High Protection Voice Identification Based Bank Locker Security System With Live Image Authentication-A Literature Survey

B. Sudarshan
Akshaya R.k Mohan Reddy B Srinivasa Ramya L.K
Electronics and Communication 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. EXISTING WORK

[1] Security is a defense against threats which provides an assurance of safety. Now and before security is one of the major concern in places like home, offices, institutions, laboratories etc. in order to keep our data confidentially so that no other unauthorized person could have access on them. In olden days the security mechanisms are less in order to prevent unauthorized access. Nowadays lot of security mechanisms have been introduced for such places and applications. But along with a wide variety of security methods, the techniques of theft are also changing and it's increasing day by day. With the available systems we can protect home and institutions to some extent. But that's not the case for critical places like military offices and scientific laboratory. These places require highly secure systems at every point of time in order to protect the valuable data and money. Varieties of security systems are now available such as password protected ones, RFID card technologies, biometric protected systems, OTP based, cryptography based and many more. Each system is applicable for different application zones depending upon their technical usage. Also there are systems that use a combination of any two techniques for more security, yet they don't provide a complete secure system as there is only single factor authentication. Also these systems can be broken by hackers or burglars. So these systems cannot be taken for the critical places that need more security. Here three techniques; RFID technology, encryptions and OTP which are the best techniques that incorporate with each other and the most effective ones is chosen to build our secure system. It doesn't mean that the other technologies are not worth. Based on the survey of different door lock access control mechanisms, the above three techniques that is used in this system is much better than the other ones. Also these three methods are compatible with each other to produce a stronger system. Microcontroller PIC16F877A is used here which is a programmable device. High speed performance, programming flexibility and low-cost features are the high lights to choose microcontroller. They consist of 5 GPIO ports. However, only a single task can be executed to control a single system. This paper consists of several sections. Section 2 gives the literature review about the existing systems. Section 3 describes the methodology of the developed system. Section 4 presents the hardware implementation of the door lock. Section 5 describes the software part of the system which deals with encryption process. Section 6 introduces the android segment with the working of OTP technology and the secure wallet application. Section 7 provides the results and finally Section 8 concludes the overall work.

[2] The safety locker is a convenient way provided by the financial institution or the bank to place the valuable belongings and documents of the user. This system operates using the concept of dual keys - one provided to the user and the other held by the branch head. The main aim of this dual key system is to efficiently operate the entire safety locker system under the control of one head of a branch allotted by that particular bank's central head office. The entire system hinges on the authenticity provided and assured by the branch head. There is lot of tedious process involved in the current system of operation of the safe deposit lockers. The manual allocation of responsibility to the branch head by central head office (in a daily basis) based on the availability and the on-spot branch head approval for operation of the safety lockers by the customer are some cumbersome process involved in the current system. The main intention behind the branch head on-spot approval is to manually authenticate each individual before operation of the respective locker. The branch head is supposed to allow only the user of the locker to gain access to it. These intentions lead to the birth of the dual key system in the safety lockers of the bank. The lockers operating under these enforcement's are kept in a separate enclosure called the strong room. Access to this strong room lock is only with the branch head. So the branch head has to maintain a separate lock for each of the safety lockers inside the strong room and a lock for strong room. The access for these is manually determined by the central head office on the availability of head at each branch in daily basis.

[3] The safety locker is a convenient way provided by the financial institution or the bank to place the valuable belongings and documents of the user. This system operates using the concept of dual keys - one provided to the user and the other held by the branch head. The main aim of this dual key system is to efficiently operate the entire safety locker system under the control of one head of a branch allotted by that particular bank's central head office. The entire system hinges on the authenticity provided and assured by the branch head. There is lot of tedious process involved in the current system of operation of the safe deposit lockers. The manual allocation of responsibility to the branch head by central head office (in a daily basis) based on the availability and the on-spot branch head approval for operation of the safety lockers by the customer are some cumbersome process involved in the current system. The main intention behind the branch head on-spot approval is to manually authenticate each individual before operation of the respective locker. The branch head is supposed to allow only the user of the locker to gain access to it. These intentions lead to the birth of the dual key system in the safety lockers of the bank. The lockers operating under these enforcement's are kept in a separate enclosure called the strong room. Access to this strong room lock is only with the branch head. So the branch head has to maintain a separate lock for each of the safety lockers inside the strong room and a lock for strong room. The access for these is manually determined by the central head office on the availability of head at each branch in daily basis.

