SMARTEYE - VEHICLE SECURITY SYSTEM
USING FACIAL RECOGNITION

ALFRED RITIKOS

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

MAY 2007

DEDICATION

To my beloved wife, Phoay Eng, and sons, Ephraim and Keane.

ACKNOWLEDGEMENT

I would like to acknowledge my gratitude and appreciation to my project supervisor, Professor Dr. Ruzairi bin Hj. Abdul Rahim, for his guidance, advice and friendship throughout the period of carrying out this project as well as throughout this course, and also to Prof. Madya Dr. Syed Abdul Rahman bin Syed Abu Bakar for his assistance in providing specialist advice in the area of image processing.

Furthermore, some of my workplace colleagues have been kind to provide their face images to be captured for the needed database.

Finally, my gratitude is extended to my fellow students who have provided much encouragement and support.

ABSTRACT

Facial recognition has gained increasing interest in the recent decade. Over the years there have been several techniques being developed to achieve high success rate of accuracy in the identification and verification of individuals for authentication in security systems. This project experiments the concept of combining of multilevel wavelet decomposition transformation and neural network for facial recognition in a specific application with its own limitations, in that of vehicle security access control system. The approach of this project is to conceptualise by simulation of the various processes involved in developing an implementable system.

Keywords: Facial Recognition, Facial Verification, Image Extraction, Image Processing, Principal Component Analysis, Edge Detection, Wavelet Transformation, Neural Network

ABSTRAK

Dalam masa singkat kebelakangan ini pengenalan muka (facial recognition) telah banyak menerima tumpuan. Beberapa teknik atau cara telah dikaji dan dibangunkan untuk mencapai tahap ketepatan dengan kadar kejayaan yang tinggi dalam usaha mengenalpasti seseorang individu untuk diberi kebenaran laluan dalam sistem-sistem keselamatan. Projek ini telah menyelidiki penggabungan konsep multilevel wavelet decomposition transformation dan neural network untuk Facial Recognition dalam penggunaan yang tertentu yang mempunyai had-hadnya tersendiri, iaitu system kawalan keselamatan kenderaan. Projek ini tertumpu kepada membuktikan konsep tersebut dengan cara simulasi berbagai proses aturcara yang terlibat dalam sesuatu system yang boleh direka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2D	-	Two-dimension
3D	-	Three-dimension
AAM	-	Active Appearance Model
ANN (NN)	-	Artificial Neural Network (Neural Network)
CWT	-	Continuous Wavelet Transform
DWT	-	Discreet wavelet Transform
EBGM	-	Elastic Bunch Graph Matching
FERET	-	Face Recognition Technology
FFT	-	Fast Fourier Transform
FPGA	-	Field-Programmable Gate Array
FR	-	Facial (or Face) Recognition
HMM	-	Hidden Markov Model
ICA	-	Independent Component Analysis
ID Card	-	Identity Card
KLT	-	Karhunen-Loeve Transform
LDA	-	Linear Discriminant Analysis
PCA	-	Principal Components Analysis
PIN	-	Personal Identification Number
ROI	-	Range of Interest

LIST OF SYMBOLS

$c(x,y)$	-	correlation
D_j	-	Euclidean distance
$\gamma(x,y)$	-	correlation coefficient
m_j		mean vector of patterns
N_j		number of pattern vectors
ω_j		pattern class
x_j		unknown pattern vector

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Biometrics for Identification and Verification

Biometrics is an emerging set of pattern-recognition technologies which accurately and automatically identifies or verifies individuals based upon each person’s unique physical or behavioural characteristics. Identification using biometrics has advantages over traditional methods involving ID Cards (tokens) or PIN numbers (passwords) in that the person to be identified is required to be physically present where identification is required and there is no need for remembering a password or carrying a token. PINs or passwords may be forgotten, and tokens like passports and driver's licenses may be forged, stolen, or lost.

Biometrics methods work by unobtrusively matching patterns of live individuals in real-time against enrolled records. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. Because of these inherent attributes, biometrics is an effective means to secure privacy and deter identity theft.

Various biometric traits are being used for real-time recognition, the most popular being face, iris and fingerprint. Other biometric systems which have found their usefulness are based on retinal scan, voice, signature and hand geometry. By using them together with existing tokens, passwords and keys, biometric systems are being deployed to enhance security and reduce fraud.

In designing a practical biometric system, a user must first be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to him. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in verification (authentication) or identification mode.

1.2 Verification vs. Identification

There are two different ways to recognize a person: verification and identification. Verification (answers the question "Am I who I claim I am?") involves confirming or denying a person's claimed identity. In identification, the system has to recognize a person (addressing the question "Who am I?") from a list of *N* users in the template database. Identification is a more challenging problem because it involves 1:N matching compared to 1:1 matching for verification.

1.3 Incentives for Facial Recognition Application in Vehicle Security

Research on automatic face recognition in images has rapidly developed into several inter-related lines, and this research has both lead to and been driven by a disparate and expanding set of commercial applications. The large number of research activities is evident in the growing number of scientific communications published on subjects related to face processing and recognition.

