



International Journal of Intellectual Advancements and Research in Engineering Computations

Bike security based on fingerprint authentication with one time password

**Mr.G.Pradeepkumar¹, Depak Sailenthira kumar.G², Dhivya.M², Methon
Sarravanan.M.G², Naveen.R²**

¹Asst.Professor, Department of ECE, Nandha Engineering College, Erode-52.

²UG Scholars, Department of ECE, Nandha Engineering College, Erode-52.

ABSTRACT

In modern days a vehicle anti-theft system is of prime importance. Currently public having an own vehicle, theft is finding on parking and sometimes during insecurity places. The safe of vehicle is extremely essential for public vehicles. The first layer of protection in the system is a Fingerprint recognition, based on which the locks are opened. The Fingerprint matching is done by utilizing the minutiae based Fingerprint recognition scheme. The vehicle is unlocked only with the bike key. One turned on the user should keep them finger to the fingerprint sensor. If the finger ridges matched, then the bike gets started. If fingerprint matching fails means our system generates an OTP and then a message is sending to the user by using GSM [Global System for Mobile Communication]. Then that OTP is used to start the vehicle which is enter by the use of keypad.

INTRODUCTION

Automation is the use of control system for handling different processes and machineries to replace human efforts. Automated system use complex algorithm which increase the cost of design and power consumed. But this not only reduced manual effort but also time management and provide high productivity. In various research, mostly product developers have used color sensor detecting color. Sometimes, sensor creates complexity. Thus, this method is a new attempt to detect color by image processing.

The traditional authentication systems are based on cryptographic system and security protocol, such as static password, one-time password (OTP), digital certificate, hardware devices and so on. The static password authentication system is easy to use but it cannot provide sufficient accessing security due to its vulnerability to attacks, such as guessing attack, replay attack, password leakage, and exhaustive attack [3]. The authentication system based on

digital certificate provides high security with high complexity to prevent its perform ability [4]. The authentication system based on a hardware device can provide a very high level of security, but it is not suitable for identity authentication of mobile terminals because it is not portable and it requires additional hardware, whose cost is usually high. Different from the above schemes, OTP authentication scheme can provide high secure level with acceptable implementation complexity. Moreover, the passwords of OTP authentication scheme are used only once and then thrown away. Hence, an OTP authentication scheme may be a viable development alternative to the mobile communication system. Lamppost primitively proposed an OTP authentication scheme based on a hash chain. Later, Haller polished it to the S/KEY standard. Subsequently, many researchers proposed other improved OTP authentication schemes for enhancing the security via increasing the efficiency or decreasing the cost [2, 3, 5–9]. However, most of these existing OTP authentication schemes are developed based on the

PC platform and are still too complex to implement under mobile terminals. Besides, they do not satisfy anonymity, nor are they resistant to the cloning attack. Therefore, it is necessary to

Color is one of the most important characteristics of an image, if color in a live video or in a digital image can be detected, then the results of this detection can be used in various industrial and scientific applications. Color detection is the fundamental step in many computer vision systems. In this paper Image Processing toolbox in MATLAB is used for detection of a particular color in a given image. Image Processing Toolbox provides wide variety of referenced algorithms, methods and applications for image processing, visualization and segmentation. MATLAB based Image Processing is well suited and most commonly used platform for implementation of an image-based algorithm. An image is a matrix of pixel values. MATLAB takes every input as a matrix that is why, it is most commonly used platform for image processing. An image can be represented using many color models like gray-scale, RGB, HSV etc. Here RGB model is used to detect the colors in an image. RGB model is a color model in which red, green and blue lights are added together in various ways to produce wide range of colors. In RGB model image is composed of a matrix of $M \times N \times 3$ pixels with M rows and N columns of pixels for each red, green and blue color components of an image. The RGB model uses 8 bits for representation of red, green and blue color components of an image. Since in an RGB model image is represented in the form of a matrix, mathematical operations on the image can be applied to detect a particular color in an image.

RELATED WORK

Human identification is field very significant and which has undergone rapid changes with time. An important and very reliable human identification method is fingerprint identification. Fingerprint of every person is unique. So, this helps in identifying a person or in improving security of a system. Finger print of a person is "read" by a special type of sensor. Finger print sensor can be interfaced with a microcontroller.

design lightweight, simple and secure identity authentication schemes for the mobile terminal communication system with abilities against the cloning attack.

