ENGINEERING IN ADVANCED
RESEARCHSCIENCE AND
TECHNOLOGY

ISSN 2352-8648
Vol.03, Issue.01
June-2022
Pages: -376-386

AADHAAR CARD VOTING SYSTEM

[1]ISHTAMSETTY KEERTHY,[2] KURRA SUSHMITHA,[3] SONTI VAMSI ,[4]KAYALA MOUNIKA,[5] YEUMULA NARENDRA,[6] MR A MANIKANTH
[1,2,3,4,5] Student Of ECE Dept. ,KHIT, Guntur
[6] M.TECH, MISTE, Associate Professor

Abstract: Now-a-days a reliable voting system is needed for our society to eliminate the fake voting and to improve flexibility, transparency, and reliability. This paper presents a novel voting system by using QR code of Aadhaar card. The Aadhaar QR code is decrypted by using binarization and Reed–Soloman error correction. Based on the decrypted Aadhaar number in the QR code, it provides a citizen's name and fingerprint details in our database. This Aadhaar voting system (AVS) accepts a citizen fingerprint. If the authentication is success, then it allows the citizen to vote otherwise it does not allow the citizen to vote. This paper provides three document files by using DIARY technique. First document file provides voter's name and voting time. Second document file provides voter's address and information. Third document provides individual party votes and total number of votes. These three document files can be generated and deleted by given specific password through special officer. This AVS machine ON/OFF can be controlled by specific password through special officer. By using this type of system, it will eliminate fake voting and provides more transparency and reliability.

Keywords: Aadhaar card ▪Binarization, Reed–Soloman, errorcorrection Diary technique Minutiae, Ridges Fingerprint

Introduction: So far in India two types of voting systems are used. First one is ballet voting system and second one is Electronic voting machine (EVM). In EVM voting system, the machine does not recognize the authorized person but this is being done manually which can be overcome in this proposed Aadhaar card Voting System (AVS). Nowadays, Aadhaar card utilization is increasing day by day in India. Aadhaar card is used in electronic mobiles, money transactions, to identify the authorized person, etc. This paper develops a novel voting system using Aadhaar card. Aadhaar card contains a citizen information, Aadhaar number, QR code. In that, Aadhaar QR code contains a valid Aadhaar number. By decoding the QR code, the Aadhaar number is obtained. The citizen information can be accessed by using the Aadhaar number. The citizen information contains an iris data, fingerprint data, address, etc. Based on the Aadhaar QR code, a virtual voting System using diary technique is developed. The AVS allows the citizen Aadhaar QR code. The Aadhaar number is extracted by the decoding of QR code. Extract the citizen information and fingerprint from the database based on the Aadhaar number. Next AVS allows the citizen finger print in run time. If database fingerprint and runtime fingerprint matches, then it allows for voting, otherwise it does not accept the citizen to vote. The AVS generates three document files. First document file contains the voter's name and voting time. Second document file contains complete voter information like voter's name, address, and voting time. Third document file produced by specific officer with specific password. This file contains a data of the voter or individual party data. It also provides the total number of votes and percentage of the voting.

Decoding the QR Code

This stage consists of several stages. First stage is identifying the QR code from the Aadhaar card. Second stage is finding the finder patterns and QR code version. Third stage is identifying the alignment pattern. Final stage is performing the Reed– Solomon error correction for decoding the text in QR code (Fig. 1).

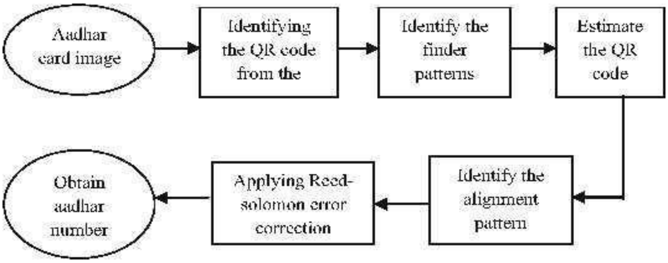

Aadhar card image
Identifying the QR code from the
Identify the finder patterns
Estimate the QR code
Identify the alignment pattern
Applying Reed-solomon error correction
Obtain aadhar number

