IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10632

Intruder Detection System

[1]Sathisha G, [2]Anjali Sharma, [3]Avinash Kumar, [4]Manish Kumar Mishra, [5]Sahil Bhuwalka

[1]Professor, Department of Computer Science and Engineering, Atria Institute of Technology, Bangalore, India - 560024

[2,3,4,5] Department of Computer Science and Engineering, Atria Institute of Technology, Bangalore, India - 560024

Abstract: The system proposed is a solution for securing any physical system at a particular place. Deep Learning has been used to develop the system. We have used Viola Jones's one of the facial features-based face(s) detection algorithm, along with Local Binary Pattern Histogram (lbph) algorithm for face recognition to recognize whether it's an intrusion or not. Open CV has been used for computer vision for image processing. The result of the proposed system shows that the system is able to detect all the faces trying to come inside the secured area and recognize the intruders, along with sending a notification to the owner or the required authority and activate the alarm on intrusion. This IDS can also be used for observational purposes.

Keywords: Viola Jones, Open CV, IDS, Linear Binary Pattern Histogram, Haar Cascade

1. INTRODUCTION

We are now living in a world with increased thefts and criminal activities, where criminals wants to steal personal belongings or access public systems. For such purposes there is a definite need for protection against such activities and thus calls for a need for a personal security system. Any security system consists of camera(s) which acts as a hidden eye in public places like banks, homes, etc. These continuously records all the activities going in the particular place and is either monitored manually or by an automated system [2]. An Intrusion Detection System (IDS) is a system that surveils a system or an area of interest for any suspicious activities and raises an alarm whenever such activities are found by the system. It constantly scrutinizes a system for any kind of intrusion. Any malicious action or breach is normally reported to an administrator or the one operating the system and a designed security and event management system takes care of the action needed. Although intrusion detection systems monitor a system or an area of interest for any potentially infringing actions, they might also raise faulty alarms. Therefore, the person or any organization using it, first needs to fine-tune their IDS products when they first plant the system. That is it is necessary to properly setup the intrusion detection systems to recognize who is authorized and who is an intruder, and if it is an intruder what action must be taken is set. Basically, IDS is able to detect an intruder, inform the authority about the intrusion and take an appropriate action.

Today's era is reigned by peculiar minds seeking innovation in everything. One of the technological advances that focuses on processing digital information is digital image processing (DIP). The majority of cutting-edge technologies pertaining to images and their uses are currently generated with the use of DIP because to more affordable computers and specialized hardware [1]. An Intelligent IDS creates virtual boundary zones for recognizing intruder activity using dual cameras, image processing, computer vision, and deep learning technologies [4]. Now to detect anyone first, picture frames from the collected video are extracted. Second, the face area portion of the image frames is separated. Thirdly, a grayscale image is created by converting an RGB color image to a grayscale image. Fourth, the face in the image is discovered using the histogram [3]. The IDS's main feature includes the recognition of authorized person. While recognizing any individual, the most important attribute is face [5] for that it follows a series in which the initial step is to identify the face, after which the various characteristics that make it distinctive are extracted which are later used for recognition [1]. Now that the individual has been authenticated, if the person is not permitted to access the secured system, action is performed, such as raising an alarm when an intruder is discovered and automatically directing and zooming in on the intruder using a different TV camera [8].

In the system we've developed, we employ face detection based on the histogram to identify faces and a face recognition module to determine whether or not a user is authorized to access the system. By using Open CV we process the image to enhance the image and extract important features from it. Whenever a person tries to access the system his/her face will be detected and recognized if they are authorized or not. If it is an intrusion an alarm will be raised and a notification will be sent to the administrator on the mobile application and appropriate action will be taken for the intrusion.

DOI: 10.17148/IJIREEICE.2022.10632

2. METHODOLOGY

The method was developed once it became clear that individual asset protection was necessary. Various algorithms were looked into while developing the system.

The proposed system captures the image of the person trying to access the secured area, using Viola-Jones's Haar Cascade Classifier to detect the face(s) in the captured image. The detected face is then recognized using Local Binary Pattern Histogram (LBPH) algorithm and if the face is not recognized by the system it raises an alarm and also sends a notification to the owner or the person handling it.

