International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-10, Issue-3, May 2022
https://doi.org/10.55524/ijircst.2022.10.3.16
Article ID IRP1178, Pages 83-86
www.ijircst.org

Development and Analysis of Biometric Ingress Surveillance

Shweta Sinha[1], and Juhi Singh[2]

[1]Associate Professor, Department of Computer Science and Engineering, Amity University Haryana, India
[2]Assistant Professor, Department of Computer Science and Engineering, Amity University Haryana, India

Correspondence should be addressed to Shweta Sinha; shwetakant.sinha@gmail.com

ABSTRACT- Face recognition is a classic problem in the field of computer vision and popular due to its wide applications in real-world problems such as access control, identity verification, physical security, surveillance, etc. Recent progress in deep learning techniques and the access to large-scale face databases has led to a significant improvement of face recognition accuracy under constrained and semi-constrained scenarios. Deep neural networks are shown to surpass human performance on Labelled Face in the Wild (LFW), which consists of celebrity photos captured in the wild. This technology can be used to create a surveillance for the ingress systems with broad scope of application in multiple scenarios. The major ingress problems that will be address will include, but are not limited to: lack of automata, robust face normalization, discrimination, representation learning and the ambiguity of facial features caused by information loss. This paper discusses biometric ingress surveillance. With a brief review of the subject the paper presents an application in this domain that highlights the true potential of a surveillance system that can have face recognition as a biometric authentication to ingress at homes, offices, universities and other potential ingress systems.

KEYWORDS- computer vision, face recognition, internet of thing, biometric surveillance.

I. INTRODUCTION

In biometric and computer vision communities, face recognition (FR) has emerged as one of the major research fields focusing on the design of algorithms that can automatically authenticate people's identities based on their digital face images. With the rapid proliferation of face images or "selfies" on social media websites, such as Facebook, Twitter, and Instagram, researchers in the FR community have access to abundant images and videos of human face, which has rapidly accelerated the development of FR systems and extended its applications. For example, FR systems are widely adopted for security-related applications (e.g., access control, surveillance systems), forensic applications (criminal identity verification), and entertainment applications on desktops and mobile devices, for example, mobile apps for face photo editing.

As a convenient authentication tool, FR requires minimal interaction with users and can even operate under uncontrolled environments and at a distance [1]. Compared to other biometric traits (i.e., iris, fingerprints, voice, etc.), in addition to identity, a human face image contains several useful information, including demographics (gender, age, race/ethnicity), facial expression, and emotion cues. As a result, a further in-depth study on IoT is conducted to support the idea of this project. The growing demand for connected devices and the increase in investments in the Internet of Things (IoT) sector induce the growth of the market for this technology. IoT permeates all areas of life of an individual, from smart-watches to entire home assistants and solutions in different areas. The IoT concept has been gradually increasing all over the globe. IoT projects induce an articulation of studies in software engineering to prepare the development and operation of software systems materialized in physical objects and structures interconnected with embedded software and hosted in clouds. IoT projects have boundaries between development and operation stages.

Towards exploring face recognition and Internet of Things, a solution had emerged to develop a general purpose biometrically authenticating ingress system. This paper focuses on the design, implementation, application and evaluation and presents empirical results towards the development of the system. Today as the population increases, there is a rise of human interaction that makes it difficult for a human system to track every person and also keep a record. There are some places where humans cannot be trusted of their safety may be compromised. There are multiple problems that this ingress system targets as well as create more solutions than just being a security camera. The purpose of this project is to see all the perspectives for the system and the suitable execution for any future systems.

The paper begins with a brief review of the concept in section 2, followed by the design methodology in section 3. The architecture of the model, and working on the way of testing and implementing the concept in real life is discussed in section 4. In the end the paper concludes all the observations and discusses about the potential future scope of the system to see where this project can go in the future.

II. BACKGROUND INFORMATION

To understand computer vision based project some fundamentals must be addressed to have a clear picture of how the system runs. Let's start by thinking how important vision can be. Most people rely on it to prepare food, walk around obstacles, read street signs, watch videos and do hundreds of tasks. Vision is the highest bandwidth sense, and it provides a firehose of information about the state of the world and how to act on it. For this reason, computer scientists have been trying to give computer vision for half a