Fig. 1 Block diagram of QR code decoding

Fig. 2 QR code image using binarization

Identify the Appropriate Alignment Patterns

Low-resolution images and inappropriate binarization make the deformation of alignment patterns. To find out the alignment patterns, first roughly locate and extract one alignment pattern with specified radius by using finder patterns. This alignment pattern can be taken as a sub-image. Next the need is to calculate the connected component of black pixel and white pixel of the sub-image. The connected component of black pixels and the connected component of white pixels are shown in Fig. 4. For each connected component of black pixel Ci in Fig. 4b, check its border pixels. If all border pixels are adjacent to the same connected component of white pixel Cj in Fig. 4c, then check all border pixels in Cj. Once all border pixels in Cj are adjacent to the same black pixel connected component Ck in Fig. 4b, these components possibly contain alignment pattern. Finally, calculate the centroid Ci as the centroid of alignment pattern.

Identify the Appropriate Alignment Patterns

Low-resolution images and inappropriate binarization make the deformation of alignment patterns. To find out the alignment patterns, first roughly locate and extract one alignment pattern with specified radius by using finder patterns. This alignment pattern can be taken as a sub-image. Next the need is to calculate the connected component of black pixel and white pixel of the sub-image. The connected component of black pixels and the connected component of white pixels are shown in Fig. 4. For each connected component of black pixel Ci in Fig. 4b, check its border pixels. If all border pixels are adjacent to the same connected component of white pixel Cj in Fig. 4c, then check all border pixels in Cj. Once all border pixels in Cj are adjacent to the same black pixel connected component Ck in Fig. 4b, these components possibly contain alignment pattern. Finally, calculate the centroid Ci as the centroid of alignment pattern

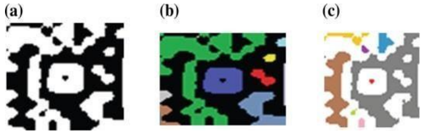


Fig. 3 a Extracted image with radius = 30 pixels, b connected component of black pixels, c connected component of white pixels

2.2 Error Correction

This paper uses Reed–Soloman code for error correction. In this error correction Peterson–Gorenstein–Zierler algorithm is used.

Authentication of Fingerprint

In authentication of fingerprint, stored template fingerprint is compared with the input fingerprint. In authentication of fingerprint consists of two stages. First stage is minutiae extraction and second stage is minutiae matching (Fig. 5).

Minutiae Extraction

In this stage consists of two steps. First step is image enhancement and image segmentation and second step is final extraction.

Image Enhancement and Segmentation

Image enhancement is used to improve the contrast of ridges and furrows in fingerprint. It also connects the false break points of the ridges. Adaptive histogram equalization technique and adaptive binarization method comes under the image enhancement.

Final Minutiae Extraction

The final minutiae extraction consists of four operations. The four operations are ridge thinning, minutiae marking, removal of false minutiae, and finally minutiae representation.

Ridge Thinning: The ridge thinning process reduces the redundant pixels of ridges. It is repeated until the obtained ridges are only one pixel wide. This can be achieved by using the following MATLAB function.

Diary Technique

It is a command in MATLAB software. This function creates a word file with a specific file name. It saves the word file to a particular path, specified in current folder of the MATLAB. If you do not specify the file name to the word file then MATLAB creates a file named as DIARY in the current folder. DIARY command makes the word file to hold the output data. 'Diary('filename')' writes a copy of all subsequent keyboard inputs and the resulting output to the named file where filename is the full path name or file name in the current MATLAB folder but it does not hold the figure result.

