SECURE E-VOTING SYSTEM

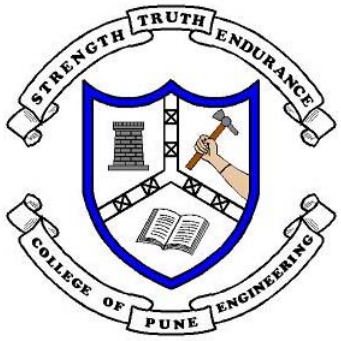
A project report submitted in partial fulfillment of
the requirements for

SE miniproject

by

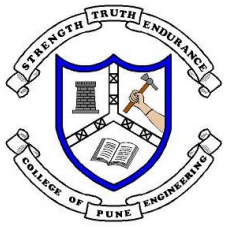
Utkarshbhanu Andurkar, Shivam Marathe
(MIS No. 111708073, 111708035)

Under the guidance of
Mr. Shirish Gosavi



Computer Engg. and Information Technology
COLLEGE OF ENGINEERING–PUNE

CERTIFICATE



This is to certify that the report, entitled **"Secure E-Voting System"** submitted by **Mr. Shivam Marathe (MIS No.111708035)** and **Mr. Utkarshbhanu Andurkar (MIS No. 111708073)**, in partial fulfilment of requirement for the Software Engineering Miniproject at College of Engineering, Pune, affiliated to Savitribai Phule Pune University is a bonafide record of the work carried out by them under the supervision and guidance of Mr. Shirish Gosavi.

Mr. Shirish Gosavi
Guide
Department of Computer Engg. and
Information Technology
College of Engineering, Pune.

Dr. Vahida Attar
Head
Department of Computer Engg. and
Information Techonology,
College of Engineering,
Pune-411 005.

Dr. B. B. Ahuja
Director
College of Engineering
Pune - 411 005.

Declaration

We declare that the report, titled **"Secure E-Voting System"**, submitted by us for the partial fulfillment of Software Engineering miniproject is the record of work carried out by us under the guidance of **Mr. Shirish Gosavi** and has not formed the basis for the award of any degree, diploma, associate-ship, fellowship, title in this or other university or other institution of higher learning.

We further declare that the material obtained from other sources has been duly acknowledged in the thesis.

Shivam Marathe **Utkarshbhanu Andurkar**

Date :

Place : Pune

CERTIFICATE OF THE GUIDE

This is to certify that the work incorporated in this report, titled **"Secure E-Voting System"**, submitted by **Mr. Shivam Marathe (MIS No.111708035) and Mr. Utkarshbhanu Andurkar (MIS No. 111708073)**, is carried out by the candidates under my supervision and guidance. Any such material that has been obtained from other sources has been duly acknowledged in this report.

Mr. Shirish Gosavi
Guide
Department of Computer Engg. and
Information Technology.
College of Engineering, Pune.

Date :
Place: Pune

Abstract

This project aims to develop a secure e-voting system to create any-time anywhere voting possible. This is a web based application. The concern of trust deficit of people in online voting is addressed by providing security and confidentiality through Steganography and Visual Cryptography. Voter's privacy and individual verifiability is at heart of our project. Learning to use this application is made easy by integrating necessary tutorials and FAQs with the web application.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Voting is the basis of any democracy. To keep democracy healthy, voting process must be secure and reliable. With traditional voting system it is not possible to vote from anywhere at convenient time. You have to physically go to voting centre, wait in queue, and then finally cast your vote. There is lack of vote-cast verifiability which cause loss of trust of voters. This unattractive, lengthy, process causes low voter turnout. Today is the age of Internet. Many of the things like payments, businesses are going online. So why not make voting system go online? With online voting system, voting will be much easy. People can vote from wherever they are. The process will be fast too as there will be no need to wait in queue for your turn. This will encourage voters to participate in large numbers. Traditional voting systems are also costlier than e-voting. Voting using ballot-paper or using EVM machine also has inherent cost of physical security included. In using these systems, human resource is used extensively. Also due to participation of human there is a chance of mistakes occurring during vote tallying. There are many solutions already proposed which tries to create a secure online voting system. E-voting system that we are proposing will help in cutting the election cost. As all things are automated, chances of any mistake are negligible. Further we are going to use cryptographic and steganographic methods to make voting system secure and reliable. Privacy of voter and his vote are given utmost preference. Our system also focuses on voter-verifiability through use of vote acknowledgement. We will also work on scalability of this system to become compatible with user needs. Our system is a slight modification of online voting system proposed by [1]

1.1 Aims and Objectives

- Create a full stack web application
- Make anytime anywhere voting possible.
- Provide service to create, conduct election and declare the result.
- Make the user interface of website attractive and elegant.
- Maintaining the faith of voters in voting process while making voting process convenient.

1.2 Assumptions

- User of this system has stable Internet connection.
- Administrator has all the credentials for the election and knows it's procedure.
- Every user of this system has Aadhaar No. and E-Mail address
- Users of the system knows basic English language.
- Users of the system are able to operate computer and use Internet.

1.3 Summary of main Results

This is system provided an easy to use and secure way to conduct the elections. The system responds very quickly to inputs under normal condition of operation. The elegant user interface and learning material that it provides is impressive. The system is designed to be used for only institutional elections. The scalability of the system is still a concern. This system is still hard to use for less educated public. This system cannot match the simplicity of EVM used today in India.

1.4 Organization of Report

The organization of the report is as follows.

Chapter 2 is dedicated to survey of works related to Secure E-Vote System. In this chapter various online voting system are examined and compared with E-Vote System

Chapter 3 consists of various UML diagrams used to design, model and analyse Secure E-Vote System

Chapter 4 consists of implementation details of Secure E-Vote System and Test Results

Chapter 5 concludes the project report and some suggestions regarding future work are noted.

Chapter 2

Related Works

To better understand the previous works, we studied five end to end voting systems, namely Helious open source web-based voting system, Scantegrity II optical voting system, Pret a Voter, RIES voting system and Online Voting System Based on Image Steganography and Visual Cryptography to better understand the features of the online voting systems [1] - [5].

Helios is open-source web-based voting system that offers verifiable online elections for anyone. It was designed to ensure a clean election setting with ballot secrecy and election integrity.

Scantegrity II is a practical enhancement for optical scan voting systems, which achieve increased election integrity through a novel use of confirmation codes printed on ballors in invisible inks.

The development of Pret a Voter was initially motivatred by Chaum's work of implementing visual cryptography approach proposed by Naor and Shamir in an election in 2004 to offer vote verifiability. It implements the same concept as Chaum's secret ballot receipt scheme to provide more accurate and faster tallying process, to cut unnecessary election cost and to increase voter participation.Pret a Voter offers assurance from it's election auditability.

RIES is a voting system that implements multiple types of technologies. RIES allows eligible voters to cast their vote in two forms, either by mail or electronically. Based on this key feature RIES allows it's it's user to independently verify the election result. They were used in actual governmental and organisational election, two of which are used for elections in educational institutions.

Online Voting System Based on Image Steganography and Visual Cryptography is a online voting system which uses cryptographic techniques for voter verifiability and secure elections. Use of threshold decryption for tallying is introduced in this system All end to end voting systems were designed to fulfil two main objectives

- Individual verifiability
- Universal verifiability

The five voting systems reviewed are equipped with both features. Ironically, the implementation of these features caused the initiation of some known attacks like randomised attack.

We tried to implement Secure E-Vote based on [1]. But There were certain modifications necessary. One of such was In [1] voter receipt was sent to email after voting. This receipt can be used at a tool for vote coercion. We did overcome this drawback by restricting access to vote receipt in ongoing voting session(after voters cast their vote) only. This could possibly prevent misuse of vote-cast receipt.

Chapter 3

Design and Analysis of Secure E-vote System

3.1 Software Requirement Specification

Software Requirements Specification

for

SECURE E-VOTING SYSTEM

Prepared by 1) Shivam Marathe 2) Utkarshbhanu Andurkar

COEP

<01-02-2020>

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

Voting is the basis of any democracy. To keep democracy healthy, voting process must be secure and reliable. With traditional voting system it is not possible to vote from anywhere at convenient time. You have to physically go to voting center, wait in queue, and then finally cast your vote. There is lack of vote-cast verifiability which cause loss of trust of voters. This unattractive, lengthy, process causes low voter turnout.
We can get rid of this issue with the use of online voting system. With online voting system, voting will be much easy. People can vote from wherever they are. The process will be fast too as there will be no need to wait in queue for your turn. This will encourage voters to participate in large numbers.

1.2 Document Conventions

- VC – Visual Cryptography

1.3 Intended Audience and Reading Suggestions

- This Document is meant for teachers, students, organizations willing to use secure e-voting system.

- Begin with overall description section and follow the sequence as given.
  The sequence of documentation is overall description, external interface requirement, system features, other non-functional requirements.

1.4 Product Scope

Product Name – Secure E-Voting System.
Purpose – Making voting anytime anywhere possible.
Objective – Create a secure and reliable yet easy to use online voting system.
Goals –

- Maintain the voting process secure and reliable with the use of VC and steganography.
- Make voting anytime anywhere possible.
- Maintain reusability of code while designing the software.
- Convince organizations to use our software.

