Machine Learning Technique for Automatic Intruder Identification and Alerting

B. K. Uday, Anirudh Vattikuti, Kailash Gogineni and P. Natarajan

Abstract Security has become an important factor. Intruders have become prominent factors for all the data/property theft. The basic idea in this paper is to identify the intruder and alert owner/administrator in different possible ways. This paper discusses different ways such as "a message (SMS)", "WhatsApp message", "location of intruder", "an immediate call", and "intruder's image to owner's/administrator's WhatsApp" to alert owner/administrator. For identifying the intruder, machine learning algorithm is used. A camera placed at the locality is trained such that it can identify the familiar people and it is "on" all the time. Whenever an unknown/unidentified person comes to the vicinity of the camera, all the above-said features get activated and the owner gets alerted. The idea can be applied in many real-life situations, like thief identification near the house.

Keywords Intruder detection · Alerting owner · Machine learning · Image processing · Thief identification

1 Introduction

Identifying and catching intruders has become a difficult task as intruders/thieves found intelligent ways to tackle techniques used to catch them. It is similar to the story of a mosquito. Mosquitos are getting habituated for every new method to kill

B. K. Uday (✉) · A. Vattikuti · K. Gogineni · P. Natarajan
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India
e-mail: uday.nbausj@gmail.com

A. Vattikuti
e-mail: vattikuti.anirudh97@gmail.com

K. Gogineni
e-mail: gkailashnath1998@gmail.com

P. Natarajan
e-mail: palanisamynatarajan50@gmail.com

H. S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*, Lecture Notes in Networks and Systems 74,
https://doi.org/10.1007/978-981-13-7082-3_51

them. On this basis, the solution to the problem is found. In this paper, new ways are introduced to identify the intruder and alert owner/administrator. This paper discusses five different ways to catch intruder/thief viz "a message (SMS)", "WhatsApp message", "location of intruder", "an immediate call", "and Intruder's image to owner's/administrator's WhatsApp". This paper discusses how face recognition is used to detect intruders/thieves. All the familiar and known faces are trained first. If an unknown face is detected, then the owner/administrator is alerted. Machine learning is used for facial identification. Facial images of familiar persons are captured in every angle to recognize familiar persons in any angle. There are many algorithms for facial recognition. Some of them are Eigen faces [1], Fisher faces [2], and Local binary pattern histogram [3, 4].

The main purpose of the paper is to discuss and how to identify the intruder and alert owner/administrator. Intruders are mostly the ones, who does not belong to the same locality/does not belong to the same institution. Among all the methods of identifying the intruder using facial recognition, this paper discusses "Local binary pattern histogram". The system is trained in such a way that as soon as it identifies the intruder, "a message (SMS)", "WhatsApp message", "location of intruder", "an immediate call", and "intruder's image to WhatsApp" is sent. The implementation of the project is simple and more effective.

The distribution of the paper in different sections is as follows. Section 2 deals with the literature survey. In Sect. 3, description of the algorithm is provided. Section 4 deals with the technology to be used. Section 5 deals with methodology. Section 6 deals with process design. Section 7 deals with snapshots. Section 8 deals with the scope of the paper. Section 9 deals with conclusions. Section 10 deals with references.

2 Literature Survey

Florian Schroff et al. proposed that all the images are directly mapped to Euclidean distances [5]. Here, distances directly correspond to the similarity of the images. Once all the calculations are done, it is very easy to calculate the detection and recognition. Here, they mainly applied the clustering algorithm. They mainly used deep convolutional network to optimize the embedded faces and distances. The optimization has reached to that level that each face takes 128-bytes. Iti s one of the best algorithms used in "Face Recognition" history. The accuracy has reached to 99.68%, almost-human level performance.

Changxing et al. proposed a comprehensive deep learning method using neural networks [6]. The set of neural networks extracts the face features from multimodal data. Then, the extracted features are concatenated to form a high-dimensional feature vector. 9000 different subjects regarding face are considered and trained. The accuracy is about 98.4%. Almost human-level performance. These systems achieve 99.0% when we train the naturally available training dataset.

Kshirsagar proposed a methodology for recognizing the faces using principal component analysis and feature extraction [1]. The main goal is that it recognize the

face from large dataset with some real-time variations as well. Eigenfaces use PCA for face recognition.

