International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 6, June 2014 ISSN 2319 - 4847

Multi-Modality Biometric Assisted Smart Card Based Ration Distribution System

Yogesh Kumar Sharma[1], Dr K B ShivaKumar[2], Srinidhi G A[3] and Dr Manoj Kumar[4]

[1] Research Scholar, Mewar university, Rajasthan, India.
[2]Professor, Dept of TCE, SSIT, Tumkur, Karnataka, India
[3]Asst Professor, Dept of TCE, SSIT, Tumkur, Karnataka, India
[4]Professor, Department of Mathematics, RKPGC, Shamali.

Abstract

Every Indian family is issued a Ration Card by Government of India and the families are entitled to receive subsidized food grains against the card. Quantity of different grains like rice, wheat are fixed for every month for the families depending upon their income. However many families do not claim their quota of ration and yet few families manages to acquire card of other families. This has lead to anarchy and black marketing of the subsidized product.

As a solution to aforementioned problem this paper proposes a transparent and highly scalable Ration Distribution (Food Distribution) system with biometric authentication with face and fingerprint Biometric for Ration Card Holder. Every time ration is collected by the family is logged into the smart card. The data logging system is connected with cloud to maintain a centralized inventory across the nation. Biometric data of one member of the family is also logged in the card. Every time before ration collection, the authorized person needs to go through the verification phase. Once verification is done, quantity that he collects is also logged into the system.

Therefore not only false and dummy card ration collection is avoided but at the same time a proper log of quantity par product acquired by the card holder is also tracked. This architecture replaces the conventional paper ration book with RFID based smart card.

Keywords: Biometric, Ration Distribution, RFID, Face Recognition, Voice Recognition.

1. INTRODUCTION

People stand in long queues to get kerosene at ration shops Cardholders in rural areas complain that fuel is not supplied on time and in right quantities

Figure 1: Queue in Ration Shops

Figure 2: Image of a Ration Shop

In urban areas, kerosene is supplied to ration card holders in the first week of every month and the ration shop keepers are taking keen steps to distribute kerosene to cardholders a minimum of three or four days a week. But strangely, in rural areas, the general public is complaining that kerosene is not supplied to them properly. They vehemently leveled charges against the ration shop keepers for delay. In an effort to make the public distribution system (PDS) more efficient, various state government in India has decided to introduce smart cards for the consumers. In the initial phase of the project, simputers or hand-held computers would be installedSpecial training in operating these simputers is being given to ration dealers in the state.

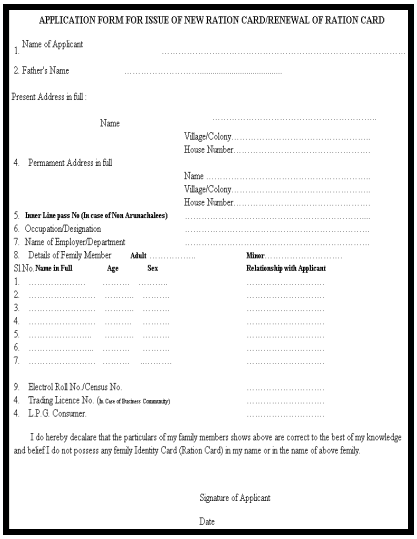
The computers would keep updated consumer information and provide online information of all stocks available in a particular PDS outlet.

Under the new system, every ration shop would have a hand-held computer, a printer and billing machine.

Many ration shop owners, however, are opposing the move.A smart card has a computer chip and enables its holder to purchase goods or avail of services, or perform other operations using data stored on the chip.

Here we listen to various kinds of news where the general public for whom the Rations shops system was established in India long back keeps on raising doubts on the system and the government trying to take actions to thwart off any misdoings by the ration shop owners.

Government provides the food, oil and fuel to economically challenged people at subsidized rates which are distributed to the public through ration shops. They also fix an upper limit on the consumption per head. For this they get a form filled which looks something like the figure on the left. Also a sample form has been attached in this document which is required to be filled for getting the ration card issued.



APPLICATION FORM FOR ISSUE OF NEW RATION CARD/RENEWAL OF RATION CARD

1. Name of Applicant .....
2. Father's Name .....

Present Address in full :

Name .....
Village/Colony .....
House Number .....

4. Permanent Address in full

Name .....
Village/Colony .....
House Number .....

5. **Inner Line pass No (In case of Non Arunachalees)** .....
6. Occupation/Designation .....
7. Name of Employer/Department .....
8. Details of Family Member **Adult** ..... **Minor** .....

Sl No.	Name in Full	Age	Sex	Relationship with Applicant
1.	.....	.....	.....	.....
2.	.....	.....	.....	.....
3.	.....	.....	.....	.....
4.	.....	.....	.....	.....
5.	.....	.....	.....	.....
6.	.....	.....	.....	.....
7.	.....	.....	.....	.....

