

ANTI PHISING I-VOTING SYSTEM USING VISUAL CRYPTOGRAPHY

Submitted in partial fulfillment of the requirements for
the award of
Bachelor of Engineering degree in Computer Science and
Engineering

by

UPPADA SRUTHI (Reg. No. 37110794)



**DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by
NAAC JEPPIAAR NAGAR, RAJIV
GANDHI SALAI, CHENNAI – 600**

119

MARCH - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **UPPADA SRUTHI (Reg. No. 37110794)** who carried out the project entitled "**ANTI PHISING I-VOTING SYSTEM USING VISUAL CRYPTOGRAPHY**" under my supervision from **August 2019 to March 2020**.

Internal Guide

Dr . S. JANCY MCA., MBA., M .Tech., Ph.D.,

Head of the Department

Dr. S. VIGNESHWARI M.E., Ph.D.,

Dr. L. LAKSHMAN M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **UPPADA SRUTHI** here by declare that the Project Report entitled “**ANTI PHISING I-VOTING SYSTEM USING VISUAL CRYPTOGRAPHY**” is done by me under the guidance of **Dr. S. JANCY MCA., MBA., M .Tech ., Ph.D.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **Sathyabama Institute Of Science And Technology** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D.,** and **Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. S. JANCY MCA., MBA., M. Tech., Ph.D., Assistant Professor**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Anti Phishing I-voting system using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. The user or the employee is allowed to cast his or her vote from any remote place. The election is held in full confidentiality where the user is allowed to vote only if he logs into the system by entering the correct password.

The password is generated by merging two shares using VC scheme. Before the election administrator sends share 1 to the voter's e-mail id and share 2 will be available in the voting system for his login during election. Voter then combines share 1 and share 2 using VC to get the secret password. No information can be revealed by observing any one share.

Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter personal information at a fake website.

TABLE OF CONTENTS

Sl.No.	TITLE	PAGE NO.
	ABSTRACT	v
1.	INTRODUCTION	1
	1.1 ROLE OF VOTING SYSTEM	1
	1.2 CURRENT PROBLEMS	2
	1.3 PROBLEM STATEMENT	3
	1.4 OBJECTIVES OF STUDY	3
2.	AIM AND SCOPE	4
	2.1 FRONT END	4
	2.1.1 .NET FRAME WORK	4
	2.1.2 ASP.NET	4
	2.1.3 VB.NET INSTEAD OF C#	4
	2.1.4 ADVANTAGES OF VB.NET	5
	2.1.5 VB.NET FEATURES	7
	2.2 BACK END	8
	2.2.1 MY- SQL	8
3.	METHODOLOGY	10
	3.1 GOALS AND OVERVIEW	10
	3.2 SYSTEM PROCEDURE	10
	3.3 MODULES	11
	3.3.1 REGISTRATION PHASE	12
	3.3.2 LOGIN PHASE	12
	3.4 SYSTEM REQUIREMENTS	13
4.	RESULT AND IMPLEMENTATION	14

	IMPLEMENTATION	14
	PROCEDURE	15
	VISUAL CRYPTOGRAPHIC ALGORITHM	16
	SHARES CREATION	17
5.	CONCLUSION	18
	REFERENCES	19
	APPENDIX	20
	(a) Code	20
	(b) Screenshots	25
	(c) paper publication	28

CHAPTER 1

INTRODUCTION

ROLE OF VOTING SYSTEM

Voting is a vital part of the democratic process. A voting system or electoral system is a method by which voters make a choice between options, often in an election or on a policy referendum.

A voting system contains rules for valid voting, and how votes are counted and aggregated to yield a final result. Since voting involves counting, it is algorithmic in nature, and, since it involves polling the sentiments of a person, this represents affective data. Together, with the exception of proxy voting, this corresponds to in-degree centrality in graph theory and social network analysis, with votes as directed edges, and voters and candidates as nodes. Common voting systems are majority rule, proportional representation or plurality voting with a number of variations and methods such as first-past-the-post or preferential voting. The study of formally defined voting systems is called voting theory, a subfield of political science, economics or mathematics.

With majority rule, those who are unfamiliar with voting theory are often surprised that another voting system exists, or that “majority rule” systems can produce results not supported by a majority. If every election had only two choices, the winner would be determined using majority rule alone. However, when there are three or more options, there may not be a single option that is preferred by a majority. Different voting systems may give very different results, particularly in cases where there is no clear majority preference.

CURRENT PROBLEMS

Nowadays, online transactions have become very common and there are various attacks present behind this. In these types of attacks, phishing is identified as a major security threat and new innovative ideas are arising on a regular basis. This helps to increase the preventive measures. Phishing is a form of online identity theft that aims to steal sensitive information like online banking passwords and credit card information from users. Phishing scams have been receiving extensive press

coverage because such attacks have been escalating in number and sophistication. Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. As the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not.

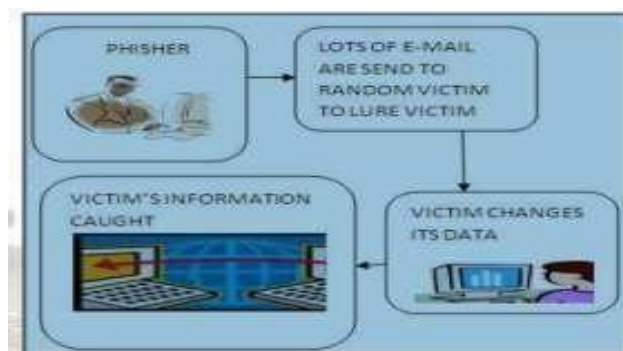


Fig:1.1 Phishing attacks

Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. One definition of phishing is given as —it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as —a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain.

Phishing attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information. Communication channels such as email, webpages, IRC and instant messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority.

Problem statement:

Internet is the large and global network. There are different kinds of applications based on the Internet. One of them is online voting system. The use of new technologies to support voting is the subject of great debate.

Several people advocate the benefits it can bring such as improved speed and accuracy in counting, accessibility, voting from home and it is also concerned with the risk it poses, such as unequal access, violation to secrecy, anonymity and alteration of the results of an election. There are two challenges to online voting system which can be seen as well technological as culture. You cannot at the same time have verifiability of an election and anonymous voting.

This implies that you have make a tradeoff between an anonymous election and verifiability. If you want to sure that each and every voter and provide him with a method to verify that his vote has been counted correctly. In order to do that, you need to link voter to vote which would make an anonymous vote impossible. There are cultures (in voting democracies) where public voting is common, so this is mostly a cultural question a cultural question on how you see voting in those cultures. Nonetheless is there a risk, if a non-functioning democracy would implement an identity-linked voting system, that the regime could after the election prosecute the defectors.

Objectives of study

Generally, the objectives of a study or research are the expected outcomes of the research or the study. This outcome may include solving a problem or bringing out statically information on the study. This section will be subdivided into two which general objectives (which is a broad statement about what I aim to achieve in this project) and the specific objectives (detailed objectives that what will be research during the project).

CHAPTER 2

AIM AND SCOPE

FRONT END:

.NET Framework:

The .NET Framework is an environment for building, deploying, and running XML Web services and other applications. It is the infrastructure for the overall .NET platform. The .NET Framework consists of three main parts: the common language runtime, the class libraries, and ASP.NET. The common language runtime and class libraries, including Windows Forms, ADO.NET, and ASP.NET, combine to provide services and solutions that can be easily integrated within and across a variety of systems. The .NET Framework provides a fully managed, protected, and feature-rich application execution environment, simplified development and deployment, and seamless integration with a wide variety of languages.

ASP.NET:

ASP.NET is more than the next version of Active Server Pages (ASP); it is a unified Web development platform that provides the services necessary for developers to build enterprise-class Web applications. While ASP.NET is largely syntax-compatible with ASP, it also provides a new programming model and infrastructure that enables a powerful new class of applications. You can migrate your existing ASP applications by incrementally adding ASP.NET functionality to them.