century, birthing sub field of Computer Vision. its goal is to give computer the ability to extract high-level understanding from digital images and videos. As a refresher, images on computer are stored in pixel grids where each pixel is defined by a color value called an RGB value. Perhaps the simplest computer vision algorithm, and a good place to start, is to track a colored object, like a bright red ball in an image of football game. The first thing we need to do is record the balls color. For that we take the RGB value of the center most pixel. With that value we can give a computer a program an image and ask it to find the pixel. An algorithm like this might start in the top right corner and check each pixel one at a time calculating the difference from target color. Now having looked at every pixel, the best match is very likely pixel from our ball. There is not a limit to run this algorithm on a single photo and therefore can be repeated for every frame in a video allowing the system to track the ball. But this system is having its limit due to variation in lighting, shadows, and other effects on the ball. Also, the field may contain more spots with the same RGB values. For this reason, color marking trackers and similar algorithms are rarely used unless the environment is tightly controlled. This type of algorithm work only on pixel and may not perform on complex features like edges of object which are made up of multiple pixels. To identify these types of features computer vision algorithm, have to consider a small region of pixel, called patches. Then these patches can be run in an algorithm to extract edges and corners which are computed by kernels. These types of kernels can begin to characterize simple shapes. When a computer scans through an image, most often by sliding around a search window, it looks for combination of features indicative of familiar shapes like faces, traffic lights, road signs, vehicles and much more. Although single kernel may be weak detector, a cluster of them are quite accurate. This was a basis of an early influential algorithm called Viola-Jones Face Detection.

III. METHODOLOGY

The methodology of this project is simple and highly accurate. The report presents a novel advanced AI face recognition-based system which can identify the person after collecting the data set from the admin/user. The system is economically feasible to prepare and purchase in near future. It is fast to detect and display the result accordingly. The system automatically and consistently keeps looking for the faces once plugged to a power source and sends the text message to the authorized person about the identified person. This report presents a system which decreases human intervention and is advanced in the technological aspects of life. This system decreases human interference where the trust is less and hence protects the data and property. With the proposal of this system our asset stays in safer hands, there is no possibility of theft and corruption. The system is installed with raspberry pi 4 and Arduino nano which is the most trusted micro-controller and is easily available with easy deployment properties. it supports python and is very easy to interact with.

IV. MATERIAL AND METHODS

A. Steps and Detailed Explanation

The process of detecting a face begins with system trying to recognize facial features like nose, mouth, eyes, ears and other features and then bring them all together to construct a face to identify it [2]. Identical work is done by the means of Open CV. a system face recognition begins with an image containing face. An image of the user's face is captured from a source which can be a photo or a still form a video feed. The face recognition algorithm looks for facial features in the image and using the data creates what can be called as a face ID which is unique to every user. Then the facial ID is compared with other face ID database to find a perfect match. An output is generated when a face ID is matched in the database.

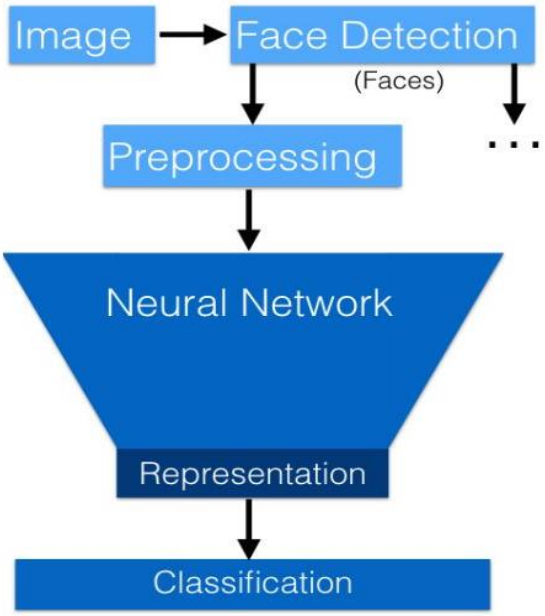

Figure. 1: Logic flow for face recognition

As shown in Fig 1, the pipeline of face recognition includes 3 steps: feature extraction, normalization and comparison. Normalization is a step where spatial modifications are performed to lessen the facial variations before sending the image data to a facial feature extractor algorithm. There are multiple possible ways to do it and to reduce these variations. As shown in Fig 2, the most suitable solution considered was to use the location of bounding box or to crop out a canonical view from the image data of the face. The eyes, nose, mouth corners are the most common landmarks the help in transforming the image.

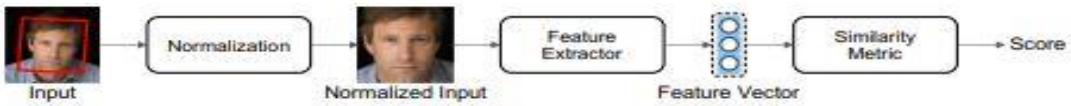

Figure. 2: Flow chart of evaluation metric

Feature Extraction step uses a manually designed or a learned representation to extract distinct facial features from the normalized images. Using LBP descriptor [3] and LDA methods [4] the features are scripted. This maps an RGB image of a fixed length to a feature vector.
Similarity Metric: The choice of similarity metric mainly depends on the representation. For example, for histogram-based features, such as LBP measure is used to compute the distance.