Anti-theft devices are not foolproof, but they can a deterrent or to slow down the process. The longer it takes to steal a car, the more attention the thief attracts, and the more likely the thief will look elsewhere. Anti-theft devices include those listed below:

- Fuel Shut Off This blocks gasoline flow until a hidden switch is tripped. The vehicle can only be driven a short distance, until the fuel already in the carburetor is used up.
- Kill Switch The vehicle will not start unless a hidden switch is activated. The switch prevents electrical current from reaching the coil or carburetor. Check your vehicle warranty before installing a “kill switch.”
- Time Delay Switch The driver must turn the ignition key from “on” to “start” after a precise, preset interval or the engine won’t turn over.
- Armored Ignition Cutoff A second tamper proof lock must be operated in order to start the car. “Hot wiring” (staring a car without a key) is very difficult with this device, so it is especially effective against amateurs.
- Hood Locks These make it difficult to get to the battery, engine, or vehicle security system.
- Time Delay Fuse Unless a concealed switch is turned off, starting the vehicle causes a sensitive fuse to burn out, cutting out power and stopping the motor.
- Armoured Collar A metal shield that locks around the steering column and covers the ignition, the starter rods and the steering wheel interlock rod.
- Crook Lock A long metal bar with a hook on each end to lock the steering wheel to the brake pedal.
- Audible Alarm These alarm systems are positioned in the engine

Systems	to set off a buzzer, bell or siren if an attempt is made to tamper with the hood, bypass the ignition system, or move the vehicle without starting the engine.

To illustrate the “evolution” of typical vehicle security system over the recent years, here is an example of development of such products from a particular brand[1] of cars:-

1995 passive security system (no remote); the system is armed by locking the doors with or without the key; windows could be open and the system would arm

1996 remote by coded alarm; unlocks all doors with one push

1997 remote by coded alarm changed to unlock only the driver's door with one push

1999 keyless remote

2003 remote buttons coloured; a 'chirp' replaces the audible honk

2005 remote fobs and immobilizer keys with remote entry as before

2006 remotes with recessed buttons which are harder to accidentally press on

2007 remote-start system

Keyless entry is becoming a standard feature in vehicles that have installed alarm systems. A small battery operated device (fob or “remote”) hangs on the key chain and features one or more buttons for arming and disarming the alarm. The button operates the door locks as well. When one approaches the car, a press of the button will not only disarm the alarm, but unlock the driver's door, making it unnecessary to use a key. Hence, it allows keyless entry.

In a biometric vehicle security system, the objective is to authenticate a user being an authorised person to have access to the ignition system. It could be a first step before ignition could commence or it could be an integrated system for auto-ignition subsequent to authorisation being cleared.

A progression from the now common keyless fob used to open a vehicle, there is a recent successful commercial implementation of biometric for authorisation, in the form of fingerprint recognition. This, however, does have its own weaknesses, such as the one depicted by a report by BBC News[2] on 31 March 2005 of a local robbery incident where the owner's finger was sliced off the end of his index finger with a machete.

Potential applications of biometrics in vehicle security are for private vehicles and especially for commercial vehicle fleet, such as rented cars, taxis, transportation lorries and public buses.

One of the most effective ways to optimise use of vehicles is to allow drivers to use vehicles from a motor pool. A "fleet management system" is an optimization tool aimed at making it very easy to manage vehicles in a motor pool. There is little need to look through paper records to see if someone is eligible to drive, or to check if he has received the proper training for that vehicle, or if someone's driver's license expired since she last used a vehicle.

Electronic key manufacturers for fleet management companies make intelligent fobs which automatically record the transaction activity by date and time both on the key cabinet and on the support software. This electronic key security makes users accountable for the keys, reducing management risk and improving efficiency. One such product for commercial fleet vehicles is available from Traka, Inc.[3]

Figure 1.1: An intelligent car fob for a fleet management system

Their iFob is inserted into receptor sockets, adjacent to the door or equipment which, check the permissions on the iFob. If acceptable, the Immobilisor will release a door magnetic lock or solenoid and the door will open. The iFob will record the access event as well as the time which it accumulates until returned to the Traka cabinet at the end of the shift, when the events are downloaded. If a user attempts to use the iFob outside its period of validity, the iFob will no longer activate the Immobilisor. The iFob contains a chip with a guaranteed unique serial number, giving every one an individual ID. The special shape of the iFob allows it to automatically lock into the Traka cabinet and its smooth surface is inherently self cleaning eliminating problems associated with dust or other contaminations. Where keys need to be managed, they are attached using special self locking security seals, so that they cannot be easily detached.

Being physically detached from the user, such a sophisticated device and system are still subject to loss and misuse. Although each fob is assigned a serial number and assigned to an individual person, there is no guarantee that another person will not use it for access to the vehicle.

Because of its many advantages, biometrics is fast being used for physical access control, computer log-in, welfare disbursement, international border crossing (e-Passports) and national ID cards, verification of customers during transactions conducted via telephone and Internet (e-Commerce and e-Banking). In automobiles, biometrics is being adopted to replace keys for keyless entry and keyless ignition. Here are some commercially available products for such vehicle access and starting applications:-

Product name[4]	Biometrics method
Identisafe-09	Fingerprint
Retinasafe-18	Eyeball Recognition
Brainsafe-72	Brain fingerprinting
Voicesafe-36	Voice
Think-Start-99	Brain waves

There is much interest in using FR for security systems due to it advantages for the above listed methods. These will be explained in the next chapter.

Among some advantages of Facial Recognition method for vehicle security application are:-

(i) more convenient, no active part of user; sensed as soon as one is seated in position (and facing the camera)

(ii) low risk scenario (failure means loss of one vehicle, compared to loss to company properties & confidential materials, national security and safety)

(iii) a “better” alternative to existing methods. (What is the chance of a thief cutting the owner’s/ authorised persons’ face or head (!) to steal the vehicle; compare to his finger – as has happened to a driver?)

Some practical questions that need to be answered include:-

(i) Is biometric really practical for this application? Even with fingerprint method, do we not need a key to lock and open our vehicle doors?

(ii) Is there a method which is fully foolproof? Hacking/bypassing the system is undeniable.