DESIGN OF A RFID BASED VEHICLE ENTRY SYSTEM WITH BIOMETRICS

Vijay Vaidyanathan, Chaney Edwards, Lee Self and Lonnie Langle
University of North Texas
Denton, TX 76207

Abstract

The paper presents a senior design project that was conceptualized, designed and implemented by seniors at the University of North Texas. The vehicle entry system designed in this project, addresses the issue of vehicle security by requiring two separate authentications before granting access to the vehicle. The first of these uses RFID and requires the user to have an authenticated RFID transponder, or "tag", in possession when trying to enter the vehicle. The second authentication is biometric in nature and uses a verification of the individual's fingerprint. Once these two conditions are met, the system activates the door's automatic lock. For added flexibility, a bypass switch was put in place, to require only RFID authentication for access. A Motorola M68HC12 micro-controller was used to provide control over the system. The processor receives inputs from both authentication processes as well as the bypass switch. Based on the existing condition, the M68HC12 code will check for proper states before granting access to the vehicle. The vehicle entry system presented in this paper offers high-level security with flexibility for customization.

Introduction

The University of North Texas at Denton is the third largest, single-campus university in Texas. The Department of Engineering Technology is one of the founding departments of the newly established College of Engineering. The department is ABET accredited and is one of 25 in the nation that offer undergraduate and graduate programs in Engineering Technology. The senior design projects class serves as the setting for the final, capstone project. Students work in teams (of 4 or 5 students) to propose, design, implement and successfully demonstrate the working of their project. Final presentations are made to an audience comprising faculty members and invited industry personnel from the area (numbering 20-25). Students are graded individually and in teams for technical content, demonstration and presentation skills. This paper is a senior design project conceptualized, designed and implemented by seniors in the Electronics Engineering Technology Program over a period of one semester.

In the world that we inhabit, the automobile is an expensive necessity. A person's car is one of the most prized possessions. It is more than just basic transportation; some people view it as an extension of their personality and a valued member of the family. Moreover, criminals use stolen cars to commit other crimes and the police need to follow up on the theft and subsequent consequences, sometimes result in impounding the vehicle. Stolen cars also raise insurance rates for all drivers and cause automobile manufacturers and owners to add anti-theft devices making car ownership more expensive [1].

Here are some disturbing facts:

- More than a million cars are reported stolen in the United States every year [2].
- In the United States, another car is stolen every 25.3 seconds [2].
- Trafficking stolen cars is the second-most profitable criminal activity next to drug dealing [2].
- Only fourteen percent of stolen cars are cleared by arrests each year [2].

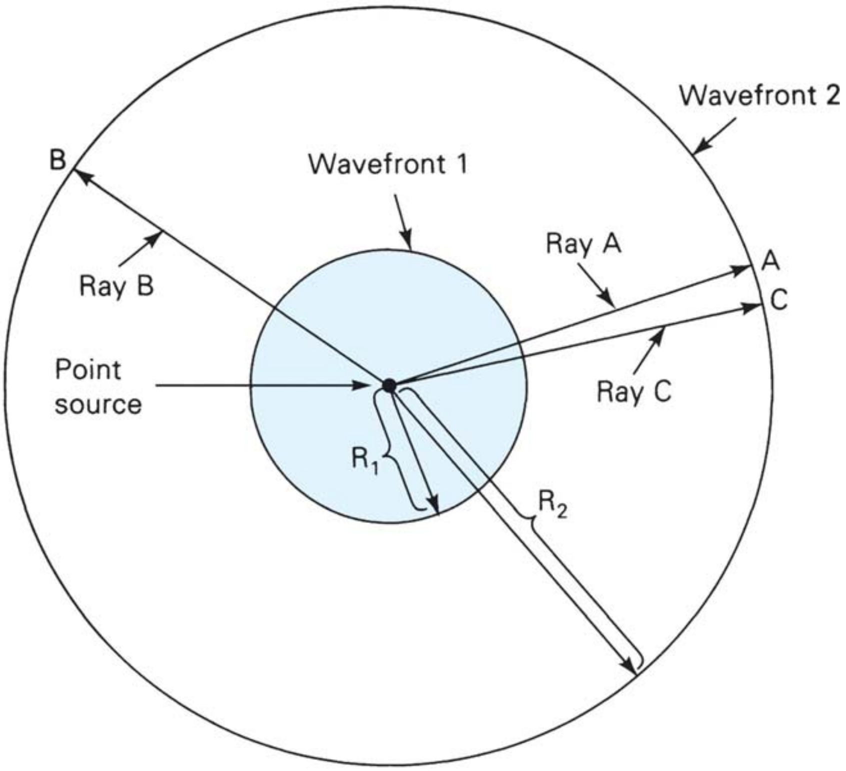
Automobile manufacturers and automobile owners have been installing more sophisticated antitheft devices over the years to protect their vehicles. Designers initially introduced door and trunk locks to deter criminals. However, criminals have found ways to overcome these safety systems. The 1970s saw the advent of car alarms. These systems, however, were prone to malfunction and bystanders grew to ignore the "warning" signals generated by alarms – soon regarding them as an irritating nuisance.

