Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 6007-6011
Research Article

Image Classification For Visitors Home Security

[1]K.B Sri Sathya, [2]Archana V,

[1]Assistant Professor, Dept. of CSE,srisathyabtech@gmail.com
[2]Deevika K, Hariharan A, Final year CSE,
archanaarchanav6713@gmail.com
deevikadv@gmail.com
hariharan8957@gmail.com
KPR Institute of Engineering and Technology.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract-The actual need of the today's organizations and residential areas is security frameworks. The security methods which were implemented on those areas are now frequently facing major issues like break-in burglar easily. And also, the major obstacle with home security is people who are being incautious about the visitors or intruders before opening the door while security alarm goes off unfortunately. As a result, to attain the desired security, there will be an additional need of particularly skilled personnel to increase the level of safety frameworks. As a human being, those personnel will likely make faults which leads to uncertainty of persons entering into the residential zones. The main motive of the project is to provide the better home security against potential harm made by intruders and unknown visitors by recognizing them with predictable accuracy.

This security system consists of hardware part and software part. The image capturing is done by camera which comes under hardware part, whereas face detection, face recognition and voice notification are all will be done based on algorithms under software part.

Keywords: Facial Detection and Recognition, Feature extraction, FaceNet, Home Security, SVM

1. INTRODUCTION

Nowadays, availing the safety environment is very important when it comes to security. The main prioritized aspect is that, as people are busy in their modern lifestyle and there will be less assurance in safety of their things in and out of their home. The theft cases are also been increasing in particular area which is not under surveillance and protection. The main biggest reason that should be considered by the homeowner installing a security system is that it offers protection to family members and their things from burglar. Sometimes, this indicates that the presence of alarm system alone fixed in certain area is enough in most of the times to protect the home and their member from break-in. In certain cases, alarm can go off unfortunately which allows the third party to walk-in. So, having the home security system installed, often provides the members of the house with enough warning by voice notification and pictures related to intruders.

This security system would help such residential zones and organizations to safeguard their areas from unwanted intruders and visitors. Thus, by using only minimal use of resources, it'll help the residential owner to keep track of visitors of that area and thereby maintain the record of the visitors for future substantiation.

In facial recognition system, it will firstly capture the pictures or videos of the human entering into the residential area. Then, the system will make comparison between the images taken and the existing images in the previously stored database. During the phase, the system will compare the biometrics of the faces. This system will compare based on some conditions like distance between eyes, ears and so on. Many images of one particular face are taken. The picture must be in different angles and expressions.

When the person stands in front of the camera, face recognition process gets started and further comparisons will take place continuously. Nowadays, facial recognition is used everywhere because it has huge benefits. The main virtue of the proposed system is being scanned even when the person is in the long distance. This security procedure is main need for some places like residential areas, governmental organization and banks. Some person will fake their face by wearing some mask, cap or cloths, since it is the facial authentication device it will recognize the face easily. But other surveillance techniques have some reduction in their accuracy.

2. EXISTING SOLUTION

In recent years, there are many security systems have been developed for face recognitions. Every system has its unique algorithms for such recognitions. To recognize the person's biometrics, some system will extract the features of the face from the input image. In some systems, the face data and input images are compared but there is a lack of liveness detection. In some systems, 3dimensional facial recognition method is used. This 3dimensional recognition method will capture the complete shape of the face and its features like cheek, chin and

eyes. The complete advantage of this method is, even though when there is change in light and angles the face can be recognized.

Alternatively, in some existing security system, there will be an option for the owner to log on to their smart gadgets and access their security system remotely from anywhere. But, the main drawback of this security is that, people cannot able to view their security status of their area all the times continuously. So, there is a need of complete monitoring which is not possible and also there is great disadvantage is that they cannot restrict intruder directly when they are in out of that residential area. Another new technique that indulges for security purpose is that analysis of skin texture. Here, the visual details of the skin was analyzed like texture, color and jaw lines.

The following are the some of the previously used software programs for facial recognition and identification for security reasons. Firstly, Face first-which is a programmed software which allows liveness detection for video surveillance and also it generates a security alarm when the face is detected. Secondly, Morpho Trak-which is the leading solution providing technology for face and iris recognizing system. Thirdly, Cross Match Technologies which encompass facial biometric identification system.