ASP.NET is a compiled .NET Framework –based environment. You can author applications in any .NET Framework compatible language, including Visual Basic and Visual C#. Additionally, the entire .NET Framework platform is available to any ASP.NET application. Developers can easily access the benefits of the .NET Framework, which include a fully managed, protected, and feature-rich application execution environment, simplified development and deployment, and seamless integration with a wide variety of languages.

Why VB.NET Instead of C#?

The new language created by is Microsoft: C# (pronounced “C-Sharp”). This is a new language, based on C/C++. C#, like VB.NET, is built specifically for

the .NET Framework, and much has been written about it. Given all the type, some people might wonder why they should choose VB.NET over C#.

Although both VB.NET and C# projects are created in the Visual Studio.NET environment, VB.NET was created specifically for VB developers and has a number of unique features that make it a great choice for building .NET applications. VB.NET is still the only language in VS.NET that includes background compilation, which means that it can flag errors immediately, while you type. VB.NET is the only .NET language that supports late binding. In the VS.NET IDE, VB.NET provides a dropdown list at the top of the code window with all the objects and events; the IDE does not provide this functionality for any other language.

VB.NET is also unique for providing default values for optional parameters, and for having a collection of the controls available to the developer. C#, like its C and C++ brethren, is case sensitive, something that drives most experienced VB developers crazy. In addition, C# uses different symbols for equality (=) and comparison (==). Finally, if you know VB, you are further down the road with VB.NET than you are with C#. Even though much has changed, the basic syntax of VB.NET is similar to VB, so you already know how to declare variables, set up loops, and so on. As you can see, VB.NET has some advantages over the other .NET languages.

Advantages of VB.NET:

1. Build Robust Windows-based Applications:

With new Windows Forms, developers using Visual Basic .NET can build Windows-based applications that leverage the rich user interface features available in the Windows operating system. All the rapid application development (RAD) tools that developers have come to expect from Microsoft are found in Visual Basic .NET, including drag-and-drop design and code behind forms. In addition, new features such as automatic control resizing eliminate the need for complex resize code. New controls such as the in-place menu editor deliver visual authoring of menus directly within the Windows Forms Designer. Combined with greater application responsiveness, as well as simplified localization and accessibility, these new features in Windows Forms make Visual Basic .NET the choice for today's Visual Basic developers.

2.Resolve Deployment and Versioning Issues Seamlessly:

Visual Basic .NET delivers the answer to all of your application setup and maintenance problems. With Visual Basic .NET, issues with Component Object Model (COM) registration and DLL overwrites are relics of the past. Side-by-side versioning prevents the overwriting and corruption of existing components and applications. XCOPY deployment enables Windows-based applications to be deployed to client machines simply by copying files into the desired application directory. In addition, the auto-downloading of applications for Windows makes the deployment of rich Windows-based applications as easy as deploying a Webpage.

3. Create Web Applications with a Zero Learning Curve:

Using the new Web Forms Designer in Visual Basic Using the new Web Forms Designer in Visual Basic .NET, Visual Basic developers can apply the skills they have today to build true thin-client Web-based applications. Drag-and-drop Web Form creation delivers Visual Basic for the Web while code behind forms enables developers to replace limited scripting capabilities of the past with the full power of the Visual Basic .NET language. New intelligent rendering capabilities and server-side Web Forms controls provide Web applications that render on any browser running on any platform. The new HTML designer delivers Microsoft IntelliSense statement and tag completion for HTML documents. In addition, separation of HTML markup and code enable more efficient team-based development.

a.Improved Coding:

You can code faster and more effectively. A multitude of enhancements to the code editor, including enhanced IntelliSense, smart listing of code for greater readability and a background compiler for real-time notification of syntax errors transforms into rapid application development (RAD) coding machine.

b.XML Web Services:

XML Web services enable you to call components running on any platform using open Internet protocols. Working with XML Web services is easier where enhancements simplify the discovery and consumption of XML Web services that are located within any firewall. XML Web services can be built as easily as you would build any class in Visual Basic 6.0. The XML Web service project template builds all underlying Web service infrastructure.

VB.Net Features:

Visual Studio .NET is now built on top of the .NET Framework. The .NET Framework takes application development to viewing the Internet as your new operating system. Your applications will no longer recognize hardware as a boundary limitation. This is an evolution of the Windows DNA model. This new framework is built on open Internet protocols for a standardized interoperability between platforms and programming languages. The .NET Framework will also allow the creation of new types of applications. Applications will now run using the Common Language Runtime (CLR). All .NET applications will use this same runtime environment, which allows your Visual Basic applications to run on equal ground with other languages.

The CLR allows Visual Basic to provide inheritance and free threading, whose absence created two glaring limitations to Visual Basic Applications. Visual Basic .NET is object-oriented. Everything is now an object, and every object is inherited from a standard base class. Another benefit of the CLR is a common type system, which means that all programming languages share the same types. This greatly increases interoperability between languages.

The Internet has entered a new phase. First, it was used to display static Web pages. Businesses soon found that this did not help them significantly. Next, the Internet evolved to dynamic content and allowing electronic commerce. The next step is to move towards complete applications running on the Internet. Visual Basic .NET promotes these new Web applications.

Web services allow objects to be located anywhere on the Internet and to be called from any application across the Internet (no more trying to get DCOM configured). Of course, extending applications across the Internet will increase security risks. The .NET Framework has many security features built-in to it to protect your applications. Type safety is now enforced. This prevents code from accessing memory locations that it does not have authorization to access. This allows you to define how your objects are accessed. Before code is run, it is verified to be type-safe. If it is not type-safe, it will only run if your security policies allow for it. Microsoft has added significant new functionality to make developers work more

effectively, without requiring them to learn entirely new ways of doing their jobs. If you have seen earlier versions of Visual Basic, the IDE for VB.NET will look very familiar. But if you have also worked with InterDev in the past, even more of the new interface will be old hat. That is because the new IDE used for VB.NET has integrated the best ideas from both environments to provide a more effective way of getting work done.

BACK END:

MS-Sql (Back-end Application):

1. Relational database management:

A relational database management system uses only its relational capabilities to manage the information stored in its database.

2. Information Representation:

All information stored in a RDBMS is represented only by data item values, which are stored in the tables that makeup the database.

3. Logical Accessibility:

Every data item value stored in a relational database is accessible by stating the name of the table it is stored in, the name of the column under which it is stored and the value of the primary key that defines the row in which it is stored.

4. Representation of Null Values:

The database management system has a consistent method for representing null values. For example, null values for numeric data must be distinct from zero or any other numeric value and for character data it must be different from a string of blanks or any other character value

5. Catalog Facility:

The logical description of the relational database management system is represented in the same manner as ordinary data. This is done so that the facilities of the relational database management system itself can be used to maintain database description

6. Data Language:

A relational database management system may support many types of languages for description data and accessing the database. However, there must be at least one language that uses ordinary character strings to support the definition of data, the definition of views, the manipulation of data, constraints on data integrity, information concerning authorization and the boundaries for recovery of units.

7. View Updating:

Any view that can be defined using combinations of base tables, that are theoretically updateable, is capable of being updated by the relational database management system.

8. Insert, Update and Delete:

Any operand that describes the results of a single retrieval operation is capable of being applied to an insert, update or delete operation as well.

9. Physical Data Independence:

Changes made to physical storage representations or access methods do not require changes to be made to application programs.

10. Logical Data Independence:

Changes made to tables, that do not modify any data stored in that table, do not require changes to be made to application programs.

11. Integrity Constraints:

Constraints that apply to entity integrity and referential integrity are specifiable by the data language implemented by the database management system and not by the statements coded into the application programs.

12. Database Distribution:

The data language implemented by the relational database management system supports the ability to distribute the database without requiring changes to be made application programs.

CHAPTER 3

METHODOLOGY

Goals and Overview:

The focus of this system was not just to measure whether security images were effective, but also to examine what makes them effective. For example, we explore the influence of factors such as the size, appearance, and customizability of security images. Also, we wanted to find out whether changes to the way the study was conducted—such as by making participants more security conscious, paying them more for the system, etc.—would cause them to pay more attention to the security images. Since the security images were typically displayed on internet banking websites and because we want to examine how users react in a high-value website, we decided to simulate a real-life internet banking scenario.

