Door Lock Control using Wireless Biometric

Netra Ghodekar[1], Kshitija Wagh[2], Rutuja Kale[3], Siddhi Kadekar[4], Mr.Vijay N. Kukre[5]

[1,2,3,4]*Students, Dept. of Computer Engineering, AISSMS's Polytechnic, Pune, Maharashtra, India*
[5] *HOD, Dept. of Computer Engineering, AISSMS's Polytechnic, Pune, Maharashtra, India*

Abstract - *Our day-to-day lives are filled with situations where we need to prove who we are; may it be for personal reasons or as part of your profession. Locks are to be opened, e-mail accounts are to be accessed and purchases are to be made – but only by the person correctly authorized to do so. It is not hard to list a wide range of activities, including everything from bank transactions to starting your car, that require fast, reliable and convenient authentication of the user. Thus, identification and authentication of us as individuals have become a cornerstone in today's society, enabling secure interactions while preventing fraud and criminality. So the biometric lock is the need of the world.*

We will see how biometric lock works in this paper.

1. INTRODUCTION

Fingerprint recognition technology is the most widely implemented biometric technology, with a number of different dealers offering a widespread variety of answers. Among the most extraordinary strong points of fingerprint identification, we can discuss the following:

- Providing a high level of identification precision.
- The rising market of low cost small-size gaining devices, allowing its usage in a wide-ranging application.
- The use of easy-to-use, ergonomic devices, not demanding complex user-system interface. On the other hand, a number of drawbacks may influence the efficiency of fingerprint recognition in certain cases.
- Its association with forensic or criminal applications.

1.1 Case Study

There are numerous ways in which the problem of interoperability can be come close to. Normally, it is the matching element that is expected to reconcile feature sets arising from the use of several sensors. However, reconciliation has to happen much earlier in a biometric system to alleviate the influence of varying sensors.

1. One of the obvious ways is to pile the raw data in its entirety in the database (during enrolment) along with the feature set obtained from it (e.g., a fingerprint image and its minutiae set). During verification, the biometric system could extract feature sets from both the database and input images, and then match them. Here, the responsibility is on the feature extraction module to create a 'compatible' feature set from the database image by explicitly taking into account the changes between the sensors used during enrolment and verification. However, storing raw data in a central repository would raise safety concerns, since negotiating this information could have severe repercussions.

2. Recognized representations of the input data might be useful to counterbalance the result of variability in data. For example, fingerprint images may be seen as a collection of ridge lines, with the inter-ridge spacing enforced to be a constant. Feature values can then be extracted from this recognized representation. however, presumes the existence of a canonical form for the raw data. It also pre-empts the likelihood of extracting a rich set of features from the unique data.

3. In some circumstances a simple transformation of the template feature set might account for sensor-specific assets. Fingerprint techniques could use the ridge count between minutiae pairs in an image, the location of core/delta points, etc. to 'normalize' the spatial distribution of minutiae points. In speaker recognition systems, certain normalization filters may be planned to account for variability due to diverse handsets

1.2 Proposed System

Initially we will create a program in Arduino IDE and upload it on Arduino development board. This Arduino program will assist establish interaction between our smartphone and Arduino over Bluetooth. This will permit it to check commands coming from smartphone to perform tasks.

To develop the code, first we would have to create a string variable that stores the distinctive device ID for lock, and then attach the servo library. Following, we will establish serial baud rate for Bluetooth communication. In this code, we have established the baud rate as 9600 for Bluetooth communication. We can use different baud rate according to the Bluetooth HC 05. After setting baud rate of Bluetooth HC 05, set the pin for servo motor.

Later, we will create a loop function to store the device ID sent by the Bluetooth in "reads" string. Afterwards we have to create an 'if condition' for examining the device ID sent from the Bluetooth. If the fingerprint matches in android application, then the application sends the device ID to Arduino. If the ID matches with the one set in Arduino then the servo motor shifts to the unlock position.

If the Bluetooth reads the incorrect fingerprint, then it without human intervention turns the servo to lock position.