9. Electrol Roll No./Census No. .....
4. Trading Licence No. (In Case of Business Community) .....
4. L.P.G. Consumer. .....

I do hereby declare that the particulars of my family members shown above are correct to the best of my knowledge and belief I do not possess any family Identity Card (Ration Card) in my name or in the name of above family.

Signature of Applicant

Date

Figure 3: A typical Ration Card Application

Here the personal details of the family are noted and then they are issued a ration card which also acts a nationality and address proof for the citizens of India. The modus operandi for these ration shops is that the material is bought from the farmers and then sold at subsidized rates. Every month fresh stock arrives at these shops and that needs to be disbursed to public. Typically the ration shop owners play foul and the 'right amount is not disbursed' or 'disbursed to unauthorized people' or 'sold out at higher rates'.

To counter these fouls government is taking some measures like introducing the smart cards. However this can also be circumvented by the wrong doers and use the same card for issuing to unauthorized people as the card owner need not be present at the time of the ration disbursement.

At this point we propose a Biometric Enabled Smart Ration Card shop which will have the following features:

1. Fitted with biometric sensors to identify the right person.
2. Will have predefined list of dependents of the ration card holder.
3. Will have prior information about the amount of ration to be disbursed.
4. Will display the current rates.
5. Will have automatic disbursing mechanism etc.
6. Will monitor the 'stock taken IN' and the 'current stock' status.

Explaining these features in details:

The ration card holder (the head of family) will get all his dependents registered at the ration card issuing authority. The thumb scans of all the family members will be recorded and kept for future records. These will be required to match at the ration card shop while disbursing the required amount. The biometric sensors will be able to co-relate as to who belongs to what family and accordingly the items will be disbursed and accounts will automatically be maintained.

Depending on the number of dependents in a family the system will calculate the upper limit of the rationing and will maintain this record for future references. It can also maintain a log as to which family has been consuming how much.

At the shop the current rates of the items will be displayed on the monitor.

In the automatic disbursing mechanism we will connect a weighing machine and a grain disbursing mechanism. Once the disbursed amount (weight) matches the requested amount then the disbursing will stop and accounts will be automatically updated.

In this project we will also be maintaining an account of the material which is coming in the ration shop and will automatically be maintaining the current status so that the owner cannot claim that the goods are over.

In all this mechanism will be a boon for the economically challenged people who depend on these shops a lot.

Areas Covered:

In this project we will be covering and understand the following topics:

- 8051 Hardware Designing

- Coding in 8051 Assembly
- Biometric sensors
- PCB designing and concepts
- Controlling and driving mechanism of Relays to control External Devices.
- Motor controlling mechanisms
- Differential amplifiers concepts
- Load cells
- PC Connectivity – Serial and Parallel Ports
- VB Coding strategies etc.

Future enhancements:
In future we can even automate firing on the unidentified boats and the messaging can be handled by satellite telephony.

