PASSWORD PROTECTED SECURITY SYSTEMS

By
Garima Agrawal 20BCE2034
Shivalika Singh 20BCE2072

DOMAIN

Design

Hardware

Software

SOCIO ECONOMIC PROBLEMS from various perspectives

- **Insecure Passwords**: IoT devices have a number of password-related issues. Device manufacturers commonly have weak default passwords that users do not change before or after deploying them. Additionally, manufacturers occasionally include hardcoded passwords in their systems that users cannot change. These weak passwords place the IoT devices at high-risk. As attackers can simply log into these devices with these easily-guessed passwords or simple brute-force attacks.

- **Untrusted Deployment Locations**: IoT devices are often designed to be deployed in public and remote places where an attacker may be able to gain physical access to the devices. This physical access may allow the attacker to bypass existing defenses within the devices.

- **Use of Insecure Protocols**: Some network protocols – such as Telnet – have been officially deprecated due to their lack of built-in security. However, IoT devices are known for using these insecure protocols, placing their data and security at risk.

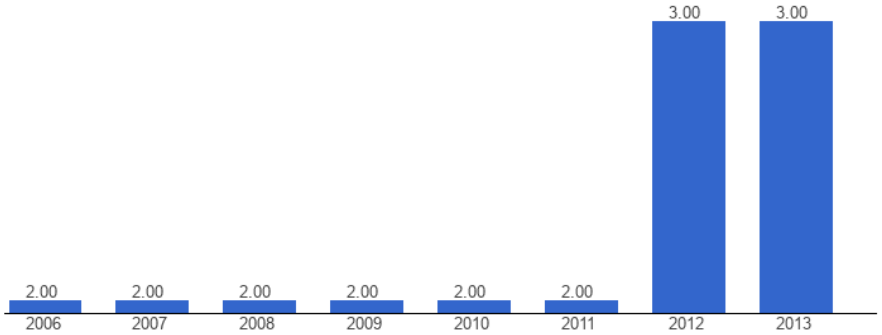
SOCIO ECONOMIC PROBLEMS from various perspectives con.

- **Old Operating Systems**: IoT devices do not always use the most up-to-date version of the operating systems that they are running. This means that the IoT devices' OSs may contain publicly known vulnerabilities that attackers can exploit to take over or damage these IoT devices.

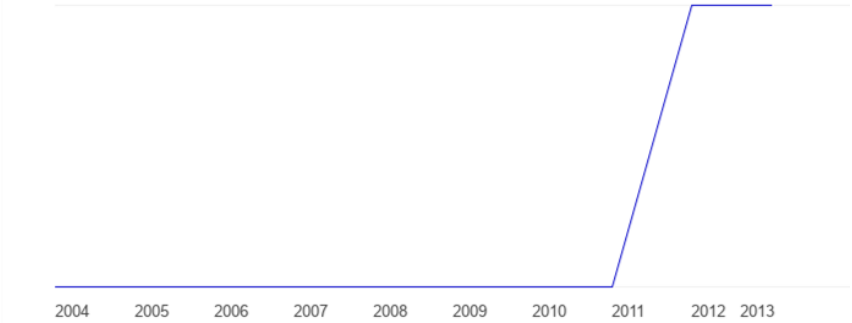
- **Lack of Integrated Security**: Unlike desktop computers, IoT devices rarely come with built-in antivirus and other security solutions. This increases the probability that they will be infected by malware that enables the attacker to use them in an attack or gain access to the sensitive data collected and processed by these devices.

- **Hard to Patch or Update**: All software requires periodic updates to update functionality or close security holes. IoT devices' unique deployment scenarios mean that they rarely receive updates (no one thinks to update their Internet-connected light bulbs or toaster). This leaves the devices highly vulnerable to targeted attacks.

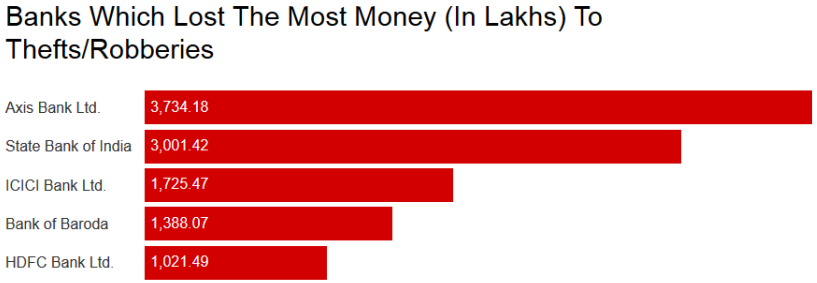
STATISTICS- Facts and figures con.



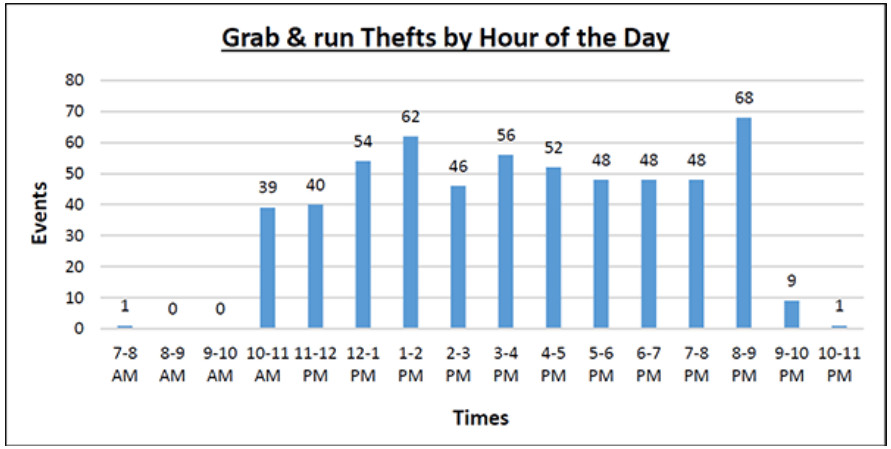
Indian Robbery rate– data, chart



- **India: Robberies per 100,000 people, 2004 - 2013**: For that indicator, we provide data for India from 2004 to 2013. The average value for India during that period was 2 robberies per 100,000 people with a minimum of 2 robberies per 100,000 people in 2004 and a maximum of 3 robberies per 100,000 people in 2012. The latest value from 2013 is 3 robberies per 100,000 people. For comparison, the world average in 2013 based on 95 countries is 119 robberies per 100,000 people. See the global rankings for that indicator or use the country comparator to compare trends over time.



STATISTICS- Facts and figures



- Criminals committing this type of crime will typically walk into a store, appearing to browse the merchandise. Usually they'll move toward the most valuable merchandise on the showroom floor and ask to see a particular piece. From there, they simply run off with whatever they asked to view.
- The number of these types of thefts reported to the Jewelers' Security Alliance every year remains staggering. According to the JSA annual report, a total of 985 jewelry store thefts were reported in 2018, resulting in $12.6 million in losses.

Burglars conscious intention

01

Based on a report by the University of North Carolina about 60% of convicted burglars affirm that the presence of a security system influenced their decision to target another home.

Almost 30% burglars enter home through unlocked door/window

02

First floor windows and doors are convenient mostly when a burglar is concealed behind shrubs and trees

Average property dollar loss per burglary is over $2,250

03

Price of home security system pales in comparison to the emotional and monetary cost of a burglary. The FBI reports that burglary victims in 2014 lost a total of $3.9 billion, and nearly 75% of the burgled locations were residential properties

Someone is home during nearly 3/10 burglaries

04

According survey conducted by the U.S. Department of Justice, a household member is present 28% of burglaries, and 7% of these victims experienced some type of violent crime

13.6% home burglaries in 2014 resulted in arrests

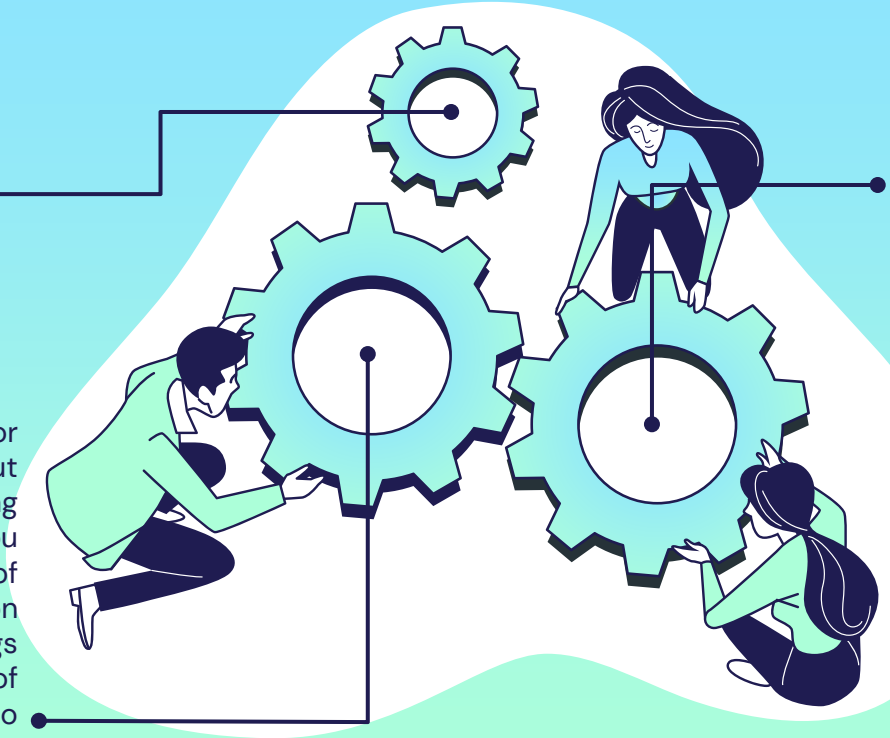
05

Burglaries are difficult crimes to solve, even if the burglar is found, you may not be reunited with your lost property