Radio Frequency Identification (RFID) has now emerged as the most advanced and commercially promising type of real world awareness technology [3]. In its basic form, RFID enables identification of individual items, distinguishing them from each other and, in turn to track their location and movement. Electromagnetic wave propagation occurs when alternating electric and magnetic fields at 90-degree angles travel in the same direction, feeding each other [4]. An electromagnetic wave may be propagated at just about any frequency, but the length of the antenna determines the propagation of the wave at a given frequency [4]. Radio frequencies can penetrate through metal and other objects. Thus, the user need not be in line of sight with his target. As shown in Figure 1, the RFID tags propagate waves in all directions.

Advanced forms of RFID are now in the market, available at reasonable prices [5].

The RFID tag is essentially a small, self-contained electronic circuit comprising two elements. One element is designed to store digital identification information. The other element is designed to transmit that information to a RFID reader located nearby [5]. Electronically, the tag remains in a 'passive' state until it is subjected to radio waves, at which instant the tag becomes active and transmits a blip of pre-stored data to the reader

Figure 1: Electromagnetic Wave Propagation[4]



that is pointed its way. Passive RFID tags are powered by the energy sent from radio waves to the tag from the reader. Additionally, passive tags have small amounts of memory to store an ID number and an antenna to receive radio waves. The logic on the tag responds to instruction sent to the reader about the information to be sent back. A combination of RFID tag and receiver can be used for a variety of applications ranging from health care to secured access to vehicles and facilities.

Recently, Texas Instruments (TI) announced its new 3D Analog Front End IC, a low frequency RF chip that simplifies vehicle access design while providing cost, time, power and board space savings [6]. Texas Instruments' new chip is a primary component of a keyless access solution and requires no action from the user to gain entry to their vehicle [6]. RFID access control systems have been developed to provide independent, non-stop systems for security, parking and access control [7]. Recently, Federal Express has used wristband RFID transponders to provide hands-free vehicle access and security to 1100 FedEX delivery vehicles [8]. The keyless entry system uses RFID transponders and readers mounted at each of the doors to the delivery vehicle. When the transponder is placed within 6 inches of the reader, the transponder's code is compared to those in the system's memory and if a match is detected, the door unlocks for 5 seconds [8]. In all these applications, keyless entry is the desired option. However, keyless entry needs to be enhanced with security for wider acceptance.

In this paper, an automobile access system that incorporates RFID and biometrics is presented. Biometrics is a statistical measurement of biological phenomena or traits [5]. Biometrics equipment is generally used to create an electronic template, and to store and access such template for access authorization. It was decided to incorporate fingerprint scanning as a biometric measure in this project for the following reasons:

- Each fingerprint is unique.
- Duplicating fingerprints is not a trivial task. It is tedious and requires the use of precise tools.
- Fingerprint scanning is not as intrusive as other means of biometric verification, like retinal scanning.

The use of fingerprint scanning will personalize vehicle ownership and limit access to only those the owner adds to the fingerprint and RFID transponder databases. The scenario envisaged for potential use of the proposed design was: The driver will carry an RFID tag on his/her person that will enable the first half of the door unlocking sequence when in range of the RFID reader antenna. Then, the driver will swipe his/her fingertip on a door-mounted reader to trigger the other half of the sequence to unlock the door. The uniqueness of fingerprints will significantly increase vehicle security, and the use of thermal fingerprint scanning virtually eliminates the ability to bypass the system using artificial prints. Additionally, the capability to easily enable and disable fingerprints (and RFID tags) within the system's database affords the owner a newly realized flexibility in vehicle access control.

Procedure

Design considerations: Prior to design of the system, its working parameters were identified. The system was designed to meet the following design considerations:

1) The RFID Reader should add and remove at least 4 tags from its look-up table.
2) The system will incorporate a Digital Signal Processor (DSP) board that will add and remove fingerprints from its look-up table.
3) The RFID reader should have a read range from 3 to 6 inches. A short read range is necessary for two reasons. Since the user would need to be close for a fingerprint scan, a short read range would work. Secondly, a short read range corresponds

with both low frequency RFID systems and passive tags.

