MECHATRONICS BOOK SERIES

CONTROL AND INTELLIGENT SYSTEMS

Momoh Jimoh E. Salami
Abiodun Musa Aibinu
Yasir Mohd Mustafah

IIUM Press
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

MECHATRONICS BOOK SERIES

CONTROL AND INTELLIGENT SYSTEMS

EDITOR

Momoh Jimoh E. Salami

Abiodun Musa Aibinu

Yasir Mohd Mustafah

IIUM Press

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Momoh Jimoh E. Salami, Abiodun Musa Aibinu, Yasir Mohd Mustafah: Mechatronics Book Series: Control and Intelligent Systems
Bibliography p.
Includes Index
ISBN

ISBN: 978-967-418-176-5

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN.BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan
Tel: +603-6188 1542 / 44 / 45 Fax: +603-6188 1543
EMAIL: iiumprinting@yahoo.com

Table of Content

Chapter 26
Development of Palmprint based Biometric System

M. A. Rotinwa-Akinbile, A.M. Aibinu and M. J. E. Salami

Department of Mechatronics Engineering,
International Islamic University Malaysia (IIUM)
P O Box 10, 50728, Gombak, Malaysia.
E-mail: maibinu@iium.edu.my

26.1 Introduction

Conventional access control devices include keys (conventional or electronic), Radio Frequency Identification- RFID devices (smartcards or tags) and the use of password or PIN for system protection. The use of keys or RFID tags is uneconomical due to the procurement cost of the device per each legitimate user. On the other hand, password and PIN are unsafe because they can be hacked by impostors or easily forgotten (Wu, Ng, Chan, Ding, Jing and Yeung, 2010). Also, these devices can be shared amongst non-authorized users and most importantly they are non-degradable thus resulting in environmental pollution. Consequent upon the low fidelity of these devices, access control and system security has experienced a paradigm shift from the use of conventional devices to biometrics based computational intelligent techniques such as fingerprint, iris, palmprint, face and voice recognition (Poinstot, Yang and Paindavoine, 2009; Wu et al., 2010).

Biometrics is the science of automated recognition of individuals through the use of any human physiological (anatomical) or/and behavioural features (traits)(Clarke 1994). This technique of physiological/ behavioural recognition of individuals has been in existence over a century but was the exclusive preserve of the law enforcement agencies for the management of crime database and profiling of crime suspects(Busch 2006). However, in the last two decades, it has been deployed for diverse civilian application such as access control (Wu et al., 2010; Bryliuk and Starovoitov, 2002), system security (Rahaman and Bhattacharya, 2003), E-security (Ali and Hassanien, 2003), smart homes (Garg, Shriram, Gupta and Agrawal, 2009). Similarly, a recent report (France-Presse, 2011) shows the interest of the Government of countries in the adoption of this technology to manage the activities of foreign workers. Thus, biometrics is increasingly becoming attractive in access control and system protection and consequently, there are greater development towards enhancing the fidelity and system integrity of the device for optimal performance.

Biometric features are generically classified into physiological and behavioural features. Physiological biometrics is concerned with the measurement of physical characteristics of the human body such as face geometry, fingerprints, hand geometry amongst others while behavioural biometrics considers the analysis of actions carried out by individuals such as in voice, keystroke dynamics, signature etc(Clarke 1994). A general illustration of biometrics classification is presented in Figure 26.1. In the contemporary biometric system environment, no single biometric feature has universal and superior fidelity than the other (Jain, Ross and Prabhakar, 2004); rather the selection of a paticular biometric feature is dependent on its intended application and other feature requirements such as: universality, distinctiveness, stability, public acceptability and collectability.

Biometric systems are basically automated pattern recognition systems that verify a user's identity by establishing the validity of the specified physiological or behavioral characteristics. The emergence of various biometric systems over the years was due to the complexity of the human physiology and dynamic behavioural features coupled with