System Procedure:

Hereby propose a system with a more protected authentication and several layers of security. This is done with the involvement of an algorithm known as Visual Cryptographic algorithm. It consists of four modules. They are Registration with code along with random number generation, image generation in captcha format from the security code, share image creation using visual cryptography method, login and onetime password (OTP) generation. The steps are as follows.

The first page will be the home page. The second page is the register page, where the user will have to type all the required details that was asked by the server. And then the secret code and the password given by him will be stored in the database and the confirmation of his/her password will be sent to his/her email id. Then some five digits will be added to this secret code and this as a whole will contribute to the creation of a new image which looks like a captcha.

This will be split into two and one share will be given to the user. When the user logs in, he/she can make use of this share to upload it in the login page. If the shares of the images from the server and the user match, the original image will be

displayed. Or else, the image will not be displayed. When the image appears, the One-Time password will be sent to the mobile user mail ID.

Visual cryptographic algorithm - The system involves an automatic segregator of Images which is a two-step process of converting any images into the required Visual cryptography formatted images. After getting the original image, the images will be bifurcated into various shares depends on the access structure.

Shares creation - Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and the information is maintained with utmost confidentiality. A sender transmits the secret image which is divided into multiple shares and it holds hidden information. When all of these shares are aligned and stacked together, they expose the secret image information to the receiver.

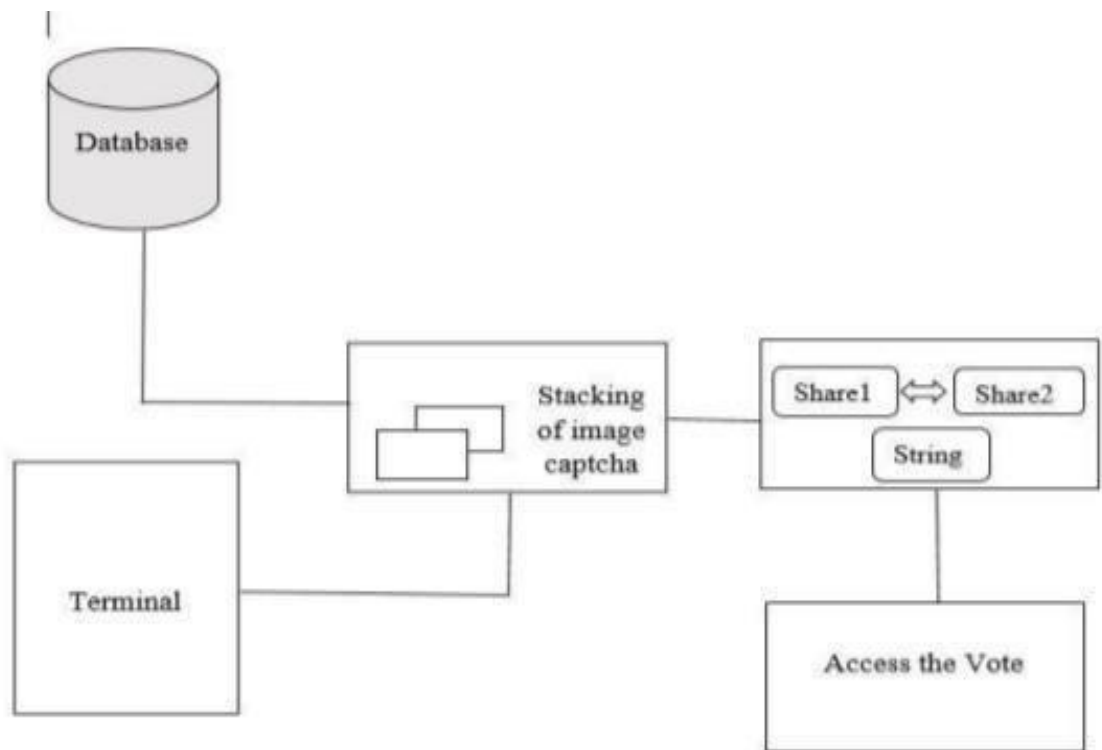


Fig:2.3: System architecture

MODULES:

The modules in our project are: -

Registration phase

Login phase

Registration phase:

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha[19] is generated. The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed.

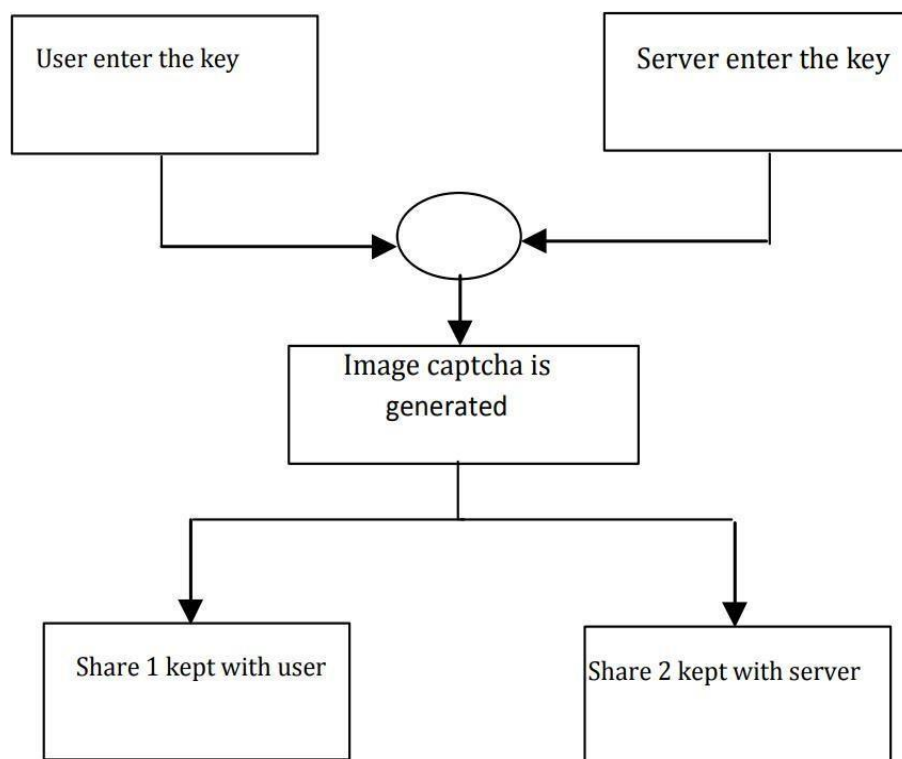


Fig:3.3: Registration phase

Login phase:

In the Login phase first the user is prompted for the username (user id). Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website, for each user, is stacked together to produce the image captcha. The image

captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. Figure can be used to illustrate the login phase.

