International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 3, March-April 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Deep Unified Model for Intrusion Detection Based on Convolutional Neural Network

**Dhanu Shree D[1], Fouzia Fathima A[1], Madhumita B[1], Akila G[2], Thulasiram S[3]**

[1]UG Student, [2]Assistant Professor,
[1,2]Department of Electronics and Communication Engineering,
Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India
[3]Hardware Engineer of Missile Ingeniator, Tamil Nadu, India

**ABSTRACT**

Indian army has always been subject to military attacks from neighbouring countries. Despite many surveillance devices and border security forces, the enemy finds a way to infiltrate deep into our borders. This is mainly because even now the surveillance in India is largely human-assisted. Therefore this automated surveillance can authenticate the authorized persons and alert everyone when an enemy intrusion is detected. In this, we proposed an automated surveillance system that tackles the predicament of recognition of faces subject to different real-time scenarios. This model incorporates a camera that captures the input image, an algorithm to detect a face from the input image, recognize the face using a convolution neural network along with transfer learning method, and verifies the detected person. The authorized person's name and details are stored in CSV format and then into the database. In case of any unauthorized person's face is detected the image of the intruder along with time is stored in the database and warning signal is also given to alert the surrounding members in case of intrusion detection.

***KEYWORD:*** *Military attacks, Face recognition system, Deep Learning, Python, Convolution Neural Network, Real time, Surveillance, Intrusion detection, Database*

***How to cite this paper:*** Dhanu Shree D | Fouzia Fathima A | Madhumita B | Akila G | Thulasiram S "Deep Unified Model for Intrusion Detection Based on Convolutional Neural Network" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-3, April 2021, pp.816-821, URL: www.ijtsrd.com/papers/ijtsrd39976.pdf

IJTSRD39976



## I. INTRODUCTION

Indian Border has been facing many attacks from the foes, which cause lot of financial as well as mental & physical crisis. In the recent years, also numerous attacks have been took place in military field. So despite many surveillance devices and border security forces, the foes find a way to infiltrate deep into our borders. This attacks are mainly due to the surveillance in India is human-assisted. With consideration of such critical conditions we developed an automated surveillance system for military purposes. This automated surveillance system is implemented using Convolution Neural Network along with transfer learning .We can use this kind of technologies in the border area to keep tracking if any enemy intrusion enters the border. Thus, military attacks can be avoided. This model incorporates a camera that captures the input image, an algorithm to detect a face from the input image, recognize the face using a convolution neural network, and verifies the detected person. The face detection in this system is done through the Haar cascade classifier. Haar cascades make use of the image subtraction morphological process to detect the face. In this, the cascades of different images of the same person are taken and recorded in the database. The recorded images are using to train the CNN model. Here we have employed our CNN through transfer learning. The transfer learning models consist of several pre-trained models. One such pre-trained model of VGG 16 is employed here. The model learns the facial features of the person images stored in the database. This trained and learned model is used in the surveillance system. Any other person's face other than the faces in the database are detected and an intrusion alert signal is given. In case of authorized person's face is detected the name and details are stored in CSV format and then stored into the database. In case of any unauthorized person's face is detected the image of the intruder along with time is stored in the database. A warning signal is also given to alert the surrounding members in case of intrusion detection.

## II. RELATED WORK

The concept of Face Recognition using Deep learning and edge computing technologies, which are used for efficient processing of huge amount of data with distinct accuracy was proposed by Muhammad Zeeshan, SaadHarous, RaziIqbal [1]. They proposed an algorithm for face detection and recognition based on convolution neural networks (CNN), which outperform the traditional techniques. The concept of Face Recognition Based on Convolutional Neural Network was proposed by YakupDemir, OzalYıldırım [2]. This method is implemented using modified Convolutional Neural Network (CNN) architecture by adding two