[4] For a common human being the bank means a place which represents a top level of security. On a daily basis we are involved in banking transaction. To secure our expensive jewellery, important documents or cash, we use to use bank locker rooms. It has become an important part of our life. To survive in this competitive world and for a continuous growth, the banking industry needs to provide a high degree of security. Because of the public interest every day new branches are opening. The more number of branches required more security. Current systems and services are becoming more and more autonomous and the banking sector is not too far from it. Video surveillance [1] in moving areas has become a current topic of interest in computer vision technology. You can see all the branches are under the surveillance of CCTV cameras, alarm systems, emergency buttons etc. The CCTV cameras are used to monitor the unauthorized activity. It needs to be monitored continuously by a human being which is very difficult work; especially in nights. The alarm emergency button also needs to be pressed manually. This conventional system requires lot of man power. A system can be developed which will automatic detect unauthorized motion and inform to the security officials of the banks by different ways without any need of a human being. The Microcontroller Based Bank Security System fulfils all these requirements. A prototype of this security system has been designed in the dissertation to increase the level of security in bank locker rooms effectively. The motion detection will be done through camera [2],[3],[4] itself and the hardware associated with it will provide 3 different ways to inform the security officials i.e. using alarm system [5], a warning message and the image which has detected the motion [6],[7] will be automatically uploaded on webpage which can be downloaded from anywhere. For messaging a GSM module [8],[9],[10] will be utilized. So the important objectives of bank security system are tracking the bank locker room areas, detection of motion and taking the necessary control action. The further sections will describe that how these objectives have been achieved.

[5] Now day's security of assets is the main concern for any person. This paper aims at providing a reliable security system. It provides a way for identifying authorized and unauthorized persons, by using RFID, keypad password and finger print technology. Atmega168 microcontroller used for controlling the hardware. The main contribution of this paper is to provide a multi stage security so that unknown person will not be able to breach the security. In Conventional security system, there is either an RFID system or a password based system or a biometric based system (which could either be a finger print based system, retina scanner or voice recognition system), there is a greater chance to break such one stage security system. To improve such systems, a multistage security system consisting of microcontroller based matrix keypad & GSM network in addition to RFID technology and finger print module can be used. In this, verification will also be involved without which the system doesn't provide access and a notification is sent to the authorized person. Related works include development of a digital security system containing door lock system using passive RFID [8] , RFID based security systems and microcontroller based reprogrammable

digital door lock security system by using keypad & GSM/CDMA technology [10]. In future we will be implementing it using FPGA as implemented in [17-18]. The microcontroller based digital door lock security system is an access controlled system in which only authorized persons can access restricted areas. The proposed security system consists of the following three stages-

Stage 1: RFID module consists of RFID tag and RFID reader. When the user punches his card (containing the tag), the 12 byte serial number of the tag is read by the RFID reader and is sent to the microcontroller. The microcontroller then compares the data with the existing data stored in the EEPROM memory(internal memory of the microcontroller). If the data matches with the existing data in the memory, it means the person is authorized and the user enters the second stage of the security system. If the data is not matched then the user will not be permitted to enter the premises. The buzzer starts ringing to provide an alarm indicating the presence of an unauthorized person and a message is sent to the authorized person via GSM module.

Stage 2: The second stage includes the entering of password via the keypad by the user. If the password is correct then he will reach the third stage of the security system. But, if the password is wrong then access is denied and the authorized person is notified through the GSM module.

Stage 3: The user reaches the third stage if his RFID tag and password is correct. In the third stage he has to punch onto the fingerprint module. If the fingerprint of the person matches with the existing finger prints stored in the memory of the finger print module, then, the lock opens and the user gets access else it is denied.

[6] Hand gesture is a non verbal way of communication. Today hand gesture has been used for human-robot interaction. Gesture recognition is also implementing using artificial neural network . Image Processing has tremendous areas of application such as watermarking, discrete wavelet transform etc. Hand Gesture recognition has been widely used for various applications but in this system we have used hand gesture recognition to provide security to banks which has never used before. In our implemented system, hand gesture is recognized using five processes such as image acquisition, skin color information for recognizing hand gesture which is obtained from the arm region of the hand, background removal, canny edge detection and contour detection. This system is used for banking security. It is very important for every bank to provide security to their customers and employees. The cases of robbery in bank risks the life of employees and customers at the bank, so the main purpose of this system is to provide security to the customers and employees in the bank. At the time of robbery in bank, the money of the bank and the life of the customers and the employees are at risk, this system uses hand gesture recognition technique of image processing to recognize the special hand gesture of the employees so that nearby police can be informed about the robbery just by recognizing the special hand gesture made by the employee in front of the camera. The employee is pre-trained about how and what gesture to make in case of robbery in bank before joining at the bank.

[7] One of the most effective methods for the sake of security is biometrics. The term biometrics is the combination of two words Bio & Metric. It is an emerging technology for recognizing the individuals based on their physical or behavioral attributes. The physical attributes are more reliable than behavioral attributes and has no risk of being used by anyone else or forgetting it or losing it and these attributes include fingerprint, hand geometry, handwriting, face, iris, voice, retina, vein etc. As far as security importance is considered, there is a need to guaranty that only authorized persons can enter to the restricted areas like bank, R&D etc. and this need is satisfied by the use of biometric technologies. Biometric identification systems are valid alternatives to traditional identification systems such as showing identity cards, use of passwords, making signatures etc. The disadvantage of traditional identification systems can be avoided by adapting the biometric methods and with the help of these biometric methods, it is possible to recognize an individual's based on who they are rather than what they possess or what they remember. Various biometric techniques that deal with automatic recognition of a person are hand geometry; face recognition fingerprint recognition, retina scanning and iris recognition. The iris recognition is based on iris biometrics.