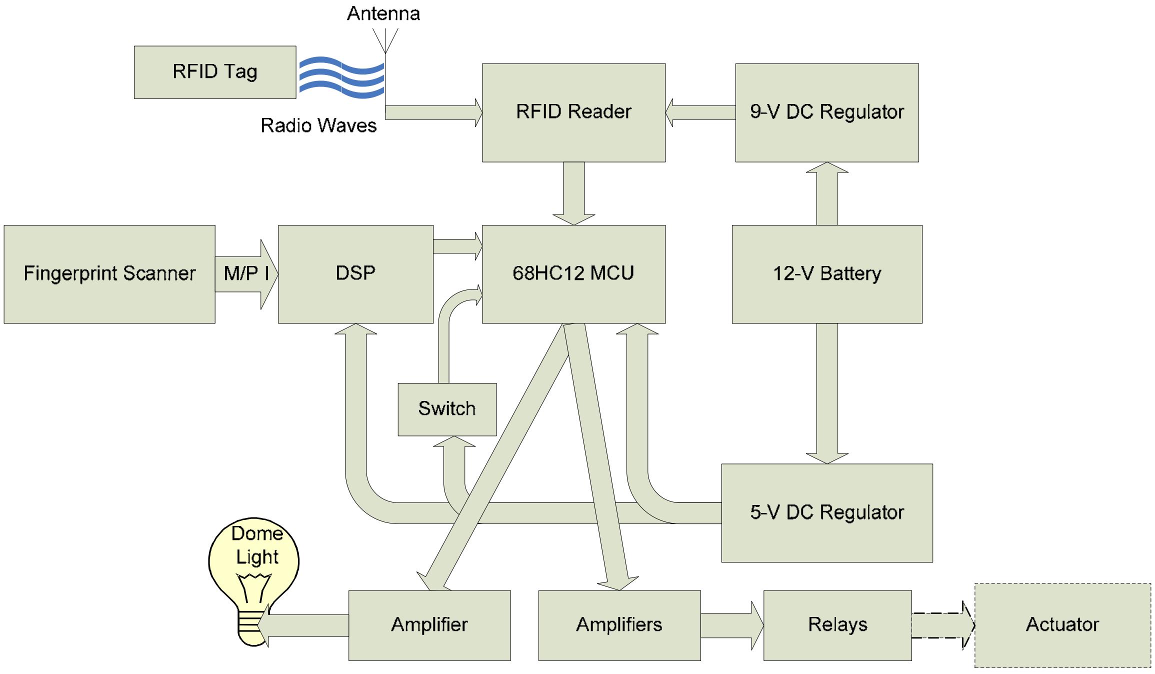
4) The system will utilize three voltage regulators operating at 5 Volts (V) and 9 V.It was decided to use two 5-V regulators to distribute the load. This ensures that a single 5-V regulator will not be overloaded and fail. One 5-V regulator supplies the DSP development kit while the other provides power to the M68HC12 (control processor) board. The 9-V regulator supplies power to the RFID reader.
5) The system is electrically isolated from the rest of the vehicle's electrical system.
6) The entire system should consume less than 2 Watts (W) of power.

System Design

As shown in Figure 2, the complete system comprises the following subsystems:

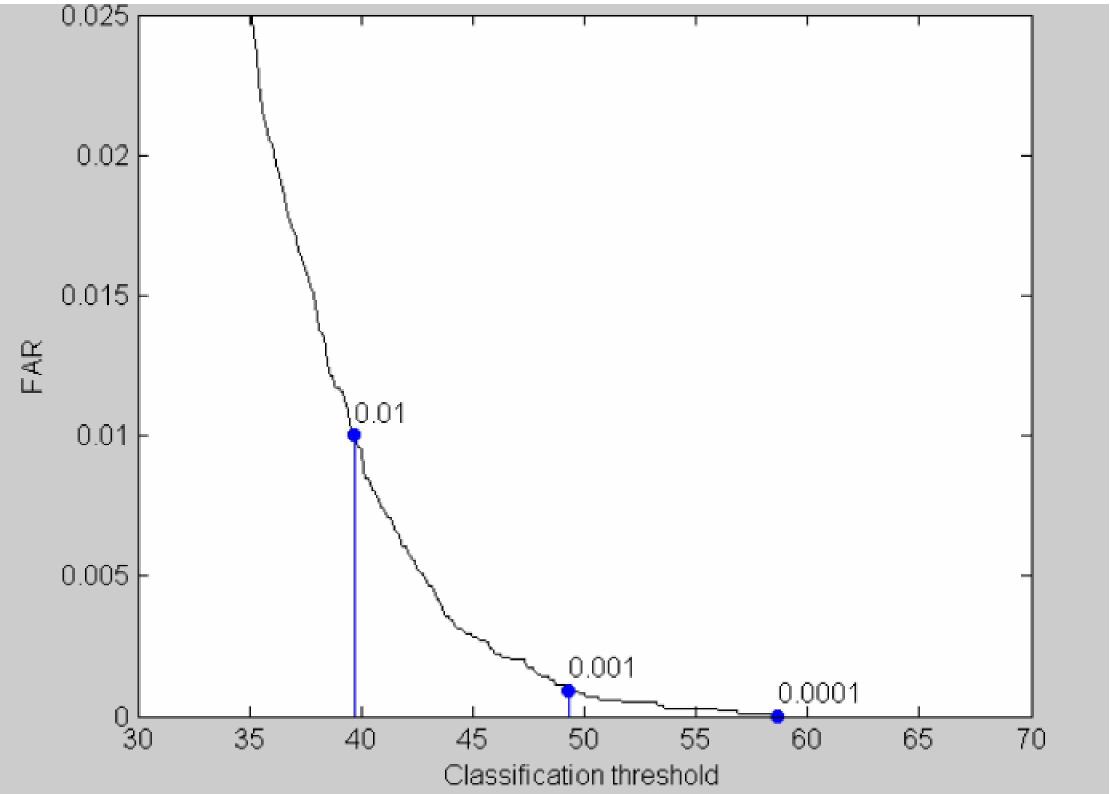
- Voltage regulators – maintain constant voltage for other subsystems.
- Radio Frequency Identification (RFID) reader – communicates with the RFID transponders (tags) used as keys. The EM H4102 RFID Reader consumes 54 mW when idle and uses a 9-V to 12-V DC power supply [9]. Since cars already have a 12-Volt battery and the regulator must have a 3-V potential difference between the input and output to function correctly, the car's battery and a regulator were used to step the voltage down to a consistent 9 V. The chosen reader has the capability to amend an internal list of recognized tags. It outputs logic high when an authorized tag comes into its read range and logic low otherwise [9]. The system in Figure 2 accepts passive tags, which have an indefinite shelf life. Since tags are passive in nature, they also have a lower read range. The low read range is of no consequence since the vehicle's owner will be close to the car door for the fingerprint scan.

