iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6062

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

High Protection Voice Identification based Bank Locker Security System with Live Image Authentication

B. Sudarshan[1], Akshaya R. k[2] Mohan Reddy B[3], Srinivasa[4], Ramya L.K[5]
[1, 2, 3,4,5]*Electronics and Communication Engg. Department, Kammavari Sangham Institute of Technology, Bangalore.*

Abstract: ***When human beings were on earth, need of various things emerged. As years passed and with tremendous development people started earning money, property, jewelry and many more precious things. With huge development people felt a need to secure their earnings. In today's a man's life the money security is an important aspect as he earns the money by his hard work, and banking is known for this. It is not enough to have these accessories, but security of this is very important, for this purpose we keep them in a bank locker. Still, we often hear or read in a newspaper that some fake person has access the locker of another person and have stolen money. In order to overcome this type of frauds, authentication of the person who wants to use the locker is very important. To overcome this security threat, a security system has been proposed using voice identification, face detection and GSM technology.***
Keywords: Authentication, OTP, GSM, Door Lock.

I. INTRODUCTION

Bank is a financial institution which provides us financial services like issuing money, saving cards, etc. Earning money and saving it is very important part in man's life for enjoying a comfortable economic status and hence banking sector plays a vital role for all of us. It is necessary to keep the cash, ornaments and other valuable under safe custody because burglars now days have a lot of modern equipment with them. As per one quotation if one looses health it can be regained, but one loses his valuable wealth it takes too much time to recollect it. To protect our valuables banks provide some other benefits like providing their customers with safety lockers to store their valuables. The need for safe locker systems is not only in banks but also in various other institutes like in Offices, shops business establishments, financial institutions, Petrol stations, Hotels and Hospitals. This need is increasingly felt in these days due to the increase in the security concerns.

II. LITERATURE REVIEW

This section describes the survey of different technology that has been used in bank locker systems. In olden days, only mechanical locks were available which was not secured enough. As technology grows, modern electronic locks were introduced into the market to avoid further theft and unauthorized access.

Password based locking system was one of the modern electronic lock system where password is used as the verification factor. Then comes the next electronic lock system which is an RFID based system. In [1] and [2], the working of RFID based system is described where RFID tag and reader are the main components and RFID value acts as the authentication factor.

Later on the biometrics lock system came into existence as described in [3], [4] and [5] such as face recognition, fingerprint recognition, voice recognition, iris recognition and identification and work on the principle "what we are". Here the personal identification of each individual is used as the factor for verification.

In [6], [7] and [8], an encryption based lock system was introduced where the original password was encrypted to generate the new password which is been used to unlock the door. This technique is mainly introduced to prevent hacking.

One Time Password (OTP) is the largest technology for secure access. As mentioned in [9], the OTP generated will be unique at each time of access and chances of hacking will be very low and is difficult. They are enhanced version of password based lock system, but the password are not consistent.

There are many more methods like IOT, Wi-Fi and Near Field Communication (NFC) based lock systems which works with the help of smart phone and network [10], [11]., [12].

But that doesn't even put and end to the theft, hacking and unauthorized access. Hence it leads to the implementation of the proposed system.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