2. RELATED WORK

[1] Elaborates the various techniques for biometric data security by proposing a matching environment based on smart cards. It also elaborates the mechanism of generating a hash from the fingerprint biometric data and encrypting data through this hash.
Authors in [2] deal with the variability in the biometric templates. According to the finding of the author, every matching for authentication must also measure the quality of the just generated template and periodically must update the template in order to maintain high accuracy in biometric authentication process. The paper also presents matrices for biometric template quality analysis which is used in the proposed benchmark analysis work.
Authors in [3] elaborate the main problem with the conventional password based security techniques and emphasizes on the facts as to why the biometric keys are better than conventional keys. The work defines the technical steps associated with the keys and also discusses the properties of good biometric keys.
For biometric key generation from biometric features like faces and fingerprints, first image specific features must be extracted which is called templates. A quantization is applied on the template to generate the key. As real number range is infinity, if a key is generated without quantization, matching becomes a difficult process. Hence authors in [4] elaborate the mechanism for the quantization process for key generation. They also suggest a log likelyhood based technique for the same.
Even though biometric keys are strong technique for cryptographic key generation, because they are stored in the database, there remains a chance for the keys to be eavesdropped by unauthenticated users which makes the system vulnerable. Therefore techniques must also be adopted for such key generation. Hence authors in [5] proposes the techniques for securing the biometric key itself.
[6] proposes an Iris recognition technique with the help of bio orthogonal wavelets. But most importantly the authors in [6] proposes an encoding technique for the templates for ease in matching.
The strength of a biometric key is defined from the inability of a propoer guessing of a key using brute force technique. A biometric key appears random to any intruder. Therefore how he guesses the key depends upon the entropy information of a random variable that generates the key. [7] defines a mathematical relationship of probability of successful guess of a key with the entropy information of the templates and hence quantifies the fact that entropy analysis of any template is an important step in deciding the strength of the key.
The closeness of a template with the stored template depends upon the distance between the templates. This distance can be represented in various mathematical forms as proposed by the authors of [8]. The authors also proves experimentally that log likelyhood measure is one of the better way of representing the closeness of two templates.
Whenever a mechanism is selected for biometric template matching for authenticating purpose, it invariably presents a false rejection and false acceptance on the biometric data and the mechanism itself. The authors in [9] presents a unique way to select the appropriate tradeoff between the rejection and acceptance tradeoff so that the adopted technique is acceptable and efficient. The author also presents a benchmark analysis for optimality for any recognition technique in [10] and illustrate the proposed theory with the help of character recognition system.
Gabor based techniques are widely adopted for biometric feature representation or generation of templates. But the size of such initial vectors is so high that it presents a practical problem of storage. Thus biometric template reduction becomes an important aspect for biometric key generation or authentication technique. [12] presents a technique for minimizing the number of feature vectors for template generation.
Out of all the possible attacks on biometric keys the most severe attack is on the stored keys. This findings of [13] forms a base for our assumption that if a system can be deviced without the necessatiy for the key to be saved, a biometric system can be made un-attackable. Even though the authors present multi biometric model for hardening the security of a biometric system, the system still remains vulnerable against the attacks.
For any biometric like face or fingerprints or iris, templates will differ from one instance to the other instance of acquisition. Therefore out of N number of aquistion of the templates of a single feature type of a person there would certainly exist a variability amongst the templates. Therefore authors in [14] presents a systematic way of extracting the

best template out of all the templates. This paper also presents an important step for biometric feature benchmark analysis by proposing a clustering technique for seggegating the biometric features by their average distance measures.

3. PROPOSED SYSTEM

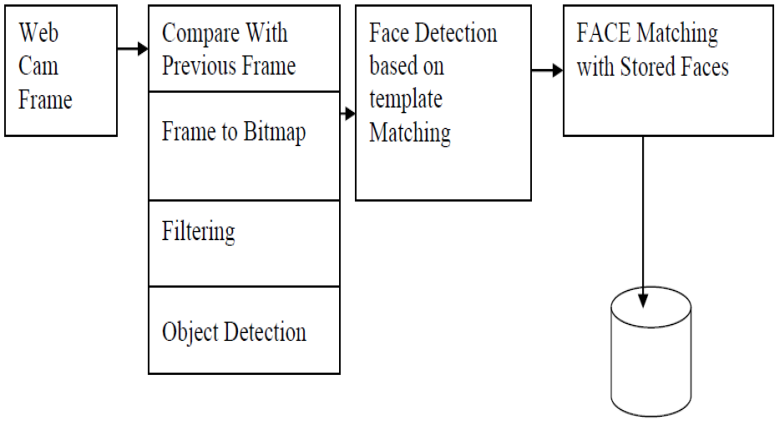


Figure 4: Block diagram of the proposed system

The function of the system is as follows
1) Every User is Provided with a Card which is of EPROM type
2) The Card is Registered by the Government Authority
3) At the time of Registration, The Users Face Sample and Other Details are Stored
4) At the Time of Authentication, duplicate users presence is checked
5) Once a card is allotted, the User Needs to Bring the Card Every time he visits the Ration Shop to collect the Ration.
6) At the Time of Ration Distribution, first his Face is verified. Once face verification is successful, user is asked for a PIN, if PIN is valid, then he is subjected to get the Ration.
7) Before Distribution, Ration Distributors voice is authenticated.
8) The Weighing Machine is checked for proper weight. If the Weight is proper, then the ration is distributed and the distribution details are stored.

4. METHODOLOGY

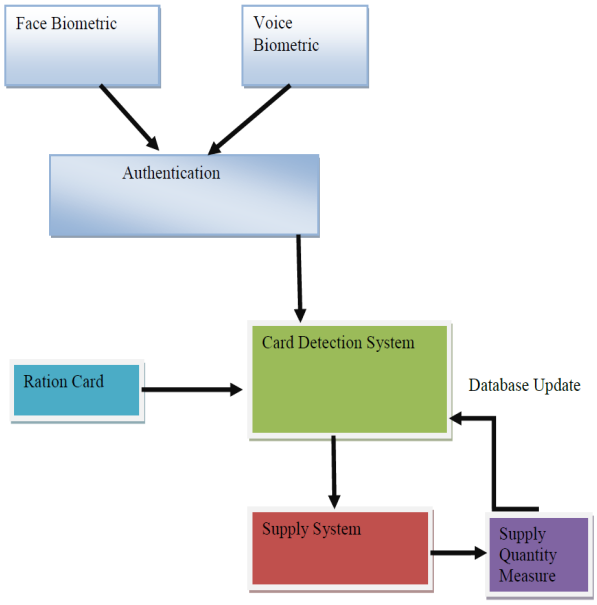


Figure 5: Typical Architecture Diagram of the Proposed System

Figure 5 clearly explains the system. It is a depiction of proposed work as elaborated in section III.