This product is developed for voting inside organizations only.

1.5 References

Research Paper:

Title: Online Voting System Based on Image Steganography and Visual Cryptography.
Authors: Lauretha Rura, Biju Issac and Manas Kumar Haldar

2. Overall Description

2.1 Product Perspective

Today voting habits of people are changing. People prefer voting from where they are rather than going to Poll Booths. Our product tries to satisfy this need by creating a voting service which is secure, verifiable, reliable. This service is usable from anywhere.

2.2 Product Functions

- Create Election – Administrator will be able to create an election.
- Add election candidates – Administrator will be able to add candidates for the election.
- Add polling officers – Administrator will be able to add polling officers
- Add eligible voters – Polling officers will add eligible voters
- Authenticate voters – System will authenticate voters using username and password to login.
- Vote – Voters will be able to vote only once through their login.
- Steganographic encryption – Steganographic encryption will be used to transfer vote from browser to e-vote server.
- Visual encryption and decryption will be used to create vote receipt service for verifiability.
- Real time Vote statistics display to administrator
- Results of election will be declared on the day of result using threshold encryption cryptography.

2.3 User Classes and Characteristics

1) Administrator – Admin will use this online software to create election, add polling officers, add candidates, supervise the election, declare the results. They have the highest privilege.
2) Polling officers – Polling officers will add voters for the election, edit voters' information, At the time of result they will give secret keys for threshold decryption. They have medium privilege.
3) Voters – Voters can vote, see candidate's profile, get encrypted receipt of vote. They have lowest privilege.

2.4 Operating Environment

1) This system is designed to operate in web-based environment.
2) Supported by devices like pc, laptops, smartphones, tabs.

2.5 Design and Implementation Constraints

1) Maximum number of users at one time will be limited by resource availability.
2) This system is designed to work within an organization only. Any attempt to use it on large scale may fail.
3) The updates and maintenance of software will not be quick as developers are only 2 students.

2.6 User Documentation

1) A user manual will be provided for this software to explain Graphical UI.

2.7 Assumptions and Dependencies

1) Voter is voting in secure and private environment.
2) User has Internet connectivity.

3. External Interface Requirements

3.1 User Interfaces

1) Graphical User Interface –
    a) It will be based of 8 golden rules of UI design by Ben Shneiderman.
    b) The interface will be interactive and user friendly.

3.2 Hardware Interfaces

Supported Devices – Personal Computers, Laptops, Tabs, Smartphones

3.3 Software Interfaces

Languages – HTML, CSS, Javascript, Python3
Libraries – Bootstrap, PIL

Steganographic Encryption Algorithm –
Inputs – 1) Ballet image with information about vote.
Output – 1) Stegano object
Provides service for encrypting the ballet image before sending to E-Vote server.

Steganographic Decryption Algorithm –
Inputs – 1) Stegano object
Output – 1) Ballet image 2) Information about vote.
Provides service for decrypting the stegano object to create ballet image and information about vote.

Visual Cryptographic encryption –
Inputs – 1) Receipt for vote
Outputs – 1) Share-1 2) Share-2
Provides service to save vote receipt securely in the database.

Visual Cryptographic decryption –
Inputs – 1) 1 Share from user 2) 1 share from system's database
Outputs – 1) Vote receipt
Provides service to generate vote receipt for user verifiability.

3.4 Communications Interfaces

1) High level use of HTTPS protocol.
2) Socket Size (Bandwidth) for 8192 Bytes for receiving and sending data (minimum requirement)

4. System Features

4.1 Create Election:

4.1.1 Description and Priority

i) This feature will be used by Administrator to create election.

ii) Administrator will select day and time duration for election.

iii) Administrator will add polling officers for the election.

iv) Administrator will give secret key to each officer.

vi) This feature has high priority.

4.1.2 Stimulus/Response Sequences

i) Administrator signs up in the system.

ii) Administrator creates election and adds polling officers.

iii) Polling officers receive message with link to register themselves.

4.1.3 Functional Requirements

REQ-1: Registration of administrator.

REQ-2: Administrator must have election credentials (time and date information).

REQ-3: List of polling officers.

REQ-4: Good Internet connectivity for administrator.

REQ-5: Admin's browser is supported by e-vote system.

REQ-6: Polling officers are assigned secret keys.

4.2 Conducting election

4.2.1 Description and Priority

i) This feature will be used by polling officers and voters.

ii) Polling officers registers themselves in the system using the link.

iii) Each polling officer adds list of authentic voters and then voters can register themselves for the election.

iv) Voters can vote securely through their login.

v) Admin and polling officers can track the election statistics.

vi) This feature has high priority.

4.2.2 Stimulus/Response Sequences

i) Polling officers signs up and adds list of voters from their departments.

ii) Voters receive message with link to register.

iii) Voters register in the system.

iv) Voters get login credentials.

v) Voters login in the system at election day.

vi) Voters vote according to their choice.

vii) Vote is encrypted with steganography and sent to server.

viii) Vote is decrypted and counted for respective candidate.

ix) Receipt of vote cast is generated using visual cryptography.

x) One share is given to voter and other is kept in the system.

xi) Voter can upload his share to see vote cast receipt.

4.2.3 Functional Requirements

REQ-1: Registration of polling officers.
REQ-2: Registration of voter.
REQ-3: Voters logging in and voting privately.
REQ-4: Vote encrypted with steganography and sent to server.
REQ-5: Vote decryption and counting.
REQ-6: Use of visual cryptography to create shares from vote cast receipt.
REQ-7: Voter getting share and using it to generate vote cast receipt.

4.3 Declaration of results:

4.3.1 Description and Priority

i) This feature will be used by Administrator and polling officers to declare results.

ii) Voters can see the results through this feature once results are declared.

iii) This feature has high priority.

4.2.2 Stimulus/Response Sequences

i) Administrator collects secret keys from polling officers.

ii) Administrator signs up in the system.

iii) Administrator adds all secret keys in the system.

iv) Using threshold decryption results are declared.

4.1.3 Functional Requirements

REQ-1: Collecting Secret keys from polling officers.

REQ-2: Use of threshold decryption.

REQ-3: Only Voters and election officers can see the result.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

1) The system should be highly responsive as it is web based.
2) Vote receipt generation should be fast (within 3 seconds).

5.2 Safety Requirements

1) Voters private information should be protected.
2) Information about vote (who gave vote to whom) should not be stored.

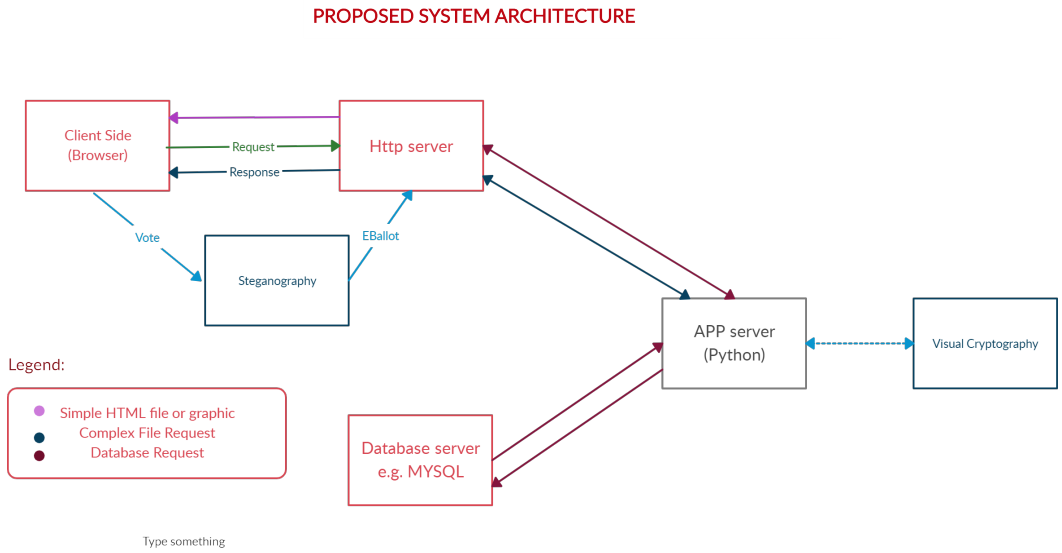


Figure 3.1: Proposed system architecture of Secure E-Vote System

3.2 Proposed System Architecture

As the figure 3.1 shows

- Browser interacts with http server to provide necessary functions.
- An e-ballot is generated for voter using steganography to cast his vote.
- This vote is counted at application server using database server and further encrypted using visual cryptography.
- One share generated from visual cryptography is given to the user and other share is kept in the database server.
- User can upload his share to create vote cast receipt. (The receipt does not contain information about to whom the vote was given)

