Journal of Web Development and Web Designing

Conference Paper · January 2021

CITATIONS
0

READS
1,115

4 authors, including:

Biplab Poudyal
Siddaganga Institute of Technology
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Suman Ranabhat
Nepal College of Information Technology
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Sweta Subedi
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Journal of
Web Development and Web Designing

Volume-6, Issue-1 (January-April, 2021)

www.matjournals.com

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

Advanced Safe Home Systems using Face-Recognition with Unique Passcode Systems

Biplab Poudyal[1*], Suman Ranabhat[2], Saroj Khadka[3], Sweta Subedi[4]
[1]UG Student, Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India
[2]Software Engineer, Marco Nepal, Nepal
[3]UG Student, Department of Computer Science and Information Technology, Sagarmatha Engineering College, Balkhu, Lalitpur, Nepal
[4]UG Student, Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India

Corresponding Author: poudyalbiplab@gmail.com

ABSTRACT

In this paper, we present a model for advanced security measure for safe home security system using face-recognition system and a unique pass-code for each user. Both face as well as unique passcode must be verified for the user to gain access to the building. For face-recognition system, we use HAAR cascade object detection algorithm by using HAAR classifiers. For unique passcode, we use google api for voice input submission and verification.

Keywords-- Face recognition system, HAAR cascade object detection, HAAR classifier, google, pass-code

INTRODUCTION

Whenever, there is term security, we are not ready for a compromise in what so ever manner. Whether it is related to their property or any other daily necessities, they always prefer for the best. In such, with increasing crimes that are occurring day by day, people prefer the best security to be provided for their homes. Facial-recognition and voice recognition are the two major aspects in which proper security can be provided for people for their house. Facial-recognition is a biometric technique in which a person's facial features are mathematically mapped and stored as data as a faceprint. Voice -recognition is a technique or an ability of a machine in which the person's voice is received and interpret dictation or to understand do the commands that are given by the end-users [1]. With these two techniques implemented, it is very difficult for the intruders to get access to the house unless permitted by the owner [2]. For the people living in the house, it is comparatively easier to monitor the entry and exit time of the people living there. To gain access to the house, both voice and facial samples must be stored first in the database with the house owner's permission. Because of which, the owner need not need to go and open the house by themselves. The guests can enter and exit at their own suitable time. All will be taken care of by the algorithm automatically. The only hard work to be done by the owner is when he/she has to store the image and voice sample in the database. The Biometric system has been in focus for quite some time nowadays. Till today, only fingerprint analysis or voice recognition has been able to claim the spotlight for providing security measures. But these two have never been combined into a single system for security measures [3]. Today, various effective measures are applied in regarding the safety of homes which are quite effective. But in all measures, the home-owner will be playing a major role and is not system-automated. The biometric-system will not only be able to keep the unwanted guest away from home but also keep the unknown person from entering the house [1, 2]. It is an absolute waste of time for home-owner to go to see the door whether the people there are known or not [1, 2]. If they are legitimate visitors, the system will automatically allow them to enter the house. Else will be stopped and prevent them from entering the house. The security measures used till now involve either a smartphone, or tablets, or any other such third-party systems which need to be controlled by

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

the homeowner. The use of a biometric system is not only limited in homes. It can also be used in various offices where highly confidential works are being carried out. And in such offices, it is not possible to install the security system where a third person or a third-device has to be in charge of whom to allow and whom to not in the office. Although, other biometric systems are already in effect, this model will further increase the accuracy and strength of the security system [3]. Currently, security measures such as monitoring cameras, smoke alarm systems, burglar alarm systems, medical alarm systems, critical alarm systems, etc. are in effect and all these systems have to be monitored by someone. Even in the security cameras that are fitted in the house, it is only capable of looking at the guests. The owner themselves have to decide whether to allow or not for them to enter the house [3].

This paper is organized in such a way that first it will give a brief introduction about the different biometric systems available, the current status of the biometric system in security measures that are in action today, the proposed model, and the advantages and disadvantages of using this model.

RELATED WORK

A number of works have been carried out in the field of security and countless research is still going on to make sure humans are living in a safe house without any fear of theft or any burglaries especially for old-aged people. Although, some works are already in progress, the only best method of providing security as of now is either fingerprint or retina scanning which is quite expensive and quite difficult to maintain it [4]. The proposed model provides maximum security with minimum budget and low maintenance cost but highly manual updating [5].