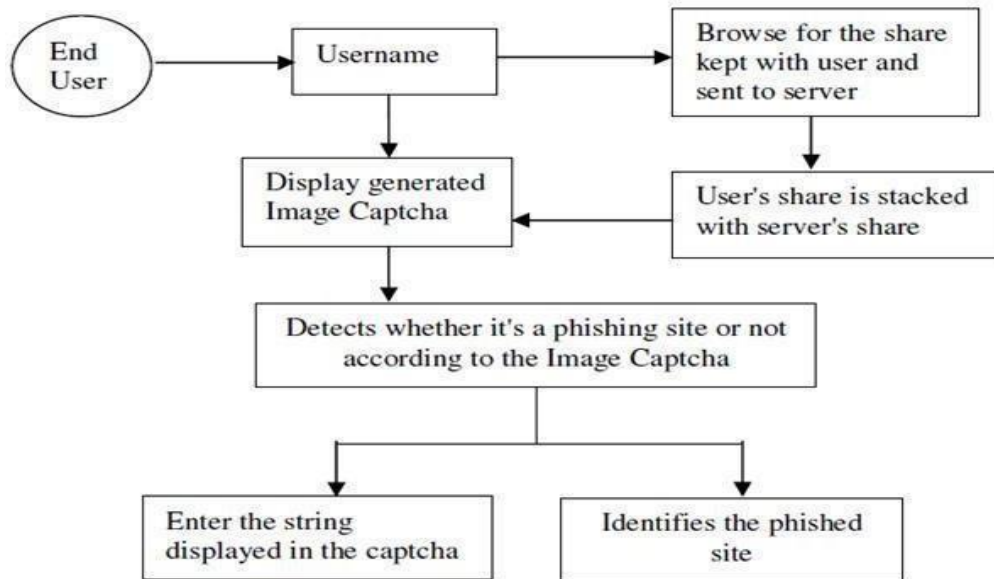


Fig:4.3: Login phase

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : - Windows XP.
- Coding Language : ASP.NET, C#.Net.
- Data Base : SQL Server 2005

CHAPTER 4

RESULT AND IMPLEMENTATION

IMPLEMENTATION:

1. Technical Feasibility:

The application will require an internet connection, a device with Windows OS as the hardware for running the website successfully. Thus the website to be developed is technically feasible.

2. Operational Feasibility:

New user will register and use the system. For this a small training program is required which will include briefing the working of the system. Demonstration will be performed so that the user actually gets to know the working of the system and what they need to do. Thus the required knowledge regarding the operations will be imparted to the users.

3. Financial Feasibility:

It is concerned with the cost involved at the time of development and maintenance of the website. The overall feasibility analysis shows that the proposed system will be beneficial in terms of knowledge base provided as well as the cost than the older existing system.

4. Faster:

The time span needed for the system is less than the manual voting system. Because the results are electronic. It saves a lot of time.

5. More accurate:

The margin of error is greatly reduced with online surveys because participants enter their responses directly into the system. Traditional methods rely the attentiveness of staff to enter all details correctly, and naturally human error can creep in whenever a person has to perform a repetitive task.

6. Easy to use for participants:

The majority of people that have access to the Internet prefer to answer surveys online instead of using the telephone. With an online survey, participants can pick a moment that suits them best and the time needed to complete the survey is much shorter.

PROCEDURE:

Here by propose a system with a more protected authentication and several layers of security. This is done with the involvement of an algorithm known as Visual Cryptographic algorithm. It consists of four modules. They are Registration with code along with random number generation, image generation in captcha format from the security code, share image creation using visual cryptography method, login and onetime password (OTP) generation. The steps are as follows.

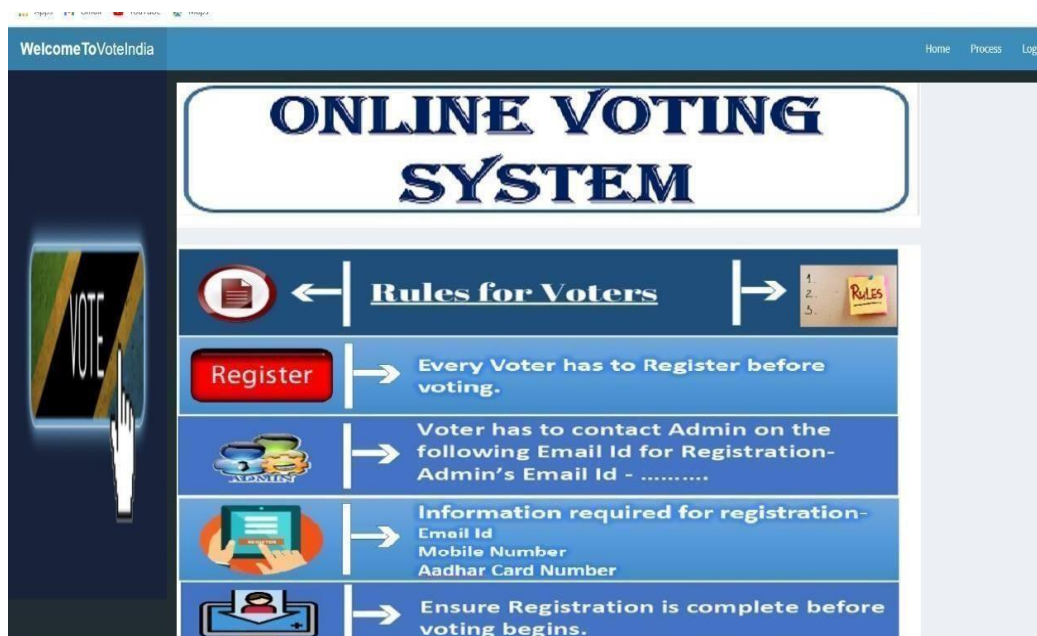


Fig:5.4: Home page

The first page will be the home page. The second page is the register page, where the user will have to type all the required details that was asked by the server. And then the secret code and the password given by him will be stored in the database and the confirmation of his/her password will be sent to his/her email id. Then some five digits will be added to this secret code and this as a whole will contribute to the creation of a new image which looks like a captcha. This will be split into two and one share will be given to the user. When the user logs in, he/she can make use of this share to upload it in the login page.

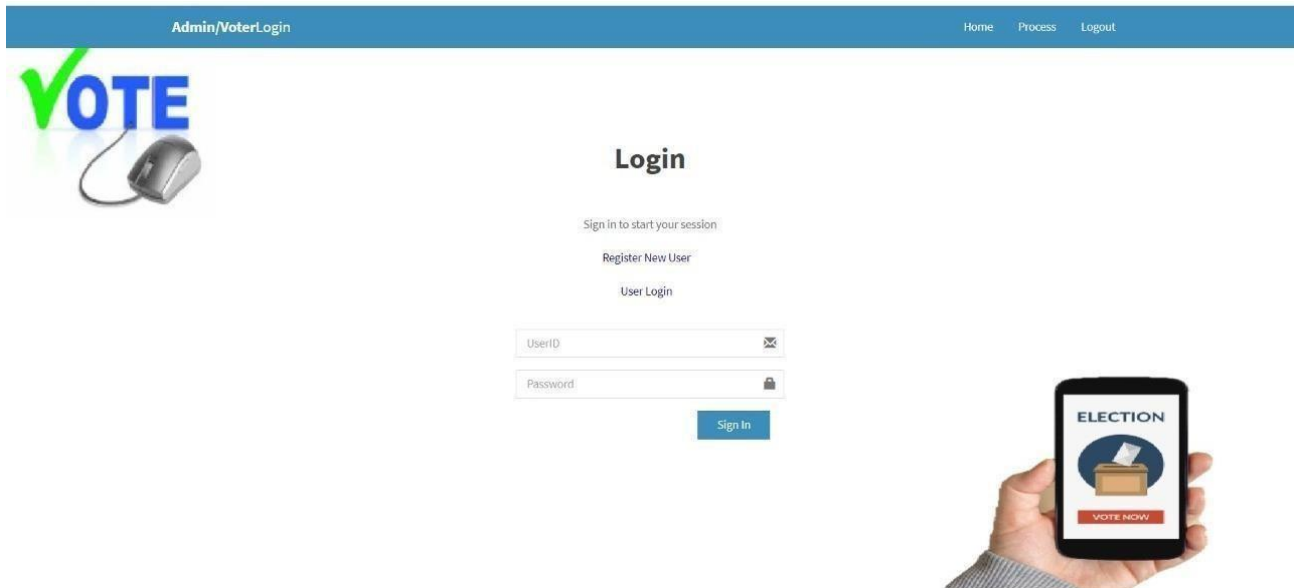


Fig:6.4: Login page (if new to registering go to register now user)

If the shares of the images from the server and the user match, the original image will be displayed. Or else, the image will not be displayed. When the image appears, the One-Time password will be sent to the mobile user mail ID.

VISUAL CRYPTOGRAPHIC ALGORITHM:

The system involves an automatic segregator of Images which is a two-step process of converting any images into the required Visual cryptography formatted images. After getting the original image, the images will be bifurcated into various shares depends on the access structure.