3.3 UML Design

3.3.1 ER Diagram

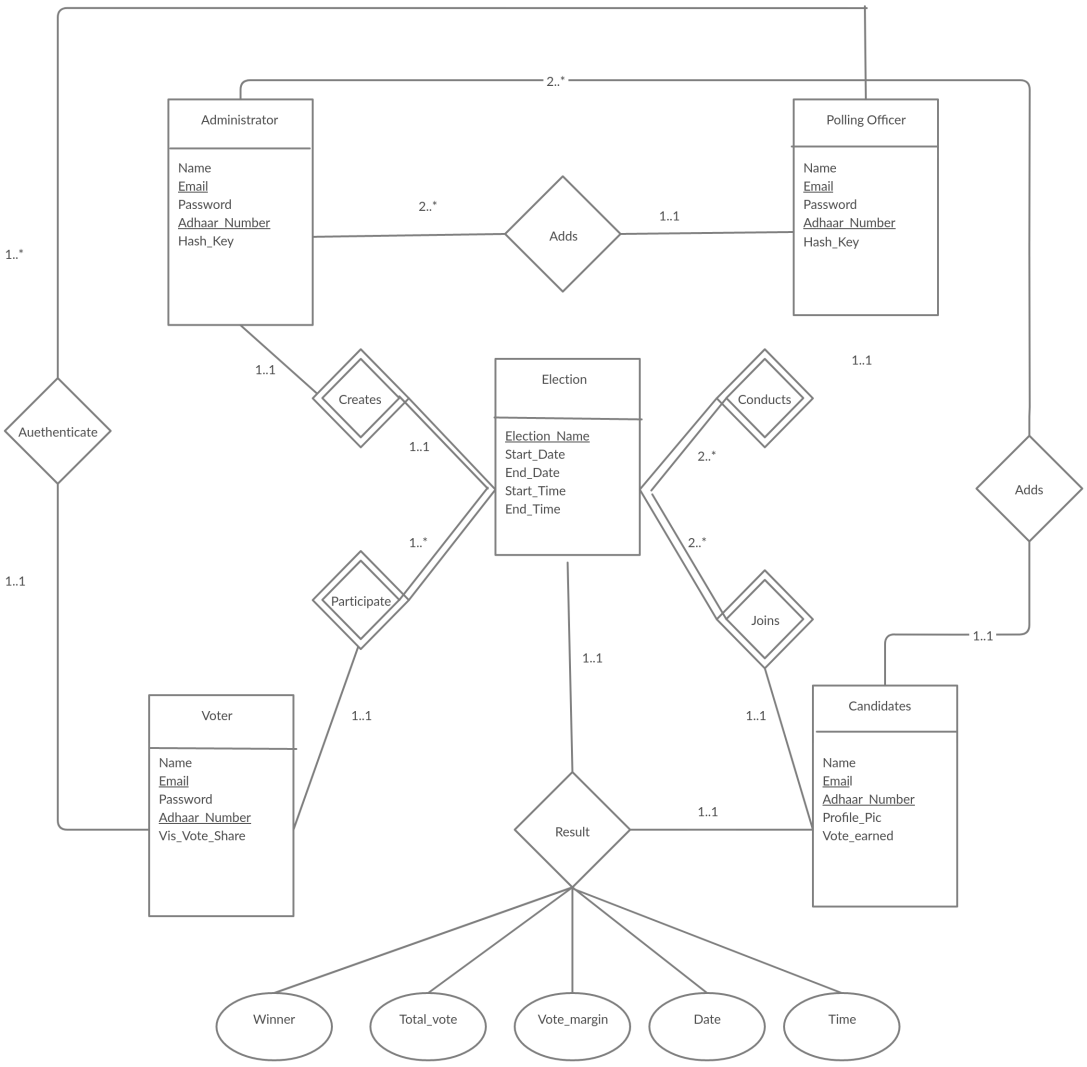


Figure 3.2: Entity Relationship Diagram for Secure E-Vote System

3.3.2 Use Case Diagram

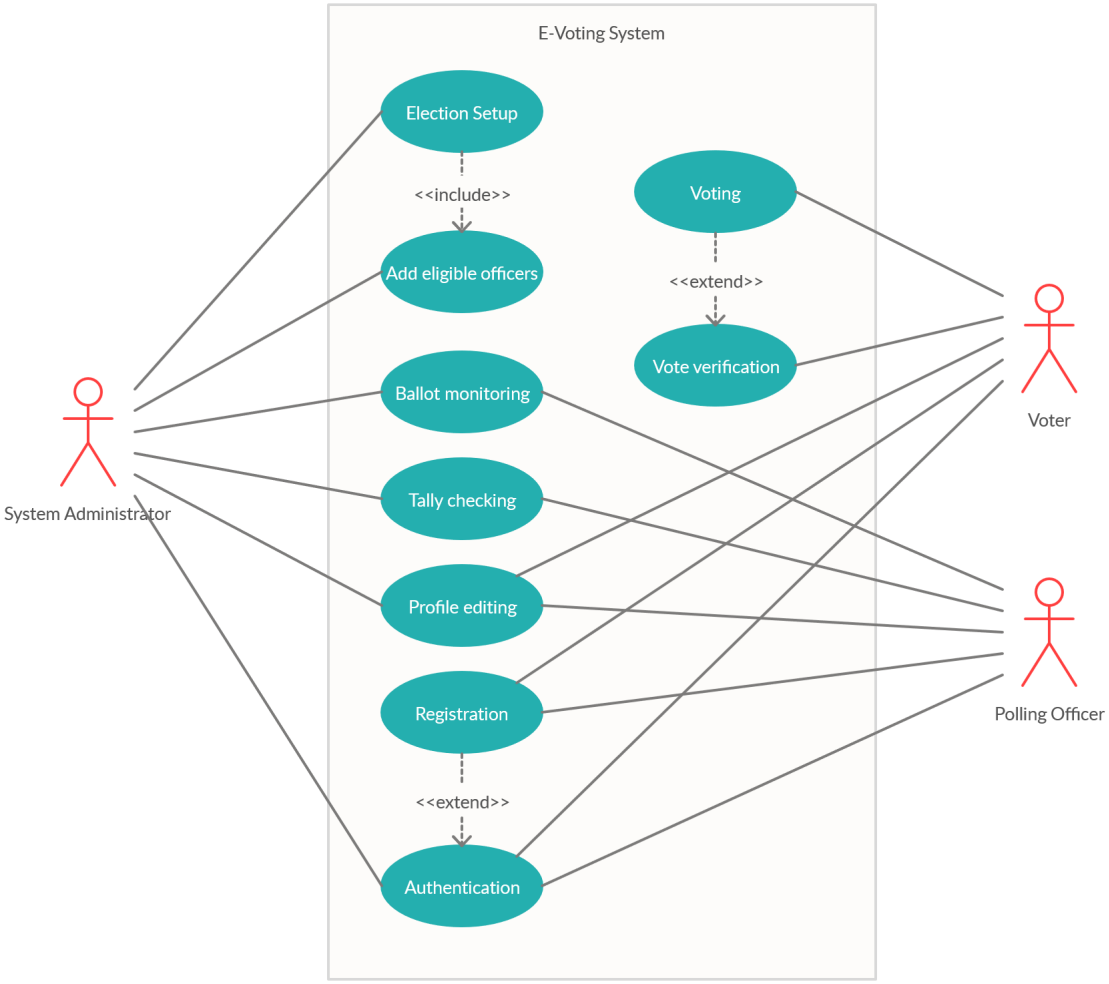


Figure 3.3: Use Case Diagram for Secure E-Vote System

3.3.3 Class Diagram

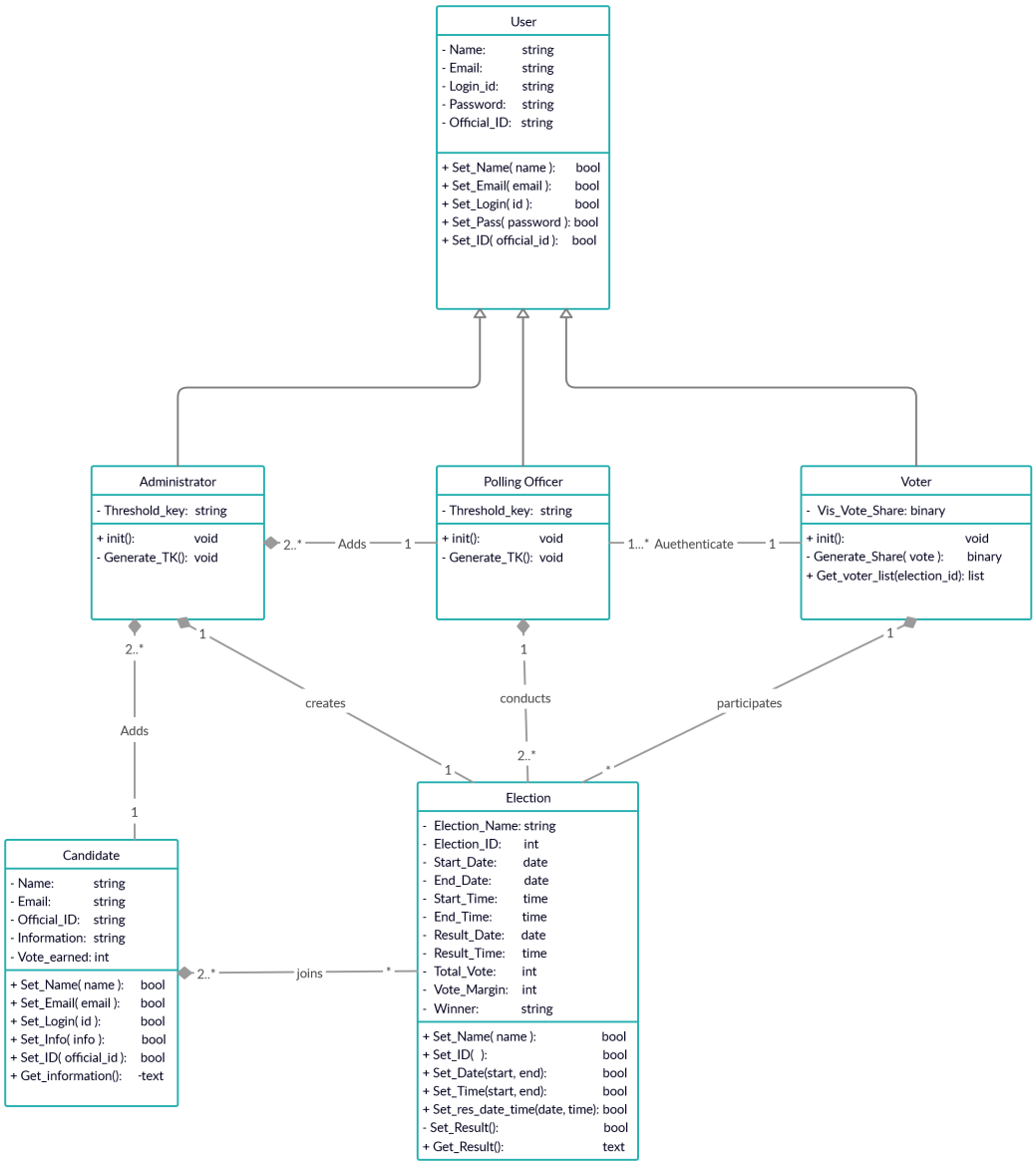


Figure 3.4: Class Diagram for Secure E-Vote System

3.3.4 State Diagram

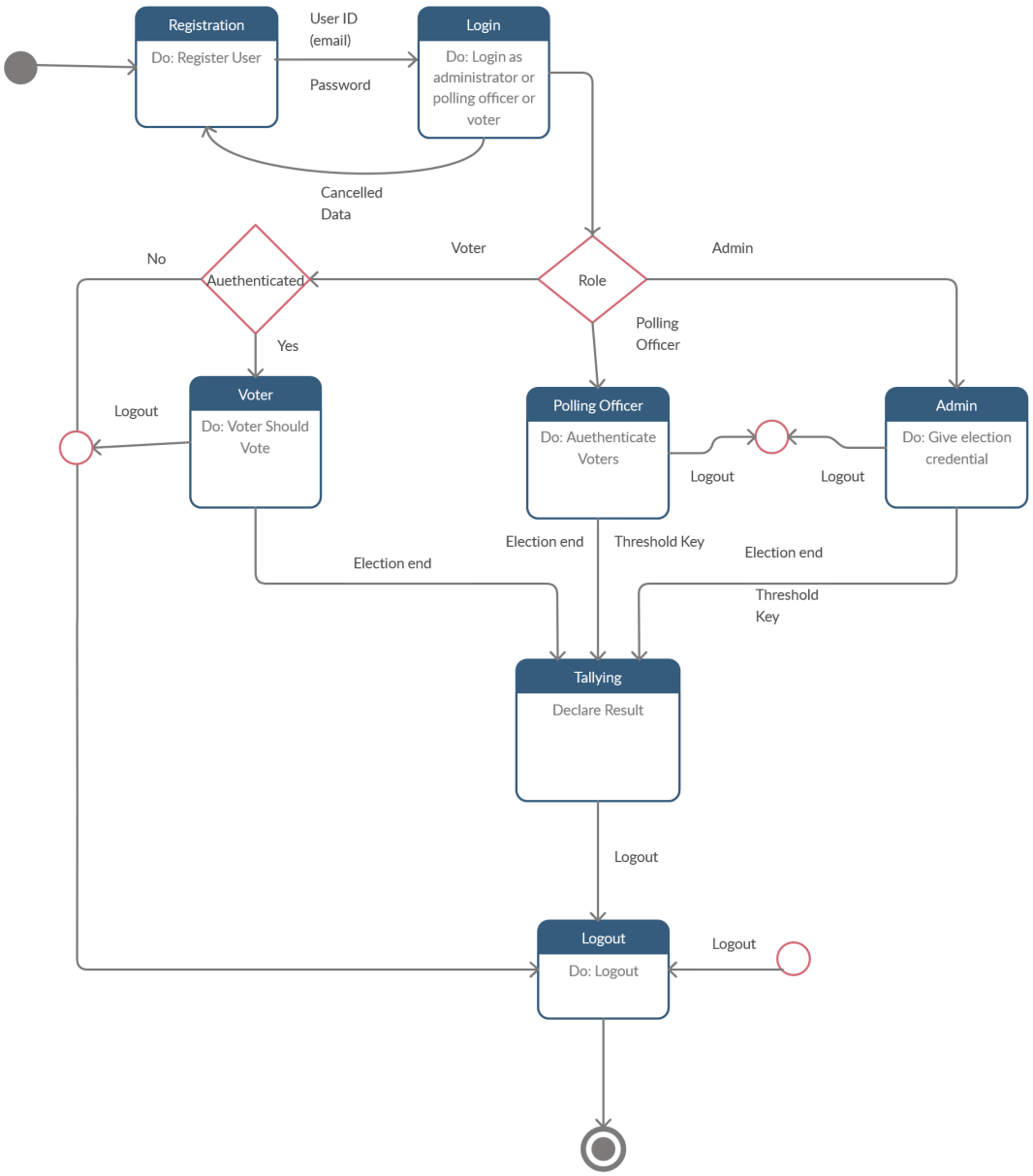


Figure 3.5: State Diagram of Secure E-Vote

3.3.5 Data Flow Diagrams

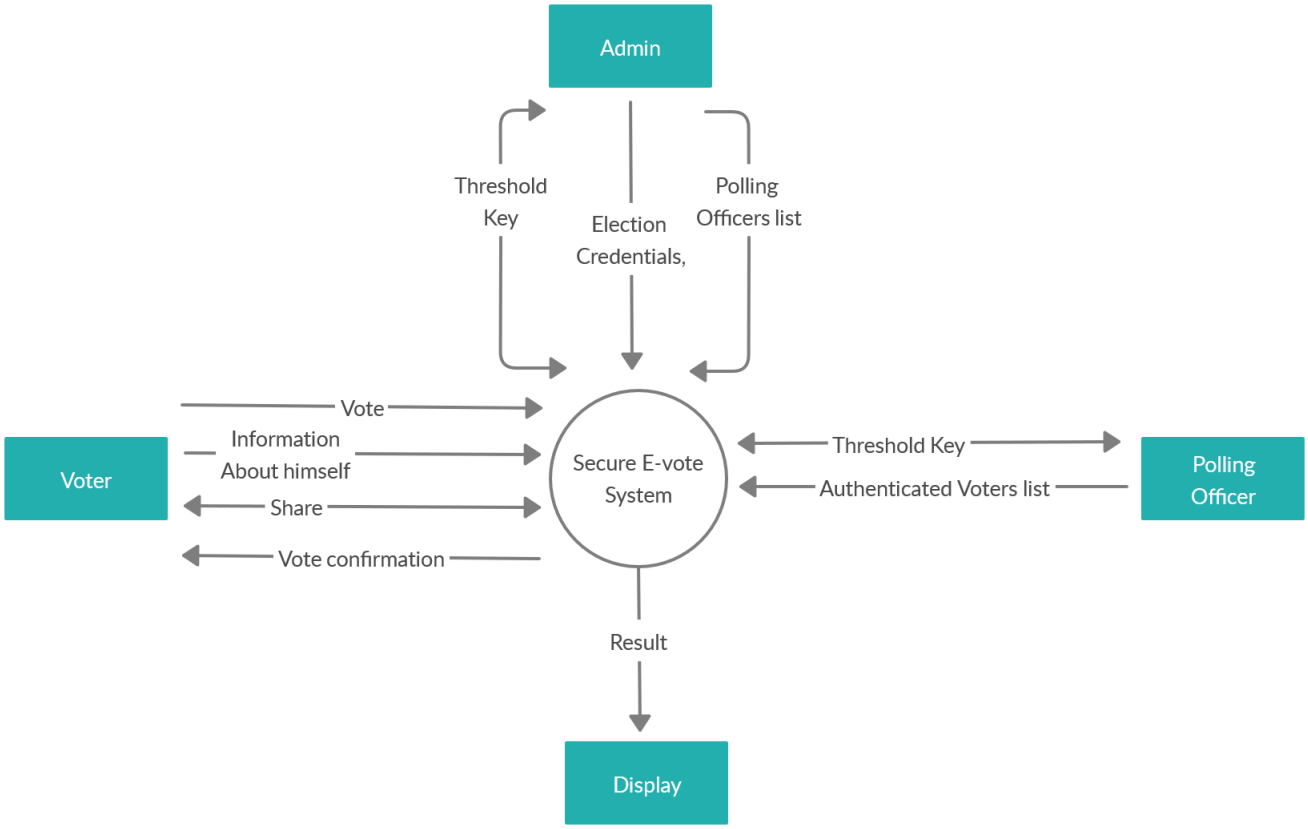


Figure 3.6: Context diagram for Secure E-Vote system

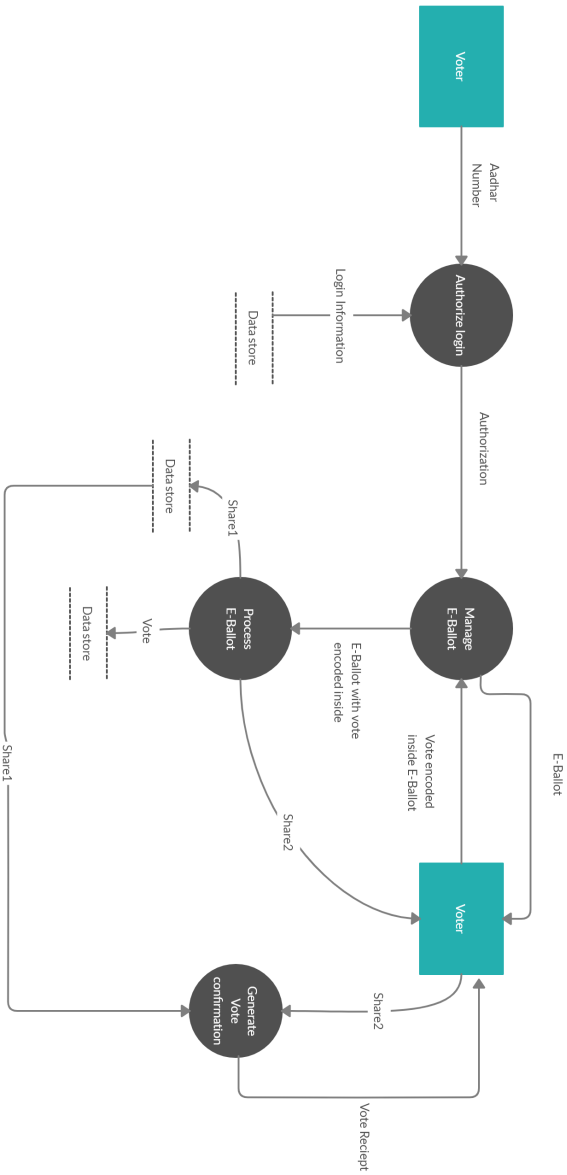


Figure 3.7: Level 1 DFD for voting

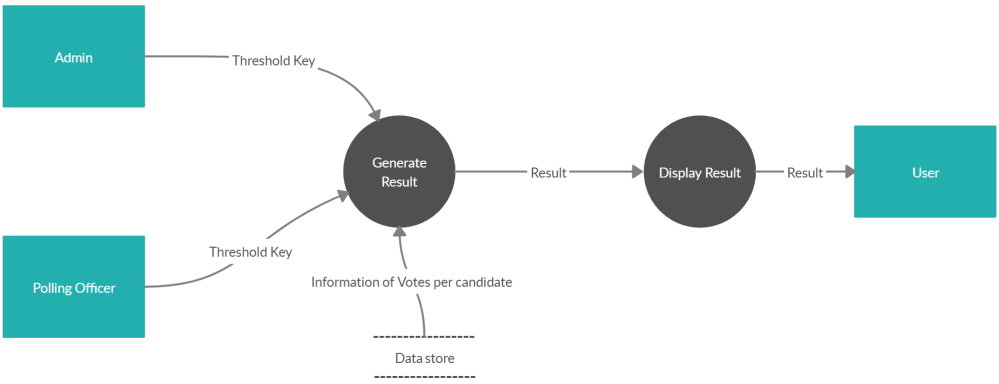


Figure 3.8: Level 1 DFD for result declaration

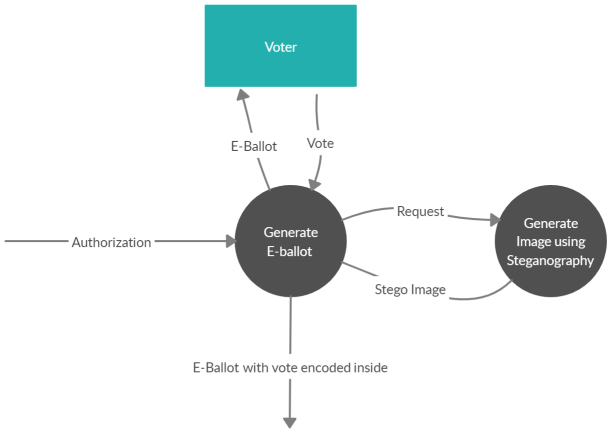


Figure 3.9: Level 2 DFD for Generate E-Ballot Process

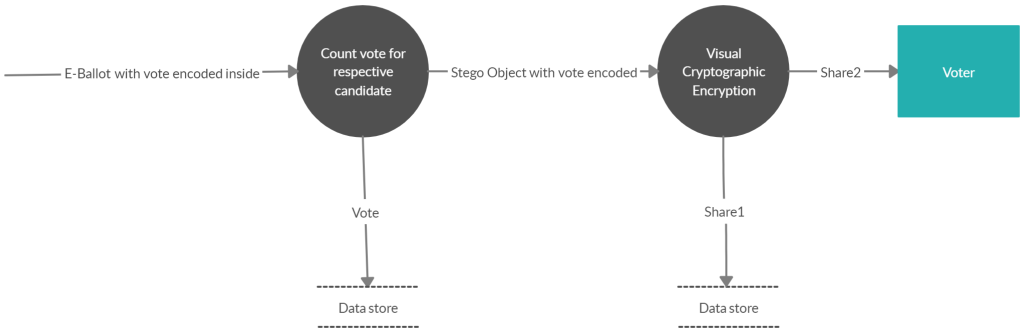


Figure 3.10: Level 2 DFD for E-Ballot Processing

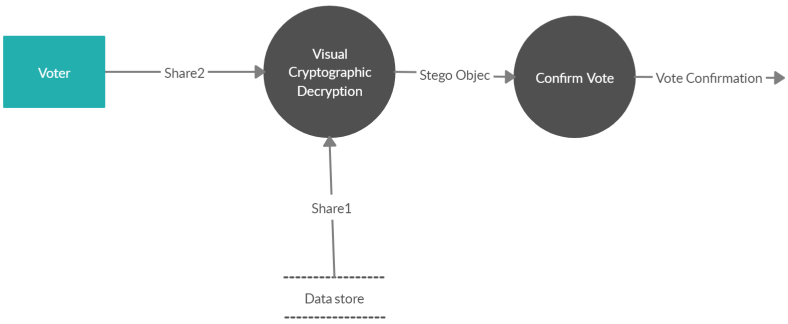


Figure 3.11: Level 2 DFD for Generate Vote Confirmation Process

3.3.6 Activity Diagram

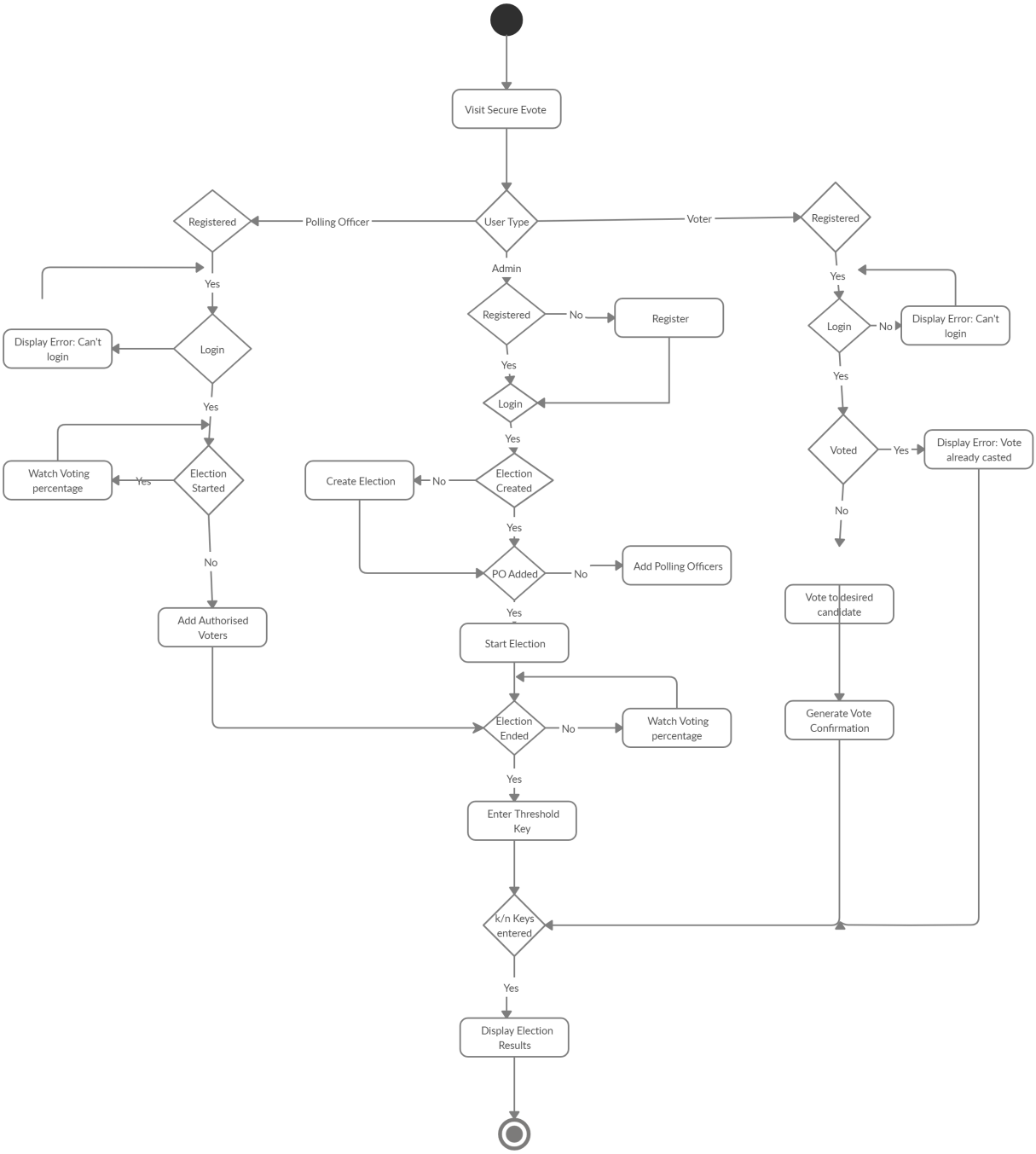