[8] At whatever point individuals sign onto PCs, get to an ATM, go through air terminal security, utilize charge cards, or enter high-security ranges, they have to confirm their characters. Individuals commonly utilize client names, passwords, and recognizable proof cards to demonstrate that they are who they claim to be. In any case, passwords can be overlooked, and recognizable proof cards `can be lost or stolen. Thus, there is tremendous interest in improved methods of reliable and secure identification of people. Biometric methods, which identify people based on physical or behavioral characteristics, are of interest because people cannot forget or lose their physical characteristics in the way that they can lose passwords or identity cards. Biometric methods based on the spatial pattern of face and the iris is believed to allow very high accuracy, and there has been an explosion of interest in iris biometrics in recent years. This paper justifies the novelty of combining face and iris recognition based on several techniques used in different processes . Due to physical obscures such as hair growth or loss, age, scares, lighting, glasses, masks and injury at the iris or face may lead to the security system failure. As the user population increases the demand of storing all the data also increases that require large memory space. In order to address these two limitations the Change detection method can be used. Change detection is a statistical analysis used for comparing two images taken in different period of time. Classification is the process of identifying to which of a set of categories a new observation is belonged to. There are

several algorithms used in classification process. Classifiers play a pivotal role in recognition process. The process of incorporating change detection into classifiers is expected to increase the reliability and performance likely.

[9] Automatic digit recognition system aims at recognizing human speeches, which has words and sentences using algorithm's that can be evaluated by the computer without human intervention. Digit identification is to design a recognition task, which takes digit signal, and classify it as a sequence of previously learned patterns, e.g. words or sub-word units such as phonemes. This system is indicated by the parameters, such as speaking style, vocabulary, speaking model etc. A constant speech recognition system does not pause the speaker between the words, where as an isolated digit identification system does. Generated the extemporaneously or Spontaneous, it is much more difficult to recognize than speech read from script. A few digit recognition systems need speaker enrolment; an user provide a speech samples, while other systems does not require enrolment. Voice recognition is conversion of acoustic signal recorded with a microphone to a set of words. The identified words are the final result, regarding applications such as data entry, doc preparation, commands and control. People may prefer this system instead of typing on a keyboard or smart phones or tablet. Physically disabled people can easily communicate using this system. The proposed idea of introducing this system making the next generation of automation technology based on speech data to control the lights in a room, or the temperature of our home with a simple spoken command security of getting our home to recognize and respond to our voice only. The idea of this project is developing voice recognition system on easily accessible electronic components and hardware. The system will respond to some identified spoken commands, and control the household devices, a lamp, and fan. The overall performance of the speech identification systems is measured in terms of word identification rate (%) which is a measure for technology it uses for a given task, with specified structure for vocabulary in a specified mode and the word given. The speech recognition system is used for recognition of PID (Person Identification numbers), telephone numbers, and credit card numbers. Continuous speech recognition system finds applications in eyes free, hands free voice repertoire dialer. The user communicates through computer using activity of speech from text message, voice identification and speaker recognition. Speaker recognition is mainly used to recognize the person who has spoken from the population or to identify the people. The speech digit algorithm is implemented using MATLAB.

[10] In telephony, Interactive Voice Response, or IVR, is a computerized system that allows a person, typically a telephone caller, to select an option from a voice menu. In some of the applications like bank account balances, transfers and accessing databases of strategic organizations etc. require high level of security. In such applications the information to be provided is made secure by the use of Personal Identification Number (PIN). However, this approach is not secure and is prone to tampering and misuse. To overcome this problem a pattern recognition approach based on neural network is proposed. User specific patterns such as fingerprint, retina, facial features, DNA sequence identification and voice etc. can be used for authentication. However, among these, voice authentication is readily available and most suitable for this application. The speaker recognition area has a long and rich scientific basis with over 30 years of research, development and evaluations. Inherent in attempts at speaker identity verification, it is the general assumption that at some level of scrutiny, no two individuals have exactly the same voice characteristics. In the proposed approach, besides entering the PIN code, the user will also be asked to get himself recognized through his voice signatures which further enhances the secure access to various applications. The results are promising based on false accept and false reject criteria offering quick response time. It can potentially play an effective role in the existing authentication techniques used for identity verification to access secured services through telephone or similar media. In the proposed model, speaker specific features are extracted using Mel Frequency Cepstral Coefficient (MFCC) while Multilayer Perception (MLP) is used for feature matching. Our model is based on 8 kHz, 8 bit format using Pulse Code Modulation (PCM).

