ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
THE ORGANIZATION OF THE ISLAMIC COOPERATION (OIC)

MCE: PROJECT
STUDY OF CAR AUTHENTICATION TECHNOLOGY FOR THE SAFETY OF CAR

Supervisor

Prof. Dr Anayet Ullah Patwari

Department of MCE

Academic Session: 2012-2013

Submitted by:

Abdulrashid Umar	**11 34 32**
Said Ali Saandi	**11 34 19**
Aminu Ibrahim Zayyana	**12 34 32**

Department of Mechanical and Chemical Engineering

Program: B.Sc.T.E 2 yrs

Specialization: Automotive- Engineering

Organization of the Islamic Cooperation (OIC)

Islamic University of technology (IUT)

Department of Mechanical and Chemical Engineering (MCE)

DECLARATION

It is here by declared that this project or any part of it has not been submitted elsewhere for award of any degree or diploma to the best of knowledge.

Name: **Said Ali Saandi**
Student No: **113419**
B Sc T E. Mechanical and Chemical Engineering

Name: **Abdulrashid Umar**
Student No: **113432**
B Sc T E. Mechanical and Chemical Engineering

Name: **Aminu Ibrahim Zayyana**
Student No: **123432**
B Sc T E. Mechanical and Chemical Engineering

Supervisor

Prof. Dr Anayet Ullah Patwari

Department of MCE

Table of Contents

LIST OF FIGURES

Acknowledgement

Our special gratitude goes to Allah the Almighty, who render us this golden opportunity to complete this project successfully.

We would also like to thank **Professor Dr.Annayet Ullah Patwari**. His role extended well beyond what can be expected from a supervisor. We would like to express our gratitude to him for his time, support and guidance throughout the course of this work. His supervision and encouragement in completing this work was of paramount important. It was a pleasure working with him and learning the different facets of research. We really appreciate his generous help in this regard.

We must also express our gratitude to our colleagues for the strength they have given us throughout the different stages of this project. Specialty **Isah Usman** and **Abdouraouf Said** who's tirelessly help in organizing and arranging this work.

Abstract

This project will be presented or constructed on a safety and security system based on nine (9) digit remote control system technology. The results suggested a new scenario where the new car can use remote control integrated in the car ignition to allow access and in the dash board as starter button.

A remote and panic button operated security system utilizing a password of an authorized user to control access to the security system, such the ignition system of an automobile. An intelligent security system has a micro controller, a memory card and electrical contact to provide an effective and intelligent security capable of distinguishing between different passwords. A memory is inter forced to the micro controller which control the operation thereof and reads data from the memory to correlate the password of an individual user against one or more users passwords of authorized user of security system stored within the memory. The remote has an electrical contact which is connected to the Car security system, the password are applied therein, to provide electrical power to the circuitry of the remote control to enable a signal to be transmitted from the remote through the electrical contacts to the security system which response controls the security function of the car.

CHAPTER I

INTRODUCTION

The development of innovative self-Authentication Code for Automobile Security system; is an improvement upon the Biometric finger-print anti-theft device. The biometric finger-print device is applied to encode the car security system by using Key or Keyless ignition device which will not allowed the unauthorized person, Unless authorized finger-print recognition is initialed. Any unauthorized persons who gain entry to your vehicle without your permission will set off the quick alarming function. The settings are guided by the master driver through the password controller by hand instruction. It happens that cars are been stalled rampantly, carjacking are becoming more frequent. For you not to become the next victim protect your car by using this highly advancement up to date technology, don't just wait for recovering an already stolen vehicle or puffing a gaudy cumbersome steering wheel brake device, wheel boot or brake lock on or in your car. Now the modern professional thieves already know how to overcome this old technology. The system requires a live finger-print of the pre-programmed authorized finger-print for the vehicle to start. The biometric finger-print authentication device determines if the finger has a pulse, blood pressure, temperature and maps the capillary pattern of the finger. It also performs a 3-D scan of the finger-print determining the width, length and finger-print valley depth of the contour of the finger-print.

In this new technology we intend to introduce a more advanced solution to the problems of car stolen and frequent carjacking. The modern technology provides authorized users the ability to restrict or prevent vehicle operation: through the use of an emergency notification panic buttons for disabling the vehicle in case of emergency.

The disabling systems can also be integrated in to a remote panic and emergency notification system whenever a vehicle is highjack a driver can press a panic buttons hide by this side and in this situation it is only a programmed and authorized passwords of the owner can de-activated the system and potentially start the vehicle to allow the departure. In order to reduce the cost for the construction of this security device a remote disabling systems can also be integrated into a

remote panic buttons to provide authorized users at a remote locations the ability to prevent an engine from starting, prevent movement of the vehicle and to stop or slow an operating vehicle. The driver uses passwords, pin numbers ranging from one to four (4) digits to start the vehicle. All activities related to the use of the vehicle are associated with the driver signed-in at the time. This information can be used for driver performance and driver log purposes. The driver Authentication is vital part of many vehicle disabling systems. Through the use of a driver login process, the login information (4 digits pin password) entered into the remote controller that consist of 10 digit keypad members.

1.1 Objectives

An innovative self-authentication code for Automobile security system is used to prevent the unauthorized users from initially operating a vehicle and to gradually decelerate and stop a vehicle in-transit under certain pre-determined conditions. This system can be designed to achieve the following objectives:

1. Unauthorized access or use of a vehicle without permission of the owner.

2. Using of security panic buttons when any security violations occur.

3. Vehicle entry into unauthorized areas.

4. Vehicle departure from predetermined routes.

5. Prevention of engine damage due to detected system failures.

6. Crisis or emergency situation and mandatory maintenance needs.

1.2 Field of the Inventions

This invention relates generally to a four digit point-code security system and also in addition to this, a remote panic buttons can also be integrated which is programmed with a unique pin code by the owner, and more particularly per trains to an innovative self-authentication code for automobile security system which is implemented in association with a key operated automobile ignition switch security system.

1.3 Discussion of the Prior Art

Traditional methods of turning on the ignition system in an automobile have relied upon a key operated, rotating cylinder lock ignition switch in which a key has encoded pattern cut in to an edge thereof. The mechanical rotating tumbler locking, devices are coupled to an electrical ignition switch, and effectively decode the key and operate the ignition switch. Later advancements have included a series of jumper connection embedded in the key which in effect, act as a programing mechanism for the key. All of these locking mechanisms have shared a common problem: they can be relatively easy by passed and defeated, particularly by professional thieves. Two common methods of automotive theft rely upon speed, and include shorting together the wires connected to the ignition switch or breaking apart the ignition lock assembly to there by defeat its integrity, and have not change much over time despite many advances in technology. The risk to a criminal being caught increases in proposition to the time required to steal a vehicle. A third Common method of an automotive theft is simply due to the carelessness of an owner inadvertently learning the keys in the ignition.

Higher levels of security for locking mechanism have been achieved by mechanical or optical scanners which correlate some unique biometric parameters of an individual, such as a finger-print. A scanner of this type, however, have been much too large and expensive to embed in a typical automotive ignition key, so we intend to introduce this new technology in order to facilitate the cost for construction and easy purchase in the market for users.

A 10 digit remote control and emergency panic button was design to be flexible in order to be enabled and disabled any time, so you may use only 4 digit password to start your car. The system can be designed in such a way to store up to 3 different passwords and one specific password for the owner in case, when a panic buttons is activated. This means that a total of four (4) different passwords can be used to allow you to register your family members and probably your friend.

Thesis Organization

This thesis has three major parts: the front matter (abstract, table of contents, etc.), the text, and the back matter (references, appendices). The text of the thesis is the subject of this section. The text of the thesis is usually divided into chapters and provided with introductory and concluding sections, which is designated as chapters. There are also subheadings within the chapters which is indicating the orderly progression of topics and their relation to each other. Two major types of headings are frequently used, one indicating levels of headings by variations in capitalization, position, and formatting, and one using a decimal system. All chapter headings are typed consistently, however, as well as all first-level subheadings, and so on. For headings, work downward from the top without skipping levels. The chapters were not subdivide each to the same degree (you might have first- through fourth-level headings in one chapter but only first- and second-level headings in another). All level of heading are clearly distinguished typographically from the other levels, and the variations were selected so as to reflect in an obvious way the hierarchy of headings (that is, higher level headings should look more important). We always allow at least one extra line of space above subheadings, and preferably below as well. Without this extra space, it is sometimes difficult to distinguish headings from text.

This thesis covered the sum of six chapters each of which we discus different concept about Authentication security for car safety. This Thesis include introduction, literature review proposed car code algorism, fabrication procedure of the proposed code, conclusion and recommendation, references. Each of this chapters is further divided into subheadings.

Chapter I:

Introduction consists the objectives, field of invention, discussion of the prior art.

Chapter II:

Literature review consists the background of the development, why we need fingerprint for identification, prehistoric, the historical background of an innovative technology for car safety.

Chapter III:

Propose car algorithm consists the description and working principle, automotive conventional ignition system, wiring diagram for car starting system, battery circuit, fuse, remote, starter, neutral safety switch, panic bottom.

Chapter IV:

Fabrication procedure of the proposed code which include the design and construction, identification and authentication of password, description of vehicle disabling system, remote and non-remote disabling system and their applications, operation and benefits, fabrication process.

Chapter V:

Conclusion and recommendations.

Chapter VI:

References.

CHAPTER II
LITERATURE REVIEW

2.1 Background of the Development

In the twenty-first century, both developed and developing countries are characterized with rapid changes in a transition that is modeling the world into a “global village” full of competitions and interdependency. Major forces are driving change in the world of work. The technological development in an innovative technology for car authentication requires a live fingerprint verification of the pre-programmed authorized fingerprint for the vehicle to start.

2.2 Why Fingerprint Identification?

Fingerprints offer an infallible means of personal identification. That is the essential explanation for fingerprints having replaced other methods of establishing the identities of criminals reluctant to admit previous arrests. The science of fingerprint Identification stands out among all other forensic sciences for many reasons, including the following:

- Has served governments worldwide for over 100 years to provide accurate identification of criminals. No two fingerprints have ever been found alike in many billions of human and automated computer comparisons. Fingerprints are the very basis for criminal history foundation at every police agency on earth.
- Established the first forensic professional organization, the International Association for Identification (IAI), in 1915.
- Established the first professional certification program for forensic scientists, the IAI's Certified Latent Print Examiner (CLPE) program (in 1977), issuing certification to those meeting stringent criteria and revoking certification for serious errors such as erroneous identifications.

- Remains the most commonly used forensic evidence worldwide - in most jurisdictions fingerprint examination cases match or outnumber all other forensic examination casework combined.
- Continues to expand as the premier method for positively identifying persons, with tens of thousands of persons added to fingerprint repositories daily in America alone - far outdistancing similar databases in growth.
- Worldwide, fingerprints harvested from crime "scenes lead to more suspects and generate more evidence in court than all other forensic laboratory techniques combined.

Other visible human characteristics tend to change - fingerprints do not. Barring injuries or surgery causing deep scarring, or diseases such as leprosy damaging the formative layers of friction ridge skin (injuries, scarring and diseases tend to exhibit telltale indicators of unnatural change), finger and palm print features have never been shown to move about or change their unit relationship throughout the life of a person. In earlier civilizations, branding and even maiming were used to mark the criminal for what he or she was.

The thief was deprived of the hand which committed the thievery. Ancient Romans employed the tattoo needle to identify and prevent desertion of mercenary soldiers from their ranks. Before the mid-1800s, law enforcement officers with extraordinary visual memories, so-called "camera eyes," identified previously arrested offenders by sight. Photography lessened the burden on memory but was not the answer to the criminal identification problem. Personal appearances change. Around 1870, French anthropologist Alphonse Bertillon devised a system to measure and records the dimensions of certain bony parts of the body. These measurements were reduced to a formula which, theoretically, would apply only to one person and would not change during his/her adult life.

The Bertillon system was generally accepted for thirty years. But it never recovered from the events of 1903, when a man named Will West was sentenced to the U.S. Penitentiary at Leavenworth, Kansas. It was discovered that there was already a prisoner at the penitentiary at the time, whose Bertillon measurements were nearly the same, and his name was William West. Upon investigation, there were indeed two men who looked exactly alike. Their names were Will and William West respectively. Their Bertillon measurements were close enough to identify them as the same person. However, a fingerprint comparison quickly and correctly identified

them as two different people. (Per prison records discovered later, the West men were apparently identical twin brothers and each had a record of correspondence with the same immediate family relatives.)

2.3 Prehistoric

Picture writing of a hand with ridge patterns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals. In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike.

Marcello Malpighi [1], an anatomy professor at the University of Bologna, noted fingerprint ridges, spirals and loops in his treatise. He made no mention of the value of fingerprints for human identification. A layer of skin was named after him; "Malpighi" layer, which is approximately 1.8mm thick. John Evangelist Purkinje [2], anatomy professor at the University of Breslau, published his thesis discussing nine fingerprint patterns, but he too made no mention of the value of fingerprints for personal identification. William James Herschel [3], the English first began using fingerprints in July of 1858, when Sir William James Herschel, Chief Magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts. On a whim, and without thought toward personal identification, Herschel had Rajyadhar Konai, a local businessman; impress his hand print on a contract. The idea was merely "to frighten [him] out of all thought of repudiating his signature." The native was suitably impressed, and Herschel made a habit of requiring palm prints--and later, simply the prints of the right Index and Middle fingers--on every contract made with the locals. Personal contact with the document, they believed, made the contract more binding than if they simply signed it. Thus, the first wide-scale, modern-day use of fingerprints was predicated, not upon scientific evidence, but upon superstitious beliefs.

As his fingerprint collection grew, however, Herschel began to note that the inked impressions could, indeed, prove or disprove identity. While his experience with fingerprinting was admittedly limited, Sir William Herschel's private conviction that all fingerprints were unique to the individual, as well as permanent throughout that individual's life, inspired him to expand

their use. P j Coulier, V D -Grâce [4] published his observations that (latent) fingerprints can be developed on paper by iodine fuming, explains how to preserve (fix) such developed impressions and mentions the potential for identifying suspects' fingerprints by use of a magnifying glass.

