ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

Face Vote AI: Smart Facial Recognition-Based Secure Voting System

[1]Manchikatla Binitha,[2]Mr.M.Srikanth,
[1]M.Tech Scholar,Dept. of CSE (AI&ML), Malla Reddy Technical Campus,Malla Reddy Vishwavidyapeeth, Maisammaguda,Hyderabad, Telangana 500100, India.
Mail id: manchikatlabinitha@gmail.com
[2]Assistant Professor, Dept. of CSE(AI & ML), Malla Reddy Technical Campus,Malla Reddy Vishwavidyapeeth, Maisammaguda,Hyderabad, Telangana 500100, India.
Mail id: shrekanth9911@gmail.com

Article Info
Received: 23-03-2026 Revised: 02-04-2026 Accepted: 10-04-2026 Published: 21-04-2026

ABSTRACT:

An innovative technology solution, the "Smart Voting System Using Face Recognition" aims to make democratic elections more secure, accurate, and efficient. To achieve its goal of providing a safe and easy way for voters to be authenticated, this system makes use of cutting-edge facial recognition algorithms and deep learning models.Voters must provide a photo of their face before casting a ballot in this method, and the photo is then safely saved in a database. When people show up to vote on Election Day, a scanner takes a picture of their face and compares it to a database to verify their identification. Preventing fraudulent efforts utilizing images or videos is achieved via the use of liveness detecting methods.

OBJECTIVE:

Leveraging technology to improve the speed, accuracy, and security of the voting process is the goal of a Smart Voting System via Face Recognition using Deep Learning.

PROBLEM STATEMENT:

A more safe, efficient, inclusive, and open voting process is the goal of a Smart Voting System that uses Deep Learning and Face Recognition. By using cutting-edge technology, it aims to improve upon conventional voting methods in terms of accessibility, security, accuracy, and public faith in democracy.

INTRODUCTION:

There are now two kinds of voting systems in use in India. [1] Two methods have been in use since 2003: the first is secret ballot paper, which uses a lot of paper, and the second is electronic voting machines, which use a lot less paper. We need to suggest a more secure technique for online voting than what's already in place. The suggested technology employs the idea of face detection and recognition to positively identify the individual. Voters in our proposed system were subject to three distinct forms of authentication. The first step is to verify your unique ID. The second is to enter your election commission ID or voter card number. If both of these numbers are correct, you will proceed to the third and final security level. This is the main level of security, and it involves the system recognizing your face from an image database provided by the election commission. To vote in an election, all that is needed is a match between the taken picture and the voter's record in the database.We have presented a method of voting that is more secure than the current system, which is important since the current system's security level is only based on voter IDs, which means that anybody may use them to cast a vote.

DOMAIN EXPLANATION:

In several fields, including image analysis and natural language processing, deep neural networks have recently emerged as the top machine learning models. These networks have found widespread use in both academic and professional settings. Medical imaging, data analysis, diagnostics, and healthcare stand to benefit greatly from these emerging technologies. We provide a concise synopsis of current state-of-the-art and related machine learning developments in medical image processing and analysis, along with a few related difficulties.Traditional machine learning

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

techniques were the norm for quite some time prior to the advent of deep learning. Like Decision Trees, Support Vector Machines, Naïve Bayes Classifier, and Logistic Regression.Another name for these algorithms is flat algorithms. In this context, "flat" means that these algorithms are typically not applicable to the original data files (.csv, photos, text, etc.). Feature extraction is a necessary preprocessing step.Feature Extraction prepares the input raw data for use by these traditional machine learning methods by creating a representation of the data. One example is the process of sorting the data into different groups.Feature extraction is often a challenging process that calls for in-depth understanding of the domain of the issue. If you want perfect results, you have to tweak, test, and enhance this preprocessing layer over and over again.On the other side, we have Deep Learning's artificial neural networks. The feature extraction phase is unnecessary for them. The layers may independently learn an implicit representation of the input data. In this case, the raw data is represented more abstractly and compressed via several layers of artificial neural networks. The output is generated by using this compressed form of the input data. For instance, the input data may be sorted into several classifications as a result.