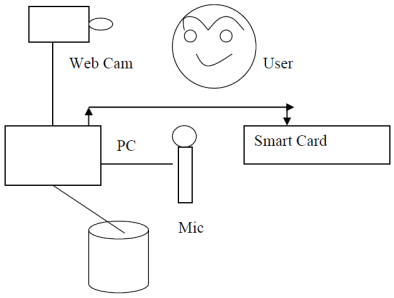


Figure 6: Block Diagram of Face Matching Stage

Figure 6 clearly explains the face matching stage. As it is seen from the above diagram that the face matching is divided into two parts : Registration and verification. Registration is performed at the time of issueing the card. This stage includes extracting facial templates which are Eigen component of normalized eigen face. This data is stored in the RFID card.

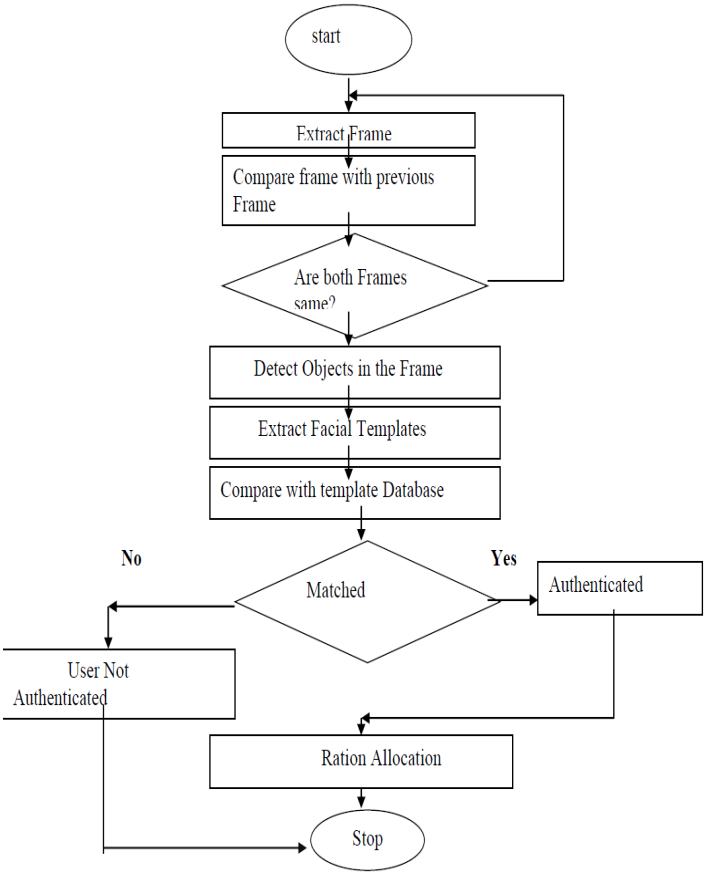
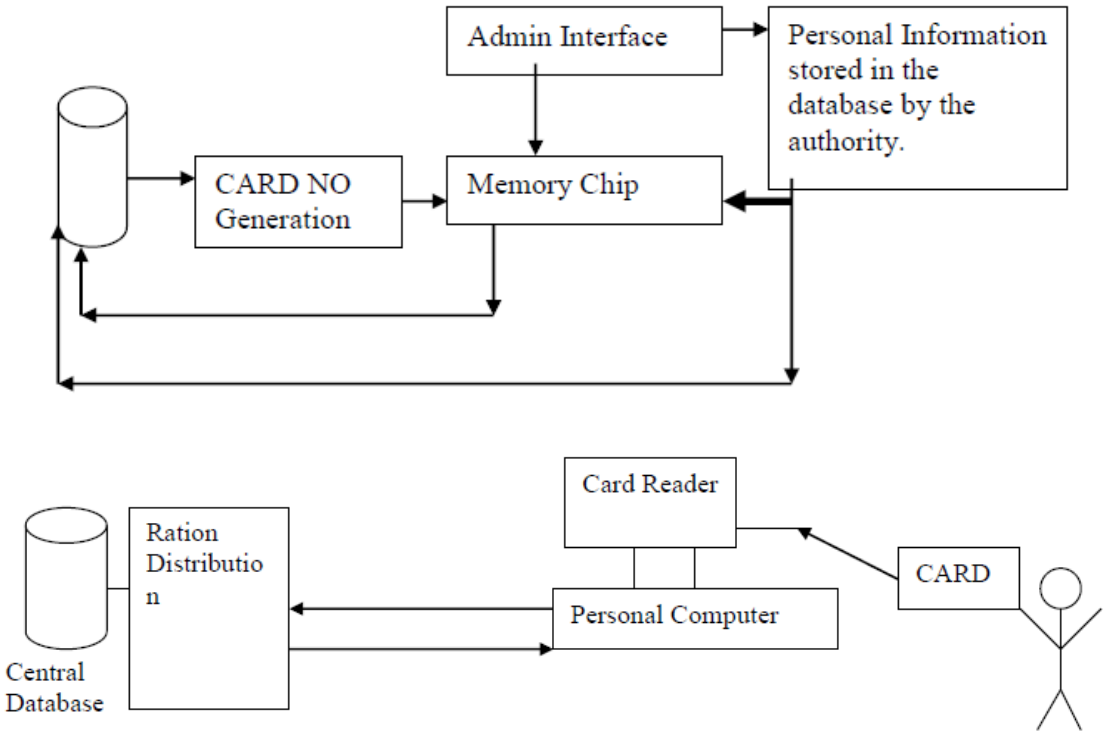