Henry Faulds [5], the British Surgeon-Superintendent of Tsukiji Hospital in Tokyo, Japan, took up the study of "skin-furrows" after noticing finger marks on specimens of "prehistoric" pottery. A learned and industrious man, Dr. Faulds not only recognized the importance of fingerprints as a means of identification, but devised a method of classification as well. Faulds [6], forwarded an explanation of his classification system and a sample of the forms he had designed for recording inked impressions, to Sir Charles Darwin. Darwin, in advanced age and ill health, informed Dr. Faulds that he could be of no assistance to him, but promised to pass the materials on to his cousin, Francis Galton. Also in 1880, Dr. Henry Faulds published an article in the Scientific Journal, "Nature" (nature). He discussed fingerprints as a means of personal identification, and the use of printers ink as a method for obtaining such fingerprints. He is also credited with the first fingerprint identification of a greasy fingerprint left on an alcohol bottle.

Gilbert Thompson [7], of the U.S. Geological Survey in New Mexico used his own thumb print on a document to help prevent forgery. This is the first known use of fingerprints in the United States. Click the image below to see a larger image of an 1882 receipt issued by Gilbert Thompson to "Lying Bob" in the amount of 75 dollars. Alphonse Bertillon [8], a Clerk in the Prefecture of Police of at Paris, France, devised a system of classification, known as Anthropometry or the Bertillon System, using measurements of parts of the body. Bertillon's system included measurements such as head length, head width, length of the middle finger, length of the left foot; and length of the forearm from the elbow to the tip of the middle finger. Bertillon [9], was made Chief of the newly created Department of Judicial Identity where he used anthropometry as the primary means of identification. He later introduced Fingerprints but relegated them to a secondary role in the category of special marks. Samuel L. Clemens **[10]** Mark Twain's book, "Life on the Mississippi", a murderer was identified by the use of fingerprint

identification. In a later book, "Pudd'n Head Wilson", there was a dramatic court trial on fingerprint identification. A movie was made from this book in 1916 and a made-for-TV movie in 1984. Sir Francis Galton [11], a British anthropologist and a cousin of Charles Darwin, began his observations of fingerprints as a means of identification in the 1880's. Juan Vucetich [12], an Argentine Police Official, began the first fingerprint files based on Galton pattern types. At first, Vucetich included the Bertillon System with the files. Juan Vucetich [13], made the first criminal fingerprint identification in 1892. He was able to identify Francis Rojas, a woman who murdered her two sons and cut her own throat in an attempt to place blame on another. Her bloody print was left on a door post, proving her identity as the murderer. Sir Francis Galton published his book, "Fingerprints", establishing the individuality and permanence of fingerprints. The book included the first classification system for fingerprints.

Galton's primary interest in fingerprints was as an aid in determining heredity and racial background. While he soon discovered that fingerprints offered no firm clues to an individual's intelligence or genetic history, he was able to scientifically prove what Herschel and Faulds already suspected: that fingerprints do not change over the course of an individual's lifetime, and that no two fingerprints are exactly the same. According to his calculations, the odds of two individual fingerprints being the same were 1 in 64 billion. Galton identified the characteristics by which fingerprints can be identified. A few of these same characteristics (minutia) are basically still in use today, and are sometimes referred to as Galton Details. The Council of the Governor General of India [14], approved a committee report that fingerprints should be used for classification of criminal records. Later that year, the Calcutta (now Kolkata) Anthropometric Bureau became the world's first Fingerprint Bureau. Working in the Calcutta Anthropometric Bureau (before it became the Fingerprint Bureau) were Azizul Haque and Hem Chandra Bose. Haque and Bose are the two Indian fingerprint experts credited with primary development of the Henry System of fingerprint classification (named for their supervisor, Edward Richard Henry). The Henry classification system is still used in English-speaking countries (primarily as the manual filing system for accessing paper archive files that have not been scanned and

computerized. Henry [15] the United Kingdom Home Secretary Office conducted an inquiry into "Identification of Criminals by Measurement and Fingerprints." Mr. Edward Richard Henry (later Sir ER Henry) appeared before the inquiry committee to explain the system published in his recent book "The Classification and Use of Fingerprints." The committee recommended adoption of fingerprinting as a replacement for the relatively inaccurate Bertillon system of anthropometric measurement, which only partially relied on fingerprints for identification.

The Fingerprint Branch at New Scotland Yard (London Metropolitan Police) was created in July 1901 using the Henry System of Fingerprint Classification. First systematic use of fingerprints in the U.S. by the New York Civil Service Commission for testing. Dr. Henry P. Deforest pioneers U.S. fingerprinting. The New York State Prison system [16] began the first systematic use of fingerprints in the U.S. for criminals.

Fingerprints began in Leavenworth Federal Penitentiary in Kansas [17], and the St. Louis Police Department. They were assisted by a Sergeant from Scotland Yard who had been on duty at the St. Louis World's Fair Exposition guarding the British Display. Sometime after the St. Louis World's Fair, the International Association of Chiefs of Police (IACP) created America's first national fingerprint repository, called the National Bureau of Criminal Identification.

U.S. Army [18] begins using fingerprints. U.S. Department of Justice forms the Bureau of Criminal Identification in Washington, DC to provide a centralized reference collection of fingerprint cards. Two years later the U.S. Navy started, and was joined the next year by the Marine Corp. During the next 25 years more and more law enforcement agencies join in the use of fingerprints as a means of personal identification. Many of these agencies began sending copies of their fingerprint cards to the National Bureau of Criminal Identification, which was established by the International Association of Police Chiefs. U.S. Navy begins using fingerprints. U.S. Department of Justice's Bureau of Criminal Identification moves to Leavenworth Federal Penitentiary where it is staffed at least partially by inmates. Harry H. Caldwell (1995) wrote numerous letters to "Criminal Identification Operators" in August 1915, requesting them to meet in Oakland for the purpose of forming an organization to further the

aims of the identification profession. In October 1915, a group of twenty-two identification personnel met and initiated the "International Association for Criminal Identification" In 1918, the organization was renamed the **International Association for Identification** (IAI) due to the volume of non-criminal identification work performed by members. Sir Francis Galton's right index finger appears in the IAI logo. The IAI's official publication is the Journal of Forensic Identification. Edmond Locard wrote that if 12 points (Galton's Details) were the same between two fingerprints, it would suffice as a positive identification. Locard's 12 points seems to have been based on an unscientific "improvement" over the eleven anthropometric measurements (arm length, height, etc.) used to "identify" criminals before the adoption of fingerprints. An act of congress established the Identification Division of the FBI. The IACP's National Bureau of Criminal Identification and the US Justice Department's Bureau of Criminal Identification consolidated to form the nucleus of the FBI fingerprint files. The FBI had processed 100 million fingerprint cards in manually maintained files; and by 1971, 200 million cards. With the introduction of automated fingerprint identification system (AFIS) technology, the files were split into computerized criminal files and manually maintained civil files.

Many of the manual files were duplicates though, the records actually represented somewhere in the neighborhood of 25 to 30 million criminals, and an unknown number of individuals in the civil files. Four employees of the Hertfordshire (United Kingdom) Fingerprint Bureau contacted fingerprint experts throughout the UK and began organization of that country's first professional fingerprint organization, the National Society of Fingerprint Officers. The organization initially consisted of only UK experts, but quickly expanded to international scope and was renamed **The Fingerprint Society** in 1977. The initials F.F.S. behind a fingerprint expert's name indicate they are recognized as a Fellow of the Fingerprint Society. The Society hosts annual educational conferences with speakers and delegates attending from many countries.

The New Orleans, Louisiana [19], delegates to the 62nd Annual Conference of the International Association for Identification (IAI) voted to establish the world's first certification program for fingerprint experts. Since 1977, the IAI's Latent Print Certification Board has proficiency tested

thousands of applicants, and periodically proficiency tests all IAI Certified Latent Print Examiners (CLPEs). Contrary to claims (in the 1990s and later) that fingerprint experts profess their body of practitioners never make erroneous identifications, the Latent Print Certification program proposed, adopted, and in-force since 1977, specifically recognizes that such mistakes do sometimes occur, and must be addressed by the Latent Print Certification Board. During the past three decades, CLPE status has become a prerequisite for journeyman fingerprint expert positions in many US state and federal government forensic laboratories. IAI CLPE status is considered by many identification professionals to be a measurement of excellence. The world's largest annual meeting of fingerprint experts is hosted by the IAI - this year it will be during 22-28 July in Phoenix, Arizona, USA. INTERPOL's Automated Fingerprint Identification System repository exceeds 150,000 sets fingerprints for important international criminal records from 190 member countries. Over 170 countries have 24 x 7 interface ability with INTERPOL expert fingerprint services.

The Unique Identification Authority of India [20] operates the world's largest fingerprint (multi-modal biometric) system, with over 200 million fingerprint, face and iris biometric records. UIAI plans to collect as many as 600 million multi-modal records by the end of 2014. India's Unique Identification project is also known as Aadhaar, a word meaning "the foundation" in several Indian languages. Aadhaar is a voluntary program, with the ambitious goal of eventually providing reliable national ID documents for most of India's 1.2 billion residents. With a database many times larger than any other in the world, Aadhaar's ability to leverage automated fingerprint and iris modalities (and potentially automated face recognition) enables rapid and reliable automated searching and identification impossible to accomplish with fingerprint technology alone, especially when searching children and elderly residents' fingerprints.

2.4 The Historical Development of an Innovative Technology for Car Authentication

An innovative technology for car authentication had a slow start and developed less quickly than other forms of technology. This was partially due to the fact that the traditional methods of turning on the ignition system in an automobile have relied upon a gaudy cumbersome steering wheel lock device, wheel boot or brake lock on or in the car. Later another technology was introduce by Ronne Bonder, New-York and this was operated by rotating cylinder lock ignition switch in which a key has encode pattern cut into an edge thereof. A mechanical rotating tumbler locking mechanism is coupled to an electrical ignition switch, and effectively decodes the key and operates the ignition switch.

Despite the traditional method of turning on the ignition system in automobile, pioneers include a series of jumper connections embedded in the key which in effect, act as a programming mechanism to operate the ignition system. Moreover, the situation was further complicated by the fact that most of those pioneers were unable to increase or popularized the old invention due to the fact that the former technology is much more expensive to purchase.

2.5 An Innovative Technology for Car Authentication

This system requires a live fingerprint verification of the pre-programmed authorized fingerprint for the vehicle to start. The Biometric Fingerprint Authentication device determines if the finger has a pulse, blood pressure, temperature and maps the capillary pattern of the finger. In addition it performs a 3-D scan of the fingerprint determining the width, length and fingerprint valley depth of the contour of the fingerprint. Most system today are optical and can be easily fooled by photocopying or wax imaging a finger in 2 dimensions and pressing that image on the reader pad. The Biometric Fingerprint Authentication Car Anti-Theft device/system cannot be fooled as

it requires a LIVE owners or owner permitted pre-programmed fingerprint to start the vehicle.

Fig: 2.1Use of Verifinger inside the car [21]

Nero-technology [21] developed VeriFinger, a fingerprint identification algorithm, designed for biometric system integrators. Since that time, the company has released 15 algorithm versions, with the current version, VeriFinger 6.6, providing the most powerful fingerprint recognition algorithms to date. VeriFinger fingerprint engine performance and reliability has been recognized by NIST as MINEX compliant.

SDK is intended for adding fingerprint verification functionality into various applications. The SDK is most suitable for developing biometric logon applications, but it can be used also for any other application that does not require storing more than 10 fingerprints. In 2008 Nero-technology released Free Fingerprint Verification SDK. This freeware. This technology was further improved through the application of mega matcher system which was introduced November 14, 2011. The Mega Matcher technology is intended for large-scale AFIS and multi-biometric systems developers. The technology ensures high reliability and speed of biometric

identification even when using large databases. Mega Matcher is available as a software development kit that allows development of large-scale single- or multi-biometric fingerprint, iris, face, voice or palm print identification products for Microsoft Windows, Linux and Mac OS X platforms.

Fig:2.2 Use of multi-biometric systems for car security systems[21]

2.6 VeriLook SDK

Face identification for PC or Web applications

VeriLook facial identification technology is designed for biometric systems developers and integrators. The technology assures system performance and reliability with live face detection, simultaneous multiple face recognition and fast face matching in 1-to-1 and 1-to-many modes. VeriLook is available as a software development kit that allows development of PC- and Web-based solutions on Microsoft Windows, Linux and Mac OS X platforms.

Fig:2.3 Use of VeriLook for car security systems [21]

2.7 VeriFinger SDK

Fingerprint identification for PC and Web solutions

VeriFinger is a fingerprint identification technology intended for biometric systems developers and integrators. The technology assures system performance with fast, reliable fingerprint matching in 1-to-1 and 1-to-many modes.

VeriFinger is available as a software development kit that allows development of PC- and Web-based solutions on Microsoft Windows, Linux and Mac OS X platforms.

Fig: 2.4 Finger print algorisms verification [21]

2.8 VeriEye SDK

Iris identification for PC and Web solutions

VeriEye iris identification technology is intended for biometric systems developers and integrators. The technology includes many proprietary solutions that enable robust iris enrollment under various conditions and fast iris matching in 1-to-1 and 1-to-many modes.

VeriEye is available as a software development kit that allows development of PC- and Web-based solutions on Microsoft Windows, Linux and Mac OS X platforms.

