Prevention of Phishing Attack on Voting System Using Visual Cryptography

By

ADAMU HALIDU
HND/23/COM/FT/0377

A Project Submitted to the

Department of Computer Science,

Institute of Information and Communication Technology

Kwara State Polytechnic, Ilorin

In Partial Fulfillment of the Requirements for the award of Higher National Diploma (HND) In Computer Science

June, 2025

CERTIFICATION

This is to certify that this project was carried out by **ADAMU HALIDU** with matriculation number **HND/23/COM/FT/0377.** It has been read and approved meeting part of the requirements for the Award of Higher National Diploma (HND) in Computer Science.

_____ _____

MR. OLAJIDE A. T. **DATE**
(Project Supervisor)

_____ _____

MR. OYEDEPO F. S. **DATE**
(Head of Department)

_____ _____

DATE

External Supervisor

DEDICATION

This project is dedicated to Almighty God and to my beloved parents.

ACKNOWLEDGEMENT

All praise is due to Almighty God the Lord of universe. I praise Him and thank Him for giving me the strength and knowledge to complete my HND program and also for my continued existence on the earth.

I appreciate the utmost effort of my supervisor, **MR. OLAJIDE A. T.** whose patience, support and encouragement have been the driving force behind the success of this research work. She took time out of her tight schedule to guide me and go through this project. She gave useful corrections, constructive criticisms, comments, recommendations, advice and always ensures that an excellent research is done. May the Lord Almighty strengthen her knowledge and understanding.

Let me use this moment to appreciate the HOD of my department (comp. science) **MR. OYEDEPO** and the project coordinator in person of **MR. SAKA** and the entire lecturers of this great department may God bless you all in abundantly.

I want to use this opportunity to say a big thanks, and appreciate my parents **MR.** & **MRS. ADAMU** for their support and prayer over me, my prayer is that you shall reap the fruit of your labor. **(AMEN).**

TABLE OF CONTENTS

ABSTRACT

Phishing attacks pose a significant threat to the security and integrity of voting systems, which are critical components of democratic societies. These attacks can manipulate voters into disclosing sensitive information or casting fraudulent votes, undermining the democratic process. To address this challenge, the concept of Visual Cryptography (VC) emerges as a potential solution. This abstract explores the use of Visual Cryptography techniques to prevent phishing attacks on voting systems. Visual Cryptography is a cryptographic technique that involves splitting a secret image into multiple shares, which individually reveal no information about the original image. When the shares are stacked or overlaid together, the secret image becomes visible. This inherent property of Visual Cryptography makes it suitable for safeguarding sensitive information, as it requires no complex computations for decryption and minimizes the risk of information leakage. In the context of voting systems, Visual Cryptography can be applied to protect voter credentials and choices. During the authentication phase, the voter's authentication credentials, such as voter ID and password, can be divided into shares using Visual Cryptography. These shares can be distributed to the voter through separate communication channels, minimizing the chances of an attacker obtaining both shares. Only when the voter presents both shares will the authentication information become apparent, preventing phishing attacks that attempt to steal credentials. Furthermore, Visual Cryptography can be employed to secure the voter's choice. When a voter casts their vote, the chosen candidate's details can be encoded into shares using Visual Cryptography. These shares can be transmitted separately to the voting system, eliminating the possibility of a single share revealing the complete vote. The voting system can then combine the shares to obtain the final vote count without exposing individual choices, thus thwarting attempts to manipulate or intercept votes. In conclusion, the application of Visual Cryptography in voting systems presents a promising approach to prevent phishing attacks. By leveraging the inherent properties of Visual Cryptography, such as secret sharing and secure reconstruction, voting systems can enhance their security measures against phishing attempts. However, practical implementation considerations, user experience, and potential scalability challenges should be thoroughly evaluated before deploying such a system on a large scale.

Keywords: *Phishing attack, Voting system, Visual Cryptography, Security, Authentication, Credential protection, Secret sharing, Voter choice, Information security, Democratic process, Fraud prevention, Cryptographic techniques.*

CHAPTER ONE
INTRODUCTION

1.1 Background to the Study

In recent years, the use of digital systems for voting has gained popularity due to its convenience and efficiency. However, the increasing reliance on technology in the electoral process also introduces new risks and vulnerabilities. One significant threat is phishing attacks, which can compromise the integrity and security of voting systems. Phishing attacks have become a significant concern in the digital age, posing a threat to the security and integrity of various systems, including voting systems. Phishing involves the fraudulent attempt to obtain sensitive information, such as usernames, passwords, or financial details, by disguising oneself as a trustworthy entity. (Yao and Tang, 2016).

In the context of voting systems, phishing attacks can lead to unauthorized access, manipulation of votes, and compromised election results. To address this issue, the study proposes the use of visual cryptography as a preventive measure against phishing attacks in voting systems. Phishing attacks involve deceptive tactics to trick individuals into revealing sensitive information or performing unintended actions. In the context of voting systems, attackers may send fraudulent emails or messages disguised as official communication from election authorities, political parties, or candidates. (Dharshini and Vinothina, 2017).

These messages often contain links to fake websites that mimic legitimate platforms, prompting voters to enter their confidential information such as login credentials or personal identification details. Once the attackers obtain this information, they can gain unauthorized access to the voting system, manipulate votes, or even impersonate legitimate voters to cast fraudulent ballots. The consequences of such attacks can undermine the democratic process, erode public trust, and compromise the legitimacy of election results. Traditional security measures, such as firewalls, encryption, and user authentication, can provide some level of protection against phishing attacks. However, they may not be foolproof, as attackers constantly evolve their techniques to deceive users and exploit

system vulnerabilities. Therefore, there is a need for innovative and robust preventive measures to counter phishing attacks in voting systems. (Jhaveri and Shah, 2018).

Visual cryptography offers a promising approach to enhance the security of voting systems against phishing attacks. It is a cryptographic technique that involves splitting a secret image or information into multiple shares, which individually reveal no meaningful information. Only when these shares are properly combined or overlaid, the secret image becomes visible. This property of visual cryptography makes it suitable for preventing unauthorized access and ensuring the integrity of sensitive information. By leveraging visual cryptography, a voting system can protect confidential data, such as voter credentials and ballot information, by distributing them among multiple visual shares. (Abhishek and Bansal, 2019).

This approach introduces an additional layer of security, as attackers would need to obtain all the shares and correctly combine them to gain access to the sensitive information. As a result, phishing attacks targeting voting systems can be significantly mitigated, safeguarding the integrity and authenticity of the electoral process. This study aims to explore the use of visual cryptography as a preventive measure against phishing attacks in voting systems. By developing and evaluating a secure voting system that employs visual cryptography techniques, this research seeks to contribute to the advancement of secure and trustworthy electronic voting systems. (Desoky and Ghonaimy, 2020).

1.2 Statement of the Problem

The problem at hand is the vulnerability of voting systems to phishing attacks, which can compromise the security and accuracy of elections. Traditional security measures like strong passwords and two-factor authentication may not be sufficient to protect against phishing attacks. Therefore, there is a need for an alternative approach that leverages visual cryptography to enhance the security of the voting system and prevent unauthorized access.

1.3 Aim and Objectives

The aim of this study is to explore and implement visual cryptography as a preventive measure against phishing attacks in voting systems. The specific objectives are as follows:

1. To develop a system that shall be user friendly application that allow user to vote swiftly.
2. To design and develop a system that shall monitor the voting processes and avoid manipulations.
3. To provide recommendations for the integration of visual cryptography into existing voting systems.
4. To implement the system using PHP.

1.4 Significance of the Study

The study's findings and proposed preventive measures are significant in several ways. By leveraging visual cryptography, the study aims to mitigate the risks posed by phishing attacks, thereby ensuring the integrity and confidentiality of the voting process. By implementing robust security measures, voters can have increased confidence in the accuracy and fairness of election results. The study contributes to the existing body of knowledge on voting system security and explores the practical implementation of visual cryptography for preventing phishing attacks. The outcomes of this study can serve as a foundation for further research and development of advanced security measures in voting systems.

1.5 Scope of the Study

The study focuses on the prevention of phishing attacks in voting systems using visual cryptography. It involves an analysis of current vulnerabilities, the design and implementation of a secure voting system, and the evaluation of its effectiveness. However, the study does not delve into other potential security threats or comprehensive assessments of the entire voting infrastructure.

1.6 Organization of the Report

This report is organized as follows. Chapter one discusses the general introduction and overview of the whole project. It also discusses the statement of the problem, aim and objectives of the proposed system, significance of the study, scope and limitations of the project, organization of the report and the definition of technical terms used. Chapter two deals with the literature review, it reviews related topic to the project, discussion of related aspect of the project topic relative. Chapter three deals with analysis of the system which include the data collection method employed, the description of the existing system and its problems and the description of the proposed system and possible advantages it will provide the will solve problems encountered in the existing manual system. Chapter four deals with the design, implementation and the description of the proposed system. It covers description of the output design, input design, database design and procedure design.

The implementation techniques used, the programming language used in developing the new system and system requirements for running the system. And also talks about the program documentation as well user documentation. Lastly chapter five presents a brief summary of the work done, experience gained and problems encountered in the course of the project, conclusion and recommendation. Other appendices included after the references used are; algorithm, system flowchart, program flowchart, program source listing and generated computer output.

CHAPTER TWO

LITERATURE REVIEW

2.1 Review of Related Work

Anmyinray *et al.,* (2016). Online voting using visual cryptography, aimed in casting vote for critical and confidential internet co-operate decision, using Pixel encoding scheme method and RSA Algorithm using visual cryptography model, to overcome the limitation of existing traditional voting system by providing security and less timer. The study lack internet facilities in some remote area.

Kayal *et al.,* (2014). Malicious website detection using visual cryptography and OTP. This research aim to cross verify website identify and prove it is genuine using malicious link verifiable technique with Visual cryptography and OTP algorithm it result was Preventing and detecting phishing web page. The current existing system might as for vital details with the help of phishing website without authentication.

Adewale *et al.,* (2020). Visual semegram an enhanced technique for confidentiality requirement of electronic voting system. Aimed to design a technique that would conceal the sensitive message toward achieving a confidentiality requirement of e-voting system and to formulate mathematical equating for concealing sensitive message. Insertion of enhanced semagram and an advanced encryption standard method with Visual semagram algorithm. Confidentiality security requirement of the electronic voting system. The transition of a sensitive message through public and unprotected network could be a cheaper avenue for the fraudster to attack.

Jyoti and Vikram, (2015). Visual cryptography for image privacy protection using diverse image media. This research aim to present it customer secure information storage media using Secret sharing technique and Visual cryptography and diverse image media algorithm. It provide perfect secrecy and secure decryption. It increase computer hackers and power abuses.