III. PROPOSED BLOCK DIAGRAM

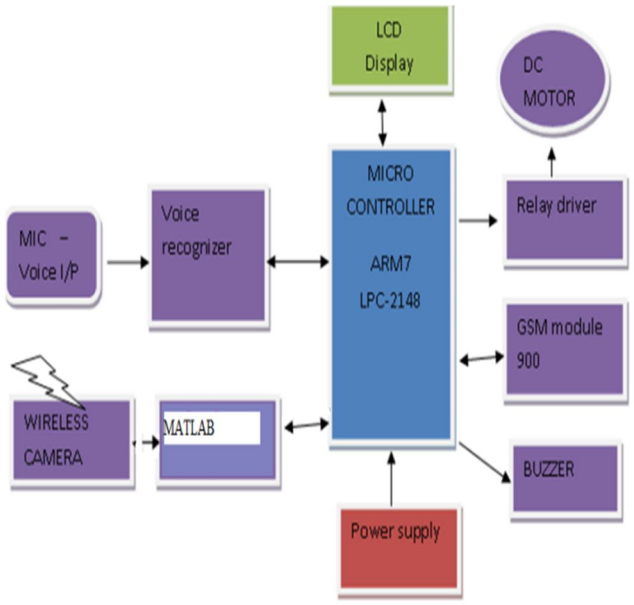


Fig. I. Transmitter section

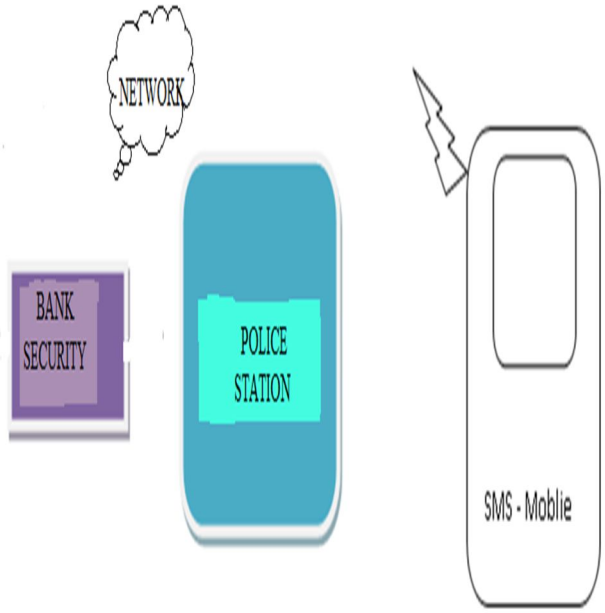


Fig. II. Receiver section

The system contain the ARM-7 as the main processor. The power supply is used is 3.3v which is directly attached to the ARM-7 processor. Then the 16x2 LCD display is interfaced with ARM-7 to display the command. Here the LCD 16x2 means it has 16-columns and 2-rows. The voice recognizer is directly interfaced with ARM-7 to recognize the authorized voice. The MIC is directly connected to the voice recognizer so as to give the user voice. The MATLAB is a matrix laboratory and is used to store the data and recognize the user image to check whether he is a valid user or not. The wireless camera is directly attached to the MATLAB so as to capture the image and send it to MATLAB. On the output side we are using Stepper motor to be used opening and closing of the locker. And the Relay driver is used here is an electromagnetic device and is used to overcome any voltage and current variation. The GSM module is used to send the message to the authorized person if he allows then the locker is open. If he block the message then it message will send to bank security, police station and SMS mobile to the user.

©IJRASET: All Rights are Reserved

Used to send the message to the authorized person if he allows then the locker is open. If he block the message then it message will send to bank security, police station and SMS mobile to the user. Finally the Buzzer will used when the password is invalid. If the user is accept then the locker is open otherwise the Buzzer is start functioning. The whole system is work is as follows:

In the first the user will provide the voice command through the mic. The command will send to the voice recognizer where it recognize the valid user or not. If he is a valid user then the information will send to the MATLAB.

In MATLAB it will check the user face with precise dimension. Before we compare to the user we can train them. If the MATLAB detection is success the user will access his belongings. If the voice is valid user and the Face will not match then the GSM module will send the message indicating whether it can allow or block the locker. If the user enter the allow using command ALW then he will access the locker. If he send block using command BLK then the display will show the system will blocked. At this time there were three process will happen.