Figure 2: Block Diagram of the RFID system.



- RFID Tag – passive RFID transponder. Passive tags do not use batteries, but instead utilize power received from the signal coming from an RFID reader's antenna. Passive tags have an indefinite shelf life by default. These are more abundant and less expensive than active tags.
- Biometric scanner with DSP – the biometric scanner scans fingerprints and uses the DSP to compare and calculate the probabilities of a matched fingerprint. Based on design considerations and upward mobility of the device, it was decided to use the Atmel® fingerprint scanner. This device requires the Texas Instruments (TI) TMS320C6713 DSP [10] to operate. Since, we already had the DSP board in our laboratory, the ATMEL scanner was finalized. Users swipe their fingers across a 1.5 by 15 millimeter sensor strip instead of placing them onto a pad, which eliminates the possibility of leaving a latent print that someone could duplicate. The scanner utilizes the DSP board to run software that compares the fingerprint against a pre-recorded template that users enroll upon first use. The software uses image-processing algorithms for the comparison, and calculates the probability of a match. Should the probability of a match exceed the threshold set by the algorithm, the software will indicate a match. Figure 3 shows the false acceptance rate of Bioscrypt's software. The acceptance threshold was set at 50%, which allows for less than a 0.1% false acceptance rate (FAR).

Figure 3: False Acceptance Rate of Bioscypt's software [11].



- Motorola M68HC12 series micro-controller – uses outputs from the RFID reader and Biometric scanner to control the output of the system. The Motorola M68HC12 (HC12) provides overall system control - deciding when to lock and unlock the door and for deciding when to turn on or turn off an interior light of the automobile. The micro-controller uses the outputs from the RFID and fingerprint scanning subsystems to directly control the door lock actuator. The HC12 is a common, inexpensive micro-controller (available in our laboratory). The HC12 was programmed for operation using assembly language. When the system is first turned on the HC12's program locks the doors by default. This would prevent a thief from unlocking the automobile by triggering a reset state. After a user meets the security checks, the HC12 will unlock the door and turn the light on for thirty seconds. When thirty seconds expires, the doors will lock again and the dome light will turn off. Signal conditioning and driving circuitry – form the interfaces between the subsystems for communication purposes and driving high current devices. The output of the ATMEL device switched between a 0-V (ground) and 2-V level. It needed to be interfaced to the HC12 series micro-controller that utilized 5-V transistor-transistor logic (TTL). To condition the signal to correspond with the HC12, an operational amplifier (op-amp) was used to amplify the voltage states. The op-amp of choice was the LM386 single-sided op-amp. The LM386 is single-sided meaning that it will operate on a supply that provides only positive voltage. The non-inverting configuration was chosen to produce a positive gain. To convert 2-V to 5-V, a gain factor of 2.5 was implemented. Since, the LM386 used a power of 5 Volts, even if the gain was slightly more than 2.5, the amplifier will saturate at 5 V and will not exceed the required level. Another LM386 was used to affect dome light control.
- Automobile door lock actuator – direct current (DC) motor that extends and retracts an arm to lock and unlock the door. The car door lock actuator is a DC motor that switches direction based on the polarity of the input voltage. So, to extend the arm of the actuator, the system must provide 12 V on pin A and ground on pin B. Likewise, to retract the actuator arm, system must provide 12 V on pin B and ground on pin A. To enact the polarity inversion for the actuator, the system used two relays to switch between ground and 12-V for each pin. The relays required more power than the HC12 could provide. The Apex PA26 power amplifier was used to drive the relays with the requisite voltage and current.