normalization operations to two of the layers. The normalization operation which is batch normalization provided accelerating the network. The concept of Face Detection and Tracking using OpenCV proposed by by KrutiGoyal, KartikeyAgarwal, Rishi Kumar [3].In this method they have developed a application for tracking and detecting faces in videos and in cameras which can be used for multipurpose activities. The concept of Eigen-faces for recognition was proposed by Mathew Turk and Alex Pent land [4]. In this method they developed a near-real time computer system that can locate and track a subject's head, and then recognize the person by comparing characteristics of the face to those of known individuals. The concept of Face recognition using Eigen-face sand artificial neural networks was proposed by MayankAgarwal, Nikunj Jain, Mr. Manish Kumar and HimanshuAgrawal [5]. This paper presents a methodology for face recognition based on information theory approach of coding and decoding the face image.

The work in this paper has two methods.1)Face recognition using encoding technique 2)Face recognition using CNN and transfer learning method. Face recognition without using CNN is done by using encoding method. Here we will find all of the faces in the given image and label them and then we will compare the input image with the encoded file. The face distance is calculated to find the image that matches with the input image. The best match is found using the image with the smallest face distance. The label of the original image is displayed to detect the face of the given input image. Face recognition using CNN and transfer learning method is done by using the concept of transfer learning and using the pre-trained weights of VGG16 architecture, we can save both our time and resources.

## III. METHODOLOGY

Face recognition is the problem of identifying or verifying faces in a photograph.

### 3.1. Face recognition using encoding technique:

Face recognition is often described as a process that first involves four steps; they are: face detection, face alignment, feature extraction, and finally face recognition.

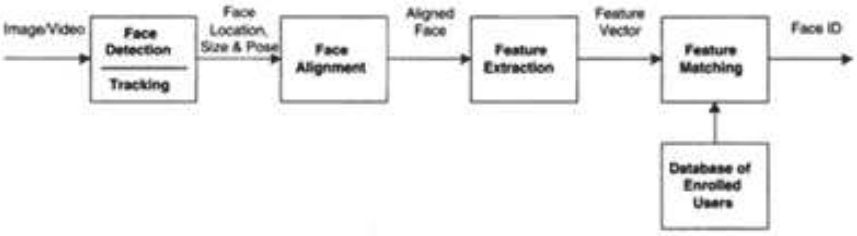


**Figure 1: Face recognition processing flow**

The description of each block is explained below:

1. Face Detection. Locate one or more faces in the image and mark with a bounding box.
2. Face Alignment. Normalize the face to be consistent with the database, such as geometry and photometrics.
3. Feature Extraction. Extract features from the face using Haar feature extraction method, that can be used for the recognition task.
4. Face Recognition. Perform matching of the face against one or more known faces in a prepared database using encoding method.

### 3.2. Face recognition using CNN:

Convolutional Neural Networks expect and preserve the spatial relationship between pixels by learning internal feature representations using small squares of input data. Feature are learned and used across the whole image, allowing for the objects in the images to be shifted or translated in the scene and still detectable by the network. VGG 16:

VGG 16 was proposed by Karen Simonyan and Andrew Zisserman of the Visual Geometry Group Lab of Oxford University in 2014 in the paper "Very deep convolutional networks for large-scale image recognition". This model achieves 92.7% top-5 test accuracy on ImageNet dataset which contains 14 million images belonging to 1000 classes. The ImageNet dataset contains images of fixed size of 224*224 and have RGB channels. So, we have a tensor of (224, 224, 3) as our input. This model process the input image and outputs the a vector of 1000 values.