Voice Recognition

Voice recognition is a process, where the voice samples are collected and compared with the speakers to identify and recognize them on the basis of some patterns. When the term security is involved in any building, the voice recognition is least used, as it is the most difficult to install as well as maintain. There is no system developed with 100% protection but the only belief we would like to cling on is to get maximum security. Se we are emphasizing on a unique passcode for a unique user, which can be changed often by the user. This enables user from getting their voice recorded and used by some random guests. Even if they have the voice sample, without the correct passcode, the guest will be denied from accessing the building. The maintenance of voice recognition requires frequent update in the database as pass-codes might be leaked unintentionally. And for our system to provide maximum security, it plays a vital role.

Face Recognition

A face is an identity of any person. People adapt to respond more to a face than any other part of a body for recognizing them. With comparison to other biometric research topics, facial recognition is a popular research topic among others. With a number of applications such as surveillance and security, entertainment, virtual recognition, etc. facial recognition has always been recognized as a top research component in various industries [6]. With the advance in image processing, facial recognition has been easier [7]. Maintaining records and keeping track of it has also become more and more simplified for all applications. Here, we store all the faces of all the people who might visit us in a database [7]. This is of course a hectic task but will save a lot of our time later. Whenever, a new guest/person has to enter a house or an office, he/she has to enroll his/her face on a database with the permit of superuser, i.e., home-owner himself. Once the face is scanned, if is present in the database, then the entrant will be allowed for permission to enter the house [8]. Once the voice recognition test case passes, the control flows towards the facial recognition of that person for safety purposes as people may imitate the voice sample or record and use it as a password [8]. If any of these two fails, then the guest will not be allowed for the entrance of the home or building (Fig. 1).