[11] As bank IC cards are now facing threats from kinds of attacks, including non-invasive, semi-invasive and invasive attacks, security of the bank IC card is a serious problem. Some of the attacks intend to recover secret keys in the IC card by detecting the bus, such as power analysis, fault attacks and bus probing. At 20 I 0 Black Hat Conference, Christopher Tamovsky presented his achievements in cracking Infmeon SLE66 CL PE, one type of widely used security integrated circuit. Bank IC cards carry sensitive information, and could be cracked for financial benefits. More and more methods are now developed to attack IC cards to obtain secret keys, including power analysis attacks and fault injection attacks. Bank IC cards without countermeasures are vulnerable to these attacks, and could be a serious problem once a bank IC card is cracked. Five levels of security are proposed as a systematic way to implement countermeasures in bank IC cards, which are chip level, system level, algorithmic level, gate level and transistor level. A novel bus security solution is proposed in this paper, two methods in the system level are proposed to improve the security of bank IC cards, more precisely, on the AMBA. These two methods including power balance with 8BIl OB encoding and fault attack detection with CRC check.

[12] Bank locker room security is important for many reasons. One of those reason is it secures precious things like jewels, hard cash, property papers many things which is very difficult to earn. The present security systems are suffering with the issue of security levels. The less number of security levels can be easily faked by the robbers. In this paper "A Multi Layer Bank Security System" has been designed. This particular security system does not need presence of any human being. The security system itself consists of two distinct security systems which are independent of each other. The first system will be placed at the front door of the locker room area and another will be placed at the gate of the locker room. Most doors are generally manually controlled by

the security person employed by the bank with the use of handle locks operated by a key. In this system each user will be provided with a unique RFID card. The front door will open only when a authorize person wants to enter with an authorize card. In the locker room area a passive infrared sensor will be mounted with a camera. In case if a person gets enter at the locker room area without any authorize card then a passive infrared sensor is actively waiting for it, which will send a signal to a microcontroller and the microcontroller will take two actions, first it will switch on the alarms which will inform the local security and second it will take a snapshot of the locker room area and mail it to the authorize person using a personal computer. The second system which is placed at the locker room entrance consist a biometric system. To open the gate of the locker room the person needs to get his/her iris scanned and fingerprints to be verified. When these two processes will complete, only then the locker room will be opened.

[13] A 24 x7 self banking service has made the ATM the heart of banking. The surplus use of ATMs, has not only lead to an increase in their number but has also increased fraudulent attacks on the ATMs. This calls for the biometric systems to be integrated in the traditional ATM. The author in [1] Built an ATM based on fingerprint verification and incorporated the fingerprints of the users into the database of the respective banks to simulate it for ATM operations. Due to the lack of the fingerprint matching algorithm it proved to be inefficient. [2] Proposed a system which performed authentication by including both the fingerprint and GSM technology into the traditional PIN based ATM system. In [3] an algorithm was constructed based on Short Message Service (SMS) verification to enhance the ATM authentication system. Authors in [4] secured the system using fingerprint and iris, along with this the system used RFID reader module. [5] developed a RFID card as input to the microcontroller for identification and a GSM module to send messages involving three options (yes, no, action) to the authorized user's mobile. Authors in [6] proposed an efficient system which used the method of analyzing iris patterns for user identification In [7] a system using iris recognition and palm vein recognition technology was proposed in order to avoid crimes in the ATM transactions. Authors in [8] proposed a system which incorporated facial recognition in the traditional ATM for authentication of users. In [9] authors used Hough Transform for iris recognition in order to isolate the unique features of particular shape within an image. In [10] an Advanced Encryption Standard (AES) algorithm was used in order to enhance the security of the ATM transaction. [11] described a system which used face as a key. The system performed facial recognition using Principal Component Analysis for facial recognition along with OTP for security of transaction. This proposed system utilizes minutiae matching algorithm for fingerprint recognition and Circular Hough Transform for iris recognition. The later part of this paper is designed as follows: The system development is furnished in Section II .Proposed Biometric identification techniques are described in Section III. GSM technology for OTP generation is explained in Section IV. Experimental results are focused upon in Section V. In Section VI finally conclusion are drawn with the help of comparisons with the previous systems.

[14] The rapid growth in Automatic Teller machines (ATM) has made life easy for the day to day man, but it is not so for operators who manage it. ATMs are not owned by banks, rather they are outsourced to managed service providers (MSPs) from purchasing to maintaining the machines. Several factors like the maintenance, money filling, security and therefore the passive assets within the ATM rooms are responsible for keeping the ATM active [7]. Typically, an ATM site consists of anywhere between 8 to 12 passive assets which include two air conditioners, two light collection boards, Associate in Nursing inverter/UPS, a security camera and a minimum of eight to twelve light- weight bulbs. Currently, since the security and passive assets in ATM rooms are managed manually, it ends up in larger physical interaction, that increase the time period and therefore shrinks the gross margin of ATM operators. These MSPs are duty-bound and every ATM site is up as costs of downtime are too high. With rising overheads ATM operators struggle to pass on the cost and so are looking for a reliable remote monitoring solution to revitalize ATM maintenance [3].

