User authentication techniques for implementation of Smart Card Based Ration Distribution System

Yogesh Kumar Sharma[1], Dr Manoj Kumar[2]
[1]Research Scholar, Mewar university, Rajasthan,INDIA
[2]Department of Mathematics, RK(PG) College, Shamli,INDIA

Abstract: Ration Distribution System means distribution of essential commodities to a large number of people. It is done by the government. Since the distribution of ration is done without any computerized systems in India, there are high chances that people involve in distribution can do corruption and illegal smuggling of goods. All these happen because every job in the ration shop involves manual work and there are no specific high-tech technologies to automate the job. The main objective here is to automate the process of the distribution by using a smart card based model with helps in proper distribution of ration to authentic persons.

1. Introduction

In urban areas, kerosene, wheat and rice etc 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 and other items are 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 installed. Special 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

2. Literature Survey

Recently Vikram et al. [1] has proposed Smart Ration Card System. The smart card is modified as a smart ration card by coding Microprocessor chip present in it according to the requirement. The smart card contains unique barcode. When the consumer visits the ration shop, he has to show this card in front of barcode reader. Dealer verifies the smart card & accordingly delivers ration.

S.Valarmathy et al. [2], Mohan et al. [4] has proposed an automatic ration material distribution based on GSM (global system for mobile) and RFID (Radio Frequency Identification) technology instead of a ration card. This system is automatic and provides ration without interference of human. In this system various sensors are used to measure and dispense the commodities.

Dhanashri et al. [5] and Neha et al. [3] has developed web enabled superior public distribution system. The system remotely monitors the outlets of various goods and vehicles, providing ration to ration shop. In this system, subscriber has to access the website every time they desire to get a ration.

Sharma et. al. [6] has proposed new ration distribution system using biometrics, face recognition and voice recognition system.

In automated ration distribution system the setup is to be installed in every ration shop. In present scenario more than 0.5 million ration shops exist in India. So it is very costly to have an automated PDS and it is a tedious job for illiterate people operating such complex system. On the other hand barcode based systems are not secure because the dealer can have duplicate barcode on the basis of which fake ration cards can be made.

The strength of a biometric key is defined from the inability of a proper 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. James L. Maseey [7] derived 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 Asker M. Bazen et al. [8]. The authors also prove 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. C. K. Chow et al

[9] presents a unique way to select the appropriate trade-off between the rejection and acceptance trade-off so that the adopted technique is acceptable and efficient. The author also presents a benchmark analysis for optimality for any recognition technique [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. Daniel et al.[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 finding of V. S. Meenakshi et al. [13] forms a base for our assumption that if a system can be deviced without the necessity 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.

3. Tools of Authentication

3.1 Physical Appearance: - Physical appearance is the token of authentication prevailing in the physical world. How we look: height, complexion, eye-colour, hair-colour physique etc all such characteristics that determine a particular personality decide whether someone is a stranger or a known person to one who is seeking authentication through physical appearance. But physical appearance can be changed to deceive a person.

3.2 Digital Signature: - Digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

3.3 Message Authentication Code (MAC) :- It is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. A message integrity code (MIC) is different from a MAC in that a secret key is not used in its operation. Although the terms are sometimes used interchangeably, a MIC should always be encrypted during transmission if it is to be used as a reliable gauge of message integrity.

3.4 Biometric Authentication:- biometric is the next generation of authentication methods. Although it's number of false results, biometrics will change the way we authenticate ourselves, hopefully with 99% accuracy. Biometric systems may include fingers systems, voice recognition systems, eye/retina scanner systems, hand geometry systems and handwriting systems or the system regarding other unique physiological characteristic. Its is beneficial over authentication methods because biometrics cannot be stolen, cannot be forgotten; neither can they be given to another person.

3.5 Smart Card Authentication: Smart card Authentication is supported by Windows 2000/XP out of the box, and provides an extra layer of security because not only must the user provide something he/she knows to log on (in this case a Personal Identification Number) but must also provide a physical object – the card itself. A Smart card is credit card sized Plastic card with an embedded chip that can hold a digital certificate so user authentication is accomplished through a public key infrastructure. A smart card reader attachment (a hardware device is required through which the card is swiped).

4. Structure of the Smart Card

The smart is a credit card sized plastic card, embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory- chip card, (for example, prepaid phone cards) can only undertake a predefined operation. Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of transaction. Smart card provides not only memory capacity, but computational capacity as well. The self-containment of smart card makes it resistant to attack as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications that require strong security protection and authentication. Today smart cards are being used in different areas because they can be used together with other technologies, such as asymmetric cryptographic algorithms and biometric identification.