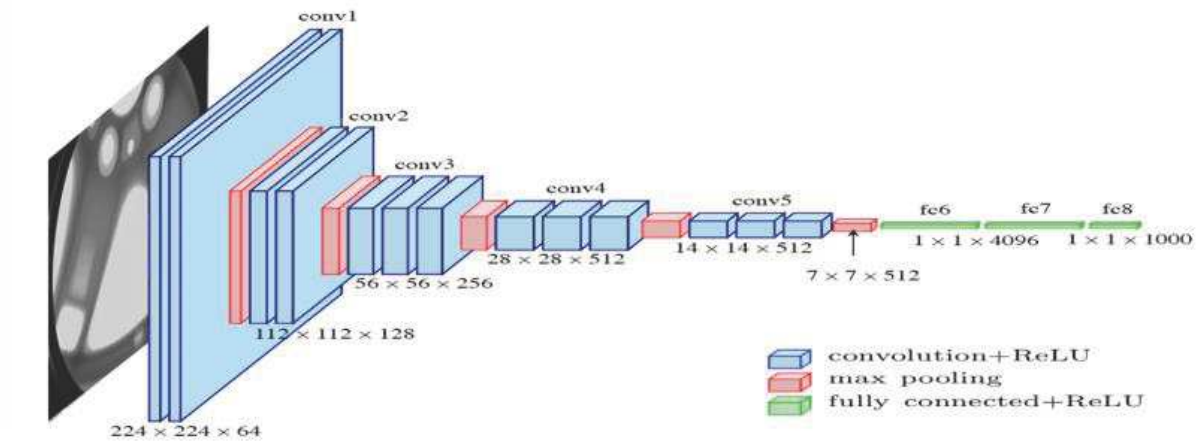


**Figure 2: Architecture of VGG-16**

**Block Diagram:**

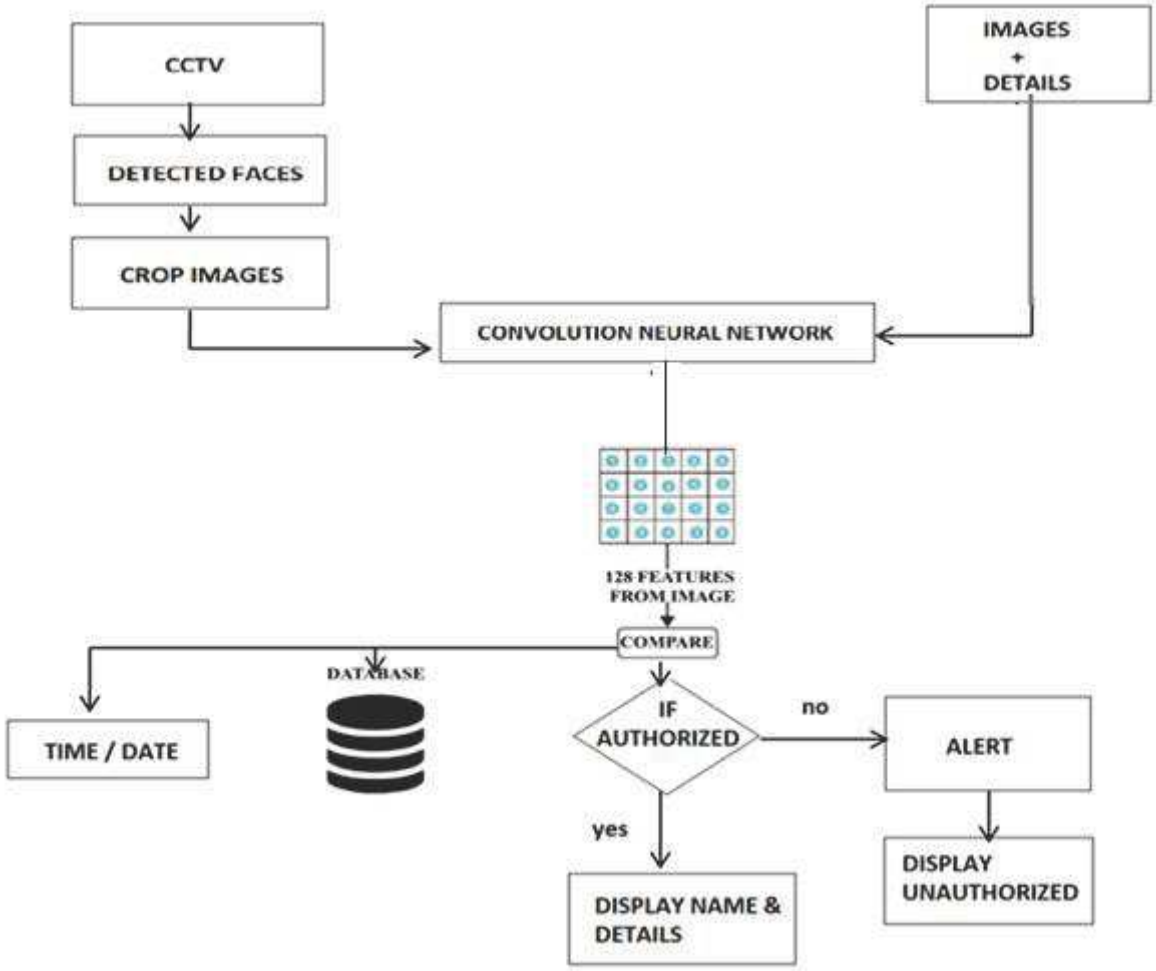


**Figure 3: Block diagram of face recognition using CNN & transfer learning method**

The description of each block is explained below:

1. Capturing using camera: Camera installed in army camp is used to capture the face of the persons who are present in the camp.
2. Image processing: Facial detection and recognition algorithm is applied on the captured video frames. The detected face is cropped and stored for processing. The module recognizes the images of the face which have been registered manually with their names in the database. We use Open CV for all the image processing and acquisition operations.
3. Convolutional layers: Convolutional layers are comprised of filters and feature maps.

3.1. Filters: The filters are the "neurons" of the layer. The have input weights and output a value. The input size is a fixed square called a patch or a receptive field.

3.2. Feature maps: The feature map is the output of one filter applied to the previous layer. A given filter is drawn across the entire previous layer, moved one pixel at a time. Each position results in an activation of the neuron and the output is collected in the feature map.

3.3. Padding: The distance that filter is moved across the the input from the previous layer each activation is referred to as the stride. If the size of the previous layer is not cleanly divisible by the size of the filters receptive field and the size of the stride then it is possible for the receptive field to attempt to read off the edge of the input feature map.

