Design and Implementation of a Vault Security System

Md. Mahadi Hasan Moon
Dept. of Electrical and Electronics Engineering
American International University-Bangladesh
Dhaka, Bangladesh
mahadihasanmoon95@gmail.com

Debashish Kumar Ghosh
Dept. of Electrical and Electronics Engineering
American International University-Bangladesh
Dhaka, Bangladesh
debashishkumarghosh786@gmail.com

Nafiz Ahmed Chisty
Faculty of Engineering
American International University-Bangladesh
Dhaka, Bangladesh
chisty@aiub.edu

Md. Mahidul Islam
Dept. of Electrical and Electronics Engineering
American International University-Bangladesh
Dhaka, Bangladesh
mahidulislam2021@gmail.com

Md. Aurongo Jeb
Dept. of Electrical and Electronics Engineering
American International University-Bangladesh
Dhaka, Bangladesh
Aurongoj24@gmail.com

***Abstract*—In the era of technology, humankind is now looking for a rapid and prominent solution for day to day problems which can meet the demand and makes life easier. As security is an essential perspective with the end goal to protect our secret belongings, people are looking for an advance, unbreakable and user-friendly solution. However, considering a vault security system, we have to think a step further, as vaults usually used for higher security purposes. Security system using facial recognition, fingerprint scanner, password lock and RFID reader is going popular and common these days because of the availability and trustable security. The main goal is to implement a security system including all of these four sensors in single hardware which is able to provide much stronger security. The system is able to detect multiple human faces and also able to monitor the area continuously using one single camera sensor with the help of real-time video processing using open CV method. The system implemented in such a way that anyone who wants to enter the vault has to pass through all of these four (facial recognition, fingerprint, password and RFID scanner) steps. Neither one can be skipped. All the sensors are connected with Raspberry Pi to achieve the goal.**

Keywords— Security, Facial recognition, Open CV, Raspberry Pi, Fingerprint scanner.

I. INTRODUCTION

At present human work diminished by technology, thus technology plays a major role to ensure possession of individuals belongings. The automation of electronic equipment made it possible rather than wasting human resources and money for security [1]. Relying on technology this project develops a system that restrains human substances in a comprehensive way. This system can be served any individuals or any institutions to defend their confidential such as bank vault, money locker etc. Consider a breach of security the system is a combination of biometric and prior tech to ensure security escalation of this system. The objective is delivering security progression over extremely concealed premises effortlessly at an affordable cost [1]. Surveillance and facial recognition being operated by a camera for premium security purpose as it stores surveillance data on a memory chip for a definite period. The camera is continuously searching for a human face, and an authorizer is able to see the situation through the camera in real time. To achieve this goal, wireless communication established between the security system and the authorizer via VNC viewer. When a person places himself in front of the camera, the camera immediately scans his face with the image database stored in Raspberry Pi. The authorizer is able to see the name of that person at the top of his face in real time video. If the face doesn't match with the database, the name will be replaced by an unknown, and the system generates a sound which indicates the sound of an unknown person. After facial recognition, the system will ask for fingerprint, password and RFID card scan.

II. PRIOR AND RELATED WORK

Almost every smart device uses facial recognition to secure their devices from unauthorized people. It is also massively used for smartphone, network security and Deep learning-based video analytics. Other sensors like Fingerprint sensor, RFID reader are also used in security system and various application. A smart security system based on face recognition was proposed by Dwi Ana Ratna Wati and Dika Abadianto in 2017 [2]. The security system was based on MyRIO 1900 and programmed using LabVIEW [2]. The system can detect a person's face when the distance is less than or equal to 240 centimeters or even if the person uses various accessories like glasses or cap [2]. But it cannot identify the face if there is too much change or if the person is a little far from the camera. Another face recognition security system was implemented in 2018 by Ibrahim Mohammad Sayem and Mohammad Sanaullah Chowdhury using Raspberry Pi based on Python language with the help of OpenCV Library which is very similar to the face detection process used in this paper [3]. The device also sends email to the authorizer if there is an unknown person in front of the camera [3]. But as the system is only based on face detection, it is easy to break or bypass. An improved version of the security system was implemented by Teddy Mantoro and