TECHNOLOGY PERSPECTIVE

If you use the same password across all your accounts, once it's been cracked, All of your accounts become vulnerable. Just as you use different keys to protect different places, use different passwords to protect important accounts

Use two-factor or multi-factor authentication. It sounds pretty fancy, but all it really means is instead of just entering a password to log in to your account, you will also need to enter a second piece of information. You can usually find this option in the account settings or security settings of the online service. There are a variety of options out there, and they fall within two distinct categories: "something I have" or "something I am". Currently most services use the "something I have"



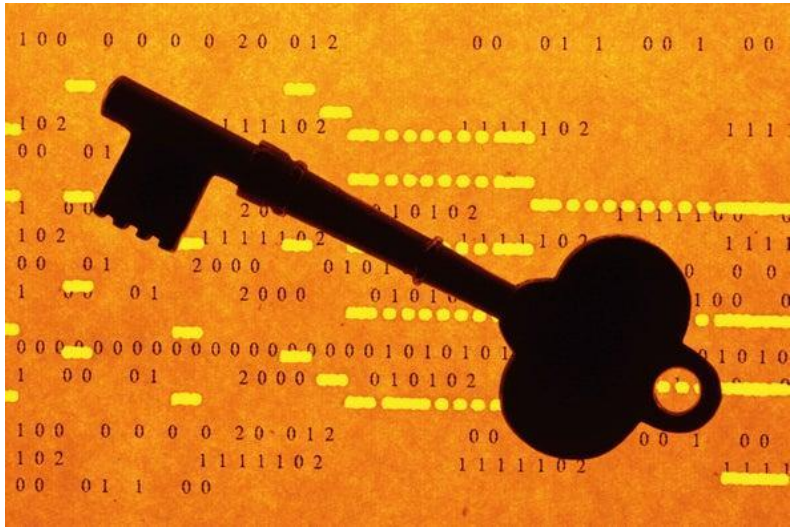
Be wary of single sign-on. Many websites offer you the ability to use your social media or email account credentials to sign into their website, without having to create a new account. While this can be helpful because it means one less account you have to remember a username and password for, there are a number of possible risks involved with using it. When you choose to do this, you are also likely giving Facebook, Google, etc. access to more information about you than they already have, and sharing information from your social media account with the new site or service

MATHEMATICAL MODEL

Passwords are encrypted on end services, that data is stored somewhere and can be stolen and copied onto many computers used to guess potentially billions of character combinations per second. The primary limitations here are the complexity of the password and the complexity of the algorithms used for encrypting the password. These sorts of attacks could be left running for months attempting guesses and are embarrassingly parallelizable.

It is this last attack vector that is key for choosing a randomized password.

MATHEMATICAL MODEL con.



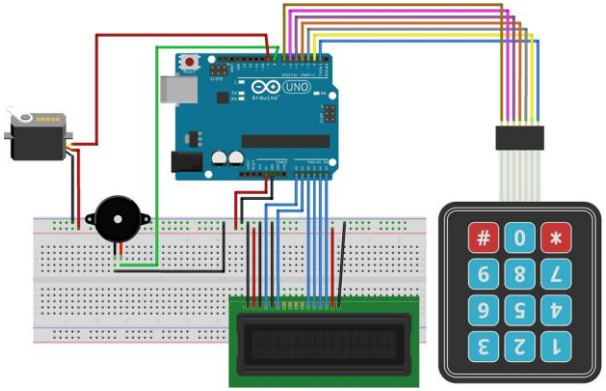
Suppose you have picked a randomized, unique password using a password manager, with 92 symbol choices and 8 characters, or 928 possibilities. With GPU computing hardware in 2012 computing 350 billion guesses per second across 25 boards, the total number of seconds to exhaust all possibilities would take:

$t = 928350 \times 109 \approx 5.2$ hours

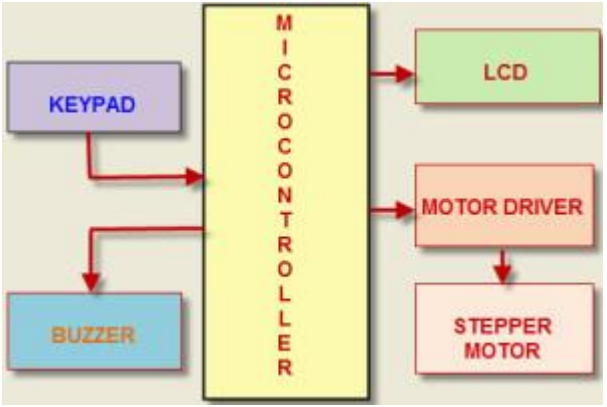
However, it is important to keep in mind that after only half of the time, there is a 50% chance of one of the guesses being correct or about 2.5 hours. Push the password up to 15 characters and the timing is:

$t = (12)(9215350 \times 109) \approx 25,921,330,490$ years

CIRCUIT & BLOCK DIAGRAM



Circuit diagram



Block diagram

The working of this project can be described by the above block diagram. It consists of blocks as a microcontroller, a keypad, a buzzer, an LCD, a stepper motor and a motor driver

OBJECTIVES

The main goal of this project is to design and implement a highly secured and reliable smart security system based on **RFID, Biometric fingerprint, password and GSM technology**. This can be organized in **bank, offices**(treasury), **schools** and **homes**. In this system only the authentic person can open the lock and collect the **important documents, jewellery or money** from the lockers.

MODULES

RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator).

A GSM modem or GSM module is a hardware device that uses GSM mobile telephone technology to provide a data link to a remote network. From the view of the mobile phone network, they are essentially identical to an ordinary mobile phone, including the need for a SIM to identify themselves to the network.

Biometric systems consist of seven basic modules that operate .These building blocks or modules include

(i) a user interface incorporating the biometric reader or sensor

(ii) a quality check module to determine whether the acquired biometric sample is of sufficient quality for further processing,

(iii) an enhancement module to improve the biometric signal quality, (iv) a feature extractor to glean only the useful information from a biometric sample that is pertinent for the person recognition task.

CHALLENGES

FUNCTIONAL REQUIREMENTS

NFC tag It is a technology that works with radio waves and it will be a bit long procedure for us take advantage of it in the requirements to facilitate for us to enter and open the lock by using this technology and it is located inside the control device.

PERFORMANCE REQUIREMENTS

We need to get a WI-FI to get high and fast performance in transferring data from the control device to the lock so that we can control perfectly.

POWER REQUIREMENTS

The controller is used to control locking features, and it needs to be energy efficient to last longer. It uses a rechargeable battery.

ENVIRONMENTAL REQUIREMENTS

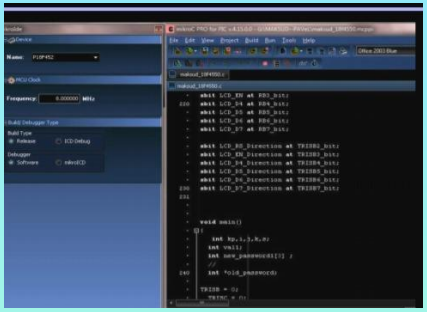
The temporary key is a good option for preserving the environment, which is to give a virtual key that is given to other users through the application instead of keys made of aluminium, so that we have to make sure that we are preserving the environment as well.

SAFETY REQUIREMENTS

The camera and the motion sensor are safety systems that must be provided in the lock in order to protect it from many things, and it must be operable for a longer period and with high protection.

Fig. 1

Fig. 2



ANTICIPATED RESULTS

ANTICIPATED RESULTS con.

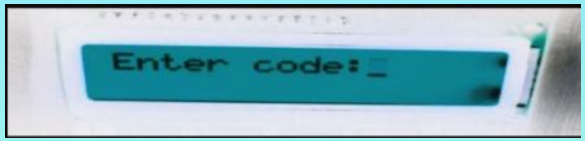


Fig. 3: Enter code in the LCD display

When the power button is switched ON; microcontroller, servo motor, LCD gets power. Now to OPEN the lock enter password when LCD displays Enter code as shown in Fig. 3.

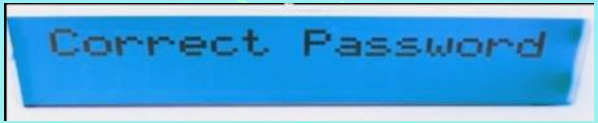


Fig. 4: Correct Password in the LCD display

If password is correct, Correct Password will be displayed in the LCD as shown in Fig. 4 and the lock will be opened which is showed in Fig. 5.

Fig. 5: Lock is opened

On the other hand, if password is wrong, Wrong password will be displayed, the buzzer will give an alarm and the lock will remain closed which is showed in Fig. 6.

ANTICIPATED RESULTS con.

Fig. 6: Lock is closed

Now this system also gives us an extra benefit to change its password. To go to password change option press A.

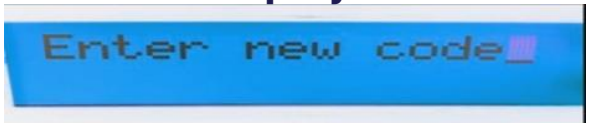
Fig. 7: Enter old code in the LCD display

Enter old password, when LCD displays Enter old code as shown in Fig. 7 and then enter the Security Code, as LCD displays Security code which is given in Fig. 8.

Fig. 8: Security code in the LCD display

Now enter the new Password that is to be set which is given in Fig. 9 and thus the password change operation will be terminated.