Voltage Regulation: The product includes voltage-regulating circuits to maintain a constant, nominal direct current (DC) voltage for the subsystems and protect them from higher than normal voltage levels. Since the system will eventually reside inside an automobile, the normal voltage at which the electrical system operates is 12.6 Volts (V). The voltage regulators ensure that these subsystems will receive 5 V, even in the presence of erratic voltages the alternator may produce. Also, the voltage regulators hold a constant voltage level, so consumers can implement the system in utility vehicles that use 24-V systems, like diesel trucks.

Common problems for automobile electrical systems are weak/old batteries, or malfunctioning alternators. If either or both of these irregularities occur, the effects could be higher than normal voltages in the automobile's electrical system. It is possible for an alternator (whether malfunctioning or without the load of a battery) to output voltage levels in excess of 24 V. Such extreme voltages could damage any electronic system in the automobile, if present for long periods of time. In this worst-case scenario, the voltage regulator IC would be less expensive to replace than a micro-controller or other programmable device. The LM317 was chosen to implement voltage regulation. The LM317 is a variable regulator and was used to regulate 5 V and 9 V.

Results

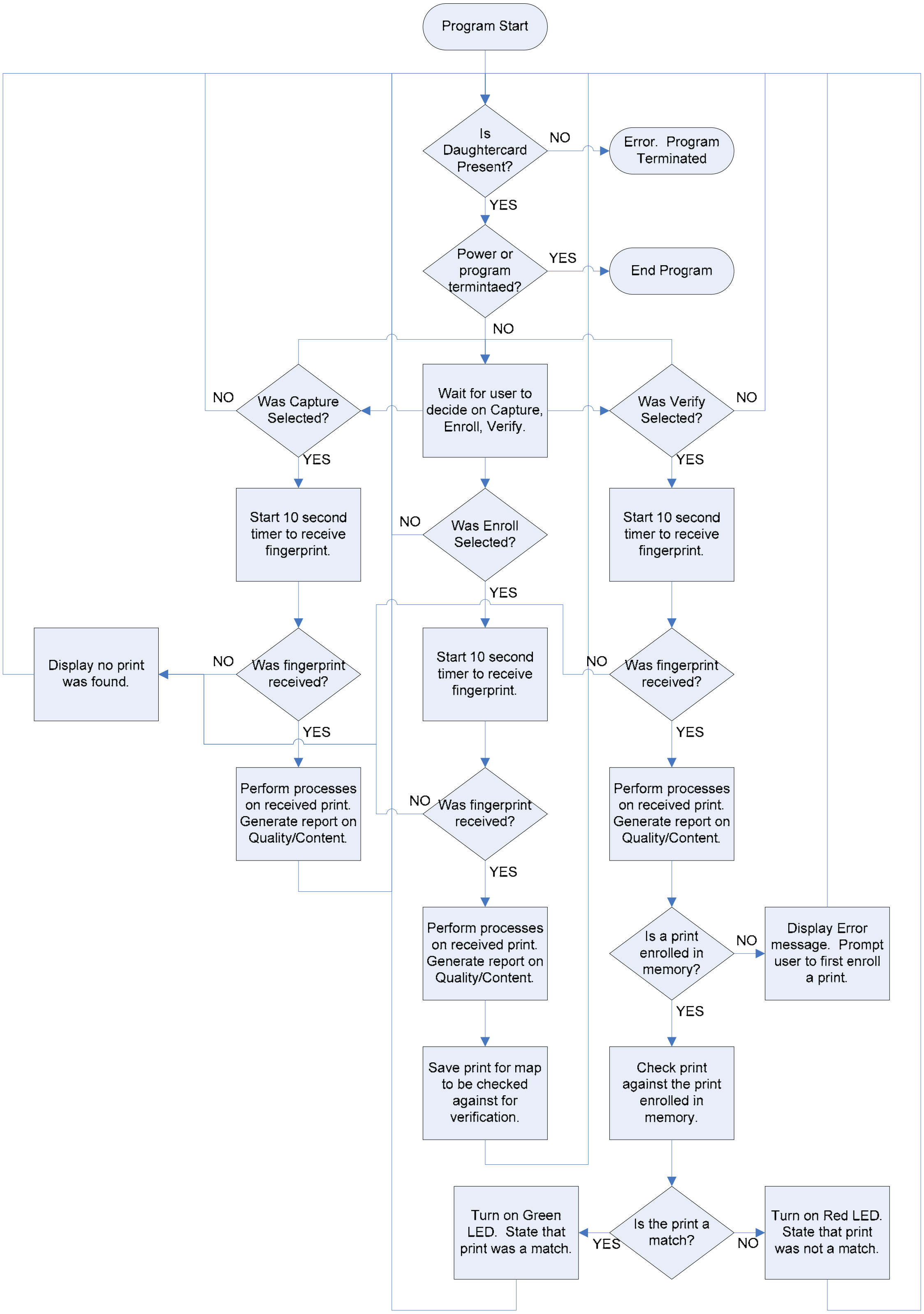
Fingerprint scanning Process: Fingerprint capturing happens when the biometrics reader takes an image of the individual finger. This process is only used to show the fingerprint to the user after a capture and to determine the quality as well as number of minutia present. The enrollment of a print is performed by the DSP. It first receives an input signal telling the biometrics scanner to prepare for a read. The daughter-card then allows a ten-second period when a print will be scanned. If no prints are detected within this time, it will return back to a standby state. If a print is detected, the DSP will accept the scan and prepare to store it in memory. Prior to the print being stored, the image scanned in is first cropped down as to save on memory space and to make the execution of the code quicker. Once the image is cropped, the minutia is then located on the print. More minutiae that can be detected in the verification process by the DSP constitute a higher-quality scan. With the image now cropped and minutia map created, the print can now be stored in memory as a template to be used in the verification process. The verification process is very similar to the enrollment process. During verification, the image is scanned again, cropped down to a smaller size, and then a minutia map is created. The difference is that the print accepted during the verification phase will never be stored in memory for further use. The main goal in verification is to receive a minutia map to check against existing maps in memory. The algorithm that performs this verification is proprietary software and is different for each company as well as for different types of biometric scanners. Bioscrypt has housed this algorithm as data burned into a memory chip on the daughter-card itself and thus users are unable to gain access to it.