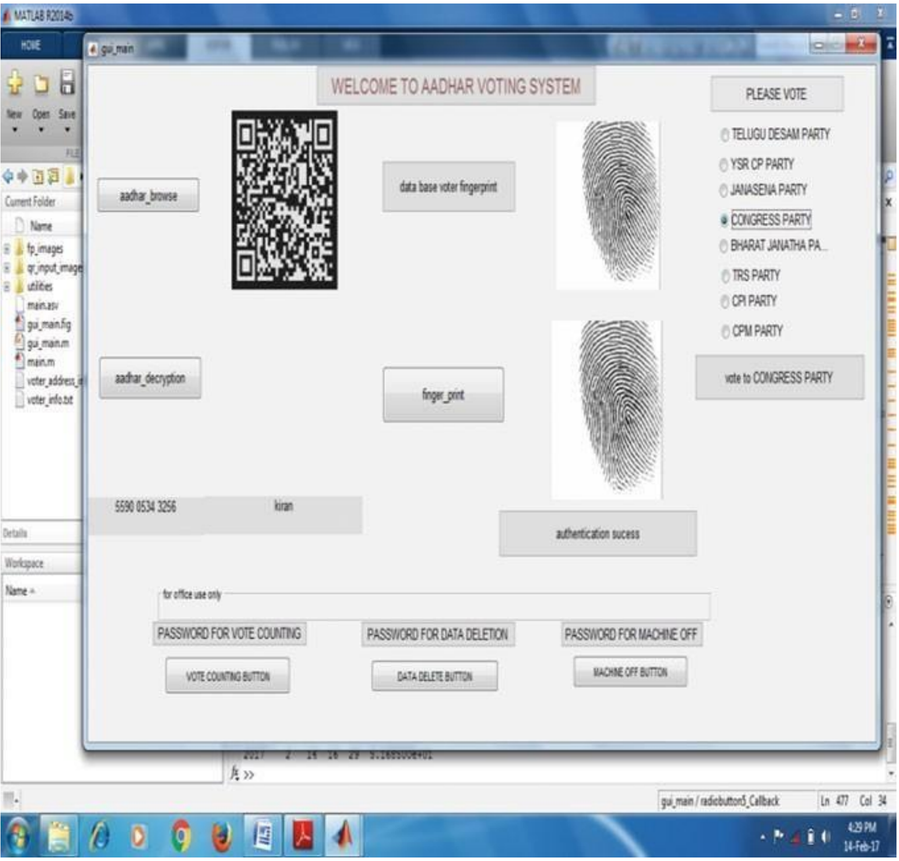
Authentication

Authentication is a very important tool to every application. There are several methods existing to provide the authentication. This paper provides the authentication through the password. This password system is used to keep the machine ON, generate the voting information files, delete the voting information file, and switch the machine OFF.

Results

The machine will be activated through the specific password. If password is correct, it will show "WELCOME TO THE AADHAR
VOTING SYSTEM" and allows the voter to vote. The machine will ask for Aadhaar card and scans it to generate the QR code.

Machine performs QR decoding operation and shows the Aadhaar number. Aadhaar number will be checked with database and will generate the citizen fingerprint. It asks the runtime fingerprint and compares



