Chapter 41
Identification of a Person From Live Video Streaming Using Machine Learning in the Internet of Things (IoT)

Sana Zeba
https://orcid.org/0000-0003-1311-7817
Department of Computer Engineering, Jamia Millia Islamia University, New Delhi, India

Mohammad Amjad
Department of Computer Engineering, Jamia Millia Islamia University, New Delhi, India

ABSTRACT

In this paper, the authors develop an efficient face recognition algorithm from images or live video streaming for IoT systems based on K-nearest neighbor and support vector machine learning to recognize the person from the local database and extract the features of the face. Because of the complexity of the conditions, there might be some factors of facing errors like the size; the angle; the distance from the ear, nose, and eyes; etc. This sustainable machine learning-based IoT system is designed for sovereign face recognition with features extraction with improved accuracy near about 96%. The experimental study is done to test the performance of the face recognition in the changes of number of persons in video or images. Finally, this manuscript recognized persons from live video or images with accuracy approximately 96% by using the SVM and KNN classifiers and discussed with the block diagram and proposed algorithm.

DOI: 10.4018/978-1-6684-7132-6.ch041

INTRODUCTION

An Evolutionary and Emerging technology, the Internet of Things (IoT) generates new scopes and opportunities in engineering and science applications for cracking humans' problems. Without the interference of human beings, different emerging technologies make our life fully or partially automated. (Kumar & Mallick, 2018) Face recognition algorithm considers as an important factor in various areas such as identification, authentication of the persons, identification of criminals, security, and privacy of sovereign information of users in IoT applications. The Internet of Things (IoT) environment is the collection of computing devices, mechanical object, and digital machines thing, object, electronic devices which can communicate and access the data among devices from anywhere in the network (Haque et al., 2021). Each thing or objects have unique identifiers (UIDs) for identification purpose. Recently, IoT applications had one major problem which is the security of applications because of their rapid growth, heterogeneities of devices, and complex nature. Security is a big concern and needs to tackle in the network because of its nature.

Recent Biometric technology is based on face recognition and image processing concepts. The biometric research field has not only become common in computer vision, but it is also become popular in neuroscientists and psychologists due to its secure nature. (Balla & Jadhao, 2020) The biometric credentials enable users to use users' physical traits like the face, retina, eyes, nose, fingers, voice and gait, etc. instead of PINs or passwords as accessing any critical IoT systems or a database. The Biometric approach is based on the perception of replacing "one thing you have with you" with "who you are," which has been realized as a safer paradigm to preserve private information. (Ferrag et al., 2019) Biometric identification and authentications are applied in the sectors where security is the main concern like a residential area, airports, banks lockers, ATM, air frontier and crossing the borders, etc.

Face recognition system has been used in different small-scale applications to identify the face from the captured image or group of images. In this paper, the idea behind developing an IoT application with a face recognition concept that recognizes only trained data that are stored in the database. Through this recognition IoT system, only authorized users can enter or access any sovereign information and prevent any fraud or crimes remotely. This system used the K-nearest neighbor and Support Vector Machine classification algorithm to recognize the face from the captured images and extract the features of the faces. The main contribution of this system is to recognize the faces from the trained database and categorized the recognized database based on different parameters like odd coming time, covering faces, etc. for securing and preventing criminal activities through the IoT system.

This paper is systemized as follows. Section2 explains previous work review on the IoT and face recognition in ML, Section 3 discusses some preliminaries related to the IoT and Face Recognitions algorithms KNN, SVM, LBPH. Section4 discusses the research gaps; section 5 defines the problem statements related to the data analysis of IoT with face recognition. Section6 proposed the ML-based face recognition methodology of the problem and the section7 evaluate the result and comparison analysis of the proposed solution. Section 8 discussed some future work and section9 gives a conclusion of the overall research work.