Figure 7: Flow chart of face matching stage

In the face recognition process following are the functionality are Performed

1) In the first module The face of the user is captured. The program is developed with c#.Net. Here a camera interface is interrupted with a timer to capture the face of the user . Once user selects save option the image is saved in the database with the name “face1a.jpg” for user with card number 1 and so on.
2) At the time of testing, again, the face is captured and it is saved as face1c.jpg and are matched with the faces in the database.
3) The matching process is based on Eigen Face. In this technique, first all the faces in the database are added to get an eigen face. The test face is subtracted with this average eigen face minus the user instance. The smallest difference is selected as matching face.



Initial Logic of SSN generation
Figure 8: Block Diagram of RFID Stage

In the next section we discus the details of the card and the electronic aspect of the Transceiver system.

Memory Organization

The card memory is organized as 8192 Bit EEPROM, which is split into 16 sectors with 4 blocks. One block consists of 16 bytes (1 Byte = 8 Bit).

The card memory organization is as:

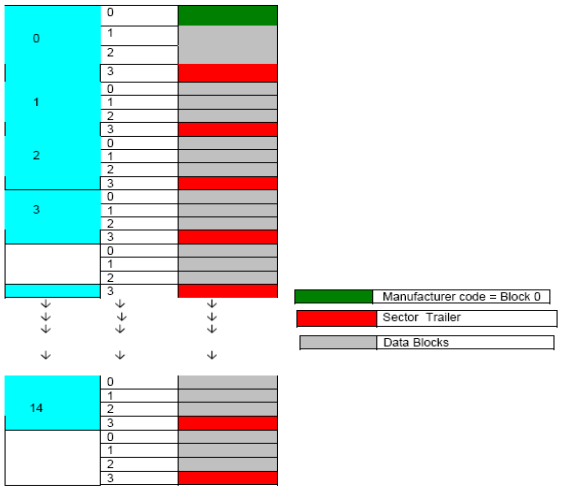


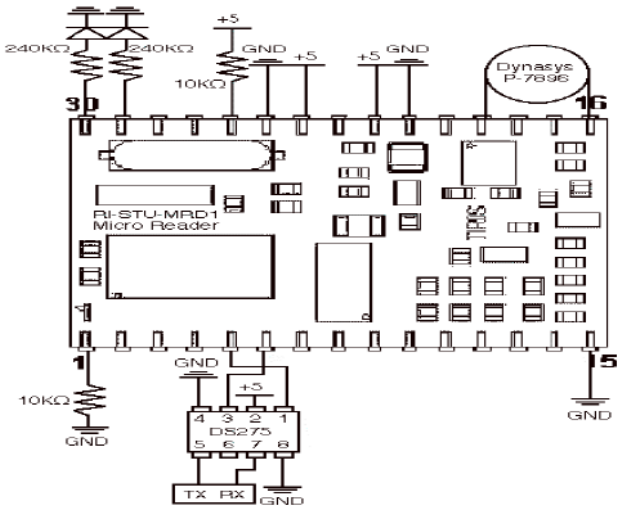
Figure 9: RFID Card Memory Structure

Manufacturer Code (Block 00 of Sector 0)

The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. It is named as “Block 0”.