[15] In this modem age, where technology is advancing, innovation are increasing day to day, the banking sector are the one where this technology and advancement are not in use to its fullest potential. The present banking system offers its user with fast and ease way of banking like online banking, mobile banking, etc. at the same time this banking systems are lacking in security. Bank is a financial institution where business transactions, money transfer, A TM, credit card are some tasks that are performed every day. Banks also store some customer's personal property and information and it should not be disclosed without any authorization. But to the controversy there always exist some irresponsible people to challenge the robustness of the banking system. Around the globe bank hacking causes million dollars losses. This intrusion like hacking and other illegal activities could be done by anyone with security knowledge and for the purpose of gaining or altering the confidential data because of this intrusion the client and customer stress towards the financial institution is decreasing in order to avoid this insecurity and intrusion high level of security system should be implemented.

[16] Security is needed for human being for many references, to protect or their data/information people generally use password or personal identification number but there are chances to lose security because if someone lost their personal identification number or somehow password known by someone else so that data is not secured as much as necessary. There are lots of cases of scams of data and stealing of personal identification number so to overcome from this problem there is need of a new technology which is more secure and new technology which is more secure and not easy to fraud and theft the technology is Biometric Identification Techniques. In this technology biometric characteristics are uses as security factor since it is unique for individual

therefore these can be used to authenticate the user for access control. There are many biometric identification techniques are such as face recognition, finger print, Iris, voice recognition and speaker recognition etc. In recent speaker recognition is more suitable and secure technology for recognizing a people. The automatic speaker recognition systems have two main components one is feature extraction and second is feature matching.

[17] Utilizing biometrics i.e. the unique characteristics of a user such as fingerprints, voice, vein patterns etc. is an efficient methodology of improving security. This is because biometric data cannot be forgotten or copied and is more difficult to hack when compared to traditional security systems. Speech is the most natural form of communication for humans and the speech of every individual is unique. This is mainly due to biological factors such as size of vocal tract or due to behavioral characteristics such as accent, speaking speed etc. A voice recognition system is a biometric system that can identify an individual via the unique acoustic characteristics of the individual's voice. This system has a wide variety of applications in the field of security such as granting access to a system, a secure location and providing services such as telephone banking, voice dialing, surveillance etc. Voice recognition systems have two phases namely training and testing. During the training phase, the speaker registers into the system by providing their voice sample so that the system can be trained to recognize them in the future. In the testing phase, the voice sample provided is compared with the existing samples in a database. If a match is obtained, the system will provide the user access. This paper aims to design a text dependent voice recognition system to be used to secure a given user's system so that only the user may access it. The system will also support a multi user database should the user want to provide access to a select few.

[18] At whatever point individuals sign onto PCs, get to an ATM, go through air terminal security, utilize charge cards, or enter high-security ranges, they have to confirm their characters. Individuals commonly utilize client names, passwords, and recognizable proof cards to demonstrate that they are who they claim to be. In any case, passwords can be overlooked, and recognizable proof cards `can be lost or stolen. Thus, there is tremendous interest in improved methods of reliable and secure identification of people. Biometric methods, which identify people based on physical or behavioral characteristics, are of interest because people cannot forget or lose their physical characteristics in the way that they can lose passwords or identity cards. Biometric methods based on the spatial pattern of face and the iris is believed to allow very high accuracy, and there has been an explosion of interest in iris biometrics in recent years. This paper justifies the novelty of combining face and iris recognition based on several techniques used in different processes . Due to physical obscures such as hair growth or loss, age, scares, lighting, glasses, masks and injury at the iris or face may lead to the security system failure. As the user population increases the demand of storing all the data also increases that require large memory space. In order to address these two limitations the Change detection method can be used. Change detection is a statistical analysis used for comparing two images taken in different period of time. Classification is the process of identifying to which of a set of categories a new observation is belonged to. There are several algorithms used I classification process. Classifiers play a pivotal role in recognition process. The process of incorporating change detection into classifiers is expected to increase the reliability and performance likely.