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

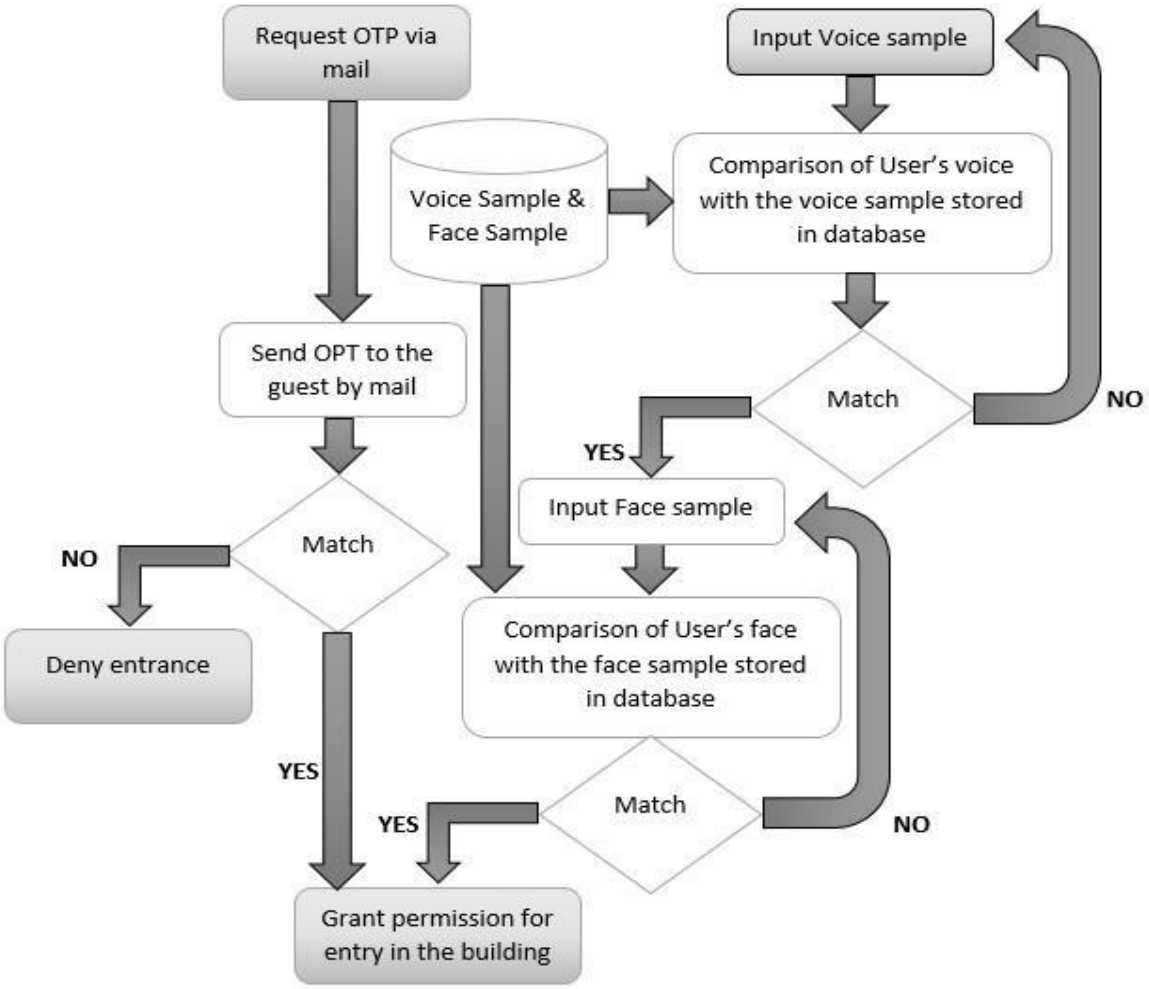

Figure 1: *A detailed process of the proposed model.*

PROPOSED MODEL

Our model is highly dependent on face-printing and voice-printing. With these two-security measure applied, it becomes one of the toughest to crack by some unwanted guests except for some exceptional hackers who has sound knowledge of computer and its technology. Whenever, the guest appears on the doorstep of the building, the project starts by taking in the face sample and then compare it with the image stored in the database. If a proper match is not found, the guest is immediately denied from access to the building. And for more than 5 failure attempts, the face sample will be immediately sent to the house owner via mail. If a match is found, the user has to provide his unique passcode. If face-recognition is working just as fine but due to some technical issues, the guest is denied from the access to the building, he/she needs to gain access via the one-time passcode which will be sent to the owner's mail only. But if the match is found in the database, access to house is gained. If any of the above two conditions fails, it is impossible to gain access. But what if the owner is not around the server where he/she can update new records in the database and the guest still wants to gain access. And sometimes, the owner themselves, due to some circumstances such as illness, their face and voice do not match the sample they provided in the database. So, the homeowner can provide a One-Time-Password to the guest, from which they can get access to the building. For that purpose, the guest has to send mail to the owner's phone, by selecting the option in the interface to send mail. The one-time password will be sent to the owner's mail and he can forward it to the guest for entrance. And even sometimes, they themselves can use it.

Pre-Processing

For voice recognition, we use the 'SpeechRecognition' package for this proposal create recognizer class instances. There are several api's available for this: google (), houndify (), ibm (), etc. But among these. We will be using google () for our project. For face recognition, in this model, we are using the default camera, i.e., web camera. So first we take in the input from the camera and

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

create a face cascade [9-11]. The images obtained are then transferred frame by frame [10].

Listening to Video

For listening to video, we will be using HAAR cascade algorithm for object detection. HAAR classifiers consists of a chain of stages, strong classifiers and 'committees' of classifiers [12]. The OpenCv classifier (H) structure is shown in the following Fig. 2.

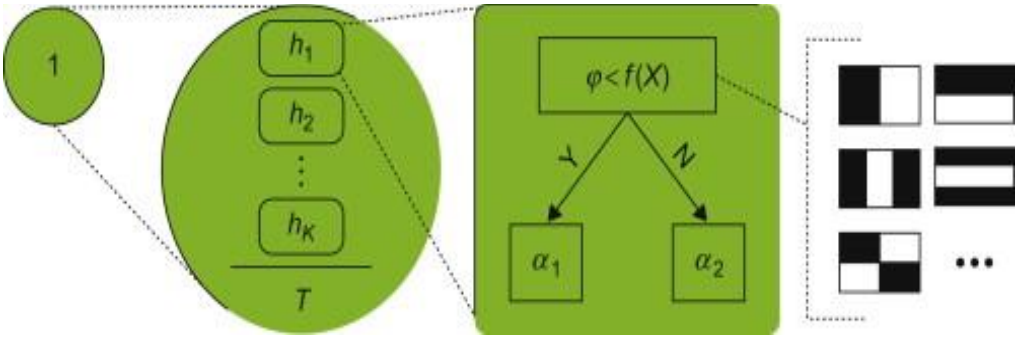

Figure 2: *OpenCv classifier structure.*

A set of K-weak classifiers (hi) and a stage threshold (T) is contained within the OpenCv classifier. They are responsible for calculating some function on the region of pixel and produce binary response, which is chosen on the base of HAAR features [12]. The weak classifier is calculated by:

$$h_i(X) = \begin{cases} \alpha_1, & f_i(X) > \varphi_i \\ \alpha_2, & \text{otherwise} \end{cases}$$

where, φi = threshold

Fi = one HAAR feature

A feature in weak classifier is a rectangular template, which is laid on the tested region. The black and white color indicates the change of sign when taking the sum of pixel value of input image, where black pixel denotes positive contribution and white denotes negative [12]. HAAR features consists of a list of tuples. The rectangle corners are integers and lies inside the classifier X * Y. After the summation of pixels which are under the rectangle, sum will be multiplied by the weight, i.e., a floating-point number [12]. A weak classifier is also represented as a decision tree, where nodes are HAAR feature and threshold and the leaves are α values [12]. As the depth of the tree increases, the time also increases [12] (Fig. 3).

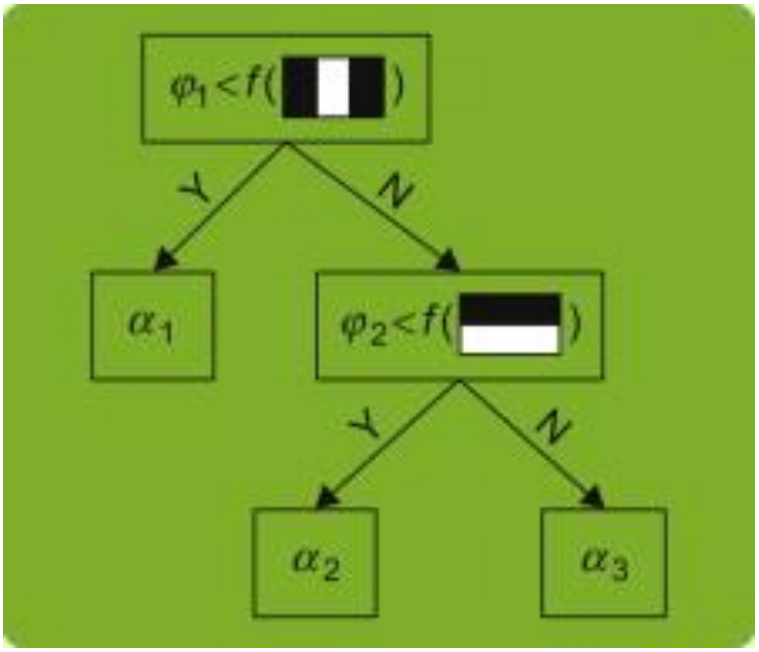

Figure 3: *Weak classifier.*

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

EXPERIMENTS

Dataset

The aim of the project is to take the image on-time from the installed webcam and compare the image stored in the database. The images can be stored in the database only by home-owner. The dataset we have used in this project is of 15 people where, the owner has to store the image in the database. The experiment was conducted in a broad day-light and a mic with good sound quality with minimum ambient noises. After the successful facial recognition, for super user, i.e., home-owner, it is responsible for the home-owner to store the database with sufficient encryption for security purposes as we are not handling the security for the database here in this project.