3.4. Relu: ReLU stands for rectified linear activation unit and is considered one of the few milestones in the deep learning revolution. It is simple yet really better than its predecessor activation functions such as sigmoid or tanh.

3.5. Pooling layer: The Pooling layer is responsible for reducing the spatial size of the Convolved Feature. This is to decrease the computational power required to process the data through dimensionality reduction. Furthermore, it is useful for extracting dominant features which are rotational and positional invariant, thus maintaining the process of effectively training of the model.

3.6. Fully connected layers: Fully connected layers are the normal flat feed-forward neural network layer. These layers may have a non-linear activation function or a softmax activation in order to output probabilities of class predictions.

4. Database: The database stored the time and details of the detected person. We have implemented using MySQL database. It is an open source relational database. The prediction from the CNN is in the form of CSV which is the converted into a table format of rows and columns. If there is an unauthorized person the persons face is cropped and stored with time and a warning signal is given.

## IV. EXPERIMENTAL RESULTS

The final result of face recognition is shown in figure 4,5,6,7,8,9. figure 4 shows the keys and the values of the encoded image, figure 5 shows the accuracy plot we got accuracy percentage of 98.76, figure 6 shows the loss plot we got a loss percentage of 9.79,figure 7 and 8 represents the face recognition of person, that is If the person is authorized then it will display the face of an authorized person under the green colour rectangle, else it will display unknown person in red rectangle, figure 9 shows how details are stored in the database.