Data Block (Block 0 to 3 except "Block 0")

Access conditions for the Data Blocks are defined in the Sector Trailers.
According to these conditions data can be read, written, incremented, decremented, transferred or restored either with Key A, Key B or never.
The card consists of two types of Data Blocks:
1. Read/write blocks:
These blocks are used to read and write general 16 bytes of data.
2. Value blocks:
These blocks are used for electronic purse functions like read, increment, decrement, transfer and restore. The maximum size of a value is 4 byte including sign bit, even when a complete 16 byte block has to be reserved. To provide error detection and correction capability, any value is stored 3 times into one value block. The remaining 4 bytes are reserved to some extent for check bits.



Circuit Overview

Figure 10: Circuit diagram of RFID reader

This circuit design enables the RI-STU-MRD1 Micro Reader to communicate with a computer or other device using the RS-232 protocol. The DS275 chip changes the 5 volts communications signal from the Micro Reader to a standard 12 volts. Connected between pins 16 and 19 on the Micro Reader is a Dynasys P-7896 antennae. The status of the antennae is shown via the LED connected to pin 30. If the antennae is active the pin will go low, turning the LED off, else it will be high. The LED connected to pin 29 goes high to signal a successful tag read.

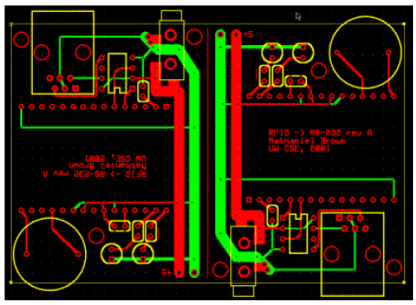


Figure 11: RFID Board PCB Layout

Two RFID boards are combined onto a single board to take advantage of ExpressPCB's cheaper mini board prices. Power is connected to the board using 3.5mm audio jacks. There is a surface mounted jack on one side of the board and a panel mounted one on the other. This enables meeper receiver stations and RFID tag readers to be easily chained together, thus needing only one power supply for several boards. The communications port on this board is a RJ-11 style connector,

which is the same as on the meeper receiver station. This is much more compact for communications between the RFID tag reader and the meeper receiver station, and can be connected to a DB-9 connector using an adapter. Pin 2 on the RJ-11 connector is set up for transmit and pin 5 is receive. Pins 3 and 4 are tied to ground.

Voice Biometric System

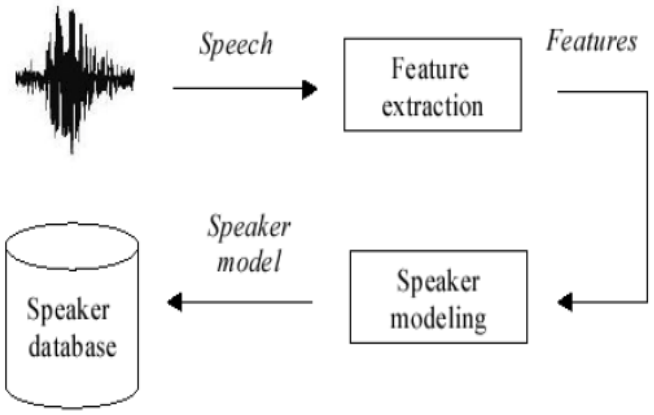


Fig.12: Block Diagram of Enrollment Phase

In the second phase, verification phase as shown in the Fig, features are extracted from the speech signal of a speaker and these current features are compared with the claimed features stored in the database by a process called Feature matching. Based on this comparison the final decision is made about the speaker identity.

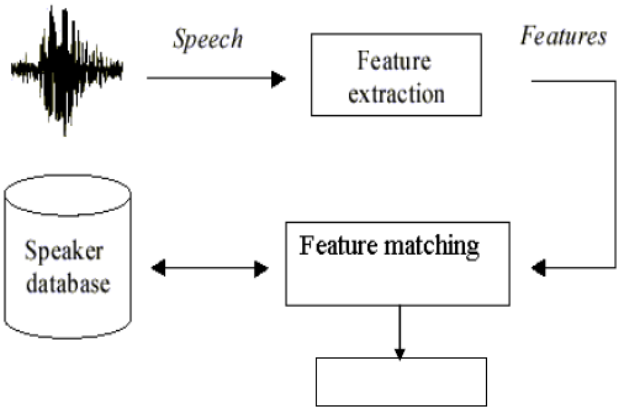


Fig.13: Block Diagram of Verification Phase

Both these phases include Feature extraction, which is used to extract speaker dependent characteristics from speech. The main purpose of this process is to reduce the amount of test data while retaining speaker discriminative information.

