SMART AND SECURE LOCKER SYSTEM

Mrs. Rasika Naik
Assistant Professor,
Vivekanand Education Society's Institute of Technology
Mumbai, India
rasika.naik@ves.ac.in

Mr. Sanchit Agarwala
Student, Vivekanand Education Society's Institute of Technology
Mumbai, India
2016.sanchit.agarwala@ves.ac.in

Mr. Siddanth Raisinghani
Student, Vivekanand Education Society's Institute of Technology
Mumbai, India
2016.siddanth.raisinghani@ves.ac.in

Mr. Swapnil Satam
Student, Vivekanand Education Society's Institute of Technology
Mumbai, India
2016.swapnil.satam@ves.ac.in

Mr. Shubham Sawant
Student, Vivekanand Education Society's Institute of Technology
Mumbai, India
2016.shubham.sawant@ves.ac.in

***Abstract* – Due to the fast-paced life nowadays, people are unaware of keeping their lockers safe and secure. There are very few systems, which allow the users to know who visits locker rooms in their absence and also communicates with authorized user. A new system proposed by us, allows the user to know when someone else tries to access their locker, immediately sends the alarm to the authorized user, and also provides the option to either give access to legitimate user or to deny the permission. In this paper, a camera is continuously monitoring the area, and detects a person, within 14 seconds if the image of the user in front of the camera does not match with the authorized user database of images, then Raspberry Pi system instructs the camera to click a picture. Once that has been ascertained that it is a unauthorized person near the locker, notifies the legitimate user with a message that a unauthorized person is trying to access the locker. The system designed collates other information from the server along with the image and sends the notification to the authorized user. After reviewing the image and associated data, the user can further decide the next course of action.**

***Index Terms*– Lockers, Safe, Secure, Raspberry Pi, Internet of Things (IoT), Encryption, Decryption, Elliptic Curve Cryptography (ECC), RSA, Advanced Encryption Standards (AES), Data Encryption Standards (DES), User Interface, Web application.**

I. INTRODUCTION

The image capturing based locking system is an enhancement to the traditional locking system that uses physical keys. The traditional locking system uses two keys for the transaction by the authorized user in the banking system wherein the bank's key and the owner's key are used to access the locker. Some of the banks uses nowadays software-based access control through the logins. If the necessary protection is not provided then these logins can easily be copied, decrypted and used by the unauthorized user/hackers. These keys/logins must be kept secured, confidential to avoid loss or access due to negligence. This paper describes Image capturing based locking system an attempt to solve the issue of such malpractices and human negligence.

II. MOTIVATION

The motivation behind this paper is to increase the knowledge about image processing and to know how exactly facial recognition works. Also, this paper helps to increase knowledge about the latest hardware, while simultaneously assisting the user in solving a pertinent everyday issue. Therefore, it would help in gaining expertise in topics that are not covered in detail in the curriculum, while simultaneously gaining practical experience of programming and hardware.

III. AIM

As Hacking and security issues are increasing now-a-days, the security related problems are observed within various locking systems. The aim is to design a system which will recognize the authorized user by face recognition. To make it more user friendly, a system is proposed which will provide an interface with user to allow or deny access to any person by capturing his/her image.

IV. APPROACH

Implementation of the system is done by using a platform of Internet of Things (IoT); provides a better system and user interface. This paper consists mainly of three parts namely,

- To recognise the face
- Encrypt the image
- Unlocking mechanism.

V. PROBLEM STATEMENT

Now-a-days, with increasing number of security key hacking issues, a solution is needed that will restrict the access only to user of locker. Implementing such a system will not be possible using OTPs or Unique keys because those details can easily be leaked or can be hacked due to negligence. The proposed paper contains a solution based on IoT and Image Encryption for authentication of owner credentials for operating the locker system.