Once the verification process has been executed, the results have two possibilities: either there was a successful matching of the two minutia maps or there was not. Since the system is only concerned with a successful match, this is the only state monitored. When this happens, a pin goes low which is being monitored by the HC12 micro-controller. The status of this pin determines how the code will execute on the HC12. Figure 4 is a flowchart describing the process of the code during execution on the DSP.

Micro-controller Code: The first process that occurs inside the code executing on the HC12 is to lock the vehicle door. This accomplishes two conditions, the first being that the car door is now in a known state while the second is that if someone disconnects the system and then reconnects it, the first action taken by the program is to lock the door to ensure security. Once this locking has occurred, the program checks the state of the bypass switch installed in the vehicle. Since the bypass switch used is a toggle switch with two states, it will either be seen as enabled or disabled.

In the enabled state, the system looks for both the biometrics scan verification as well as the presence of a RFID tag. As stated in the DSP software discussion, the HC12 waits for logic low from the DSP board while at the same time looking for logic high from the RFID reader output. If these both occur while the switch is enabled, then a successful verification has occurred and the HC12 will begin the action phase that is described in the discussion that follows.

Figure 4: DSP Code Flow Chart.


Program Start
Is Daughtercard Present?
NO
Error. Program Terminated
YES
Power or program termintaed?
YES
End Program
NO
Wait for user to decide on Capture, Enroll, Verify.
Was Capture Selected?
NO
YES
Was Verify Selected?
NO
YES
Start 10 second timer to receive fingerprint.
Was Enroll Selected?
NO
YES
Start 10 second timer to receive fingerprint.
Display no print was found.
NO
Was fingerprint received?
YES
Start 10 second timer to receive fingerprint.
NO
Was fingerprint received?
YES
Perform processes on received print. Generate report on Quality/Content.
NO
Was fingerprint received?
YES
Perform processes on received print. Generate report on Quality/Content.
Perform processes on received print. Generate report on Quality/Content.
Is a print enrolled in memory?
NO
Display Error message. Prompt user to first enroll a print.
YES
Save print for map to be checked against for verification.
Check print against the print enrolled in memory.
Turn on Green LED. State that print was a match.
YES
Is the print a match?
NO
Turn on Red LED. State that print was not a match.

When the switch is in the disabled state, the HC12 will only look for the RFID tag presence before proceeding to the action phase. Disabled state does not literally mean that the DSP has been disabled. Instead, what this means is that the HC12 code ignores the state of the DSP. The micro-controller does not care if logic high or logic low is currently being read. Upon a registered RFID tag coming into the presence of the reader, a call to jump to the action phase is initiated. The code constantly verifies the switch is still in the disabled position as to ensure the verification criteria are correct.