Lauretha *et a.,* (2017). Online voting system based on image steganography. The research aimed to provide more secured election than the paper base election using Image

stegamography and visual cryptography algorithm. It Improved version of the existing and to end verifiable voting system. The system was insecure traditional voting system.

Trihasti and Rinald, (2019). Secure E-payment method based on visual cryptography. Security online payment using visual cryptography. Using Secret sharing scheme method and Visual cryptography algorithm. It result was Detecting and preventing phishing and identify theft. Credit card frauds over the internet due to security weakness.

Nisha, (2016). Secured authentication for internet voting in co-operate companies to prevent phishing attacks. The aim of this research is to verify that you are not an imposture. Encryption of information and decryption method with Visual cryptography algorithm. There was improvement in the voting system. The system has time consuming both capture and low tally speed.

Nisha and Neela, (2016). Prevention of phishing attack in voting system using visual cryptography. Aimed to prevent phishing attack using Visual cryptography algorithm. In the system there was improved in Number of voters. It has problems of online voting such as security risk.

Abhishek *et al.,* (2015). An anti-phishing framework using visual cryptography. The aim of this research is to prevent online users from phishing attack. Extended visual cryptography scheme and balanced block replacement (BBR) advanced encryption standard (ACS). It result has Web application security. Rampart phishing attack on web based application.

Dhanashree *et al.,* (2015). An efficient approach for phishing website detection using visual cryptography (VC) and Quick Response Code (QR code). This research aim at preventing website from phishing and securing confidential information. Encryption and decryption of shares and Threefold algorithm. Quick response code and visual cryptography are merged which prevent password and other information from phishing website. In the existing system visual cryptography and QR code are used separately.

2.2 Overview of Phishing Attacks

Phishing attacks are a prevalent form of cybercrime that aim to deceive individuals and obtain sensitive information, such as usernames, passwords, or financial details. Attackers often disguise themselves as trustworthy entities, such as banks, social media platforms, or government agencies, to trick users into revealing their confidential information or performing unintended actions. Phishing attacks have severe consequences, including financial loss, identity theft, and unauthorized access to sensitive systems. They can also pose a significant threat to e-voting systems by compromising the integrity and security of the electoral process. (Dhamija *et al.*, 2006).

Phishing attacks typically involve the following characteristics and techniques:

i. **Email Spoofing:** Attackers send fraudulent emails that appear to be from legitimate sources, using spoofed email addresses and logos to deceive recipients. (Jakobsson and Myers, 2007).

ii. **Deceptive Websites:** Phishers create fake websites that closely resemble the legitimate websites of banks, online services, or e-commerce platforms. These websites often trick users into entering their login credentials or personal information. (Dhamija and Dusseault, 2008).

iii. **Malicious Attachments:** Phishing emails may contain malicious attachments, such as infected documents or executable files. When users open these attachments, malware is installed on their devices, allowing attackers to gain unauthorized access. (Whitty, 2011).

iv. **Social Engineering:** Phishers employ psychological manipulation techniques to exploit human vulnerabilities. They create a sense of urgency, fear, or curiosity to persuade users to take immediate action without proper verification. (Herley, 2015).

2.3 Description of E-Voting System

E-voting systems refer to the use of electronic platforms and technologies to facilitate the casting, counting, and tallying of votes in elections. These systems aim to

enhance the efficiency, accuracy, and accessibility of the voting process. E-voting systems aim to improve accessibility for voters, reduce errors in the vote counting process, and provide more efficient election administration. However, they also face challenges related to security, privacy, and ensuring trust in the system. (Kantarcioglu and Clifton, 2004).

E-voting systems typically consist of the following components:

1. **Voter Interface:** This component provides the interface through which voters interact with the e-voting system. It can be a web-based application, a dedicated electronic voting machine, or a mobile application. The voter interface allows voters to authenticate themselves, view candidate information, and cast their votes securely. (Groza and Vancea, 2013).
2. **Election Authority System:** The election authority system manages the overall operation of the e-voting system. It includes functionalities such as voter registration, candidate registration, ballot creation, and result tabulation. The election authority system ensures the integrity, confidentiality, and accuracy of the voting process. (Teague and Yu, 2010).
3. **Voting Infrastructure:** The voting infrastructure encompasses the hardware, software, and network infrastructure required to support the e-voting system. It includes servers, databases, communication networks, and security mechanisms. The voting infrastructure should be robust, reliable, and scalable to handle the voting load and protect against potential security threats. (Hao and Ryan, 2004).
4. **Security Measures:** E-voting systems implement various security measures to protect against unauthorized access, tampering, and data breaches. These measures include encryption of sensitive data, secure authentication mechanisms, digital signatures, and auditing capabilities. Security protocols are designed to ensure the confidentiality, integrity, and availability of the voting system. (Sandler and Wallach, 2004).

E-voting systems typically consist of the following processes:

1. **Voter Registration:** Before participating in an e-voting system, eligible voters need to register their information, such as their name, address, and identification details. This step ensures that only authorized individuals are allowed to vote. (Benaloh and Tuinstra, 1994).
2. **Authentication and Authorization:** E-voting systems employ various mechanisms to authenticate and authorize voters. This may involve using unique identifiers, such as voter ID cards or biometric information, to verify the identity of voters and ensure that they are eligible to cast their votes.
5. **Ballot Creation:** E-voting systems generate digital or electronic ballots that include the names of candidates or issues being voted upon. These ballots are designed to be user-friendly, ensuring that voters can easily navigate and make their selections. (Groza and Vancea, 2013).
3. **Casting Votes:** Voters can cast their votes electronically using different methods. This may include using web-based platforms, mobile applications, or dedicated electronic voting machines. Voters typically make their choices by selecting options on a screen or through touch interfaces.
6. **Vote Encryption:** To ensure the confidentiality and integrity of votes, e-voting systems employ encryption techniques. Votes are encrypted before transmission to prevent unauthorized access or tampering. Encryption algorithms and secure communication protocols are used to protect the votes during transmission and storage. (Teague and Yu, 2010).
4. **Vote Tabulation:** Once the voting process is complete, e-voting systems aggregate and tabulate the votes. This may involve counting the votes electronically, checking for errors or discrepancies, and generating final reports or results.
7. **Auditing and Verification:** E-voting systems often include auditing and verification mechanisms to ensure the accuracy and integrity of the voting process. These mechanisms may involve conducting post-election audits, comparing digital

records with physical ballots, or allowing for recounts in case of disputes. (Sandler and Wallach, 2004).

2.4 Overview of Visual Cryptography Algorithm

Visual cryptography is a cryptographic technique that allows for the secure sharing of secret information through the use of visual images. It provides a means of distributing and reconstructing secret data without the need for complex computations or cryptographic keys. Visual cryptography algorithms can be categorized into different types, such as XOR-based algorithms, additive algorithms, and visual secret sharing schemes. Each type has its own characteristics and suitability for specific applications. (Naor and Shamir, 1994).

Visual cryptography algorithms typically operate as follows:

i. **Secret Sharing:** The secret data is divided into shares, each encoded as a visual image. These shares are distributed to different participants involved in the communication or authentication process. (Shamir, 2017).

ii. **Pixel Expansion:** The visual cryptography algorithm expands the pixel resolution of the shares to create additional noise-like pixels. This ensures that individual shares do not reveal any information about the secret unless combined with other shares. (Wu and Guo, 2019).

iii. **Reconstruction:** To recover the secret data, the participants overlap or superimpose their shares using a specific reconstruction procedure. The superimposed shares reveal the secret information when visually combined, while individual shares remain visually meaningless. (Naor and Shamir, 1995).

Visual cryptography algorithms aim to provide the following properties:

i. **Perfect Secrecy:** The secret information remains confidential even if some shares are compromised.

ii. **Security without Computation:** The reconstruction of the secret data does not require any computational operations.

iii. **Easy Verification:** The authenticity and correctness of the reconstructed secret can be easily verified visually.

CHAPTER THREE

METHODOLOGY AND ANALYSIS OF SYSTEM

3.1 Research Methodology

In this chapter, we will discuss the research methodology used to prevent phishing attacks on a voting system using visual cryptography. The methodology outlines the steps and processes undertaken to analyze the existing system, identify its problems, propose a new system, and highlight the advantages of the new system over the existing one.

The research methodology followed for this study consists of the following steps:

i. **System Requirements:** Define the specific requirements of the voting system, including the number of voters, level of security needed, and any regulatory or legal constraints that must be adhered to.

ii. Threat Analysis: Conduct a thorough analysis of potential phishing attacks on the voting system. Identify the different attack vectors, such as email or website spoofing, social engineering, or malware distribution.

iii. **Visual Cryptography:** Visual cryptography is a method of encrypting an image into multiple shares, which can be distributed to different participants. Each participant will hold one share, and the original image can only be revealed when the shares are combined.

iv. **Image Encoding:** Determine the format and structure of the voting system's images, such as ballots or voter identification cards. Define the encoding scheme that will be used to convert the image into shares for visual cryptography.

v. **Share Distribution:** Establish a secure process for distributing the shares to the voters. This can involve physical distribution of printed shares or secure electronic transmission. Ensure that the distribution method is resistant to interception and tampering.

vi. **Share Verification:** Implement a mechanism for voters to verify the authenticity and integrity of the shares they receive. This could involve cryptographic techniques such as digital signatures or hash functions.

vii. **Vote Casting:** Design the voting interface to incorporate the visual cryptography shares. Voters will need to combine their shares to reveal the original image and cast their votes. Implement appropriate security measures to prevent tampering or manipulation during this process.

viii. **Verification and Counting:** Develop a secure mechanism for verifying and counting the cast votes. Ensure that the process is transparent and auditable, providing a reliable tally of the votes while maintaining voter privacy.

ix. **Phishing Prevention:** Integrate security measures to prevent phishing attacks. This may include multi-factor authentication, secure communication protocols, user awareness training, and monitoring mechanisms to detect and respond to phishing attempts.

x. **Testing and Evaluation:** Thoroughly test the system to ensure it functions as intended and is resistant to various types of attacks, including phishing attempts. Conduct security audits and evaluations to identify any vulnerabilities and address them before deploying the system.

xi. **Deployment and Maintenance:** Once the system has been thoroughly tested and deemed secure, deploy it for use in actual voting scenarios. Continuously monitor the system, update security measures as needed, and address any emerging threats or vulnerabilities.