VI. BLOCK DIAGRAM

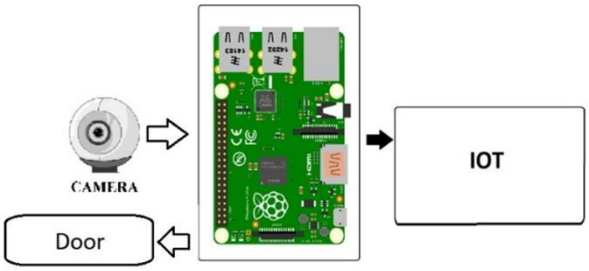

Fig. 1. General Block Diagram of paper. [1]

VII. SYSTEM SPECIFICATIONS

A. *RASPBERRY PI*

SOC: Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC

1) CPU: 1.4GHz 64-bit quad-core ARM Cortex-A53 CPU
2) RAM: 1GB LPDDR2 SDRAM
3) WIFI: Dual-band 802.11ac wireless LAN (2.4GHz and 5GHz) and Bluetooth 4.2
4) Ethernet: Gigabit Ethernet over USB 2.0 (max 300 Mbps). Power-over-Ethernet support (with separate PoE HAT). Improved PXE network and USB mass-storage booting.
5) Thermal management: Yes
6) Video: Yes – VideoCore IV 3D. Full-size HDMI
7) Audio: Yes
8) USB 2.0: 4 ports
9) GPIO: 40-pin
10) Power: 5V/2.5A DC power input
11) Operating system support: Linux and Unix

Features:

1) Improved compatibility for network booting
2) New support for Power over Ethernet
3) Processor speed increased from 1.2Ghz on Pi 3 to 1.4Ghz
4) New dual band wireless LAN chip, 2.4Ghz and 5Ghz with embedded antenna
5) Bluetooth 4.2 Low Energy
6) Faster onboard Ethernet, up to 300mbps speed

B. *RASPBERRY PI CAMERA SPECIFICATION*

Following are the specifications of the camera to be interfaced with the Raspberry Pi modal:

- Resolution: 5 MP
- Interface Type: CSI (Camera Serial Interface)
- Dimensions: 25x23x8 (LxWxH) mm
- Supported Video Formats: 1080p @ 30fps, 720p @ 60fps and 640x480p 60/90 video

C. *INTERFACING OF RASPBERRY PI B+ AND CAMERA MODULE*

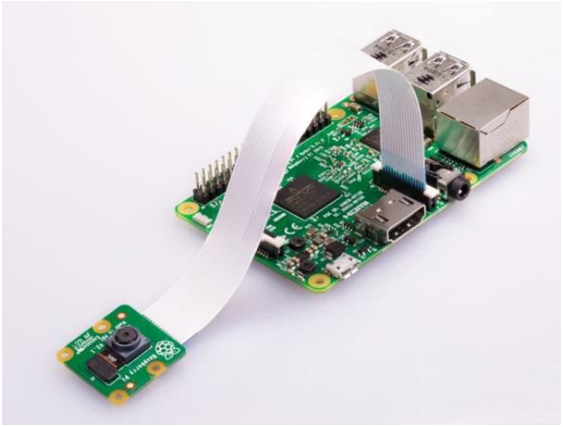

Fig. 2. Camera interfaced with Raspberry pi B+. [2]

VIII. SOLUTION IMPLEMENTED

This paper will provide a solution to the above issue of locker security by using image encryption. Whenever user will try to access the locker, the system will detect the face stored in the existing database. If the face matches then the lock will open. If the image does not match with the authorized user's database then system will click a image. The system will send that encrypted image to the authorized user, so that he/she gets to know about who is accessing his/her locker. That will provide a better and enhanced encrypted security to the locker. If any suspicious activity is made by that person, it will also help in further investigations if needed. Also, the authorized user can inform the authorities immediately for the necessary action to examine the culprit in case of any malpractice. The proposed paper of Face recognition-based locker system is an attempt to solve the issue of such malpractices and provide a centralized system with security to the authorized user.

IX. METHODOLOGY

The system first recognizes a person before the camera. If the person infront of the camera is verified with the images in the database then processor will activate motor system to automatically open the locker without taking the image of the authorized user. Capturing of image will take place whenever unauthorized user tries to access the locker. The captured

image will be encrypted using an algorithm and system will directly send the image to legitimate user along with details through notification/SMS. So, the owner/user can allow or deny access to the visitor.

