International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | may 2022 www.irjet.net p-ISSN: 2395-0072

Dynamic Based face authentication using Video-Based Method

Srikar Banka[1], Smit Parikh[2], Isha Gupta[3], Sambhaji Sarode[4]

[1,2,3] *Student & Dept.of Computer Science and Engineering, MIT-ADT University, Pune Maharashtra, India*
[4] *Professor & Dept.of Computer Science and Engineering, MIT-ADT University, Pune Maharashtra, India*

Abstract: *A system of facial recognition is a computer program for a person to automatically recognize or verify from a digital image or a video source. This can be done by comparing selected face characteristics from the picture and the face database. Face recognition is one of the most important biometric methods. The recognition function is performed by obtaining the facial features from an image of the user's face. However, the current facial authentication system, for instance, the attendance system that uses an image-based approach, has a few drawbacks especially by hacking and granting access to an unauthorized person who does not work in that industry. The proposed system would build a video-based mechanism based on the drawbacks of the current existing system by establishing a dynamic face authentication system. During the user verification, it will be checked by video instead of checking photos in this proposed system. As a result, this system will be more secure for access control. This system can be used in industries, residential, and many more.*

Keywords: Face Authentication, Dynamic System, Video-Based Approach.

1. INTRODUCTION

The level of security implemented in any project management software [32] determines how secure the project is going to be. This includes the privacy and confidentiality of our data, as well as infrastructure security, and network stability. We need to understand the risks and what cyber-criminals are searching for, to understand security better. While ransomware (encrypting files and demanding money to get them back) and major frauds dominate the headlines, something far and less apparent is what most companies face. The offenders simply want to steal our data as well as our business and personal information.

Hackers and scammers will open us up if there is too little security. But too much security can limit our own team's access to the data that they need. Only when security is regularly addressed and referred to at any stage of the planning and implementation of a project, then only can the awareness increase. Facial recognition limits and restricts access to information to those who own it. It made authentication fairly simpler, with nothing much to be fitted and lots of information within minutes to reach.

The facial authentication program has been used in the top institutions and workplaces as a test of securities to ensure there is no space for vandalism. This type of software leaves no room for human error at all and is a big helping hand. Authentication is the method of deciding whether someone is really who or what they believe themselves to be. The authentication method gives control of system access by checking if the user data matches the credentials throughout the authenticated user database or authentication server program. Authentication is important because it allows businesses to safeguard their networks by allowing only authenticated users or processes to access their protected resources, which can involve computer systems, networks, databases, websites, and other software or services based upon the network. The password-based vulnerabilities in authentication are sometimes solved with smarter usernames and password rules such as minimum length and difficulty stipulations, such as capitals and symbols. Password-based authentication and authentication based on knowledge are more vulnerable than systems that need multiple separate methodologies.

In paper [9], there are different types of authentications such as Two-factor authentication, Multi-factor authentication, One Time Password authentication, API authentication, Public-key Cryptography, and biometrics authentication. In Biometric authentication, there are many types such as: - 1) Signature Dynamics, 2) Eye Scans, 3) Fingerprint Recognition, 4) Hand or palm geometry, 5) Voice Recognition, and 6) Facial Recognition. Some other authentication types are:

1. Email Authentication
2. Database Authentication

In paper [25], cloud computing has an on-demand delivery over the online platform of wages-as-you-go IT service providers, which increase costs. Rather than procure, own as well as operate physical cloud servers, a cloud service like Amazon Web Services (AWS) can acquire internet services including computing, storage, and database systems, as required.

There are some benefits to this. We could swiftly change resources from service providers like processing, storing, as well as database systems to the IOTs, machine learning, data lakes, as well as for analytics, and much more, and hence, it provides **agility.** With cloud services, to

interact with future access levels of corporate tasks, we will not have to excessively-provide resources upside. To expand and shrink capability as the business needs shift, we will instantly reduce the operating costs of those tools thereby providing us **elasticity.** Cloud computing enables us to swap capital expenditure economic costs (like data centers and physical servers), and charge for using its services for a lower amount. Hence, it is **cost-saving.**

In most of the existing solutions [14], the face authentication system is static and image-based. When a person comes in front of the camera, the face of that person gets captured, and it gets checked with the face image that is uploaded to the database; if the person is verified, then the person is allowed to enter and if the person is not verified, then the person is not allowed to enter. Here, the image processing method is used for face authentication.