Through keypad we can add new user and delete the existing user, also identify the user by selecting corresponding option through keypad. In this paper we use a fingerprint module to read once identity to start the equipment. For this we use a microcontroller to enable the ignition system if the matching between scanned data and the already existing data is correct. Comparison is done inside the fingerprint module itself and its output is given to microcontroller. Result is displayed in an LCD display whether the user is authorised or not. The sensor used is FIM 3030 by NITGEN. Microcontroller used is AT89c52. AT89c52 is a low power, high power CMOS 8-bit microcontroller. It consists of 32 I/O lines. The other main components are the decoder and the latch. The decoder used is DM74LS138 whereas the latch used is 74HC373.

In this modern technology, Fingerprinting is more authentic tool used for security basis. Fingerprint of every person is unique, so the identification or authorization of a person becomes more and more reliable. This lead to an enhancement of the security in starting of the Engine. Biometrics' authentication is used in computer science as a form of identification and access control. Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyzes human body characteristics, such as DNA, fingerprints and other recognition pattern. The special type of a sensor is used to read the fingerprint of a person and matches the data by comparing it with the authorized fingerprint image, which is stored in the database. If the match is found, then the vehicles will be started. In this project, digital image processing algorithms is employed to identify whether the incoming fingerprint image is genuine or forgery.

Car and light van thefts are increasing alarmingly around the world and new guidelines driven by the insurance companies, are being set for vehicle manufacturers to make their products more secure. POLLUX has been developed as a

vehicle guard against theft and alarm system, this security system based upon machine vision technology adds a new level of theft protection to vehicle security systems in a manner that does not intrude the drivers. It is based on hardware system, for real time acquisition of driver's images using an active IR illuminator. This system can locate and recognize the driver's face, identify the unauthorized driver. When the unauthorized driver is driving, POLLUX will alarm and send the unauthorized driver's image to car owner or police through CDMA or GPRS networks. The system was tested in a simulating environment with subjects of different ages, with/without glasses, and under different illumination conditions, and it was found very robust, reliable.

PROPOSED SCHEME

The data acquisition component acquires the biometric data in digital format by using a sensor. The second and third components of the system are optional, based on the system's storage requirements. The fourth component employs a feature extraction algorithm to produce a feature vector whose components are numerical characterizations of the underlying biometrics. The fifth component of the system is the matcher which

compares feature vectors to produce a score which indicates the degree of similarity between the pair of biometrics data under consideration. The sixth component of the system is a decision-maker that can be programmed to accommodate system specifications. Fingerprints are made of a series of ridges and furrows on the surface of the finger and have a core around which patterns like swirls, loops, or arches are curved to ensure that each print is unique. An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger. The ridges and furrows are characterized by irregularities known as minutiae, the distinctive feature upon which finger scanning technologies are based. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

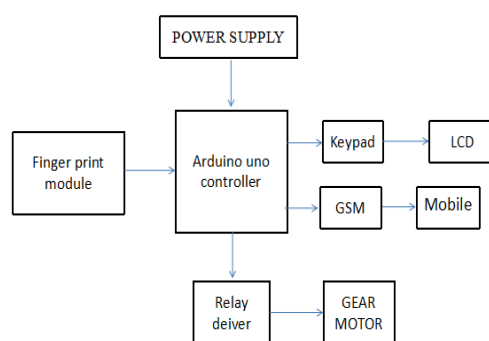


Figure 3.1 Block diagram of proposed method

A sensor takes a mathematical snapshot of the user's unique pattern, which is then saved in a fingerprint database. A fingerprint enhancement algorithm (that uses Gabor filters as band-pass filters to remove the noise and preserve true ridge/valley structures) is included in the minutiae extraction module to ensure that the performance

of the system is not affected by variations in quality of fingerprint images. From an extensive research of available literature, it was found that software based on competing matching algorithms had been developed and were available as freeware. Most of them were built upon a common MATLAB based platform by picking up m-files

from an open source and integrating them according to the algorithm that they desired to implement. Two such software – one based on the traditional Minutiae-Matching Algorithm developed at the Hong Kong Baptist University, and the other a hybrid of the former and a novel Gabor-filter bank technique developed at the Michigan State University in the USA – were downloaded and compared against a common database. The proposed methodology contains step down transformer, which is used to convert 230V to 5V (AC). Then the current enters into the rectified circuit, which is used to convert the alternating current into direct current (DC). Now the entire circuit drives at 5V dc supply. In Arduino UNO, digital pins are connected to the LCD and Fingerprint sensor and the Analog pins are connected to the GSM, relay and push-buttons. Relay allows the DC motor to run.

