Retraction

Retraction: A Fast and Accurate Face Recognition Security System (J. Phys.: Conf. Ser. 1916 012185)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
A Fast and Accurate Face Recognition Security System

Sruthi M S1, Sarath S1, Sathish R1, Shanthosh S1
1Department of Computer Science & Engineering, Sri Krishna College of Technology, Kovaipudur, Coimbatore, Tamilnadu, India
Sruthi.ms@skct.edu.in, 17tucs206@skct.edu.in, 17tucs208@skct.edu.in, 17tucs216@skct.edu.in

Abstract. Using facial recognition technology, provide the best security system with alerts for smart devices such as laptops and PCs. The design descriptions of the various modules involved in automatic face recognition are presented in this paper: face detection, face identification, and face verification. Also we're visiting further process the image captured by CV to test whether the person is allowed or unauthorized to access the laptop or PC using openCV and native Binary Pattern Histogram (BPH) Algorithm. The LBPH algorithm is also a simple solution to the problem of face recognition, since it can identify both the front and side faces. A updated LBPH algorithm assisted pixel neighbourhood grey median (MLBPH) is proposed to solve this problem. After detection, the image is verified and allows only the user to access the laptop or PC if he/she's authorized. And if not, an e-mail or message is pushed to the respective person to alert that somebody else is using his/her laptop by enhance the privacy.

Keywords: OpenCV, face detection, face identification, face verification, Local Binary Pattern Histogram (LBPH).

1. Introduction

In this project, a secure face recognition system is presented, during which face detection is performed with facial expression. Facial detection might be a lively area of research. It entails extracting data such as key-points, poses, expressions, gender, age, and identity, among other things. It has a variety of uses, including law enforcement, active user authentication, face biometrics for purchases, and self-driving cars [1]. Face detection is one of the biometric data processes; its applicability is easier, and its working range is broader than other biometric data processes, such as fingerprint, identity, signature, and so on. These devices are often used for crime prevention, video monitoring, individual verification, and other types of protection. Face recognition devices are suitable for such systems because they have recently improved in speed, cost, and robustness [2].

Computer programs analyse photographs of human faces in order to recognise them, which is how facial recognition systems function. These devices recognise and detect human faces automatically. Recognition algorithms such as the LBPH algorithm are used in these systems. The first step in face recognition is to recognise a person's face and separate it from the rest of the scene. The machine then calculates nodal points on the forehead [3]. These nodal points are then compared to nodal points computed from a database of images in order to determine whether they are a match.
2. Aims and Objectives

To provide best security with alert for smart gadgets like laptops with the employment of identification technology [4].

The objective of the project is to propose an enhanced method to detect intruders who tries to realize illegal access of a laptop or the other gadget.

The objectives are:

- Identifying somebody's within the frame.
- Identifying whether the human is that the rightful owner or an intruder.
- Extracting face features from the frame.
- Designing a enhanced tool to send notification to the rightful owner of the gadget.

3. Related Work

Many authors have explored numerous face recognition techniques over the last 30 years, encouraged by the growing number of universe applications involving the popularity of human faces [5]. Face recognition is one of the few biometric techniques that have the advantages of high accuracy and low intrusiveness [6]. It's a physiological approach that's both accurate and non-intrusive. Leading to a variety of problems, automatic face recognition is incredibly difficult. When an individual's face image is placed into a database, however, it is typically collected in a number of circumstances. Face recognition is useful for resolving variations in the following parameters: expression, lighting, voice, gesture, facial hair, glasses, and image history [7].