The drawback of the existing system [20] is that it is not secure, even with additional security in the system. A hacker can easily hack the system and then upload a fake profile of a person that he or she desires, who could be a criminal. Once the profile is uploaded, then that person could enter the building and no one would know that the person is unauthorized.

However, the video stream processing of facial images has already been gaining growing attention in biometric technology. A possible outcome of using data integrity that's present in the video frames to focus on improving still picture systems is an instant advantage when using video data. While a substantial amount of study has been performed in comparing still facial photos, the use of face detection videos is much less investigated. The very first stage of video-based face recognition (VFR) is to conduct identification, where a gathering of videos is jump-matched to identify the possible suspect in all occurrences.

In common, VFR methods [16] can be divided into two groups depending on how we exploit the wide range of information present in a video frame: sequence-based, and (ii) set-based, then at a top standard, what separates these different objectives is not whether they use temporal features.

So, by using this method, the system will be able to check the AWS bucket where the video is stored so that the person who is at the gate is granted access or is rejected accordingly.

Based on the above reading, we proposed a face authentication system dynamically using the video-based method.

2. PROPOSED SYSTEM

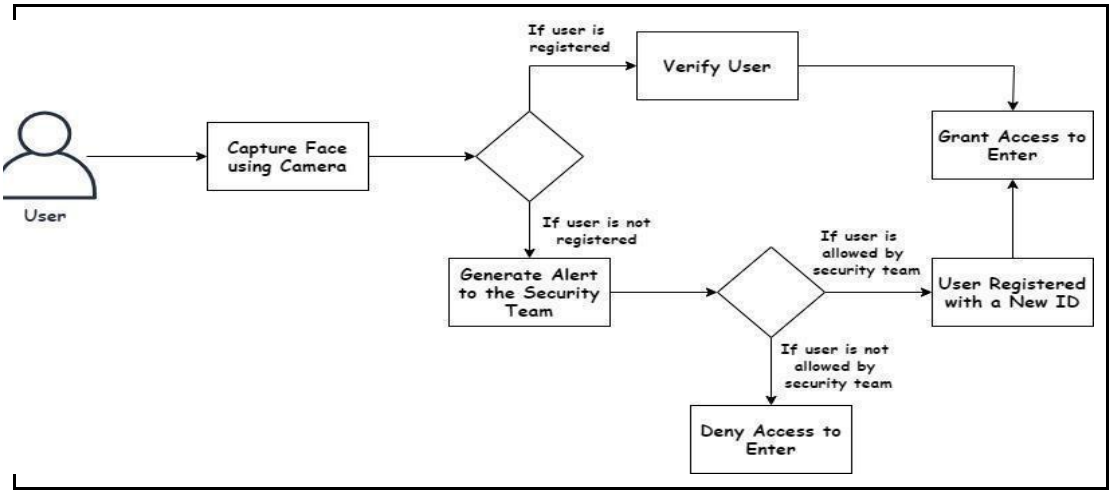


Figure 1 - Working of the Security Protocol

- From this system (Fig, 1), a safer way to facial authentication can be offered to industries, offices, buildings, and residential apartments.
- In the existing system [4], the user's picture is captured by the camera at the entrance. Then the system checks if the user is registered or not by checking his/her picture from the database. This method is proven to compromise security at times.
- In the working of the security protocol (Fig. 1) when a user reaches the entrance, the camera at the entrance will capture the user's face to allow his/her entry. A video-based approach is used in the proposed solution, in which a video is taken and saved into the AWS Bucket. Then, the video is checked frame by frame dynamically with the other existing videos present inside the AWS bucket. And this footage is picked up directly from

CCTV cameras present in the industry, office, etc. for a more secure system.

- If the user is registered, then he will be granted access to enter the premises. And if the user is not registered, an alert will get generated to the security team that he/she is not authorized or not registered. The alert will get generated on a web portal for the Security Team to keep track of the security.

- So, the security team determines whether to allow a person inside or not after the alert is witnessed. If the individual is allowed, then a new user with a new ID is created and the video is saved inside the AWS bucket [25][26].