Figure 3.12: Activity Diagram for Secure E-Vote System

3.3.7 Sequence Diagrams

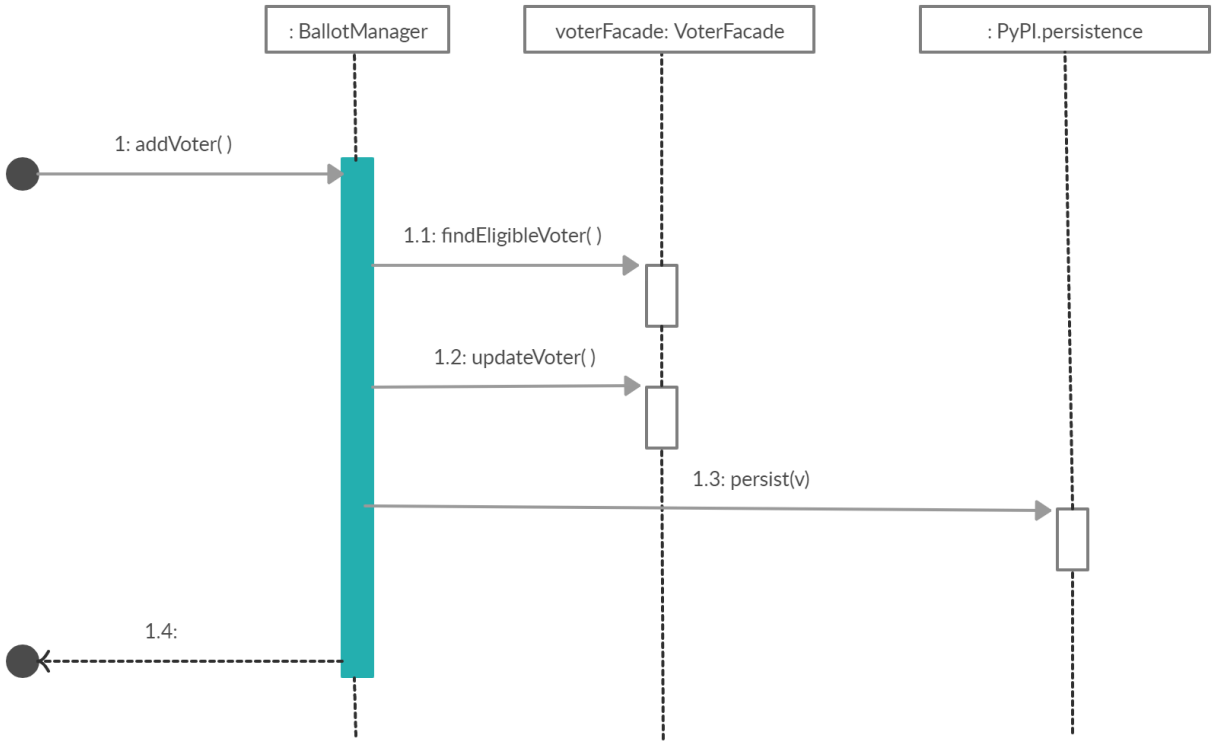


Figure 3.13: Sequence diagram of voter registration process

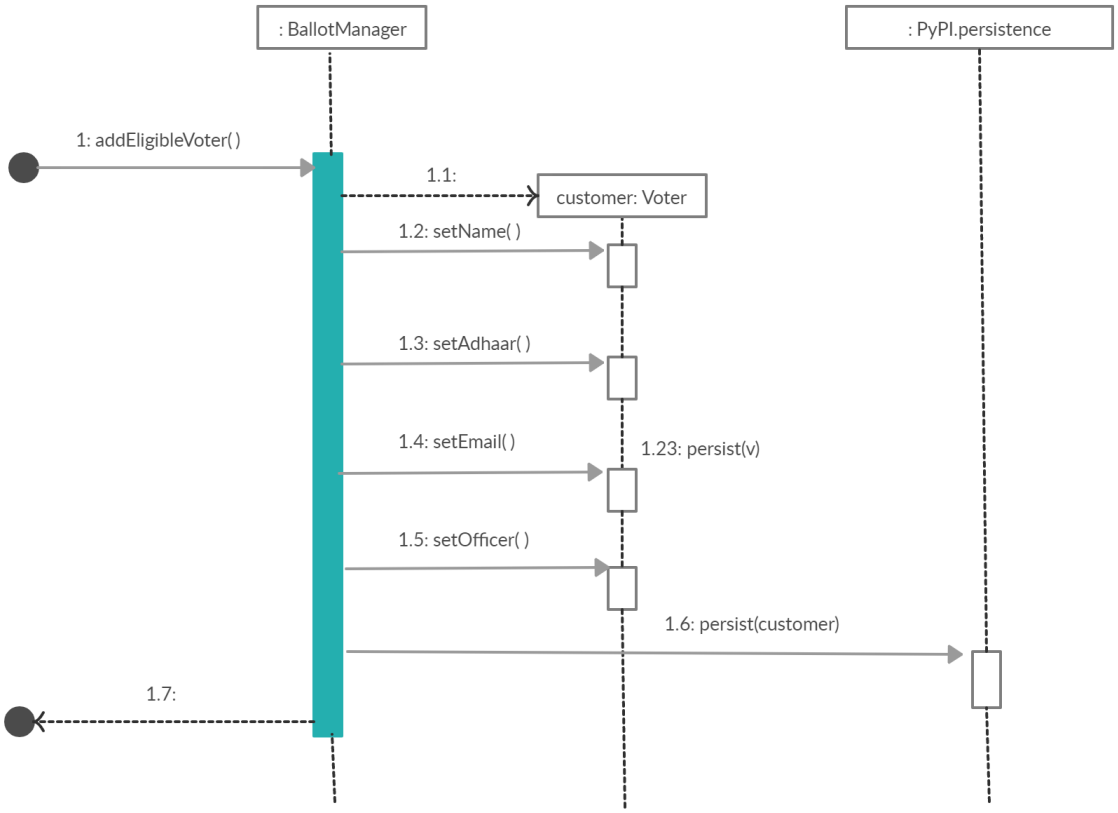


Figure 3.14: Sequence diagram of addEligible Voter() function

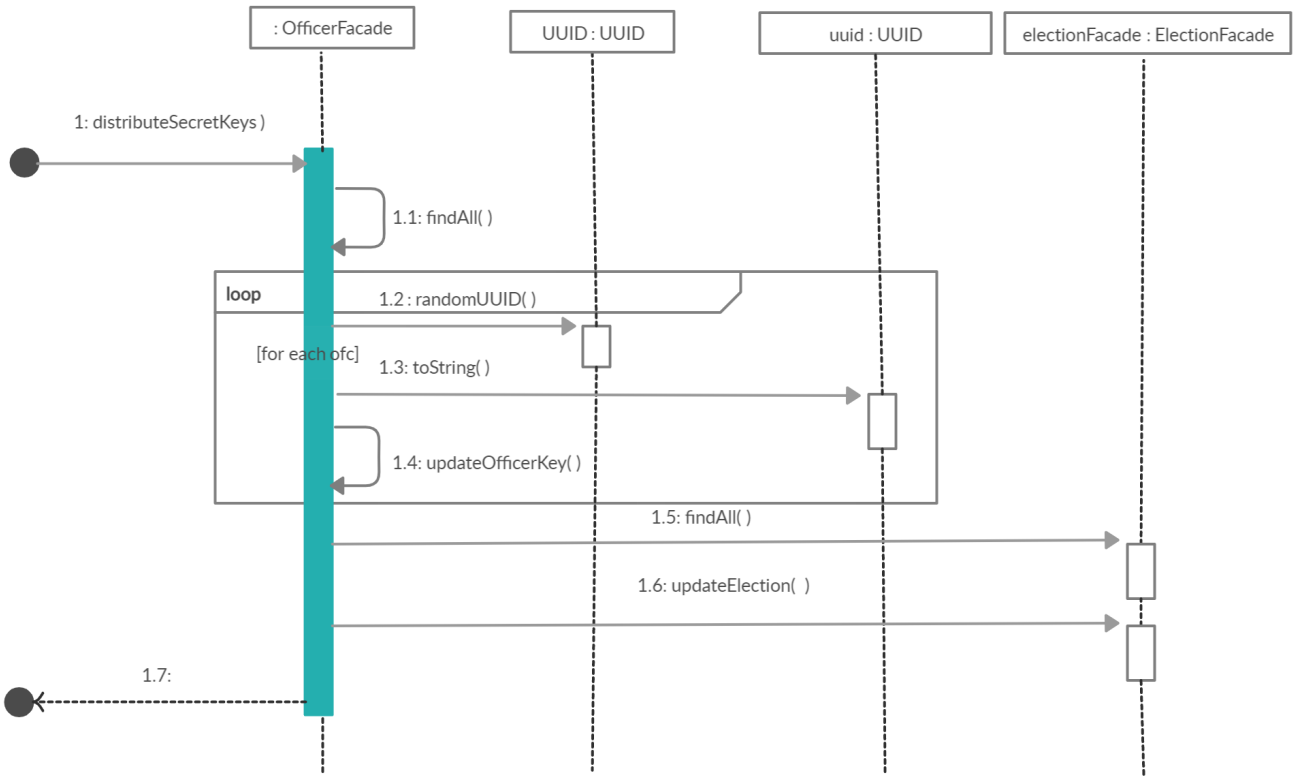


Figure 3.15: Sequence diagram of secret key distribution process by system administrator

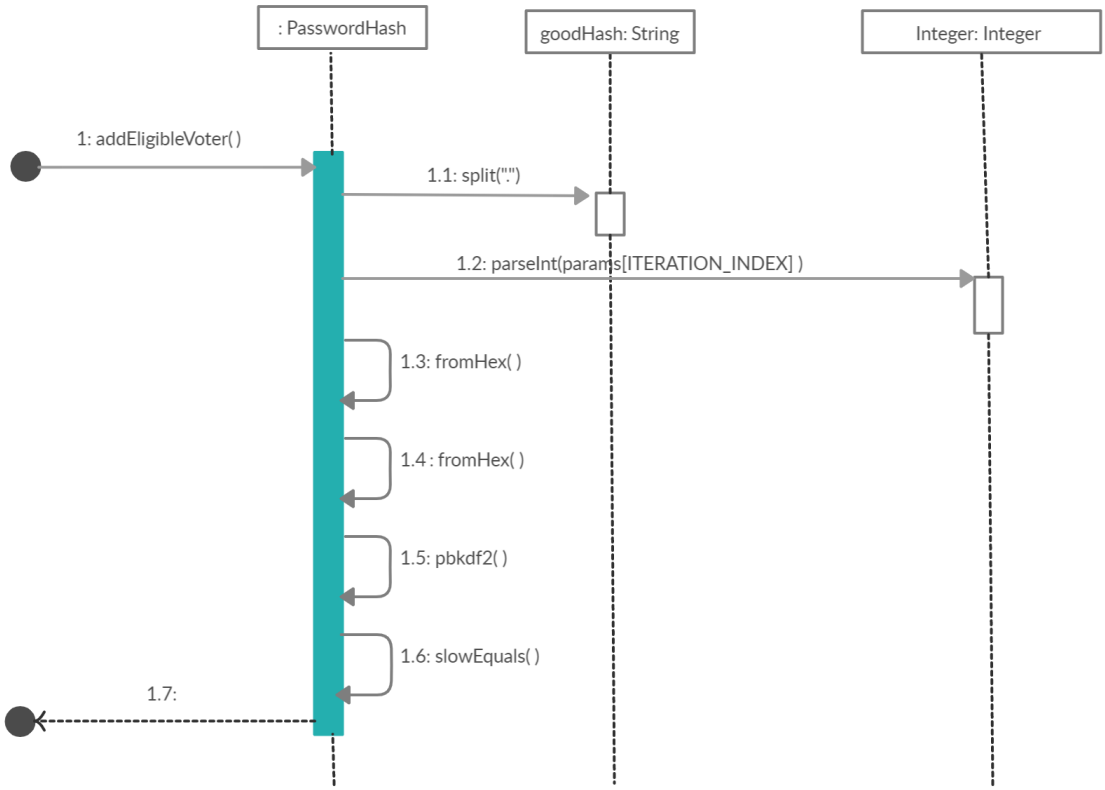


Figure 3.16: Sequence diagram of user authentication process

Chapter 4

Implementation details and Testing results

4.1 Implementation Details

This section describes the implementation details of **Secure E-Vote System**

- Static features of front end of Secure E-Vote System is implemented using HTML, CSS(with bootstrap).
- Dynamic features of the system are implemented with Javascript using JQuery.
- Backend is implemented using Python with Django framework.
  Code for Steganography and Visual Cryptography are written in python.
- For this system Apache server and SQLite database are used.
- This website is supported by Javascript supporting browsers like Chrome, Firefox etc.
- This website is hosted on pythonanywhere.com as shitkarsh.pythonanywhere.com