1.3 System Diagram

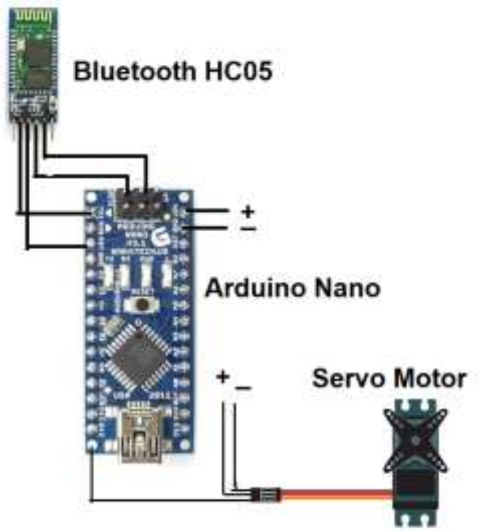

Fig. -1: System Diagram

Fig.1 shows design and operation of a fingerprint-based fingerprint system rather than customization and flexibility. This door lock method works well compared to the higher cost than the traditional lock systems available. Our fingerprint scanning system is unique and quick to understand fingerprints that enable user interaction and provide strong security. In our country, private and governmental organizations are very concerned about security. Many companies have the desire to use this type of lock but the available system has too many installation costs. Due to this exorbitant cost, many small firms cannot afford such programs. Keeping installation costs in mind we have developed a to development system that will be able to finance large and small companies. This design can be enhanced with further improvements and additional features such as multiple clocks can be added to the system. So we don't need to spend a fortune to get one lock only if this can be used to control several departments. A system that saves repairs without using a computer might have been done, but would require more components than we used. In order to maintain safety, the entire path must be placed inside the door panel or the other side of the door. The battery system is also made or made of solar power. One of the main benefits of this program is its flexibility. Many other programs can be implemented with this program. The system is very safe. Fingerprints are unique and the sensor is able to identify all printers during testing. Provides greater access control to restricted areas. There are certain drawbacks of this system such as this system that are complex and they have difficulty making any changes to Hardware as it is a closed system. And requiring operating power to provide continuous power through batteries is a challenge. If so, we can connect the system with IPS or add batteries that can be re-identified in the system.

1.4 Architectural Diagram

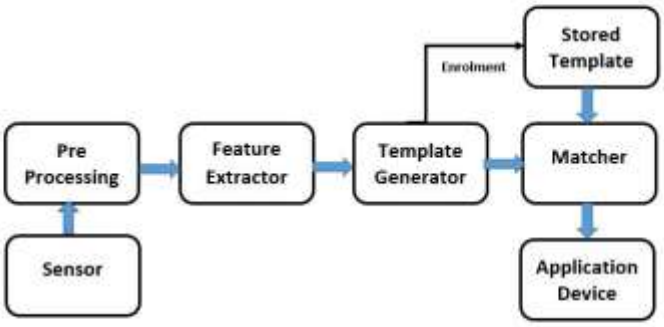

Fig -2: Architectural Diagram

The Fig.-2 shows two basic agendas for biometric systems. First, the most authentication mode (or authenticity) system works with each biometric comparison captured for a specific example including biometric data to verify your identity. three steps involved in the validation of a person. periodically at the beginning, the reference models of all the generated users and periodically store the model details. occasionally the second step, certain samples compared to the connection prove the true and false scores and calculate the limit. The third step is the analytical step. This method can use a smart card, username or ID varies (e.g. PIN) for the purpose that the layer you can use for comparison. 'Good recognition' may be a general use of the authentication method, "where the purpose is to prevent large numbers of people from operating in the same identity".

Second, occasionally the diagnostic mode of the system compares comparisons with most people compared with biometric data in an effort to determine the identity of an unknown person. The program area unit that will be realized is that when each person examines a biometric sample in a very large dataset} the information is below a set limit. Diagnostic mode is used for any 'good recognition' (so that the user should not give details about the model to be used) or 'bad recognition' of a person as long as the system produces a UN agency that person (truthfully or publicly) denies that. "due to certain types of personal recognition such as passwords, PINs or keys, biometric does not work." The first time a person using a biometric system is considered a subscriber of all registrations, biometric information from non-public is held and stored. biometric is available and compared with the information stored throughout the registration. Note that it is important that the storage and restoration of the systems themselves is safe if the biometric system is to operate in the first block (sensor) that the connection between the vital earth and thus the system; image, but it can change the betting on the features you want. ancient species, etc. During block blocking times, the desired options are released. This step can be a step in the right direction because the right decisions have to be forced to be chosen as dead right. A choice expert or image is used to make an example. An example is likely to be made of the relevant signals derived from the acquisition. this type of systems that measure decisions that can be used in an algorithmic comparison program is occasionally discarded for example to reduce file size and protect user identity.

2. PERFORMANCE EVALUATION

As compared to the normal protection system, our fingerprint lock system is value effective, economical and extremely secure. The traditional security system contains locks, that secure measure connected to the proper buttons and square measure turned on. In our system, a licensed fingerprint is that the solely key to unlocking secure key system. Protection system square measure significantly required in our day to day life to shield one's personal estate and privacy from one, there's nothing you'll do as to lock and key. As for the sort of system in use, it tells you tons concerning a lot of what proportion what quantity and the way much it is often protected. It's safe and safer because the fingerprints square measure completely different and might be derived. Three square measure basic variations between several protection process, traditional key and key system, fingerprint system, password/pin, biometric locking system are some of the security features that a person a can simply perform for security purposes. The advantages and disadvantages of each program make them efficient, protected, isolated and difficult to break. Some of the basic differences and structural inefficiencies between these security systems are as follows:

Table -1: types of lock systems

ypes of

differences

Lock & key Biometric

Lock

Fingerprint

Lock

Composition Composed of

simply lock and its

key

Composed of

LCD display,

number pad,

fingerprint scanner

and/or retina

scanner.