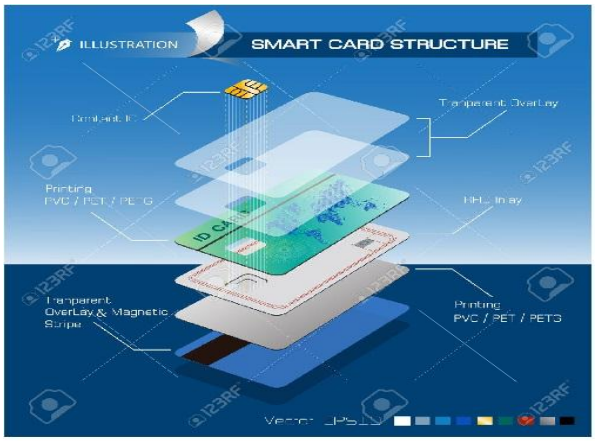

Fig1. Structure of smart card

5. Proposed System

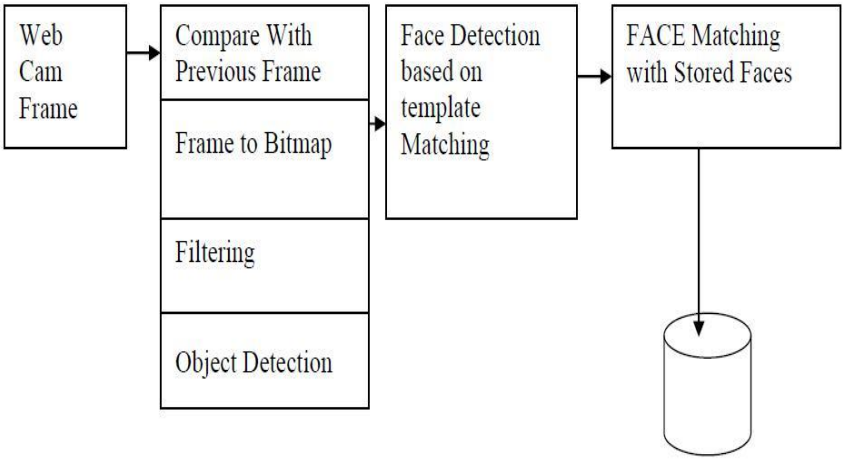

Figure 2: Block diagram of the proposed system

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, Users Face Sample and Other Details are Stored.
4) At the Time of Authentication, duplicate user's 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.

6. Methodology

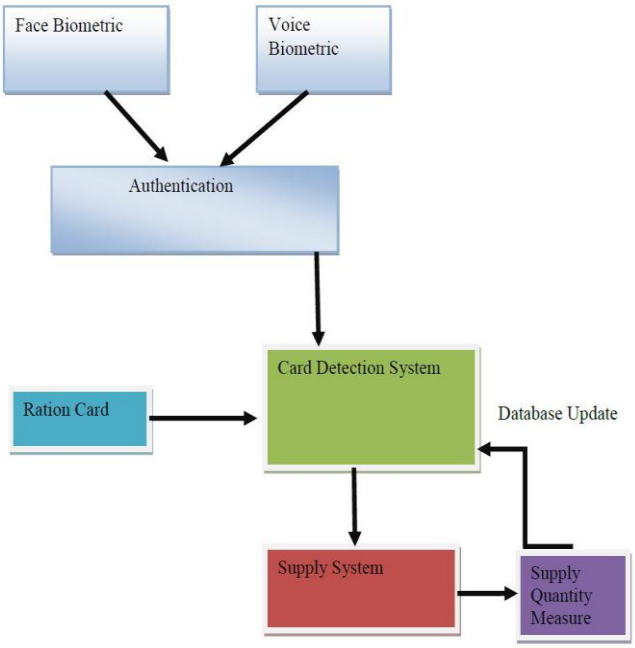

Figure 3: Typical Architecture Diagram of the Proposed System

6.1 Algorithm for face recognition process

Step1: In the first module, 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.

Step2: At the time of testing, again, the face is captured and it is saved as face1c.jpg and is matched with the faces in the database.

