DUAL BIOMETRIC ENCRYPTED AUTHENTICATION USING RASPERRY PI PROCESSOR

Sivasankari Narasimhan
Assistant Professor, Electronics and Communication Engineering,
Mepco Schlenk Engineering College, Virudhunagar Dt, (India).
E-mail: sivani.sivasankari@gmail.com ORCID: https://orcid.org/0000-0002-3162-4751

Muthukumar Arunachalam
Assistant Professor, Electronics and Communication Engineering,
Kalasalingam University, Virudhunagar Dt, (India).
E-mail: muthuece.eng@gmail.com ORCID: https://orcid.org/0000-0001-8070-3475

Recepción: 05/12/2019 **Aceptación:** 20/12/2019 **Publicación:** 23/03/2020

Citación sugerida:
Narasimhan, S., y Arunachalam, M. (2020). Dual biometric encrypted authentication using Rasperry PI Processor. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Marzo 2020*, 35-49. http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

Suggested citation:
Narasimhan, S., & Arunachalam, M. (2020). Dual biometric encrypted authentication using Rasperry PI Processor. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Marzo 2020*, 35-49. http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

ABSTRACT

Security is one of the main concerns in many sectors especially in banking. Many protection mechanisms such as passwords and number locks, PIN numbers have been used to identify the correct person. The biometric protection mechanism using fingerprints are also implemented. To ensure more security double biometric factors are implemented in this paper. Voice is a powerful factor to identify a speaker who is holding the account in banks. In addition to voice, usual face biometric features also considered for security in bank lockers. Both are transformed into encrypted format and stored to avoid database hacking. In this, Raspberry Pi board is used for implementation. To manipulate voice, devices like USB microphone and sound cards are used. For processing face image Raspi Cam is used. When the given image and voice matches with that of the image and voice stored in the database, then login process starts else the person trying to unlock the locker is not the bank account holder. For new users, signup process will be provided by administrator by capturing voice and face images for enrollment. This system can be helpful for maintaining the customer's confidentiality in bank lockers.

KEYWORDS

Authentication, Face recognition, Voice recognition, Encryption, Enrollment.

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

1. INTRODUCTION

The most basic requirement of any bank locker is high security and getting high privacy regarding bank locker. Every person has precious accessories like jewelry or cash in it, so authentication of the person who wants to use the locker is very important. Effective security can be provided by using face and voice recognition biometrics. In olden days secret key is used by customers. Now-a-days customers' biometric attributes are additionally included which are unique and act as one identity for individual. A secret key can be stolen or changed. But biometric characteristics won't be changed, for example, an individual's face or voice can't be changed or imitated. The distinguished protocol for the execution of a bank locker security framework, with the authentication of human face and voice recognition, to confirm the person's character has been proposed in this paper.

The database creation phase for banking utilizes image and voice of the client to be stored using Raspberry pi. The access to open the locker is provided only to the authorized customers. If the image and the voice are not present in the database, the access permission is denied.

2. RELATED WORKS

Sahani, Nanda, Sahu and Pattnik (2015) proposed a remote access control framework for smart home condition. Raspberry Pi based entry to control and design home security framework through site page with ZigBee is implemented. The framework distinguishes the visitor's quality and exchanges the picture through email and SMS by GSM to already stored numbers. The client can specifically login and cooperate with the inserted gadget progressively without the need to keep up an extra server.

Baby, Munshi, Malik, Dogra and Rajesh (2017) proposed an empowering mechanism for home automation with web application for electrical apparatuses (such as fan and light) control. They are dependent on sensor inputs to indicate movements and temperature. The lock can be controlled by giving voice directions. Thus, utilizing this framework, it is currently progressively advantageous to control the machines in homes.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

Kaur, Sharma, Jain and Raj (2016) proposed an automation system using voice. With voice as information, the system interprets or follows the importance of that input and creates a proper voice yield. Utilizing voice as information, it tends to be changed over to content. This work experiences the disadvantage that just predefined voices are feasible, and it can store just restricted voices. Subsequently, the client can't get the full data.