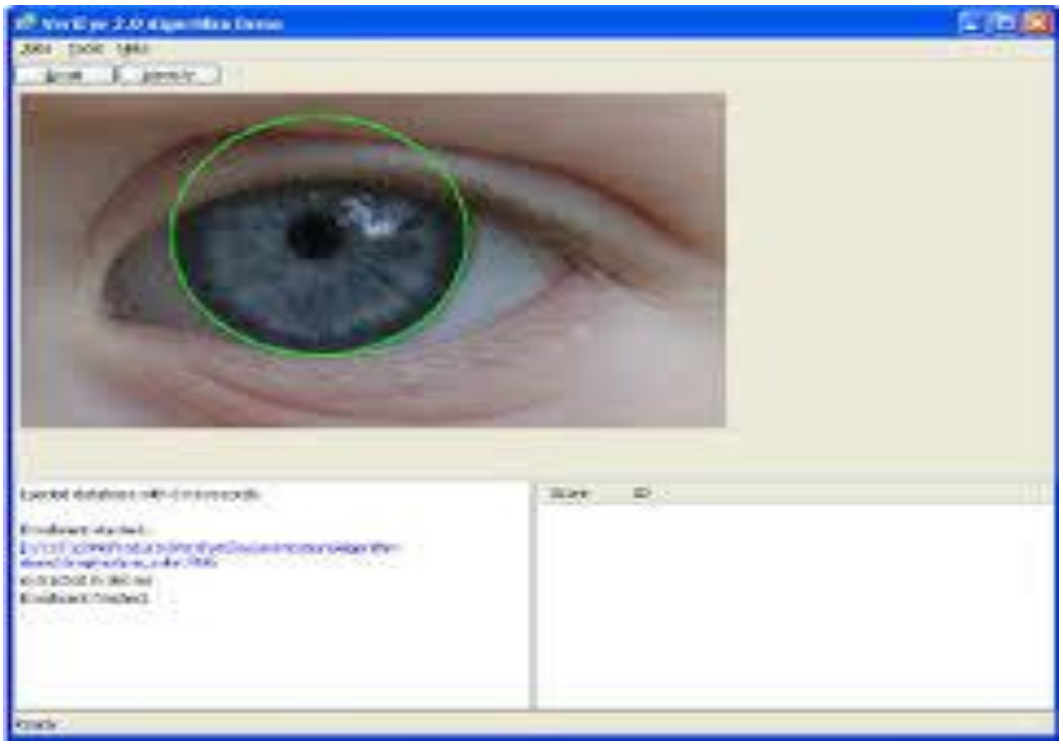


Fig:2.5 Use of Verieye for car security systems [21]

2.9 VeriSpeak SDK

Speaker recognition for PC or Web applications

VeriSpeak voice identification technology is designed for biometric system developers and integrators. The text-dependent speaker recognition algorithm assures system security by checking both voice and phrase authenticity. Voiceprint templates can be matched in 1-to-1 (verification) and 1-to-many (identification) modes.

VeriSpeak is available as a software development kit that enables the development of PC- and Web-based applications on Microsoft Windows, Linux and Mac OS X platforms.

Fig:2.6 Use of VeriSpeak for car security systems[21]

This Biometric Fingerprint Car Anti-theft System allows authorized drivers with enrolled fingerprint to access the system in order to start their car. The car fingerprint security system is designed to be flexible in order to be enabled and disabled anytime, so you may use only your key to start your car, in case you wish to lend your car to a friend. It's simple, place the fingerprint scanner on the car's dash board or by the driver's door for easy accessibility to start your car's engine. After swiping your fingerprint, the fingerprint scanner compares the finger impression with the fingerprints that were stored in its memory when the system was first installed in your car. The fingering car security system can store up to 3 categories with each category storing 3 fingerprints. This means a total of 9 fingerprints can be stored allowing you to

register your friends and family members.

Although there has been a great deal of research directed as the investing the problems facing on the car security system, so as to prevent car stolen and carjacking around the world. So to overcome this problem, those less effective devices are replaced by the par tend biometric fingerprint authentication vehicle anti-theft starter anti carjacking system. This new technology is the wave of the future in security system.

The system may be very much expensive to purchase, here we intended to develop a new system that may require no computer system application. The fingerprint can be replaced by nine digits remote control for use to select as a password to secure the vehicle. And the use of an extra panic button in case of carjacking or any emergency attack.

CHAPTER III

PROPOSED CAR CODE ALGORITHM

3.1 Description and Working Principle

Usually, system may consist of a number of sub-systems or modules. An innovative technology for car authentication involves several points all combined together to produce authentic car security system. The basic structure of an innovative technology for car authentication is very complex but we represented it in a simplified way so, as to facilitate the complexity of understanding its structure. An innovative technology consists of four (4) basic parts which include the battery, remote control, starter motor and ignition switch. And other subsystems which include battery-cables, starter-relay, neutral-safety, starter-solenoid, fuse and panic button. In the figure the basic systems are noted A, B, C and D and the other subsystem are noted I, II, III, IV, V and VI respectively. Before we discuss about the basic system structure, let us describe how a basic system are handle using conventional ignition system.

3.2 Automotive Conventional Ignition System

The circuit shown in Fig below is for a coil-**ignition system** with main components. The heart of the **system** is the **ignition** coil, which transforms the low-tension (LT), 12 V supply given by the battery to the high-tension (HT) with voltage needed to produce a spark at the spark plug.

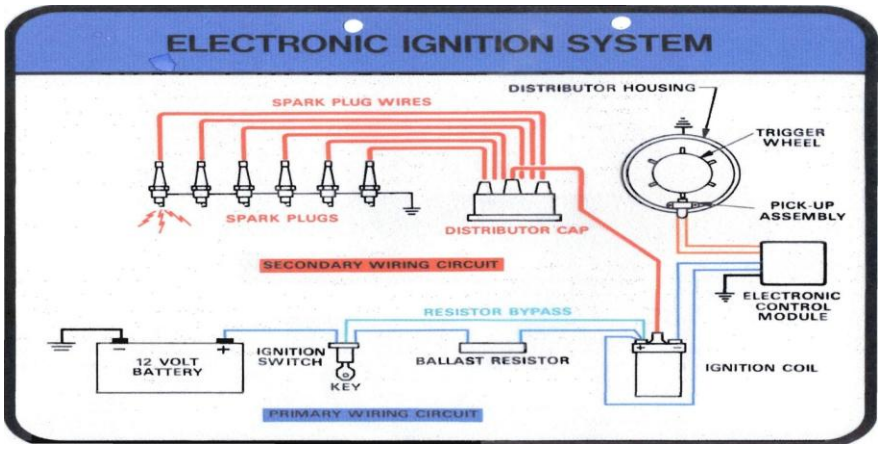


Fig: 3.1 Lay out of an automotive electronic Ignition System [23]

3.3 Wiring Diagram for Car Starting System

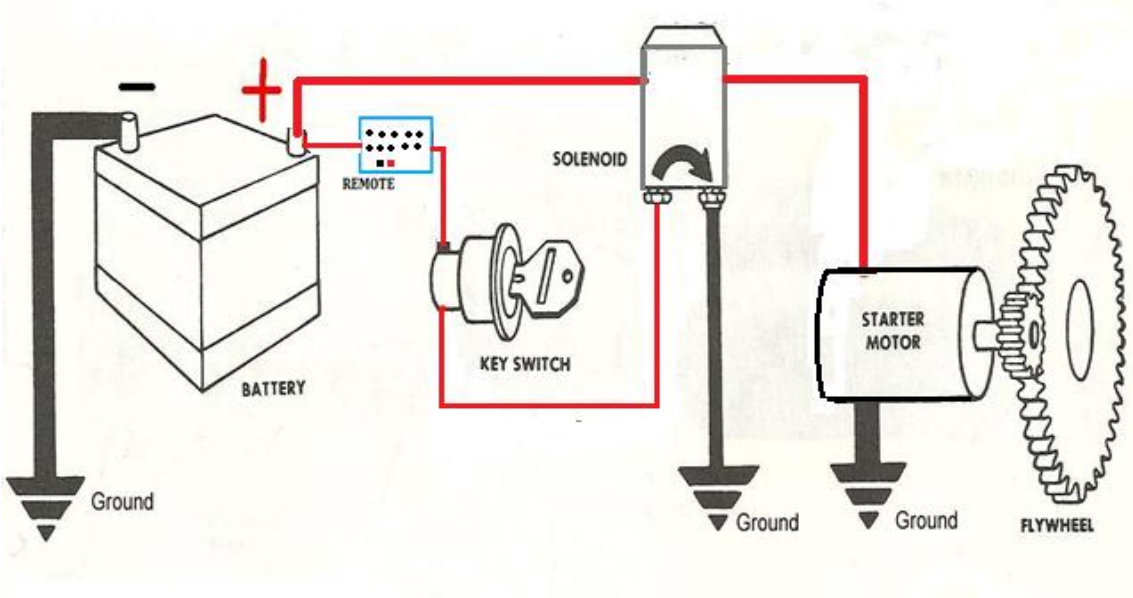
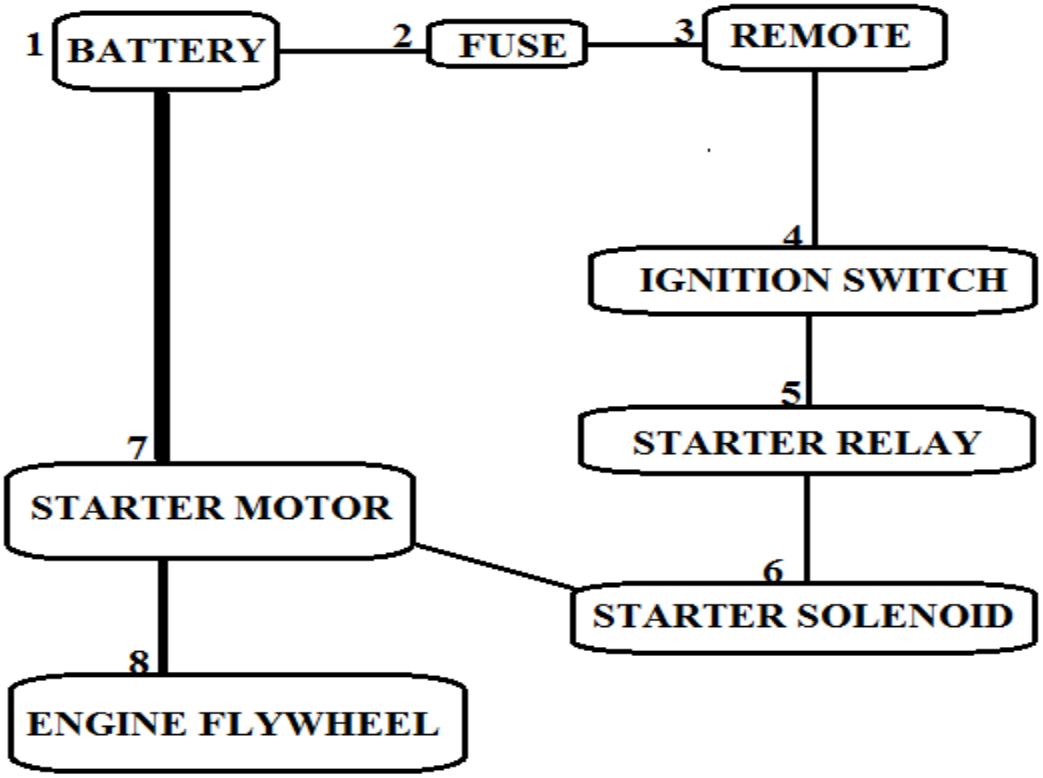


Fig: 3.2 Inter facing process sequence for remote vehicle Starting System



Block diagram of the inter facing process sequence for remote vehicle Starting System

3.4 Battery Circuit

General

The battery is the primary "source" of electrical energy on Toyota vehicles. It stores chemicals, not electricity. Two different types of lead in an acid mixture react to produce an electrical pressure. This electro-chemical reaction changes chemical energy to electrical energy.

3.4.1 Battery Functions

1. ENGINE OFF:
Battery energy is used to operate the lighting and accessory systems.

2. ENGINE STARTING:

Battery energy is used to operate the starter motor and to provide current for the ignition system during cranking.

3. ENGINE RUNNING:

Battery energy may be needed when the vehicle's electrical load requirements exceed the supply from the charging system. In addition, the battery also serves as a voltage stabilizer, or large filter, by absorbing abnormal, transient voltages in the vehicle's electrical system. Without this protection, certain electrical or electronic components could be damaged by these high voltages.

The electrical circuits of an automobile (one example)

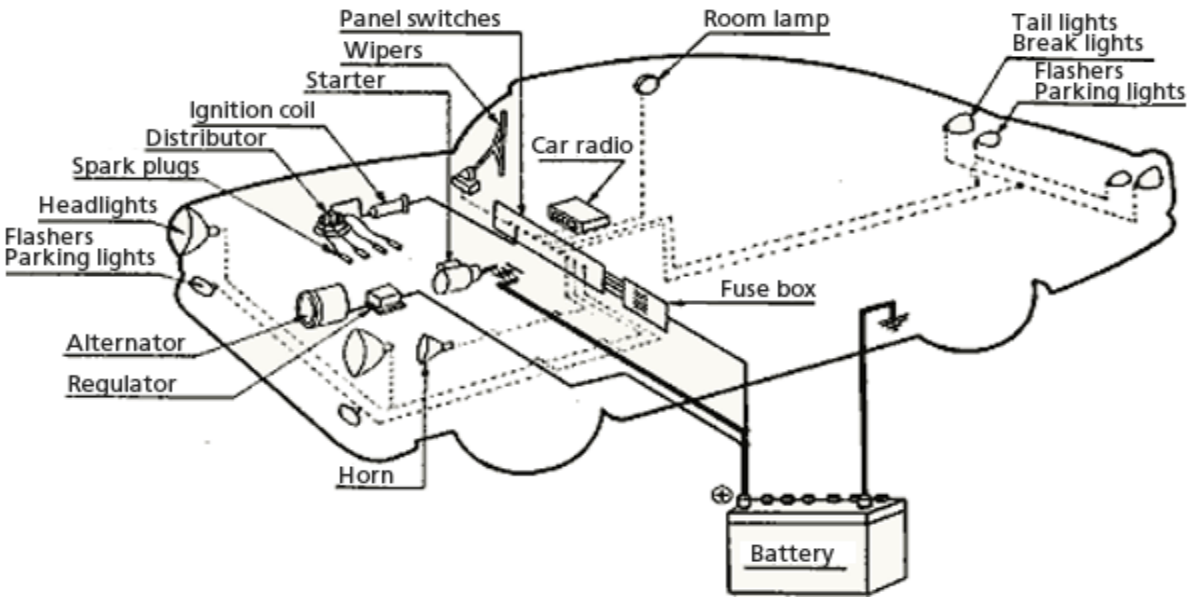


Fig: 3.3 Battery Diagram [23]

The battery supplies power to the starter when starting the engine. When the engine is running, the alternator (generator) supplies electric power to the electric equipment and the battery is recharged at the same time.