Fig. 9: Enter new code in the LCD display



REFERENCES

- Mathematica model of the project

https://www.media.mit.edu/posts/password-security/

- Technology perspective

https://www.techsafety.org/passwordincreasesecurity

- Facts and figures about the issue

https://www.yardian.com/blogs/articles/home-burglary-statistics-and-facts-you-may-not-want-to-know-but-need-to-know/

- Challenges faced(Requirement specifications)

https://www.researchgate.net/publication/347837838_Security_Lock_systems_From_Problem_Statement_to_System_Design_Name_of_the_Author

- Socio-economic problem from various perspectives

https://www.checkpoint.com/cyber-hub/network-security/what-is-iot-security/iot-security-issues/

THANK YOU!!

PASSWORD PROTECTED SECURITY SYSTEMS

REVIEW - 2

COURSE - CSE 3009

Internet of Things

FACULTY - YOKESH BABU

DOMAIN - IoT Security aspects

MEMBERS - Shivalika Singh(20BCE2072) and Garima Agrawal(20BCE2034)

Research paper 1

A biometric authentication model using hand gesture images (static)

By - Simon Fong , Yan Zhuang , Iztok Fister and Iztok Fister Jr

ABSTRACT

A novel hand biometric authentication method based on measurements of the user's stationary hand gesture of hand sign language is proposed.

As an analogue, instead of typing a password 'iloveu' in text which is relatively vulnerable over a communication network, a signer can encode a biometric password using a sequence of hand signs, 'i' , 'l' , 'o' , 'v' , 'e' , and 'u'.

Simple and efficient image processing algorithms are used in hand sign recognition, including intensity profiling, color histogram and dimensionality analysis, coupled with several popular machine learning algorithms.

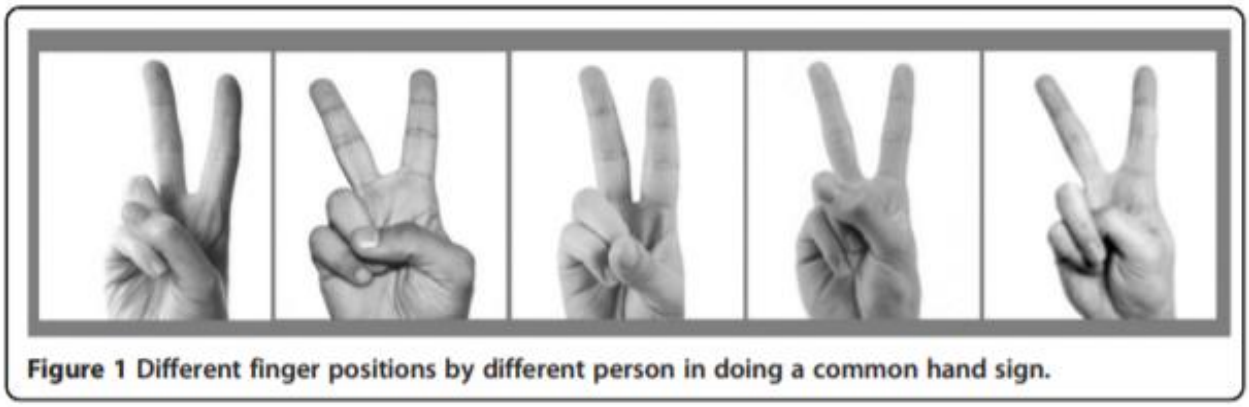


Figure 1 Different finger positions by different person in doing a common hand sign.

Pros

Hand-features biometric recognition has many advantages when compared to other types of biometric features like face, eyes and DNA etc., in authentication.

The advantages of hand-based recognition include the following:

(1) Contactless capture.

(2) Non duplicability; Passwords and signatures would sometimes be needed to be printed on hard copies that could be stolen, forged and duplicated. The hand gestures however are required to be momentarily projected upon a video-camera usually at a perpendicular angle, and this process can be performed in a block box to which the hand is inserted and the actions within concealed. The image data captured would not leave behind any record in the system. The instant image would be transformed and encoded into some numeric features which are fuzzy in nature, to enable approximate-matching in the internal classifier model. In this case, the recognition system is a probabilistic model, instead of a deterministic model, as there is no need exact for matching point-to-point. In each round of hand gesture performance the encoded digest would be very slightly different; it is the underlying core patterns that would be used for authentication. This core patterns are hidden among a vast number of image features, hence they are not easily duplicated.

(3) Non-repudiation; The signer/user is required on the spot to perform a hand gesture. During the authentication the presence of the signer is expected to be in person. Therefore the transaction could be proven non-repudiated with the gesture that is being authenticated can only come live from the legitimate signer.

(4) Proof of liveliness. Falsification is relatively difficult on live hand gestures.

Cons

1) In hand gesture recognition using image processing, when hand is not moving it maybe detected as background.
2) Gesture recognition should bring great results no matter the background: it should work whether you're in the car, at home, or walking down the street. Machine learning gives you a way to teach the machine to tell the hand apart from the background consistently. But for this lots of data is required to train the model.
3) Common sense suggests that gesture is rather a movement than a static image. Gesture recognition should thus be able to recognize patterns, ex. instead of recognizing just an image of an open palm, we could recognize a waving movement and identify it e.g., as a command to close the currently used application. This project does not contain this feature.

Conclusion

Biometrics is a scientific approach that involves recognizing people by measuring their physical and/or behavioural characteristics. In this paper, proposed idea was a novel biometric discipline that uses hand sign gestures as captured in static images in signing. The motivation of using hand sign as biometric authentication is its ease-of-use and the intrinsic behavioural characteristics in signing. Furthermore, signing can convey some secret message which tops up another level of secrecy in authentication from the underlying hand patterns and hand movements.

Future work

Predictions show that the market for gesture recognition technologies is growing, and there are some interesting projects that already use it. The full potential of using hand sign biometric is yet to be unleashed, in a spectrum of security applications.

In future we can try to get the operational cost further down by implementing this and getting more customers. The model can also be redesigned to make the weight lighter.

Maximum 93.75% accuracy could be achieved by artificial neural network, in predicting signers' identities by static hand static gesture which can further be increased. The on par accuracy was observed in predicting contents by static hand sign images too. It is believed that plenty of research niches and opportunities exist, both at the level of technical methods and functional policies, by using hand sign data for biometric authentication.

Tools Used

This new form of biometric authentication is leveraged by the prevalence of sign language. In our system, the biometric model is trained to recognize 26 letters in American Sign Language (which is shown in Figure 2) by using a simple video camera to capture the real time hand gestures. Alternatively, the user can be challenged to input the secret message via a keyboard (just like a password) and it will be verified together with a secret hand gesture that would be known to only the original person.

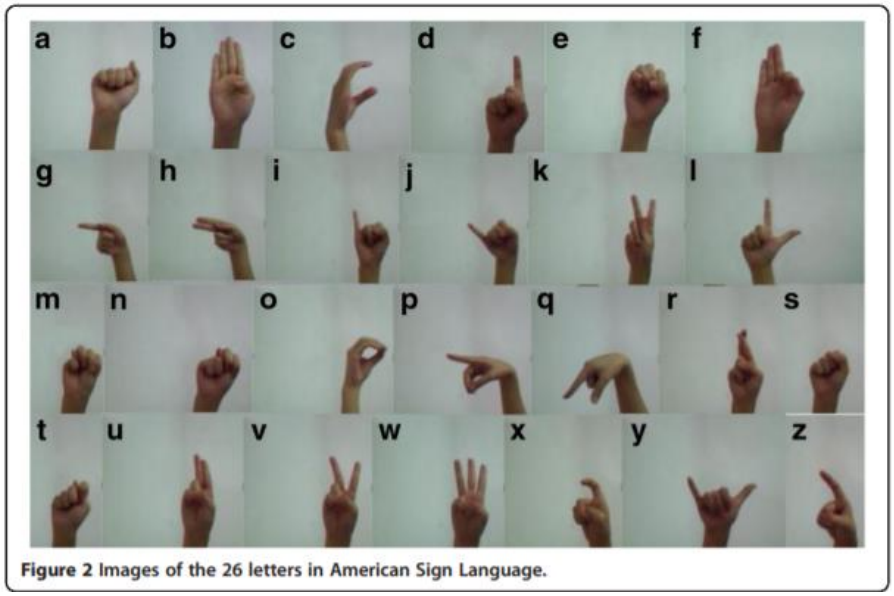


Figure 2 Images of the 26 letters in American Sign Language.

Figure 2

Data Used

In this paper, a new concept for classifying a set of static data from hand gestures for biometric user authentication is proposed.

The main novelty of this approach is in two-fold:

(1) its convenience in acquiring both types of data in a single session, the allowance of certain ambiguity hence extra security in sending and testing the feature data at the classifier, and perhaps most importantly its ability to recognize the contents of the hand signs and to differentiate different signers.

(2) The recognition is based on the signers' hand shapes, or hand postures to be precise, when doing the hand signs. It is believed that by instinct everybody has his/her unique style in addition to the hand shape in performing a hand posture. For an example that is shown in Figure 1, a simple victory hand sign when made by different persons can essentially be very different in a close-up. Therefore it is supposed that the finger positions and hand postures would differ from one individual to another during communication of hand sign languages.

Cloud/ Database:

The composite template that was created for the purpose of registering the user is then used for training (or updating) the classifier model. At the same time his submitted identity together may be coupled with some deciphering keys and an optional PIN are sent to and stored up in a secure database for future reference. A copy of the memories that are resulted from the classifier after being trained to recognize this new user is deposited in the secure database too.

The database entry is now carrying information of the user, his security keys and a copy of the classifier (sometimes in knowledge rules) that was induced to recognize his registered hand signs. Upon authentication challenge by the system, a user who claimed who he is, submits his claimed ID and he performs a series of hand signs in front of the camera.

By referring his claimed ID to the database, the entry is retrieved if it exists. A copy of the knowledge rules that were trained to recognize his hand signs is launched to verify his hand signs under test. If the verification is successful the user who has the claimed ID is authenticated as the legitimate user, and vice-versa. The workflow is shown in Figure 3.