2.1 Research Method

The researchers have used the waterfall methodology where the development process can be considered as a sequential flow in the waterfall. It divides the life cycle into a set of phases and the phases do not overlap with each other. The requirements needs to be clear and precise before going to the development stage. It is useful when the resources are available and trained and requirements doesn't change frequently. Any changes required are made during the development phase of the project.

2.2 Hardware devices

A raspberry Pi 3B+ which acts as the computer where the code will be executed. It comes with different ports so we can attach it to any monitor screen, speakers for alarm purpose and Ethernet port as well for internet connection. Then we also use IP camera with a quality of minimum of 8 megapixel (MP) to capture the images. IR sensors are used to detect the face in the dark and have greater accuracy.

2.3 Software devices

For coding Python3 has been used on PyCharm IDE as it is more resource intensive. OpenCV has been used as it is a video and image processing library for image and video analysis.

2.4 Algorithms

For face detection facial features has been used rather than using image's pixel as it is operated faster than operating with the pixels. Viola Jones's Haar Cascade algorithm has been used to detect the faces as it is extremely fast to compute in cases of millions of faces in the captured image. We first extract the Haar like features that are face discriminative using Haar filters that are based on squared functions.

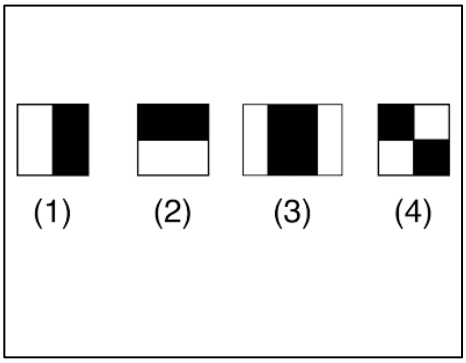


Fig 1.a Haar Filters

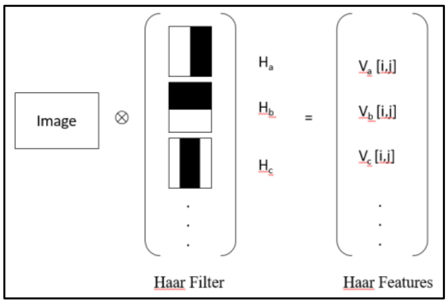


Fig 1.b Correlation of Haar Filters on image

Each of the Haar filters are applied as correlation on the image as shown in Fig 1.b and that gives a number at each pixel, so at any pixel we end up with all these Haar filters and we get the feature vector. Finding the total of the pixels under white and black rectangles is necessary for each feature computation. Harr like features can simply be given as:

V_a [i,j] = ∑(pixel intensities in white area) - ∑(pixel intensities in black area)

In fig 1.a the white part of the boxes represents the light part of the face while the black is the darker part. Haar features are sensitive to directionality of patterns. Before classification the image must be normalized for different positions along with different lightning.

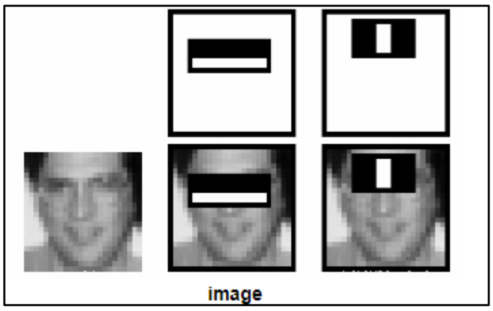
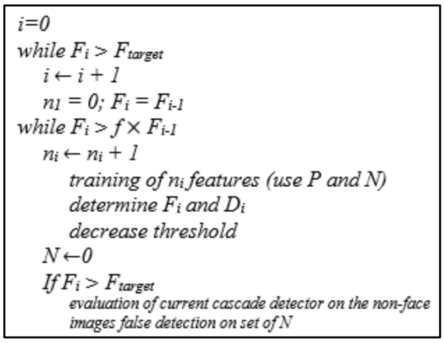