4.2 Testing Summary

This section gives the summary for testing of **Secure E-Vote System**

4.2.1 Application Overview

Secure E-Vote System is a web-based voting application. Conduction of various institutional elections can be done using online facilities. Administrator can conduct the election with the help of Polling Officers. The security of the system is insured by using Steganography and Visual Cryptography. A report for the election can also be generated at the end of election.

4.2.2 Testing Scope

1. **In Scope**: Functional Testing for the following are in Scope of Testing
    - Steganography Module
    - Visual Cryptography Module
    - Integration Test
2. **Out of Scope**: Performance Testing was not done for this application, seperate Testing of utilized libraries is not done.

4.2.3 Functional Testing Results

1. Steganography Module
    - **Input**:
        (a) Ballot Image
        (b) Vote
    - **Expected Output**:
        (a) Ballot Image encoded with vote
    - **Observed Output**:
        (a) Ballot Image encoded with vote
    - **Test Status**: Passed
2. Visual Cryptographic Encryption
    - **Input**:
        (a) Ballot Image encoded with vote
    - **Observed Output**:
        (a) Two image shares
    - **Observed Output**:
        (a) Two image shares
    - **Test Status**: Passed
3. Visual Cryptographic Decryption
    - **Input**:
        (a) Two image shares generated by Visual Cryptographic encryption
    - **Expected Output**:
        (a) Ballot image with vote encoded
    - **Observed Output**:
        (a) Ballot image with vote encoded
    - **Test Status**: Passed

4.2.4 Integration Testing

Integration testing of the system is done after connecting all the modules by hosting a test election on the system. The working of the system is normal and as expected. System passed the Integration test.

4.2.5 Conclusion

Secure E-Vote System passed all tests performed.

Chapter 5

Conclusion and Future Scope

5.1 Conclusion

- Secure E-Vote system shows that it is possible to provide a secure voting service using Internet.

- Secure E-Vote has potential to reduce expenses for elections. This include both money and human resource.

- Fair and limited use of resources by this system proves it's efficiency.

- Secure E-Vote System provided elegant yet easy to use voting service. Tutorials and FAQs provided with the system tries to answers most queries asked by users. Result of "User acceptance" testing support these conclusions.

- The scope of this system is limited to elections within an organisation. Using this system in large elections like elections in state/country may cause scalability issues.

5.1.1 Issues

- This system assumes that it's users have sufficient knowledge of operating computers.
- Although this assumption is true for most organisations it fails in some cases, e.g. elections in organisation like "Krushi Utpanna Bajar Samiti" which involves less educated farmers.
- For these exceptions, use of traditional methods for elections will perform better than Secure E-Vote System.
- Building trust about this system is major challenge in today's environment.

5.1.2 Future Scope

We are thinking to use Blockchain technology to make database more secure and reliable. The scalability of secure E-Vote is also a major concern. We would like to improve scalability of this system so that it can be used in large scale elections. To improve scalability we are thinking of using client side computation.