- If an unregistered user comes to visit the premises after the working hours, the user will not be allowed inside. The video of the user that is captured will get deleted. However, his/her picture will be captured and the name and the time of the visit will get stored in the database for security purposes

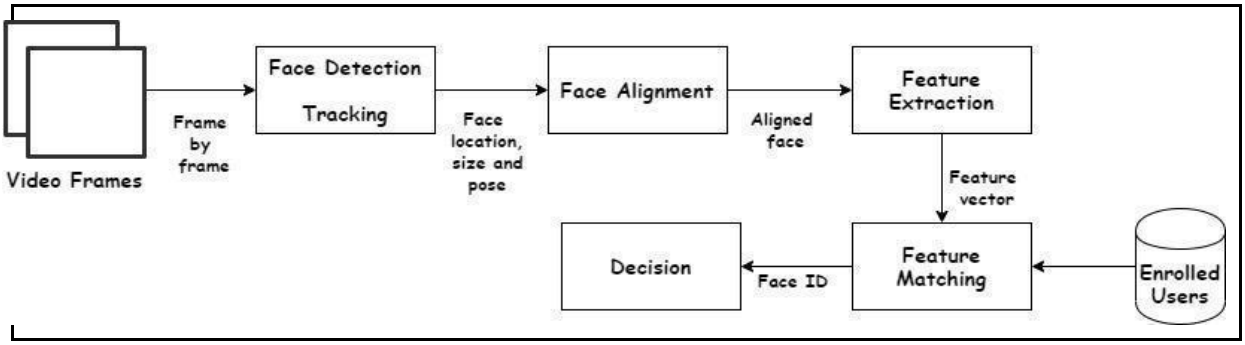


Figure 2 - Video-based Approach

- In the video-based approach figure (Fig. 2), the video is checked frame by frame dynamically with the other existing videos present inside the AWS bucket. And this footage is picked up directly from CCTV cameras present in the industry, office, etc. for a more secure system.

- In the existing systems [5], static facial authentication methods are being used. However, a dynamic facial authentication method will be used in the proposed system.

2.1 Mathematical Model

Local Binary Pattern (LBP) [29] is a fast and convenient way operator that identifies the pixels in the image by thresholding almost every pixel's neighbourhood as well as considers the outcome as a binary number

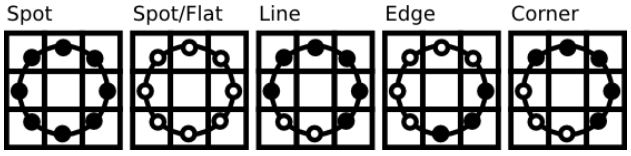
Algorithm description of LBP: - A more normal description of LBP can be written as: -

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p s(i_p - i_c)$$

with the help of x_c and y_c as central pixel with intensity i_p and i_c of the neighbour pixel S is sign function defined as: -

$$s(x) = \begin{cases} 1 & if \quad x \geq 0 \\ 0 & if \quad x < 0 \end{cases}$$

This definition helps you to capture an image with very fine-grained descriptions. The authors were able to compete for texture classification with state-of-the-art tests. It was noted soon after the operator was written that a fixed neighbourhood fails to encode information that varies in size. Therefore, the operator has been generalized in [AHP04] to use a variable neighbourhood. The idea is to match an arbitrary number of nearest neighbours with a variable radius on a circle, which allows the following neighbourhoods to be captured:



For a given point x_c and y_c, the position neighbour x_c, y_c, pϵP can be calculated by: -

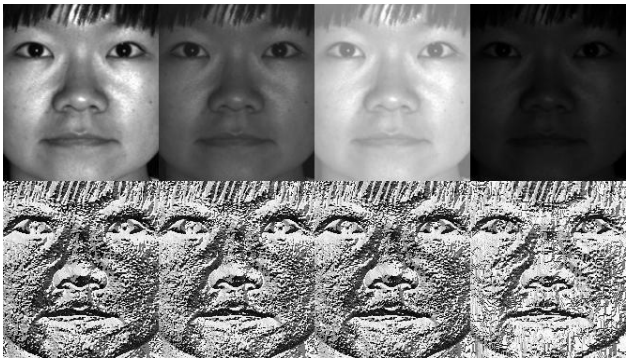
$$x_p = x_c + R\cos(\frac{2\pi p}{P})$$

$$y_p = y_c - R\sin(\frac{2\pi p}{P})$$

where R is the radius of the circle and P is the number of sample points.

$$f(x,y) \approx \begin{bmatrix} 1-x & x \end{bmatrix} \begin{bmatrix} f(0,0) & f(0,1) \\ f(1,0) & f(1,1) \end{bmatrix} \begin{bmatrix} 1-y \\ y \end{bmatrix}.$$

The LBP operator is by default robust against monotonous gray-scale transformation. By looking at the LBP picture of a digitally transformed image, we can easily notice how an LBP image looks like.