Senthilkumar, Gopalakrishnan and Sathish Kumar (2014) wished-for image capturing system based on Raspberry Pi. Face acknowledgment is the principal concern and has the least false acknowledgment rate. The structured stage gains the pictures and stores them into the ongoing database, which is later utilized for contrasting the principles of the clients.

Shah, Patel and Patel (2018) develops a model for storing the data in computers using Rasperry PI. It can be programmed with languages like JAVA, HTML, .NET, Python in it. Rasperry PI and digital signal controller (DSC) is designed for monitoring multiple parameters based on Ethernet.

Ramani, Selvaraju, Valarmathy and Niranjan (2012) projected a secure bank locker system based on RFID and GSM. In this framework, true individual can recover cash from bank locker. This is used to approve the client and open the entryway continuously for bank locker secure access. This is more secure than different frameworks. The RFID examines the ID number from detached tag and send to the microcontroller, if the ID number is legitimate, at that point microcontroller send the SMS and ask for the confirmed individual portable number. The secret code is necessary to open the bank locker. If the individual sends the secret word to the microcontroller, it will check the passwords entered by the console and get verified from the cell phone. If these two passwords are coordinated, the locker will be opened else it will be stay in bolted position. This framework is more secure than different frameworks since two passwords required for confirmation.

Our project gives the following significant works:

- With face and voice recognition for accessing the bank locker account.
- Login page to unlock the locker of the bank account holder.
- Signup page for a new user.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

- Encrypted database for storing the voice and facial features.

The remaining sections are organized as follows: section 3 provides the proposed methods and section 4 gives the implementation results followed by conclusion in section 5.

3. PROPOSED METHODOLOGY

The main module in our processor is Rasperry Pi kit which collects all details regarding biometric and customer's details. Raspberry Pi 3 is used for programming to create login and signup web pages by coding in PHP, capturing images, recording voice, creating databases for storing the necessary details, performing image encryption process and to perform voice and image recognition.

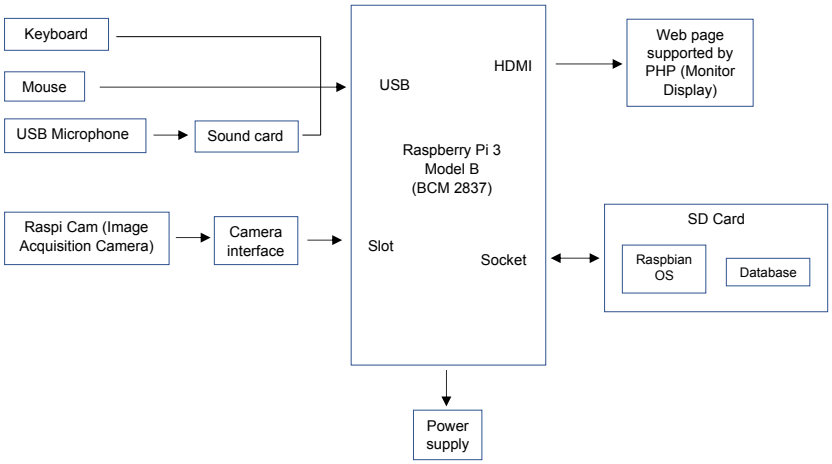

Figure 1. Overall block diagram.

Raspbian Stretch OS is used by this kit. The modules connected with Rasperry kit is shown in Figure 1. Now let us see the process involved and used components in the encrypted authentication process one by one.

3.1. ENROLLMENT AND AUTHENTICATION PROCESS

Bank customers account number, type of account and the persons involved in the particular ID and their facial biometric features, voice features have been collected in the process of new user enrollment. In bank database, they are stored in encrypted form.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

During login phase the customer must provide all the details to open the locker. If the details match with the database, then the locker will be opened; otherwise the person trying to open the locker is blocked by bank and alert is given to police station also. Sometimes voice features do not get matched and the facial biometrics gets matched, then there will be some likelihood that he/she may be the customer. But if face does not match, he should not be allowed to access the locker. Because face is an important feature in any individual. But voice may vary due to some unavoidable situations like cold, fever.