### 4.1. Face recognition using encoding technique:

Face is recognized using encoding technique. In this technique the image is broken down into pixels of arrays.First the path directory of the image is given. Then the function looks through all the faces in the folder and returns the encoded faces. Only images stored in file format of .jpg and .png is acceptable. Thus the figure 4 shows the keys and the values of the encoded image.

```
faces = get_encoded_faces()
faces_encoded = list(faces.values())
known_face_names = list(faces.keys())
```

```
  3.15563649e-01 -2.07867086e-01  2.31499985e-01  2.00786456e-01
 -4.37566265e-02  1.14323556e-01  7.05450028e-02  1.38322473e-01
 -1.08849958e-01 -5.01409099e-02 -1.90896854e-01 -1.27284288e-01
 -5.06866276e-02 -1.04236186e-01 -3.17125581e-04  1.03849143e-01]
{'bill gates': array([-9.66997370e-02,  7.64617771e-02,  7.49358386e-02,  6.52936026e-02,
       -1.30877569e-01, -1.64903030e-02, -4.42924462e-02, -1.38482258e-01,
        8.18997324e-02, -7.89919123e-02,  1.54310763e-01, -4.71304264e-03,
       -3.01714987e-01, -4.53581586e-02, -2.30973177e-02,  8.61688778e-02,
       -1.34310290e-01, -3.01792808e-02, -1.34122640e-01, -1.39717087e-01,
       -7.92492852e-02,  2.71101780e-02,  8.87625143e-02, -5.51768355e-02,
       -1.08454302e-01, -2.28425652e-01, -1.18895046e-01, -1.33575395e-01,
        1.00208841e-01, -8.01836848e-02,  6.42742440e-02,  6.65364489e-02,
       -1.54251754e-01, -7.37076029e-02, -3.82892229e-02,  1.39695406e-01,
       -5.73962107e-02, -7.05046766e-03,  2.11846560e-01, -5.95448688e-02,
       -1.53120235e-01,  2.86596082e-02,  3.69631797e-02,  2.69950539e-01,
        2.45754197e-01,  1.92170348e-02, -2.80094258e-02, -5.01595996e-02,
        1.52577981e-01, -2.76513875e-01,  7.17312098e-02,  1.27777874e-01,
        1.37651026e-01,  6.52648956e-02,  1.06730439e-01, -1.58272728e-01,
        6.51731193e-02,  1.79224446e-01, -1.38644412e-01,  1.00935310e-01,
        1.20939352e-01, -1.48580253e-01,  3.77498940e-02, -1.93176232e-02,
        1.23646341e-01,  3.80572714e-02, -4.09558378e-02, -6.45784438e-02,
        2.26812169e-01, -1.98242307e-01,  5.13286795e-04,  1.26905218e-01,
       -8.21852982e-02, -1.33324265e-01, -3.50793600e-01,  2.23459247e-02,
        3.99945259e-01,  1.84157744e-01, -9.02191848e-02, -4.47266586e-02,
       -6.70497790e-02, -4.97399867e-02,  1.29505256e-02,  3.46676633e-02,
       -8.33717957e-02, -1.50001198e-01, -1.32447124e-01,  2.65080817e-02,
        1.92666978e-01, -4.90123034e-02,  4.08788770e-02,  2.10005313e-01,
```

**Figure 4: Encoded values**

### 4.2. Face recognition using CNN:

The output from the face recognized using CNN is shown in figure 5,6,7,8,9.