2.2 Results

2.2.1 Face Data set: -

OpenCV (Open-Source Computer Vision Library) [30] is also an open-source computer vision and application library for machine-learning. OpenCV was designed to provide a shared computer vision platform and to promote its use of machine perception in commercial applications. As a BSD-licensed software, OpenCV [30] allows the use and modification of the code for companies.

OpenCV face recognizer [31] accepts information in a given format to know which face belongs to which person. It has two vectors to it:

- One is a human's face.
- The second is the labels of an integer for each face.

In data gathering (Fig. 4), the face is detected in the stored video which is downloaded from the S3 storage provided by the AWS services. Then, 30 images of that detected face are captured, which will get used for training the model.

All the 30 images will get stored in the dataset folder with a unique user number and will get uploaded in the database.

In the face dataset module (Fig. 3), the process of data gathering is explained which will be required for creating a face dataset.

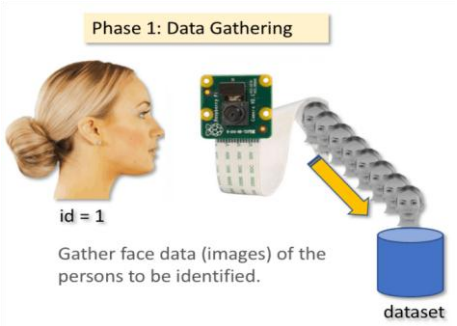


Figure 3 [21] - Face dataset module

The steps to create the data set are:

1. Read all the videos from the AWS bucket.
2. Extract unique user ID and also images of the person containing the unique user ID.
3. Read all the person's images, and apply face detection to each of them.
4. Add each face-to-face vector with the unique user ID of the corresponding individual.

The data gathering figure (Fig. 4) depicts how the face is detected and how the unique user id is used to store the face dataset.

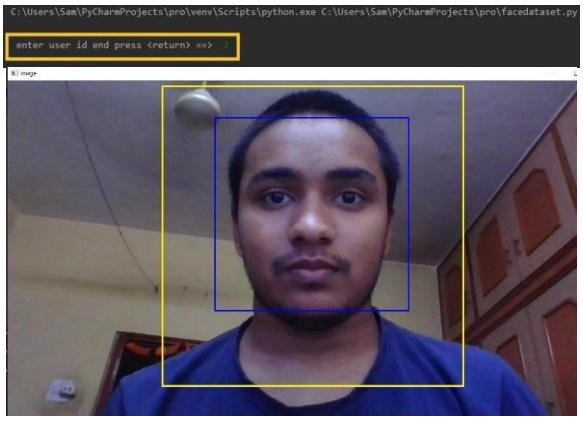


Figure 4 - Data gathering

30 images are captured from the video (Fig. 5). and this is how the face dataset can get stored in the specific user dataset folder, respectively.

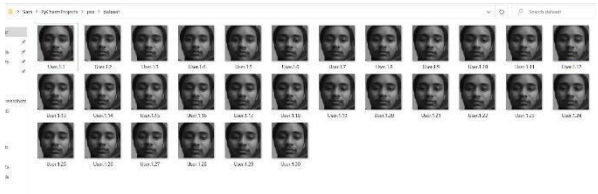


Figure 5 - Images captured from video

In the AWS bucket (Fig. 6), after the dataset folder is created, the entire folder is uploaded to the bucket under the images' folder.

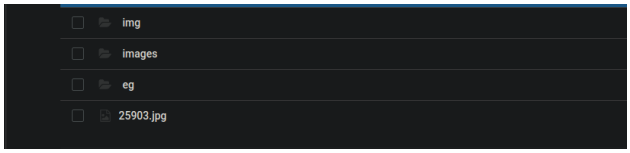


Figure 6 - AWS Bucket

2.2.2 Face training: -

OpenCV uses a different type of face recognition method, they are: -

1. Eigenface
2. Fisherface
3. Local binary pattern Histogram (LBPH)

In this project, the local binary pattern histogram (LBPH) method has been used.

The images which are stored in the dataset folder are then used to train the model which can detect that particular person.