3.2. FACE RECOGNITION MODULE

Camera module captures image when capture image button is pressed in the webpage. When the button is pressed, the python code for capturing image should run. While storing that image in the database during signup, the image can be encrypted for better security. This 8mp camera module is equipped for 1080 pixel video and still pictures that associate straightforward to Raspberry Pi. The camera module associates with the Raspberry Pi board through the Camera Serial Interface (CSI) connector to interface with camera. The CSI transport is prepared to have high information rates, and it only conveys pixel information to the processor. The picture of Raspi camera is portrayed in Figure 2.

Figure 2. Raspi camera.

From the continuous pictures face image must be detected and recognized. Face detection is performed by HAAR Cascade Classifiers (Tabora, 2011). There is eye, head, and mouth and nose detectors in the HAAR cascade classifiers. Detected and processed face is compared to a database of known faces, to decide who that person is. Face Identification

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

can be performed reasonably dependably, for example, with Open CV's face Identifier, working in about 90-95% of clear photographs of an individual looking forward at the camera. The preprocessing is done to efficiently recognize the face of the customers. For that preprocessing, Eigen Face methodology concept is applied.

It is normally harder to identify an individual's face when they are seen from the side or at an edge, and occasionally this requires 3D Head Posture Estimation. Principal component analysis (PCA) is a statistical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components. If the image elements are considered as random variables, the PCA basis vectors are defined as eigen vectors of the scatter matrix (ST) defined as:

$$S_T = \sum^M (x_i - \mu) \cdot (x_i - \mu)^T \qquad (1)$$

where μ is the mean of all images in the training set and xi is the ith image with its columns concatenated in a vector.

3.3. VOICE RECOGNITION MODULE

Voice authentication is implemented in Raspberry Pi in order to add an extra layer of security. Raspberry Pi does not have a sound card and therefore it won't support microphones on audio jack, so we should use a USB microphone. Hence some additional modules are installed in Python for recording voice to perform voice recognition. The recorded voice should be of maximum 3 seconds duration. The customer can speak any of his/her secret code in their own tone. Voice recognition is done by matching the pitch of the captured speech signal and the speech stored in the database. Basic process is shown in Figure 3.

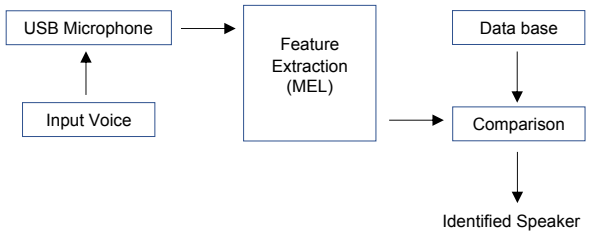

Figure 3. Voice biometric processing.

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

Microphone is used to capture the voice of the customer. It is a transducer that changes over sound into electrical signal.

Figure 4. (a) Sound card (b) Microphone

Components used in our voice processing are shown in Figure 4. Raspberry Pi kit does not have an internal sound card. Also, the voice signal must be amplified prior to be given as input to the processor. For all these purposes an USB sound card must be used in between the USB microphone and the kit.

The sequence of steps followed in voice processing is:

- Frame the signal into short frames.
- For each frame, periodogram, power spectrum is calculated.
- Mel filter bank is applied to the power spectra.
- Energy is summed in each filter.
- DCT of Logarithm of all filter bank energies is taken.
- DCT coefficients 2-13 are kept and the remaining things are discarded.

In certain cases, the image may get matched, but the voice may not get matched. These cases may arise because of an individual's personal conditions. These situations are unavoidable. In such cases, the algorithm must be designed in such a manner that at these situations, the concerned person must be allowed to login by satisfying some threshold.

3.4. ENCRYPTION

The image obtained from RASPI camera is encrypted with AES algorithm before saving it in database. The Advanced Encryption Standard (AES) is a symmetric-key block cipher

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

algorithm with Cipher Block Chaining Mode. As usual with the normal AES algorithm (Stallings, 2005) Substitute bytes, shift rows, Mix columns, Add round keys operations are taken place, Encrypted facial biometric data is stored in database.