#### 4.2.1. Accuracy plot:

On implementing this model we got a accuracy of 98.76%

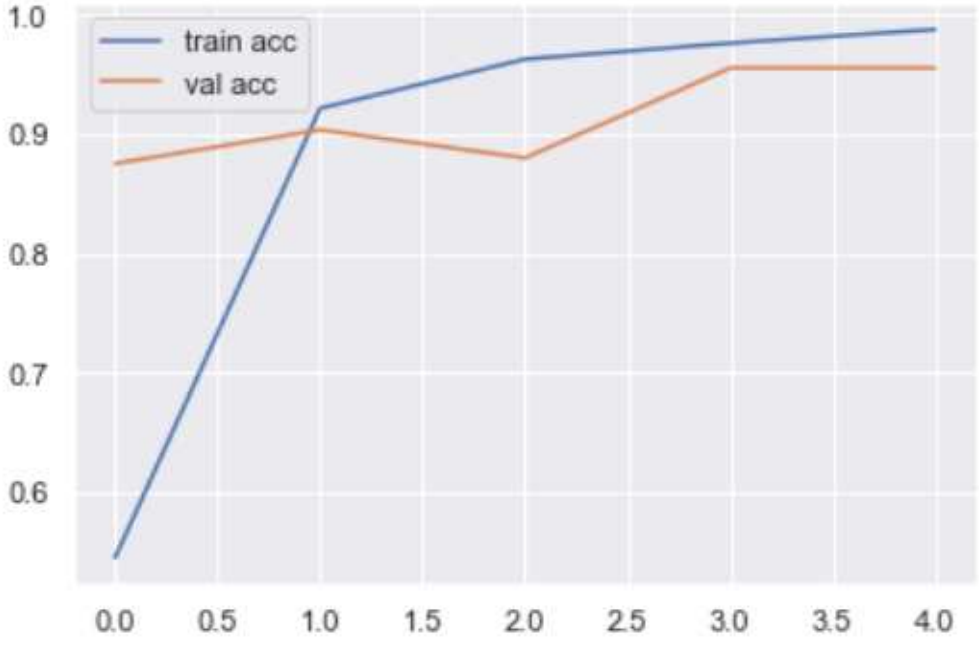


**Figure 5: Accuracy plot**

#### 4.2.2. Loss plot:

On implementing this model we got a loss of 9.79%

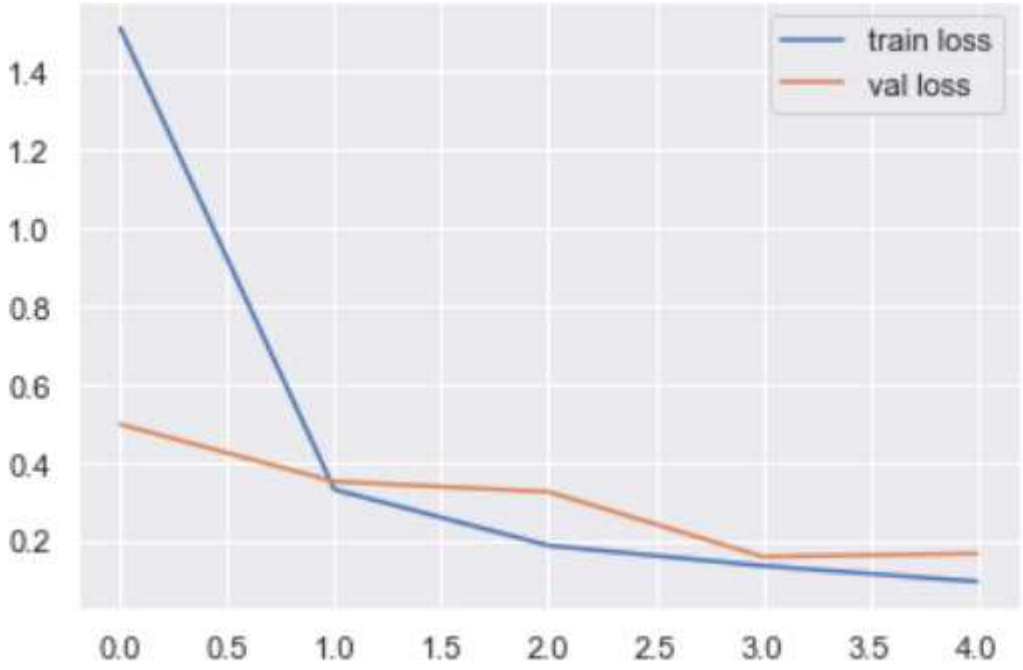


**Figure 6: Loss plot**

#### 4.2.3. Model detection and prediction of a person:

If the person is authorized then it will display the face of an authorized person under the green colour rectangle, else it will display unknown person in red rectangle.