In the face training module (Fig. 7), the trainer will get the dataset and the assigned user id for training and storing the data in the trainer.yml file.

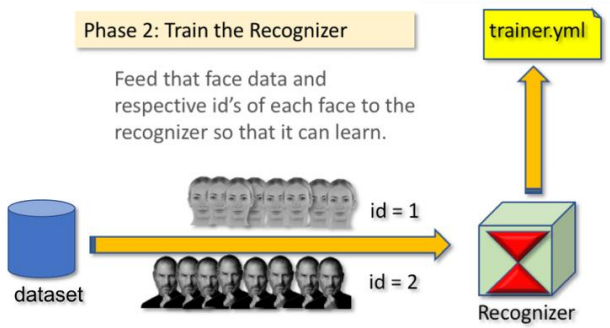


Figure 7 [21] - Face training module

Once the face dataset module is initialized, the Haar cascade trainer will get used to training our model.

The training facial dataset (Fig. 8) depicts the process of training, which takes a few seconds to get trained. The time to train depends on the number of images present in the database.

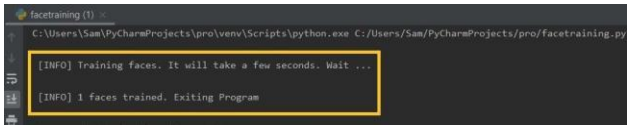


Figure 8 - Training facial dataset

2.2.3 Face Recognition: -

In the face recognition module (Fig. 9), the system detects the face to check whether the face is detected or not.

Then, the system takes the help of the trained model (trainer.yml file) to check from the database whether the person is recognized or not.

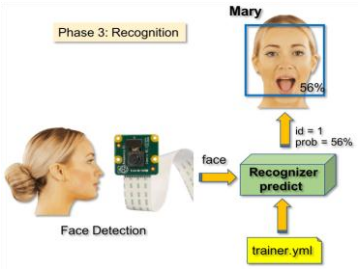


Figure 9 [21] - Face recognition module

In the recognition accuracy figure (Fig. 10), after using the given face dataset, gathered from the uploaded video and trained dataset file, we got the recognition accuracy of 70% from the webcam. The recognition accuracy will increase for higher quality cameras.

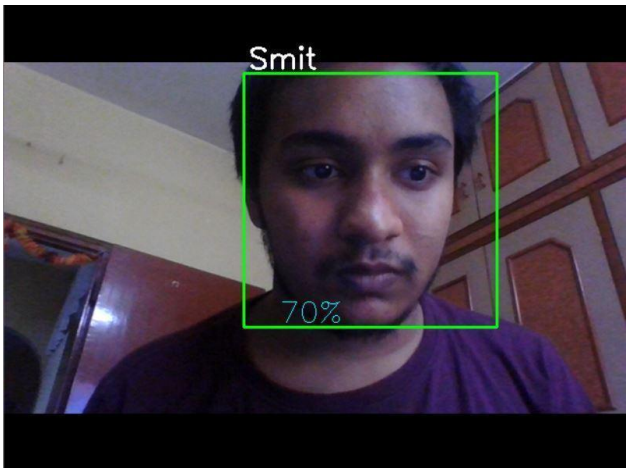


Figure 10 - 70% Recognition Accuracy

The integrated module workflow figure (Fig. 11) shows how all the integrated modules will work together, right from the data gathering of the face dataset to the facial recognition of the person.

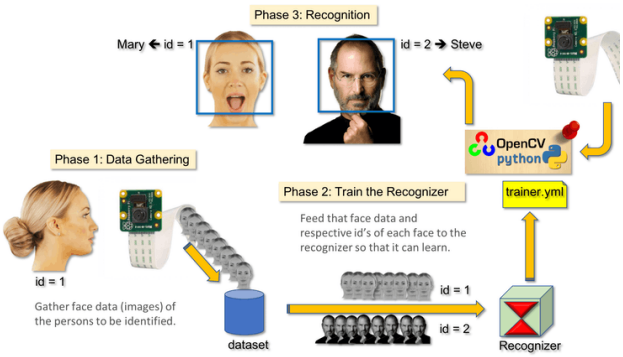


Figure 11[21] - Integrated module workflow

The table for factors affecting the recognition accuracy (Table 1) shows us about the performance evaluation of our proposed video-based method.