4. IMPLEMENTATION

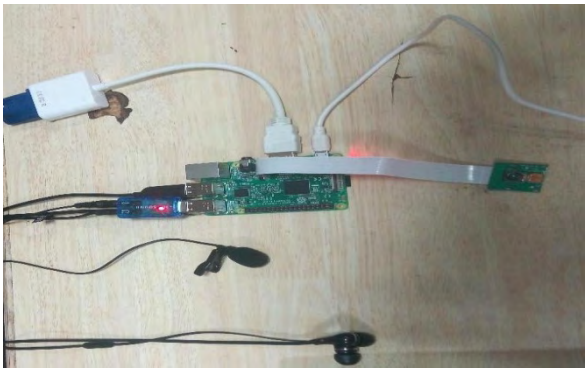

Figure 5. Hardware Setup.

Through the USB ports the keyboard, mouse and the sound card with which the microphone connection are to be made are connected. A High Definition Multimedia Interface (HDMI) to Video Graphics Array (VGA) connector is used to connect the processor to the monitor. An SD card is inserted in the slot provided at the right side. Raspi Camera module is connected to the Raspberry Pi camera interface. Hardware set up is shown in Figure 5. The face recognition module is to capture images through the Raspberry Pi camera. The images get stored in database which is created. The images shown in Figures 6(a) and 7(a) are registered face, which is stored as encrypted form as shown in Figures 6(b) and 7(b).

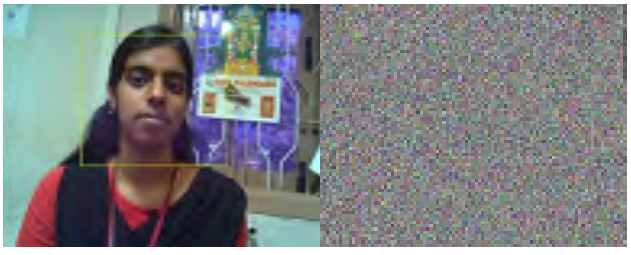

Figure 6. (a) Captured Image 1 (b) Encrypted image.

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

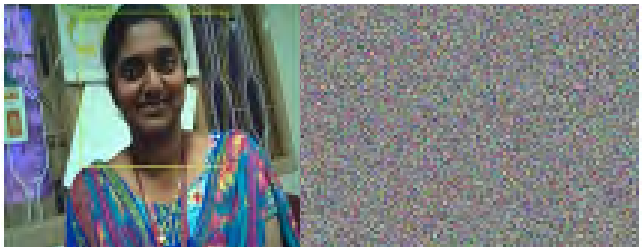

Figure 7. (a) Captured Image 2 (b) Encrypted image.

The face image from the passport size photo is located first and facial image is encrypted and stored in database. By using python coding for face recognition, first we are detecting the face and then the captured image is compared with the image that has already been captured and stored in the database. The stored images should be optimized because of the total data storage capability of the system. Since the encrypted image stores much space than the captured image, they must be compressed and then must be stored. The database contains the details of all the registered customer details. The database must be created through MySQL. The details to be stored are the customer ID, customer name, customer image and the customer voice. The sample login page created in our work is shown in Figure 9.

Voice Recognition Module: The audio signal input should be more or less 3 seconds of a wave (.wav) format file. Because for authentication due to the storage space constraints, there is limitation imposed on the length of the audio signal. That audio signal must be a code word of the customer of his own desire. The pitch values only will be compared for authentication. The sample voice images are shown in Figure 8.

Login page (shown in Figure 10) has been created for the customer to login to access his/her bank locker if he is an already registered user. This login page asks for customer id, customer image and the customer voice. The customer image and voice are given as real time data. If the image is not registered and have customer ID and ask for authenticity means he/she will be marked as intruder.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

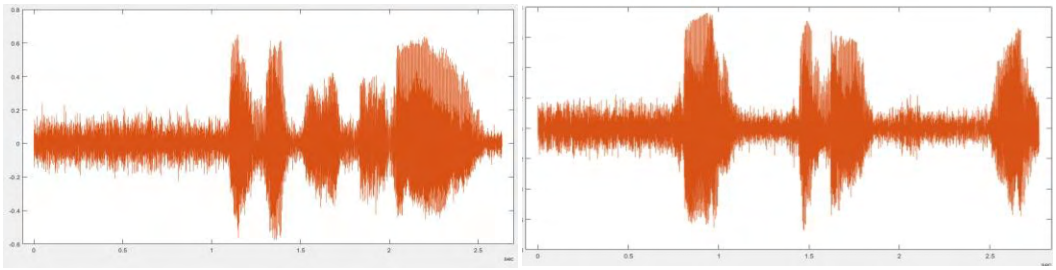

Figure 8. (a) Sample voice 1 (b) Sample voice 2.