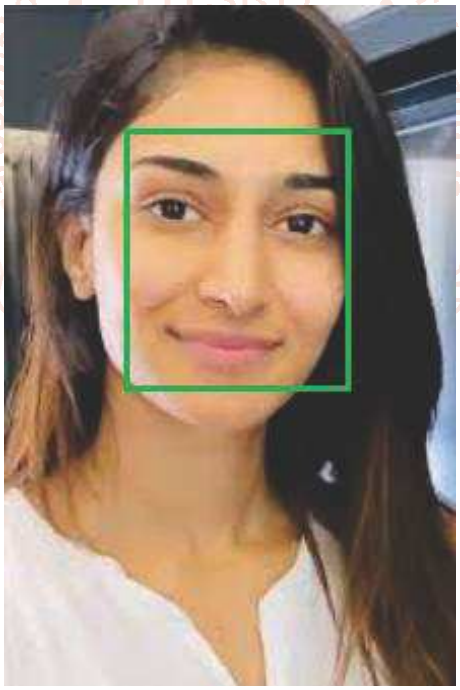

**Figure 7 Model prediction of an authorized person**

**Figure 8 Model prediction of an unauthorized person**

#### 4.2.4. Database:

Figure 9 shows how details are stored in the database.

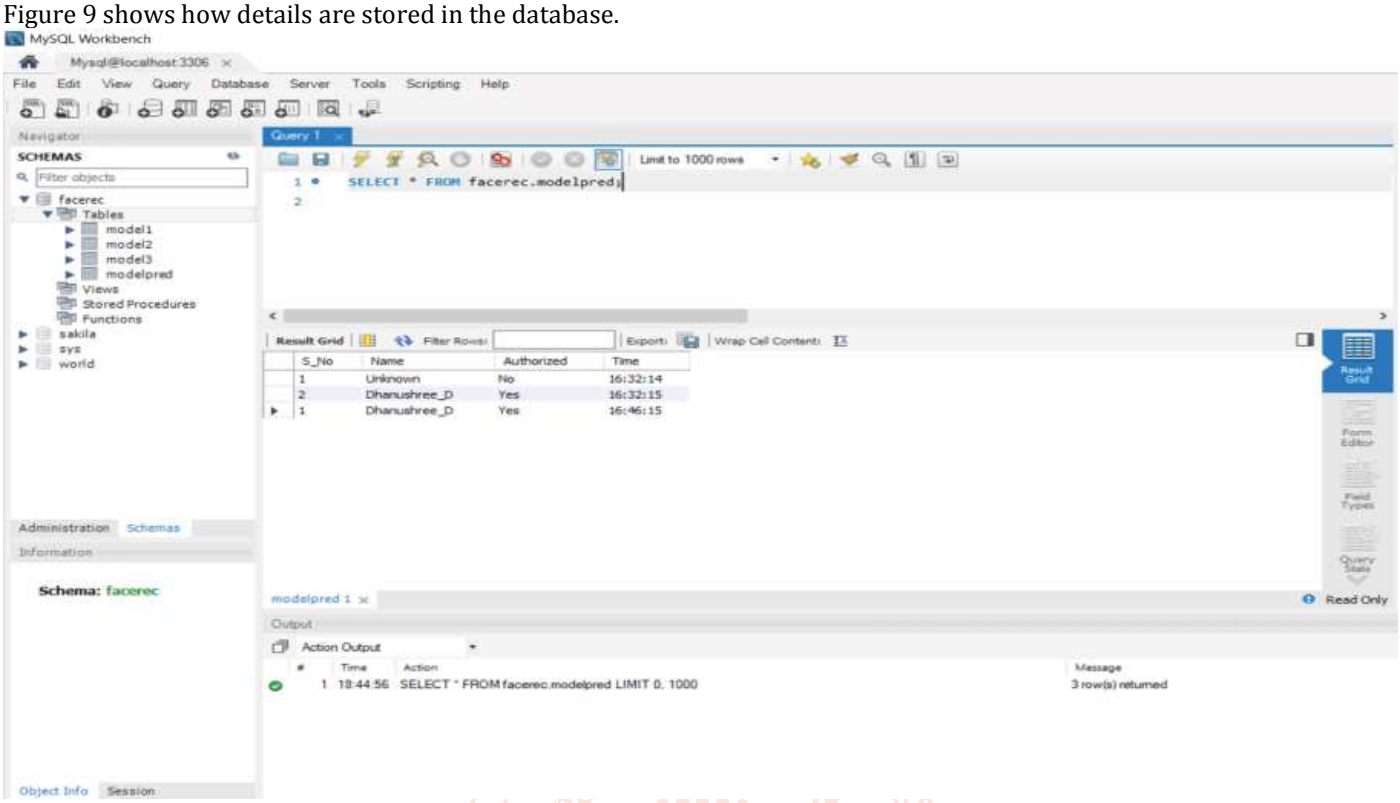


**Figure 9 MYSQL database**

## V. CONCLUSION

Thus an efficient automated surveillance system is designed and implemented successfully using deep learning with Convolution Neural Network. With the help of this surveillance system an enemy intrusion can be detected easily and thus numerous attacks can be avoided.

## REFERENCES


[1] N. Hazim Barnouti, S. Sameer Mahmood Al-Dabbagh, and W. Esam Matti, "Face Recognition: A Literature Review," Int. J. Appl. Inf. Syst.,vol. 11, no. 4, pp. 21–31ov 2016.

[2] P. Savitra, J. Padwal, J. Chaitali, M. Surabhi Nilangekar, and U. K.Bodke J, "Automated Attendance System in College Using Face Recognition and NFC," Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 6,pp. 14–21, 2017.

[3] S. Aly and M. Hassaballah, "Face recognition: challenges, achievements and future directions," IET Comput. Vis., vol. 9, no. 4, pp. 614–626, 2015.

[4] P. Liu et al., "The false-positive and false-negative predictive value of HIV antibody test in the Chinese population," J. Med. Screen., vol. 15, no. 2, pp. 72–75, 2008.

[5] Trigueros D S, Meng L and Hartnett M 2018 Face Recognition: From Traditional to Deep Learning Methods