Appendix I

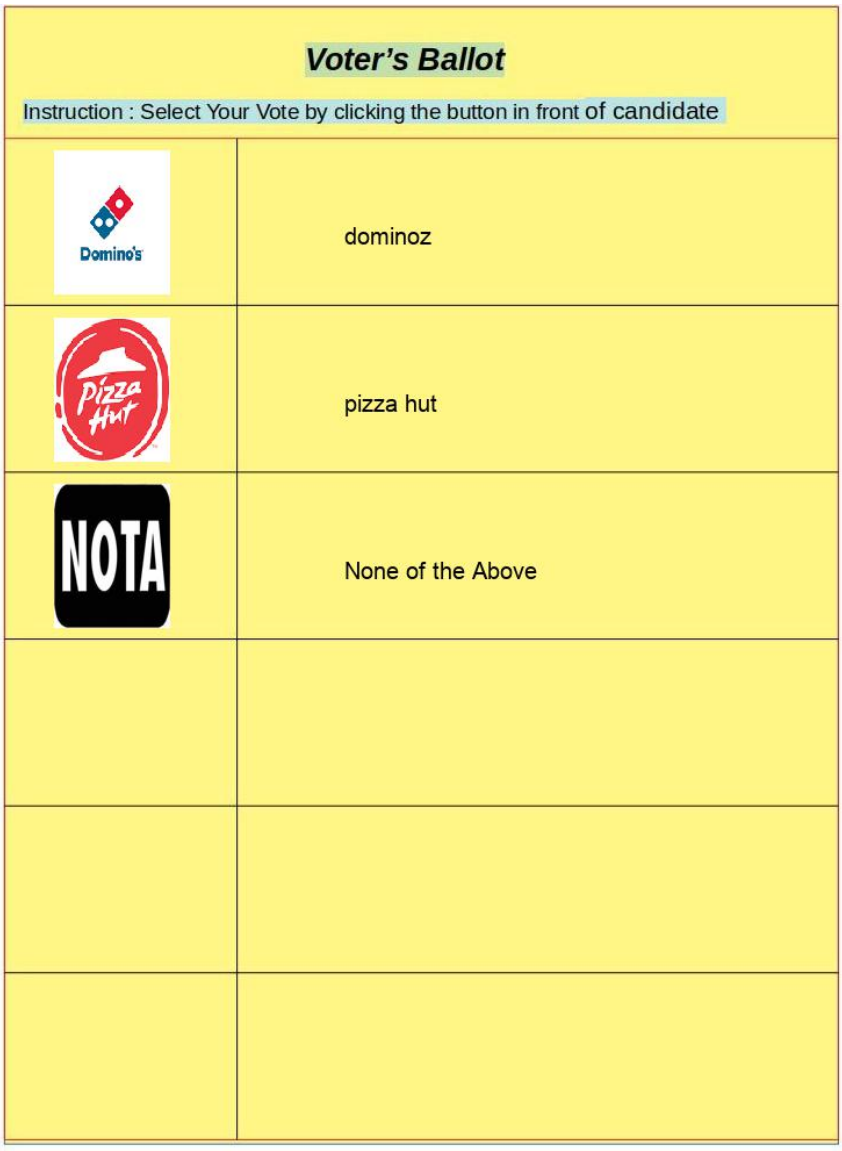


Figure 1: Ballot image encoded with vote generated by Steganography in Test election

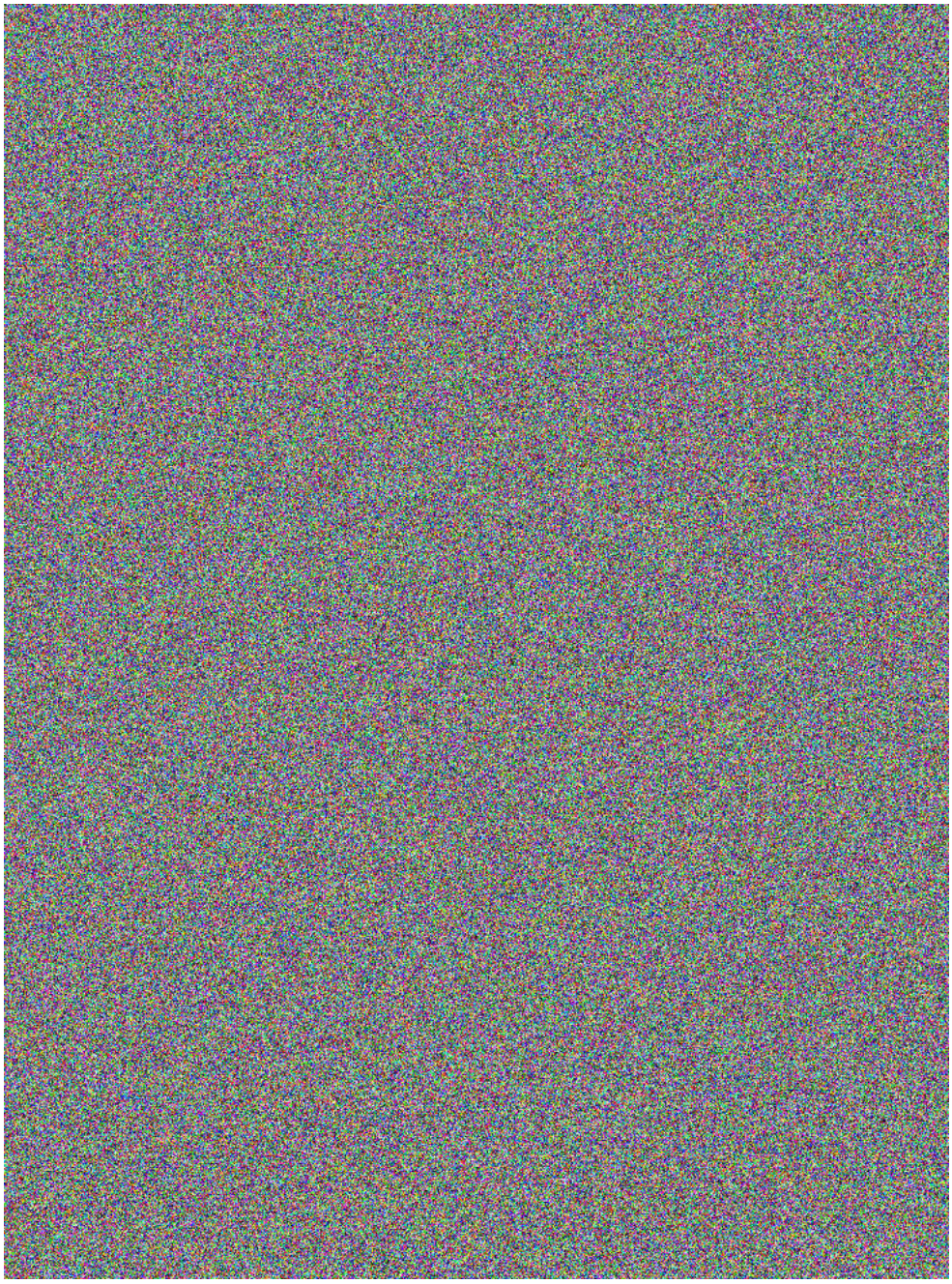


Figure 2: Share generated after Visual Cryptographic Encryption

References

[1] Lauretha Rura, Biju Issac and Manas Kumar Haldar. *Online Voting System Based on Image Steganography and Visual Cryptography*. [Journal of Computing and Information Technology, vol.25, No. 1, March 2017, doi: 10.20532/cit.2017.1003224].

[2] B. Adida, *et al., "Helious: Web-based Open-Audit Voting",* [in Proceedings of the 17th Conference on Security Symposium USENIX Association, Berkley, USA, pp. 335-348, 2008].

[3] E. Hubbers *et al., "RIES-Internet Voting in Action",* [in Proceedings of the 29th Annual International Computer Software and Application Conference, IEEE Computer Society, Washington DC, USA, pp.417-424,2005. http://dx.doi.org/10.1109/COMPSAC.2005.132].

[4] D Chaum *et al., "Scantegrity II: End-To-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes",* [in Proceedings of the Conference on Electronic Voting Technology, USENIX Association, Berkley, USA, no. 14, 2008].

[5] P.Y.A Ryan *et al., Pret a Voter:a Voter-Verifiable Voting System* [IEEE Transaction on Information Forensic and Security,vol.4,No.4, doi:http://dx.doi.org.in/10.1109/TIFS.2009.2033233].

Acknowledgment

This is the right moment to express sincere gratitude towards our guide Prof Shirish Gosavi for his invaluable guidance and perceptive suggestions at every stage during project work.

We express sincere gratitude towards Dr. Vahida Attar, Head of the Department and Dr. B.B. Ahuja for their moral spport and for providing all the necessary facilities for completing this project.

We are also thankful to all faculty members of Department of Computer Engineering and Information Technology COEP for their valuable insights. I also take the opportunity to thank the departmental staff for their timely help.

Lastly, We express sincere thanks to my friends, my family members and all those who directly or indirectly, have helped us in completing the project.

Date: _____ Utkarshbhanu Andurkar, Shivam Marathe