Fig 2: Haar filter on the image

Then the integral images are created to make the boxes faster as shown in Fig 2, first box covers the eye part and the second one covers the nose bridge. The optimal threshold for each feature is determined, and the faces are then classified as positive or negative based on that threshold. After computation, a training set of negative and positive images is produced [1]. To eliminate the wrongly classified images AdaBoost classifier is used, which combines all the weak classifier into a strong one for better face detection. On all of the training images, we apply each and every characteristic for this. The system's accuracy is improved by using features with low error rates. The parts of the image having no face are then discarded for optimization. Then, using the command opencv_traincascade we create a file cascade, the system trains the cascade classifiers, where features are organized into several stages of classifiers and applied one at a time. In order to calculate the false positive rate cascade Fi and the detection rate Di for face detection, AdaBoost technique evaluated the performance of the present cascade classifiers while training on sets of negative and positive examples. [10].



```
$i=0$
while $F_i > F_{target}$
    $i \leftarrow i + 1$
    $n_1 = 0; F_i = F_{i-1}$
while $F_i > f \times F_{i-1}$
    $n_i \leftarrow n_i + 1$
        training of $n_i$ features (use $P$ and $N$)
        determine $F_i$ and $D_i$
        decrease threshold
    $N \leftarrow 0$
    If $F_i > F_{target}$
        evaluation of current cascade detector on the non-face
        images false detection on set of $N$
```

Fig 3: Training algorithm for building cascade detector [10]

DOI: 10.17148/IJIREEICE.2022.10632

After the faces are detected it will recognize whether the detected face is the authorized or not. For this we have used Local Binary Pattern Histogram (LBPH). It is based on the neighbourhood binary operator. Due to its strong discrimination and straightforward computation, it is a very popular and commonly used method. [11]. Here an image taken of size NxM is divided into mxm regions where the local binary operator is applied, comparing a pixel to its eight adjacent closest pixels. Then, if the value of the neighbouring pixels is higher than the centre one, it returns a value of "1," otherwise "0." The LBP value, which can be expressed as a decimal number, is created by adding up all eight of these neighbouring digits to create an 8-bit binary number. The number of times all of the LBP values appear in the current region is then calculated to construct the histogram for this region. Similarly, for all regions of the image histograms are created and at last feature vectors are defined. For recognition, the system uses these feature vectors and finds the distance between different feature vectors and best match for the image is returned. The system compares the detected faces from the captured image with the already stored authorized faces in the system giving whether it’s the authorized person or not.

3 RESULTS AND DISCUSSION

The major goal of the research was to develop an intruder detection system that can be quickly and simply utilized to identify intruders and alert the owner. Intruders are accurately identified by the system using image processing algorithms. In order to train the system and determine who is authorized to access it, the system was tested in a real-world setting and a number of photographs were taken. Three distinct people's pictures were submitted as test subjects, and OpenCV prepared a CSV file of the images it had taken so it could be compared to the originals. Once the system had been trained, it was simple to identify faces, identify people who were authorized, and raise an alarm if someone was not authorized while also sending a notification to the appropriate authority. When kept five to six metres away from the secured area's entrance, the system was also able to identify and detect people. It was seen that system was also able to recognize in inefficient lightning as well. The figure below shows the interface of the application fig 4 and its working as well fig 5.