B. LFW Verification

This verification system predicts whether there exists a pair of images in which there are identical faces. The LFW has 13,233 images from 5,750 people and this experiment provides 6,000 pairs broken into ten folds. The accuracy in the restricted protocol is obtained by averaging the accuracy of ten experiments [5]. The data is segregated into ten equal folds and each of the experiment starts to learn on nine folds. The results of Open Face are collected by processing the squared Euclidean distance on the pairs and marking pairs under a threshold as a unique identity of a person and above the threshold as completely non-identical population. The most optimized threshold on the training fold is taken and the applied to all the other remaining folds. The best threshold outcome is 0.99 that comes from nine folds out of ten folds.
The verification threshold can be varied and plotted as shown in fig 3, an (receiver operating characteristic) ROC curve. The ROC 0curve shows the trade-offs between the TPR and FPR. The perfect ROC curve would have a TPR of 1 everywhere, which is where today's state-of-the-art industry techniques are nearly at. The area under the curve (AUC) is the probability the classifier will rank randomly chosen faces of the same person higher than randomly chosen faces of different people [6]. Every curve is an average of the curves obtained from thresholding each fold of data.

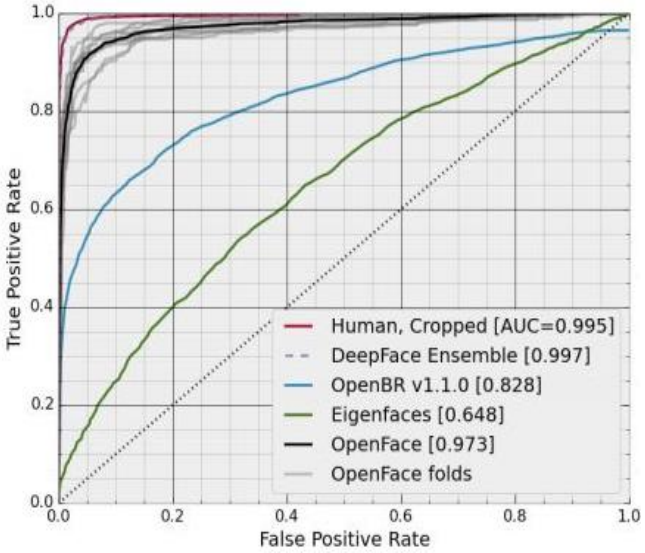

Figure. 3: To train the data,the database has been extracted from crowd sourced directory [7]

C. Design

As shown in Fig 4, The system comprises of Raspberry pi, Arduino nano, Arduino nano-servo moter/Gate, an LCD Display and a camera. The connection is as follow:

- A RED wire connected to 5Volt power and green connected to ground.
- Physical pin 39 of the raspberry pi is connected to the power distribution board which denotes the ground.
- Then a red wire of 5 Volt (physical pin 2 of raspberry pi) is connected to the bread board.
- For output we have selected physical pin 16 and 18 of Raspberry pi which are connected to the A0 and A1 of the Arduino nano respectively.
- Then a servo moter/Gate is connected to the Arduino nano
- Blue wire of servo moter/Gate is connected to the D6 of the Arduino nano.
- The red wire is connected to the 5V power supply and green wire is connected to the ground of the power distribution board (bread board).