Suhendi which can detect multiple faces at a single time using a hybrid method of Haar Cascade Classifier [4]. This system is more efficient and accurate compared to others. An advanced bank security system was designed by Raj Gusain, Hemant Jain and Shivendra Pratap which use face recognition, iris scanner and palm vein for authorization [5]. But the system is hard to maintain and very costly. Whether there is also a cost-effective solution, which is based on Arduino designed and implemented by Kanza Gulzar, Jun Sang and Omar Tariq [6]. But the time consumption is higher in that device and the device is not able to recognize a human face in real time video [6].

III. System Overview

The following "fig. 1" represents the block diagram of this system. To assure real-time broadcasting without interrupting the whole system, two of the separate virtual environments introduced. One is for live image processing (Open CV), and another is for other sensors (fingerprint, password and RFID). i2c communication is established to ensure a continuous connection between these two virtual environments. The camera sensor is continuously monitoring the area send signals to another environment if there is a person (e.g. alpha for an unknown, beta for David, gamma for Raj etc.). Thus, the Open CV environment is only focusing on video broadcasting and transferring signal. As a result, an authorizer is able to monitor the area continuously without any interruption. The second environment analyzes the signal received from the Open CV and commands the system for further instruction. In this case, if the signal represents an unknown person (e.g. the signal alpha which represents an unknown person) the system provides a buzz. But if the signal represents a known person (e.g. the signal beta which represents David) the system will command for fingerprint scan with the help of a 20x4 LCD display which placed at the system. When the person/visitor placed his/her finger on the fingerprint scanner, the system matched the fingerprint template with stored fingerprint of that person. If the fingerprint is matched, the system will give the confirmation and ask for a password to the person/visitor via a 20x4 LCD display. At this time, the visitor will place his password to the system via a 4x4 matrix keyboard and can also able to see whether it matched or not. If the password is matched, the LCD display confirmed it to the visitor and asked for RFID card scan. In this stage, the person/visitor will place the RFID card in front of the RFID scanner. And if the RFID card is matched, the system will activate the electronic door lock and allow that visitor/person to enter the vault.

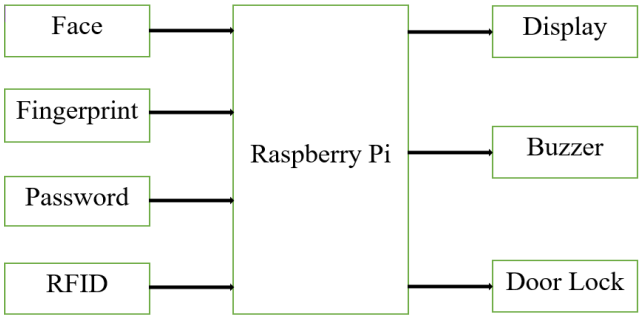

Fig. 1. System block diagram

If one of these steps is failed or not matched, the system will start from the beginning. Keep in mind that, password, fingerprint and RFID card vary from person to person (for example, if the face matches with David, the system require Divides fingerprint, password and RFID card). Neither of them can be entered changeable even if both of them are authorized.

IV. System Methodology

This section demonstrates the methodology of how this system work and interfacing with sensors and Raspberry Pi. Raspberry Pi is the main brainer in this system which interprets all the data to establish a decision.

A. Facial Recognition using Open CV

The facial recognition of a human is made possible with the help of Open CV library in python language. Open Source Computer Version Library which is known as Open CV, provide a common infrastructure for computer vision application [7]. Open CV library contains over 2500 optimized algorithms including a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms which can be used to detect and recognize a face, identify objects, classify human actions in videos, track camera movement, track moving object and many more [7].