Face recognition algorithms come in a variety of forms, such as:

- Eigen faces (1991)
- LBPH - Local Binary Patterns Histograms (1996)
- Fisher faces (1997)
- SIFT - Scale Invariant Feature Transform (1999)
- SURF - Speed Up Robust Features (2006)

Works:

- A PIN (Personal Identification Number) Code: Here a singular number is assigned to users. That’s matched with the user credentials stored within the database.
- An ID (Identification)/Password: To Open a session on a computer or to authenticate on internet, the authentication is completed by verifying whether the password matches with the user name stored within the database [8].
- An RFID Card: Radio-frequency identification (RFID) is a technology that recognise and detects tags attached to items using electromagnetic fields. Data that has been stored in an electronic format should be included in the tag.
- A Webcam-based identity verification system: face recognition is a form of biometric authentication that identifies countenance by extracting points of interest, or highlights, from a photograph of the subject's face.
4. Tools Used and Its Description

4.1 OpenCV
Open Source Computer Vision is also a programming library with functions aimed at computer vision around the world. It's possible that the library will be cross-platform, and it's free to use under the open source BSD licence. TensorFlow, Torch, Caffe, and other deep learning frameworks are supported by OpenCV. It had been written in C and C++ programming languages. OpenCV has a variety of uses, including:

- 2- Toolkit for dimensional and three-dimensional features.
- System for facial recognition.
- Communication between humans and computers.
- Robotics on wheels.
- Identifying the items.

4.2 Anaconda
Anaconda is an open-source platform for scientific computing that aims to make package management and deployment easier. It is written in the Python and R programming languages. Conda, the package management system, is in charge of managing package versions. Spyder is the Integrated Development Environment (IDE) used in Anaconda [9].

4.2.1 Spyder
Spyder is a cross-platform open source application. It's a Python-based Integrated Development Environment (IDE) for scientific programming. Spyder works with a variety of Python packages, including NumPy, SciPy, Matplotlib, pandas, IPython, SymPy, and Cython, as well as other open source applications, and is licenced under the MIT licence.

4.3 Python
Python is an interpreted high-level general-purpose programming language. Python's design philosophy puts a focus on code readability, as shown by its liberal use of whitespace. Its object-oriented technique and language constructs were aimed to help programmers in creating quick, logical code for both small and large projects [10].

Python is dynamically typed and garbage-collected. Structured (especially procedural) programming, object-oriented programming, and functional programming are one of the programming paradigms it supports. Because of its wide standard library, Python is very often referred to as a "batteries included" language [11].

5. Algorithms Used in Project
The Local Binary Pattern Histogram (LBPH) is a simple but effective texture operator that threshold each pixel's neighborhood and treats the result as a binary number to classify pixels in an image. Since it can recognize both front and side faces, the Local Binary Pattern Histogram (LBPH) algorithm is another straightforward solution to the problem of face recognition. This project proposes an improved LBPH algorithm that includes pixel neighborhood grey median (MLBPH).

It was first established as a texture classification function in 1994 (LBP) and has since been discovered to be very successful. Combining LBP with the histograms of focused gradients (HOG) descriptor has also been found to dramatically improve detection accuracy on a few datasets.
We may represent the face images with a simple data vector using the LBP combined with histograms. LBP could be used for face recognition tasks as it can also be a clear descriptor, as seen in the following step-by-step clarification.

5.1 How It Works
Face recognition is the process of identifying someone based on their facial expression in technology. It has gained a high reputation in the last two decades, owing to the development of modern methods and, as a result, the best output of these videos/cameras.

5.2 Various Phase In Algorithm:
- Face Detection: the purpose here is to identify (and hopefully remove) the faces in an image so that the face recognition algorithm can use them.
- Face Recognition: The face recognition algorithm is responsible for selecting the best characteristics to classify the image after it is extracted, cropped, resized, but often converted to grayscale.

5.3 Working Of Face Recognition:
At this stage, the algorithm has already been developed. A different histogram is also used to represent each object in the training dataset. As a result, we repeat the steps after an input image to create a histogram that represents the image.

We simply compare two histograms and return the image with the neighbouring histogram to find the image that corresponds to the input image. We are using a variety of methods to match the histograms such as euclidean distance, chi-square, number, and so on. In our project, we can use the Euclidean distance by the following equation (1):

$$D = (\text{hist}_1 - \text{hist}_2)^2$$

The ID from the image with the nearest histogram is the result of the algorithm. The algorithm should also return the measured distance, which can be used as a measurement of confidence.