IV. FACEDETECTION METHODOLOGY

The face detection algorithm contains different methodology of detecting the face. The algorithm used is AdaBoost algorithm. AdaBoost, short for Adaptive Boosting, is a machine learning meta-algorithm formulated by Yoav Freund and Robert Schapire, who won the 2003 Gödel Prize for their work. It can be used in conjunction with many other types of learning algorithms to improve performance. The output of the other learning algorithms ('weak learners') is combined into a weighted sum that represents the final output of the boosted classifier. AdaBoost is adaptive in the sense that subsequent weak learners are tweaked in favor of those instances misclassified by previous classifiers. AdaBoost is sensitive to noisy data and outliers. In some problems it can be less susceptible to the overfitting problem than other learning algorithms. The individual learners can be weak, but as long as the performance of each one is slightly better than random guessing, the final model can be proven to converge to a strong learner.

A. AdaBoost refers to a particular method of training a boosted classifier. A boost classifier is a classifier in the form where each is a weak learner that takes an object as input and returns a value indicating the class of the object. For example, in the two class problem, the sign of the weak learner output identifies the predicted object class and the absolute value gives the confidence in that classification. Similarly, the classifier is positive if the sample is in the positive class and negative otherwise. Each weak learner produces an output hypothesis, for each sample in the training set. At each iteration , a weak learner is selected and assigned a coefficient such that the sum training error of the resulting -stage boost classifier is minimized. Here is the boosted classifier that has been built up to the previous stage of training, is some error function and is the weak learner that is being considered for addition to the final classifier. The system will work is as follows

B. When the instruction from the controller it will directly through the MATLAB software. Where it check the user face.

C. Before it check the valid user the MATLAB is trained in such a way that it can store the 15 images of each user. Then it will compare the user with these 15 set of images

D. If it matches then the instruction will send back to controller where controller can do some specific task as mentioned aboe

E. If it not match the controller will do some specific task to block the locker.

The experimental setup with all the interfaced components is shown is Fig. 3

V. EXPERIMENTAL SETUP

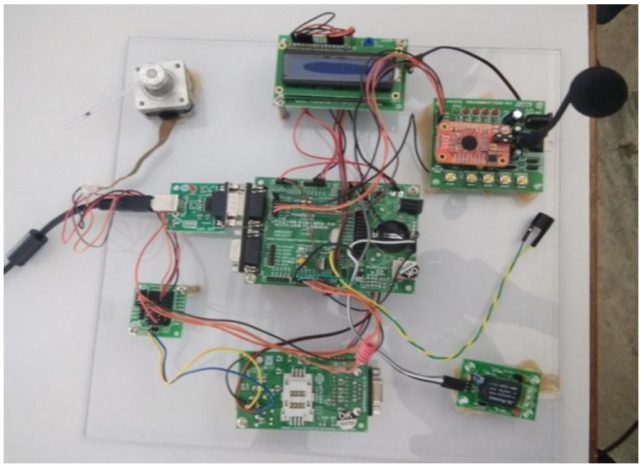


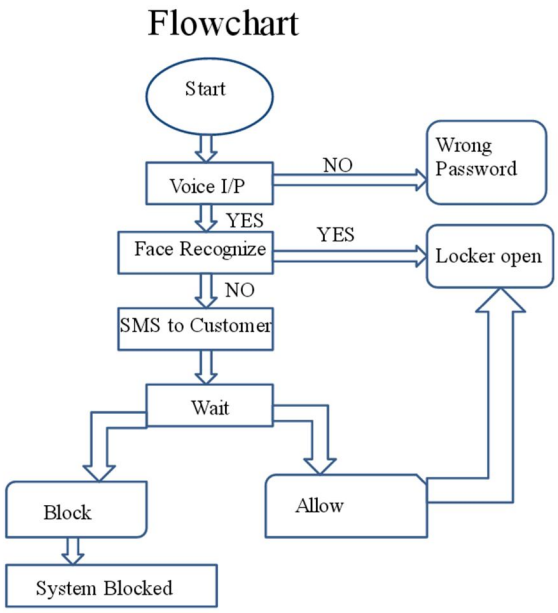
Fig.2 Experimental Setup

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

VI. SOFTWARE FLOW DIAGRAM

The Software Flow Diagram of the system in Fig. 4.