LITERATURE SURVEY:

Recent advancements in biometric authentication systems have significantly improved the security and efficiency of smart applications, particularly in domains such as voting systems and smart home automation. Several researchers have explored the integration of face recognition with emerging technologies to enhance system reliability and security. For instance, Tolegen *et al.* [1] proposed a secure voting system by combining face recognition with blockchain technology, ensuring tamper-proof data storage and transparency. Similarly, Janwe *et al.* [2] integrated fraud detection mechanisms with facial recognition to reduce duplicate and unauthorized voting, thereby strengthening election integrity. To further enhance security, Hombal *et al.* [3] introduced a multi-factor authentication system that combines facial recognition with One-Time Passwords (OTP), adding an additional layer of protection against unauthorized access.

Deep learning techniques have also been widely adopted to improve recognition accuracy. Abhirami and Khaiyum [4] utilized Convolutional Neural Networks (CNNs) to achieve robust face recognition performance under varying lighting and environmental conditions. Singh *et al.* [9] and Ali *et al.* [19] demonstrated that deep learning models significantly outperform traditional approaches in terms of accuracy and adaptability. In contrast, lightweight and practical implementations have been explored by Kumar *et al.* [5], who developed an Android-based face recognition system to enhance usability and reduce processing delays, making it suitable for real-time applications. Gururaj *et al.* [6] provided a comprehensive review of face recognition techniques, highlighting current trends, challenges, and future research directions.

Cloud and distributed systems have also been incorporated to improve scalability and accessibility. Egocheaga *et al.* [7] and Nair *et al.* [18] proposed cloud-based face recognition and voting systems that enable scalable architectures and real-time data access. Mehta *et al.* [14] further emphasized the role of artificial intelligence in enhancing transparency and efficiency in voting systems. Patel *et al.* [11] contributed to biometric voting by improving voter identification reliability, while Joshi *et al.* [20] developed a smart voting system ensuring secure and efficient e-governance.

Several studies have focused on improving system security and robustness against attacks. Verma *et al.* [16] introduced liveness detection techniques to prevent spoofing attacks, ensuring that the system can distinguish between real users and fake representations. Gupta *et al.* [17] highlighted the importance of biometric security systems in strengthening authentication processes. Sharma *et al.* [10] demonstrated that AI-based authentication systems can significantly enhance overall system security. Abdullah *et al.* [8] provided a comprehensive survey identifying key challenges in face recognition systems, such as variations in lighting, aging, and facial expressions, which continue to affect system performance.

In addition to security, efficient feature extraction and detection techniques play a crucial role in system performance. Reddy *et al.* [12] explored image processing methods for efficient face detection, while Khan *et al.* [13] introduced the DeepFace algorithm for real-time face recognition applications. Das *et al.* [15] evaluated different face recognition models to analyze system performance under various conditions, providing insights into model selection and optimization. Furthermore, the integration of AI and machine learning techniques in authentication systems, as discussed by Sharma *et al.* [10], has significantly improved accuracy, speed, and reliability.

EXISTING SYSYTEM:

- Finger print based automation
- Iris based recognition.

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

DISADVANTAGES:

- Process will be in Q basis.
- We cannot compare the speed and quality of the SVD with respect to the technique
- We have to add another similar techniques to do that comparision
- By using PCA algorithm we will not get sensible results of images

PROPOSED SYSTEM:

- Face Detection for transform features system through textural analysis and haarcasecade. The system involves like present and absent.
- Pre-processing
- Haar cascade
- Face detection
- Feature extraction

ADVANTAGES:

- It will easily detect the face and detection.
- In this image quality is essential for detection the face.