[19] Face based secure access systems are increasingly becoming popular for many applications such as unlocking the Smartphone, e-commerce and e-banking. The ease of unconstrained imaging using a simple color camera has led face recognition to be employed in secure systems, operating in various environments. Recent interest in this direction has led to the use of smart phones for capturing the face characteristics to authenticate the subjects. The key factor to be noted in Smartphone based biometric systems is the unsupervised data capture. The use of Smartphone-based biometric system for authentication is highly intended to provide the convenience to the user for authentication from any location in an unconstrained manner and thereby is allowed to capture the biometric data in an unsupervised manner. The freedom of unsupervised data capture, especially in the Smartphone based face recognition can be misused by the unauthorized users. The abundant availability of the face pictures on various social media sites can be used for gaining unauthorized access in such unsupervised biometric systems operating on the smart phones[1]. Any attempt to gain the secure access by presenting the arte- fact of the genuine subject is classified as presentation. All the three authors have contributed equally to this article. Attack or spoofing attack. Primitively, an unauthorized user can display the facial image on the electronic screen to gain access to the face-based biometric system on the Smartphone. Alternatively, the image can be printed on a paper and presented back to the Smartphone data capture system. The failure to detect such attacks on face- based biometric system defeats the purpose of security in the context of face based authentication. Such attacks can be addressed by presentation attack detection (PAD) algorithms incorporated in the biometric system. Many approaches have been proposed to counter such attacks on face-based biometric systems which leverage on the textural characteristics of the live attempt and the presentation attack [2], [3], [4], [5]. Variants of the Local Binary Pattern (LBP) was explored from the images using Support Vector Machine (SVM), and Linear Discriminated Analysis (LDA) was used to differentiate the attacks from live presentation [6], [7]. In a similar way, LBP was used in temporal domain to detect replay attacks using SVM and LDA [8], [7]. Another key factor of difference in the of live presentation and attack presentation was fully utilized to detect the presentation attacks by assessing the image quality on both full reference and no-reference quality metrics using LDA and Quadratic Discriminated Analysis (QDA) [9], [10]. Recently, the distortions such as Moir pattern in the live image and attack images were identified to classify the attacks [11], [12]. Further, applicability of the deep features for detecting the presentation attacks was demonstrated in a recent work [13]. It has to be noted that, all the current state of the art

works have focused on the final images obtained from the camera's imaging pipeline to classify the attacks. In a very different paradigm, earlier works have demon- started the use of raw sensor data to obtain the unique sensor noise pattern to establish the authenticity of the imaging camera [14], [15]. Another work recently used the raw sensor noise to identify the device and the user in the context of visible spectrum iris recognition [16]. Motivated by the use of raw data for various applications, in this work, we look at the specific characteristics demonstrated in the raw data at the sensor level to determine the presentation attacks against the live (a.k.a bona-fide) at- tempts. The characteristics are demonstrated at the sensor level is used with simple image analysis and a threshold.

<table>
<tr><th colspan="5">Detecting the authorized users</th></tr>
<tr><th>GSM</th><th>Image Processing</th><th>LCD display</th><th>Stepper motor and Buzzer</th><th>Voice recogrnizer</th></tr>
<tr><td rowspan="11">A GSM approach to Tracking the persons locations and his details.</td><td>For the purpose of storing the live image database to identify the authorized users or not.</td><td>This is for the displaying the user input for identifying the authorized users.</td><td>For door opening and closing purpose.</td><td>It is to check the valid users.</td></tr>
<tr><td>An capturing of the live image and save it to the database.</td><td rowspan="10">For displaying the users input to compare it to the database information.</td><td>Design of real-time techniques of systematic door opening and closing systems.</td><td rowspan="10"></td></tr>
<tr><td>Algorithm reasearch on capturing live image.</td><td>Real Time door opeing and closing system using stepper motor along with Buzzer.</td></tr>
<tr><td>Voice identification using database.</td><td>This can provide real-time safety measure for while door closing and opening.</td></tr>
<tr><td>Here we are using MATLAB it is easy to detect and store the databse.</td><td>Smart system using relay it will control the stepper motor and buzzer is to tune.</td></tr>
<tr><td>Vision based image storing on database is to compare the authorized persons.</td><td>A comprehensive solution to the indication of authorized users are not.</td></tr>
<tr><td>Real time checking the users using the MATLAB.</td><td>Automatic door opening and closing Technique: A Brief Survey</td></tr>
<tr><td>A Camera Setup for storing the image to the database.</td><td rowspan="3">Intelligent Stepper motor with Buzzer System for automatic door opening and closing systems.</td></tr>
<tr><td>This live image based system for Bank, and other high security field.</td></tr>
<tr><td>A novel approach in real time Bank securiy system using ARM - 7</td></tr>
</table>