Composed of

LCD display,

fingerprint scanner

and GSM module.

Interfaces Key Fingerprint

and/or retina

Fingerprint

Function Unlocks by key

only

Unlocks by

fingerprint and/or

retina scan

Unlocks by

fingerprint

Performance Low Very high High

Strength Moderate Very high High

Efficiency &

vulnerability

Less effective

and highly

vulnerable

Very effective

and less vulnerable

Highly effective

and less vulnerabl

ypes of

differences

Lock & key Biometric

Lock

Fingerprint

Lock

Composition Composed of

simply lock and its

key

Composed of

LCD display,

number pad,

fingerprint scanner

and/or retina

scanner.

Composed of

LCD display,

fingerprint scanner

and GSM module.

Interfaces Key Fingerprint

and/or retina

Fingerprint

Function Unlocks by key

only

Unlocks by

fingerprint and/or

retina scan

Unlocks by

fingerprint

Performance Low Very high High

Strength Moderate Very high High

Efficiency &

vulnerability

Less effective

and highly

vulnerable

Very effective

and less vulnerable

Highly effective

and less vulnerabl

ypes of

differences

Lock & key Biometric

Lock

Fingerprint

Lock

Composition Composed of

simply lock and its

key

Composed of

LCD display,

number pad,

fingerprint scanner

and/or retina

scanner.

Composed of

LCD display,

fingerprint scanner

and GSM module.

Interfaces Key Fingerprint

and/or retina

Fingerprint

Function Unlocks by key

only

Unlocks by

fingerprint and/or

retina scan

Unlocks by

fingerprint

Performance Low Very high High

Strength Moderate Very high High

Efficiency &

vulnerability

Less effective

and highly

vulnerable

Very effective

and less vulnerable

Highly effective

and less vulnerabl

Types of differences	Lock & key	Biometric Lock	Fingerprint Lock
Composition	Composed of basically lock and its key	Composed of LCD display, number pad, fingerprint scanner and/or retina scanner.	Composed of LCD display, fingerprint scanner and GSM module.
Interfaces	Key	Fingerprint and/or retina	Fingerprint
Function	Unlocks by key only	Unlocks by fingerprint and/or retina scan	Unlocks by fingerprint
Performance	Low	Very high	High
Strength	Moderate	Very high	High
Efficiency & vulnerability	Less effective and highly vulnerable	Very effective and less vulnerable	Highly effective and less vulnerable

3. CONCLUSION

Our fingerprint scanning system is unique and quick to understand fingerprints that enable user interaction and provide strong security. Many companies have the desire to use this type of lock but the available system has too many installation costs. Due to this exorbitant cost, many small firms cannot afford such programs. Keeping installation costs in mind we have developed a to development system that will be able to finance large and small companies. This design can be enhanced with further improvements and additional features such as multiple clocks can be added to the system. A system that saves repairs without using a computer might have been done, but would require more components than we used. In order to maintain safety, the entire path must be placed inside the door panel or the other side of the door. One of the main benefits of this program is its flexibility. Many other programs can be implemented with this program. The system is very safe. Fingerprints are unique and the sensor is able to identify all printers during testing. Provides greater access control to restricted areas. There are certain drawbacks of this system such as this system that are complex and they have difficulty making any changes to Hardware as it is a closed system. And requiring operating capacity to provide continuous power through batteries is a challenge at times. A power failure will make it inactive.

ACKNOWLEDGEMENT

It gives us a great pleasure to finalize this paper on Biometric Lock based on IoT.We are thankful to our guide Mr.V.N. Kukre for the encouragement and support that they have extended and also for their effort. We would also thank to all Staff members of Computer Engineering Department for showing us the way for finalizing project proposal.

REFERENCES

[1] "Smart door access system using finger print biometric system" Department of Biomedical Engineering, J.C. Bose Block, Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Sonepat) Haryana-131039,)

[2] Kumar, D. and Ryu, Y. (2009) 'A brief introduction of biometrics and fingerprint payment technology', International Journal of Advanced Science and Technology, Vol. 4, No. 1, pp.185–192

[3] Biometrics Verification: a Literature Survey (A. H. MIR) Department of Electronics & Communication Engineering, National Institute of Technology, Hazratbal)