The action phase of the code is when the car door is unlocked, dome light tuned on and off, and the car door relocked, each with its own time constraints. The first part of this is the turning on the dome light by sending out logic high (5 Volts) from the HC12. The next step is to unlock the car door. Another output pin will go high (5 V) sending a signal to a power amplifier. This will raise the voltage to 12 V and allow for the relay to pull enough current to switch. Once this occurs, the relay puts the actuator to the battery for three seconds to ensure the actuator has had enough time to unlock. After this, the output to the relay is cut so it returns to a relaxed state. This is done to ensure that there is not a constant current pull from the actuator that could potentially damage itself and cause unnecessary drain from the battery. A thirty-second timer is then initiated. During this time the dome light remains on and the door unlocked giving the user time to get in the car and get situated. After this timer expires, the dome light is turned off and another three-second burst is put to a second relay to drive the actuator in the opposite direction, allowing for the door to lock.

Once the door is completely locked, the code returns to the initial state where it begins checking for the switch to be either enabled or disabled again. The HC12 provides three input registers consisting of eight bits each. Each bit can be used as input or output giving several possibilities for expansion on the system in the future. A flow chart showing the process of the code during its execution is in Figure 5.

The cost of the prototype and the various components used in the project is shown in Table 1.

The total cost of implementation of this prototype is relatively inexpensive and the assembly can be mounted on the door of a car.

Broader Impact of the project

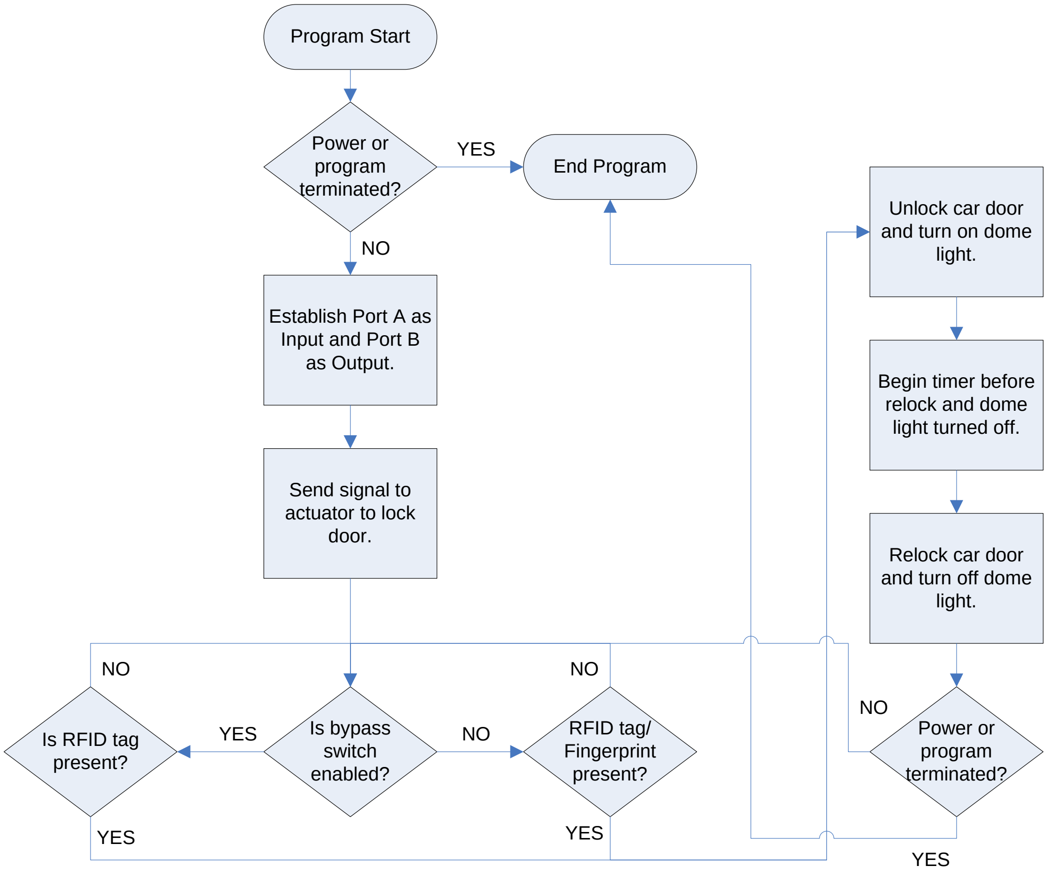
The design was completed and implemented as part of a senior design project. The project enabled students to work in teams; apply their knowledge gained from the curriculum (technical and mathematical); demonstrate a working model and make a professional presentation to their peers and others. In doing so, the students and the program fulfilled program and departmental objectives and satisfied ABET criteria for assessment.