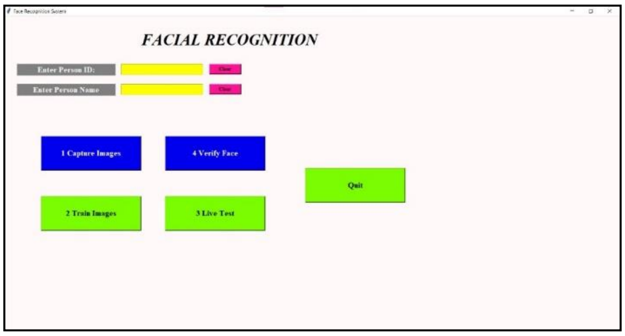


Fig 4: Application Interface

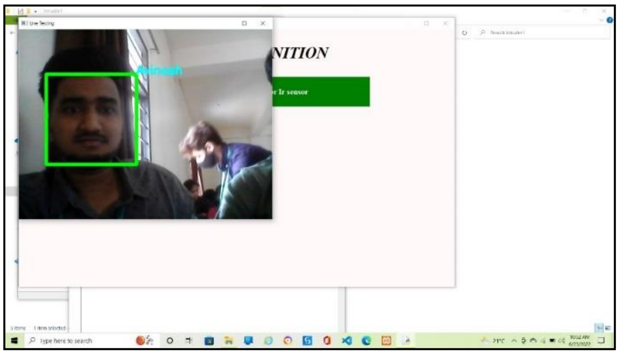


Fig 5: Recognizing authorised face

4 CONCLUSION

The designed intruder detection system can be employed in a variety of locations, including houses, public spaces like banks, business spaces, etc. Even if the responsible authority is not online, notification can still be sent to them. Thus, it can be said that the several methods employed here are apparent in identifying the intruders.

Also, various recognition algorithms can also be added in case of more accuracy and to serve the purpose efficiently for different criteria.

ACKNOWLEDGEMENT

The Atria Institute of Technology's Computer Science and Engineering department gave insight and knowledge that substantially aided the research, and we are grateful for their leadership throughout this process. The researchers would like to thank them for their assistance.

REFERENCES

[1] Nelson C. Rodelas, Melvin A. Ballera, “Intruder detection and recognition using different image processing techniques for a proactive surveillance”, Manilla Philippines.

[2] Young-Keun Choi, Ki-Man Kim, Ji-Won Jung, Seung –Yong Chun and Kyu-Sik Park, “Accoustic Intruder Detection System for Home Security”

[3] Mahasak Ketcham, Thittaporn Ganokratanaa, Sriphagaarucht Srinhichaarnun, “The Intruder Detection System for Rapid Transit using CCTV Surveillence Based on Histogram Shapes”, King Mongkut’s University of Technology North Bangkok, Bangkok, Thailand

[4] Kihyun Kim , Semyung Wang , Homin Ryu and Sung Q. Lee b” Acoustic-Based Position Estimation of an Object and a Person Using Active Localization and Sound Field Analysis”, School of Mechanical Engg, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, Korea

[5] Gurlove Singh, Amit Kumar Goel, “Face Detection and Recognition System using Digital Image Processing”, School of Computing Science and Engineering Galgotias University Greater Noida, India

[6] Maliha Khan, Sudeshna Chakraborty, Rani Astya, Shaveta Khepra, “Face Detection and Recognition Using OpenCV”, Deptt. of Comp. Sc. and Engg,School of Engg. AndTech Sharda University, Gr.Noida, Uttar Pradesh, India – 201306

[7] Kruti Goyal, Kartikey Agarwal, Rishi Kumar, “Face Detection and Tracking: Using OpenCV”, ASET, CSE Amity University Noida, India

[8] Takeyuki Takano, Katsumi Ushita, Norifumi Aoyama, Shozo Ikeda, Ikuro Nishimura, “Intruder Detection System by Image Processing”, Police Comms Research Cent., National Police Agency of Japan.

[9] P. Viola and M. J. Jones, “Robust real-time face detection,” International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154, 2004, doi: 10.1023/b:visi.0000013087.49260.fb.

[10] Nikolaos Stekas, Dirk van den Heuvel, “Face recognition using Local Binary Patterns Histograms (LBPH) on an FPGA-based System on Chip (SoC)”, 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), DOI: 10.1109/IPDPSW.2016.67

[11] YuanYuan Li and Lynne E. Parker, “Intruder detection using a wireless sensor network with an intelligent mobile robot response”, Distributed Intelligence Laboratory, Department of Electrical Engineering and Computer Science The University of Tennessee, Knoxville, Tennessee 37996-3450

[12] Shang-Hung Lin, “An Introduction to Face Recognition Technology”, Ph.D. IC Media Corporation

[13] Ashara Banu Mohamed, Norbik Bashah Idris, and Bharanidharan Shanmugum, “A Brief Introduction to Intrusion Detection System”, Universiti Teknologi Malaysia, UTM, Kuala Lumpur

[14] Mr. Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, “Intrusion Detection System”, Department of CSE, Bharati Vidyapeeth's College of Engineering, New Delhi, India

[15] Jianzhong Fang and Guoping Qiu, “A colour histogram based approach to human face detection”, School of Computer Science, The University of Nottingham