5590 0534 3256 kiran

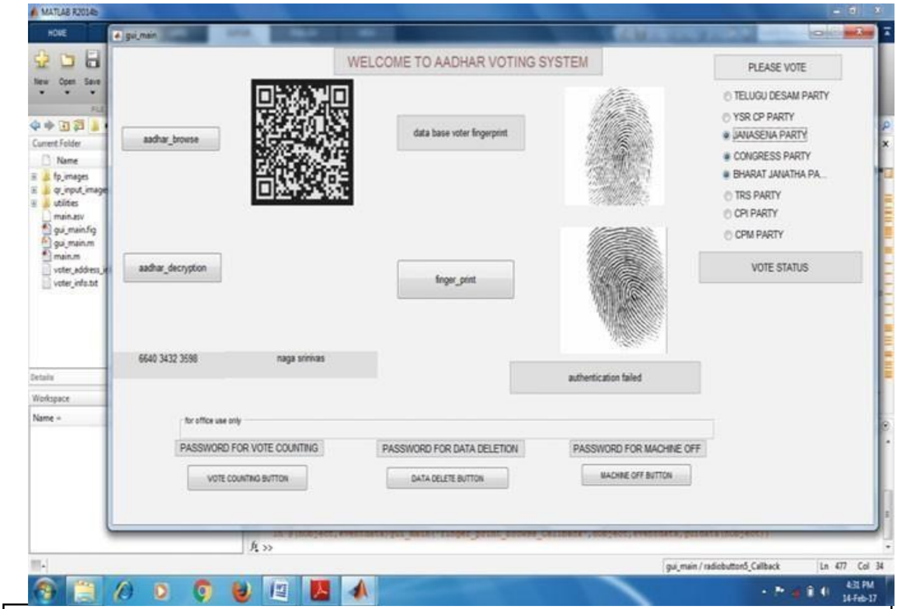
authentication sucess

vote to CONGRESS PARTY

Fig. 12 Voting success

wi

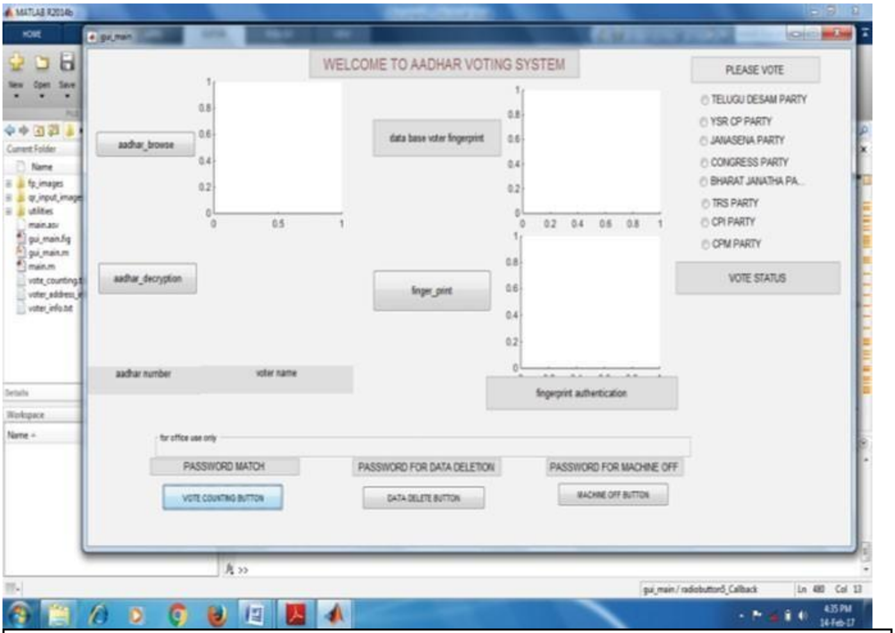
fingerprint. If it matches then it will show “AUTHENTICATION SUCCESS” and allows the voter to vote. After voting it shows the status is shown in Fig. 12. When the runtime fingerprint does not match with the database fingerprint, then it shows the “AUTHENTICATION FAILED” and does not allow for voting. Even if voted, it does not show the vote status. Result is shown in Fig.



6640 3432 3598 naga srinivas

authentication failed

Fig. 13 Voting Failure



aadhar number voter name

fingerprint authentication

PASSWORD MATCH

Fig. 14 Voting file generation

Conclusion

In this paper, it is effectively designed the QR decoding procedure and developed fingerprint matching process to identify the authorized voter to allow for voting. This paper also developed the method to generate the voting files through password which increases reliability and transparency.

References

D. Ashok Kumar and T. Ummal Sariba Begum, "Electronic Voting Machine—A Review" Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21–23, 2012

Jeng-An Lin and Chiou-Shann Fuh, "2D Barcode Image Decoding" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 848276, 10 pages

Sangram Bana and Dr. Davinder Kaur, "Fingerprint Recognition using Image Segmentation" Sangram Bana, et al./ (ijaest) international journal of advanced engineering sciences and technologies vol no. 5, issue no. 1, 012–023

L. F. F. Belussi and N. S. T. Hirata, "Fast component-based QR code detection in arbitrarily acquired images," Journal of Mathematical Imaging and Vision, vol. 45, no. 3, pp. 277–292, 2013

L. F. F. Belussi and N. S. T. Hirata, "Fast QR code detection in arbitrarily acquired images," in Proceedings of the Conference on Graphics, Patterns and Images (SIBGRAPI '11), pp. 281–288, Macei´o, Brazil, August 2011

E. Ohbuchi, H. Hanaizumi, and

L. A. Hock, "Barcode readers using the camera device in mobile phones," in Proceedings of the International Conference on Cyberworlds (CW'04), pp. 260–265,Tokyo, Japan, November 2004

Y. Liu, J. Yang, and M. Liu, "Recognition of QR Code with mobile phones," in Proceedings of the Chinese Control and Decision Conference (CCDC '08), pp. 203–206, Yantai, China, July 2008

Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain & Salil Prabhakar Fingerprint Recognition, Paper by WUZHILI (Department of ComputerScience & Engineering, Hong Kong Baptist University) 2002