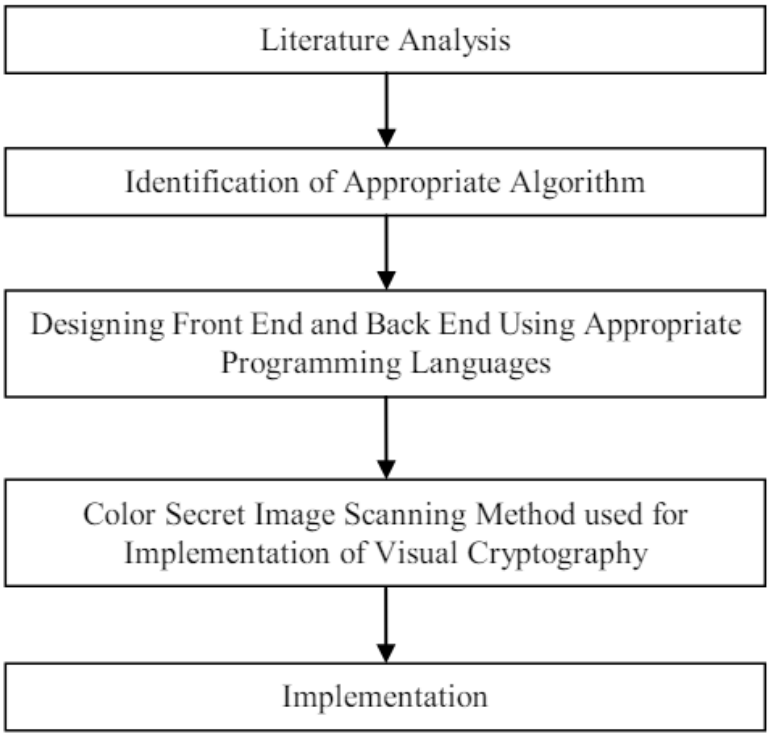


Fig. 3.1: Methodology flow chart

3.2 Analysis of the Existing System

The existing voting system is vulnerable to phishing attacks due to several factors, such as weak authentication mechanisms, lack of encryption of sensitive data, and susceptibility to spoofed websites. Phishing attacks can result in unauthorized access to sensitive data, including voter information and election results, which can compromise the integrity and confidentiality of the voting system.

3.3 Problems of the Existing System

Based on the analysis of the existing system, several problems and vulnerabilities were identified that make the system prone to phishing attacks. These problems include:

i. **Lack of Strong Authentication:** The existing system may rely on weak authentication mechanisms, such as simple username-password combinations, which can be easily compromised by phishing attacks.

ii. **Vulnerable Communication Channels:** The communication channels used in the system may not be adequately secured, allowing attackers to intercept and manipulate data during transmission.

iii. **User Interface Design:** The user interfaces provided by the system may not incorporate sufficient visual cues or indicators to help users detect phishing attempts. This can make it easier for attackers to deceive voters and collect their sensitive information.

iv. **Lack of Voter Education:** The system may not provide sufficient voter education or awareness about phishing attacks, making users more susceptible to falling for fraudulent schemes.

v. **Limited Transparency:** The existing system may lack transparency, making it difficult for voters to verify the integrity of their votes and ensuring that their votes are counted accurately.

3.4 Analysis of the Proposed System

The proposed system aims to address the problems identified in the existing system and provide a secure environment for voting by leveraging visual cryptography techniques. This section analyzes the proposed system design and its key components.

The analysis of the proposed system includes:

i. **Visual Cryptography:** An explanation of how visual cryptography works and how it can be applied to secure the voting process. This involves the generation and sharing of cryptographic shares that contain encoded information.

ii. **System Architecture:** The architecture of the proposed system, including the integration of visual cryptography techniques into the existing voting system components. This analysis highlights the modifications required to implement visual cryptography effectively.

iii. **Enhanced Authentication:** The proposed system incorporates stronger authentication mechanisms, such as multi-factor authentication or biometric verification, to prevent unauthorized access and phishing attacks.

iv. **Improved User Interfaces:** The user interfaces of the proposed system are designed to include visual indicators and cues that help users detect and avoid phishing attempts. This analysis focuses on the usability and effectiveness of these visual elements.

v. **Voting Process with Visual Cryptography:** An overview of how the voting process is modified to integrate visual cryptography techniques. This analysis explains how cryptographic shares are generated, distributed, and combined to retrieve the original vote.

3.5 Advantages of the New System over the Existing System

The proposed system offers several advantages over the existing system in terms of preventing phishing attacks on the voting system. These advantages include:

i. **Increased Security:** The use of visual cryptography enhances the security of the voting system by protecting voter information and preventing phishing attacks. The cryptographic shares make it extremely difficult for attackers to obtain meaningful information from intercepted data.

ii. **Improved User Awareness:** The visual indicators and cues incorporated into the user interfaces of the proposed system help educate and alert users about potential phishing attempts. This increases user awareness and reduces the likelihood of falling victim to fraudulent schemes.

iii. **Transparent Verification:** Visual cryptography allows voters to verify the integrity of their votes through the combination of cryptographic shares. This transparency ensures that votes are accurately counted and eliminates doubts about tampering.

iv. **Enhanced Privacy:** The use of visual cryptography techniques ensures the privacy of voters by distributing sensitive information across multiple shares. This prevents any single entity from accessing complete voter data, thus protecting voter privacy.

v. **Mitigation of Phishing Attacks:** By leveraging visual cryptography, the proposed system effectively mitigates phishing attacks, as it becomes significantly harder for attackers to manipulate or intercept voter data without detection.

Overall, the new system provides a robust defense against phishing attacks on the voting system, ensuring the integrity, security, and privacy of the voting process.

CHAPTER FOUR

DESIGN AND IMPLEMENTATION OF THE SYSTEM

4.1 Design of the System

This is the process of designing the input, output and the processing steps to meet the user's requirement identified in the system analysis. These include the data, input, output, processing storage and other control requirement.

4.1.1 Output System

In response to an event initiated by the users, the system generates appropriate output. All event or interaction with the system is through the keyboard. The important output of the proposed system is the display of selected department by the admin at a particular point in time. The following interface are the application views.

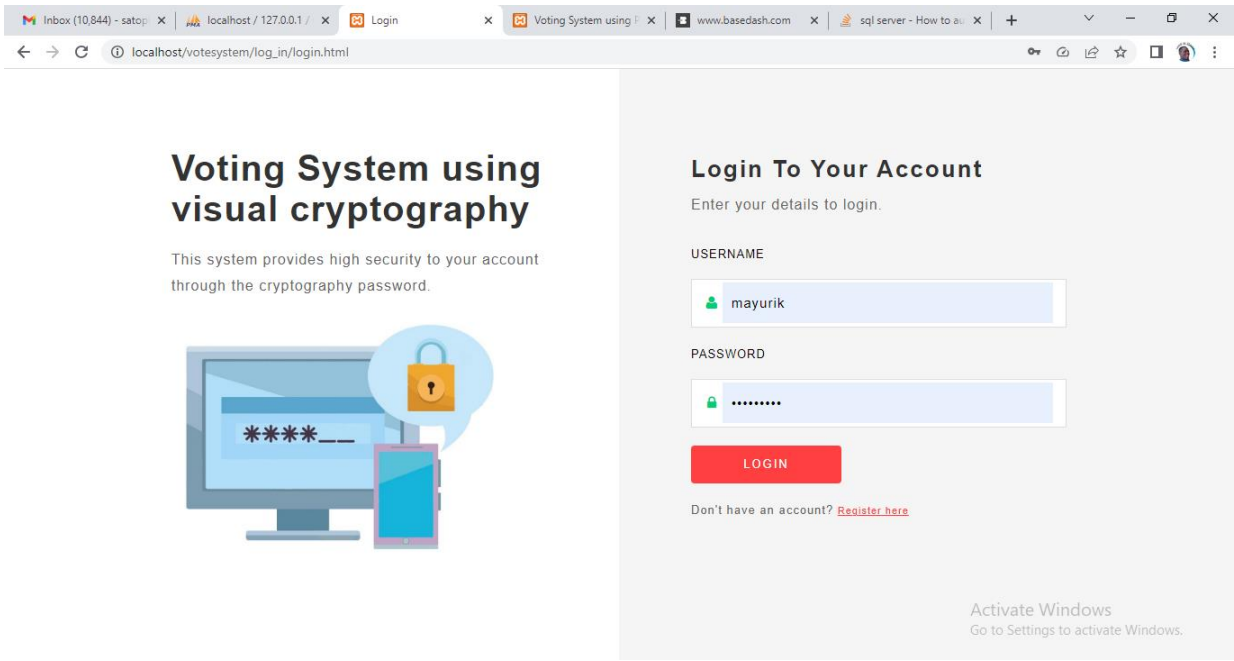


Figure 4.1. Home Page: This is the output of the operation page showing title of the web page and page for user login.

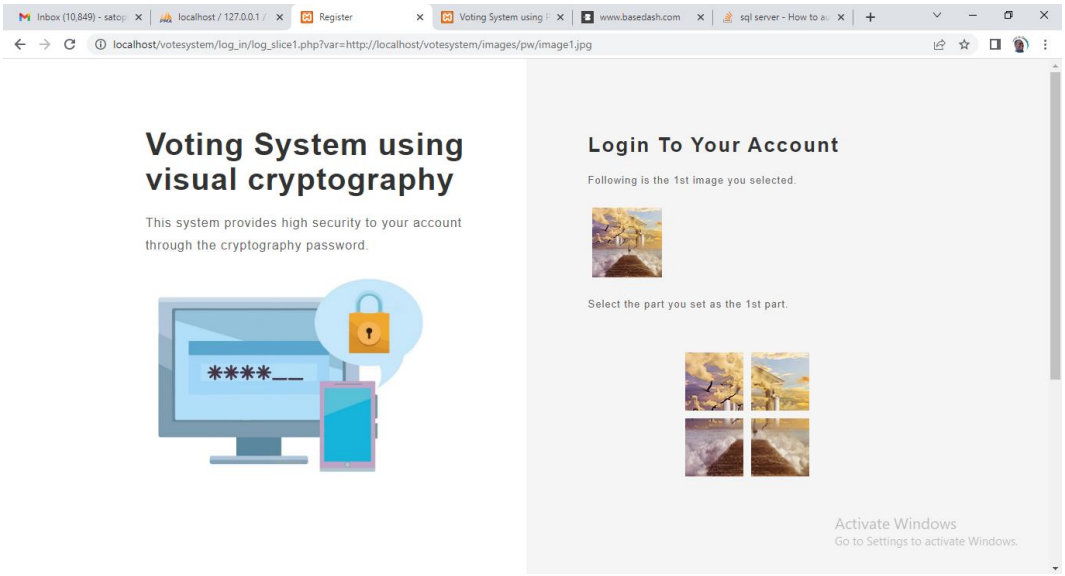


Figure 4.2. Cryptography Share Image Page: This is the output of the cryptography security image share page user have to choose some case sensitive images for security in other to access his or her page.

