Chapter 6

EarLocalizer: A Deep-Learning-Based Ear Localization Model for Side Face Images in the Wild

Aman Kamboj
National Institute of Technology, India

Rajneesh Rani
National Institute of Technology, India

Aditya Nigam
Indian Institute of Technology, India

ABSTRACT

With much concern over security, it has become essential to maintain the identity and track of an individual’s activities in the modern healthcare sector. Although there are biometric authentication systems based on different modalities, recognition of a person using the ear has gained much attention as ears are unique. Ear localization is a first step for ear-based biometric authentication systems, and this needs to be accurate, since it plays a crucial role in the overall performance of the system. The localization of ear in the side face images captured in the wild possess great challenges due to varying angles, light, scale, background clutter, blur and occlusion, etc. In this chapter, the authors have proposed EarLocalizer model to localize the ear, which is inspired by Faster-RCNN. The model is evaluated on two wild ear databases, UBEAR-II and USTB-III, and has achieved an accuracy of 95% and 99.08%, respectively, at IOU (Intersection over Union) = 0.5. The results of the proposed model signify that the model is invariant to the environmental conditions.

DOI: 10.4018/978-1-5225-7525-2.ch006
INTRODUCTION

The traditional patient tagging system in hospitals are not error-free as there are chances of wrong patient tagging and the mismatch between hospitals records and actual patient tag. This leads to the improper identification, wrong medicine given to the wrong patient, and wrong blood transfusion, which leads to many incidents where patients have lost their lives. Although, the hospitals are migrating for electronic health records (EHR), but it raises privacy concern to medical data theft as the information is accessible online to the healthcare professional, and a fraudulent can misuse the information and may corrupt the data. However, In the last decade, it has been observed that there is a rapid growth in the development of the biometric for the healthcare industry is mainly to combat fraud and to improve patient privacy and safety. As per the research firm Visiongain (Cidon, 2018) and a report (“Boom in healthcare biometric market,” 2018), it has been estimated that this growth will increase over 300% in the next 5 years. The Grand View research has also predicted that growth in the global market will reach up to $14.5bn by 2025 and highlighted the main contributors as BIO-Key, NEC, Fujistu, IRIS ID etc. So, this trillion-dollar industry is always under the threat of malicious attack and from people with wrong intent. Although, the Health Insurance Portability and Accountability Act of 1996 HIPPA act (Gold, 2013) has imposed new rules for patient privacy and safety and it leads to all the healthcare facilities to be as per compliance of new rules and regulations and encouraged healthcare sector to utilize biometric technologies at larger scale. To keep the hospital premises safe and to deliver an error-free treatment to the patient, it becomes very crucial and important to maintain the identity of an individual patient and working staff in the hospital. Although there are smart cards being used to know the identity of an individual, but there are chances that the items under possession like token and smart card may be lost or stolen. Knowledge-based methods like pin and password are also being used to provide secure access, but there are chances that the secret information may be shared, or the person may forget. Replacing smart card and knowledge-based methods with the biometric of an individual brings a lot of advantages as they cannot be lost or stolen or shared. Moreover, it is hard to spoof an individual’s biometrics, as they are unique, and the information is always carried by the person.

An Overview of Biometric Traits

Biometrics traits (Li & Jain, 2009) of an individual are broadly classified into two categories based on physiological such as the face, fingerprints, iris, palmprint, knuckle print, ear etc. and behavioral such as voice, gait, and signature as shown in Figure 1.

(R & G, 2011), (Jaswal, Nigam, & Nath, 2017) discussed various issues and challenges of each biometric traits as follows:

- **Face**: It is one of the most common and well known biometric trait. The face is a non-intrusive biometric as images can be captured at distance or extracted from video frames without any user co-operation.
  - **Challenges**: Face changes with age and is affected by the expression, eyeglasses, cosmetics and it also raises privacy concern in the medical field, identical twins have the same face, so it violates the property of uniqueness.