3.4.2 Types of Battery

- PRIMARY CELL:

The chemical reaction totally destroys one of the metals after a period of time. Small batteries for flashlights and radios are primary cells.

- SECONDARY CELLS:

The metals and acid mixture change as the battery supplies voltage. The metals become similar, the acid strength weakens. This is called discharging. By applying current to the battery in the opposite direction, the battery materials can be restored. This is called charging. Automotive lead-acid batteries are secondary cells.

- WET-CHARGED:

The lead-acid battery is filled with electrolyte and charged when it is built. During storage, a slow chemical reaction will cause self-discharge. Periodic charging is required. For Toyota batteries, this is every 5 to 7 months.

- DRY-CHARGED:

The battery is built, charged, washed and dried, sealed, and shipped without electrolyte. It can be stored for 12 to .18 months. When put into use, it requires adding electrolyte and charging.

- LOW-MAINTENANCE:

Most batteries for Toyota vehicles are considered low-maintenance batteries. Such batteries are built to reduce internal heat and water loss. The addition of water should only be required every 15,000 miles or so.

3.5 Battery cables

A starter motor requires a very high current to crank the engine, that's why it's connected to the battery with thick (large gauge) cables (see the diagram). The negative (ground) cable connects the "-" battery terminal to the engine cylinder block close to the starter. The positive cable connects the "+" battery terminal to the starter solenoid.

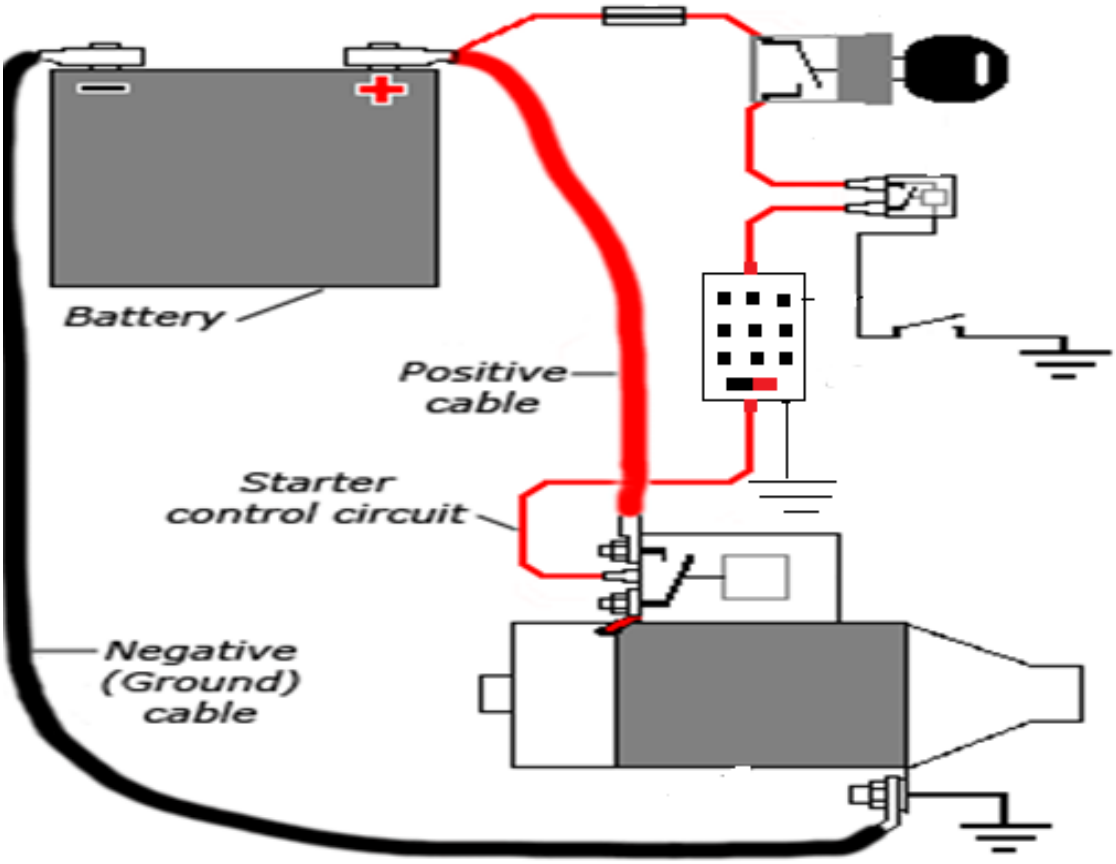


Fig: 3.4 Battery cables connected to vehicle starting system

3.6 Fuse

Fuses are an important protection component of all electrical circuits. These devices are employed in all industries and all electronic products from televisions to power generators and

home wiring grids. Without fuses electronic devices could be severely damaged in the event of a power surge or other event that causes excessive voltage.

Fig: 3.5 Fuse use for breaking circuit for starting system [25]

3.7 Remote

A remote starter allows you to start your car using a four (4) digit password or key-fob remote control-without going outside. If you left the heat or A/C on, it turns on when the engine does. The passwords are applied to operate the remote control and allowed access to the car.

Fig: 3.6 remote control use for car security [21]

3.8 Ignition Switch

A car's ignition switch serves several purposes. First, it allows you to control the power to many of the car's accessories, preventing accessories from running down the car's battery when the car is parked for a long period of time. The ignition switch also serves the far greater purpose of connecting the starter to the battery, allowing the battery to send a powerful surge of electricity to the starter when the car is being started.

Fig: 3.7 Ignition switch for vehicle starting system [24]

3.9 Starter Relay

A relay is a device which uses a small amount of power to control a larger amount of power. In the case of a starter relay, you want to control the large amount of power, sometimes up to 500 amps, flowing through that large cable from the battery to the starter motor. It would not be practical to run that large cable up to the ignition switch and then back to the battery. Instead, a very little amount of power (less than 1/10 amp) passes through the ignition switch to the relay, where it operates an electrical magnet that pulls contacts (a switch) together. The large power cables are connected to the switch in the relay, and once the contacts are pulled together the large amount of power is connected to the starter motor to operate it.

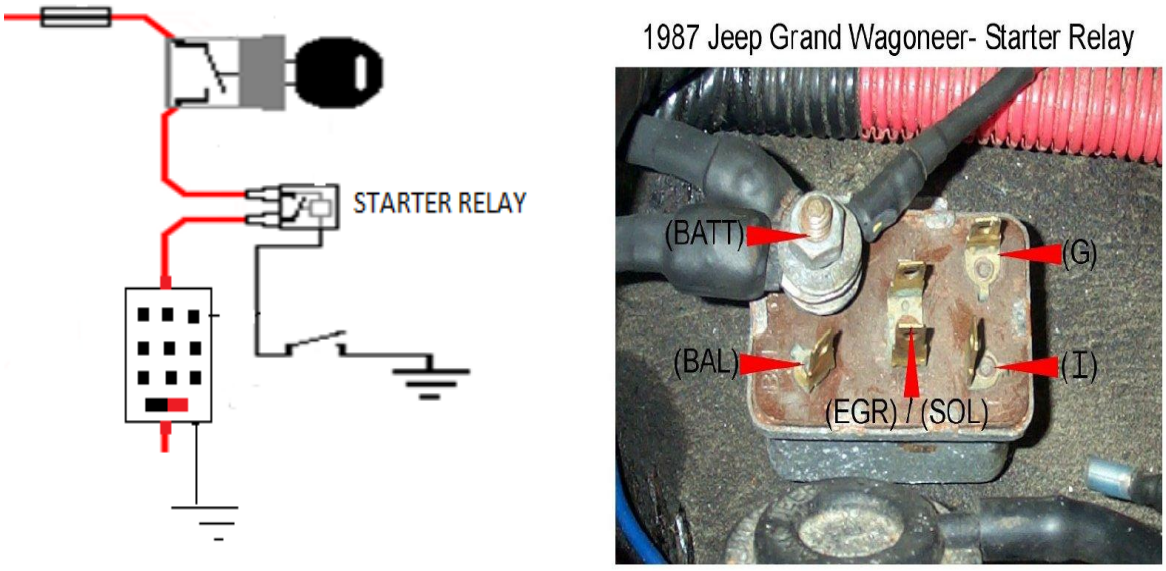


Fig: 3.8 Starter Relay connected to starting system [24]

3.10 Starter Solenoid

The starter solenoid works as a powerful electric relay - when activated, it closes the electric circuit and sends the battery power to the starter motor. At the same, the starter solenoid pushes the starter gear forward to mesh with the engine flywheel. A typical starter solenoid has one small connector for the control wire (the white connector in the photo) and two large terminals: one for the positive battery cable and the other for the starter motor.

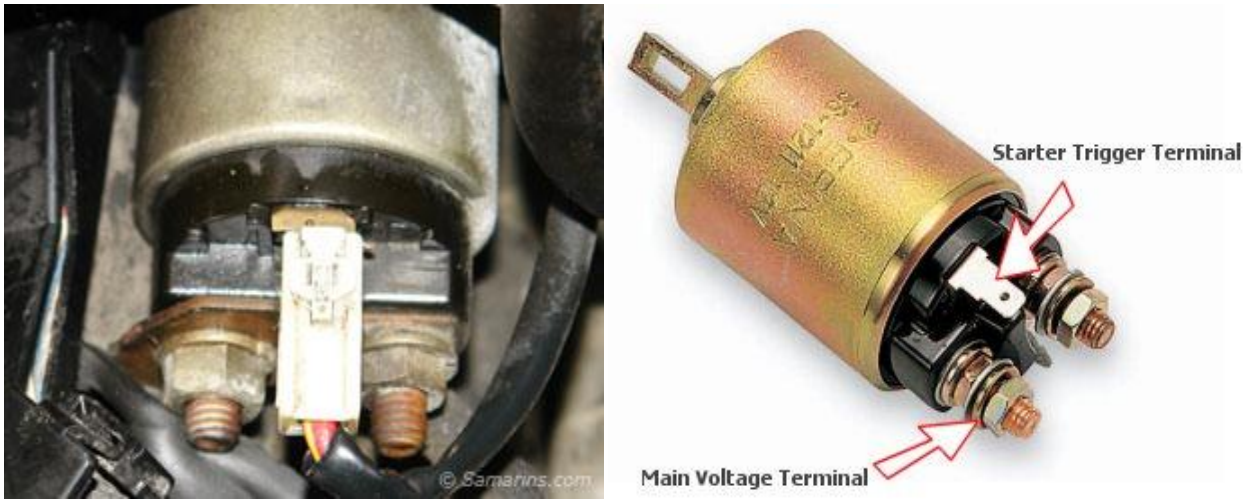


Fig: 3.9 Starter solenoid [24]

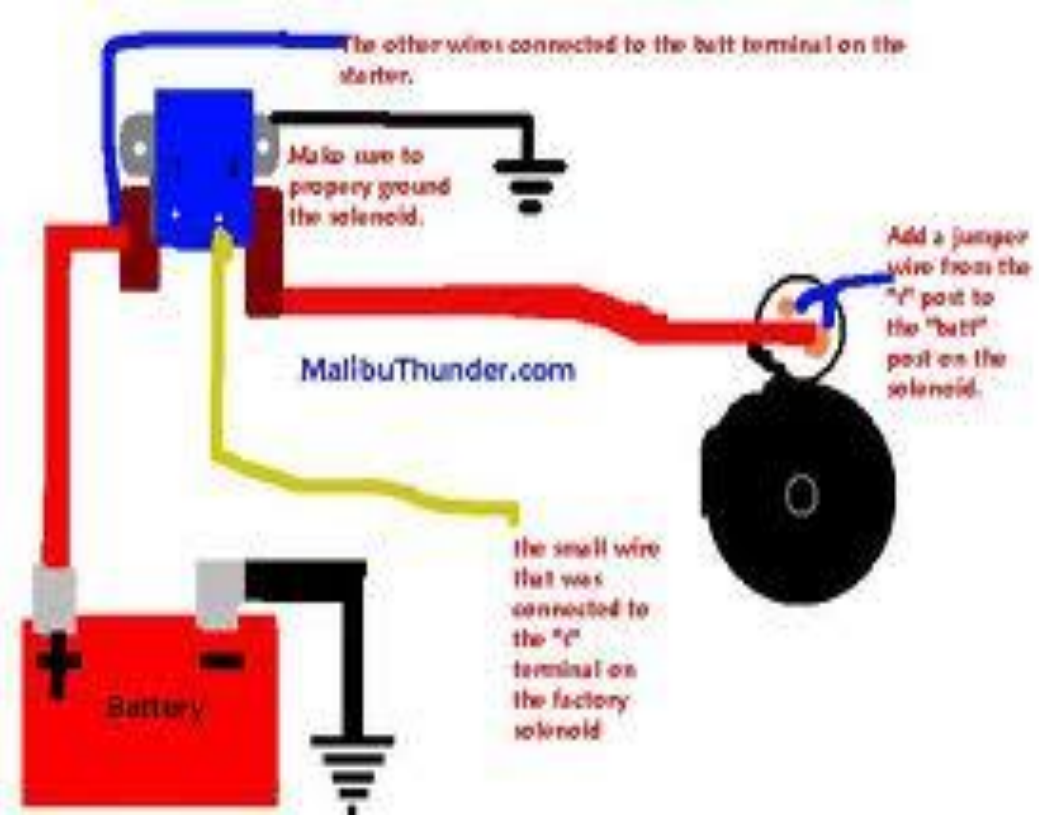


Fig: 3.10 starter solenoid arrangement [25]

3.11 Stator Motor

A starter is an electric motor that turns over or "cranks" the engine to start it. A starter consists of the very powerful DC electric motor and the starter solenoid that is usually attached to the motor (see the picture). Inside, a typical starter motor has the electric windings (coils) attached to the starter motor housing and the armature (the rotating part) that is connected through the carbon brushes in series with the windings. On the front end of the armature, there is a small gear that attached to the armature through an overrunning clutch. This part is commonly known as the *Bendix*.