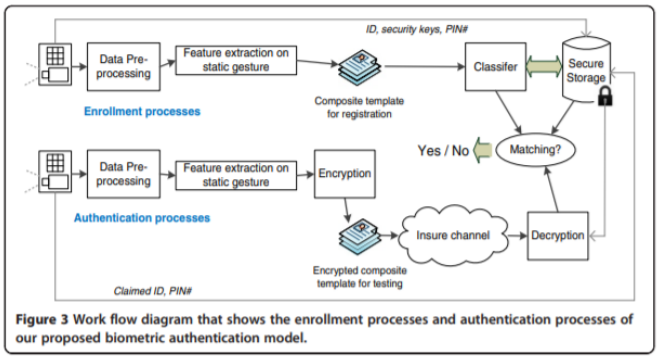


Figure 3 Work flow diagram that shows the enrollment processes and authentication processes of our proposed biometric authentication model.

Blockings

1) Combination of movements

What is more, gestures could consist of several movements, so we need to provide some context and recognize patterns like moving fingers clockwise and showing a thumb could be used to mark some limited number of files or some limited area.

Solution

The camera detects hand movements, and a machine learning algorithm segments the image to find hand edges and positions. It is a difficult part, but there are solutions ready to use ex. **MediaPipe from Google**.

2) Diversity of gestures

There is much diversity in how humans perform specific gestures. While humans have a high tolerance for errors, this inconsistency may make the detection and classification of gestures more difficult for machines. This is also where machine learning helps.

The camera captures each frame, and the system detects movement sequences for further analysis.

Research Paper 2

A Secured Entrance Door lock System using Password Based

By – Abdulraheem Ojo Umar

Abstract

Doors are medium use to keep people out of public and private places. At present, doors under mechanical lock and key are not adequately secured from authorized individual. Mechanical keys are easily destroyed using several tools such as hack-saw etc., thereby providing access to unauthorized individual. Over the years, several security measures have been employed to combat the menace of insecurity of lives and property. In this work a secured entrance door lock system was designed and developed.

Pros

1) High Security Door Locks Reduce Costs in the Long Run

The major benefit of high security locks (also known as HSEC) is that they are nearly impossible to pick.

2) Customize Your High Security Door Locks and Key Control to Meet Your Needs

3) User-Rekeyable Locks Allow You To Immediately Rekey With Ease

4) Track Serialized Keys With Cloud-Based Key Tracking Software

5) High Security Door Locks Ensure Secure Key Control

Cons

Unfortunately, some crimes are committed by the ones that know us best.

Forgetting Your Password-

Choosing a random password is suggested to maximize your security as it is easier to guess repetitive numbers or important dates.

Electric Problems-

Due to the system's reliance on electricity, electrical issues can make your home vulnerable to attacks.

Conclusion

In this study, they implemented a digital security system contains door lock system using personal identification number (PIN). Electromagnetic Lock (EM)was deployed for controlling and transaction, operations. The door locking system functions in real time as when the user enter pin this would be compared with the stored pin. they utilized Electromagnetic Lock (EM) technology to provide solution for secure access of a space while keeping record of the user.

Future Work

The area of interest is control of door lock using personal identification number. Further study of this project includes implementing more complex security mechanisms such as fingerprint detection and face detection for a more robust security mechanism as well as extending support to windows and 'iOS' devices so as to cover a wider range of devices.

Tools used

The hardware requirements for the design and implementation of a secured entrance door lock system include:

i. STEEL DOOR
ii. AT80S51 microprocessor chip
iii. AT80S51 development board
iv. AT80S51 programmer
v. USB cable
vi. DC battery
vii. 4×4 matrix keypad
viii. S1602 LCD
ix. Electromagnetic Lock (EM) unit
x. Connecting wires

Data used

RFID, Radio Frequency Identification is a fundamental and inexpensive technology that enables wireless data transmission. This technology has not been very often used in industry due to lack of standardization among the manufacturing companies earlier. RFID technologies are efficient and secure compare to other network. With RFID, wireless automatic identification takes a very specific form: the object, location, or individual is marked with a unique identifier code contained with an RFID tag, which is in some way attached to or embedded in the target.

Cloud

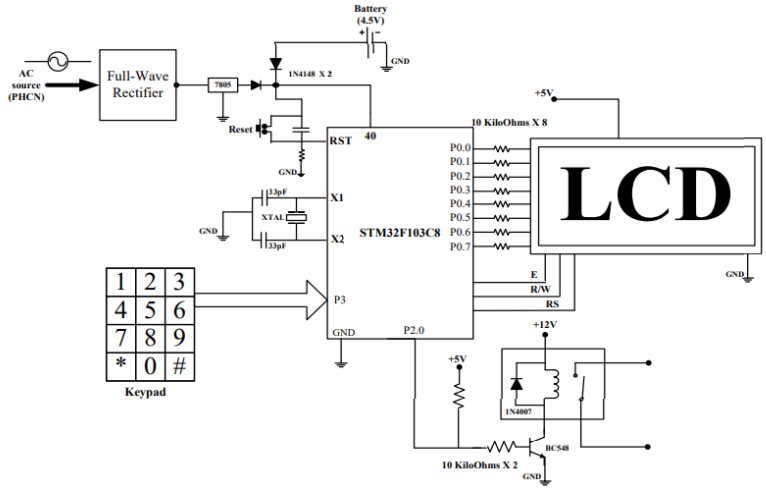
WORKING CONCEPT OF PROJECT

Once a visitor arises to your gate and press the calling switch, it accomplishes 3 tasks:

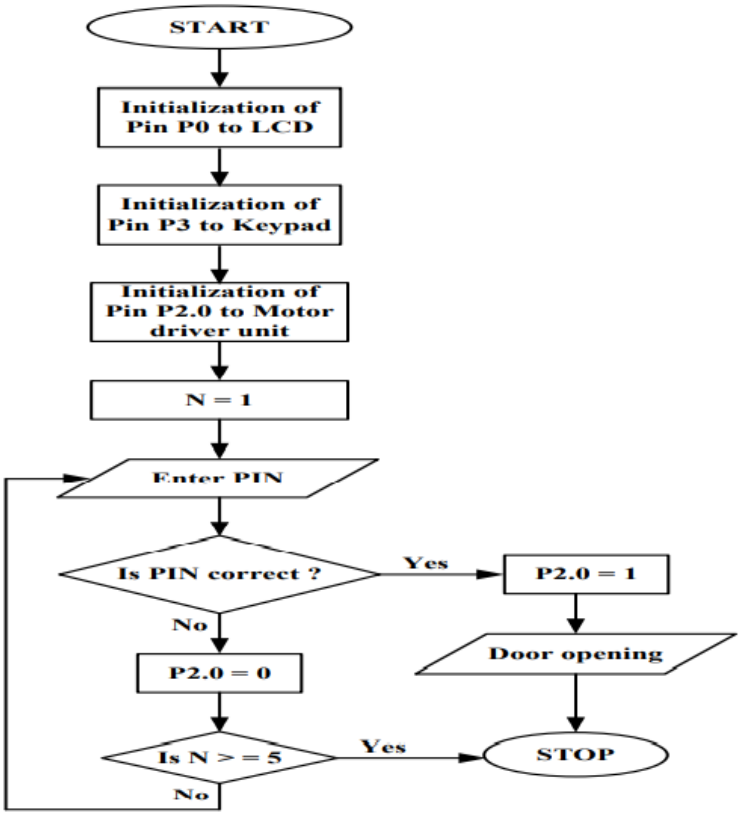
1. It takes a image of the visitor and upload it to AWS S3 Bucket and S3 Bucket generate a SNS notice.
2. It directs an electronic mail with the snapshot to the house proprietor.
3. It directs a welcoming text to AWS Polly and at that moment play the audio acknowledgment for the visitor returned by the Polly.

Circuit Diagram

Circuit Diagram Figure 6 shows the circuit diagram of a secured entrance door lock system. When the circuit is powered, the AT80S51 microprocessor sends instructions to the display unit to display “Enter PIN” on LCD. The user needs to provide the predefined PIN using the keypad. Once PIN is entered, it displays “door opening” on the LCD to indicate that microprocessor read the PIN successfully. However, if the PIN is wrong, LCD displays “Wrong PIN”.



System Flowchart



Research Paper 3

Published By

V.S.Meenakshi, Dr.G.Padmavathi

Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault with Combined Feature Points Extracted from Fingerprint, Iris and Retina for High Security Applications

Abstract

Establishing the identity of an individual is very crucial in the present times Biometric authentication has proved itself superior compared to the traditional password based authentication in many respects. Nevertheless, biometric systems are prone to a variety of attacks. The stored biometric template attack is the most severe of all the attacks. Hence providing security to this form is of prime importance. Moreover, biometric templates may reveal private information about diseases and disorders of a person. Biometric templates cannot be reissued on spoofing. Therefore, apart from security; biometric templates should be imparted with revocability. This work secures the multimodal biometric templates by the crypto biometric fuzzy vault framework. Fuzzy vault suffers from certain limitations like non-revocability, cross matching and lack of diversity. The fuzzy vault is hardened with a password to overcome these limitations. Multi biometric systems are more resistive towards spoof attacks compared to their unimodal counterparts.

Pros

- User convenience is increased by combining both iris and retinal capturing cameras in a single device.
- The proposed password hardened multi biometric fuzzy vault is robust against stored biometric template attacks.
- The performance of the vault can be improved by the application of soft biometrics, non–invertible transformation and multiple biometric traits
- Multimodal biometric system performance is well compared to single modal biometric systems
- The combined vault is hardened with user password for achieving high level of security

Cons

- Fuzzy vault suffer from certain limitations like non-revocability, cross matching.
- Security of the fuzzy vault is affected by the non-uniform nature of the biometric data.