X. WORKING

A. FACE CAPTURING AND RECOGNITION

For face recognition of the visitor who is present in front of camera, we use the "OpenCv" library on Raspberry pi B+ to initialize the camera. "OpenCV" library has following features:

- Image/video I/O, processing, display (core, img_proc, high_gui)
- Object/feature detection (object detect, features2d, non-free)

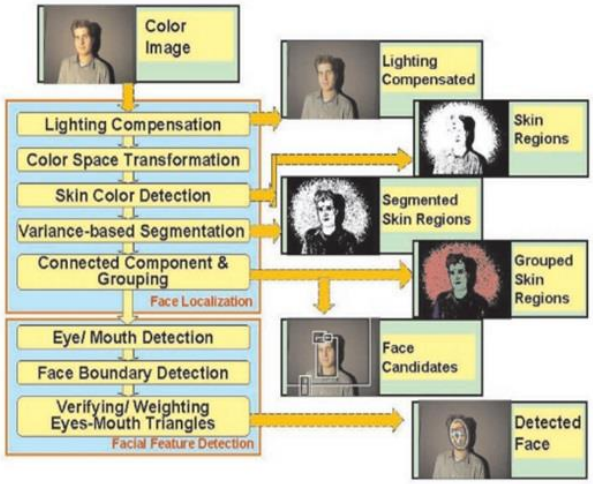

Fig. 3. Face Detection Algorithm. [3]

- Geometry-based monocular or stereo computer vision (calib3d, stitching, videostab)
- Computational photography (photo, video, superres)
- Machine learning and clustering (ml, flann)

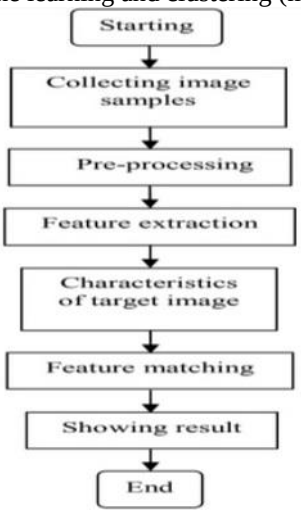

Fig. 4. Flow chart of face detection in a crowded location. [4]

B. DOOR LOCKING SYSTEM.

The system includes a locker which will be handled by solenoid locking latch. This latch will be interfaced with one of the input output ports of Raspberry pi. According to the code uploaded on Raspberry pi module, the system will lock or unlock the latch after recognizing the user's face. The latch would not be unlocked if the face is not recognized.

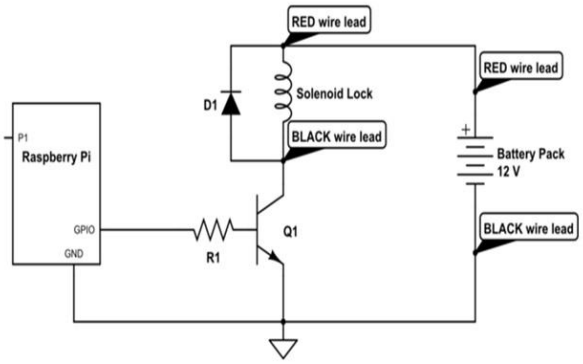

Fig. 5. Internal Block Diagram. [5]

The block diagram given represents the internal structure of solenoid latch which is interfaced with Raspberry pi.

C. ENCRYPTION AND USER INTERFACE

ECC stands for Elliptic Curve Cryptography is the latest asymmetric key encryption method offers stronger security. ECC key is very helpful for the current generation as more people are moving towards the Smartphone. As the utilization of Smartphone are growing, there is an emerging need for implementation of security with a more flexible encryption for business needs.

In mathematics, an elliptic curve is a plane algebraic curve defined by an equation of the following form

$$y^2 = x^3 + ax + b$$

which is non-singular, i.e., the curve has no cusps or self-intersections. Here, a and b are real numbers. The above equation is called a Weierstrass equation.

If we compare to the RSA and ECC algorithms, then 256-bit ECC is equal to 3072-bit RSA key. The reason behind keeping short key is the use of less computational power, secure and fast connection, ideal for Smartphones and tablets too. The elliptic curve cryptography (ECC) certificates allow key size to remain small while providing high end of security to the user. Elliptical Curve Cryptography (ECC) certificates key creation method is entirely different from previous algorithms, while relying on the use of a public key for encryption and a private key for decryption. By starting small and with a slow growth potential, ECC has longer lifespan. Elliptic curves are likely to be the next generation of cryptographic algorithms, and we are seeing the beginning of their use now.

RSA is too slow compared to ECC because ECC required smaller key size. The traditional public key cryptosystems were based on multiplicative group or multiplicative group field. These methods were further modified to have elliptic curve over large finite field.

The elliptic curve cryptography (ECC) does not directly provide encryption method. Designing a hybrid encryption scheme by using the ECDH (Elliptic Curve Diffie–Hellman) key exchange scheme can also be used to derive a shared secret key for symmetric data encryption and decryption.

