Chapter 8

Imed Bouchrika
University of Souk Ahras, Algeria

ABSTRACT
As surveillance becomes ubiquitous in such modern society due to the immense increase of crimes and the rise of terrorism activities, various government and military funded projects are devoted to research institutions to work on improving surveillance technology for the safety of their citizens. Because of the rapid growth of security cameras and impossibility of manpower to supervise them, the integration of biometric technologies into surveillance systems would be a critical factor for the automation of identity tracking over distributed cameras with disjoint views i.e. Re-Identification. The interest of using gait biometrics to re-identify people over networks of cameras emerges from the fact that the gait pattern can be captured and perceived at a distance as well as its non-invasive and less-intrusive nature.

INTRODUCTION
Although personal privacy has emerged as a major concern for the deployment of large scale surveillance systems, research into automated visual surveillance has received remarkable interest within the computer vision community with potential integration of biometric technologies and human activity recognition systems. This is mainly due to the proliferating number of crimes and terror attacks as well as the vital need to provide safer environment. In fact, the inability of human operators to monitor the increasingly growing numbers of CCTVs installed in highly sensitive and populated areas such as government buildings, airports or shopping malls, has rendered the usability of such systems to be useless. According to the British Security Industry Association, the number of surveillance cameras deployed in the UK was estimated to be more than 5 million in 2015; this figure is expected to increase rapidly particularly after the terrorist attacks that London witnessed in July 2005. Despite the huge increase of monitoring systems, the question whether current surveillance systems work as a deterrent to crime is
still questionable. Security systems should not only be able to predict when a crime is about to happen but, more importantly, by early recognition of suspicious individuals who may pose security threats via the use of biometrics, the system would be able to deter future crimes as it is a significant requirement to identify the perpetrator of a crime as soon as possible in order to prevent further offences and to allow justice to be administered. The process of tracking people from one place to another place using surveillance networked cameras would be crucial for gathering valuable security intelligence. Moreover, queries can be made to search for possible locations of a given suspect that can indeed help security officers in their investigations and can lead to further evidence. Traditionally, it is impossible for human operators to work simultaneously on different video screens in order to track people of interest as well as analyze their behaviors across different places. Thus, it has become an essential requirement for research scientists from the computer vision community to investigate visual-based alternatives to automate the process for identity tracking over different views in addition to human activity analysis. Recently, various approaches were published in the literature to accomplish this task based on using basic features such as shape or color information. However, their practical deployment in real applications is very limited due to the complex nature of such problem. An alternative solution would be to employ biometric-based systems that can work at a distance and for low-resolution images such as gait and soft-based biometrics.

Biometrics is concerned with extracting and deriving descriptive measurements based on either the human behavioral or physiological characteristics which should distinguish a subject uniquely among other people. Such measurements are compared against computer records to either confirm or verify the identity of a person. The term **biometrics** is a composite Greek word of two parts: *bios*, meaning life and *metrics*, referring to the verb “to measure”. Biometric measurements based on the physiological traits include face, ear, fingerprint and DNA whilst the behavioral features include gait, voice and signature. Apart from being unique, the biometric description should be universal and permanent. The universality condition implies that it can be taken from all the population meanwhile the permanence signifies that the biometric signature should stay the same over time. As opposed to traditional identification or verification methods such as passports, passwords or pin numbers, biometrics cannot be transferred, forgotten or stolen and should be ideally obtained non-intrusively. Even though, people intuitively use some body characteristics such as face, gait or voice to recognize each other, it is proven a challenging task to extract and quantify such measurements into a biometric signature. Biometrics can work either in verification or identification mode. For verification, the system performs a one-to-one match for the newly acquired person signature against a pre-recorded signature in the database to verify the claimed identity. For identification mode, a one-to-many matching process is conducted against all people already enrolled in the database to infer the subject identity. Biometrics is now emerging in regular use being deployed in various applications such immigration border control, forensic systems and payment authentication. The choice of a specific biometric modality depends on the nature and requirements of the intended applications in addition to the availability of biometric features. Fingerprints, face and iris are among the most popular physiological traits used in commercial biometric systems with fingerprint capturing over 50% of the market share (Jain & Kumar, 2012). Biometric systems are sold mainly for the following purposes: physical access control, logging attendance and personal identification purposes.

It is no doubt that physiological-based biometric modalities enjoy higher recognition rates however their deployment in surveillance systems is not usually a favored option. In contrast, the suitability of gait recognition for surveillance applications emerges from the fact that the gait pattern can be perceived at distance from the camera even with poor resolution as opposed to other biometric traits where their performance deteriorates severely. Furthermore, the strength of gait recognition is its non-invasiveness