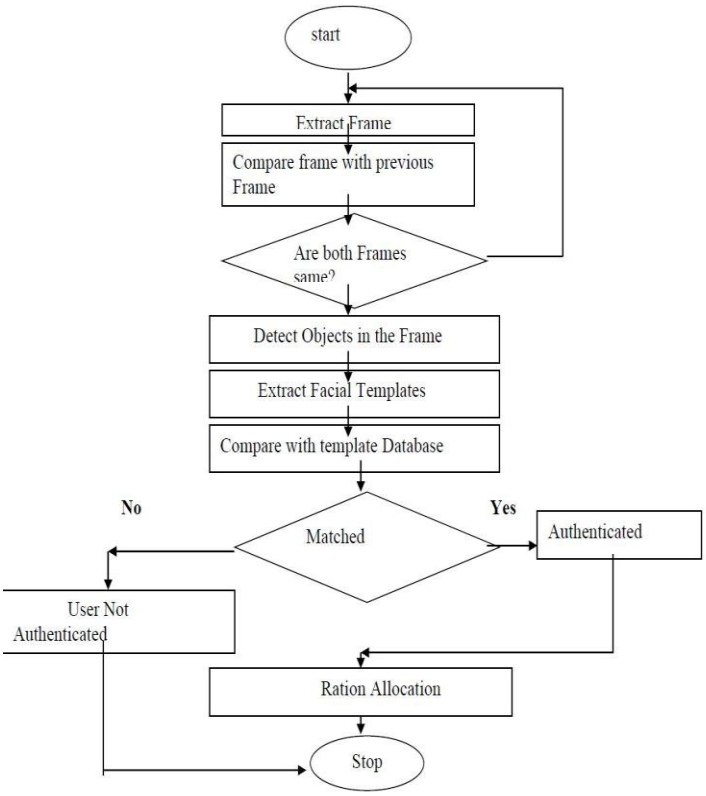

Figure 4: Flow chart of face matching stage

Step3: 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.

6.2 Voice Biometric System

In the second phase, verification phase, 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.

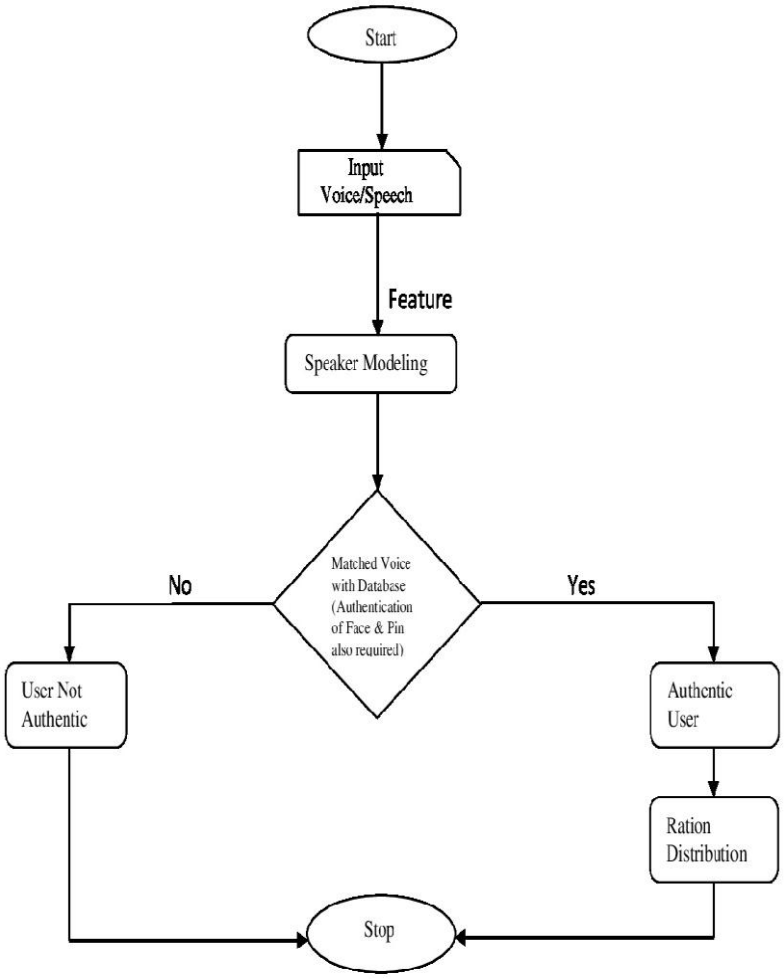

Figure5: Flowchart for voice biometric

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. In feature recognition process, 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 we have used this in this model.

7. Conclusion

Using this proposed modern system we can have Better management of the ration distribution system. Govt. can have indirect check on the availability of the ration to the beneficiary. It is transparent and has control over prices of some commodities in the open market. Dealer will not be able to keep fake ration cards with them. System helps to modernize traditional rationing and combat corruption up to a great extent. The proposed system uses Low cost biometric solution which does 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 cannot be retrieved by unknown and intruding persons. This provides a unique secured ration distribution system which if adopted can practically change the black-marketing 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.

References

[1]Vikram Singh et. al. "Smart ration card", Volume 4, No. 4, April 2013 Journal of Global Research in Computer Science.

[2]S.Valarmathy et. al. "Automatic ration material distribution based on GSM and RFID technology", I.J. Intelligent Systems and Applications, 2013, 11, 47-54 published Online October 2013 in MECS.

[3]Neha et. al. "Web-Enabled Ration Distribution and Controlling." March-2012 International Journal of Electronics, Communication and Soft Computing Science and Engineering.

[4]Mohan et. al. "Automation of ration shop using PLC." VoI.3, Issue.5, Sept-Oct 2013. International Journal of Modern Engineering Research.

[5]Dhanashri et. al. "Web- Enabled Ration Distribution and Corruption Controlling System." Vol.2, Issue 8, Feb 2013, International Journal of Engineering and innovative technology.

[6]Sharma et. al. "Multi-Modality Biometric Assisted Smart card Based Ration Distribution System", volume 3 June 2014, International Journal ofApplication or Innovation in Engineering of Management.

[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