- Calculate EncryptionKey(pubKey)-->(sharedECCKey, ciphertextPubKey)
- Generate ciphertextPrivKey = new random private key.
- Calculate ciphertextPubKey = ciphertextPrivKey * G.
- Calculate the ECDH shared secret: sharedECCKey = pubKey * ciphertextPrivKey.
- Return both the sharedECCKey + ciphertextPubKey.

Use the sharedECCKey for symmetric encryption. Apply the randomly generated ciphertextPubKey to calculate the decryption key later.

- Calculate DecryptionKey(privKey, ciphertextPubKey) --> sharedECCKey
- Calculate the the ECDH shared secret: sharedECCKey = ciphertextPubKey * privKey.
- Return the sharedECCKey and use it for the decryption.

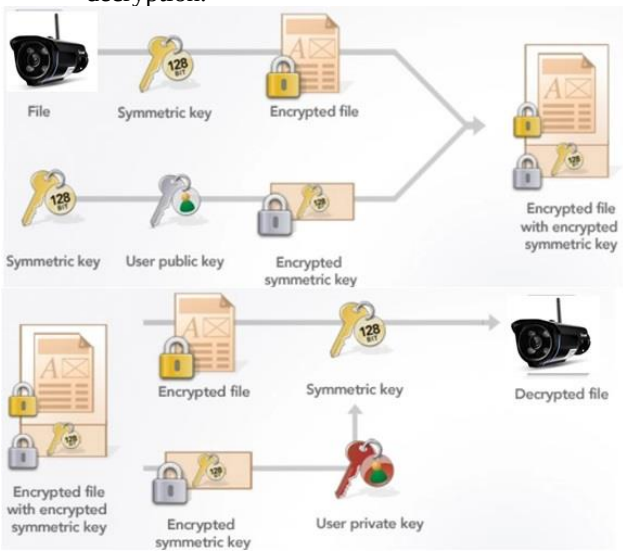

Fig. 6. Flowchart representing the ECC encrypting and decrypting process

XI. RESULT

This paper can resolve the problem of leakage of the authorized codes like OTPs and security pin. It will personalize the process of accessing any locking system. Based on the facial expressions of the user, the access will be granted to the authorized user. In case the person is not recognized, the primary authorized user will be notified regarding giving or denying the access which will personalize the process and provide encrypted security to the user. This is a real time application based which tells that there is a need to bring in a revolution in the security by making the procedure a little easy and more systematic for the officials. Since the system stores all the information which can be used for analysis and corrective actions with regard to any expected malpractices, access pattern of the legitimate user and of unauthorized user. This helps in identifying and providing services to the people in real time.

XII. ADVANTAGES

The tangible and non-tangible advantages are listed below

- Provides two stage security.
- High accuracy in terms of security.
- Security Resilience.
- Low cost and power consumption.
- Compact in size and standalone system.
- Uses web application for transaction.
- Easy to use, does not require special training or equipment. [6]

XIII. LIMITATIONS

Following are the limitations of the proposed solution

- Secondary user to wait for the processing from the primary owners end till the access is granted.
- Every new user will have to go through a procedure of database formation.
- Remote user giving access will require Internet access. However, a message will be sent to the authorized user that ‘Someone is trying to access your locker ’.

XIV. APPLICATION

The solution developed can be used for the following day to day applications

- Bank/Home/Industrial Security System
- School/College Treasuries
- VIP Vehicles
- Hospital and offices.

XV. CONCLUSION

This proposed solution is for highly secured reliable smart locker system.The system will effectively detect and control unauthorized access by considering safety of the locking system. It will convince the customers to use the specified system and hence defend their valuable things from robber and also any harm. Where top level security is needed, this system can be implemented. The future enhancement to this work could be done by adding some more aspect such as Field Programmable Gate Array (FPGA), Radio frequency Identification(RFID). Therefore, it improves the reliability of locker and unauthorized access will be minimized. The enhancement could be further applied to identify the illegal entrance.Security can be provided without the human intervention by automating the device using IOT. Here, any intrusion can be detected. This information can be used for maintenance of the devices and also for providing the

registered owner/user with any information about the intrusion. Thereby, this system can find its applications in many fields such as home automation, office security system and so on. Thus, by implementing this Smart locker security system using face recognition and image processing technology money, jewellery and any other important documents of a every citizen can be kept under safe custody. Using this smart technology a authorized person can only open the lock and collect the money, jewellery and any other important documents.