Conclusion

To ensure security and revocability, this work implemented a hybrid template protection approach combining password hardening which is salting and then applying fuzzy vault. This

work also compares the security of the unimodal and multimodal fuzzy vault. Password hardening of the multi biometric fuzzy vault introduces two layers of security namely password and biometrics. It is computationally very hard for an attacker to compromise the password hardened multimodal biometric fuzzy vault. Vault can be captured by the attacker only if he compromises all the three biometrics and password simultaneously. This is not possible in real life situation as it requires more computational effort. The proposed password hardened multi biometric fuzzy vault is robust against stored biometric template attacks. User convenience is increased by combining iris and retinal capturing cameras in a single device. Biometrics traits like iris and retina are internal parts of human and are less prone to damage. They can be employed with other biometric traits like fingerprint in high security applications.

Related work

Juels and M.Sudan [4] introduced the concept of fuzzy vault. Umut Uludag et al [9] used the fuzzy vault to protect a secret key and fingerprint templates. Karthick Nanda Kumar et al [7] enhanced and studied the performance of fingerprint fuzzy vault. Karthick Nanda Kumar et al [10] password hardened the vault which is a hybrid approach comprising the concepts of salting and fuzzy vault. This approach apart from providing security introduces revocability and avoids cross matching of biometric templates across databases. Karthick Nanda Kumar[11] in his work clearly explained the fusion of multi biometrics and minentropy calculations to compute the security of the fuzzy vault. E.Srinivasa Reddy et al [12] hardened iris based fuzzy vault and morphological operations are used to extract feature points from iris. The general vulnerabilities, issues and challenges of the biometric system are understood from the work of [13, 14, 1, 2]. The work of Anil K.Jain [1] provides a survey on the vulnerabilities, attacks and solution schemes related to biometric templates. W. J. Scheirer and T. E. Boult[8] illustrated the specific attacks against fuzzy vault. The work of Anil K.Jain [5] and Karthick Nanda Kumar [11] highlights the merits of multibiometric systems. Sharat Chikkarur [15] discusses on fingerprint minutiae extraction. The work of [16] [17] introduced retinal feature bifurcation extraction. Anil.K.Jain et al [18] and Jung-Eun Lee et al [19] show the significance of Soft biometric is human identification. The password hardened retina based fuzzy vault[20] and password hardened fingerprint and retina based multimodal fuzzy vault
[21] forms the primitive idea for the proposed work.

Proposed method

As a result of the literature survey it is found that fuzzy vault is a proven technology for biometric template security. It mixes the idea of biometrics with cryptography. Fuzzy vault eliminates the key management problem as compared to other practical cryptosystems. The security of the fuzzy vault lies in the polynomial reconstruction problem. Multi biometrics are more significant than uni-biometric systems. Password hardening is a hybrid approach to biometric template security. Hardening provides security as well as revocability. Anyhow, very few have worked in multi biometric template security and retinal template security. Providing security to retinal template is very crucial as it reveals diseases and disorders of a person. This method constructs a fuzzy vault by combining feature set from fingerprint, iris and retina. The proposed work constructs the password hardened multimodal fuzzy vault in three steps. In the first step the fingerprint, iris and retina are subjected to random transformation using password separately. This process enhances the user privacy and facilitates the generation of revocable templates that resists cross matching. This

transformation reduces the similarity between the original and transformed template. In the second step, multimodal fuzzy vault is constructed to secure the transformed templates.

Real time data acquisition

The parameters used in this implementation are shown in Table II. Chaff points hide the genuine points from the attacker. More chaff points makes the attacker to take much time to compromise the vault but consumes additional computation time. The chaff points added are 10 times in number that of the genuine points.

Table II Parameters for Vault Implementation

Parameter	Iris	Retina	Multimodal
No. of. Genuine points(r)	20	30	50
No. of Chaff points(c)	200	300	500
Total no. of points (t = r + c)	220	330	550

Mathematical model

Umut uludag et al [1] uses the concept of fuzzy vault to protect a secret S of 128 bits length. The general notations used in the literature are shown in table I. The x and y coordinates of the iris minutiae and retinal bifurcation feature are used as the locking/unlocking unit 'u' (x|y) of the vault. The secret key S (128 bits) is added with its CRC code (16 bit) to obtain SC (144 bits). SC is divided into 16 bit segments to obtain the polynomial coefficients. Two sets namely, the Genuine set (G) and chaff set (C) are generated.

$$G = [(u_1, p(u_1), (u_2, p(u_2), \ldots\ldots (u_N, p(u_N)].$$

$$C = [(c_1, d_1), (c_2, d_2) \ldots\ldots (c_m, d_m)].$$

$$c_i \neq u_i, (j = 1,2,\ldots\ldots M, i = 1,2,\ldots\ldots N)$$

$$d_i \neq P(c_i), j = 1,2,\ldots\ldots M.$$

$$VS = \text{Listscramb led } (G \cup C)$$

During decoding process, query minutiae set (Q) is compared with the vault to isolate the genuine point set. These points are used to reconstruct the polynomial. The coefficients are

mapped back and SC* is obtained. SC* is divided by the CRC primitive polynomial. If the Remainder is not zero, Query template (Q) does not match and the secret decoded is not correct. If the Remainder is zero, Query Template (Q) matches and the Secret(S) is decoded successfully.

Algorithm

Steps in hardening scheme:

A random transformation function is derived from the user password.

2. The password transformed function is applied to the retina template.

3. The password transformed function is applied to the Iris template.

4. Fuzzy vault frame work is constructed to secure the transformed templates by using the feature points from both the retina and iris.

5. The key derived from the same password is used to encrypt the vault.

Figure 1 depicts the steps involved in the construction of the password hardened multi biometric fuzzy vault.

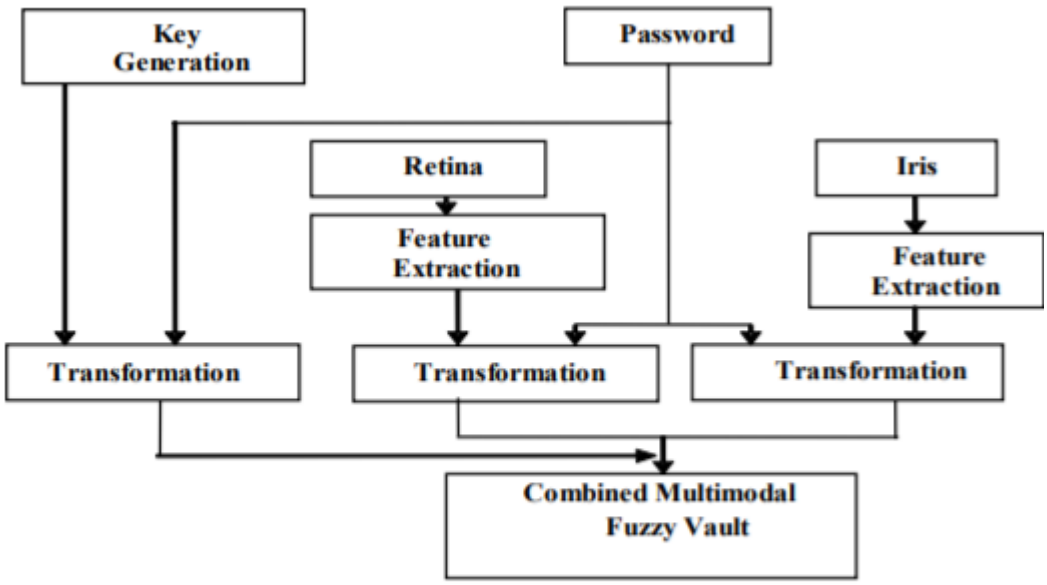


Fig. 1 Steps in Password Hardened Multimodal Biometric Fuzzy Vault

Database

The proposed system is implemented in Matlab 7.0. Iris samples are taken from CUHK Iris Image Dataset. Both the images are resized to 256 x 256 grey scale image by bilinear interpolation for further processing.. Retina samples are taken from DRIVE database. The retinal images taken from the DRIVE data base are resized to the standard 256 x 256 format.

Analytics

In the proposed method the security of the fuzzy vault is measured by min-entropy which is expressed in terms of security bits. According to Nanda Kumar [7] the min-entropy of the feature template MT given the vault V can be calculated as

$$H_{\infty}(M^T \mid V) = -\log_2 \left(\frac{\binom{r}{n+1}}{\binom{r+c}{n+1}} \right) \quad \ldots\ldots\ldots\ldots (1)$$

Where
r = number of genuine points in the vault
c = number of chaff points in the vault
t = the total number of points in the vault (r + c)
n = degree of the polynomial

The security of the fuzzy vault can be increased by increasing the degree of the vault. Polynomial with lesser degree can be easily reconstructed by the attacker. Polynomial with higher degree increases security and requires lot of computational effort. This makes more memory consumption and makes the system slow. However they are hard to reconstruct. In the case of the vault with polynomial degree n, if the adversary uses brute force attack, the attacker has to try total of (t, n+ 1) combinations of n+ 1 element each. Only (r, n+1) combinations are required to decode the vault. Hence, for an attacker to decode the vault it takes C(t, n+1)/C(r, n+1) evaluations. The guessing entropy for an 8 ASCII character password falls in the range of 18 – 30 bits. Therefore, this entropy is added with the vault entropy. The security analysis of the password hardened multi biometric fuzzy vault is shown in Table V. If the number of feature points is less than (n+1) then Failure to Capture Rate occurs. (FTCR). Multi modal biometric fuzzy vault minimizes the FTCR.