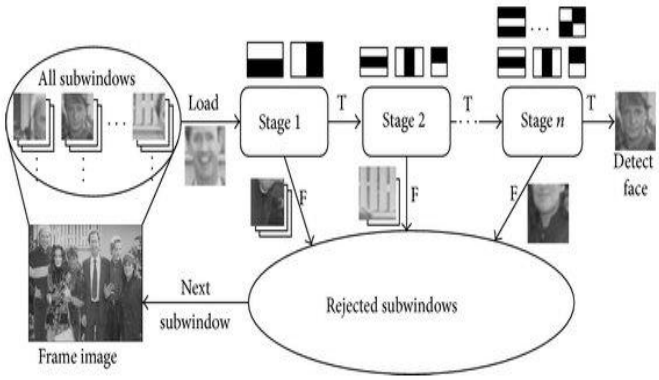

Fig. 2. Cascade structure for Haar classifiers [8].

Here, the goal is to detect/identify a human face in real time video. The algorithm used to achieve the goal is Haar Cascade Classifier. The hybrid method of Haar Cascade Classifier is used in this system so that the system can detect multiple faces at a single time. The cascade function is trained from a lot of positive and negative images to detect an object in other images [7]. Three types of features (edge features, line features and four-rectangle features) are used to train the classifier obtaining single value by subtracting the sum of pixels under the white rectangle from a sum of pixels under the black rectangle [7]. The classifier uses a fixed scale, for example, 50x50 pixels. Applying each and every feature on all the training images, the classifier can find the best threshold which will classify the faces to positive and negative [7]. As most of the image is non-face region, the features are grouped into different stages of classifiers and applied one-by-one [7]. The window, which passes all the stages is a face region [7]. Open CV contains two parts (Trainer and detector). Trainer is used to train the classifier and the detector is used to detect the face. To train the

classifier a dataset of images is needed. Every image contains cropped face of a human from a different angle in grey scale.

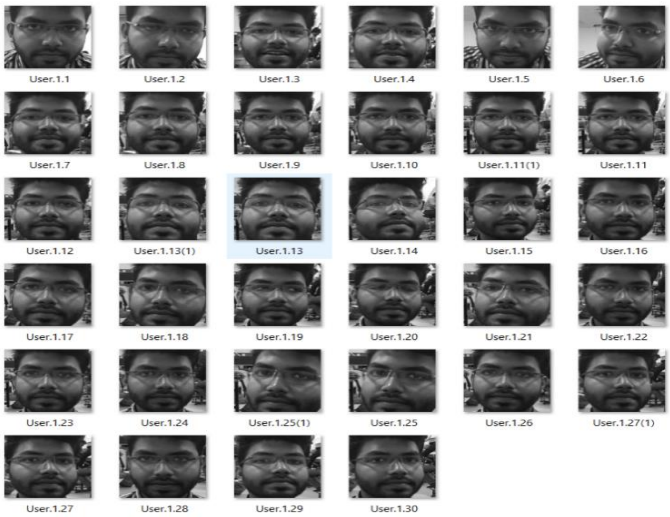

Fig. 3. Dataset of images in grey scale.

With the help of python language, the detector continuously matches the real-time image with those images stored in the dataset.

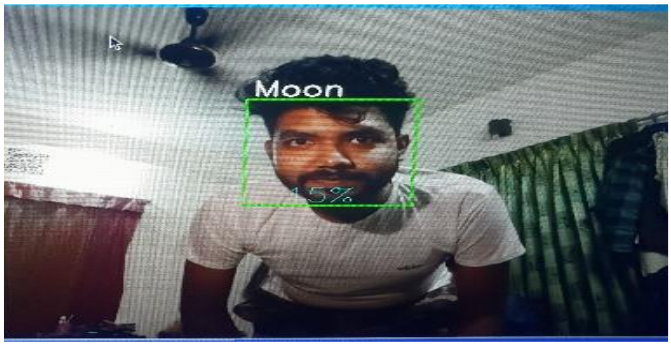

Fig. 4. Face recognition using Open CV.