6. Overview of Work

![Figure 1. Overview of work](Retracted)
7. Module Description Of Project

7.1 Face Acquisition:
The picture is shot using the camera in the initial process. To remove the face position issue, the captured image is transformed to grayscale and resized. To remove noise from images, the pre-processing is completed. Also, to eradicate illumination and darkness, various basic methods such as Histogram Equalization (HE) and Discrete Wavelet Transform (DWT) are used.

7.2 Pre-processing:
"Image pre-processing" refers to operations on images from the most foundational level of abstraction. If entropy is a metric, these operations reduce image information content rather than increase it. Pre-processing is a method for improving image data by eliminating unwanted distortions or enhancing specific image features that are important for future processing and analysis.

7.3 Feature Extraction:
Feature Detection Process: In this phase, the LBP operation is used to remove the countenance from an image by comparing the intensity value of each component to the values of the 8 nearest neighbour pixels. If the neighbouring pixel's price is higher than the centred pixel's price, it will be assigned 1; otherwise, it will be assigned 0. This task generates an 8-bit string for each pixel. The LBP value is determined by the decimal value of an 8-bit pixel array.

7.4 Authorization:
Authorization is also a protection mechanism for determining user/client privileges and access levels to system resources such as files, facilities, computer programmes, data, and application features. This may be a strategy for granting or refusing access to a network resource that grants the user access to a variety of services that are tied to the user's identity.

8. EXPERIMENTAL RESULTS
Analysis of Face Recognition security system using LBPH is predicted in Figures 2-5.

Figure 2. Create Training Face Data
Figure 3. Train Model with Captured Image

Figure 4. Face Recognition – verifies either authorized person or unauthorized person

From the Analysis it is found that Linear Binary Pattern Histogram algorithm provide maximum accuracy compared to other algorithm. In this recognition security system, If the person is authorised and matched with Dataset it is “UNLOCKED” else it is “NOT UNLOCKED” and send a security message alert to respective system user using Twillo trial account.
9. Conclusion

Face recognition technology is usually associated with high-end, high-security applications. Today's core technologies have progressed, and equipment costs have decreased. Face recognition technology is now cost-effective, dependable, and highly accurate in many applications. The proposed framework would help to improve the security of personal data stored on physical devices. This method would aid in the enhancement of security in ATMs and other platforms.

References

[1] B. QIN, D. LI, identifying facemask-wearing condition using image super-resolution prevent covid-19 (2020).
[2] S. Li, X. Ning, L. Yu, L. Zhang, X. Dong, Y. Shi, W. He, 2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS) (IEEE, 2020), pp. 1–5
[3] P. Khandelwal, A. Khandelwal, S. Agarwal, using computer vision to enhance safety of workforce in manufacturing in a post covid world, arXiv preprint arXiv:2005.05287 (2020).
[4] M. Jiang, X. Fan, Retinamask: A face mask detector, arXiv preprint arXiv:2005.03950 (2020)
[5] S. N.C. Ristea, R.T. Jonesu, are you wearing a mask? improving mask detection from speech using augmentation by cycle-consistent gans, arXiv preprint arXiv:2006.10147 (2020).
[6] W. Liu, Z. Wang, X. Liu, N. Zeng, A survey of deep neural network architectures and their applications 234, 11 (2017).
[7] H. Anandakumar and K. Umamaheswari, Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers, Cluster Computing, vol. 20, no. 2, pp. 1505–1515, Mar. 2017.
[8] H. Anandakumar and K. Umamaheswari, A bio-inspired swarm intelligence technique for social aware cognitive radio handovers, Computers & Electrical Engineering, vol. 71, pp. 925–937, Oct. 2018. doi:10.1016/j.compeleceng.2017.09.016
[9] Mangmang, G. B. Face Mask Usage Detection Using Inception Network. Journal of Advanced Research in Dynamical and Control Systems, 12(SP7), 1660–1667. (2020).
[10] Fuchs, E. J. (n.d.). Face mask removal time of four face mask extrication devices.
[11] Siegfried, I. M. Comparative Study of Deep Learning Methods in Detection Face Mask Utilization (2020).