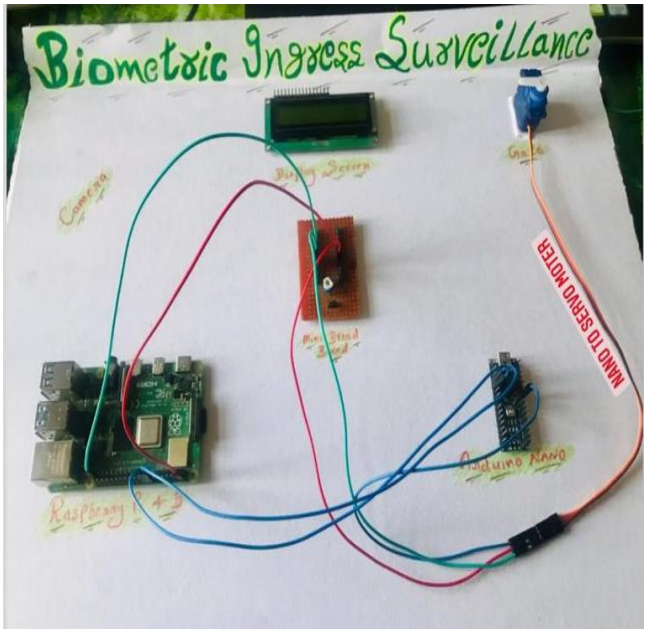

Figure. 4: Design of the system

The whole system consists of 5 elements which are Raspberry pi 4, Arduino nano, Mini bread board, display screen, servo moter. When the camera detects a face and44 recognizes it with the authorized person then the raspberry pi give output on its 16and 18 physical pin which are connected to the arduino nano. Then the arduino nano give output on the display screen and servo moter comes in action. If image is recognised the display screen will show the access status and gate will open with a notification [8] on the owner's mobile and after 10 seconds it gets closed.

D. Application

This section includes the result and applications of the system proposed. This project presents with certain that the internet of things and computer vision will be an important field for humans. This technology is really promising and will be greatly applicable to support human ingress. The main purpose of this system is to deliver a secure system for better trust and future. It can be used where confidentiality is the prior concern of everyone and man power could not be trusted.
As it has the surveillance property it can maintain a proof of theft and hence can help in avoiding too. This can be installed

in bigger banks and safes where situation is always critical and trust is less worthy. The potential application of this project is in homes, offices, courts, evidence room, hospitals, banks etc.

The system can be installed in big homes where there is constant movement of servants and caretakers. The system can be used in banking locker system to authenticate the admin. The system can be integrated into classrooms to keep track of their attendance system.

V. RESULT

A fully functional system which is a combination of hardware and software (hardware: Arduino UNO Board, software: python, OpenCV, Haarcascade classifier.). The mail is being received by the authorized person on the spot which makes the environment easily surveillant. The proposed system can be installed anywhere according to the need with least complexity and human interference.

To test the system, four random users face data was selected and input in the system. The system was trained and hence detected the users with high accuracy rates. After multiple testes conduction, the following graph was produced:

Figure. 5: Accuracy Rate Plot

In the graph plotted, there are four bars against different values. The bar represents the values of the success of the system of different user in four different scenarios that are labeled as

- Face without mask
- Face with mask
- Face in low light
- Instant process

This graph shows the systems high accuracy. Further as soon as the system detects the face it sends the notification to the admin/owner informing if the access is granted or not.

VI. CONCLUSION

A face detection and notification sender system using Arduino UNO and OpenCV. It has many different day to day uses like: in banks for surveillance and security purpose, in homes for surveillance, in hospitals to maintain confidentiality of the patients, in offices for access management, etc. The system uses the idea of free platform i.e.; OpenCV and Arduino has the hardware support to give the access to the idea proposed. More human intervention in the critical area is harmful for the user and can lead to many more severe losses. Therefore, the system was introduced to lower the human interference and increase the security aspect of life and the data involved.

Some potential improvement can be proposed it the system as the technology advances. Cameras can be replaced with lidar scanners where the security needed is highest, higher processing to be designed for a bigger large-scale project where the system needs to look into hundreds or thousands of people at the same time. For instance, an office hall, a classroom or an auditorium. The system can also have an SOS system for home breach with an alarm system. The project can further be improved by adding a human AI face on a display at ingress that gives the user a much better and organic feel while interacting with the system.

REFERENCES

[1] P. Viola and M. J. Jones, “Robust real-time face detection,” International journal of computer vision, 2004.
[2] M. Ghallab,“Robotics and Artificial Intelligence: a Perspective on Deliberation Functions,” pp. 1–19.
[3] B. Maze, J. Adams, J. A. Duncan, N. Kalka, T. Miller, C. Otto, A. K. Jain, W. T. Niggel, J. Anderson, J. Cheney, et al., “Iarpa janus benchmark-c: Face dataset and protocol,” in ICB, 2018.
[4] B. F. Klare, B. Klein, E. Taborsky, A. Blanton, J. Cheney, K. Allen, P. Grother, A. Mah, and A. K. Jain, “Pushing the frontiers of unconstrained face detection and recognition: Iarpa janus benchmark a,” in CVPR, 2015.
[5] http://vis-www.cs.umass.edu/lfw/#download
[6] Gary B Huang, Manu Ramesh, Tamara Berg, and Erik Learned-Miller. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Technical report, Technical Report 07-49, University of Massachusetts, Amherst, 2007.
[7] http://vis-www.cs.umass.edu/lfw/#download
[8] Neeraj Kumar, Alexander C Berg, Peter N Belhumeur, and Shree K Nayar. Attribute and simile classifiers for face verification. In Computer Vision, 2009 IEEE 12th International Conference on, pages 365–372. IEEE, 2009.