Industry personnel (typically 20-25 invited personnel) and faculty complete evaluations of the presentations. Preliminary results from the Senior Projects/Capstone of Spring 2005 (using assessment methods) showed a positive feedback (a rating of 4.1 on a scale of 5) from industry personnel and faculty on the RFID project. The positive feedback from all constituents has encouraged the program to contemplate including a sub-part of the project as laboratory assignments.

Conclusion

The project accomplished the task of building an inexpensive, RFID based vehicle entry system incorporating biometric scanning. In these times of increased security and public fear, RFID coupled with biometrics offer a solution that can be implemented commercially in daily use. Another possible application of the product beyond cars is doors for houses, where only certain people may have access to particular rooms. The same tag could operate every door;

Figure 5: M68HC12 Code Block Diagram.


Program Start
Power or program terminated?
YES
End Program
NO
Establish Port A as Input and Port B as Output.
Send signal to actuator to lock door.
Unlock car door and turn on dome light.
Begin timer before relock and dome light turned off.
Relock car door and turn off dome light.
NO
Is RFID tag present?
YES
Is bypass switch enabled?
NO
RFID tag/ Fingerprint present?
NO
NO
Power or program terminated?
YES
YES
YES

Product	Qty.	Cost Per Unit	Sub Total
TMS320C6713 DSP Evaluation Kit	1	$395.01	$395.01
TMDSFDCATM31 Biometrics Reader	1	$245.01	$245.01
H4102 RFID Reader (Tags Included)	1	$14.95	$14.95
M68EVB912B32 HC12 Evaluation Kit	1	$198.83	$198.83
LM317T Voltage Regulator	3	$0.45	$1.35
PA26 Power Amplifier	1	$1.39	$1.39
LM386 Operational Amplifier	2	$0.48	$0.96
MTS102 Toggle SPDT	1	$1.15	$1.15
Light bulb	1	$0.35	$0.35
Vehicle 12-Volt Relay	2	$5.99	$11.98
Heat sink for LM317	3	$0.99	$2.97
Heat sink for PA26	1	$0.39	$0.39
Prototyping Board	1	$6.95	$6.95
Fuse Harness	1	$3.29	$3.29
Fuses	4	$0.40	$1.60
Resistors	14	$0.10	$1.40
Capacitors	6	$0.10	$0.60
Total			$888.18

Table 1.

the system could have concurrent tags for both car household doors. For higher security, the HC12 could include a retinal or iris scan, or combinational keypad code expansions. For more flexibility, the owner of a commercial or industrial building could place several of these systems as nodes on an internal network or as removable bypass devices so security guards or employed personnel can unlock any door.

The project could potentially be used for one or more laboratory exercises in the Digital Systems class, where subsequent batches of students could write code, in assembly or C++ to modify or improve the working of the system. The project will also serve to introduce RFID concepts to the next generation of students.

References

1. "Car anti theft prevention," PageWise, Inc., 2002, [Online document], Available HTTP: http://la.essortment.com/antitheftcarp_rhme.htm

2. "NICB," National Insurance Crime Bureau, 2002, Available HTTP: http://www.nicb.org

3. Tomasi, Wayne, "Electronic Communic- cations Systems, Fundamentals Through Advanced," Fifth edition, Prentice Hall 2004.

4. "Production of New PB & KWs Begins," PACCAR, Inc, Volume 1, Number 4, April 2000, [Online document], Available HTTP: http://www.paccar.com/corp/Newsletter/April/NewPB_KWs.asp

5. Steven Shepard, "RFID- Radio Frequency Identification," McGraw Hill, 2005.

6. http://www.ti.com/rfid/docs/news/news_releases/2000

7. http://www.dassnagar.com/Software/AmGm/RF_products

8. Dan Schell, 'RFID keyless entry and ignition system speeds FedEX couriers," Business Solutions, October 2000.

9. "EM Microelectronic-Marin SA H4102," 2000, Swatch Group, Available HTTP: http://home.btconnect.com/QTEKNOLOGY/rfid/H4102_C.pdf

10. "TMS320C6713, TMS320C6713B Floating-Point Digital Signal Processors," 2004, Texas Instruments, Available HTTP: http://focus.ti.com/lit/ds/symlink/tms320c6713.pdf

11. "Biometric Development Kit TI 6713 DSK with FADT", Bioscrypt Inc, Version 1.1.

Biographical Information

Dr. Vijay Vaidyanathan is an Assistant Professor and Coordinator of Electronics Engineering Technology at the University of North Texas. His areas of Research are: Biomedical Optics, Biomedical Engineering and Electronics Instrumentation. He has received the following degrees: a B.S. in Physics in 1985 from the University of Bombay, a B.S in Electronics Instrumentation in 1988 from the University of Bombay, a M.S. in Biomedical Engineering in 1991 from Texas A&M University and a Ph.D in Biomedical Engineering in 1998 from Texas A&M University. His publications can be accessed at his e-mail address: vvaidyan@unt.edu.