XVI. FUTURE WORKS

To record direct videos and send to nearest investigating agency such as police stations,etc. and also send alert voice messages to authorized persons.In addition to this the future scope of this paper is to develop Security system with combination of biometrics Scanning for more accurate identification of the person.

XVII. REFERENCES

[1] https://nevonpapers.com/face-recognition-door-lock-system-using-raspberry-pi .

[2] https://papers.raspberrypi.org/en/projects/getting-started-with-picamera .

[3] Rein-Lien, Hsu,Mohamed, Abdel-Mottaleb and Anil K.Jain, "*Face Detection in Colour Images*", IEEE Transactions on pattern analysis and machine learning, Vol 24, No.5, 2002. Copyright 2009 by IEEE Association.

[4] Deng-Yuan, Chao-Ho Chen, Tsong-Yi Chen, Jian-He Wu and Chien-Chuan Ko, *"Real-Time Face Detection Using a moving Camera*", 'International Conference on Advanced Information Networking and Applications Workshops'. Copyright 2018 by IEEE Association.

[5] https://raspberrypi.stackexchange.com/questions/92573/how-to-use-solenoid-lock-12v-dc .

[6] Mr. Lokesh M. Giripunje, Suchita Sudke, Pradnya Wadkar, Krishna Ambure, *"IOT Based Smart Bank Locker Security System"*, 'International Journal for Research in Applied Science and Engineering Technology (IJRASET)'. Volume 5 Issue XI November 2017- Available at www.ijraset.com. .

[7] Yasir M. Mustafah, Abbas Bigdeli, Amelia W.Azman, Brain C. Lovell, "*Face Detection System Design for Real Time High Resolution Smart Camera"*, 'International Journal of Recent Trends in Engineering and Research'-IEEE,2009.

[8] Suchitra, Suja P., Shikha Tripathi, "*Real-Time Emotion Recognition from Facial Images using Raspberry Pi II"*, IEEE-2016.

[9] Ahmed Shabaan Samra, Salah El Taweel Gad Allah, Rehab Mahmoud Ibrahim, "*Face Recognition Using Wavelet Transform, Fast Fourier Transform and Discrete Cosine Transform"*, IEEE 2004.

[10] Ruolin Zhang, Jian Ding, "*Facial Recognition Based on Wavelet Transform"*, IEEE 2012.

[11] Deng-Yuan, Chao-Ho Chen, Tsong-Yi Chen, Jian-He Wu, Chien-Chuan Ko, *"Real-Time Face Detection Using a moving Camera"*, 'International Conference on Advanced Information Networking and Applications Workshops'-IEEE,2018.

[12] Faiz Aman, Anitha C, *"Motion Sensing and Image Capturing based Smart Door System on Android Platform"*, International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)-IEEE.

[13] Arti Barde, Swapnil Bilbile, Shubham Waghmare, Prof. J. D. Dorve, *"Review on doorbell notify with image capture and forward through email"*, IEEE 2018.

[14] Sarita Kumari *"Encryption and Compression Techniques"*, https://www.ijecs.in/index.php/ijecs/article/download/3630/3378/ .

[15] Kamlesh Gupta, Sanjay Silakari, Ranu Gupta, Suhel A. Khan, *"An Ethical Way of Image Encryption Using ECC"*, First International Conference on Computational Intelligence, Communication Systems and Networks-IEEE, 2009.

[16] Quist-Aphetsi Kester, Koumadi, Koudjo M, *"Cryptographic technique for image encryption based on the RGB pixel displacement"*, IEEE Association,2012.

[17] Mohammed Ghazal, Samr Ali, Marah Al Halabi,Nada Ali, Yasmina Al Khalil, *"Smart Mobile-based Emergency Management and Notification System"*, 4th International Conference on Future Internet of Things and Cloud Workshops, IEEE Association 2016.

[18] Vaibhav Sharma, Pankaj Babu, Uttam Singh, Vipin Garg, Er Rahul Agarwal, *"Dual Secured smart Locker security System"*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering-2017.

[19] Hemlata Agarwal, Dimple Kalot, Ankita Jain, Narendra Kahtri, "*Image Encryption Using Various Transforms-A Brief Comparative Analysis*", International Conference on Magnetics, Machines and Drives (AICERA-2014 iCMMD)-IEEE.

[20] Sarita Kumari, *"A research Paper on Cryptography Encryption and Compression Techniques"*, International Journal Of Engineering And Computer Science 2017.