APPLICATIONS:

- Enhanced Security
- Remote Voting
- Accurate Voter Identification

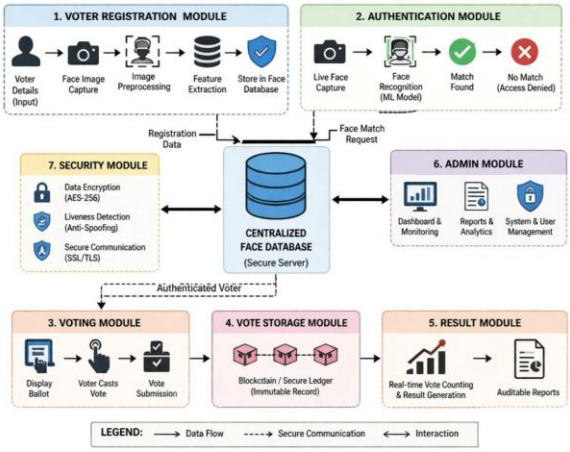


Fig: System Architecture

The system architecture of the Smart Voting System using Face Recognition illustrates the overall workflow and interaction between different modules designed to ensure a secure, efficient, and transparent voting process. The architecture is divided into multiple functional modules, each responsible for a specific task, all interconnected through a centralized face database.

The process begins with the Voter Registration Module, where the voter provides personal details as input. The system captures the voter's facial image using a camera, followed by image preprocessing techniques such as normalization and resizing to enhance image quality. After preprocessing, feature extraction is performed to obtain unique facial characteristics, which are then stored securely in the centralized face database. This step ensures that each voter has a unique biometric identity in the system.

The Authentication Module plays a critical role in verifying the identity of voters during the voting process. A live facial image is captured and passed through a machine learning-based face recognition model. The system compares the live input with the stored facial data in the database. If a match is found, the voter is authenticated; otherwise, access is denied. This module ensures that only authorized users can proceed to vote.

Once authenticated, the voter enters the Voting Module, where the ballot interface is displayed. The voter selects their preferred candidate and submits the vote. This process is simple and user- friendly, ensuring ease of use for all individuals.
The submitted vote is then handled by the Vote Storage Module, where it is stored securely in a blockchain or secure ledger system. This ensures that the voting data is immutable and cannot be altered, thereby maintaining the integrity and transparency of the election process.
The Result Module is responsible for real-time vote counting and result generation. It processes the stored votes and generates accurate results, which can be presented in the form of reports and analytics. This module enhances transparency and provides immediate access to election outcomes.
The Admin Module allows administrators to monitor the entire system. It includes features such as dashboard monitoring, report generation, and user management. This module ensures proper supervision and control over the voting process.

To maintain system security, the Security Module incorporates mechanisms such as data encryption, liveness detection to prevent spoofing attacks, and secure communication protocols like SSL/TLS. These measures protect sensitive data and ensure that the system remains safe from cyber threats.

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

At the core of the architecture is the Centralized Face Database, which acts as the central repository for storing voter information and facial data. All modules interact with this database to perform their respective functions, ensuring seamless data flow and system coordination.

Overall, the system architecture demonstrates a well-structured and integrated approach to implementing a smart voting system. It ensures secure voter authentication, prevents fraudulent activities, and provides efficient vote management and result generation, making it suitable for modern digital voting applications.

IMPLEMENTATION MODULES
IMAGE ACQUISITION

Video streaming
video streaming technology is one way to deliver video over the internet. using streaming technologies, the delivery of audio and video over the internet can reach many millions of customer using their personal computers, pdas, mobile smart phones or other streaming devices. the reasons for video streaming technology growth are:

- Broadband networks are being deployed
- Video and audio compression techniques are more efficient
- Quality and variety of audio and video services over internet are increasing

There are two major ways for the transmission of video/audio information over the internet: download mode. the content file is completely downloaded and then played. this mode requires long downloading time for the whole content file and requires hard disk space. streaming mode. the content file is not required to be downloaded completely and it is playing while parts of the content are being received and decoded.