5. FEATURE EXTRACTION PROCESS

In speaker recognition first we convert the speech waveform to some type of parametric representation (at a considerably lower information rate) for further analysis and processing. This is often referred as the signal-processing front end.
A wide range of possibilities exist for parametrically representing the speech signal for the speaker recognition task, such as Linear Prediction Coding (LPC), Mel Frequency Cepstrum Coefficients (MFCC), and others. MFCC is perhaps the best known and most popular, and this will be used in this project.
MFCCs are based on the known variation of the human ear's critical bandwidths with frequency, filters spaced linearly at low frequencies and logarithmically at high frequencies have been used to capture the phonetically important characteristics of speech. This is expressed in the mel-frequency scale, which is a linear frequency spacing below 1000 Hz and a logarithmic spacing above 1000 Hz. The process of computing MFCCs is described in more detail next.

Mel-frequency Cepstrum coefficients processor:
A block diagram of the structure of an MFCC processor is given in Fig.. The speech input is recorded at a sampling rate of 16 KHz. This sampling frequency was chosen to minimize the effects of aliasing in the analog-to-digital conversion.

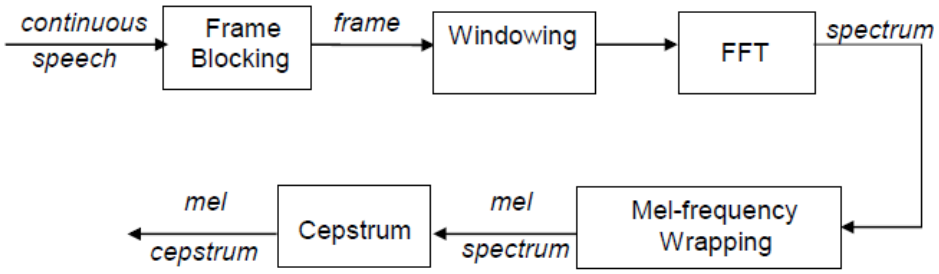


Fig 14: Block diagram of the MFCC processor

The processor takes continuous speech signal as input and generates mel-frequency cepstrum coefficients as outputs. It uses the following 5 steps to accomplish this task:

6. RESULTS

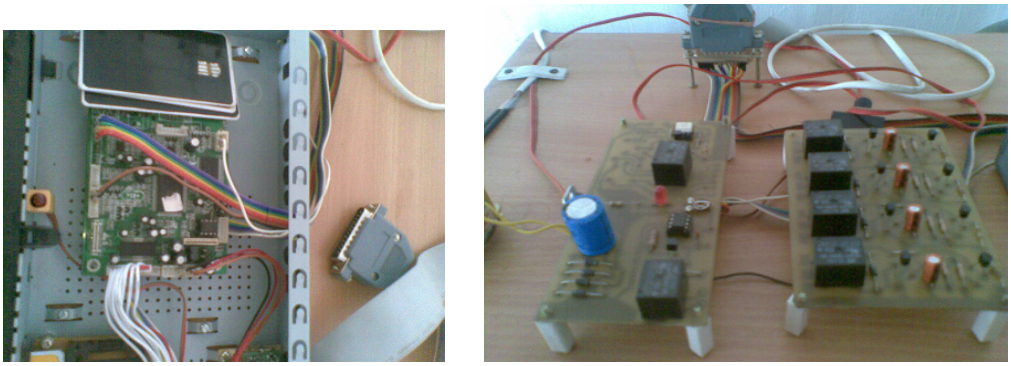


Figure 15(i): Hardware System of RFID Card and Receiver (ii)Relay Drive for triggering a) Authentication b) card validation c) card writing and d) ration allocation

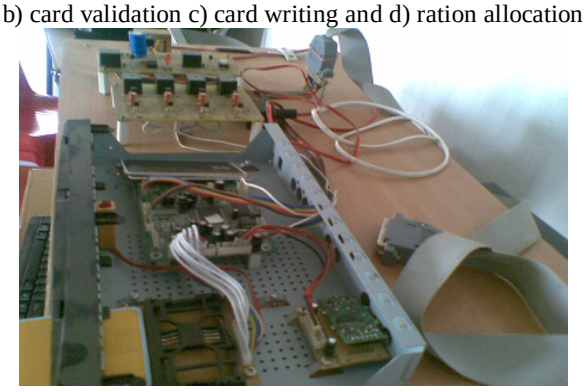


Figure 17: Overall System

7. CONCLUSION:

The proposed system uses Low cost biometric solution which do not require costly sensors like that of fingerprint sensors. It mainly comprises of three different software which are best for the respective selected processing the system provides security to both the distributor as well as the user. Other than admin nobody can temper with the card.