3.12 Neutral Safety Switch

The purpose of this switch is to prevent the engine being started while in gear - when the switch is operating correctly, the engine will only start while in the park or neutral settings

Fig: 3.12 Neutral safety switch for starting system [25]

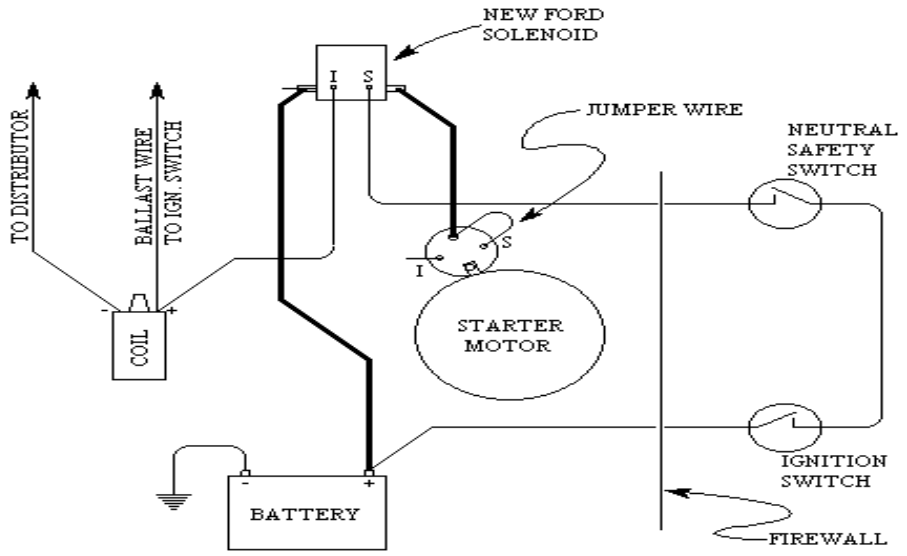


Fig: 3.13 Neutral safety switch wiring arrangement [25]

3.13 Panic Button

A *panic* alarm is an electronic device designed to assist in alerting somebody in emergency situations where a threat to persons or property exists

Fig: 3.14 Panic Button [23]

3.14 Car panic alarms could be an effective tool to scare off intruders

This technique involves taking your car keys out of your pocket or purse and putting them on your nightstand or headboard when you go to bed. If you're awakened by an intruder or perceived intruder, you merely grab your car keys and hit the panic button.

This would cause your car in the garage, driveway or street to start sounding its horn. The noise of the horn and the fact that the intruder would then know someone is awake in the home would scare away most intruders. Secondarily, the noise of the horn would attract attention from neighbors.

Fig: 3.15 key components panic button [24]

The key components of this panic button alarm system are your neighbors. If you're going to use this technique, you should contact your neighbors and ask them to call the police if they ever hear your car alarm sounding. Tell your neighbors how you're using the panic button to make noise to thwart an intruder, draw attention and summon help. If you have no neighbors nearby,

you'll be dependent on the car's horn alone scaring the intruder. In that case, you'd be better off investing in an alarm system, dog or a firearm for home defense.

If you decide to use the car key panic button method, trial runs of very short duration should be attempted. Make sure the radio wave will reach your car from your bedroom. Make sure you can operate the panic alarm in low light or no light conditions. This includes being able to turn the alarm off, should it activate unintentionally. Furthermore, in an actual emergency, you should call 911 as soon as you trip the panic button to get the police moving toward your home as soon as possible.

Calling 911 is another motor skill that should be practiced, especially if you are using a cell phone with small buttons. To practice, remove your phone battery or disconnect the phone at the phone jack and practice dialing 9-1-1-SEND, 9-1-1-TALK or just 9-1-1, depending on your phone. Practice so you can do it in the dark and without eyeglasses. It is important to practice because when you are under intense stress, fine motor skills become impaired. If you are a neighbor and hear a car alarm sounding and it isn't stopping, call the police. Officers will respond to the car alarm, ascertain the source, run a registration check on the plate or just knock on the door if the vehicle is in a driveway or garage. Either way, police will try to make contact with the vehicle owner to make sure all is well and get the horn shut off. Therefore, a car key fob panic button alarm could be an effective tool to ward off intruders and call for help.

3.15 Flywheel

A **flywheel** is a rotating mechanical device that is used to store rotational energy. Flywheels have a significant moment of inertia and thus resist changes in rotational speed. The amount of energy stored in a flywheel is proportional to the square of its rotational speed. Energy is transferred to a flywheel by applying torque to it, thereby increasing its rotational speed, and hence its stored energy. Conversely, a flywheel releases stored energy by applying torque to a mechanical load, thereby decreasing its rotational speed.

Common uses of a flywheel include:

- Providing continuous energy when the energy source is discontinuous. For example, flywheels are used in reciprocating engines because the energy source, torque from the engine, is intermittent.
- Delivering energy at rates beyond the ability of a continuous energy source. This is achieved by collecting energy in the flywheel over time and then releasing the energy quickly, at rates that exceed the abilities of the energy source.
- Controlling the orientation of a mechanical system. In such applications, the angular momentum of a flywheel is purposely transferred to a load when energy is transferred to or from the flywheel.

Flywheels are typically made of steel and rotate on conventional bearings; these are generally limited to a revolution rate of a few thousand RPM Some modern flywheels are made of carbon fiber materials and employ magnetic bearings, enabling them to revolve at speeds up to 60,000 RPM

3.16 Starter Flywheel

Fig: 3.16 Starter flywheel connection [24]

Flywheels are often used to provide continuous energy in systems where the energy source is not continuous. In such cases, the flywheel stores energy when torque is applied by the energy source and it releases stored energy when the energy source is not applying torque to it. For example, a flywheel is used to maintain constant angular velocity of the crankshaft in a reciprocating engine. In this case, the flywheel-which is mounted on the crankshaft-stores energy when torque is exerted on it by a firing piston and its releases energy to its mechanical loads when no piston is exerting torque on it. Other examples of this are friction motors, which use flywheel energy to power devices such as toy cars.

Fig: 3.17 Modern automobile engine flywheel [24]

A flywheel may also be used to supply intermittent pulses of energy at transfer rates that exceed the abilities of its energy source, or when such pulses would disrupt the energy supply (e.g., public electric network). This is achieved by accumulating stored energy in the flywheel over a

period of time, at a rate that is compatible with the energy source, and then releasing that energy at a much higher rate over a relatively short time. For example, flywheels are used in riveting machines to store energy from the motor and release it during the riveting operation. The phenomenon of precession has to be considered when using flywheels in vehicles. A rotating flywheel responds to any momentum that tends to change the direction of its axis of rotation by a resulting precession rotation. A vehicle with a vertical-axis flywheel would experience a lateral momentum when passing the top of a hill or the bottom of a valley (roll momentum in response to a pitch change). Two counter-rotating flywheels may be needed to eliminate this effect. This effect is leveraged in reaction wheels, a type of flywheel employed in satellites in which the flywheel is used to orient the satellite's instruments without thruster rockets.

Fig: 3.18 Pinion of Starter Motor with Flywheel [24]

The starting system consists of the battery, cables, starter motor, flywheel ring-gear, and the ignition switch. During starting two actions occur. The pinion of the starter motor engages with the flywheel ring gear, and the starter motor then operates to turn over, or 'crank', the engine. The starter motor is an electric motor mounted on the engine block, and operated from the battery. It is designed to have high turning effort at low speeds. The starter cables are the thickest on the vehicle, as a high current must be delivered to the starter motor, to turn the crankshaft from rest, and keep it turning until the engine fires, and runs on its own.

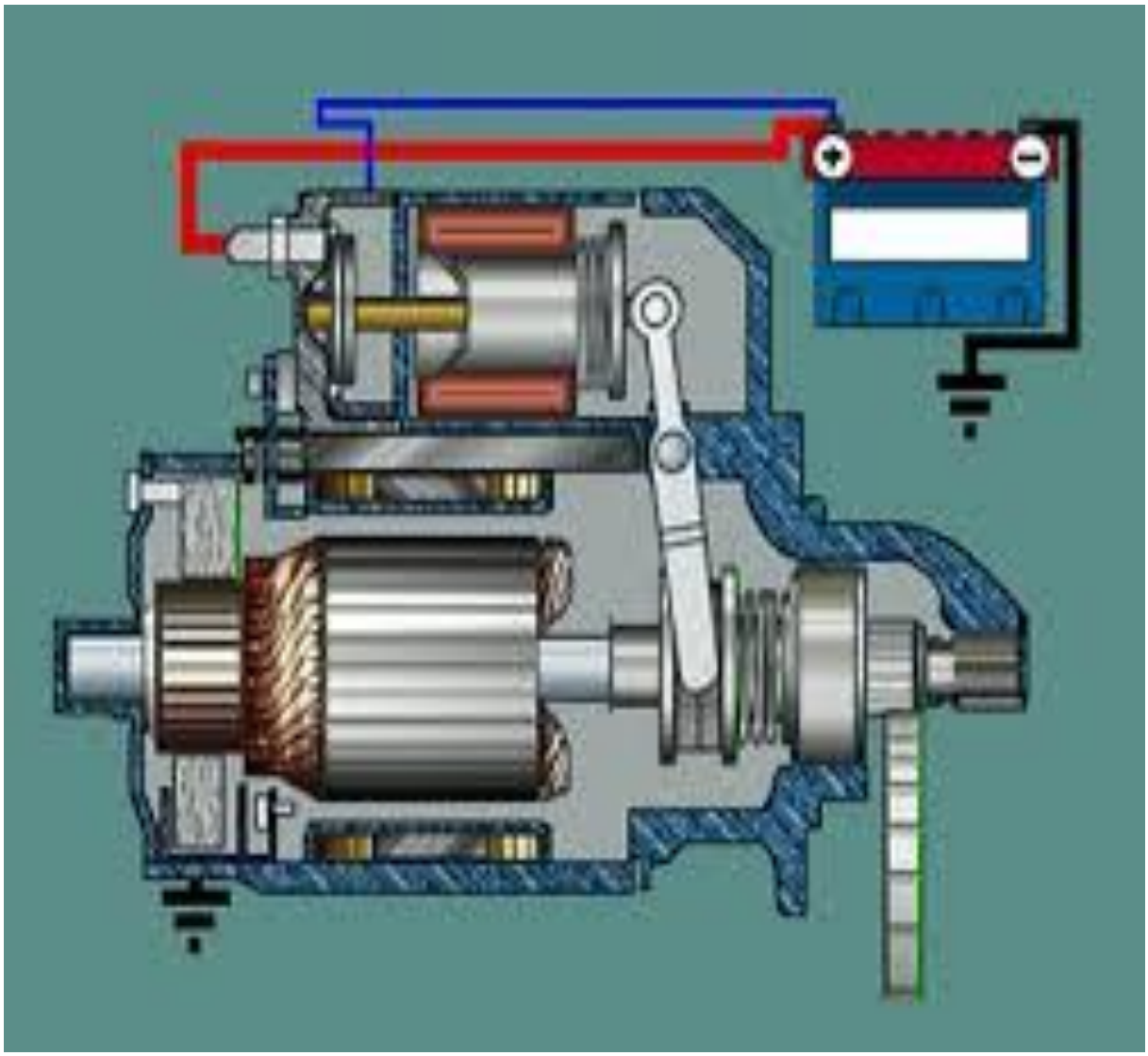


Fig: 3.19 Starter Motor Diagram [24]

CHAPTER IV

DEVELOPMENT PROCEDURE OF THE PROPOSED SAFETY CAR FEATURES

4.1 Design and construction

So far, in chapter three (3), we describe the basic system and other sub-system and the application provide by each to enable the system to work effectively. For now we will focus on how these features will be design and implemented and what is needed for this implementation. The password portion is left to a later section called the processing system.

4.2 Design

This system is design for a vehicle disabling which is use to prevent unauthorized users from initially operating a vehicle and to gradually decelerate and stop a vehicle in-transit under certain pre-determined conditions. These systems can be designed to be activated for specific situations, such as unauthorized access or use of a vehicle; loss of communication with a driver; discovery of security violations; vehicle entry into unauthorized areas; vehicle departure from predetermined routes; prevention of engine damage due to detected system failures; crisis or emergency situations; and mandatory maintenance needs.

4.3 Identification and Authentication

Access control is more than simply requiring usernames and passwords when users want to access resources. It can be much more. There are multiple methods, techniques, technologies, and models that can be implemented, there are different ways to administer controls, and there are a variety of attacks that are launched against many of these access control mechanisms. We cover it all. So get comfortable-this is an important chapter. Access controls exist to keep the bad guys out and to keep the good guys honest.

Companies need to ensure that unauthorized access is not allowed and that authorized users' cannot make improper modifications. The controls exist in a variety of forms, from passwords and ID badges to remote access authentication protocols and security guards. The tricky part is that they must be incorporated in a layered approach and that each layer needs to be understood,

along with its relationship to the other layers, to ensure that vulnerabilities are not overlooked or introduced and that different controls do not step on each other's toes.

4.3.1 Three Steps to Access Control

There are three important components of access control: identification, authentication, and authorization. *Identification* is the activity of the subject supplying information to identify itself to an authentication service. Some examples of identification mechanisms are username, account number, and memory card. *Authentication* is the second part of a credential set to verify the identity of the subject. These mechanisms could be passphrases, passwords, cryptographic keys, PIN numbers, or tokens. You may tell me your name, but I have no proof that you are who you say you are until you demonstrate the secret handshake. Only then will I be convinced of your identity. *Authorization* is the process of determining what this identified subject can actually access and what operations it can carry out. Authorization is based on some type of predefined criteria, which is enforced through access control lists, security labels, capabilities tables, or user profiles. These three components of access control usually work together in a synergetic relationship and can be found in applications, operating systems, firewalls, routers, databases, domain controllers, and more.