Table V Security Analysis of the Password Hardened Multibiometric Fuzzy Vault

Vault Type	Degree of polynomial	Min-entropy of the vault (in security bits	Total no: of combinations	Combinations required	No: of Evaluations	Min-entropy + guessing entropy of the password (in security bit)
Iris	8	34	2.8187×10^{15}	167960	1.6782×10^{10}	52 to 64
Retina	8	33	1.1457×10^{17}	14307150	8.0079×10^{9}	51 to 63
Combined Iris and Retina	10	40	3.1559×10^{22}	3.7354×10^{10}	8.4487×10^{11}	58 to 70

User interface

Iris and retinal capturing cameras can be combined as a single device to improve user convenience

Blockings

Fuzzy vault being a proven scheme has its own limitations:

(i) If the vault is compromised, the same biometric data cannot be used to construct a new vault. Fuzzy vault cannot be revoked. Fuzzy vault is prone to crossmatching of templates across various databases.

(ii) Due to the non-uniform nature of the biometric features it is easy for an attacker to develop attacks based on statistical analysis of the points in the vault.

(iii) The vault contains more chaff points than the genuine points. This facilitates the attacker to substitute few points from his own biometric feature. Therefore the vault authenticates both the genuine user and the imposter using the same biometric identity. As a consequence, the false acceptance ratio of the system increases.

(iv) Original template of the genuine user is temporarily exposed. During this exposure the attacker can glean the template. To overcome the limitations of fuzzy vault, password is used as an additional authentication factor. The proposed multimodal fuzzy vault is hardened by password. This enhances the user-privacy and adds an additional level of security.

Performance measures

- The performance of the vault can be improved by the application of soft biometrics, non–invertible transformation and multiple biometric traits.
- The security of the fuzzy vault can be increased by increasing the degree of the vault. Polynomial with lesser degree can be easily reconstructed by the attacker. Polynomial with higher degree increases security and requires lot of computational effort. This makes more memory consumption and makes the system slow. However they are hard to reconstruct.

Results

The vertical and horizontal distances of the retinal bifurcation features and iris minutiae are used for the polynomial projections. The retinal and finger print template is transformed for three different user passwords to check for revocability. The feature point transformation is done with other two user passwords namely ‘template’ and ‘quadrant’ whose ASCII codes are (116, 101, 109, 112, 108, 97, 116 101) and (113, 117, 97, 100, 114, 97, 110, 116) respectively. For the same original template different transformed templates are obtained when password is changed. This property of hardened fuzzy vault facilitates revocability. Different passwords can be utilized for different applications to avoid cross matching.

RESEARCH PAPER 4

Automatic Door Lock System by Face Recognition

Sharvani Yedulapuram, Rajeshwarrao Arabelli , Kommabatla Mahender, Chintoju Sidhardha

ABSTRACT

In this paper we have proposed face recognition door lock system using raspberry pi for security purpose. Implementation of the system is for monitoring whether any unknown person is entering in to the door. We have established communication with electronic devices through face detection with the help of Pi camera Raspberry Pi platform. For software coding Python and Open CV libraries are used. In order to get accurate and clear picture of an intruder we have proposed Haar classifier method for face detection.

CONCLUSION

In this paper we have implemented a face recognition door lock system. Recognizing of faces is done by using cascade classifiers, which gets a high accuracy and will store in the database. For this testing, we have used 40 images only. Computer vision is used in the IOT. For security purpose, we have implemented real time face detection by Haar classifier. Thus this system can useful for senior citizens living alone and for immobilized people. Hence the proposed system is practically easy to construct and easy to track the path.

PROS

- The main advantage of this is it very low cost and expandable, and it is noise free system
- We don’t need to keep in hand any key or physical item with us, hence it is user-friendly.
- The main advantage of this is it very low cost and expandable, and it is noise free system
- This system can useful for senior citizens living alone and for immobilized people

CONS

- The threat to individual privacy is a significant downside of facial recognition technology
- Imposes on personal freedom: Being recorded and scanned by facial recognition technology can make people feel like they’re always being watched and judged for their behaviour
- Creates data vulnerabilities: There is also concern about the storage of facial recognition data, as these databases have the potential to be breached

RELATED WORK

The author D Aishwarya et al [5] proposed a method for face detection by using algorithm known as viola-jones and recognition of face is done by the revised Gabor filter and multi key point. Using Neural Networks, Nandini M et al [6] proposed a facial recognition system. For training and to extract the local features like nose, eyes, shoulder and mouth they have used back propagation algorithm. Using MATLAB PCA (Principal component analysis) is implemented by M Mulla et al [7] for face recognition.

PROPOSED

After preprocessing like resizing and cropped images, Haar cascade classifier is used to detect whether there is a single face detected or not. Edge, line, and center surround are the features of Haar which are acting as inputs. By these cascade features the test of the image is done. The features of Haar are divided into various different stages [9]. Stage by stage the window will be tested. Usually initial stages will have less Haar-like features. If the first stage window fails, then it is to be discarded and the next stages will not be tested. If all the stages successfully passes then it is considered to be face is detected and checks with the images already stored in database of raspberry Pi [9, 12, 13, and 14]. The advantage of Haar cascade classifiers is fast detection speed compared to other classifiers.

TOOLS

- Raspberry Pi- The version of the model (A or B) doesn't really matter. But we have used Raspberry Pi model B with Wi-Fi.
- Pi Camera -It comes with a flex cable. This is inserted into the connector located in between the Ethernet and HDMI port. When there is someone next to the door, by using face recognition software it can capture the image and store it in the database using python and then it can be send to the owner through android application, this can help in providing security to home.
- Relay- In our system we have used two channel relay for device control.
- DC Motor -A DC motor is rotary electrical equipment which converts electrical energy into mechanical energy.

MATHEMATICAL MODEL

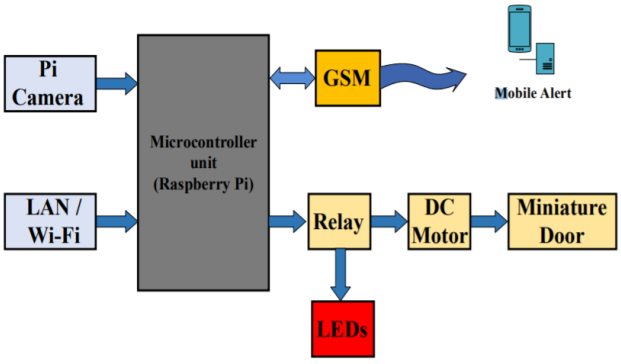


Figure1. The proposed system block diagram

ALGORITHM

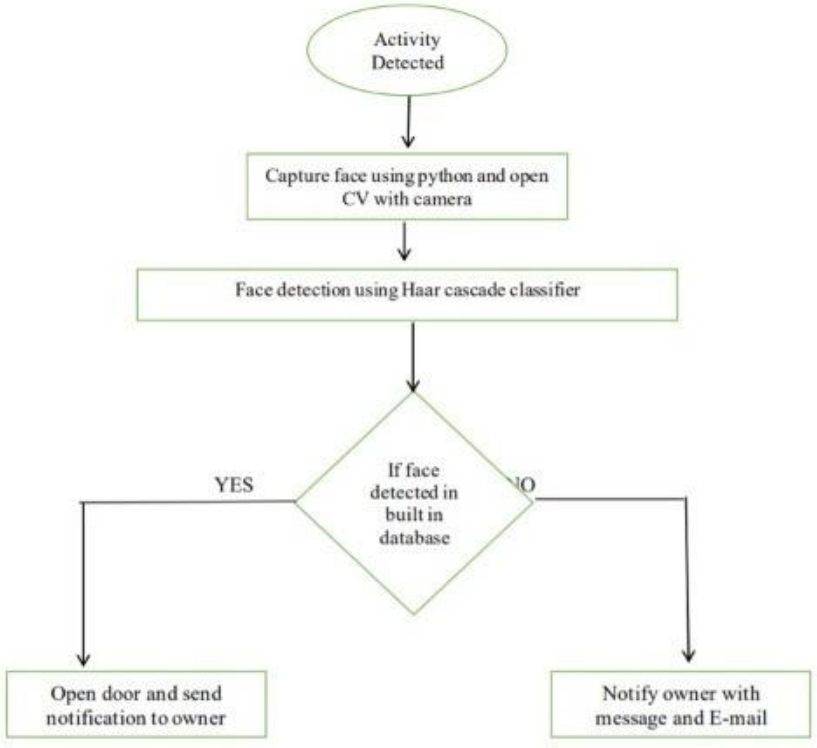


Figure3. Flow chart of the proposed system

DATABASE

Raspberry Pi processes the captured image coordinates with the existing coordinates in the database. If it matches then it sends the signals to relay switch through GPIO pins. DC motor drives a miniature door which is being used for a door locking system. If the intruder's face doesn't match then the LED's are on and the door remains closed.

USER INTERFACE

As soon as the person enters near the door, pi camera captures the image and face detection process is done then if it matches with database images then the door is unlocked otherwise a message with the picture of a person will be sent to the registered mobile through GSM and LAN network. The system which is based on SMS technology have only two components [4] i.e. GSM and micro controller. Here micro controller is acting like bridge between the user, sensors and actuators.

RESULTS

When any motion is detected the Pi camera effectively captures the pictures. The real time face detection is done by cascade classifier. The system starts running once the picture is captured. The figure 4 shows that the face is detected. The figure 5 shows the received notifications and the captured image on the smart phone. The overall execution time is capturing of images, detecting of faces through cascade classifier and for sending the message with the image of unknown person to the owner.

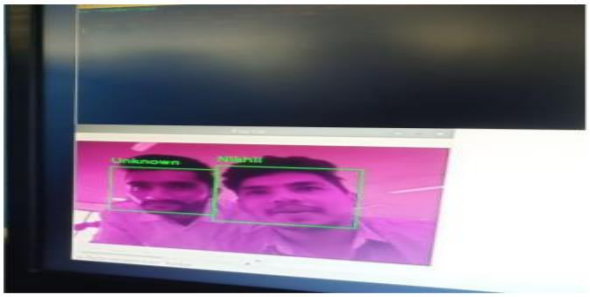


Figure 4: Face is detected

Figure 5: Received notification in mobile.