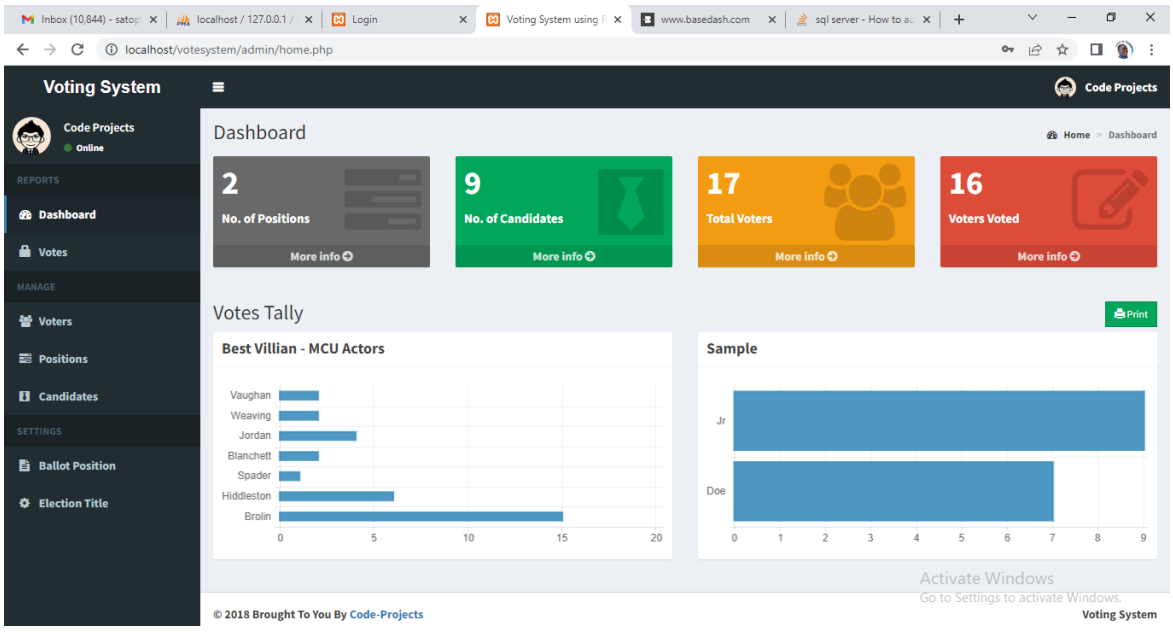


Figure 4.3. Admin Dashboard Page: This is the output of the Admin Dashboard of the system.

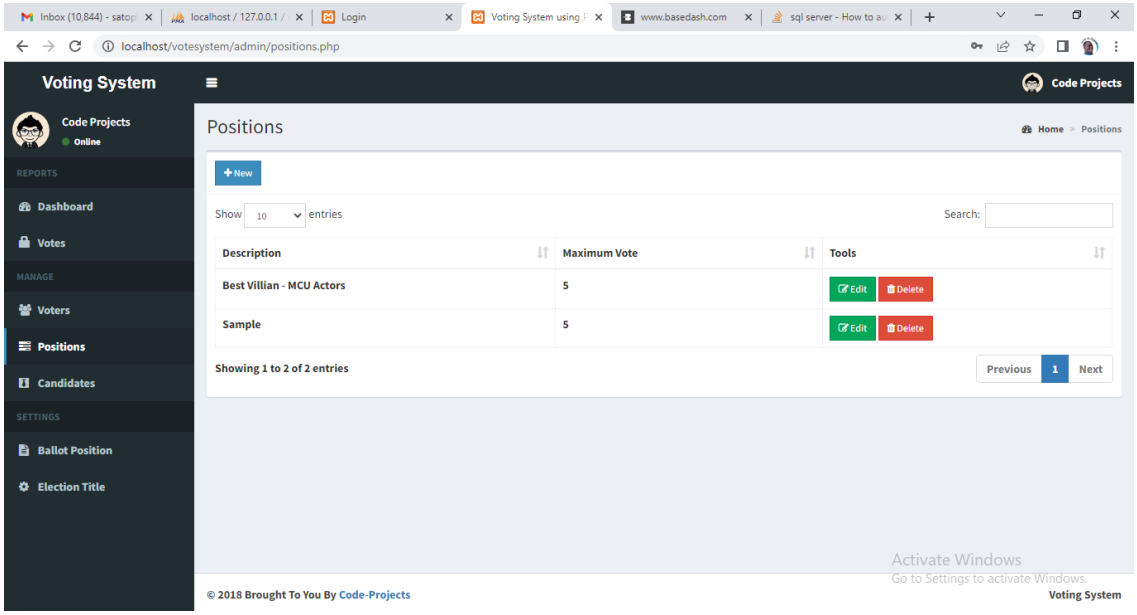


Figure 4.4. Candidates Position Page: This is the output of the list of candidate's position.

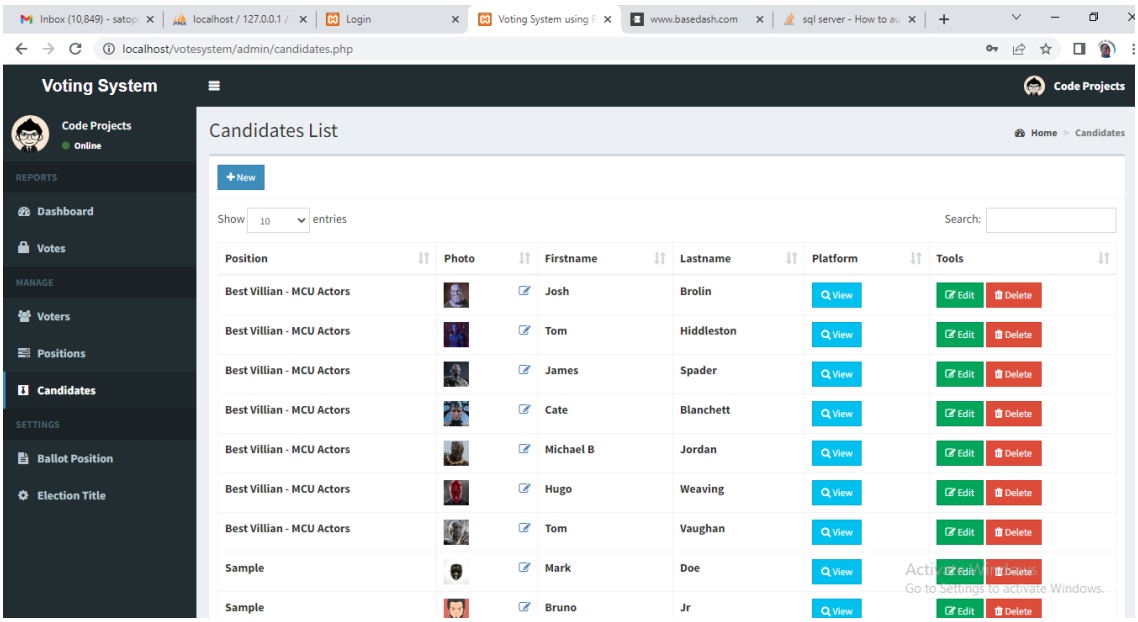


Figure 4.5. List of Candidates Page: This is the output of the list of candidates page.

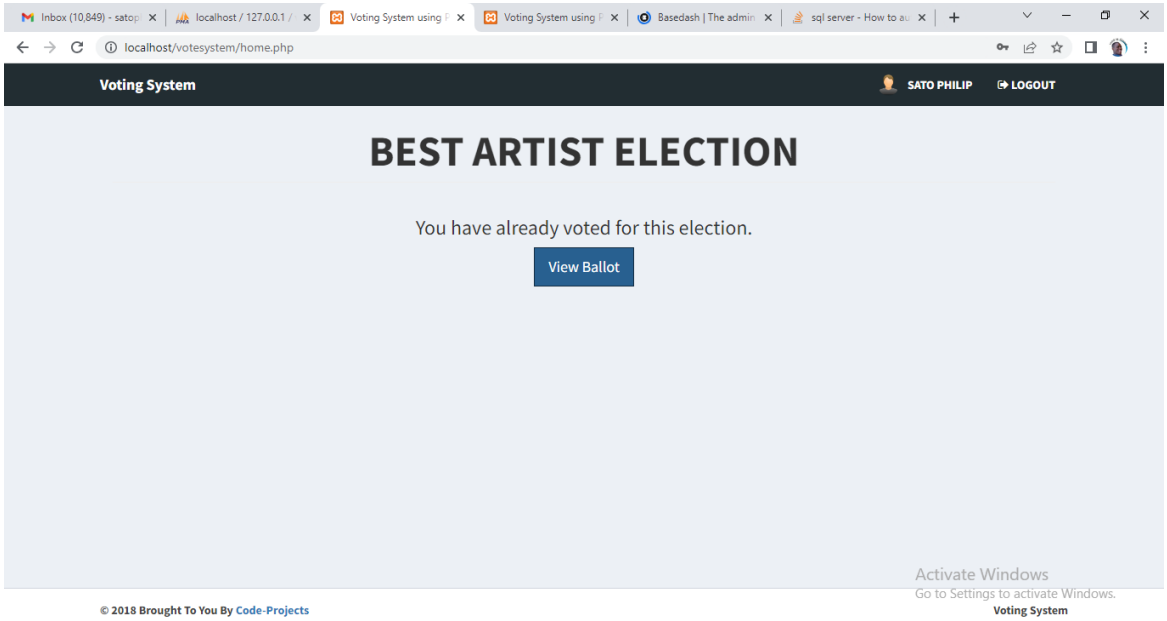


Figure 4.6. Vote Result Page: This is the output of the vote result page.

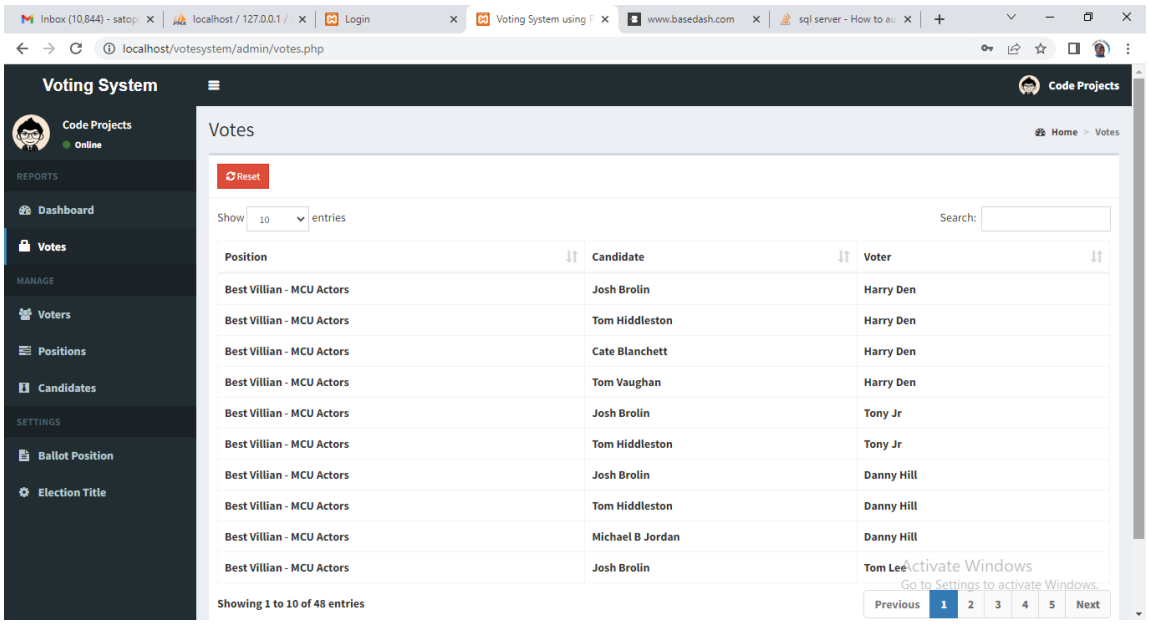


Figure 4.7. List of votes Page: This is the output of the votes page.