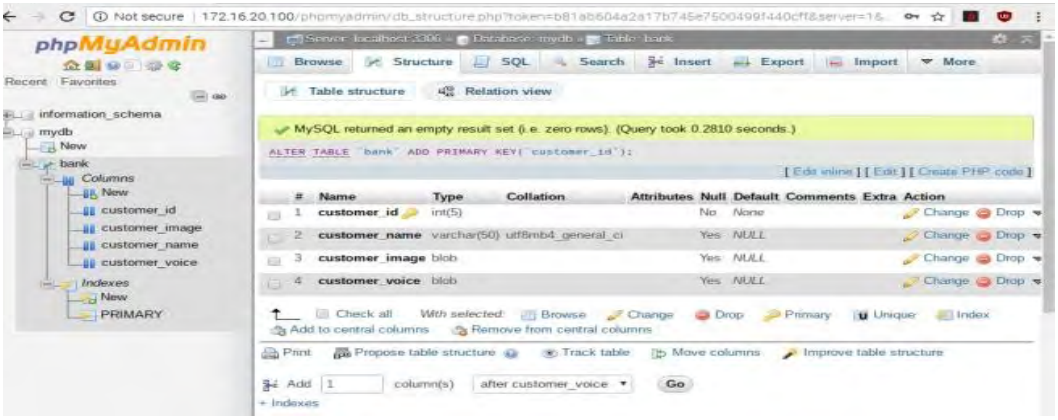

Figure 9. Database template.

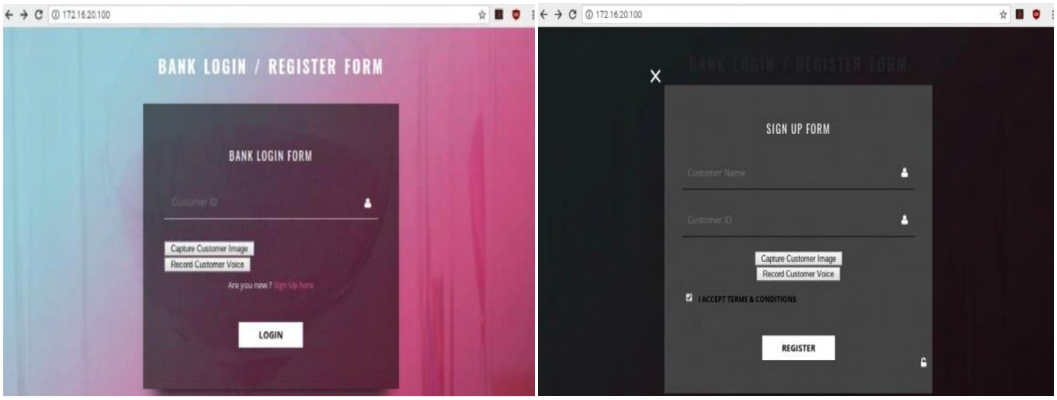

Figure 10. (a) Login form (b) Sign up form.

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

4.1. MATCHING

The fresh images taken at the time of verification are compared in time by time manner with the stored templates for both voice and face image in our work.

Our work has been compared with others with methodology. Certain works have been designed for some intended purposes and they are designed to meet that. and the comparison of some works is given in Table 1.

Table 1. Comparison of previous works.