Research Paper 5

Published By

Manasa Pisipati, Amrit Puhan, Arun Kumar, Vijay Bhaskar Semwal and Himanshu Agrawal

A Dynamic Hand Gesture-Based Password Recognition System

Abstract

Hand gesture recognition systems are used as an interface between computers and humans. An electronic machine capable of recognizing various types of hand gestures is easily operable using natural languages. This way of controlling a device is much more intuitive and effortless as compared to using a touch screen, manipulating a mouse or remote control, tweaking a knob or pressing a switch. This paper presents a dynamic hand gesture-based password recognition system which uses feed-forward back-propagation neural networks. The uniqueness of this system lies in the fact that it would use an ordinary low-cost webcam (built into the laptop) rather than a high-resolution Kinect camera.

Pros

1. This way of controlling a device is much more intuitive and effortless as compared to using a touch screen, manipulating a mouse or remote control, tweaking a knob or pressing a switch.

2. An electronic machine capable of recognizing various types of hand gestures is easily operable using natural languages.

3. The uniqueness of this system lies in the fact that it would use an ordinary low-cost webcam (built into the laptop) rather than a high-resolution Kinect camera.

4. The advantage of using such a camera is that this software can be integrated as a security tool into everyday electronic devices such as laptops and smart phones.

5. This can provide an additional layer of protection to security devices when combined with other security tools such as alphanumeric passwords, biometric passwords, etc.

6. The obtained results show the best accuracy of 100% for the training dataset and average accuracy of 96.16% for the testing dataset.

Cons

The human hand has very complex articulations compared with the rest of the body, and therefore, it can be easily affected by errors. Thus, it is a very challenging problem to recognize hand gestures.

Conclusion

In this paper, a password system using a low-cost and low-quality camera (video specs of 720p, 16:9 ratio and 30 fps) has been successfully implemented. The dataset consists of 1714 pre-existing gestures, has processed the images into a suitable format and has classified the gestures with an accuracy of 96.16%. This work also highlights the development of an efficient and accurate locking–unlocking system based on gestures. Such systems can improve the security level of everyday gadgets such as laptops and mobile phones. The biggest advantage of such a password recognition system is the strength in system security that it provides.

Future Work

The future scope for this work includes improvement of efficiency and accuracy of the password recognition system. Additionally, as mentioned earlier, the program works most accurately only when the background is clear and the hand faces the camera directly. Since this is difficult to achieve in a real-life scenario, the background subtraction and gesture recognition algorithms can be improved. Another important aspect of implementing a hand gesture-based password recognition system is to secure it from a snooping or shoulder-surfing attack.

Related Work

Hand gestures can be used in various applications. This type of gesture recognition involves selecting a particular sign language, storing in the database and just recognizing the hand gestures from those set of stored images. The research work has been done on a variety of sign languages like the Japanese sign languages, Indian sign languages, American sign languages and also sign languages which speech-disabled people use. Gesture control, on the other hand, involves using the set of recognized gestures and assigning some task to it. The research work has been done on controlling a video on a media player using gestures and looking at a 3D model from various angles by translating and rotating it using gestures. This type of modeling can also come in handy for medical imaging and applications.
Hand gesture control video games using Kinect have also been developed. Gesture control robots have been built which involve making the robot do human-like activities just by gestures. Hand gesture control is now being incorporated into automobiles for a more convenient and distraction-free driving experience.
Gesture-based password systems can improve the security level of everyday gadgets such as laptops and mobile phones. The user does not fall prey to typing text capturing, dictionary attacks or man-in-the-middle attacks. Also, the risk of losing stored passwords to attackers is eliminated. Since the human hand is capable of a very large number of gestures, it becomes more difficult to crack the password through brute-force method as well. However, considering hand gesture-based password systems, very few research works have been done in this field. A majority of the research on hand gesture-based passwords have been using Kinect camera. For example, the research focused on tracking the motion of a user's hand in front of a Kinect camera and unlocking the device by comparing the shapes created in the air by the finger. Their main focus is to improve gaming security. Another gesture-based password system uses a Leap Motion device which tracks a user's hand in three-dimensional space using infrared sensors. Their research also used RDF and neural networks.

Tools Used

In this paper, a password system using a low-cost and low-quality camera (video specs of 720p, 16:9 ratio and 30 fps) is used. The proposed system will consist of a desktop or laptop interface.

Data Used

In this work, there are 1714 images (dataset source: GitHub—Rishabh Gupta's Indian Sign Language Recognition) of size 50 × 50 pixels which are saved as 1714 × 2500 size matrices where each column represents pixel from the image. Also, the matrices are randomly split into two separate sets. A training matrix will contain 80% of the images which will act as training feature vector and the test matrix with other 20% of the images which will act as testing feature vector. Here, 9 different classes of gestures are taken. So, a label matrix of dimension 1 × 9 is made where each index can contain either 1 or 0. Say an image belongs to the third class, the vector will look like:

$$[0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0]$$

where the third index is set to 1 and the rest of the indices are set to 0 to show that the image belongs to the third class.

Mathematical model

There are 5 steps to make the ML model:

1. ***Load the features and labels***: The first step is to load the features and labels that have already been created. This can be done by using dlmread function of Octave.

2. ***Randomly initialize theta values (weight of the nodes of neural network)***: The statistics formula of uniform distribution of variance has been used to initialize the weight of the nodes.

3. ***Create the cost function and forward propagation***: The next goal is to implement the cost function defined in Eq. (1).

$$J(\theta) = -\frac{1}{m}\sum_{i=1}^{m}\sum_{k=1}^{K}\left[y_k^{(i)}\log\left(\left(h_\theta\left(x^{(i)}\right)\right)_k\right) + \left(1 - y_k^{(i)}\right)\log\left(1 - \left(h_\theta\left(x^{(i)}\right)\right)_k\right)\right] + \frac{\lambda}{2m}\sum_{i=1}^{8_l}\sum_{i=1}^{8_l}\sum_{i=1}^{8_{l+1}}\left(\theta_{j,i}^{(l)}\right)^2 \quad (1)$$

where g is the activation function (sigmoid function in this case).

$$a^{(j)} = g\left(\theta^{(j-1)}a^{(j-1)}\right) \quad (2)$$

$$h_\theta(x) = a^{(j+1)} \quad (3)$$

In order to compute the cost, feed-forward computation is used. A for-loop has been used over the examples to compute the cost. Also, an extra column of 1's needs to be added to the matrix which represents the "bias" values. The θ1 and θ2 values are parameters for each unit in the neural network—the first row of θ1 corresponds to the first hidden unit in the second layer.

4. ***Create the gradient for neural network cost function, i.e., back-propagation***:
To be able to minimize the cost function, the gradient for the neural network cost function must be computed.
5. ***Minimize the cost function***: One of the gradients is computed, and the neural network can be trained by minimizing the cost function *J*(_) using an advanced such as fmincg. This function is not a part of the Octave, so it is obtained from machine learning course by AndrewNg. This function is faster than the ones implemented in Octave, and it uses conjugate gradient method.

Algorithm

2. Initialize random values to weights of neural network as

```
epsilon = sqrt (6) / (L_in + L_out);
      W = zeros (L_out, 1 + L_in);
      W = (rand (L_out, 1 + L_in) * 2 * epsilon) - epsilon;
```

3. Declare the sigmoid activation function

$$a^{(j)} = g\left(\theta^{(j-1)} a^{(j-1)}\right)$$

$$h_\theta(x) = a^{(j+1)}$$

4. Define the cost function and forward propagation

$$J(\theta) = -\frac{1}{m}\sum_{i=1}^{m}\sum_{k=1}^{K}\left[y_k^{(i)}\log\left(\left(h_\theta\left(x^{(i)}\right)\right)_k\right) + \left(1 - y_k^{(i)}\right)\log\left(1 - \left(h_\theta\left(x^{(i)}\right)\right)_k\right)\right]$$
$$+\frac{\lambda}{2m}\sum_{i=1}^{8_l}\sum_{i=1}^{8_l}\sum_{i=1}^{8_{l+1}}\left(\theta_{j,i}^{(l)}\right)^2$$

5. Create a gradient for the cost function using back-propagation algorithm.
6. Once the gradient is computed, the neural network can be trained by minimizing the cost function $J(\Theta)$ using an advanced optimizer such as fmincg.
7. Compare the gesture from a database of gestures once the model is trained by predicting the label of the test image given the trained weights of neural network.
8. Compare the label sequence of the test image with label sequence of the training image. If they match then unlock, else keep it locked.

Cloud/Database

Comparing the Gesture from a Database of Gestures

Before this step, a database of the password must be created. Each time a new password is created, a new database must be developed for that specific password. Once the database is created, comparing the input-gestures with it can begin. Since it is a password system, it must be ensured that the sequence of the input-gestures must be the same as the sequence of gestures in the database. Therefore, the proposed method includes a comparison of two things:
1. The gestures in the database with gestures that have been given as input.
2. The time stamps of gestures in the database with the time stamps of the gestures given as input for a live system to be possible.

Analytics

Figure 5 shows the accuracy of the training and test datasets with increasing iterations. It has been observed that with an increase in iteration, the accuracy of the result also increases.

Figure 6 shows the dependence of cost function on the number of iterations.

As seen from the graph, the cost function is inversely proportional to number of iterations. Hence, the developed method is successfully reducing cost function with increase in iterations.