John Wright et al. proposed that human should express all the feelings in front of a camera [7]. The algorithm trains itself. The cast recognition problem is one of the classifiers among multiple linear regression models and argues that new theory from sparse signal representation offers the key to addressing this problem. Based on a sparse representation computed by 1 minimization, we propose a general classification algorithm for (image-based) object recognition. This new framework provides new insights into two crucial issues in face recognition: feature extraction and robustness to occlusion. For feature extraction, this shows that if sparsity in the recognition problem is properly harnessed, the choice of features is no longer critical.

Yaniv Taigman et al. proposed 3D modeling transformation from nine-layer neural network by revisiting the important steps in face recognition [6]. This deep face recognition needs 120 million parameters. So, Yaniv et al. trained the algorithm over the biggest dataset to date. Over 4000 identities were covered. This method reached an accuracy of 97.35% on Labeled Faces in the Wild (LFW) dataset, almost approaching human-level performance.

3 LBPH Algorithm

LBPH stands for local binary pattern histogram. It is a descriptor used for facial recognition. The main algorithm behind this is LBP (local binary pattern). It is one of the best algorithms for texture or feature extraction. LBPH algorithm is a combination of LBP and HOG (histogram of orientated gradients) [8].

3.1 Concept

The process of LBPH algorithm is as follows:

The given image is converted into a matrix. Consider a pixel "a". Find the neighbors of the pixel (8-way connected).

- The formula for calculating the LBPH is

$$\mathrm{LBP}_{p,r}(N_c) = \sum_{n=1}^{8} N_p - \bar{N}_c \, 2^p$$

- Binary threshold function g(x) is

$$g(x) = \begin{matrix} 0, & x < 0 \\ 1, & x \geq 0 \end{matrix}$$

where N_p is neighbor pixel, N_c is pixel "a".
P = 0, 1, 2, …, 7 for 3 * 3 matrix, r = 1 for 3 * 3 matrix (radius).

- Now, LBP is combined with HOG.

4 Technology Stack

The paper deals with identifying the intruder and alerting owner/administrator. It implies that it recognizes known faces. It also implies that it detects the unknown faces. Technology stack includes machine learning and image processing.

- **Machine Learning**: It is the advanced technology in computer science, which helps the system to behave as a human. The base of the Machine learning is pure mathematics, which helps to perform wonderful tasks. "Haarcascades" are used to detect the structure of the face. Later, "LBPH face recognizer" is used to train the images for recognition. Now, the machine is trained to recognize some faces. Recognized data is loaded into the program and tested against the known and unknown faces.
- **Image Processing**: Image processing helps to do some processing techniques which help to improve the accuracy of face recognition.

5 Methodology

The methodology contains step by step to identify the intruder.

The first step in the process is to scan the faces of all known members of the vicinity. Each person will have a name and a unique ID number. He/She shall enter her details. After registering each person, training him/her is done. Every time this process is continued. The next step is the recognition. This whole process of the scanning, training, and recognition are made possible through GUI [9].

Later, the implementation code is dumped into Raspberry Pi, so that it becomes a real-time system. For scanning, training and recognizing machine learning is used. An algorithm named as Local Binary Pattern Histogram (LBPH) [*for recognition*] and haarcascades [*for detection*] are used. If an intruder is detected, automatically "a message (SMS)", "WhatsApp message", "location of intruder", "an immediate call", and "intruder's image to owner's/administrator's WhatsApp"is sent to the owner/administrator. The messaging/calling service is done by importing the TWILIO [10] library. TWILIO is a cloud platform for sending trial messages and calling services. It provides five trial messages and calls per day.

6 Designing the Process

The design includes the following steps.

The first step is the implementation of detection, training, and recognition. Later, the GUI part is integrated into the code. Then, the code is dumped into the Raspberry pi. The process of detection is started. The first step is to scan the faces of all the members of the vicinity. For each person, 25 images are captured and stored as a dataset. This set of images is trained. Each person has an ID value. Then, the next step is the recognition. When the trained members are recognized, the ID of the person will be displayed. Whenever the intruders are detected, then all the above-said ways to catch intruder are activated.

7 Output Screen Shots

7.1 Message Service and WhatsApp Service Snapshots

Figure 1 explains the core architecture and workflow. Figure 2 explains the message service. The message is triggered when an intruder is detected. Twilio [10] is used for this free message service. Figure 3 explains the WhatsApp service which triggers when an intruder is detected. Customized message can be sent to the owner/administrator. Selenium [11] module is used for this automation. The message in Fig. 2, "Sent from your Twilio trial account—Intruder Detected. Please call 100" is sent to the owner with the help of Twilio, when an intruder is detected. The message as shown in Fig. 3, "Intruder Detected Please Find Help" is sent from an automated system to the owner (*Samba*), when an intruder is detected.