[6] R. T. Schirrmeister et al., "Deep learning with convolutional neural networks for EEG decoding and visualization," Hum. Brain Mapp., vol.38, no. 11, pp. 5391–5420, 2017.

[7] S. Kumar, S. Singh, and J. Kumar, "A study on face recognition techniques with age and gender classification," Proceeding - IEEE Int.Conf. Comput. Commun. Autom. ICCCA 2017, vol. 2017-January, no.May, pp. 1001–1006, 2017.

[8] R. Sharma and M. S. Patterh, "Face Recognition using Face Alignment and PCA Techniques: A Literature Survey," IOSR J. Comput. Eng. Ver.III, vol. 17, no. 4, pp. 2278–661, 2015.

[9] H. Yu and H. Liu, "Combining appearance and geometric features for facial expression recognition," Sixth Int. Conf. Graph. Image Process. (ICGIP 2014), vol. 9443, p. 944308, 2015.

[10] S. Tseng, "Comparison of Holistic and Feature Based Approached to Face Recognition," no. July, 2003.

[11] Lata P Y V, Kiran C, Tungathurthi B, Rao H R M, Govardhan A and Reddy L P 2009 03_Facial Recognition using Eigen faces by PCA Int. J. Recent Trends Eng.1 587–90

[12] J. S. Bedre and S. Sapkal, "Comparative Study of Face Recognition Techniques:A Review," IJCA Proc. Emerg. Trends Comput. Sci. Inf.Technol. (ETCSIT2012) etcsit1001, vol. ETCSIT, no. 1, pp. 12–15, 2012.

[13] Lee H, Lee W and Chung J 2018 Face Recognition Using Fisher face Algorithm 998–1001

[14] Belhumeur P, Hespanha J and Kriegman D 1997 Face recognition: Eigen faces vs. Fish-erfaces: Recognition using class specific projection IEEE Trans. Pattern Anal. Mach. Intell.19 711–20