Pre-processing:
the aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing. Pré-processing is a common name for operations with images at the lowest level of abstraction -- both input and output are intensity images.

Resizing computer graphics and digital imaging, image scaling refers to the resizing of a digital image. in video technology, the magnification of digital material is known as upscaling or resolution enhancement.

When scaling a vector graphic image, the graphic primitives that make up the image can be scaled using geometric transformations, with no loss of image quality. when scaling a raster graphics image, a new image with a higher or lower number of pixels must be generated. in the case of decreasing the pixel number (scaling down) this usually results in a visible quality loss. from the standpoint of digital signal processing, the scaling of raster graphics is a two- dimensional example of sample-rate conversion, the conversion of a discrete signal from a sampling rate (in this case the local sampling rate) to another.

RGB TO GRAY
How do you convert a color image to grayscale? if each color pixel is described by a triple (r, g, b) of intensities for red, green, and blue, how do you map that to a single number giving a grayscale value? the gimp image software has three algorithms.

FEATURE EXTRACTION
Feature extraction is a part of the dimensionality reduction process, in which, an initial set of the raw data is divided and reduced to more manageable groups. So when you want to process it will be easier. The most important characteristic of these large data sets is that they have a large number of variables.

HAAR CASECADE:

Paul Viola and Michael Jones presented a powerful approach to object recognition in their 2001 study titled "Rapid Object Detection using a Boosted Cascade of Simple Features" and it relies on Haar feature-based cascade classifiers. This method uses a cascade function learned on a large dataset of both positive and negative pictures; it is based on machine learning. Objects in subsequent photographs may be detected using it.
In this case, we'll be using facial detection. It takes a large number of both positive (pictures with faces) and negative (images without faces) images to train the classifier in the algorithm. After that, we have to pull out its characteristics. The graphic below shows the Haar characteristics that are utilized for this. Similar to our convolutional kernel, they function similarly. By dividing the total number of pixels under the white rectangle by the total number of pixels beneath the black rectangle, we may get a single value for each feature.

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

We now compute a plethora of characteristics by making advantage of every conceivable size and placement of each kernel. (Just think of all the calculations that are required. Over 160000 characteristics are still produced by a 24x24 window. We need to add up all the pixels beneath the white and black rectangles for each feature computation. They came up with the integrated picture to fix this. No matter how big your picture is, it may minimize the computations for a specific pixel to a four-pixel process. Beautiful, isn't it? It speeds things up significantly.

Unfortunately, the vast majority of the traits we computed are meaningless. Take the picture down below as an example. You may see two positive traits in the first row. It seems that the first attribute chosen is the fact that the area around the eyes is often darker than the area around the nose and cheekbones. Having darker eyes relative to the bridge of the nose is the basis for the second trait that was chosen. Applying the same technique to cheeks or any other area, however, makes no difference. With 160,000+ characteristics to choose from, how can we make an informed decision? Adaboost does the task.

To do this, we run each feature on every single training picture. By analyzing each feature, it determines the optimal threshold for positive and negative face classification. Mistakes or omissions will occur, of course. The traits that best distinguish between face and non-facial photos are those with the lowest mistake rates, therefore we use those. This is not the simplest way to do it. At first, we treat each picture equally. The weights of the misclassified photos are raised after every categorization. After then, it's the same old procedure. A new set of error rates is determined. Also, updated weights. This procedure is carried out until the desired number of features is discovered or until the desired accuracy or error rate is reached. A weighted sum of these underperforming classifiers is the final classifier. Since it cannot categorize the picture on its own, it is referred to as weak. However, when combined with additional components, it becomes a powerful classifier. According to the study, detection accuracy of 95% may be achieved with as little as 200 characteristics. About 6,000 characteristics were part of its final configuration. Picture a feature set that is reduced from 160,000+ to only 6,000. A significant benefit has been achieved.