8 Scope

The work might be extended as—if an intruder is identified, location and call can be sent to the nearby police station. Image of the intruder can also be sent to police mobile, this will help police to catch thief/intruder easily. By this, the probability of catching an intruder/thief will be much easier. By installing this kind of systems, the security will enhance exponentially.

9 Conclusion

Security is utmost important and face recognition plays a very important role. Using technology to solve real-world problems is the actual use of technology. This paper discussed how machine learning and image processing can be used to find intruders.

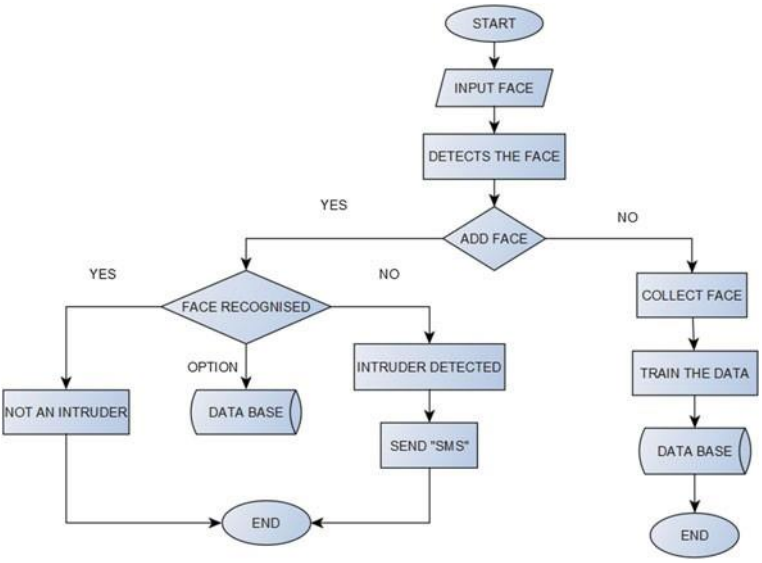
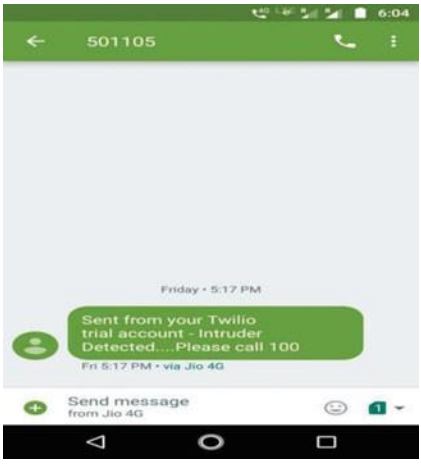


Fig. 1 Represents the architecture of intruder detection system

Fig. 2 Screenshot of message service



Machine learning algorithm local binary pattern histogram (LBPH) is used. Usually, it is very hard to identify intruders/thieves without any proofs, but with features such as “a call”, “a message”, “whatsapp messages”, “location of intruder”, and “Image of intruder” becomes very convenient and easy for police department to catch intruders. “Call” feature will serve as an immediate alert, which helps the owner/administrator to act quickly. If the image of an intruder is not known, it becomes very hard to find thieves. “Image of Intruder” will help to identify intruder easily. It also works as a proof to find the intruder. “Location” will help us to know where exactly the theft has

Fig. 3 Screenshot of WhatsApp service

taken place. With these features, it is very much possible to find the intruder and get back all the property/information. This paper concludes how intruder is efficiently identified with mentioned features.

References

1. Kshirsagar VP Prof, Baviskar MR, Gaikwad ME Face recognition using Eigenfaces
2. Lee H, Lee W-S, Chung J-H Face recognition using fisherface algorithm and elastic graph matching
3. Ahonen T, Hadid A, Pietikäinen M Face description with local binary patterns: application to face recognition
4. Ahonen T, Hadid A, Pietikäinen M Face recognition with local binary patterns
5. Schroff F et al FaceNet: a unified embedding for face recognition and clustering
6. Ding C et al Robust face recognition via multimodal deep face representation
7. Wright J et al Robest face recognition via sparse representation
8. Pang Y, Yuan Y, Li X et al Efficient HOG human detection
9. https://wiki.python.org/moin/TkInter
10. https://www.twilio.com/
11. https://www.seleniumhq.org