B. *Fingerprint Scanner*

The fingerprint matching algorithm is responsible for producing a similarity score for the input and template prints. After analyzing similarity, the resulting match score will be compared with a certain threshold if both original fingerprints are formed (or not) from the same finger. Many methods are available for fingerprint matching among them minutia-based matching technique commonly used due to his less computational cost and good performance [9]. Minutiae-based algorithm established on local structure (point pattern matching), and global structure (finding the alignment of the corresponding pair of minutiae sets) [9].

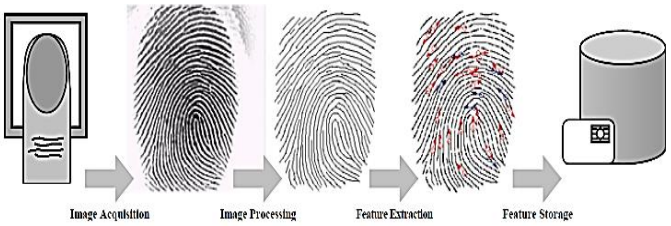

Fig. 5. Finger-print enrollment process [9].

First, the local structure of each minutia point is obtained in both minutiae sets to determine the similarity of fingerprints. The local structure describes minutiae spatial characteristics taking into account its meticulous neighborhood. This local descriptor (ridge ending, ridge bifurcation) is an invariant feature of rotation and translation that is inherent in minutiae [9]. Comparing both the template and the input minutiae a similarity matrix formulated in order to analyze the score of similarities between any combination of minutiae pairs. Local structure similarity scoring allows the best-matched minutia pair to be identified and exercised as a reference for global structures.

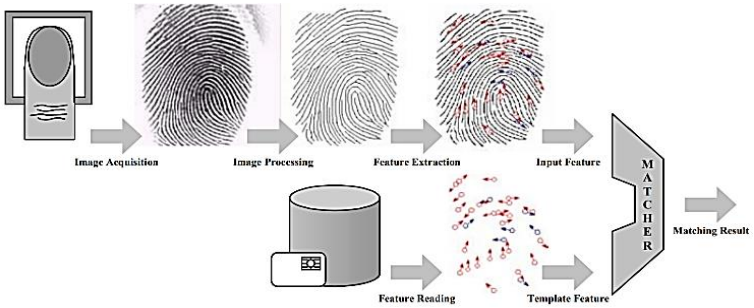

Fig. 6. Finger-print authentication process [9].

Global structures defined by minutiae sets where it describes the spatial characteristics from a reference point. After accomplished with the global structures the system decides the results obtain from global structure compared with the certain threshold.

C. *4x4 Matrix Keypad*

The 4x4 matrix keypad is used to input a password into the Raspberry Pi. The number of pin requirement for digital input can be reduced, by using the matrix keypad. The matrix keypad contains 16 pins in 4 rows and 4 columns. The keypad has 8 pins. 4 is for columns and 4 is for rows. By making 4 rows as output and considering them logic low, and 4 columns as input, the possible key pressed can be detect when correspondent columns gets o or low [10]. When the switches are not pressed it needs to make the column pins as high or 1, otherwise it is not possible to detect the logic changes when the switch is being pressed [10]. But there is a chance of spikes or noise generation if multiple switches are pressed at a time [10]. To avoid the noise, a few milliseconds delay is required to recheck the switch conditions [10].

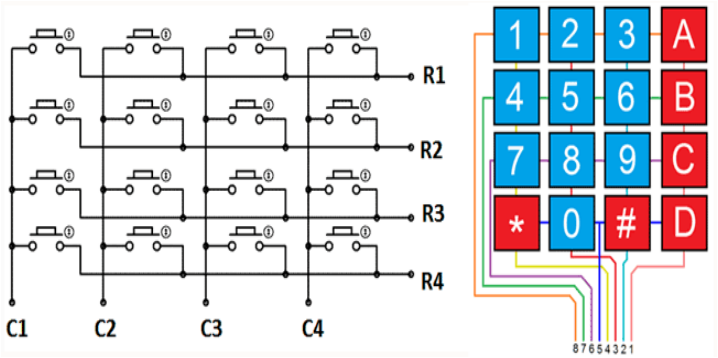

Fig. 7. Connections of a 4x4 matrix keypad [10].

