Member, IEEE), Cagatay Catal , And Deepti Mishra , (Senior Member, IEEE).” A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System”. Date of publication June 13, 2022 in IEEE Access.

[9] Harshit Nigam, Mohammad Nabigh Abbas , Mohneesh Tiwari , Himanshu Mali Shalaj , Ms. Nida Hasib.” Review of Facial Recognition Techniques”. International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue I Jan 2022- Available at www.ijraset.com.

[10] Al-Assam, H., Hassan, W. and Zeadally, S., 2019. Automated biometric authentication with cloud computing. In Biometric-Based Physical and Cybersecurity Systems (pp. 455-475). Springer, Cham.