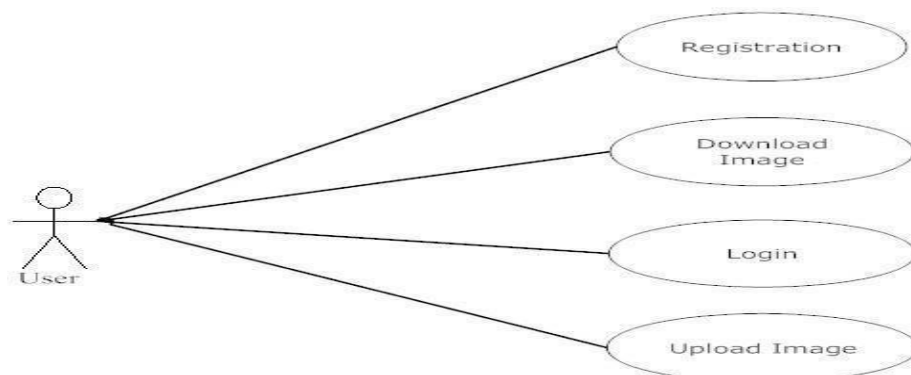


Fig:7.4: Visual cryptography

SHARES CREATION:

Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and the information is maintained with utmost confidentiality. A sender transmits the secret image which is divided into multiple shares and it holds hidden information. When all of these shares are aligned and stacked together, they expose the secret image information to the receiver.

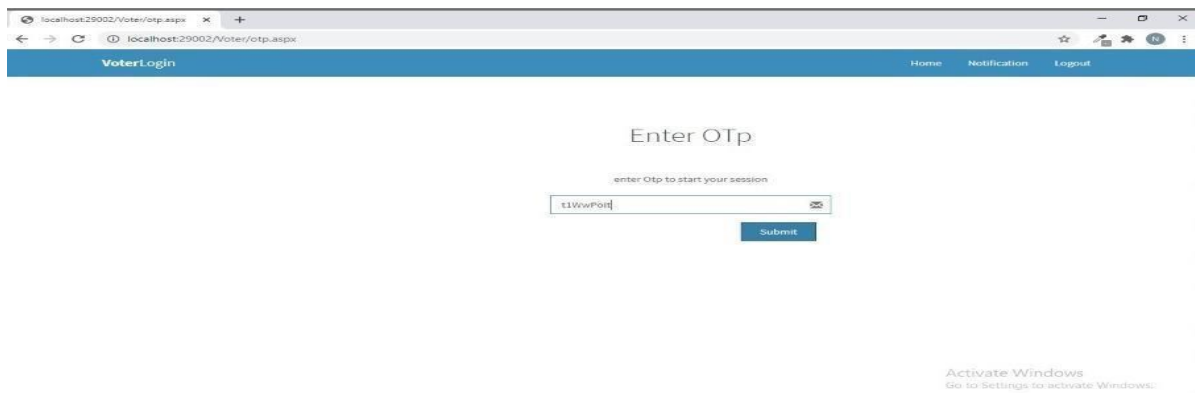


Fig:8.4: One time password

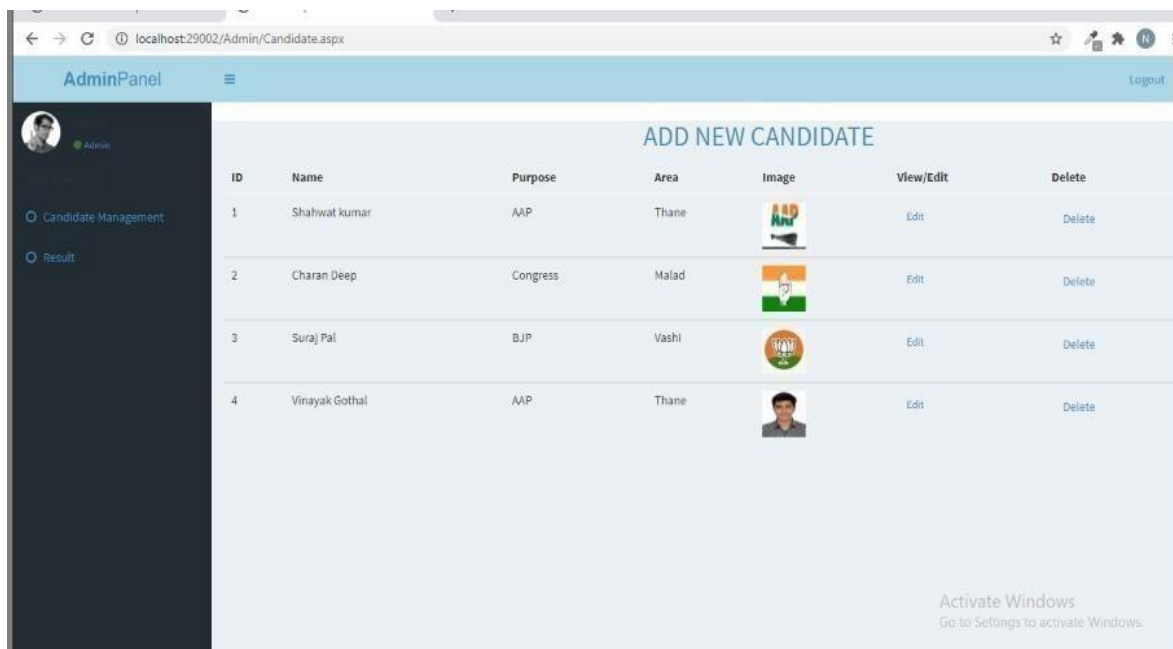


Fig:9.4: Administrator can add the candidate or delete the candidate

CHAPTER 5

CONCLUSION

Day by Day population is increasing enormously which in turn demands improvement in the current voting system. Security plays a major role in I-voting. The proposed method uses Visual cryptography to prevent the rapidly growing phishing attack. If this method is implemented, it will be useful for the voters and organization in efficiently reducing cost and time. The physically disabled and aged people can gain a significant advantage of this I-voting system and can cast their valuable votes in a secured manner for all the critical decisions of corporate companies. The proposed methodology allows a user to vote only once. It verifies whether the website is genuine or a phishing website. If the website is phishing website then it can't display the image for a user. The intruder can't enter into the system even if he knows the username.

REFERENCES

- [1]. Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE- International Conference on Communications and Computational Intelligence, 2010.
- [2]. Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.
- [3]. Ren-Junn Hwang, "A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).
- [4]. Divya James, Mintu Philip, "A novel Anti-phishing framework based on visual cryptography", IEEE 2012.
- [5]. M.Naor and A.Shamir, "Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3, No.1, 2012.
- [6]. N.P. Singh. "Online Frauds in Banks with Phishing". Journal of Internet Banking and Commerce, vol.12, 2009.
- [7]. Juan Chen and Chuanxiong. "Online Detection and Prevention of Phishing Attacks". IEEE Communications and Networking, NSFC, 2005.
- [8]. Bryan Parno, Cynthia Kuo, and Adrian Perrig. "Phoolproof of Phishing Prevention". Financial Cryptography and Data Security, Springer, 2006.
- [9]. PhishGuard.com. Protect against Internet Phishing Scams
.http://www.phishguard.com/.
- [10]. M. Jakobsson, and S. Myers: „Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft Wiley, 2010.
- [11]. M. Naor and A. Shamir, "Visual cryptography," in Proc. Advance in Cryptography (EUROCRYPT'94), 2005, vol. 950, LNCS, pp. 1–12.