4.1.2 Input Design

Data can be supplied to the new system from two source, namely from standard keyboard device and/or from a disk file. When data is supplied from the keyboard, the software has a standard text input and editing box where the user can type, delete, copy, paste and perform all other usual text creation and editing operations. Inputs to the system consists of usual characters found on a standard. The data input box can handle up to 64kb of plain text data.

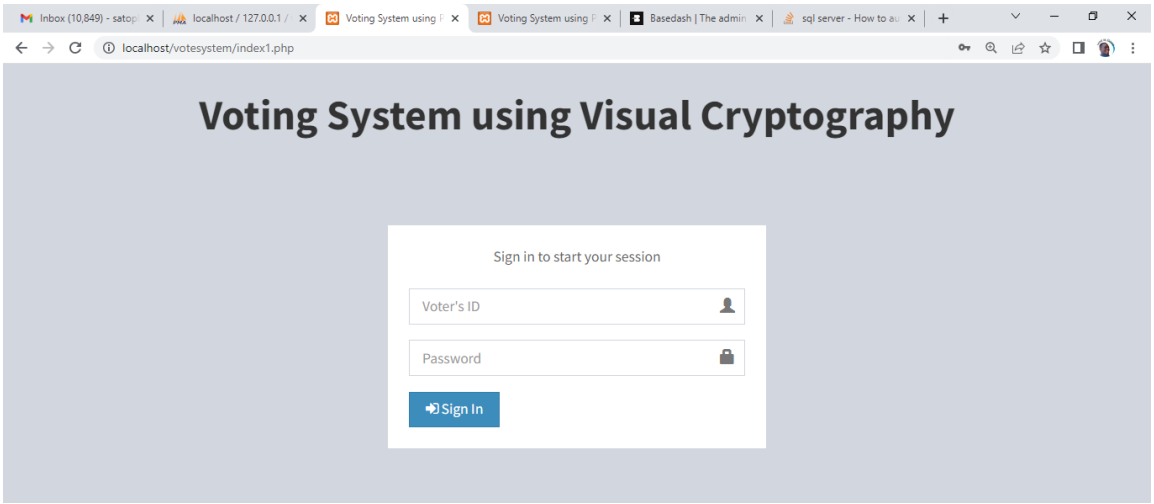


Figure 4.7. Login Page: This is the input interface of voter's login then he can access the voting web page here.

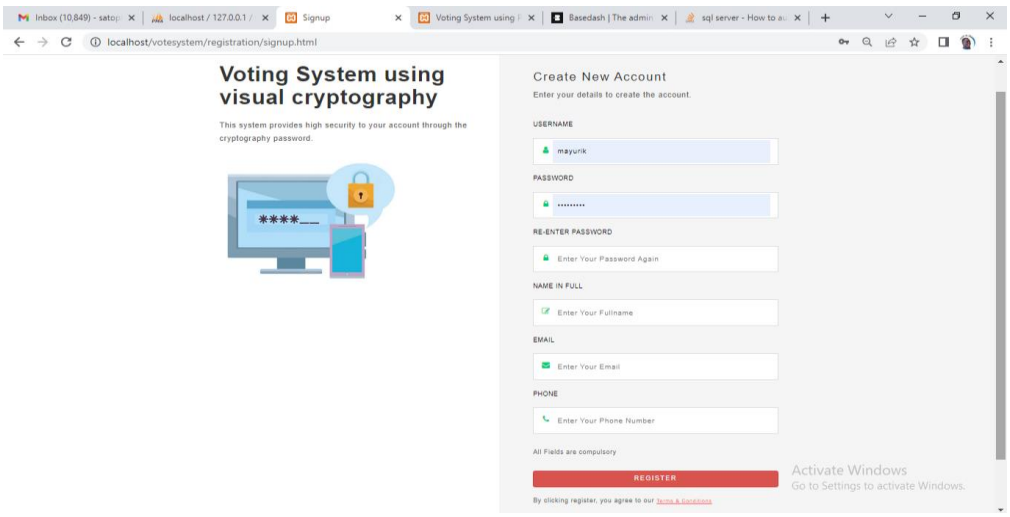


Figure 4.8. Registration Page: This is the input interface for user registration, new patients can register on the page.

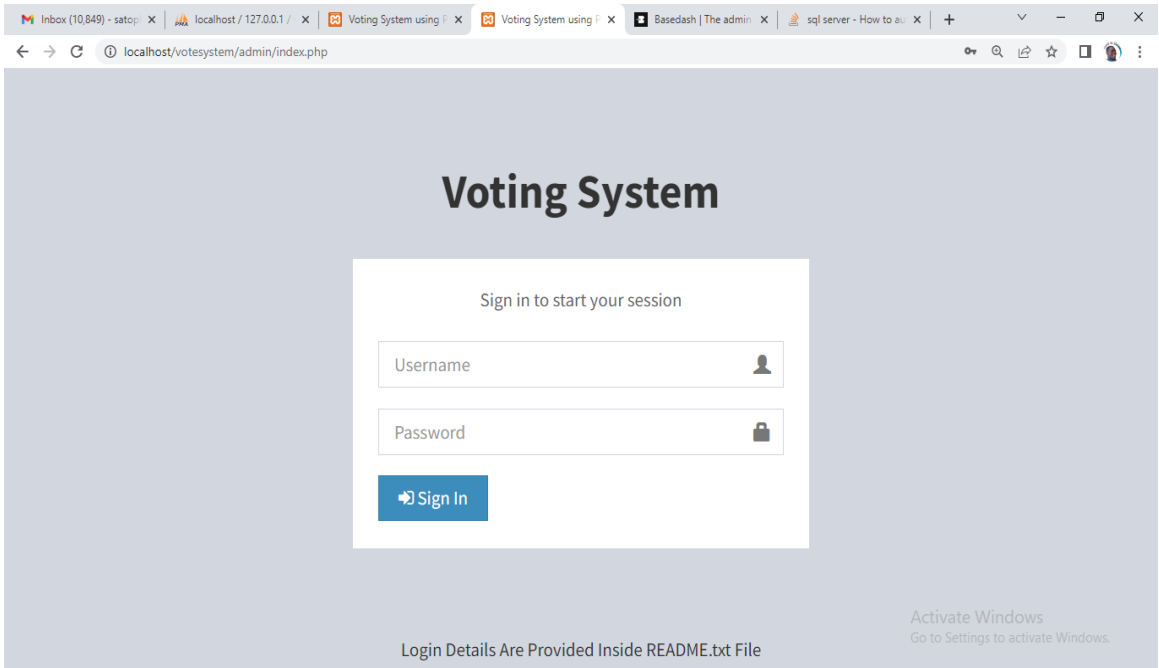


Figure 4.9. Admin Login Page: This is the input interface for Admin login so he can access the dashboard of the system.

4.1.3 Database Design

The coding of the program development used for this project help us to have access to the MYSQL which happens to be our database and which is used in storing the required information.

Table 1: Output for report showing the data of all appointments in the Doctor Appointment Management System.

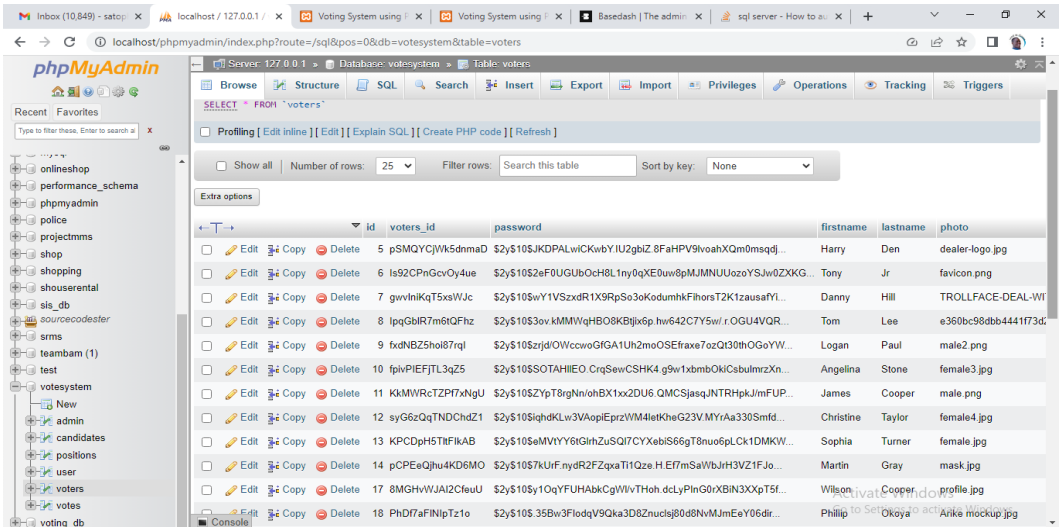
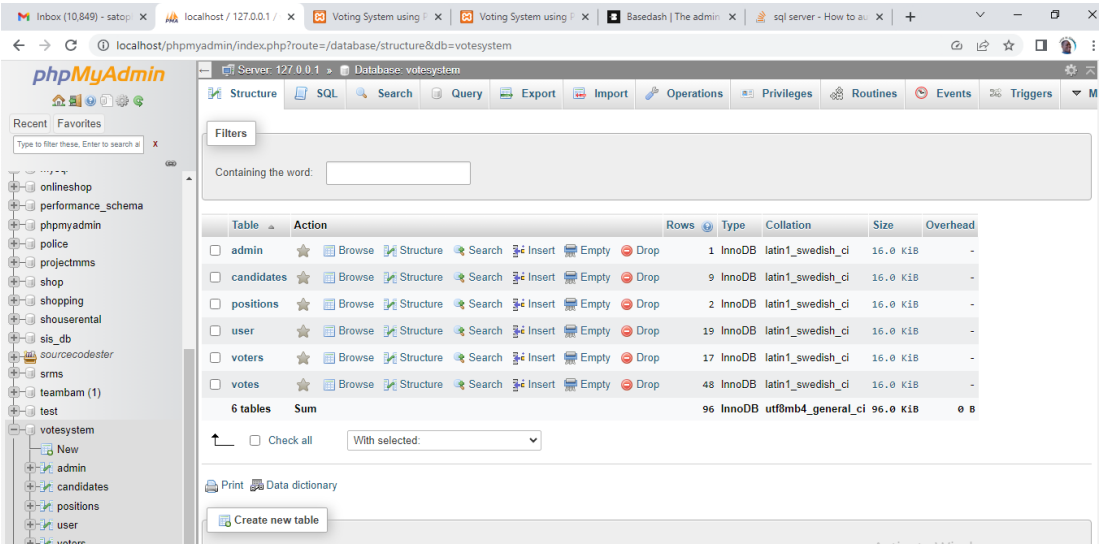


Table 2: Output of report showing the data all pages.