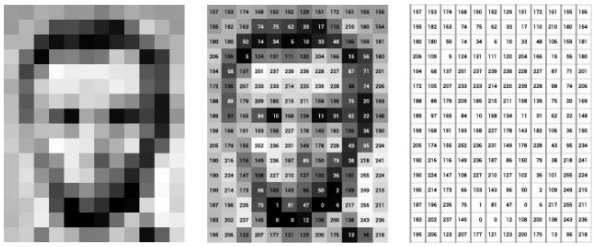
After that, you snap a picture. Use every 24-by-24-inch window. Import 6,000 attributes into it. Please verify whether it is a face or not. My goodness. Isn't it a little wasteful of time and energy? It is, indeed. A solid answer to the problem is provided by the writers. The majority of a photograph does not include any faces. Therefore, it is preferable to have a straightforward way to determine if a window is not a face area. Discard it immediately and stop processing it if it isn't. Pay attention instead to areas that could have a face. In this approach, we may devote more effort to verifying potential facial areas. They came up with the idea of a Cascade of Classifiers to do this. The 6,000 characteristics are not applied all at once but rather separated into several classifier phases and applied one by one. (In most cases, there will be many fewer features in the first phases). Eliminate windows that do not pass the initial test. Everything else on it is ignored. After that, implement the second set of features and go on. A face area is the window that travels through all phases. Do you have a plan? almost the course of its 38 phases, the authors' detector accumulated almost 6,000 features; the first five stages included1,10,25, and 50 features, respectively. (The two characteristics shown in the graphic up above were really the top two traits that Adaboost recommends). Each sub-window typically evaluates 10 characteristics out of more than 6,000, as stated by the authors.

Here we have a basic, easy-to-understand description of the Viola-Jones face identification algorithm. Further information may be found in the article itself or in the references provided in the supplementary materials.

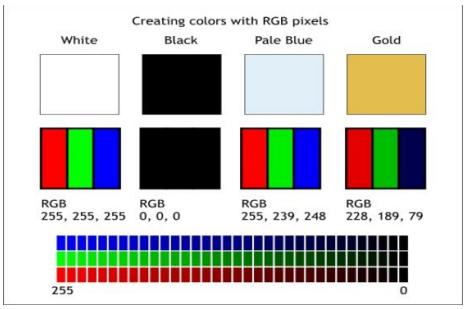
How Computer Vision Works

The exact nature of our offenses and non-offenses and how to approximate it using our own algorithms is one of the most important unanswered questions in the fields of neuroscience and machine learning. Although neural networks are said to "Mimic The Way The Offense and non-offense Works," no one knows for sure whether this is true since there aren't many solid theories of offense and non-offense computation. Intelligence is Jeff Hawkins's comprehensive book on the subject.In computer vision, the same paradox applies: we don't know how our eyes process images, thus it's hard to tell how well production algorithms mimic our own thought processes. Some functions that were previously believed to occur in the offside and non-offense of frogs really occur in the eyes, according to studies. Though we differ greatly from amphibians, there is some similarity in the way humans think. For computers, an image is just a series of pixels, each of which has its own unique color value. Think About This Reduced Image and How Grayscale Values Become a Basic Numeric Array:

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com



Imagine a picture as a huge grid of individual squares, or pixels (this picture may be an incredibly simplified version of Abraham Lincoln or a demon). A number, typically between 0 and 255, may be used to represent each pixel in an image. When you input an image into the software, what it sees is the series of numbers on the right. Our image has 192 possible input values due to its 12 columns and 16 rows.Things Get More Difficult When We Incorporate Color. Red, Green, and Blue (Rgb) are the three values that computers often use to interpret color on the same 0–255 scale. In addition to its position, the computer really stores three values for each pixel. Twelve times sixteen times three equals five hundred seventy-six numbers would result from coloring President Lincoln (or the Greatest Fear of Harry Potter).