3. METHODS FOR FACE RECOGNITION

In Face recognition, the risks related to human facial detection and recognition can be stated. The main factor of risks is that human faces are all relatively of same kind, yet differentiating facial expressions makes it more tedious process to simplify the suited algorithms. Every face has certain facial features. The surrounding factor which are considered during facial detection is that lightning and angles from which the face is detected through camera site.

Considering all into certain criteria, the security should be incorporated with the capability of measuring various feature of same and different faces. The software testing has to be done based on the numerous images that are stored in the database having different luminous condition, different angles, and various facial expressions. So that software will get trained and percentage of facial recognition will be done accurately. For home security access control, the technology used majorly is face recognition. As a result, the important tasks for the betterment of home security is that storing the database of known person details based on certain predefined conditions and testing, permitting access control for providing voice notification and mail notification and finally database retrieval happens is the person enter into the residential zone is unknown.

4. PROPOSED SOLUTION

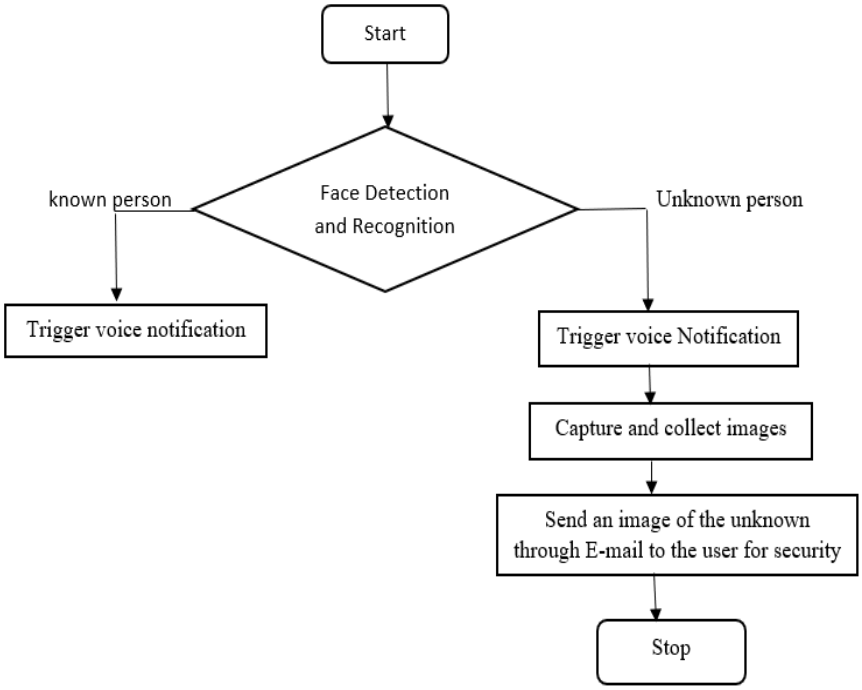

Fig 1. Proposed architecture

The proposed solution for the face recognition security system that reads the image of the person in a real time which also includes the feature of liveness detection, Voice notification to alert the user and also a mail verification to ensure the maximum security of the system. This system contains a camera which captures the image of the person and it checks if the face image of the person is present in the set of existing databases using face recognition method. It is categorized into two process: face detection and face recognition. This system also contains a feature

of mail verification for images if the face image of the person is not present in an existing database and if the person is unknown the image captured is sent to the mail of the user. This feature provides the extra security of who is encouraging at the door step.