4.1.4 Procedure Design

The structure of the program that is designed in this new system is such that it provides for various option in the different menu available for easy accessibility and manipulation of records.

In this project work, there are four major procedures used, they are:

1. Registration form: This is used to accept new applicant data filed like name, matriculation number, place of attachment etc.
2. Search Record: To retrieve the applicant record and to know the content of the file of a particular record and no amendment can be made here.
3. Report: To know the general report of houses that have been registered on the system.

4.2 System Implementation

The design system depends on the capabilities and power of the device on which the application system is installed. However, selecting a choice of application support (Hardware and Software) depends much on;

- Cost and benefits
- Managements support for changes.

The most important requirement on which the running of the program basically depends on is the provision of internet facility. It can run on any laptop and mobile devices of any operating system.

4.2.1 Choice of Programming Language

The system was developed using Ionic Framework, packed and installable in android operating system. Ionic was chosen because it is a due to the following reasons:

1. SQLite is easy to understand during designing.
2. It supports modular programming.
3. It can be easily manipulate in other to design a user friendly environment.

4. It can be used to access android built-in system to capture GPS control.

4.2.2 Hardware Support

The hardware requires for the effective running of the system are as follows:

1. Any phone that runs on all operating system irrespective of version be it laptop, tablet, iPad and other mobile devices.
2. GPS ready

4.2.3 Software Support

This application is basically designed for laptop and mobile phones with GPS capability.

Android Studio was used to design the interface, code environment as well as building the installable .apk file.

4.2.4 Changeover Techniques

The system will be implemented using the parallel approach. This approach is considered because it ensure that the new system is tested alongside with the old system to ensure the effectiveness and efficiency of the system. With this system, as soon as results are analyzed and computed using a computerized method, the existing system will serve as backup in case there is a deficiency in the system.

4.3 System Documentation

After the program has been fully install. The next thing is to locate the installed application to put it into use.

4.3.1 Program Documentation

This is the detailed description of the proposed system. It is important because it helps to design and implement a system that would allow students both old and new to experience web rich

content on any of their devices. It also helps to design and implement an application that works on android operating system.

4.3.2 System Maintenance

On the system maintenance aspect, all the network system components should be maintained and managed as the operation continues. Maintenance of a system is to enable the continuos performance of the system as expected and if includes:-

- **Hardware Maintenance:-** These involves all the activities carried out on the computer and network hardware in order to anticipate the outset of incipient faults on the hardware. Hardware technology, engineers or information technology professionals.
- **Software Maintenance:-** These include all the activities carried out in updating and modifying the programs in order to suit future challenges in software development.
- **Adaptive Maintenance:-** These involve the changes and modifications in the programs to suit the operating environment.
- **Corrective Maintenance:-** These involve the process of detecting bugs in the programs and other faults and the subsequent removal functioning and operation.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

In this chapter, we provide a summary of the research conducted on the prevention of phishing attacks on a voting system using visual cryptography. The chapter highlights the key findings, conclusions, and recommendations based on the research conducted. First, we discussed the research methodology followed, which involved conducting a literature review, analyzing the existing system, identifying its problems, proposing a new system using visual cryptography, and analyzing the advantages of the new system over the existing one.

Next, we analyzed the existing voting system to understand its architecture, components, and processes. This analysis helped in identifying the vulnerabilities and weaknesses that make the system susceptible to phishing attacks. We then presented the proposed system, which incorporates visual cryptography techniques to enhance the security of the voting system. The proposed system design addressed the problems identified in the existing system, such as weak authentication, vulnerable communication channels, and lack of user awareness. Based on the analysis, we highlighted the advantages of the new system over the existing system. These advantages included increased security against phishing attacks, improved user awareness through visual indicators, transparent verification of votes, and enhanced privacy protection.

5.2 Conclusion

In conclusion, this research focused on the prevention of phishing attacks on a voting system using visual cryptography. The analysis of the existing system revealed vulnerabilities that make it prone to phishing attacks, such as weak authentication and vulnerable communication channels. These vulnerabilities can compromise the integrity of the voting process and undermine the trust of voters. The proposed system, utilizing visual cryptography techniques, offers a solution to these vulnerabilities. By encoding the secret information into multiple shares, the proposed system enhances the security of the voting

system. The visual indicators incorporated in the user interfaces help users detect and avoid phishing attempts, increasing user awareness and reducing the risk of falling victim to fraudulent schemes.

Furthermore, the proposed system provides transparent verification of votes, allowing voters to ensure the accuracy and integrity of their votes. The use of visual cryptography also enhances privacy protection by distributing sensitive information across multiple shares, preventing unauthorized access to complete voter data.

5.3 Recommendation

Based on the research conducted, the following recommendations are proposed:

i. **Implementation and Testing:** It is recommended to implement and test the proposed system in a controlled environment, simulating real-world voting scenarios. This will help validate the effectiveness and performance of the system in preventing phishing attacks and ensuring the integrity of the voting process.

ii. **User Education:** It is crucial to provide comprehensive user education and awareness programs to voters, election officials, and administrators. This education should focus on the risks associated with phishing attacks, how to identify and avoid them, and the importance of secure voting practices.

iii. **Continuous System Monitoring:** It is recommended to establish a system for continuous monitoring and detection of phishing attacks on the voting system. This can involve the use of intrusion detection systems, log analysis, and real-time monitoring tools to identify and respond to any suspicious activities promptly.

iv. **Collaboration with Security Experts:** Collaborating with security experts and professionals in the field of visual cryptography can provide valuable insights and guidance in further enhancing the security of the proposed system. Their expertise can help identify potential vulnerabilities and suggest improvements to mitigate emerging threats.

By implementing these recommendations, the prevention of phishing attacks on voting systems can be strengthened, ensuring the integrity and security of the democratic process.

REFERENCE

Adasanya, E. (1997), "Attitude of audience members to Nollywood films". Nordic Journal of African Studies, 16(1), 90 – 100.

Adeagbo, C. (2011), "Film medium and the democratic space in Nigerian". International Journal of Multidisciplinary Scholarship (Special Issue – Motion Picture in Nigeria) Nos. 3-5, 20 – 25.

Adesanya, A. (1997). *From Film to Video: Nigerian Video Film.* Jos: Nigerian Film Corporation.

Albert, R. E. & Watters, J. P. (1963). The development of aggressive behaviour during childhood: What have we learned in the past century. International Journal of Behavioural Development. Vol. 24, pp. 129 – 141.

Asemah, H. A. (2011). Media effects advanced in theory and research. NY: Hillsdale Enterprise.

Awake, P. E. (1999), "Violent film characters' portrayal of alcohol, sex, and tobacco-related behaviors". Pediatrics, 133 (1), 71 – 77.

Babbie, F. A. (2010), "Impact assessment of western films on teenagers and the question of cultural promotion in African society". International Journal of International Relations, Media and Mass Communication Studies, Vol.2, No.3, 21 – 33.

Balogun, F. (1987). *The Cinema in Nigeria.* Ibadan: Forth Dimension Publishers.

Benson, E.V. (2003). *A Tool for Public Relations: Opinion research.* Enugu: Virgin Creation. Comstock, G. S. (1979). *Television and Human Behaviour.* New York: Columbia UniversityPress.

Bilton, J. O. (2012). Nollywood movies and youths: An evaluation. Journal of Research in National Development. Vol. 10, (2), pp. 214-222.

Bjonbekk, J. (1995), "Film review: higher learning; short course in racism on a college campus". Available at https://www.nytimes.com/1995/01/11/movies/film-review-higher-learning-short-course-in-racism-on-a-college-campus.html

Chinoy, A. O. (1967). "Childhood aggression in Ogun State, Nigeria: fallout from violent movies
viewing". Social Sciences. Vol. 3, No. 5, 162 – 169

Crewell, D. S. (2013). McQuail mass communication theory. (5th ed), London Saga Publications.

Emmanuel, A. (1988). *Television and national security in contemporary issues in mass media for contemporary issues in mass media for development of national security*. Lagos: Unimedia Production.

Eysenck, H. J. (1978*). Sex, Violence and the Media*. London*:* Oxford University Press.

Frank, A. I. (1995), "Perception of sound: a study of selected Nollywood video films". Journal of Social Sciences and Humanities. Vol. 1, No. 2, 48 – 58.

Hebert, M. and Paulson, N. (2000). The home video phenomenon, media review. http accessed 10/10/2014.

Jersler, B. J. (2002), "The effects of televised violence on students". Masters Theses. 571. Grand Valley State University. Available at http://scholarworks.gvsu.edu/theses/571.

Joseph, R. J. (2003). Mass communication research: S (8th ed) Belment, C.A: Thomson and Wadsworth.

Kuffer, E. (1982). Looking inward with a outward thrusting the age of information and globalisation. Reflections of Nigerian Video Films and Industry Paper Presented 12 at Annual Meeting International Communication Association, Singapore http Accessed on 14/2/2009.

Loras, W. W. (1973), "The social cognitive theory". Boston University School of Public Health. Available athttp://sphweb.bumc.bu.edu/otlt/MPH Modules/SB/BehavioralChangeTheories /BehavioralChangeTheories5.html

Macombs, S. (1981). *Theories of Mass Communication.* New York: Columbia University

Macombs, W. W. & Shaw, L.O. (1981), "The social cognitive theory". Boston University School of Public Health. Available at http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/Behavioral ChangeTheories/BehavioralChangeTheories5.html

McQuail, D. (2005). *Mass Communication Theory.* London: Stage Publications.

Mgbejume, O. (2001), "Video production procedure". In Ekwuazi, H.; Sokomba, M. & Mgbejume, O. (Eds.), Making the Transition from Video to Celluloid. Jos: National Film Institute, 12 – 35.

Miller, K. (2005), Communication theories, perspectives, processes and contexts. New York: McGraw-Hill Companies Inc.