D. *RFID Card Scanner*

The Radio frequency identification namely called as an RFID. It has two main components a transponder, associated with the object which is supposed to identify. The other one is Transceiver which consists of a radio frequency module, a control unit and antenna coil, which generates a high-frequency electromagnetic field [11]. When the transponder approaches towards the transceiver, a voltage induced due to induction and a microchip inside the transponder gets power to operate. Load manipulation technique is used to transfer data between transponder and transceiver. Switching of tag antenna using control unit causes a voltage drop that resultant in ones and zeroes [11]. This data used to transmit the signal between the transponder and transceiver.

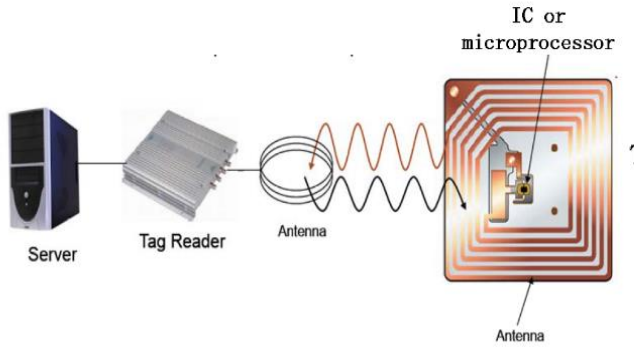

Fig. 8. RFID system [11].

V. Experimental Setup & Programming Flow Chart

The Experimental Setup with all the interfaced components are shown in "Fig. 9".

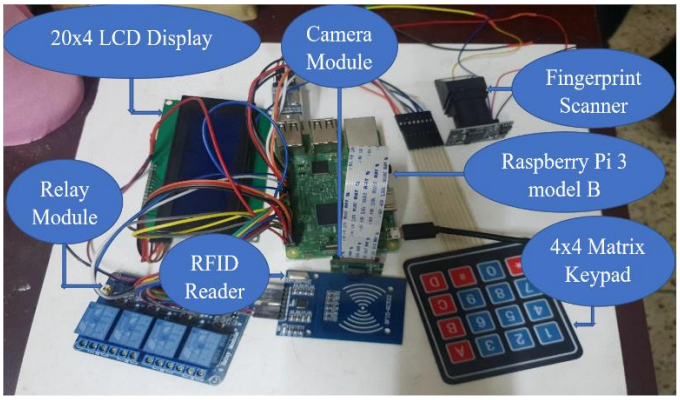

Fig. 9. Experimental setup of the system.

The programming flow chart of the system is shown in "Fig. 10".