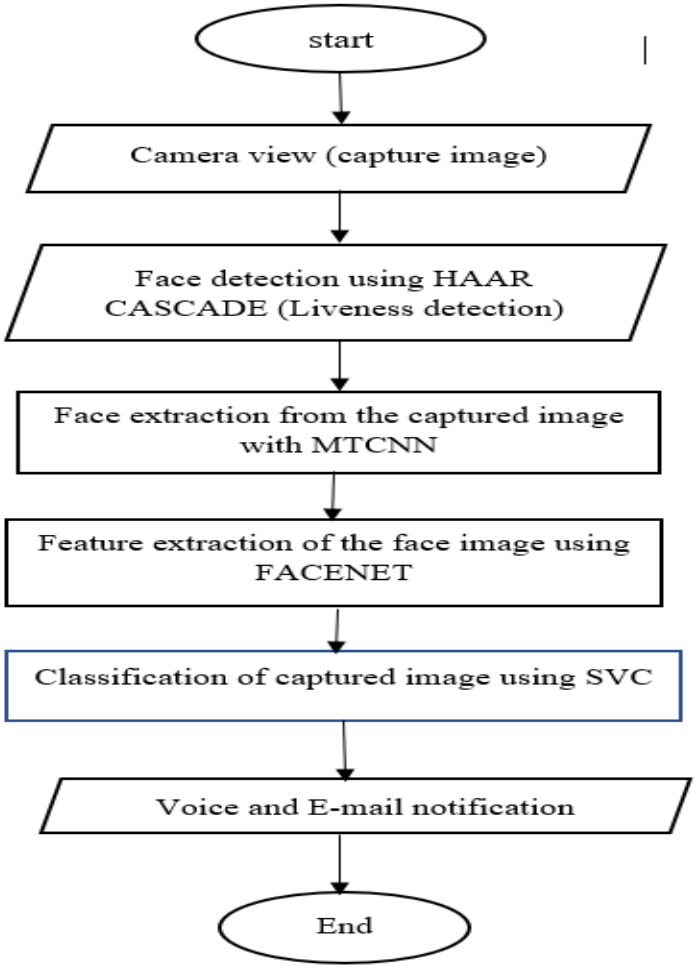

Fig 2. Data flow diagram

i. Face detection and liveness detection:

First, face Detection is a technology which is used to detect the presence of the person's face within digital images. Face detection identifies the person's face with an image or even with the video. This system uses Face Detection using Haar cascades.

Haar Cascades

Haar cascade is one of the effective ways for face detection. Haar cascade trains the classifier with positive and negative images. The Positive images are something which the classifier wants to identify whereas negative image contains everything else other than the positive image has. The Haar cascade uses matrices to represent the image that is captured. Each feature of the image is calculated by subtracting the sum of mixes under each category. At the end the sum of values of each classifier is compared with the threshold of the cascade and the decision is made whether the object is found or not by the cascade. This system also includes the feature of liveness detection in face detection. The process of liveness detection can be achieved by identifying whether the person is blinking his eyes while recording the image.

ii. Face extraction

Face extraction is the nothing but extraction the features of the person's face like eyes, nose, mouth, etc. Face extraction is the important process when it comes to face recognition. This system uses MTCNN (Multi-Task Cascaded Convolution Neural Network).

MTCNN (Multi-Task Cascaded Convolutional Neural Network)

MTCNN is a neural network which is used to detect faces and the facial landmarks of a person on images. MTCNN has 3 neural network connected in a cascade. The first process of MTCNN is creating the pyramid of the given image to identify the faces of different sizes. It creates different copies of the same image and also at different sizes to search for different sized face within the image. After passing each image it is scaled up to create

a multiple copy of the image and pass it to gathers the output. The output is created by listing the confidence level of the image using boundaries. The lower confidence boundaries are deleted and the boundaries with higher confidence are picked up.

iii. Face recognition:

Face Recognition is a method of identifying and verifying the individual using the image of the face. This security system uses embedded face net algorithm to recognize the faces of the captured image. It also uses SVM (Support Vector Machine).

Embedded FaceNet: FaceNet is used for performing tasks such as face recognition verification and clustering. FaceNet maps each image into a Euclidean space so that the distance in that spaces corresponds to face similarity. And when the embedding are created then all other tasks like verifying the person, recognizing the image of the person will be performed by the standard technique of the particular domain using the generated embedding as the feature vector. The system is trained so that the square distance between the embedding corresponds to the similarity in the face. The image used for training also scaled up and cropped around the face area

Support Vector Machine

SVM (Support Vector Machine) is used for both verification and identification of the image. For identification the system is given with the unknown images of the person. The algorithm checks with the existing database of known person and tries to identify the person and returns. For verification the known image of the person is given and the system claims that the person in known by going through the existing database, or the algorithm returns the confidence measure of validity of the claim.