Neala, O. S.; Edemode, J. O. & Ihevba, P. (2017), "Impact of Nollywood films on children's behaviour in Ekpoma, Nigeria". Asian and African Studies, Volume 26, Number 2: 350 – 374.

Obasi, F. (2008). *A Handbook on Proposal Writing*. Enugu: Ruwil Nudas Graphics.

Ofonagora, J. B. (1987), Models and theories of communication. Lagos: African Renaissance Books Incorporated.

Ogbuoshi, B. L. (2005). *The Technique of Films And Television Production.* Enugu: Rhyce Kerex Publication.

Okunna, C. S. (1990). *Introduction to Mass Communication.* Enugu: New Generation Books.

Oparadudi, E. (1987). Themes and content of Nigerian home movies "UNILAAG" personality and social psychology. Vol.4 (1), pp.589-595. Press.

Osuala, S. O. (2011). Showcasing Nigeria through the home videos. IOSR Journal of Humanities and social Science. Vol. 13, (1), pp. 25-33.

Rotta, P. (1994). *The Film Till Now*. London: Vision Press Limited.

Sandler, D. G., & Wallach, D. S. (2004). Electronic voting and election integrity. ACM Transactions on Information and System Security (TISSEC), 7(3), 499-520.

Schaefer, J.A. & Larum, O. G. (1997). A dramatisation society: Representing rituals of human sacrifice as efficacious action, in Nigerian home videos. Zaria. Journal of African Cultural Studies. Vol. 16, pp. 7-23.

Shamir, A. (2017). Visual cryptography. In Encyclopedia of Cryptography and Security (pp. 1512-1515). Springer.

Skonia, S. (1965), "On the continuing problems of media effects research". In Curran, J. & Gurevitch, M. (Eds.), Mass media and society, 2nd Edition. London: Edward Arnold, 305 – 324.

Skornia, L. (1965). *Effect of Television on Children And Youth*. New York: Academic Press.

Skornia, S. (1996), "On the continuing problems of media effects research". In Curran, J. & Gurevitch, M. (Eds.), Mass media and society, 2nd Edition. London: Edward Arnold, 305 – 324.

Sobowale, E. (1998). Attitude of audience members to Nollywood films. Nordic Journal of African studies. Vol. (1), pp. 90-100.

Teague, V., & Yu, T. (2010). Trustworthy voting systems. In Proceedings of the 4th International Conference on Cybercrime Forensics Education & Training (CFET '10) (pp. 39-46). IEEE.

Time Magazine, (2016), "Impact assessment of western films on teenagers and the question of cultural promotion in African society". International Journal of International Relations, Media and Mass Communication Studies, Vol.2, No.3, 21 – 33.

Ugboruah, M. F. (2015), "Media and legacies of war: responses to global film violence in conflict zones". Current Anthropology, 56 (5), 678 – 700.

Vivian, Y. (1995). "Constructing the paradigm of violence: mass media, violence and youths". Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.2349& rep=rep1&type=pdf

Erwon, B. J. & hues Mann, K. (1989), "The effects of televised violence on students". Masters Theses. 571. Grand Valley State University. Available at http://scholarworks.gvsu.edu/theses/571

Whitty, M. T. (2011). People get phished: Exploring the role of individual differences in phishing susceptibility. In Proceedings of the 5th Annual Conference on Information Security Curriculum Development (pp. 18-24). ACM.

Wood, L. (1983), "Some effects of thoughts on anti- and prosocial influences of media events: A cognitive-neoassociation analysis". Psychological Bulletin, 95, 110 – 427.

Wu, Z., & Guo, F. (2019). Visual cryptography: A review. Journal of Visual Communication and Image Representation, 63, 102585.

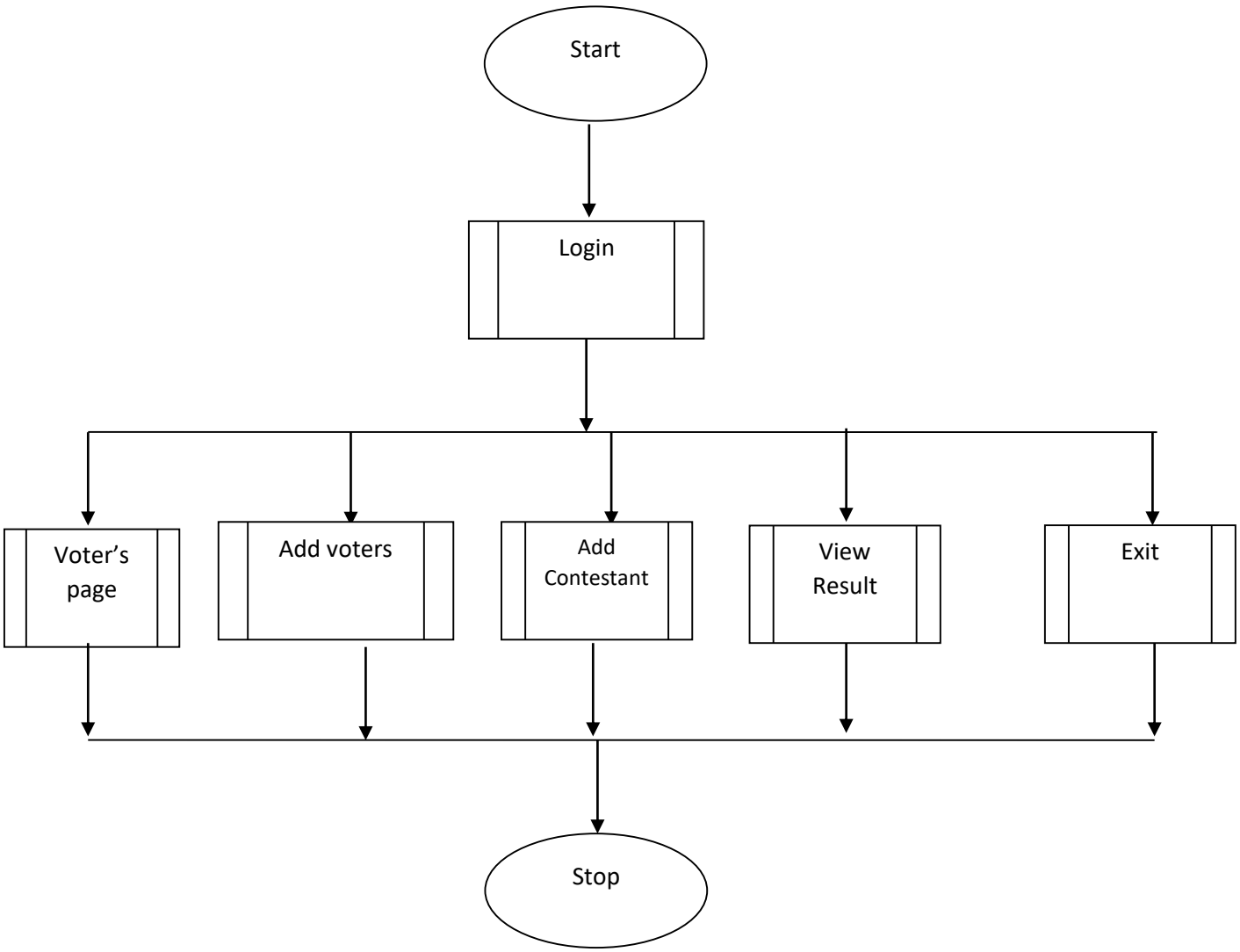
Yang, C. Y., & Chang, C. C. (2017). Visual cryptography based on hierarchical visual secret sharing. Journal of Visual Communication and Image Representation, 48, 238-246.

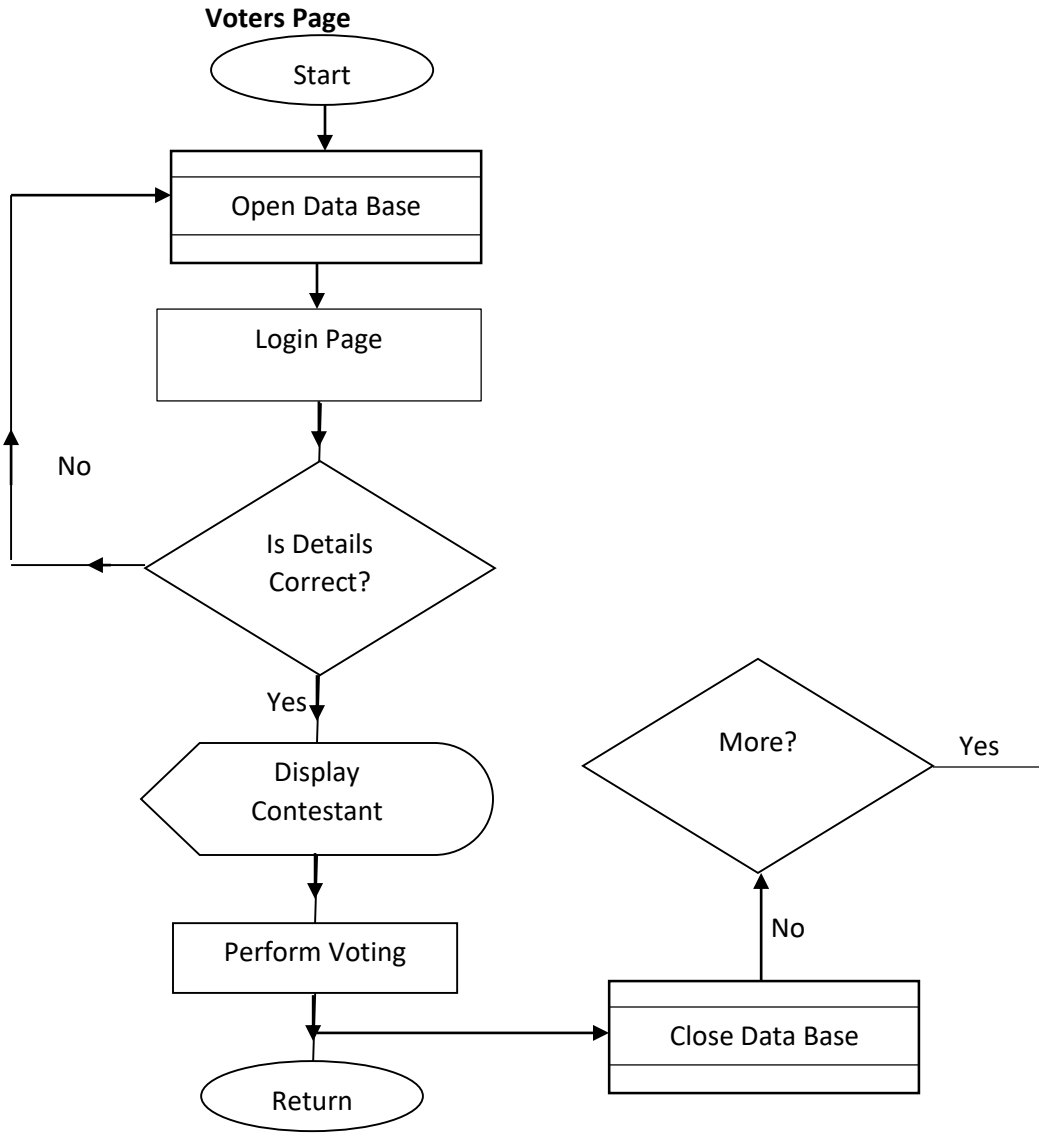
Yao, J., & Tang, Y. (2016). A secure e-voting scheme based on visual cryptography and chaotic maps. PloS one, 11(4), e0153450.

