Fingerprint Biometric based Access Control and Classroom Attendance Management System

Yash Mittal[1], *Aishwary Varshney*[2], *Prachi Aggarwal*[3], *Kapil Matani*[4] and *V. K. Mittal*[5]
Jaypee University of Information Technology, Solan[1]; *LNM Institute of Information Technology, Jaipur*[2,3,4];
Indian Institute of Information Technology Chittoor, Sri City[5]
yashmittal@hotmail.co.in[1], *y13uc195@lnmiit.ac.in*[2], *y13uc132@lnmiit.ac.in*[3], *y13uc015@lnmiit.ac.in*[4],
vkmittal@iiits.in[5]

***Abstract*—Fingerprint is a reliable biometric feature having a wide range of applications that require authentication. Person-specific verification is needed in many scenarios such as access-control, classroom attendance and financial transactions etc. In this paper, two applications of fingerprint biometric are proposed. An *Access Control System (ACS)* prototype is demonstrated for person-specific door access, using a fingerprinting device. Another prototype of a *Classroom Attendance Management System (CAMS)* is developed that uses fingerprint as biometric feature for classroom attendance. The CAMS consists of modules for database, web-user interface and views at multiple levels of access. Both systems are expected to mitigate the shortcomings of alternative existing systems, and eliminate the possibilities of spoofing or proxy. These systems store fingerprints along with the date/time-stamp for each user. Fingerprints are stored dynamically in a database for computing the different statistics, e.g., month-wise or semester-wise trends in the case of CAMS. The CAMS can also provide a solution to the problem of late-coming. Experiments are conducted for measuring the recognition accuracy, i.e., fingerprint match. The initial results of recognition accuracy at 87% for ACS and 92% for CAMS are encouraging. The proposed systems can be further scaled-up for real-time deployment, in applications such as employee attendance and controlled access to high-security areas etc.**

Keywords: fingerprint biometric, access control system, classroom attendance management system, ACS, CAMS

I. Introduction

With the exponential growth of the digital world, our lives are increasingly becoming dependent on countless digital applications and softwares. In many scenarios, access to these needs to be secure and authenticated, necessitating the creation of multiple user accounts. Each user account needs to secure key details, that must be accessible to only the account holder and to nobody else. Hence, reliable person-verification and authentication mechanisms are increasingly becoming important, also due to associated challenges of impersonation, spoofing, proxy, phishing and information theft etc. Traditional authentication and verification measures have focused on something that *the user knows*, for example passcode or PIN, or something *the user possesses*, for example RFID card. *Biometric Systems* provide the next layer of security by focusing on a few *physical* characteristics of the human body, i.e., *what the user is*, such as fingerprints or eyes' retina.

Biometrics is the umbrella term used for a wide variety of technologies, where uniquely identifiable person-specific attributes are required for the purpose of user identification and authentication. These attributes may be categorised as: (i) *physiological* such as fingerprint, iris print, face recognition, voice recognition etc., or (ii) *behavioural* such as signature, handwriting, typing pattern, emotional cues and paralinguistic cues etc. [1]. These attributes help to *verify the identity* of users seeking access to *places* such as buildings, rooms, doors, lockers, file-cabinets etc., or to computer *systems* such as desktops, phones, tablets etc. Thus, person-authentication using biometric verification is becoming increasingly common in corporate/public security systems, consumer electronics and payment applications, needing security. Another key-factor of growing applications of biometric verification is operational convenience. Hence, these systems can be used at a wide range of locations such as airports, secured labs, hotels, offices, schools, colleges etc. Biometrics is being used in the government issued identification cards in several countries, namely, India, Australia, Hong Kong and Malaysia. Few airports in Australia also use face recognition technology for immigration purposes [2].

The most commonly used biometric technology currently is the *fingerprint recognition*, which involves imaging of the fingerprints. Fingerprint recognition is extensively used for official governmental purposes wherein unique identification needs to be provided to each citizen, for example, *Aadhaar* ID cards provided by the 'Unique Identification Authority of India' (UIDAI) [3]. This may be required for passport, social security or voting purposes in India. Fingerprint recognition is also used for high security purposes, e.g., in banks, military locations, research facilities, where access needs to be restricted to only a few select individuals. Personalized-use of fingerprint recognition is possible by using standalone fingerprint scanners fixed in offices and high-end laptops. Recently, the fingerprinting is also extended to smartphones and tablets, by placing a small fingerprint scanner in the device body itself. Though fingerprint recognition saves time by automating the process of identity verification, it is still not very common due to high installation costs. To further promote wider applications of the fingerprint recognition technology, some low cost solutions with minimal set-up time need to be developed.