APPENDIX

A.SOURCE CODE:

REGISTRATION.aspx

```
<%@ Page Title="" Language="C#" MasterPageFile="~/MasterPage.master"
AutoEventWireup="true" CodeFile="Registration.aspx.cs" Inherits="_Default" %>
<%@ Register Assembly="MSCaptcha" Namespace="MSCaptcha" TagPrefix="cc1" %>
<asp:Content ID="Content1" ContentPlaceHolderID="head" Runat="Server">
```

```
    <meta charset="UTF-8">
    <title>Sign-Up/Login Form</title>
    <link href='http://fonts.googleapis.com/css?family=Titillium+Web:400,300,600'
rel='stylesheet'
```

```
    type='text/css' />
    <link href="css/normalize.css" rel="stylesheet" />
    <link href="css/style.css" rel="stylesheet" />
    <style type="text/css">
```

```
        #table2 tr td {
            border: 1px solid black;
        }
```

```
</style>
```

```
<script language="JavaScript" type="text/javascript">
```

```
    function ss(ctrl) {
```

```
        var checkBox1 = document.getElementById(ctrl.id);
```

```
        if (confirm('Are you sure want to submit?')) {
```

```
            __doPostBack(ctrl.id, "");
```

```
        }
```

```
        else {
```

```
            return false;
```

```
        }
```

```
    }
```

```
</script>
```

```
<style type="text/css">
```

```
    #newtable {
```

```
        .auto-style1 {
            width: 217px;
        }
```

```
        .auto-style2 {
            width: 217px;
            height}
```

```

.auto-style3 {
    height: 40px;
    text-align: left;
}

.auto-style4 {
    width: 274px;
}

.auto-style5 {
    height: 40px;
    width: 274px;
}

#container {
    text-align: center;
}

.auto-style6 {
    width: 217px;
    text-align: right;
}

.auto-style7 {
    text-align: left;
}

.auto-style8 {
    text-align: center;
}

.style1 {
    text-decoration: none;
}
</style>

```

</asp:Content>

<asp:Content ID="Content2" ContentPlaceHolderID="ContentPlaceHolder1" Runat="Server">

```

<div class="wrapper col1">
</div>
<!--
#####
##### -->
<div class="wrapper col2">
    <div id="header" class="clear">
        <!--
#####
##### -->
        <div class="wrapper col3">
            <div id="featured_slide">
                <!--

```

```

#####
##### -->
    <!--
#####
##### -->
    </div>
  </div>
  <!--
#####
##### -->
    <div class="">
      <div class="clear">
      </div>
      <div class="register-logo">
        <h1 class="auto-style8">
          <a href="Login.aspx" style="color: #23395d;" class="style1">USER
LOGIN
          </a>
        </h1>
        <p class="auto-style8" style="font-size: medium; color: #FFFFFF">
          Web Security
        </p>
      </div>
      <div id="container" class="clear">
        <asp:Label ID="Label1" runat="server" Text="New User Register Here!"
Font-Bold="True"
        Font-Size="Larger" ForeColor="Black"></asp:Label>
        <table id="newtable" align="center" style="border:double;font-family:'Times
New Roman';font-weight:200;" >
          <tr>
            <td class="auto-style1"></td>
            <td class="auto-style4">
              <asp:Label ID="lblShow" runat="server"
ForeColor="Red"></asp:Label>
            </td>
            <td></td>
          </tr>
          <tr>
            <td class="auto-style2" font-size: xx-large;">Username:
            </td>
            <td class="auto-style5">
              <asp:TextBox ID="txtUsername" runat="server" Height="24px"
Width="190px"></asp:TextBox>
            </td>
            <td class="auto-style3">
              <asp:RequiredFieldValidator ID="RequiredFieldValidator1"
runat="server" ControlToValidate="txtUsername"
              ErrorMessage="Username Required"
ForeColor="#CC0000"></asp:RequiredFieldValidator>
            </td>
          </tr>
          <tr>
            <td class="auto-style6" font-size: xx-large;">Password:
            </td>
            <td class="auto-style5">

```

```

        <asp:TextBox ID="txtPassword" runat="server" Height="24px"
Width="190px" TextMode="Password"></asp:TextBox>
    </td>
    <td class="auto-style7">
        <asp:RequiredFieldValidator ID="RequiredFieldValidator2"
runat="server" ControlToValidate="txtPassword"
        ErrorMessage="Password Required"
ForeColor="#CC0000"></asp:RequiredFieldValidator>
    </td>
</tr>
<tr>
    <td class="auto-style6" font-size: xx-large;">First Name:
    </td>
    <td class="auto-style5">
        <asp:TextBox ID="txtFirst" runat="server" Height="24px"
Width="190px"></asp:TextBox>
    </td>
    <td class="auto-style7">
        <asp:RequiredFieldValidator ID="RequiredFieldValidator3"
runat="server" ControlToValidate="txtFirst"
        ErrorMessage="First Name Required"
ForeColor="#CC0000"></asp:RequiredFieldValidator>
    </td>
</tr>
<tr>
    <td class="auto-style6" font-size: xx-large;">Middle Name:
    </td>
    <td class="auto-style5">
        <asp:TextBox ID="txtMiddle" runat="server" Height="24px"
Width="190px"></asp:TextBox>
    </td>
    <td class="auto-style7">
        <asp:RequiredFieldValidator ID="RequiredFieldValidator4"
runat="server" ControlToValidate="txtMiddle"
        ErrorMessage="Middle Name Required"
ForeColor="#CC0000"></asp:RequiredFieldValidator>
    </td>
</tr>
<tr>
    <td class="auto-style6" font-size: xx-large;">Last Name:
    </td>
    <td class="auto-style5">
        <asp:TextBox ID="txtLast" runat="server" Height="24px"
Width="190px"></asp:TextBox>
    </td>
    <td class="auto-style7">
        <asp:RequiredFieldValidator ID="RequiredFieldValidator5"
runat="server" ControlToValidate="txtLast"
        ErrorMessage="Last Name Required"
ForeColor="#CC0000"></asp:RequiredFieldValidator>
    </td>
</tr>
<tr>
    <td class="auto-style6" font-size: xx-large;">Address:
    </td>