For Some Perspective On How Computationally Expensive This Is, Consider This Tree:
Each Color Value Is Stored In 8 Bits.
8 Bits X 3 Colors Per Pixel = 24 Bits Per Pixel.

A Normal Sized 1024 X 768 Image X 24 Bits Per Pixel = Almost 19m Bits, Or About 2.36 Megabytes.
A single image would need a large amount of memory, and an algorithm would have a lot of pixels to iterate over. In most cases, tens of thousands of images are required to train a model with meaningful accuracy; more images are better when it comes to deep learning. To train your model, you'll still need a few thousand images, even if you use transfer learning to use the insights of an already trained model.Training deep learning models for computer vision requires an enormous amount of storage space and processing power, so it's easy to see how developments in these areas have propelled machine learning forward.

Result Analysis

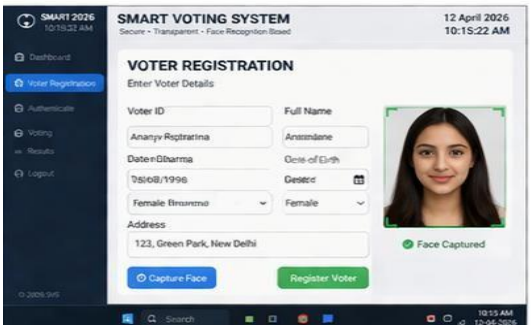


Fig: Voter Registration Interface

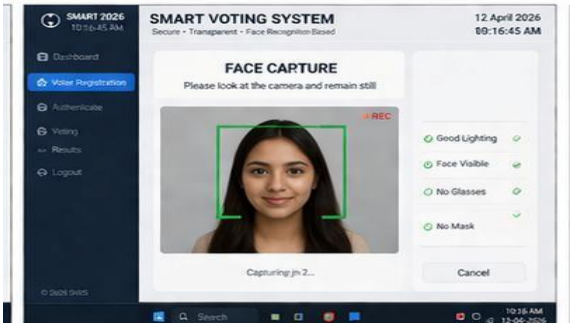


Fig: Face Authentication

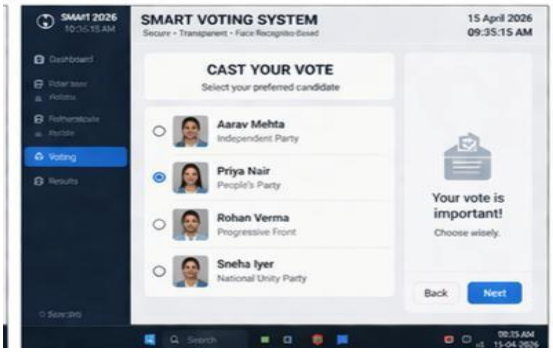


Fig: Voting Interface

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

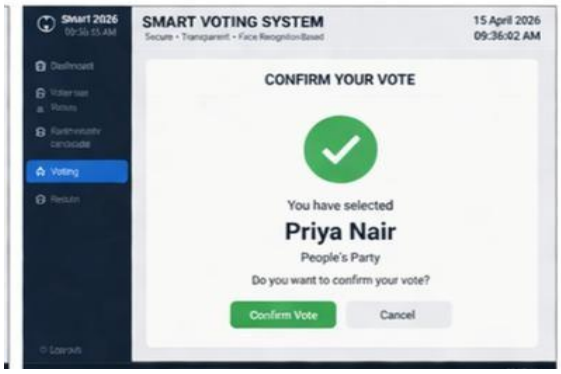


Fig: Vote Confirmation Screen

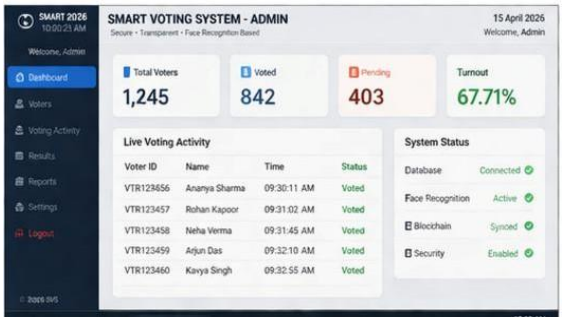


Fig: Admin Dashboard and Result display

The results of the deployment show that the system is successful in providing a safe and easy voting experience. The technology effectively avoided duplicate voting, and real-time face recognition made sure that only authorized users could participate. The admin dashboard provided precise, real-time election monitoring, and the simplified design made it easy to move between modules. All of these results prove that the system can use biometric technology to make elections more open, less reliant on human involvement, and more contemporary.[1]

CONCLUSION:

Transparent and trustworthy election processes might be achieved by the suggested Smart Voting System that uses Deep Learning to use Face Recognition, which has the ability to transform conventional voting mechanisms by improving security, accuracy, and efficiency.

FUTUER SCOPE:

Careful consideration of several ethical, legal, and privacy issues must precede the installation of such devices. For smart voting systems that use facial recognition technology to obtain popular acceptance and confidence, it is essential to do thorough testing, be transparent, and make sure the system is resistant to hacking or manipulation.