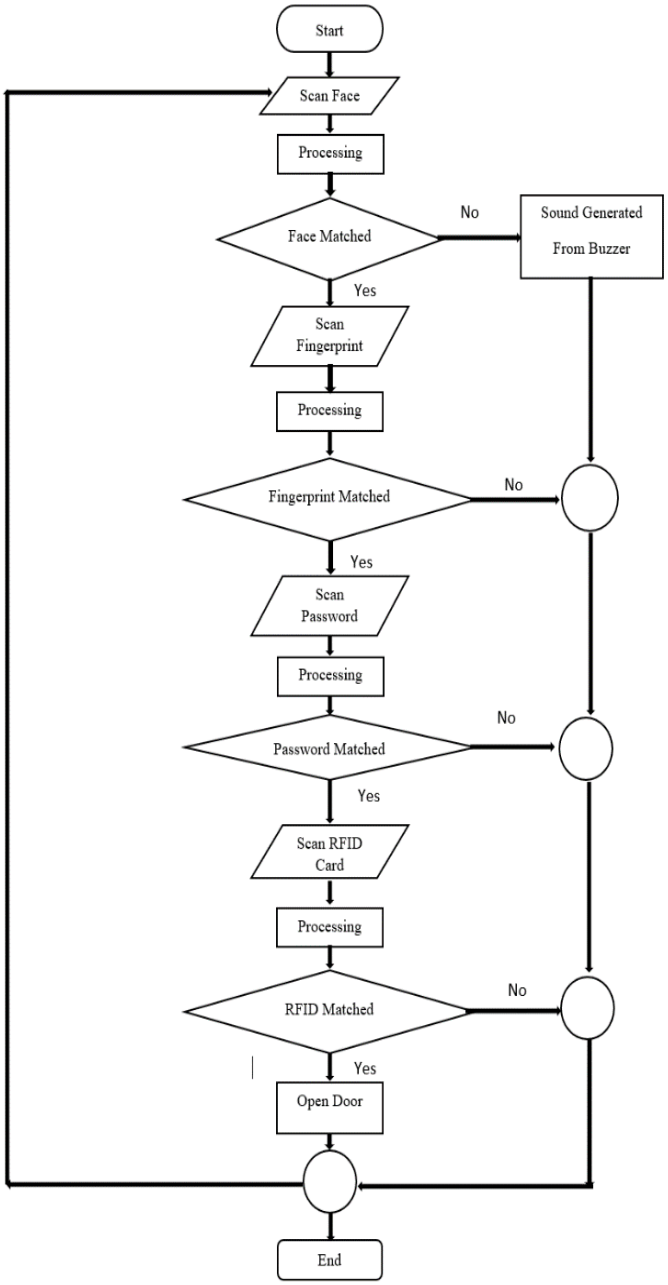

Fig. 10. Flow chart of the program.

VI. Implementation & Results

The system is developed in a single Raspberry Pi board using python language. Raspberry Pi is a mini portable onboard computer which has 4 USB ports, an Ethernet port, a HDMI port, a 3.5mm audio jack, onboard camera and display port, a MicroSDHC slot, 40 GPIO pins including power and ground and a micro USB port to provide 5 volts dc power. The system is powered by a Broadcom BCM2837 chip with ARMv8-A instruction set architecture (ISA) using 4 core Cortex A53 based CPU clocked at 900 MHz. It has 1GB RAM shared with Broadcom VideoCore IV GPU. The Raspberry Pi 3 model B also comes with on-board network (2.4 GHz wireless and Bluetooth 4.2). The system consists of a controlling device (e.g. laptop, smartphone etc.) over same Wi-Fi connection, a camera module, fingerprint scanner, matrix keypad, RFID reader/scanner, relay module, electronic door lock, buzzer and some LEDs. "Fig. 11" shows the real time monitoring over wireless communication via VNC viewer.

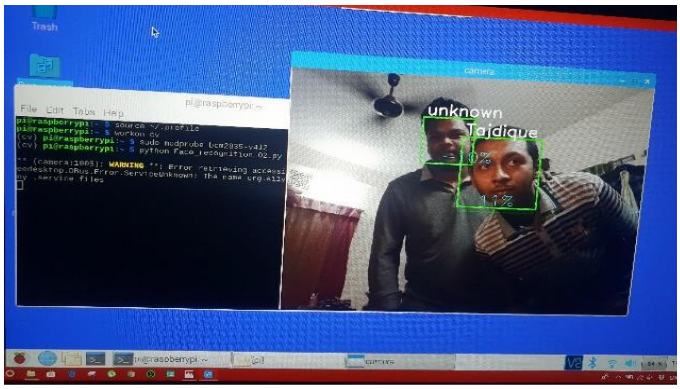

Fig. 11. *Monitoring real time video streaming via VNC viewer.*

A 20x4 Character LCD Display is used in this system to communicate with the user. The display is connected with the GPIO pins of the Raspberry Pi. An I2C LCD Gadgeteer module is used to reduce the connecting wire. The display provides instructions to the user. “Fig. 12” shows the initial state of the LCD display.

Fig. 12. Initial stage of the LCD display.