VII. TEST RESULTS & DISCUSSION

The test results are divided into three phase. One is voice from the authorized user and same face, second is the voice is authorized but face is not matched and the third is the voice is unauthorized.

A. When Voice is Matched

In this phase, the voice is given by the authorized user and the face will be authorized. It will ask the user for user input. If the user input will match go to face active. If face will match then the locker will open to display the message as “locker open take care.

Fig.5. First display message

Fig.6. Second message

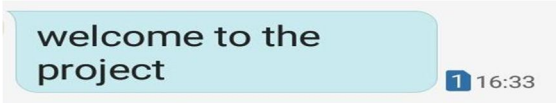


Fig.7. Message from GSM on mobile

Fig.8. Message for user data

©IJRASET: All Rights are Reserved

Fig.9. Message when user gave a voice

Fig.10. Message when face will match

B. When Voice is Matched but Face is not Matched

The initial step is similar to the first procedure but here the user voice will be authorized but the face will mismatch. In this situation the GSM module send the message to the user will it allow or block. If the user will send the message allow then the system will access the locker else it will block it.

Fig.11. Asking user voice

Fig.12. When voice is recognized

Fig.13. MATLAB command to GSM module

Fig.14. MATLAB command to GSM to ALW or BLK

1) If it is allowed

Fig.15. If ALW is send through mobile

©IJRASET: All Rights are Reserved

2) If it is blocked:

Fig.16. If user enter BLK through mobile

C. When Voice is not Matched

In this procedure when the voice will not matched then the GSM module send it will be an wrong password on to the LCD display.