APPENDIX 1

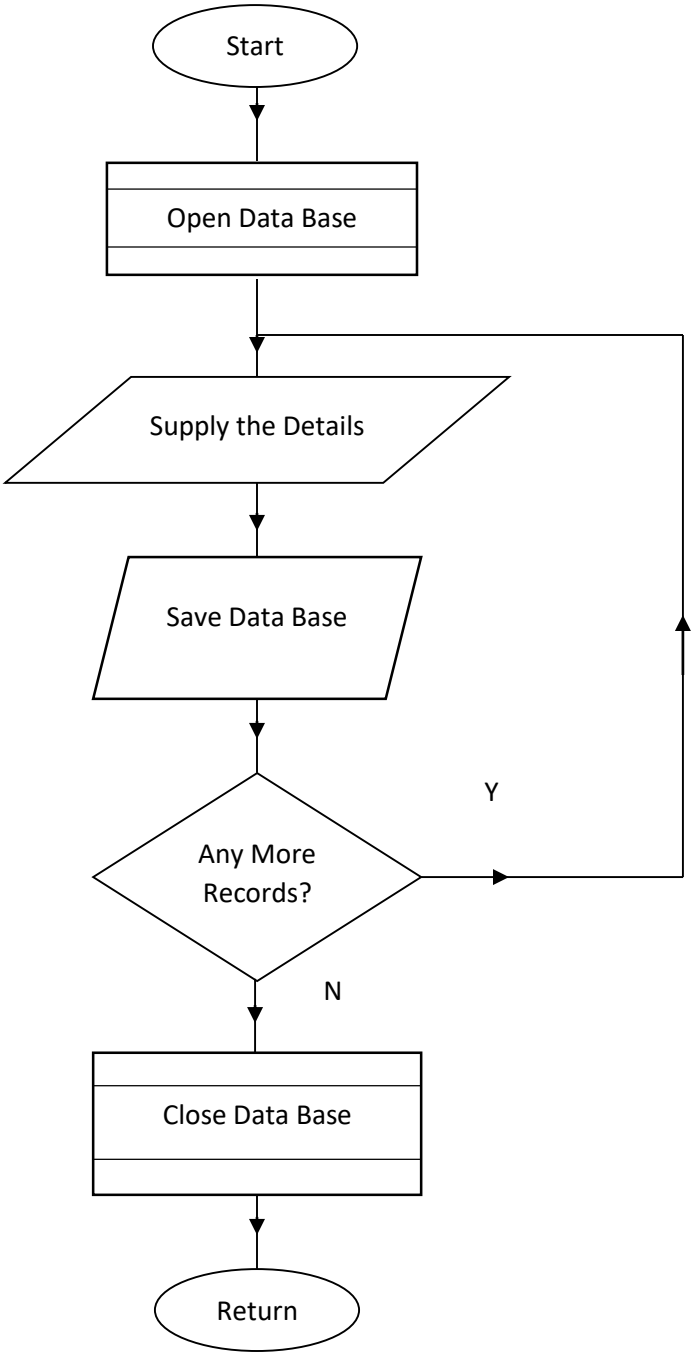
FLOWCHART

System flowchart

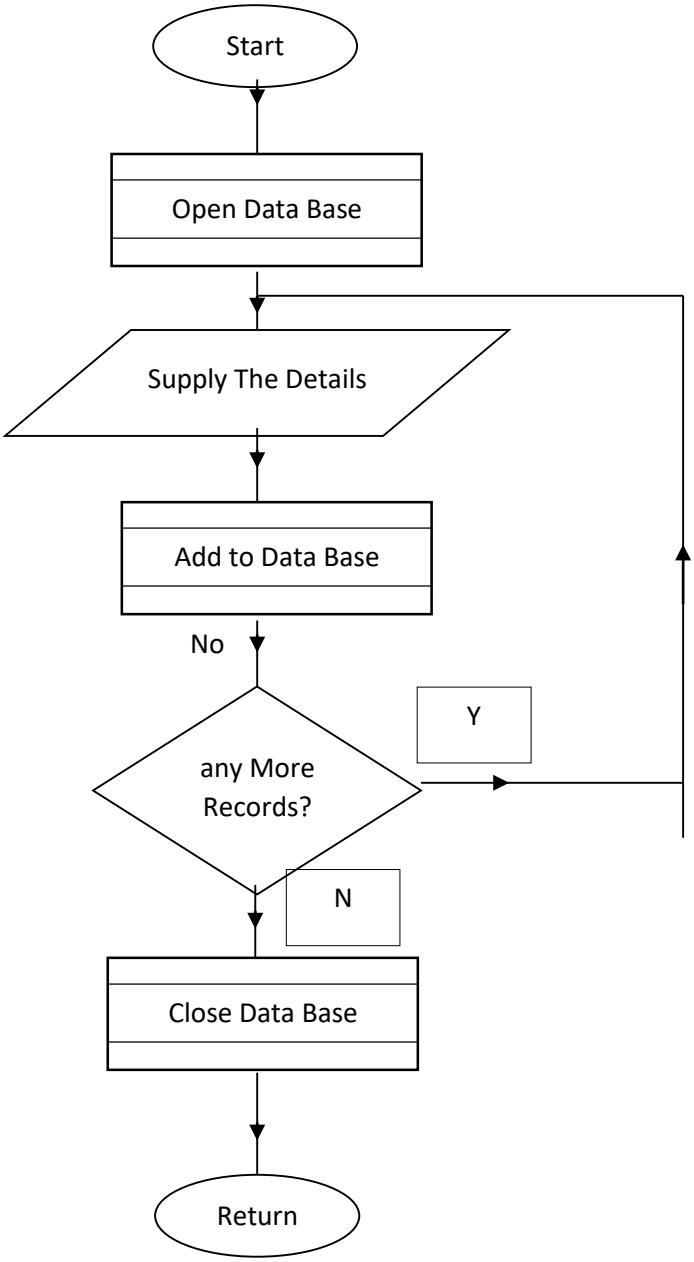



Voters Page
Start
Open Data Base
Login Page
No
Is Details Correct?
Yes
Display Contestant
Perform Voting
Return
More?
Yes
No
Close Data Base

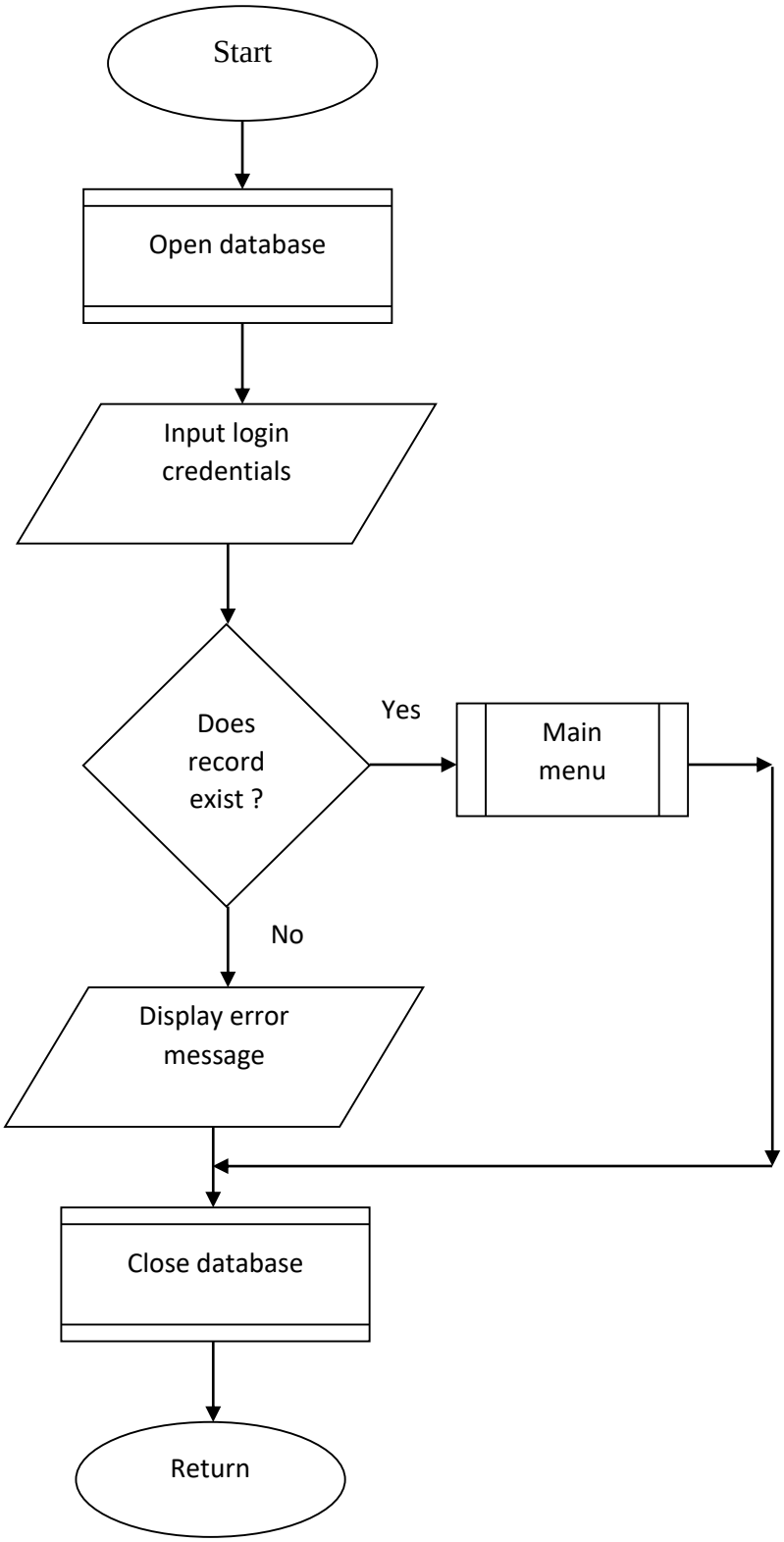
Add a Voter


Start
Open Data Base
Supply the Details
Save Data Base
Any More Records?
Y
N
Close Data Base
Return

Add Contestant



Login Flowchat



View Result