Sr.no	Year	Paper name	Basic Concept	Advantage	Disadvantage
1	2017	Super secure door lock system for critical zones.	The main-objective is to design and implement a digital security system which can deploy in critical zone where only authorized person can be entered.	There by providing a three way security mechanism with two factor authentication such as RFID matching and OTP matching.	*cost effective. *increase the scale of security provided has been designed & implemented successfully *This providing a fail proof system that cannot be tempered by anyone so easily is build.
2	2014	Authenticated secure Bio-metric based access to the Bank safety locker.	To provide a solution toward a complete biometric based authentication mechanism for operating the safety lockers & using secret code.	*Two level of authentication. *Low cost.	*Exploiting the lack of personal weakness of the customers. *Accessing customer's personal possession(the key of lockers) *Illegal access to the strong room by any individual other then branch head.
3	2014	Development of an Intelligent system for bank security.	This paper proposed an effective monitoring and controlling system for bank locker rooms.	*SMS alert providing. *Monitoring the activities & stored in the database.	*Cost effective. *Maintenance of database.
4	2016	An efficient multistage security system for user authentication.	Multistage security provide by the combination of three securities which is based on the sequence of i)RFID ii)Password iii)Biometric	*Protection levels are more. *Avoid the unauthorized person to access the locker.	High cost because number of protection levels are more.
5	2017	Locker security system using Facial Recognition & OTP.	The locker security system is proposed using IOT, face recognition and OTP.	*Security level is best because the user login & logout will be maintained in the database. *GSM technology are used for SMS alert.	*High cost. *Maintenance of database.
6	2015	Bank security system using Hand Gesture Recognition.	This paper presents hand gesture analysis for human-security system interaction.	*Speed and sufficient reliable for recognition system. *Good performance system with complex background.	*Irrelevant object might overlap with the hand. *wrong object extraction appeared if the objects larger than the hand.

7	2017	Iris as Biometrics for security system	This technology is based on the human eye pattern using Iris.	*Improved security. *Improved customer experience. Cannot be forgotten of lost. *Reduced operational costs.	*Environment and usage can affect measurements. *Systems are not 100% accurate. *Require integration and/or additional hardware. *Cannot be reset once compromised.
8	2017	Survey of integrating Face and Iris biometrics for security motive using change detection mechanism	Face and Iris recognition is a challenging and interesting research topic in the field of pattern recognition.	Iris: *Very high accuracy. *Verification time is generally less than 5 seconds. Face: *Non intensive. *cheap technology.	Iris: *Intrusive. *A lot of memory for the data to be stored.
9	2017	Performance Analysis of speech digit recognition using Cepstrum and vector quantization.	In this paper the implementation of speech digit recognition system is discussed.	Speech Digit Recognition System for various speech digits are suggested and implemented in this research paper. To build the identification or recognition system for various speech digits, the feature extraction technique – Cepstrum and the modeling technique - Vector Quantization is used for generating the person specific models. Also to test the performance of developed system, Euclidian Distance formula is used in proposed system. Overall performance shows that all digits utterance are best performing and can be used for command control applications such as to control light ,fan or voice dialing purpose etc.	First, as the cepstrum is essentially a low pass filtering of the curve of the spectrum interpreted as a signal, it will actually average-out the fluctuations of the curve of the spectrum. This is not what we want, because then the resulting curve has no longer the enveloping property to link the peaks of the curve
10	2007	Interactive Voice Response with Pattern Recognition Based on Artificial Neural Network Approach.	In the present era of information technology, Information nowadays is just a telephone call away. However, applications such as telephone banking etc. need extra security for making it a reliable service for the people. Application of PIN code/Password via telephone is not enough and additional user specific information is required that can protect the user identity in a more effective way.	An Interactive Voice Response (IVR) based on neural network approach has been proposed that incorporates user specific features in terms of voice extracted through Mel Frequency Spectral Coefficient (MFCC) while Multi Layer Perceptron (MLP) is used for feature matching. The preliminary results shows promise of the approach that can potentially bring added security in applications involving access to bank services etc. via telephone.	No good focuses on improving the error in the patterns recognition on criteria based on false accept and false reject.

11	2014	A NOVEL BUS security solution for BANK IC CARD with FPGA	Bank IC cards are now widely used all over the world, particularly in Europe and Asia, and in the meantime facing serious security problems. To protect bus in the bank IC card against attacks, a novel bus security solution including two methods are proposed in this paper to protect AMBA (Advanced Microcontroller Bus Architecture), which is used for interconnection between the 32-bit CPU and memories or cryptographic algorithms in the bank IC card SoC system.	Two countermeasures against attacks are implemented in the bank IC card SoC system: 8BI 1 0B is used to decrease the power consumption characteristics of the bus; CRC is used to detect faults injected into the bus.	Because of high complexity the efficiency of the system is very low.
12	2013	A Multi layer Bank security System.	In this paper highly reliable, multi level and most efficient locker room security system has been Designed. It include biometric system, a fingerprint scanner ,the security of the main door of the Locker room.	* Two distinct security systems. *Iris scanned and fingerprint s is available.	*This particular security system does not need presence of any human being. *Most efficient security system.
13	2016	Fingerprint and Iris biometric controlled smart banking machine embedded with GSM Technology for OTP.	This paper describes a system that replaces the ATM cards and Iris authentication. One most feature of one time password Important privacy to the users and emancipates him/her from recalling PINS.	Two methods Are used. (Fingerprint and Iris).	A password which is valid only for a single transaction a OTP.
14	2015	Design and implementation Of anti-theft ATM machine using embedded system.	The implementation is achieved with the use of machine to machine communication technology. It provides real time monitoring and control without the need for human intervention. It is based on ARM-11 and Linux OS using Raspberry pi.	*It is higher communication efficiency *Low cost.	The web server can run on an embedded system having limited resource to serve embedded web page to web browser.