```

```
  |
```

B. SCREEN SHOTS:

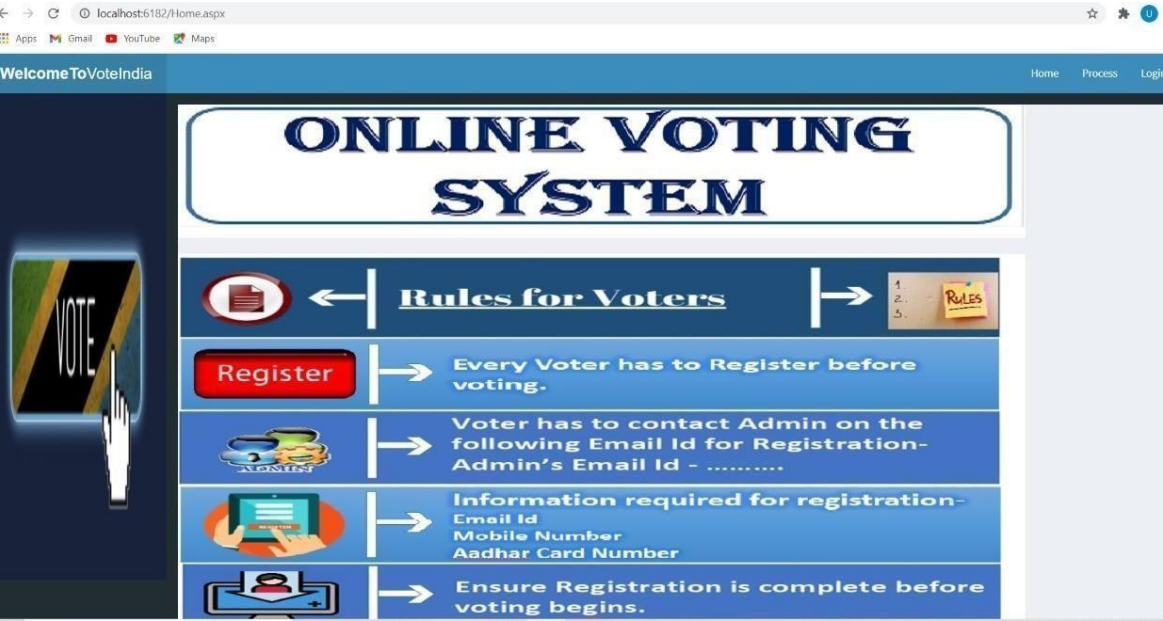


Fig:10.B: Home page

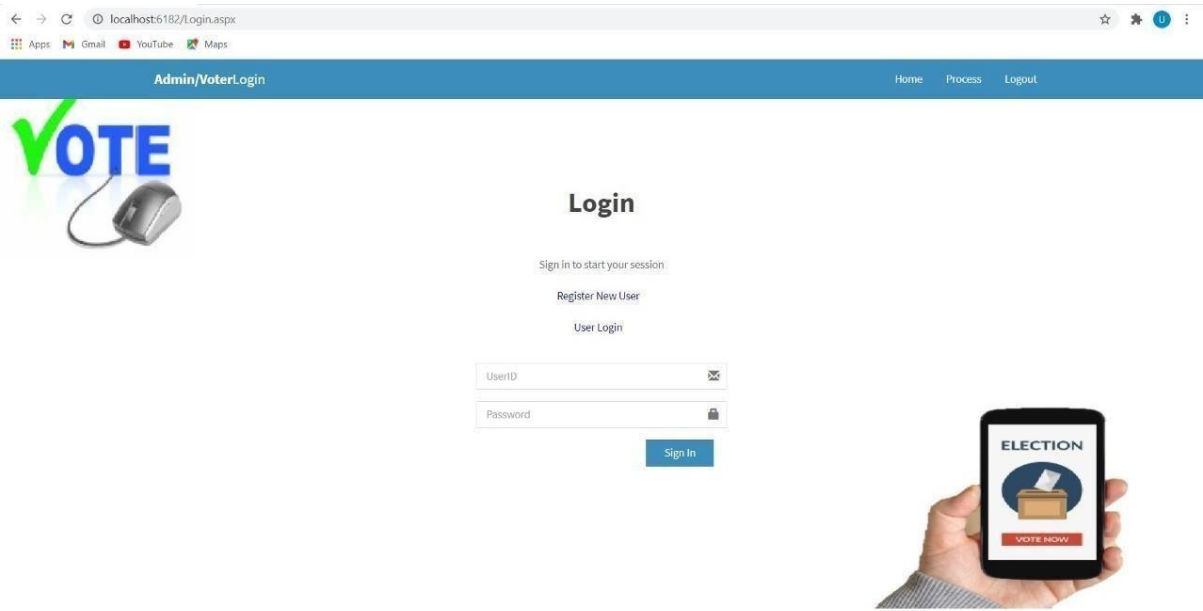


Fig:11.B: Login page

USER LOGIN

New User Register Here!

Username:

Password:

First Name:

Middle Name:

Last Name:

Address:

Email ID:

Contact No:

Aadhar No:

Enter Text:

Save Clear

Fig:12.B: New user registration

Admin/VoterLogin

Home Process Logout

VOTE

Register New User

Username:

Password:

Check Cancel

Server Image:

Upload User Image: No file chosen

Show Image

Check Captcha

ED6YC

ED6YC:

Login

ELECTION

VOTE NOW

Fig:13.B: Captcha is generated

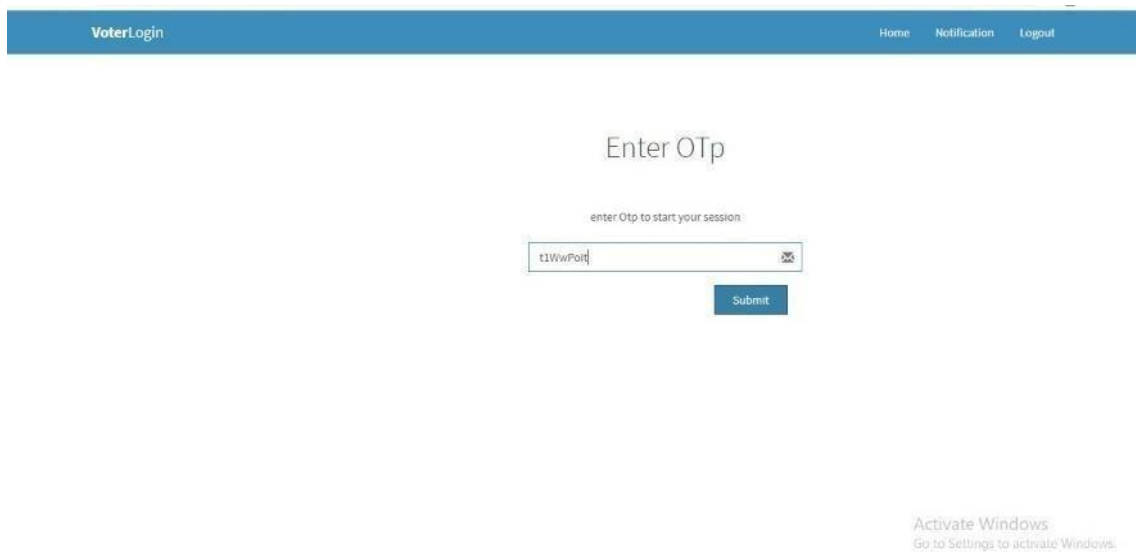


Fig:14.B: One time password is generated through mail

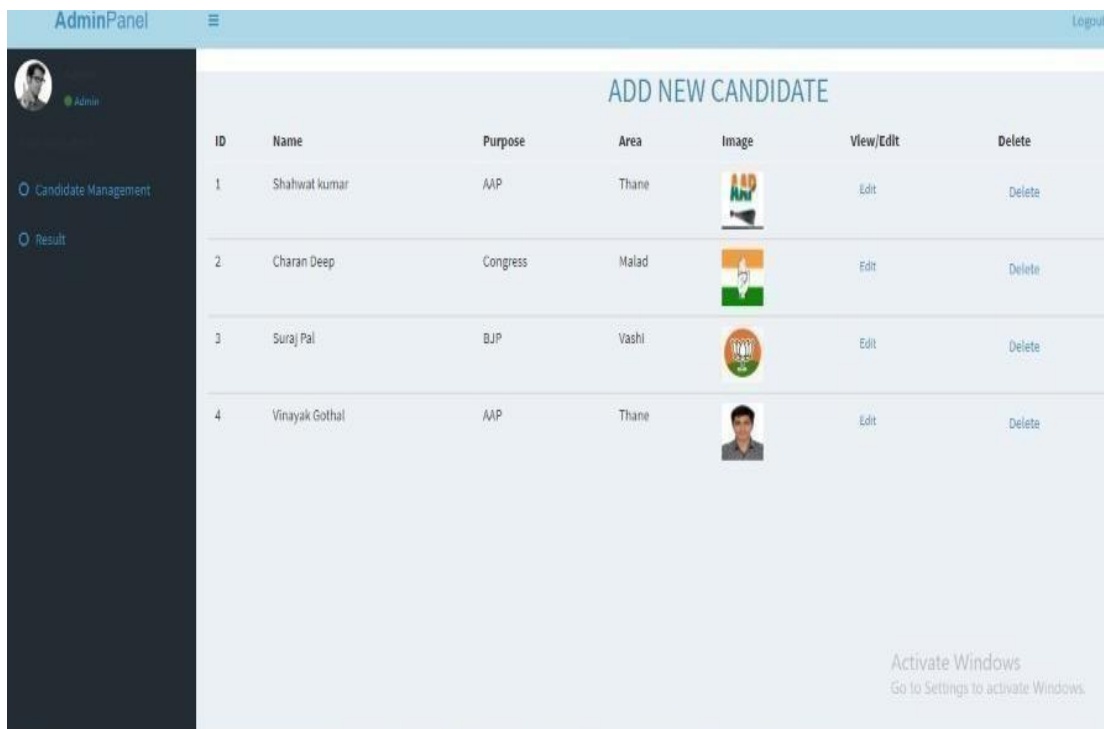


Fig: 15.B: Administrator can add the candidate or delete the candidate

C. PAPER PUBLICATION:

ANTI-PHISHING I-VOTING SYSTEM USING VISUAL CRYPTOGRAPHY

Uppada sruthi¹, Dr.S.Jancy²

Students^{1,2}, Sathyabama Institute of Science and Technology, Chennai, India

³Assistant Professor, Department of Computer Science and Engineering, SIST, Chennai, India