5. RESULT AND TESTING

In the proposed face recognition security system, the algorithm was implemented using Jupyter Notebook. The output of the system was processed by the database that was accessed by the system. This system is a real-time face detection system which reads the image of the person in real-time through camera connected to the system running that software. The system captured the image of the person and process the image with the set of images in the database. Later, it recognizes the image and produces the output. This system was tested using several images and has achieved the face detection 98% accuracy of and face recognition accuracy of 95%.

6. CONCLUSION AND FUTURE WORK

Image Classification of visitors for home security is going to become more important in future as it ensures the security for the place we live in and provides better performance than other security systems. The detailed view of face recognition of this system is presented, which is used to verify and identify the person at outdoor using the image captured. This system is performed and coded in Jupyter Notebook which is based on face detection and face recognition. Although the accuracy of the system is above 94% and this system may be improved by utilizing the additional features.

And the future work may include the improvement of the face recognition system using more specific characters of the person like Iris detection or otherwise called as eye detection. Since Iris scanning are reliable and quick when compared to other methods. By including this technique, the probability of error will be decreased in the system and will be more and more accurate

REFERENCES

1. Facial recognition security system [Online], Available at: https://www.researchgate.net/publication/259027363_face_recognition_Security_system
2. Face Detection using MTCNN https://medium.com/swlh/face-detection-using-mtcnn-part-2-d3db8abf3047
3. Find facial recognition [Online], Available at: http://findbiometrics.com/solutions/facial-recognition/
4. Clustering with faceNet- http://sersc.org/journals/index.php/IJAST/article/view/8370
5. Building face detection and face recognition -https://towardsdatascience.com/how-to-build-a-face-detection-and-recognition-system-f5c2cdfbeb8c
6. [Machine Learning algorithm for Intrusion Detection System -https://medium.com/cuelogic-technologies/evaluation-of-machine-learning-algorithms-for-intrusion-detection-system-6854645f9211
7. Image Classification https://www.google.com/url?sa=t&source=web&rct=j&url=https://scholarspace.manoa.hawaii.edu/bitstream/10125/63858/0095.pdf&ved=2ahUKEwiy8Ln5qaXvAhUUILcAHXHLCFgQFjAAegQIARAC&usg=AOvVaw3xXoK5kDuAXvD8gXoNHZ0B
8. Introduction to FaceNet - https://mediumnot busy.com/analytics-vidhya/introduction-to-facenet-a-unified-embedding-for-face-recognition-and-clustering-dbdac8e6f02

9. Premkumar Murugiah, Vidhya Kandasamy, Santhosh. R.S, Selvamoorthy, M, Soundararajan A, Vignesh Kumar. B (2020), “Artificial Intelligence Based Students Attendance Monitoring System”, International Journal of Future Generation Communication and Networking, 13(2), pp. 2432-2438.
10. N. Nandhini and R. Bhavani (2020), Feature Extraction for Diseased Leaf Image Classification using Machine Learning, 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-4.
11. V. Vijayaganth, P. Purusothaman, M. Krishnamoorthi (2020), A Comprehensive Survey on Security Challenges and Techniques in Big Data, International Journal of Psychosocial Rehabilitation, 2020,Volume 24,Issue 06, Pages 6502-6508.
12. Raut N.B., Dhanya N.M. (2020) A Green Dynamic Internet of Things (IoT)-Battery Powered Things Aspect-Survey. In: Pant M., Kumar Sharma T., Arya R., Sahana B., Zolfagharinia H. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 1154. Springer, Singapore. https://doi.org/10.1007/978-981-15-4032-5_16
13. M. M. Asha and J. J. Ranjani, "Secure image retrieval using pyramid histogram of oriented gradient descriptor," 2013 International Conference on Advanced Computing and Communication Systems, 2013, pp. 1-5, doi: 10.1109/ICACCS.2013.6938712.