References	Biometric trait	Additional Hardware Module used	Algorithm	Intended Actions
Sahani *et al.* (2015)	Face	GSM/GPRS module (For transferring information to the owner)	Eigen Methodology	The photograph of person enter into house is captured and sent to the owner for allow/deny
Baby *et al.* (2017)	Voice	Rasperry PI	Voice to text and database storage	To close the home, switch off the lights and fans.
Kaur *et al.* (2016)	Voice	Wiki, iCloud id	Voice to text	It searches the missed iPhone, Helps to search the movie, helps to search Wikipedia,reading news,describe weather.
Gyulyustan & Svetoslav (2017)	Voice	Rasperry PI	Hidden Markov Model	Speech recognition with intended words and carry out the action behind that.
Senthilkumar (2014)	Face	EICSRS platform	Eigen faces methodology	If the user is not in the stored template, reject the user.
Kishore Bhanse & Jaybhaye (2018)	Front image	Google API	Machine Learning, Neural network	To alert the user regarding correct user, or intruder.
Proposed	Image and voice	Rasperry PI	Eigen Methodology, AES (image Encryption)	Both image and voice database information's are stored in the encrypted format to avoid the hackers template hacking.

5. CONCLUSION

This work proposes the design and the development of an interactive smart bank locker security system with the raspberry pi as the processor. The PC used for interaction can be replaced with low-cost processors which would provide the administrator with parameters of the entire remote device. This setup can be implemented in banking sectors for improved security of bank lockers. It can be used to avoid access of unauthorized persons. It can be

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

easily used to track the intruders. Since, face and voice both the important features are used as the key factors, it provides an as an excellent security system. It reduces the risk of threat. Since encryption algorithms are employed, the customer images can be stored securely.

As a future scope, a separate application can be created to send the picture of the unauthorized customer through E-mail or through any other active social media in which the customers will be active and alert them with this intruder information. Also, the voice of the customer to be stored can be encrypted and then can be stored in the database. This will be an additional factor to enhance the security of bank lockers.

http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

REFERENCES

Baby, C. J., Munshi, N., Malik, A., Dogra, K. & Rajesh, R. (2017). Home automation using web application and speech recognition. In *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India*. IEEE. https://doi.org/10.1109/ICMDCS.2017.8211543

Gyulyustan, H., & Svetoslav, E. (2017). Experimental speech recognition system based on Raspberry Pi 3. *IOSR Journal of Computer Engineering (IOSR-JCE), 19*(3), 107-112. https://doi.org/10.9790/0661-190302107112

Kaur, S., Sharma, S., Jain, U., & Raj, A. (2016). Voice Command System Using RaspberryPi. *Advanced Computational Intelligence An International Journal (ACII), 3*(3), 43-49.

Kishore Bhanse, V., & Jaybhaye, M.D. (2018). Face Detection and Tracking Using Image Processing on Raspberry Pi. *International Conference on Inventive Research in Computing Applications (ICIRCA). Coimbatore, India*. IEEE. https://doi.org/10.1109/ICIRCA.2018.8597246

Ramani, R., Selvaraju, S., Valarmathy, S., & Niranjan, P. (2012). Bank Locker Security System based on RFID and GSM Technology. *International Journal of Computer Applications, 57*(18), 15-20. https://www.ijcaonline.org/archives/volume57/number18/9213-3761

Sahani, M., Nanda, C., Sahu, A. K., & Pattnik, B. (2015). Web-Based Online Embedded Door Access Control and Home Security System Based on Face Recognition. In *2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT). Nagercoil, India.* IEEE. https://doi.org/10.1109/ICCPCT.2015.7159473

Senthilkumar, G., Gopalakrishnan, K., & Sathish Kumar, V. (2014). Embedded Image Capturing System Using Raspberry Pi System. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3*(2), 213-215. https://pdfs.semanticscholar.org/d2bf/70f60dff35086fd57b28525d7e5e6ea2e1d0.pdf

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49

Shah, M., Patel, J., & Patel, V. (2018). Development of Interactive Data Storage Unit Using Raspberry Pi. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 825 – 830. Coimbatore, India.* IEEE. https://doi.org/10.1109/ICIRCA.2018.8597217

Stallings, W. (2005). *Cryptography and Network Security* (4th ed.). Prentice-Hall, Inc.

Tabora, V. (2011). *Face Detection Using OpenCV With Haar Cascade Classifiers*. https://becominghuman.ai/face-detection-using-opencv-with-haar-cascade-classifiers-941dbb25177

 http://doi.org/10.17993/3ctecno.2020.specialissue4.35-49