4.3.2 Authentication

Identification is usually providing a public piece of information (username, account number) and authentication is providing a private piece of information
(PIN number, passphrase, digital signature). Three important characteristics of the mechanisms that can be used for authentication are as follows:

- Subject must prove something he knows Example = password
- Subject must prove something he has Example = smart card
- Subject must prove something he is Example = fingerprint

If one mechanism providing one of these characteristics is used, it is referred to as *one-factor*; if two mechanisms are being used, it is *two-factor*; and you guessed it, an authentication process that requires all three is referred to as *three-factor*. For the authentication process to be

considered *strong authentication*, it must be at least two-factor User identification values should be unique to ensure accountability of individual activity. They should be non-descriptive of job functions to make them not as easily guessed and so that attackers will not know what type of account the credentials are tied to. There should also be secure and documented processes for issuing identification and authentication values and mechanisms to ensure standardization.

There are several mechanisms that can be used for authentication, each one with its own strengths and weaknesses. We take a look at the following items:

- Passwords
- Memory cards

4.4 Passwords

A *password* is a string of characters that should be different for each user and highly protected. It is something that a subject knows and is the most widely used authentication method in place today. The problem is that it is the most insecure mechanism when compared to other authentication technologies, because users and administrators do not usually practice the necessary disciplines required to provide a higher level of protection. Also, specialized utilities have been developed to uncover passwords and compromise this type of authentication method.

The following is a list of best practices that should be implemented and enforced as part of a company-wide password policy:

- Passwords should have at least eight characters (alphanumeric and symbols) and a combination of upper- and lowercase.
- Users should not be able to reuse the same passwords (password history).
- Systems should have a threshold (clipping level) configured that limits the number of unsuccessful logon attempts.
- An accurate audit log should be maintained that includes information about each logon attempt, which includes date, time, user ID, and workstation.
- The password lifetime should be short but practical.
- Passwords should not be shared.
- Passwords should not be easily guessable nor should they be dictionary words.

Passwords should never be stored in clear text; some type of encryption scheme, as in a one-way hashing method, should be used to ensure that passwords are not easily read. Servers that store passwords should have limited physical and logical access and should be highly protected.

Some companies choose to use password generators, which are software applications that create complex passwords for users instead of allowing them to come up with their own. Although this sounds like a great approach, many times the passwords that are created are too complex for the users to remember and they are quickly written down on yellow sticky notes that are then stuck to the monitor or secretly hidden underneath the keyboard. Writing down passwords and making them publicly available defeats the whole purpose of passwords and access control.

4.5 Attacks on Passwords

There are two types of attacks that are commonly used against passwords: dictionary and brute force attacks. *Dictionary attacks* are performed by software tools that contain hundreds or thousands of words that are commonly chosen as passwords. The attacker usually captures a hashed value of a password, or password file, and the tool then compares each of the words preloaded into the tool to the captured password until a match is uncovered.

Another type of attack on passwords is a *brute force* attack. In this attack type, a tool is used that tries every possible character and sequence of characters until the correct password is uncovered. So whereas a dictionary attack will attempt to match the password using a long list of words, a brute force attack will try and crack a password one character at a time.

Dictionary and brute force programs are not just used by evildoers. Oftentimes, systems administrators will use them to test the strength of users' passwords to enforce a set password policy. Because many useful tools reside on the Internet, or are accessible to the general public, attackers and security professionals are typically equipped with the same firepower. Security professionals simply need to be smarter and take more precautions to protect against these never-ending threats. The following are some countermeasures for password attacks:

- Do not allow passwords to be sent in clear text.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens.
- Rotate passwords on a frequent basis.
- Employ intrusion detection systems (IDS) to detect dictionary or brute force attacks.

• Use dictionary tools to find weak passwords chosen by users.
• Protect password files properly.

4.6 Cognitive Password

A *cognitive password* is based on fact or opinion used as the secret code, which is usually easier for a user to remember and is more difficult for an attacker to uncover. The user goes through an enrollment process by answering questions that typically deal with personal experiences and the answers to these questions are documented and used as cognitive passwords when the user needs to authenticate hem self at a later time. For example, when Chrissie calls a help desk for the first time, she is enrolled for proper authentication by being asked the following questions:

• What is your mother's maiden name?
• What is your dog's name?
• What city were you born in?
• What is your favorite color?

When Chrissie calls back to get assistance from the help desk at a later time, she is presented with one or more of these questions to prove her identity. Once the help desk person is convinced of her identification, he can move on to assisting Chrissie.

4.7 One-Time Password

A *one-time password* is a set of characters that can be used to prove a subject's identity one time and one time only. After the password is used, it is destroyed and no longer acceptable for authentication. If the password were obtained by an attacker as it was being transmitted, she would have a small window of time to try and use it and most likely it was already used once, thus it is useless to the attacker. This greatly reduces the vulnerability of someone sniffing network traffic, obtaining a password, and being able to successfully authenticate as an actual legitimate user. One-time passwords are usually generated and supplied to the user via a handheld device with an LCD display, referred to as *token device*. The user reads the password provided by the token device and enters it, along with a username, into a system for authentication purposes. The password is good for only that session and when the user needs to

authenticate again, another password is dynamically created. Token devices, also referred to as one-time password generators, are either synchronous or asynchronous.

Synchronous token devices are synchronized with an authentication service via clocking mechanism or by events. When a clocking mechanism is used, the token device and authenticating service agree upon a timing scheme. The token device presents encrypted time values to users, and they enter these values along with their usernames into their workstations, as shown in Figure 2-2. This credential set is sent to the authentication service. Because the token device and authentication service are synchronized, the authentication service is expecting a specific value to be submitted as the password. If the correct value is submitted, and it correlates with the given username, the user is successfully authenticated.

When *events* are used to establish authentication, the user is usually required to initiate the logon process, which tells the token device and authentication system to increment the one-time values. The token device and authentication system share the same list of values to be used for one-time passwords; the token device encrypts and presents the next value in the list to the user, which she enters as her password.

Asynchronous token devices use a challenge-response method to create one-time passwords

4.8 Memory Cards

A *memory card* is an authentication mechanism that holds user information within a magnetic strip and relies on a reader of some sort to process the information. The user inserts the card into the reader and then enters a set of credentials to be properly authenticated. An example of a memory card is an automated teller machine (ATM) card. The user inserts the ATM card into the ATM machine and then enters his or her PIN number. The card supplies the account number (user information) and then the user provides the secret code (PIN), together providing a credential set. Within companies, employees will often carry ID badges with magnetic strips.

In many of these implementations, a PIN is hashed and stored on the magnetic strip. In order to enter a building, the employee must enter a PIN number and swipe the badge through a reader. The reader hashes the inputted PIN number and compares it to the value on the card itself. If they match, access is granted.

4.9 Description of vehicle disabling system.

There are a number of types of vehicle disabling systems. Some utilize on-board electronics to immobilize the vehicle's engine or braking system to gradually decelerate a vehicle in transit or prevent its initial operation.

Others can be engaged remotely using a combination of on-board computers integrated with wireless communications; or non-remotely, utilizing technologies that the driver, operator, or, in some instances, the vehicle itself could execute locally. The systems can be activated manually or automatically based on pre-programmed security conditions.

Fig: 4.1 Remote vehicle disabling systems [21]

Remote vehicle disabling systems typically rely on a wireless communication system to provide their basic functionality. They can be integrated with panic buttons and on-board computers requiring user identification and/or password log-ins. For non-remote systems, a keypad or key-

fob may be utilized as a part of these systems for arming, disarming, and controlling the security system at the asset itself. Non-remote manual systems can also involve the use of in-cab shut-off devices to other vehicle systems, such as electronic ignitions and air brakes.

4.10 Remote Vehicle Disabling Systems

Remote vehicle disabling systems provide authorized users at remote locations the ability to prevent an engine from starting, prevent movement of a vehicle, and to stop or slow an operating vehicle. Remote disabling allows a dispatcher or other authorized personnel to gradually decelerate a vehicle by downshifting, limiting the throttle capability, or bleeding air from the braking system from a remote location. Some of these systems provide advance notification to the driver that the vehicle disabling is about to occur. After stopping a vehicle, some systems will lock the vehicle's brakes or will not allow the vehicle's engine to be restarted within a certain timeframe. Remote disabling systems can also be integrated into a remote panic and emergency notification system. In an emergency, a driver can send an emergency alert by pressing a panic button on the dashboard, or by using a key-fob panic button if the driver is within close proximity of the truck.

Then, the carrier or other approved organization can be remotely alerted to allow a dispatcher or other authorized personnel to evaluate the situation, communicate with the driver, and/or potentially disable the vehicle.

Fig: 4.2 Remote vehicle disabling systems Equipment's [21]

4.11 Non-Remote Vehicle Disabling Systems

Non-remote vehicle disabling systems provide authorized users the ability to restrict or prevent vehicle operation in three ways: through the use of wireless technology when they are near the vehicle; through on-board actions by the driver/operator; or through a combination of both. Non-remote vehicle disabling systems include driver identification authentication technologies, tamper detection alerts, brake locks, and emergency notification panic buttons for disabling the truck in case of an emergency or other event.

A single sign-on module is utilized for driver authentication in order to initiate the operation of a vehicle. The driver uses passwords, pin numbers, or biometrics to start the vehicle and to access other on-board wireless communications applications. All activities related to the use of the vehicle are associated with the driver signed-in at the time. This information can be used for dispatch, driver performance, and driver log purposes.

Several different types of technologies can be used to non-remotely disable a vehicle. Panic buttons carried by the driver or within reach of the driver inside the vehicle can be activated to disable a vehicle or send out an emergency notification. Electronic ignition systems allow the driver to automatically activate the system when the key is removed from the ignition and reactivate the system when the key is replaced into the ignition. A relatively low-cost means of vehicle disabling is the utilization of a brake lock device to prevent the movement of the vehicle. A brake lock device shuts down the air line from the tractor to the air brakes in the tractor (and if hooked up, to the trailer). Release of the brake lock system is the only way to move the vehicle.

4.12 Application of vehicle disabling system.

Important components of vehicle disabling systems are hardware mechanisms that restrict vehicle use. Some are on-board computer technologies that identify the driver to allow authorized use while preventing unauthorized use. Others utilize mobile communication technologies that allow a remote dispatcher or other operator to communicate with the driver and/or the vehicle, and if necessary, activate the vehicle disabling system.

Driver authentication is a vital part of many vehicle disabling systems. Intelligent on-board computers can be utilized for driver identification through global login access where a driver enters login information into a cab-based interface. Similar to a username and password on a

computer system, global login is an authentication feature of some wireless communications systems. Through the use of a driver login process, the login information (user ID and password) entered into the truck-based interface by the driver is verified by preset procedures both locally on the vehicle and over the air using the wireless communication system. If this verification fails, various configurable alerts and resulting actions can be triggered up to and including vehicle disabling with the aid of an on-board computer.

Fig: 4.3 On-board remote control [21]

Other authentication technologies utilized in several vehicle disabling systems range from PIN number entry to biometric-based systems. The most common biometric-based technologies for vehicle disabling utilize driver fingerprints. If the driver's fingerprint matches the fingerprint information on a biometric smart card carried by the driver, then the driver is verified and able to start the vehicle. If a match is not made, the vehicle cannot be started and the fleet dispatcher is typically notified of the failed attempt.

Vehicle disabling systems can be integrated with many on-board wireless communications systems that include other features, such as door sensors, cargo sensors, temperature sensors, electronic cargo seals, and trailer connection and disconnection systems. For example, if an on-board computer system detects a loss of signal from the communication network or tampering of electronic cargo seals, a pre-determined vehicle disabling protocol can be initiated.

Additional monitoring processes using on-board sensors that detect changes in load volume, door status, exposure to radiation, or temperature can a generate security alert notification that will trigger a vehicle disabling protocol. In vehicles that monitor trailer information, a vehicle

disabling protocol can be prompted when a trailer has been disconnected from its assigned tractor or when a trailer door lock system has been violated.

Vehicle disabling protocols can also be activated by critical changes in the status of important vehicle systems. Since on-board computers monitor processes such as coolant temperature and engine oil pressure, a message can be sent to the driver and dispatcher about these conditions alerting them that systems are at unsafe levels. Then, a vehicle can be prevented from starting if unsafe system parameters are discovered prior to vehicle usage. Carriers with refrigerated units (reefers) are significant users of this feature.

Vehicle disabling can be utilized by authorized personnel with a wireless communication system's geo-fencing feature. Dispatchers or fleet operators can create a geo-fence or defined electronic boundary made up of geo-coded points for particular vehicles or routes. If a vehicle enters a restricted geo-fenced area, or exits the defined areas, the dispatcher or fleet operator can be alerted to take necessary actions to secure the vehicle. Currently, no systems have the capability of engaging automatic vehicle disablement for geo-fence violations.

4.13 Remote Car Starters

Some remote car starters can be controlled by a smartphone app. Some newer vehicles roll right off the factory line with remote start functionality, and the benefits of this feature are easy to see. By warming up the engine before you ever get in the car, you ensure that the oxygen sensor is all heated up and the emission controls are working at peak efficiency from the moment you back out of your driveway. And aside from that, you can also slide into a pre-warmed passenger compartment on those cold winter mornings, and enjoy a burst of cold air before setting out on a long summer commute through stop and go traffic.