15	2016	Open CV pattern Based bank security system with the ft and identification using android.	Pattern recognition in a particular Type of biometric system using RFID tag & the password entry.	Secure access to the bank lockers and the financial institute.	In this locker key method is that any one can access the locker.
16	2016	Underlying text independent speaker recognition	Evaluation of automatic speaker recognition from numerous perspectives. Automatically recognizing a person based on their speech.	*Voice biometric can be defined as it is a human being generated voice speech. which is use for authenticating a human identity. *Easy to measure speech.	Automatic speaker recognition technology will be the challenges for the now generation.
17	2017	Test dependent voice recognition system using MFCC and VA for security app's.	Voice recognition system using Mat lab, So that users can only access it.	The noise & accuracy with be low compared to other technology.	Cost &computation time will be more.
18	2017	Survey ON integrating face and iris biometrics for security motive using chance detection mechanism.	In these face & the iris recognition have been employed in security system.	*High accuracy *Loss of password & identity cards are not needed.	Cost & computation time will be more.
19	2016	Presentation attack detection in face biometric using raw sensor data from smart phones.	Face recognition for smart phone based authentication application.	*Unlocking the smart phones. *E-commerce *E- banking.	Smart phone based face recognition can be misused by the unauthorized users.

V. PROBLEM STATEMENT

From the literature survey, it has been inferred that all the previous works on this topic either involve a system in which, the mechanism used to collect real time data such as camera, sensors, RFID etc. These are all providing security to the customer in real world also, but these are not so safe today's world. Come to the RFID as radio frequency identification technology or RFID continuously follows the line of progress in the field of business these days, people tend to arrive at a certain point where questions arise. Aside from the bucket of benefits which can be obtained from RFID, owners also tend to peek on the disadvantages of using radio frequency identification technology. As we arrive at biometric is cost. Different biometric technologies need the use of different devices that have a range of costs. Also the use of these biometric devices may cause delay in people's day. In open access the CV pattern the locker key method is that anyone can access the locker.

VI. PROPOSED FRAMEWORK

Compare to all other works proposed this proposed work uses voice module, MATLAB, Face recognition with live image authentication. In this work we are using ARM – 7 processor. It consists of 64 pins so that it can be connected with all other peripherals to it with a single processors. It can have voltages of 3.3V and 5V supply. The MATLAB coding is used to find the face recognition of a person so, we are using the OTP based information with the GSM module. The OTP has entered by user to verify if authorized person or not. The information will be stored in the database. The LCD used is 16X2 select the identity modules with giving the AT command. The proposed work provide the high security.

Block Diagram.

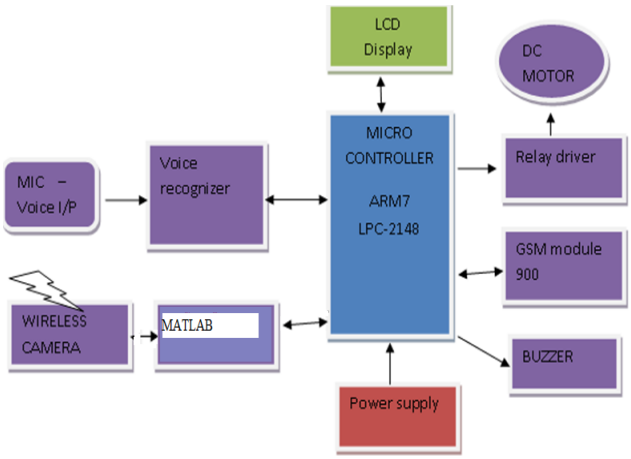

Fig. I. Transmitter section

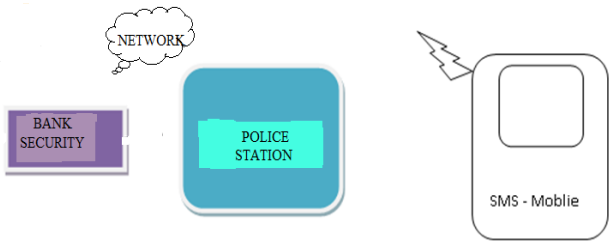

Fig. II. Receiver section.

VII. 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]Latha 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.
[15]Blessed Joshua A`. "Open CV pattern Based bank security system with the ft and identification using android", Alpha college of engineering , Chennai, 2016.
[16]R.A. khan .Underlying text independent speaker recognition", SIST-DIT babasheb bhimrao ambedkar university, 2016.
[17]Ashwin Nair Anil kumar. "Test dependent voice recognition system using MFCC and VA for security app's". Heriot –watt university , 2017.
[18]K.Suganthi^2, "Survey ON integrating face and iris biometrics for security motive using chance detection mechanism", IEEE International conference on science technology, 2017.
[19]R. Raghavendra. "Presentation attack detection in facebiometric using raw sensor data from smart phones". International conference on single image technology", 2016.