[978-1-4673-6540-6/15/$31.00 ©2015 IEEE]

Fingerprint biometrics is preferred over traditional biometric methods because in this the *person to* be identified is *required to be physically present* at the time of identification. It prevents the risks of *buddy punching*, i.e., unauthorised person attempting access using a valid card or 'fob' to enter a restricted area. Identification based on fingerprint biometric removes the need to remember a password or carry a token or a card. It also eliminates the possibility of theft of cards or fobs, thereby avoiding the expenditure on their constant replacements. Fingerprint biometric options are also cost effective as details of new individuals can be easily added to the system at no extra cost. Whereas in the card-based systems, the organisation will have to issue new cards to all the newcomers. In general, every human being has a unique and unchanging fingerprint, made up of a series of ridges and furrows on the finger surface. These characteristics are used to determine the *uniqueness* of a person-specific fingerprint.

In this paper, two novel applications of fingerprint biometric are proposed, namely, *Access Control System* (ACS) and *Classroom Attendance Management System* (CAMS). Both can be readily used in schools and colleges. The focus is on enabling the use of fingerprint biometrics technology in educational institutions, for identification purposes. First, a fingerprint is registered for each user. Then these image patterns are converted into a digital code using an algorithm. It then effectively becomes a *digital identity* of the concerned person. It is stored in a database, for comparisons needed for authentication and access control. The prototype ACS is generic in nature and can be used in places where person-identification is important, e.g., research labs, examination halls or library. Since fingerprint recognition also provides authentication, it can also be used to make payments such as college fee or for internal facilities, e.g., snacks at a cafe. The prototype CAMS is a state of the art solution for educational institutions needed for maintaining attendance records of students and staff. This CAMS provides the users a view of attendance details subject-wise or date-wise. The administrative staff can also access the attendance details of students, in order to help them identify the defaulters. Using both the proposed systems, the institutes would be easily able to automate the attendance management, exam verification and access control to multiple locations in the campus. Fingerprints can thus become the de facto mechanism for person-identification throughout an institute, and eliminate the need of issuing multiple identification cards for different facilities such as sports, library, mess, etc.

This paper is organised as follows. Section II dicusses the fingerprint biometrics and the technology used for fingerprint matching, in brief. Section III describes the generic *Access Control System* prototype developed. Section IV provides an overview of the *Classroom Attendance Management System* along with design details, modes of operation, control flow, and hardware and software architecture. Experiments conducted to measure the success/failure rates for matching of fingerprints and the results obtained are discussed in Section V. A brief summary is given in Section VI, along with scope of further work in this direction.

II. Fingerprint Biometrics

Fingerprints for identification and recognition purposes have been in use since a long time. Thumb prints using ink is one of the oldest application of biometrics. There are multiple reasons for fingerprints becoming common as biometric feature. First, the fingerprint recognition provides a reliable form of biometric security even when a person ages, whereas the iris and facial recognition are affected by ageing related feature changes. Second, fingerprint recognition is not affected much by change in appearance, whereas iris recognition needs a person to remove lenses or glasses. Third, fingerprint scanners can successfully identify a registered fingerprint even with certain amount of unwanted substance present on the skin such as dust, oil, dirt, powder or liquid etc., whereas facial recognition systems are prone to error due to occlusion by person's facial hair.

In order to use *fingerprints as biometric feature*, one needs to understand several features of the fingerprint pattern. It is essential to understand the structure and properties of the human skin, in order to employ some image processing methods to observe the unique characteristics in these patterns. These unique characteristics are: (a) *ridges* and (b) *minutia* points. (a) The fingerprint *ridges* have three basic patterns: (i) loop, (ii) whorl and (iii) arch, which constitute 65-60%, 30-35% and 5% of all fingerprints, respectively [4]. A normal fingerprint pattern is made up of *lines* and *spaces*. These lines are called *ridges*, and the spaces between the ridges are called *valleys*. (b) The unique fingerprint traits are termed as *minutiae*. The *major minutiae features* of fingerprint ridges are: (i) ridge ending, (ii) bifurcation and (iii) short ridge (or dot). It is through the pattern of these ridges and valleys, that a unique fingerprint is matched for authentication purposes. Although family members may share same general fingerprint characteristics, but these are still unique to every human being, thereby minimising the possibility of duplicity.

There are *five stages* in a *finger-scan verification and identification*: (i) fingerprint image *acquisition*, (ii) image *processing*, (iii) *locating* the distinctive characteristics, (iv) *template* creation and (v) template *matching* [5]. These five stages are generally performed by a fingerprint sensor device and accompanying software using image processing techniques and image matching approaches. A *fingerprint sensor* is an electronic device that captures a digital image of the fingerprint pattern, using any one of the fingerprint capturing technologies, that could be optical, capacitive or Radio Frequency (RF) based. The captured image is called a *live scan*. This *live scan* is then digitally processed by extracting features from the fingerprint, in order to create a biometric template which is then stored in binary format for fingerprint based matching further [6].

Fingerprint recognition generally refers to the automated method of verifying a similarity match between two human fingerprints. Biometric devices such as finger scanners consist of three parts: (a) A reader or scanning *device*, (b) A *database*