While OEM remote car starters are relatively new, these devices have been available through the aftermarket for a long time. Often paired with car alarms, keyless entry systems, and other similar devices, they are also available as standalone units

Fig: 4.4 remote car starters using a smartphone app. [24]

4.14 How Do Remote Starters Work?

Remote car starters are devices that allow a vehicle to be started up without requiring either the driver or the key to be physically present. This is accomplished through a component that is connected to the ignition system and fitted with a radio receiver. When that component receives a signal from a paired transmitter, which typically takes the form of a key fob, it activates the starter motor. Since a remote car starter just simulates the same action that takes place when you turn the ignition key, these systems have a few limitations. One is that they typically don't work very well with carbureted vehicles. Special carburetor kits are available for some remote starters, but these kits usually won't do the trick for particularly temperamental vehicles that require a lot of fiddling with the gas or choke. If a vehicle requires manual intervention, such as a tap of the gas pedal to drop off high idle, that can also cause issues.

Newer vehicles that ship from the factory with built-in anti-theft measures can also cause issues. These vehicles typically require some type of bypass component in order for the remote starter to work without a key in the ignition.

4.14.1 Additional Remote Car Starter Features

In addition to simply starting a vehicle remotely, some remote car starters offer a variety of other features and integration with other related devices. Some common features include:

- 2-way remotes
- keyless entry
- starter disconnect
- car alarm/security integration
- remote dome light activation
- control via smartphone app
- car finder
- auxiliary remote outputs

4.14.2 Way Remote Controls

Basic remote car starters use a simple transmitter/receiver setup, which allows you to start your vehicle with the press of a button. In systems that use 2-way remotes, the remote control can both send and receive information. That allows the remote to display information like the interior temperature of the vehicle, which can be invaluable if you're waiting to go out until it warms up or cools down to a comfortable level

4.14.3 Starter Disconnect

Since a remote car starter has to be hooked into an ignition system to work, some of these devices also have the ability to shut the ignition system down. If the starter disconnect feature is activated, it will typically prevent the vehicle from being hotwired. Some remote car starters also have even more advanced features that can be activated if a vehicle is stolen or carjacked, which typically sets the alarm off and then disconnects the starter after the vehicle is shut off.

4.14.4 Smartphone Apps

Remote car starters typically come with one or more remote controls that are designed to also act as key fobs, but some of these systems can also be operated via a smartphone app. These systems

are often 2-way as well, which allows the smartphone to display a variety of information transmitted by the remote starter system.

4.15 Security System Integration and Auxiliary Outputs

Some car security systems have built-in remote starters, and some remote starters include auxiliary outputs that allow alarms and other devices to be hooked up later on.

4.16 Operations and Benefits

Depending on the actual vehicle disabling technologies utilized, fleet operators can have additional connectivity and communication with their drivers and vehicles compared with fleets not utilizing such technologies. When vehicle disabling systems are integrated with on-board communications and tracking systems, fleet managers can actively monitor security parameters, vehicle routes, performance, maintenance, and fuel usage? Whether the vehicles are running locally or on a long-haul. These monitoring capabilities provide operational efficiency benefits for fleet management optimization by providing information about vehicle operation from origin to destination. Vehicle disabling systems can improve secure operations of carriers who haul high-value or high-risk cargo, such as hazardous materials. Access can be limited to authorized drivers by dispatchers or fleet managers who can manage driver authentication codes and truck identifications, change codes over the air, and disable the vehicle, if necessary.

To help prevent theft, a valid driver authentication code can be required before a vehicle can be started or moved. Also, if there is tampering with any integrated security device or fleet management system, the vehicle can be placed in a secure state and an alert can be sent over the air to the carrier. Carriers can also change driver authentication codes and secure a vehicle if a driver suddenly leaves the destination, but still has access to the vehicle. The capability to disable the vehicle over the air is also available if dispatchers become aware of a stolen or hijacked vehicle. Even if a car is moving, the vehicle's speed can be gradually reduced to allow the vehicle to be brought to a safe and controlled stop. Technologies, such as ignition locks and brake locks can also be used to minimize vehicle theft by prohibiting vehicle movement. These security devices are permanently installed in the vehicle, and they must be utilized in order to operate the vehicle.

4.17 Remote control activated Process

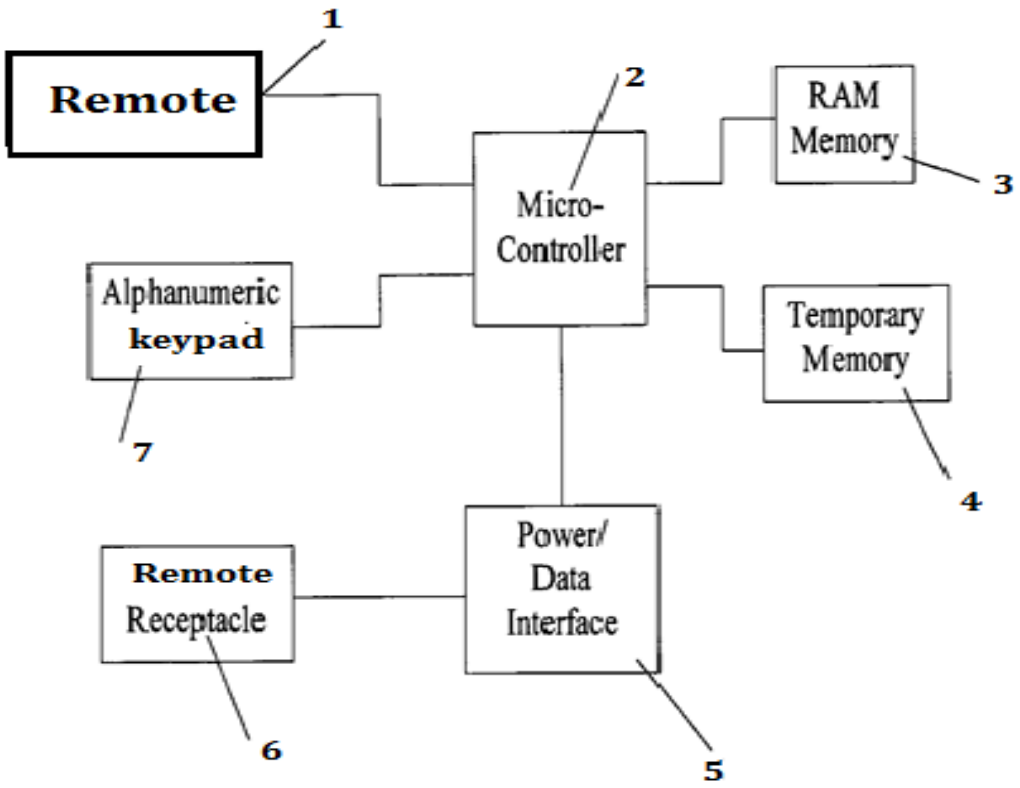


FIG: 4.5 Remote Control Programming Device

FIG, illustrates a separate remote control programming device or system which is used to initialize data stored in the remote or changes in the data as or when required. The programming device is not required by the authorized vehicle user in everyday operation; therefore, it could be used at a central programming location such as by an automobile dealer, locksmith or remote control retailer. Security of the programming operation can be maintained through a combination of measures such as by controlled production and distribution of serially numbered programmers, a dealer or operator Personal Identification Number (PIN), a valid programmer passwords identification to enable operation of the remote programming device, and the vehicle user passwords of previously programmed vehicle owner. The remote programmer contains a microprocessor or microcontroller 2, a random access memory (RAM) 3, a keypad 7 for input of alphanumeric data, an identification password 1 for validating the programmer operator and for

entering data on new authorized users of the intelligent remote control, a remote receptacle 6 for inserting an identification password to program, a power/data interface 5 to interface with the remote, and a temporary memory 4 which stores user data during programming but is erased after remote programming. The only fingerprint data which is maintained in the programmer is the data for an authorized programming operator as long as it remains valid for a particular operator. The operator data can be changed only when additional factors are entered such as a PIN number, an authorized dealer PIN number, an authorized password of a programming operator, etc. Some embodiments of the present invention may include a portable programming device to be used by the vehicle owner for limited programming of certain options available to the owner exclusive of making a new password such as programming a new authorized user, or limiting authorized access to the automobile. For example, a parent might want to restrict the authorized hours of access that a child has access to the automobile. Other embodiments of the subject invention might include an input/output device permanently connected to the remote controller, such as on the dashboard, for the purpose of limited programming of certain options available to the owner exclusive of making a new (PIN).

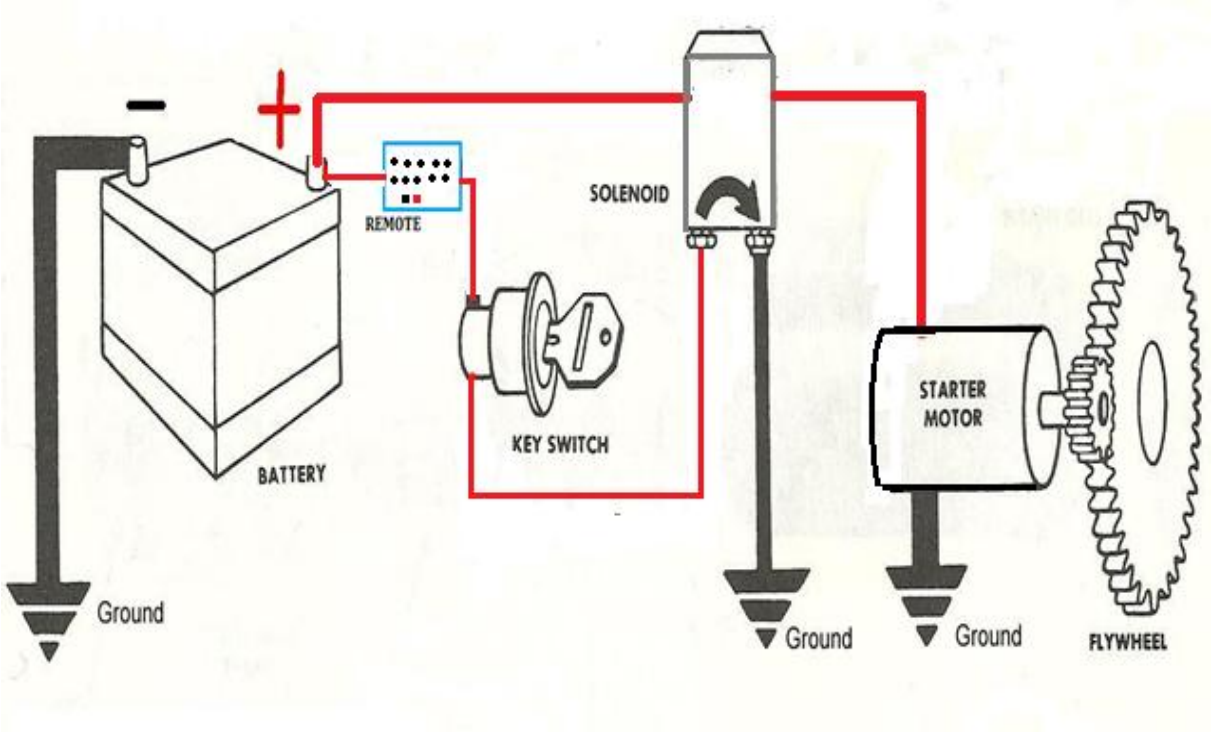


Fig: 4.6 Interfacing Process sequence for Remote-Vehicle-Starter System

The remote operated from 12V. The main unit provides an excitation coil for your car's spare smart key so that the unit can disable the car's security system when you start it remotely. The 400-foot range sounds nice, but this unit works only on automatic-transmission cars built after 1982.

Fig: 4.7 Excitation coil unit [24]

1. This large copper winding excites a spare car key that you clamp in the foam holder. It allows the system to excite the key and turn off your car alarm.
2. Two large and five small relays interface with the car's starting circuits. You can't beat a relay for isolation or low on-resistance, as well as low cost. The relay manufacturer is a Chinese company, Sanyou, not Sanyo of Japan.
3. An 8-bit 46R0662 Holtek microprocessor with ADCs, in a 44-pin QFP, controls the system.

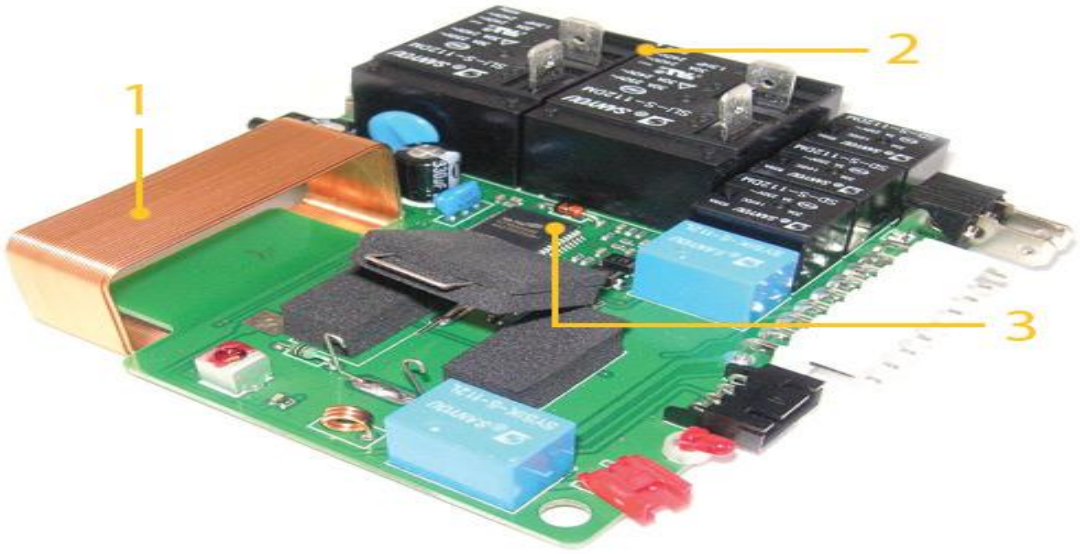


Fig: 4.8 Printed-circuit board [24]

4. Parts reside on both sides of the PCB (printed-circuit board). They include a Texas Instruments relay driver and National Semiconductor op amps.