Table 1 - Table of factors affecting the recognition accuracy.

No. of test images	No. of recognized images	Accuracy	Remark
Dataset1 (30)	30	100%	Due to the usage of a higher camera quality.
Dataset2 (30)	26	86%	Due to lower image quality captured from a general webcam.
Dataset 3 (30)	24	80%	Due to different illumination conditions captured from a general webcam.
Dataset 4 (30)	21	70%	Due to different face orientation & lower image quality condition captured from a general webcam.

The pie chart for the recognition rate (Fig. 12) is the representation of the average the recognition accuracy rate from Table 1.

Here, we get a false rate of 14% on an average because of the low camera quality as well as varying illumination conditions. However, we would easily be able to achieve a false rate of 5% or less with superior camera quality.

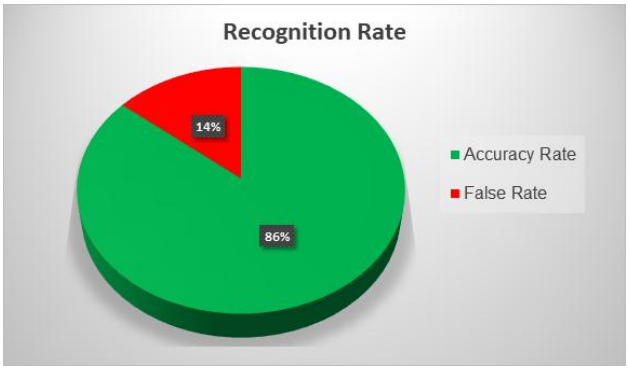


Figure 12 - Pie chart for the Recognition Rate

The bar graph (Fig. 13) is a graphical representation of the factors that affect the recognition accuracy that can be observed in Table 1.

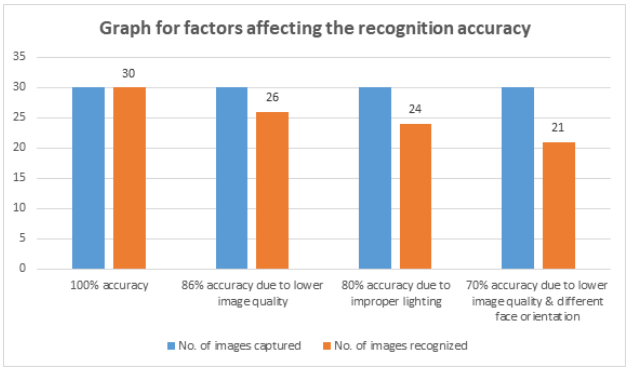


Figure 13 - Bar Graph for factors affecting the recognition accuracy

3. CONCLUSION

Face authentication technologies have traditionally been associated with extremely expensive, top-secure applications. The core technologies have advanced today and due to innovation and rising processing power, the cost of equipment is dropping dramatically. Many face authentication technology implementations are now cost-effective, dependable, and highly accurate.

This system can be used efficiently to provide safe and reliable protection. It can, therefore, be used in many organizations as a key to security solutions, as it can recognize and convey people's identities. Hence, this rectifies the drawbacks of the existing systems.

This paper has portrayed a survey related to face authentication. Here, we have surveyed the paper related to existing face authentication systems and their drawbacks. Therefore, there is a need for an efficient security system for facial authentication based on the cons of the existing systems.

REFERENCES

[1] A Real-Time Framework for Human Face Detection and Recognition in CCTV Images by Rehmat Ullah, Hassan Hayat, Afsah Abid Siddiqui, Uzma Abid Siddiqui, Jebran Khan, Farman Ullah, Shoaib Hassan, Laiq Hasan, Waleed Albattah, Muhammad Islam, and Ghulam Mohammad Karami in 2022.

[2] Face Detection and Recognition Algorithm in Digital Image Based on Computer Vision Sensor by Di Lu and Limin Yan in 2021.

[3] Face Recognition and Identification using Deep Learning Approach by KH Teoh, RC Ismail, SZM Naziri, R Hussin, MNM Isa, and MSSM Basir in 2021.

[4] Identity authentication on mobile devices using face verification and ID image recognition by Xing Wua, Jianxing Xua , Jianjia Wanga , Yufeng Lia , Weimin Lia and Yike Guo in 2019.

[5] A novel optical two-factor face authentication scheme by Gaurav Verma, Dajiang Lu in 2019.