The Raspberry Pi Camera Module V2 is connected with the Raspberry Pi using onboard camera port for the purpose of real-time video broadcasting and facial recognition. The Camera Module has a 8 megapixel Sony IMX219 sensor which can be used to take high-definition video and photo. The camera identifies the person/visitor and the LCD display sends the confirmation and farther steps to the person/visitor which are shown in “Fig. 13” and “Fig. 14”.

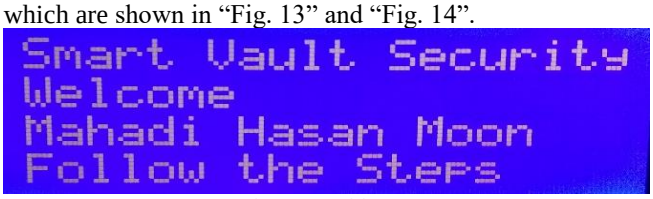

Fig. 13. Confirmation of facial recognition.

Fig. 14. Instruction for finger placement.

R30X Fingerprint Sensor is used to scan and identify the fingerprint of the visitor. It requires a UART interface over USB port. To connect the Fingerprint Sensor with Raspberry Pi a PL2303 USB to TTL Converter is needed. The voltage requirement is in between 3.6 to 6.0 volts. The Fingerprint Sensor will activate after facial recognition. The visitor is able to see whether his/her fingerprint is matched or not. All the results and steps are being placed on LCD display which will shown in “Fig. 15” and “Fig. 16”.

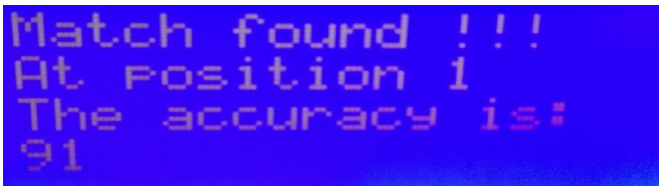

Fig. 15. Confirmation of fingerprint match.

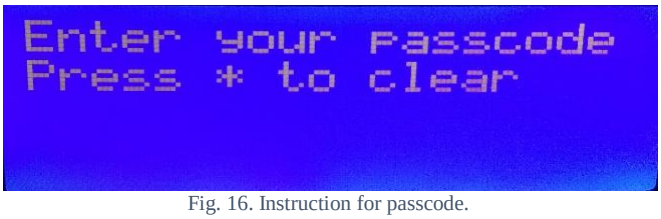

Fig. 16. Instruction for passcode.

A 4x4 matrix keyboard is used to enter the password to the system which is directly connected with Raspberry Pi GPIO pins. From total 8 connectors, 4 of them are input and 4 of them are output. The process wise results are shown in following figures from “Fig. 17” to “Fig. 19”.

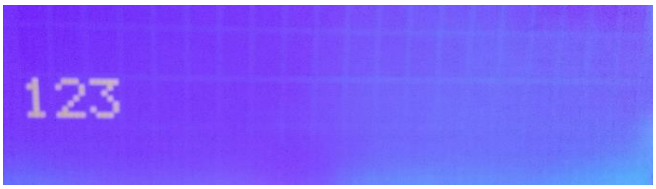

Fig. 17. Input Password.

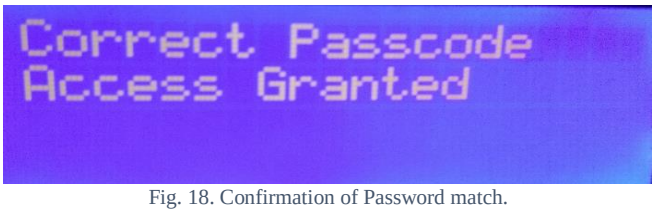

Fig. 18. Confirmation of Password match.

Fig. 19. Instruction for RFID Card placement.