Evaluation

The performance of this model is calculated by using False Acceptance Rate (FAR) and False Rejection Rate (FRR) which has been considered as one of the many standard evaluation for biometric performance systems [13]. False Acceptance Rate is the measure of the likelihood for the biometric system to accept the access attempt by an unauthorized user [14].

$$FAR = \frac{impostor\ scores\ exceeding\ threshold}{all\ impostor\ scores}$$

False Rejection Rate is the measure of likelihood for the biometric system to decline the access attempt by an unauthorized user [15].

$$FRR = \frac{genuine\ scores\ falling\ below\ threshold}{all\ genuine\ scores}$$

Result and Analysis

Dataset In this paper, images obtained from the webcam are stored in the database and is used as preprocessing. We have taken sample from 15 people and tested the system for the proposed model. This provides the guests to have an easy submission and verification in the system for their face sample and voice passcode. Hence, resolves the complexity to the user and provides maximum security.
Face Recognition For each face, we take the face-sample from the webcam and use HAAR classifier for processing the image. Then stored in the database during the registration process. For testing, again the face sample was scanned in webcam and was compare to the face that are stored in the database.
Voice Sample For voice sample, the home owner provided a unique passcode to each user and same was stored in the database and compared when spoken.

With the sample obtained from 15 people, with the proper light and less ambient noise, our model was found to be 75-78% working without any errors. Some failures were obtained due to insufficient light and some due to presence of ambient noises.

CONCLUSION AND FUTURE WORKS

In this paper, a model for advanced measure for safe home security is presented with the use of face-recognition and passcode. With the use of this above algorithm, it reduces the efforts the building owner/manager has to put on his/her building to maintain proper security. The obtained result is highly accurate and data are well managed. The performance in this model can be further enhanced by taking the input of faces directly from the social media websites as people will be frequently using their social media. Moreover, we can conclude that the above-mentioned proposal for the safety home system is much more secured and with the minimum chance of crimes being taken place in either offices, houses, etc.

REFERENCES

1. “Facial Recognition”, [Online] Available from: https://searchenterpriseai.techtarget.com/definition/facial-recognition.
2. “Voice Recognition (Speaker Recognition)”, [Online] Available from: https://searchcustomerexperience.techtarget.com/definition/voice-recognition-speaker-recognition
3. “The Best Smart Lock for 2021”, [Online] Available from: https://www.pcmag.com/picks/the-best-smart-locks.
4. Dewsbuy Guy, Bruce Taylor, Martin Edge (2001), “Design in safe smart home systems for vulnerable people”, *The 1st Dependability IRC Workshop*.
5. Suryadvara N. K., et al. (2012), “Wireless sensors network based safe home to care elderly people: Behaviour detection”, *Sens. and Actuat. A: Phys*., Volume 186, pp. 277-283, DOI: 10.1016/j.sna.2012.03.020.

https://doi.org/10.46610/JoWDWD.2021.v06i01.001

6. Tawaniya, Jaishree, et al. (2014), "Image based face detection and recognition using MATLAB", *Internat. J. of Core Eng. and Manag*., Volume 1, Issue 2.
7. Mehta Preeti, Pankaj Tomar (2016), "An efficient attendance management system based on face recognition using MATLAB and Raspberry Pi 2", *Internat. J. of Eng. Tech. Sci. and Res*., Volume 3, Issue 5, pp. 71-78.
8. "How do machine learning and facial recognition algorithms work?", [Online] Available from: https://www.quora.com/How-do-machine-learning-and-facial-recognition-algorithms-work#.
9. "How Voice Recognition Technology Works", [Online] Available from: https://www.totalvoicetech.com/how-voice-recognition-technology-works/#:~:text=Digital%20voice%20recognition%20technology%20works,segments%20which%20comprise%20several%20tones.
10. "The Ultimate Guide to Speech Recognition with Python", [Online] Available from: https://realpython.com/python-speech-recognition/.
11. "Face Detection in Python Using a Webcam", [Online] Available from: https://realpython.com/face-detection-in-python-using-a-webcam/
12. "Classifier Cascade", [Online] Available from: https://www.sciencedirect.com/topics/computer-science/classifier-cascade#:~:text=Haar%20feature%2Dbased%20cascade%20classifiers,stages%20to%20form%20cascade%20classifiers.
13. Gupta Sandeep, Attaullah Buriro, Bruno Crispo (2018), "Demystifying authentication concepts in smartphones: Ways and types to secure access", *Mob. Inform. Syst.*, Volume 2018, DOI: 10.1155/2018/2649598.
14. "False Acceptance", [Online] Available from: https://www.webopedia.com/definitions/false-acceptance/#:~:text=The%20false%20acceptance%20rate%2C%20or,the%20number%20of%20identification%20attempts.
15. "FRR – False Rejection Rate", [Online] Available from: https://www.webopedia.com/definitions/false-rejection/.