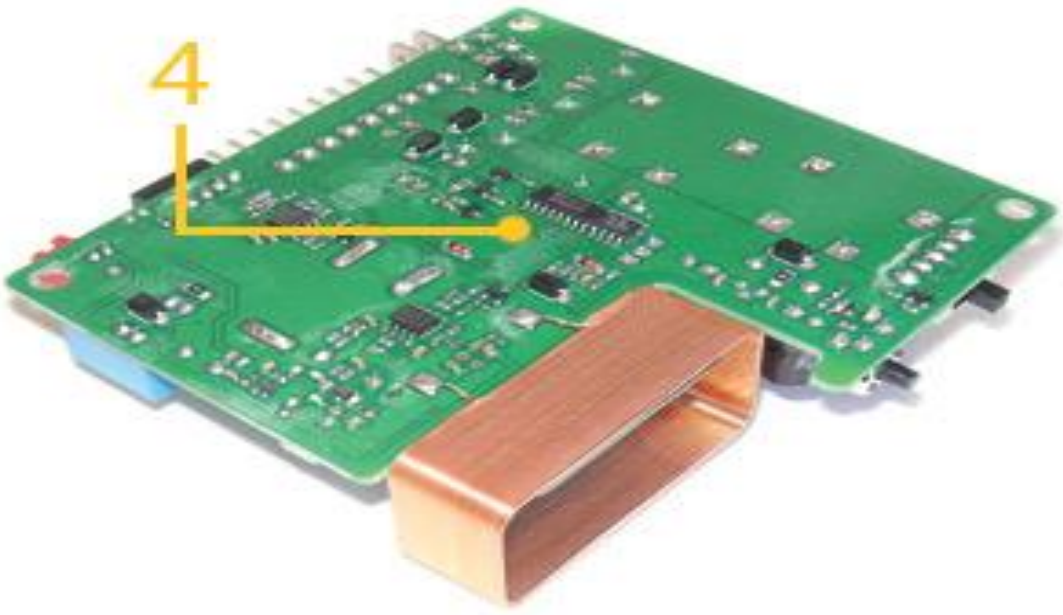


Fig: 4.9 Printed-circuit board [24]

5. A double-sided PCB has parts on one side only. A 20-bit Zhengxin Microelectronics LX-2240B remote-control encoder IC holds 1 million codes. You apply the 12V battery to the chip when you press either button. The RF amplifier is an NPN transistor with a crystal tank circuit.

Fig: 4.10 remote-control encoder [24]

4.18 Coil-ignition System

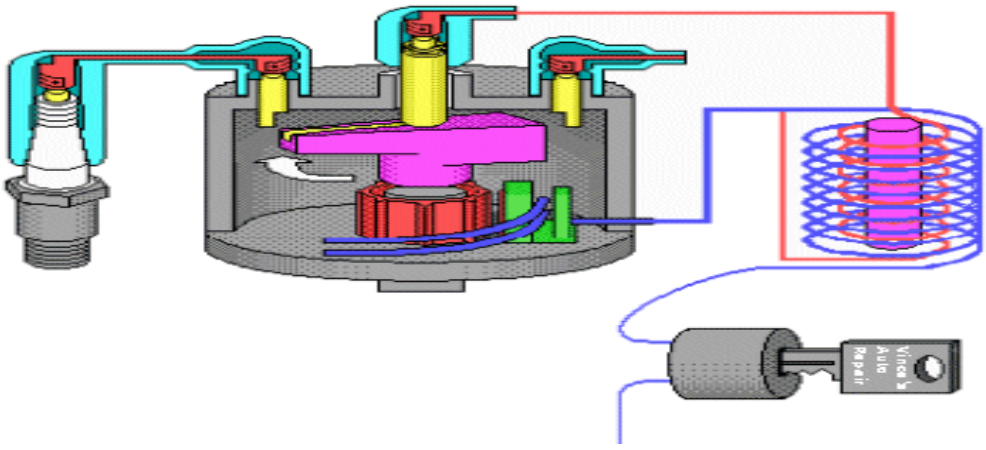


Fig: 4.11 coil-ignition system [25]

In 1908 the battery-inductive **ignition system** was introduced by C.F. Kettering of Delco, but only in the mid-1920s it could achieve its commercial status as a successor to the magneto. Up to that time very few vehicles used a battery, hence the magneto was common being a self-contained **ignition** generator. With the introduction of electric lighting, use of a battery becomes necessary. Because of this as well as the difficulty in starting of the magneto-ignited engine, the battery inductive **system** commonly known as coil **ignition** was introduced.

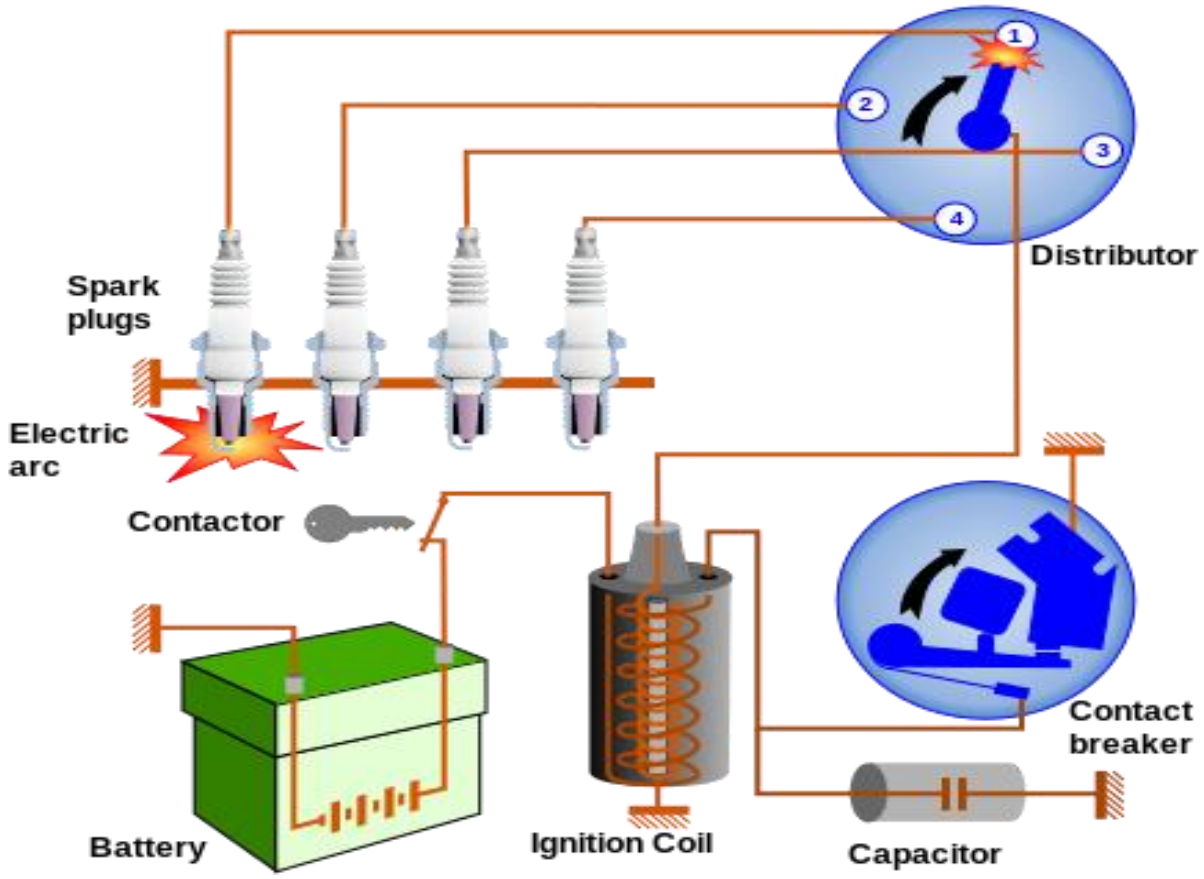


Fig: 4.12 jump-spark system used in internal combustion engine [25]

The jump-spark **system** used today in the internal combustion engine has been gradually developed through the stages of hot wire, break spark trembler coil, with each step showing a definite improvement over its predecessor. The two jump-spark **ignition** generator **systems** in use today are the battery-coil and the magneto, the latter is confined mainly to the small engines used on motor cycles and lawn mowers.

CHAPTER V
CONCLUSIONS AND RECOMMENDATIONS

This chapter highlights the goals that were accomplished in current project. A summary of the overall results is covered in the conclusion, some suggestions for future research direction are recommended to improve more realistic design for the current production.

5.1 Conclusions

The development of innovative self-Authentication Code for Automobile Security system; is an improvement upon the Biometric finger-print anti-theft device. The biometric finger-print device is applied to encode the car security system by using Key or Keyless ignition device which will not allowed the unauthorized person, Unless authorized finger-print recognition is initialed. Any unauthorized persons who gain entry to your vehicle without your permission will set off the quick alarming function. The settings are guided by the master driver through the password controller by hand instruction. It happens that cars are been stalled rampantly, carjacking are becoming more frequent.

Carjacking is a significant problem in the world, after every 26 seconds car is stolen and some cases of carjacking occurred. Where it is called *hijacking*; there are some road signs warning people that certain areas are hotspots. There were 5,184,000 carjacking in 1998 and 16,000 cases of carjacking in South-Africa (18 times the American rate per capita), and 60 murders a year resulting from these.

In this new technology we intend to introduce a more advanced solution to the problems of car stolen and frequent carjacking. The modern technology provides authorized users the ability to restrict or prevent vehicle operation: through the use of an emergency notification panic buttons for disabling the vehicle in case of emergency.

The disabling systems can also be integrated in to a remote panic and emergency notification system whenever a vehicle is highjack a driver can press a panic buttons hide by this side and in this situation it is only a programmed and authorized passwords of the owner can de-activated the system and potentially start the vehicle to allow the departure. In order to reduce the cost for the construction of this security device a remote disabling systems can also be integrated into a remote panic buttons to provide authorized users at a remote locations the ability to prevent an engine from starting, preventing movement of the vehicle and to stop or slow an operating vehicle. The driver uses passwords, pin numbers ranging from one to four (4) digits to start the vehicle. All activities related to the use of the vehicle are associated with the driver signed-in at the time. This information can be used for driver performance and driver log purposes. The driver Authentication is vital part of many vehicle disabling systems. Through the use of a driver login process, the login information (4 digits pin password) entered into the remote controller that consist of 10 digit keypad members.

5.2 Recommendations

This project addressed the current situation of the car security system across the world and in inventory design is proposed for finding its optimal ordering policy under certain assumption to reduce the rampant carjacking or car stolen. The future scope of this research is to overcome the assumption and make the design more realistic comparing to the real industrial design of the car security system in the world. Therefore there is large scope for further research. The extended research can be in different direction.

CHAPTER VI

REFERENCES

1. Marcello Malpighi [1686] an anatomy professor at the University of Bologna, noted fingerprint ridges, spirals and loops in his treatise.
2. John Evangelist Purkinje [1823] anatomy professor at the University of Breslau, published his thesis discussing nine fingerprint patterns, but he too made no mention of the value of fingerprints for personal identification.
3. William James Herschel [1858] the English first began using fingerprints when he was Chief Magistrate of the Hooghly district in Jungipoor, India.
4. P j Coulier, V D -Grâce [1863] published his observations that (latent) fingerprints can be developed on paper by iodine fuming.
5. Dr. Henry Faulds [1870] the British Surgeon-Superintendent of Tsukiji Hospital in Tokyo, Japan, took up the study of skin-furrows.
6. H. Faulds [1880] published an article in the Scientific Journal, "Nature" (nature).
7. Gilbert Thompson [1882] of the U.S. Geological Survey in New Mexico, used his own thumb print on a document to help prevent forgery
8. Alphonse Bertillon [1882] a Clerk in the Prefecture of Police of at Paris, France, devised a system of classification, known as Anthropometry or the Bertillon system.
    A. Bertillon [1888] was made Chief of the newly created Department of Judicial Identity where he used anthropometry as the primary means of identification.
9. Samuel L. Clemens [1883] Mark Twain's book, "Life on the Mississippi, a murderer was identified by the use of fingerprint identification. In a later book, Pudd'n Head Wilson.
10. Sir Francis Galton [1888] a British anthropologist and a cousin of Charles Darwin, began his observations of fingerprints as a means of identification.
11. Juan Vucetich [1891] an Argentine Police Official, began the first fingerprint files based on Galton pattern types
12. Juan Vucetich [1892] made the first criminal fingerprint identification

13. The Council of the Governor General of India [1897] approved a committee report that fingerprints should be used for classification of criminal records.
14. Henry [1900] the United Kingdom Home Secretary Office conducted an inquiry into Identification of Criminals by Measurement and Fingerprints
15. The New York State Prison system began [1903] the first systematic use of fingerprints in the U.S. for criminals.
16. The use of fingerprints began [1904] in Leavenworth Federal Penitentiary in Kansas, and the St. Louis Police Department.
17. U.S. Army [1905] begins using fingerprints. U.S. Department of Justice forms the Bureau of Criminal Identification in Washington, DC to provide a centralized reference collection of fingerprint cards.
18. The New Orleans, Louisiana [1977] delegates to the 62nd Annual Conference of the International Association for Identification (IAI) voted to establish the world's first certification program for fingerprint experts.
19. The Unique Identification Authority of India [2013] operates the world's largest fingerprint (multi-modal biometric) system, with over 200 million fingerprint, face and iris biometric records.
20. Nero-technology [1998] developed VeriFinger, a fingerprint identification algorithm, designed for biometric system integrators.
21. Benjamin C.KUO, Automatic Control Systems. The Edition (1995) prentice hall, Englewood cliffs, NJ USA.
22. J.A Dolan, motor vehicle technology and practical work Part 1& 2. 1st Edition. The English language book society (1983).
23. R.B.Gupta, Automobile Engineering. 7th Edition, tech India publication series (2012).
24. W.H Crouse & D.L.Anglin, Automotive mechanics 10th Edition Tata MCGraw hill Education private limited New Delhi. (2010).