The Face Recognition system adopted here is Pose and Light Invariant. Voice Biometric system can detect even the tempered voices. Also the cards are capable of storing the images also which provides human level visual security Card Information is protected with password and can not be retrieved by unknown and intruding persons. This provids a unique secured ration distribution system which if adopted can practically change the blackmarketing associated such a system. Results shows that face recognition system works at an independent efficiency of 90%, voice recognition works at an efficiency of 82% and collectively the system provides an accuracy of 98% with only .2% false acceptance rate.

REFERENCE:

[1] Magnus Pettersson, The Match On Card Technology, Precise Biometrics White Paper
[2] Ricardo García Noval, Francisco Perales López, Poster: Adaptative Templates In Biometric Authentication

[3] Lucas Ballard, Seny Kamara, Michael K. Reiter, The Practical Subtleties Of Biometric Key Generation,17th Usenix Security Symposium
[4] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, A.H.M. Akkermans, Multi-Bits Biometric String Generation Based On The Likelihood Ratio,Doi: Multi-Bits Biometric String Generation Based On The Likelihood Ratio,Ieee, 2007
[5] U. Korte, R. Plaga, Cryptographic Protection Of Biometric Templates:Chance, Challenges Andapplications
[6] Aditya Abhyankar , Stephanie Schuckers, Novel Biorthogonal Wavelet Based Iris Recognition For Robust Biometric System, International Journal Of Computer Theory And Engineering, Vol. 2, No. 2 April, 2010 1793-8201
[7] James L. Maseey, Guessing And Entropy,Doi: 0 - 7803-2015-8/94, Ieee,1994
[8] Asker M. Bazen And Raymond N. J. Veldhuis, Likelihood-Ratio-Based Biometric Verification, Ieee Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, January 2004, 1051-8215/04,Ieee, 2004
[9] C. K. Chow, On Optimum Recognition Error And Reject Tradeoff, Ieee Tr.4nsactions On Information Theory, Vol. It-16, No. 1, January 1970
[10] C. K. Chow, An Optimum Character Recognition System Using Decision Functions, Pgec, June 3, 1957
[11] Juels A. And Wattenberg M., "A Fuzzy Commitment Scheme", Acm Conference On Computer And Communications Security", 1999, P.28-36
[12] Daniel Gonz´Alez-Jim´Enez And Jos´E Luis Alba-Castro, Modeling Marginal Distributions Of Gabor Coefficients: Application To Biometric Template Reduction, Project Presa Tec2005-07212
[13] V. S. Meenakshi1 And Dr G. Padmavathi, Securing Revocable Iris And Retinal Templates Using Combined User And Soft Biometric Based Password Hardened Multimodal Fuzzy Vault, Ijcsi International Journal Of Computer Science Issues, Vol. 7, Issue 5, September 2010 Issn (Online): 1694-0814
[14] Anil Jain, Umut Uludag And Arun Ross, Biometric Template Selection: A Case Study In Fingerprints, Proc. Of 4th Int'l Conference On Audio- And Video-Based Person Authentication (Avbpa), Lncs 2688, Pp. 335-342, Guildford, Uk, June 9-11, 2003.

AUTHOR:

Yogesh Kumar Sharma had completed B.E.(Computer Sc. and Engineering) from Bangalore University in 1993. He Completed his M.Tech(Computer Sc.) from JRN University , Rajasthan in 2005. Currently, he is pursuing his Ph.D(Computer Sc.) from Mewar University, Rajasthan. His area of research is Cryptography and Network Security. He has published 35 papers in national and international conference proceedings. He is a member of many international bodies.

Dr K B ShivaKumar received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA Degree from Bangalore University, Bangalore and M Phil Degree from Dravidian University Kuppam. He obtained Ph.D. in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 30 years of teaching experience and has over 60 research publications in National and International conferences and journals. Currently he is working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Multi rate systems and filter banks, and Steganography

Srinidhi G A received the BE degree in Telecommunication Engineering, from Visveswaraya Technological University, Belgaum, Karnataka, MTech degree in Sensor Systems Technology from VIT University Vellore, Tamilnadu. He has over 10 research publications in National and International conferences and journals. Currently he is working as Asst Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Automotive Sensor systems, MEMS and Steganography.

Manoj Kumar received the B.Sc. degree from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography, from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi- India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to March 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. - INDIA from March 2001 to Nov 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. - INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is an Assistant Professor in Department of Mathematics, Rashtriya Kishan Post Graduate College, Shamli, (Chaudhary Charan Singh University Meerut-INDIA). He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical

Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as reviewer for various International peer review Journals. He is also working a Technical Editor for various some International peer review Journals. He is also the member of Technical Programme Committee of various national and international conferences. He has published more than 40 research papers at national and international level in review Journals. His current research interests include Cryptography and Applied Mathematics.