Fig. 5 Analyzing the accuracy of training and test datasets

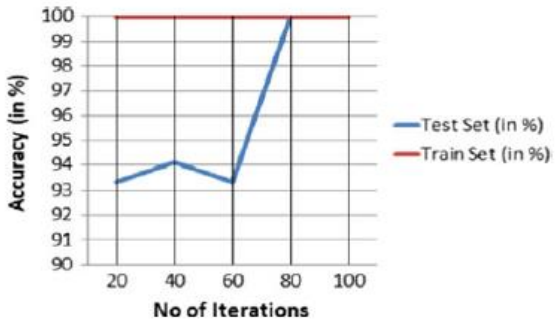
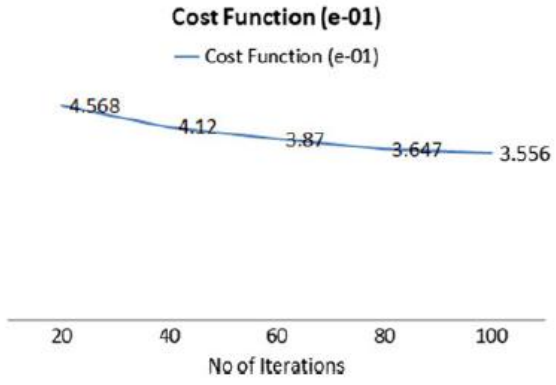


Fig. 6 Analyzing cost function



User Interface

- Hand gesture recognition systems are used as an interface between computers and humans.
- The proposed system will consist of a desktop or laptop interface.

The work is divided into 4 modules:

Module 1—Taking input from the webcam and converting it into a form that can be processed Easily.

Module 2—Intercepting the gesture from the input of the webcam.

Module 3—Creating a neural network that trains and classifies the dataset into separate classes.

Module 4—Recognizing the gesture from a database of gestures.

Module 5—According to the intercepted gesture, choose to unlock the device

Results

As shown in the flowchart, the steps are the acquisition of video, conversion into image frames, background subtraction (using three methods: Otsu's method, novel method and RGB to YCbCr method) and finally segmentation of the gestures from the image. The images below are snippets of the input and output video streams for the three methods mentioned above.

Otsu's method for background subtraction

See Fig. 2.

– ***Novel method***

See Fig. 3.

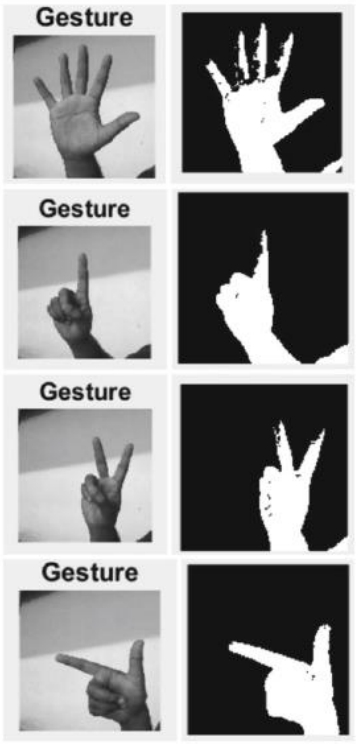


Fig. 2 Input images with gesture and background (left) and output images after background subtraction using Otsu's method (right)

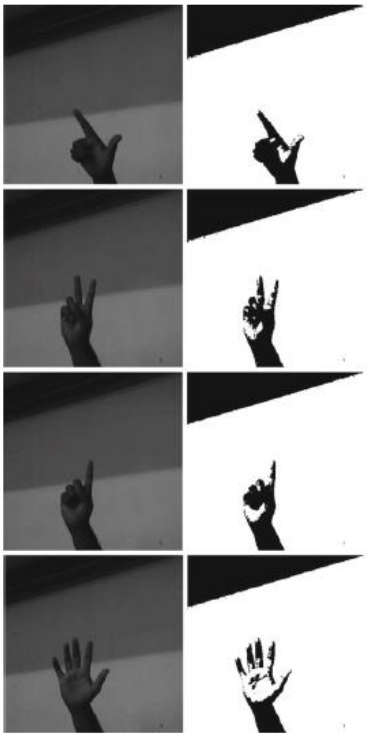


Fig. 3 Input images with gesture and background (left) and output images after background subtraction using the proposed code (right)

– ***Converting the image from RGB to YCbCr and extracting only those pixels which are in skin color range.***

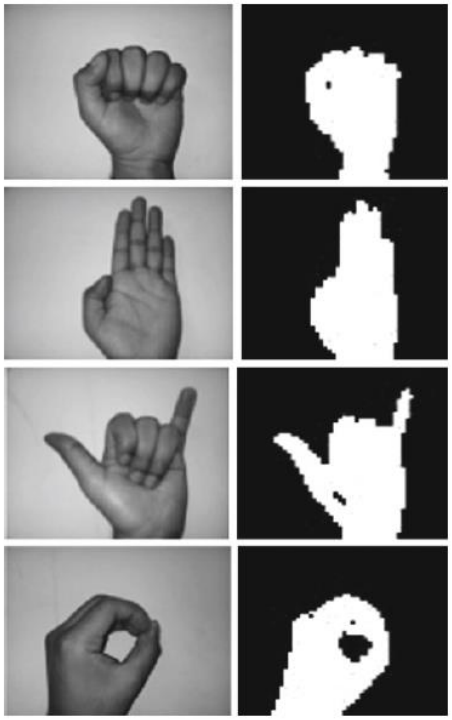


Fig. 4 Input images with gesture and background (left) and output images after binarization using the third and most optimal method (right). It proved to be computationally more efficient and accurate

See Fig. 4.

It has been observed that in order to have an efficient background-subtracted image, the hand should be completely facing the camera lens preferably at the center of the frame. In addition,

if the background is not plain, then the hand must be closer to the camera to reduce the influence of the background on the gesture. Currently, a dataset (from online hand gesture resources) of gestures which consists of 1714 samples (80% for training, 20% for testing and validation) has been collected. As of now, nine classes are considered. The algorithm has successfully classified them using feed-forward back-propagation neural networks. Although the accuracy of the network varies with the number of iterations, till now, the best accuracy achieved is 100% for the training dataset and average accuracy of 96.16% for the testing dataset (for 100 iterations).

Comparative analysis of all papers

All the above 5 research papers aim at solving the main goal of this project which is to design and implement a highly secured and reliable smart security system based on gesture recognition.

In research paper 1 we have seen a novel approach of a biometric authentication model using hand gesture images (static) to solve the problem by using Logitech Quick-Cam webcam. The concept which is used here is 10 machine learning algorithms (highest accuracy obtained from perceptron, SVM, Bayes and NB Tree).

In research paper 2 we have seen an innovative way to use a Secured Entrance Door Lock System using Password. This is a more practical solution which can be implemented in existing cities however this was just a concept which didn't provide with any complex security mechanism such as fingerprint detection and face detection for a more robust security mechanism as well as extending support to windows and 'iOS' devices so as to cover a wider range of devices.

In research paper 3 we have seen here high security applications being most efficient by combining both iris and retinal parts of human body which are less prone to damage and thus give us maximum safety.

In research paper 4 using Pi camera Raspberry Pi platform a communication is established with electronic device through face recognition

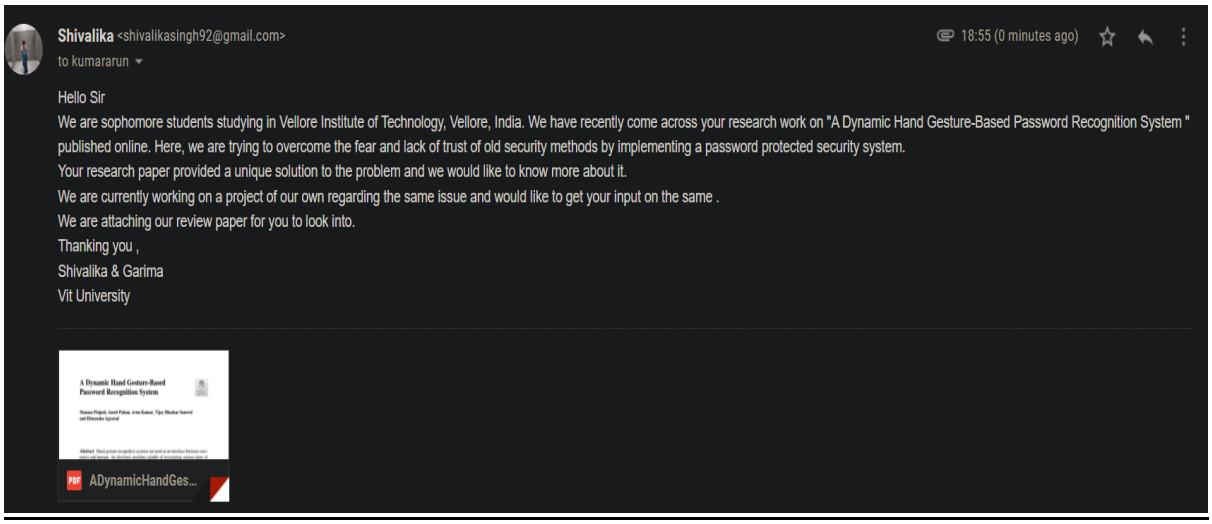
In research paper 5 we have proposed a work to solve the issue using Laptop built-in webcam where the concept of Image processing + feed-forward back-propagation neural networks is used.

Proposed Solution

Humans always look for the easiest way possible for doing a particular task. The goal of Internet of Things is to make the system more efficient and usable for all kinds of people (especially the disabled). 'Gest Lockz' focuses on gestures and motion detection techniques giving a product-based outcome. Camera Sensors applying motion detection concludes if the person is present infront of the door. Using hand gestures recognition, the passwords can be set initially and unlocked later on. Expressive body actions for interacting with the physical world are better than speaking out. Today's world requires a cheap viable solution that is technologically evolved but affordable.

Contacting The Authors

RESEARCH PAPER 5 - A Dynamic Hand Gesture-Based Password Recognition System



RESEARCH PAPER 2 - A Secured Entrance Door lock System using Password Based