Fig.17. Ask users voice

Fig.18. Display as voice is not matched

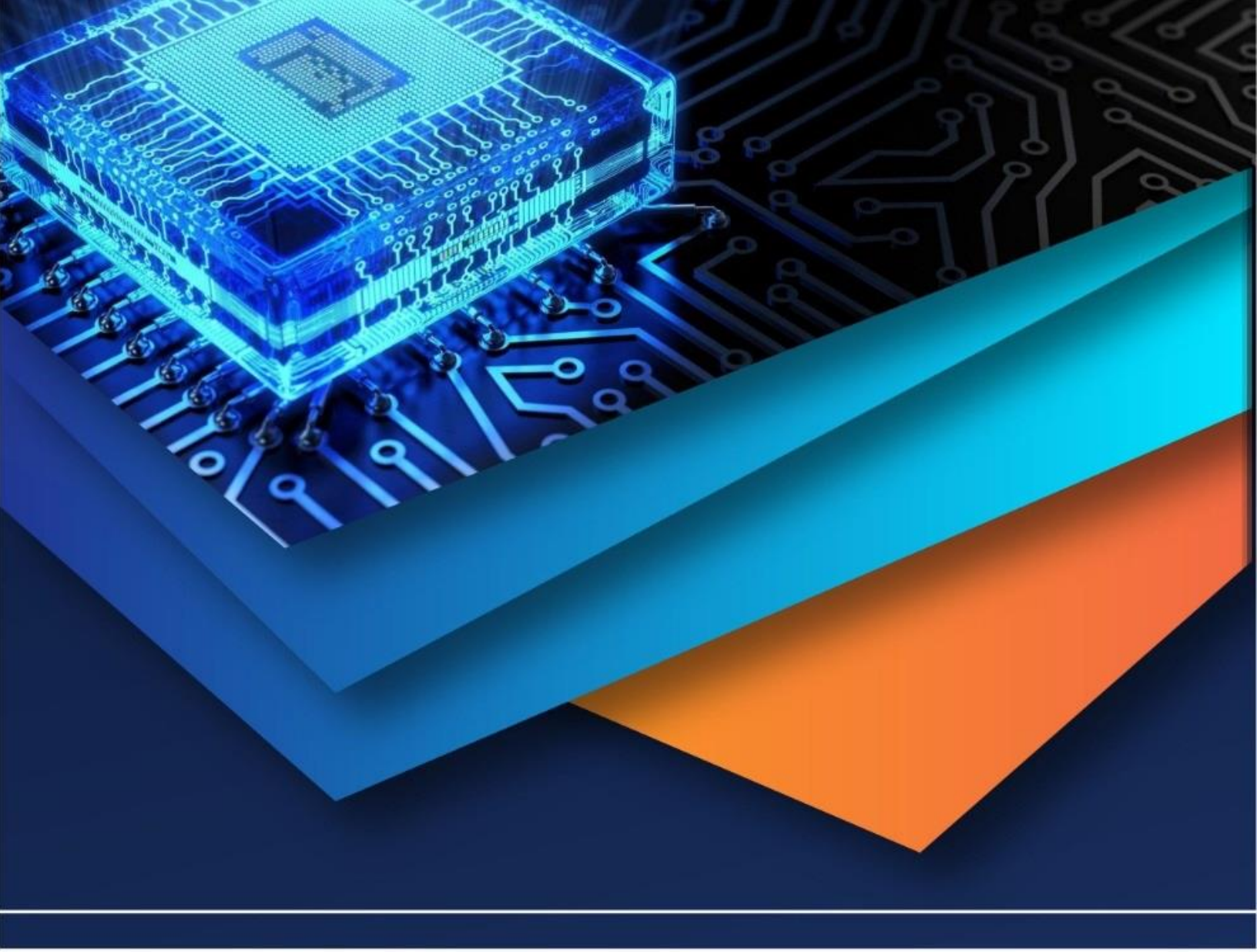
VIII. CONCLUSION

An advanced and cost effective feature for ATM security has been proposed. It can be installed in the ATM at some hidden place so that it is safe. This system is distinctive in many ways from existing ATM intrusion and theft control systems. Existing system are either very expensive and not reliable. The proposed system is reliable, inexpensive with appropriate design.

REFERENCES

[1] Divya R.S, "Super secure door lock system for critical zone". International conference on network & advance in computational technology, 2017.
[2] Srinivatsan Sridharan. "Authenticated secure bio-metric based access to the bank safety lockers", Department of computer science International Institute of Technology-Bangalore, 2014
[3] Amit verma, "Development of an intelligent system for bank security", Department of ECE, ASET, Amity University Noida, U.P IEEE Paper, 2014.
[4] Pradeep kumar, "An efficient multi stage security system for user authentication", department ECE Amity university, 2016.
[5] N. Anusha, "Locker security system using Facial Recognition & OTP", computer science and engineering sathyabamma university chennai, 2017.
[6] Sanal Malhotra, "Banking security system using Hand Gesture Recognition", Department of ECE amity university uttar pradesh, 2015.
[7] Avinash. D. Harale, "Iris as a Biometrics for Security System", SKN sinhgad college engineering korthi, Maharastra, india, 2017.
[8] K. Suganithi^2, "Survey of integrating Face and Iris biometrics for security motive using change detection mechanism", International conference on science technology, 2017.
[9] A.S. "Performance Analysis of speech digit recognition using Cepstrum and vector quantization", International Conference on Electrical, Electronics, Communication, computer and Optimization Techniques(ICEECCOT), 2017.
[10] Azzamul Asar, "Interactive Voice Response with Pattern Recognition Based on Artificial Neural Network Approach", NWFP University of engineering and technology, 2017.
[11] Sandeep kumar. "Novel bus security solution for bank ic card with FPGA", Tsingua National Laboratory for information science and Technology of Microelectronics, Tsinghua University, Beijing 100084, china IEEE Paper, 2014.
[12] Amit verma, "A multi layer bank security System", IEEE Paper, ECE department, ASET, Noida, 2013.
[13] A.N. Gaikwad "Fingerprint and Iris biometric controlled smart banking machine embedded with GSM Technology for OTP", International institute of information of technology, 2016.
[14] Anitha Julian, "Design and implementation Of anti-theft ATM machine using embedded systems", International conference on circuit, power and computing technology, 2015.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)