To read and write RFID cards, MFRC522 RFID sensor is used. It is a highly integrated RF frequency reader/writer IC for contact less communication at 13.56 MHz and also supports ISO/IEC 14443 A/MIFARE mode. The voltage requirement for the sensor is 3.3 volts. It is the last and final stage of this security system. After placing the RFID card on the RFID sensor, the system matched the card number and gives the confirmation which shown in "Fig. 20".

Fig. 20. Confirmation of RFID match.

After completing all the steps, the system turned on the 12 volts electronic door lock which is connected with the raspberry pi via relay module. A 1100mAh 12 volts Lithium Polymer Battery is used to power the electronic door lock. “Fig. 21” shows the complete setup of the system.

Fig. 21. Complete setup of the system.

VII. Limitations

Each project has some limitation that can be eliminated by conducting future research or development. In this project, the calculation of entering people in a vault or confidential room is not ensured. Face detection of the night mode is not available. In the limitation side, the real-time delay in broadcasting the surveillance has been counted.

VIII. Conclution

The ultimate goal is to provide society with a reliable and uncompromising security system that people can afford to obtain better security assurance. The system improvises the multi-step security authentication to obtain a result. It strengthens security by effectively limiting trespassing, heist, or security threats of any kind. This project has developed with the raspberry pi embedded with the identification sensors. The OpenCV environment has used for face detection, which bases on viola jones algorithm using Haar cascade classifier which superimposes the positive image over a set of negative images known as favored face detection classifier in OpenCV. The entire project framework has programmed with the python language. Future development can be developed adding gas sensors, humidity sensors for measuring their concern-parameters. An emergency alarm can be generated in the event of Emergency. Although the system is designed for vault security, it can be used for any security purpose like home security, office security etc. Considering the social impact of this project, it has done with a lot of dedication and integrity.

Acknowledgment

We would like to thank the faculty of Computer Science and Engineering (CSE) of East West University (EWU) and organizing committee for arranging this conference. Also, we would like to express our gratitude to IEEE Bangladesh section.

References

[1] K. H. S. Murugan, V. Jacintha and S. A. Shifani, "Security system using raspberry Pi," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, 2017, pp. 863-864.

[2] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, 2017, pp. 342-347.

[3] I. M. Sayem and M. S. Chowdhury, "Integrating Face Recognition Security System with the Internet of Things," *2018 International Conference on Machine Learning and Data Engineering (iCMLDE)*, Sydney, Australia, 2018, pp. 14-18.

[4] T. Mantoro, M. A. Ayu and Suhendi, "Multi-Faces Recognition Process Using Haar Cascades and Eigenface Methods," *2018 6th International Conference on Multimedia Computing and Systems (ICMCS)*, Rabat, 2018, pp. 1-5.

[5] R. Gusain, H. Jain and S. Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, 2018, pp. 1-5.

[6] K. Gulzar, Jun Sang and O. Tariq, "A cost effective method for automobile security based on detection and recognition of human face," *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, Chengdu, 2017, pp. 259-263.

[7] J. J. Patoliya and M. M. Desai, "Face detection based ATM security system using embedded Linux platform," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, 2017, pp. 74-78.

[8] Kim, Mooseop & Lee, Deok Gyu & Kim, Ki-Young,” System Architecture for Real-Time Face Detection on Analog Video Camera,” International Journal of Distributed Sensor Networks. 2015. pp.1-11.

[9] M. Fons, F. Fons and E. Canto, "Design of an Embedded Fingerprint Matcher System," 2006 IEEE International Symposium on Consumer Electronics, St. Petersburg, 2006, pp. 1-6.

[10] *Circuit Digest-4x4 Matrix Keypad Interfacing with PIC Microcontroller*[Online]. Available: https://circuitdigest.com/microcontroller-projects/4x4-keypad-interfacing-with-pic16f877a . [Accessed: 3-March-2019]

[11] Y. Chen, Z. Chen and L. Xu, "RFID System Security Using Identity-Based Cryptography," *2010 Third International Symposium on Intelligent Information Technology and Security Informatics*, Jinggangshan, 2010, pp. 460-464.