Chapter 7
Audio Visual System for Large Scale People Authentication and Recognition over Internet Protocol (IP)

Sue Inn Ch'ng
Nottingham University Malaysia Campus, Malaysia

Kah Phooi Seng
Sunway University, Malaysia

Li-Minn Ang
Nottingham University Malaysia Campus, Malaysia

Fong Tien Ong
Nottingham University Malaysia Campus, Malaysia

ABSTRACT

Biometrics is a promising and viable solution to enhance information security systems compared to passwords. However, there are still several issues regarding large-scale deployment of biometrics in real-world situations that need to be resolved before biometrics can be incorporated together. One of these issues is the occurrence of high training time while enrolling a large amount of people into the system. Hence, in this chapter, the authors present the training architecture for an audio visual system for large scale people recognition over internet protocol. In the proposed architecture, a selection criteria divider unit is used to decompose the large scale people or population into smaller groups whereby each group is trained subsequently. As the input dimensions of each group is reduced compared to the original data size, the proposed structure greatly reduces the overall training time required. To combine the scores from all groups, a two-level fusion based on weighted sum rule and max rule is also proposed in this chapter. The implementation results of the proposed system show a great reduction in training time compared to a similar system trained by conventional means without any compromise on the performance of the system. In addition to the proposal of a scalable training architecture for large-scale people recognition based on audio visual data, a literature review of available audio visual speaker recognition systems and large-scale population training architectures are also presented in this chapter.

DOI: 10.4018/978-1-61350-507-6.ch007

INTRODUCTION

Information security means protecting information and information systems from unauthorized access, usage, disclosure, disruption, modification or destruction. In the area of networked and distributed information sharing environments where prevention of unauthorized access is crucial, information security has become an important research issue. This is because finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure itself is a challenging topic. One way to protect information or information system is by ensuring that only authorized people or users are able to access it. In a generic information security system, the user authentication method used is a possession-based cryptographic method whereby the authentic user is required to "possess" the knowledge of the cryptographic key (password) in order to establish the authenticity of the user. However, the possession-based cryptographic method is insecure when too short a password is used whereas expensive to maintain when too complex passwords are used. Furthermore, in a multiuser account scenario, passwords are unable to provide non-repudiation in which case, it is difficult to ascertain the actual user when the password is divulged to a friend (Jain, Ross, & Pankanti, 2006). The limitations associated with the use of passwords can be mitigated by the incorporation of an alternative and more reliable method. A promising alternative is that of biometrics in which the biological traits of a person is used as the authentication factor.

Biometrics are automated methods of identifying a person or verifying the identity of a person based on their physiological or behavioural characteristics. Behavioural characteristics are traits that are learned or acquired whereas physiological characteristics refer to physical traits of a person (Bolle, 2004). As these characteristics are unique and differ between individuals, thus, it can be used as a form of identity access management and access control. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of commonly used behavioural characteristics. Examples of physiological characteristics used include hand or finger images, facial characteristics, and iris recognition. There are two types of functionalities of biometrics namely authentication and identification. Authentication (also called verification) is the act of verifying a claim of identity. In short, if you stand in front of an authentication system and claim to be a certain user, the system will only check if you are who you claim to be. On the other hand, identification (or recognition) is an assertion of who someone is. In this case, the decision of the recognition system will be made so as to identify the identity of the user. Hence, this makes biometrics an important emerging technology to counter security threats in the growing electronically connected world especially in applications for information systems, e-commerce, tele-health and internet applications. Nonetheless, biometric technology that relies only on a single biometric trait may not be able to meet market requirements. Multi-biometric systems (biometric systems that integrate two or more biometric traits for identity verification) have several advantages over single-biometric systems. First, multi-biometric systems can address the problem of non-universality, since multiple traits would ensure sufficient coverage even for a large-scale population (Ross & Poh, Multibiometric Systems: Overview, Case Studies and Open Issues, 2009). Secondly, multi-biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple traits of a legitimate user (Hong, Jain, & Pankanti, October 1999). However, simple integration of two or more biometric traits is insufficient. The development of cutting-edge technology that can produce new discoveries and intellectual properties for biometrics security is highly desirable.

A rapidly developing area with high potential for biometric technology is in the banking and financial sector where biometric technology can be