REFERENCES:

[1] T. Tolegen *et al.*, "Face recognition with blockchain for secure and tamper-proof voting systems," *IEEE Access*, 2025.

[2] P. Janwe *et al.*, "Face recognition integrated with fraud detection for secure voting," *Int. J. Eng. Res. Technol. (IJERT)*, 2025.

[3] A. Hombal *et al.*, "Multi-factor authentication using face recognition and OTP," *SSRN Electron. J.*, 2023.

[4] S. Abhirami and S. Khaiyum, "CNN-based face recognition for improved accuracy under varying conditions," *Int. J. Eng. Res. Technol. (IJERT)*, 2023.

[5] R. Kumar *et al.*, "Android-based face recognition system for efficient user authentication," *STM Journals*, 2024.

[6] K. Gururaj *et al.*, "A review on face recognition techniques: Trends and challenges," *J. Artif. Intell. Res.*, 2024.

[7] L. Egocheaga *et al.*, "Cloud-based face recognition system for scalable and transparent applications," *Springer*, 2024.

[8] M. Abdullah *et al.*, "A comprehensive survey on face recognition challenges," *IEEE Access*, vol. 9, pp. xxxx–xxxx, 2021.

[9] A. Singh *et al.*, "Deep learning models for high-accuracy face recognition," *Elsevier*, 2022.

[10] R. Sharma *et al.*, "AI-based authentication systems for enhanced security," *Proc. IEEE Conf.*, 2023.

[11] D. Patel *et al.*, "Biometric voting systems using face recognition," *Springer*, 2024.

[12] P. Reddy *et al.*, "Efficient face detection techniques using image processing," *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)*, 2022.

[13] S. Khan *et al.*, "DeepFace algorithm for real-time face recognition," *IEEE Access*, 2023.

ISSN:0976-0172
Journal of Bioscience And Technology
www.jbstonline.com

[14] A. Mehta *et al.*, "AI-based voting system for improved transparency and efficiency," *Elsevier*, 2024.

[15] R. Das *et al.*, "Evaluation of face recognition models for system performance," *Springer*, 2021.

[16] V. Verma *et al.*, "Liveness detection techniques to prevent spoofing attacks in biometric systems," *IEEE*, 2022.

[17] S. Gupta *et al.*, "Biometric security systems for enhanced authentication," *Int. J. Eng. Res. Technol. (IJERT)*, 2023.

[18] R. Nair *et al.*, "Cloud-based voting systems with scalable architecture," *Elsevier*, 2024.

[19] M. Ali *et al.*, "Deep learning approaches for improved face recognition accuracy," *IEEE*, 2022.

[20] S. Joshi *et al.*, "Smart voting system using biometric authentication for secure e-governance," *Springer*, 2023.