SCHEME ANALYSIS

In modern days a vehicle anti-theft system is of prime importance. Currently public having an own vehicle, theft is finding on parking and sometimes during insecurity places. The safe of vehicle is extremely essential for public vehicles. The first layer of protection in the system is a Fingerprint recognition, based on which the locks are opened. The Fingerprint matching is done by utilizing the minutiae-based Fingerprint recognition scheme. The vehicle is unlocked only with the bike key. One turned on the user should keep their finger to the fingerprint sensor. If the finger ridges matched, then the bike gets started. If fingerprint matching fails means our system generates a OTP and then a message is sending to the user by using GSM [Global System for Mobile Communication]. Then that OTP is used to start the vehicle which is entered by the use of keypad.

In this project, it contains step down transformer. It is used to convert 230V to 5V (AC). This current enters into the rectified circuit. This is used to convert the alternating current into direct current (DC). Now the entire circuit drives at 5V dc supply. In Arduino UNO, digital pins are

connected to the LCD and Fingerprint sensor and the Analog pins are connected to the GSM, relay and push-buttons. Relay allows the DC motor to run.

In future, if anyone touched our bike means, an alert message would come to the registered mobile number. In this project, by adding GPS, it will denote where the bike is currently running. If the owner of the bike forgets the parked place means, it will be helpful to him. With the help of GSM, it sends the current location to the owner's mobile number. If someone of our friend took our bike means, the owner can also possibly monitor the bike.

CONCLUSION

Fingerprint Recognition was the first biometric approach to verify the person by downloading the images of sample in the database. The image is first analyzed and then identified, extracted and stored the images in the file of database. For the identification process, first it compares the query image against with the image stored in the database and then it is verified. From the above result, it has been cleared that the use of the biometric system offers the better and more reliable resultant. Moreover, it is restricting the starting of the vehicles by unauthorized user. Only the fingerprint image verified has this ability to access the engine of the vehicle. In this paper, the proposed scheme can lighten the user's burden of ID memory and provide mutual authentication between the mobile terminal and server. It also satisfies the anonymity of mobile terminal. Theoretical analysis and verification show that the proposed scheme is not only secure but also simple, efficient and flexible, especially independent of trusted-party. In addition, our scheme could resist the cloning attack, replay attack, small integer attack, impersonating attack, system crash attack, and exhaustive attack and guessing attack. Thus, the fingerprinting recognition which is the branch of image processing is used with our implementation of providing maximum security to bikes.

REFERENCES

- [1]. Eldefrawy, M.H., Khan, M.K., Alghathbar, K.: ‘One-time password system with infinite nested hash chains’. Security Technology, Disaster Recovery and Business Continuity – Int. Conf., Jeju Island, South Korea, December 2010, 161–170.
- [2]. Gong, L.Y., Pan, J.X., Liu, B.B., et al.: ‘A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords’, J. Comput. Syst. Sci., 79(1), 2013, 122–130.
- [3]. Lamport, L.: ‘Password authentication with insecure communication’, Commun. ACM, 24(11), 1981, 70–772.
- [4]. Li, F.G., Hong, J.J., Omala, A.A.: ‘Efficient certificateless access control for industrial internet of things’, Future Gener. Comput. Syst., 76(11), 2017, 285–292.
- [5]. Mahmood, K., Chaudhry, S.A., Naqvi, H., et al.: ‘A lightweight message authentication scheme for smart grid communications in power sector’, Comput. Electr. Eng., 52(5), 2016, 114–124.
- [6]. RFC1760: ‘The S-KEY one-time password system’, 1995.
- [7]. Xi, Y.: ‘An improved OTP authentication system and its application in mobile commerce’. Int. Conf. of Intelligence Computation and Evolutionary Computation, Wuhan, PR China, 2012, 615–624.