[6] Face Authentication method by Julien Doublet and Jean Beaudet in 2018.

[7] Face authentication device having database with small storage capacity by Takayuki Kase in 2018.

[8] A face recognition Approach Using Deep Reinforcement Learning Approach for User Authentication by Ping Wang, Wen-Hui Lin, Kuo-Ming Chao and Chi-Chun Lo in 2017.

[9] An overview of various Authentication Methods and Protocols by Dwiti Pandya, Khushboo Ram Narayan and Sneha Thakkar in 2015

[10] An Automate System for Unconstrained Video-Based Face Recognition by Jingxiao Zheng, Rajeev Ranjan, Ching-hui Chen, Jun-cheng chen, CArols D. Castillo and Rama Chellappa in 2019

[11] A video database of moving face and people by A. J. O'Toole, J. Harns, S. L. Snow, D. R. Hust, M. R. Pappas, J. H. Ayyad and H. Abdi in 2005

[12] "IJB-S: IARPA Janus Surveillance Video Benchmark," by N. D. Kalka, B. Maze, J. A. Duncan, K. J. O'Connor, S. Elliott, K. Hebert, J. Bryan, and A. K. Jain in 2018.

[13] "An all-in-one convolutional neural network for face analysis," byR. Ranjan, S. Sankaranarayanan, C. D. Castillo, and R. Chellappa, in 12th IEEE FG, vol. 00, May 2017

[14] "Deep face recognition," by O. M. Parkhi, A. Vedaldi, and A. Zisserman in BMVC, 2015.

[15] "Unconstrained face verification using deep CNN features," by J. C. Chen, V. M. Patel, and R. Chellappa, in WACV, March 2016.

[16] "Video Based face association and identification," byC.-H. Chen, J.-C. Chen, C. D. Castillo, and R. Chellappa, 12th FG, 2017.

[17] "Neural aggregation network for video face recognition," J. Yang, P. Ren, D. Zhang, D. Chen, F. Wen, H. Li, and G. Hua, in CVPR, 2017.

[18] "Trunk-branch ensemble convolutional neural networks for video-based face recognition," by C. Ding and D. Tao in CoRR, 2016.

[19] "Face recognition in unconstrained videos with matched background similarity," by L. Wolf, T. Hassner, and I. Maoz in CVPR, 2011.

[20] Face Recognition Based attendance System by Nandhini R, Duraimurugan and S.P.Chokkalingam in 2019.

[21] Real-Time Face Recognition: An End-To-End Project by Marcelo Rovai in 2018.

[22] IoE-Enabled Smart Embedded System: An Innovative Way of Learning by Rathod A., Ayare P., Bobhate R., Sachdeo R., Sarode S., Malhotra J. in Information and Communication Technology for Sustainable Development. Advances in Intelligent Systems and Computing, vol 933, pp. 659-668, Springer, Singapore in 2020.

[23] Redefining smartness in township with Internet of Things & Artificial Intelligence: Dholera city by Raghav B., Manish P., Vasu G., Vishal K., Jyoti M. and Sambhaji S., in 6th International Conference on Energy and City of the Future (EVF'2019), E3S Web of Conferences 170, 06001 IN 2020.

[24] Reliable and Prioritized Data Transmission Protocol for Wireless Sensor Networks by S. Sarode, J. Bakal and L. Malik in Proceedings of the International Congress on Information and Communication Technology, Volume 439 of the series Advances in Intelligent Systems and Computing pp 535-544, June 2016.

[25] Survey paper on cloud computing security by Nimit Kaura and Abhishek Lal in 2017

[26] A Survey Paper on Security in Cloud Computing: A Bibliographic Analysis by Krutika K Shah, Rutvij H Jhaveri and Vahida U Vadiya in 2016.

[27] A Survey Paper on Data security in Cloud Computing by Vijay Ghorpade, Vishvajit Dalimbkar and Rajani Sajjan in 2016.

[28] A Comprehensive Survey on Security in Cloud Computing by Gururaj Ramachandra Mohsin Iftikhar and Farrukh Aslam Khan in 2017.

[29] Face Recognition: Understanding LBPH Algorithm by Kelvin Salton do Prado in 2017.

[30] https://opencv.org/about/

[31] OpenCV Face Recognition by Adrian Rosebrock in 2018.

[32] Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks by Mohamed Abomhara and Geir M. Køien in 2015.