ABSTRACT:

In this paper we are going to perform the Anti-phishing I -voting system using visual cryptography . It is to over come the phishing attacks in voting system . In this the main objective is to vote in highly secured way to vote key1 will be generated before voting while voting key1 is merging with key2 then we get captcha . In this while key 1 is generation it is done through registration phase .In registration phase we have to fill the necessary details after filling while we are submitting key 1 is generated as an encrypted image .While user login to cast vote then in login phase key 1 and key 2 combine to form a captcha .And through mail we are getting one time password .So in secure way we are casting vote. In this Project we are using visual cryptographic algorithm , shares creation , v c scheme(2,2). Main objective of this project is about to reduce the phishing attacks in online voting system . voting can be cast secured way with generation of captcha and one time password . we build home page ,registration phase, login phase for step by step procedure.

key words : visual cryptographic , shares creation , v c scheme(2,2)

INTRODUCTION

Voting could be an important part of the democratic process. A legal system or electoral system is a methodology by that voters create a selection between options, typically in an election or on a policy referendum. A legal system contains rules for valid selection, and the way votes are counted and aggregated to yield a final result. Since voting involves counting, it's recursive in nature, and, since it involves polling the feelings of a person, this represents emotive data. Common voting systems are majority rule, representation, or plurality voting with a variety of variations and ways similar to first-past-the-post or discriminatory voting. The study of formally outlined selection systems is

termed voting theory, a subfield of political science, social science, or mathematics.

Now a days most of the voting is effected by phishing attacks to over come this problem visual cryptography plays major role . visual cryptography means image is encrypted into characters from capital A-Z and a-z , and numbers from 1-9.

There are various kinds of attacks available in networks irrespective of the types of networks. Internet is the huge and global network. There are various kinds of applications and researches emerging day to day life to satisfy the needs of users worldwide. One of them is online polling system. Many people claim the benefits it can bring such as improved speed and accuracy in counting, accessibility, voting from home and as many are worried with the risk it poses, such as unequal access, violation to secrecy and anonymity and alteration of the results of an election.

SECURITY ATTACKS

In classification security attacks, it is common to find general categories that resemble the attacker and the approaches that are used to exploit .

Phishing is one of the attacks that became famous recently. It is to identity thievery attempt in order to obtain confidential and private information of individuals or companies for monetary to gains. The image captcha is divided into two keys and one key is kept within the authentication system and the other key is sent to their corresponding users. Once the users receive their shares, they can log into the system using their own share of image captcha. The authentication system will keep one of the keys as secret and let the users to submit another key. By receiving the main key, the system will generate image captcha. When the user properly entered the image key and entered the captcha in a correct manner, he or she is let to enter into the system.

VARIOUS VOTING SYSTEMS

1. Internet voting is used, in general refers to remote Internet voting, where the client software communicates through the Internet to the server software, say, from a voter's PC. However, there are at least two and more ways to implement voting over the Internet: kiosk voting and poll-site voting. Each of these three ways has its own security requirements.

2. Paper polling system is the commonly used traditional voting system. It is widely used before the introducing of electronic voting system. Paper polling system includes casting the vote using the paper and the stamp. Each voter uses one poll and it is not shared.

3. Electronic polling system is a type of voting system which uses electronic ballot that would allow voters to cast their secret vote polling to election officials.

PROPOSED SYSTEM

In this we would like to know about the methods that are performed. Let us know about detailed. .Net includes side-by-side installations, self-contained applications, not being a component of windows operating system and many more. With Windows Forms, developers using Visual Basic

.Net can build Windows-based applications that leverage the rich user interface features available in the Windows operating system.NET, including drag-and-drop design and code behind forms. The HTML designer delivers Microsoft Intelligence statement and tag completion for HTML documents.

Back end: Back end we are using my-sql application. In this we are having relational data base, information accessibility, representation of null values, catalog faculty, data language, view updating, insert, update, delete, physical data independence, logical data independence, integrity constraints, database distribution, not subversion.

TYPES(FEASABILITY)

1. The application will require an internet connection, a device with Windows OS as the hardware for running the website successfully. Thus the website to be developed is technically feasible.

2. Operational Feasibility:

New user will register and use the system. For this a small training program is required which will include briefing the working of the system. Demonstration will be performed so that the user actually gets to know the working of the system and what they need to do. Thus the required knowledge regarding the operations will be imparted to the users.

3. Financial Feasibility:

It is concerned with the cost involved at the time of development and maintenance of the website. The overall feasibility analysis that the proposed system will be beneficial in terms of knowledge base provided as well as the cost than the older one.

4. Faster:

The time span needed for the system is less than the manual polling system.

5. More accurate:

The margin of error is greatly reduced with online surveys because participants enter their responses directly into the system. Traditional methods rely the attentiveness of staff to enter all details correctly, and naturally.

PROPOSED ALGORITHM

Visual cryptography(2,2)scheme :

In this both keys are required to reveal secret information. So key 1 is original that means key 2 will merge and get the original captcha.

Visual cryptographic algorithm:

The system involves an automatic segregator of Images which is a step-by-step process of converting any images into the required Visual cryptography formatted images. After getting the original image, the images will be combine into various shares depends on the access structure.

Shares creation:

Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and the information is obtained. A sender send the secret image which is divided into multiple shares and it holds hidden information. When all of these shares are aligned and stacked together, they expose the secret image information to the receiver.

MODULES

The modules in our project are:

Registration phase:

In registration phase we have to enter the details of ours and in this registration we are getting key1 generation as an image it is in encrypted way using visual cryptography schema we are getting captcha .while we are voting then this key 1 is merging with key 2 then generate captcha .so voting is done with highly secured way .In this administrator will send the key 1 to user .

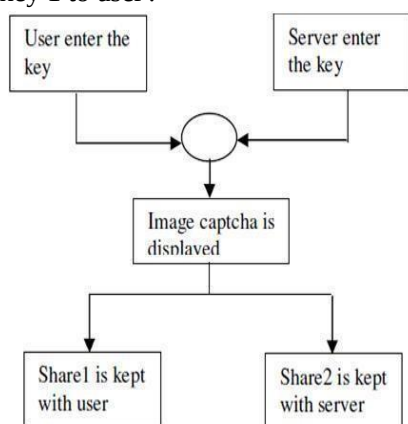


Fig.1[1] Registration phase

Login phase:

In Login phase we are having user name and password with us by registration phase so we can login through it and key 1 is merging with key 2 and generating captcha and we can vote without phishing .In this project we are having additional thing is while voting through mail we are getting password .Through this password we are highly secured while voting.

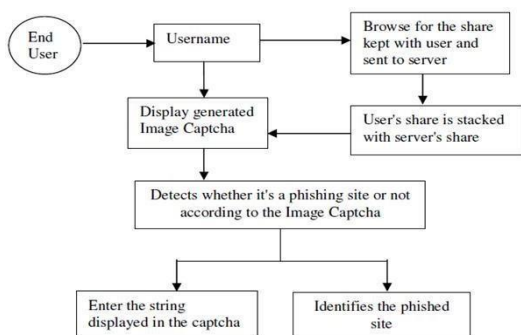


Fig.2 [1] Login phase

RESULTS & DISCUSSIONS

In this project we are implementing using VISUAL CRYPTOGRAPHIC algorithm, SHARES CREATION ,Visual cryptography (2,2) scheme.

It provides good encryption rate .It has 64 bit block size and variable key length from 32 bits. While OCR program confuse us one is character (or) not. In our method captcha consists of characters. Characters ranges from capital letters [A-Z] , small letters [a-z] , and numbers from(0-9)



Fig.3 Registration phase.

Visual cryptography(2,2)scheme : In this both keys are required to reveal secret information. So key 1 is original that means key 2 will merge and get the original captcha.

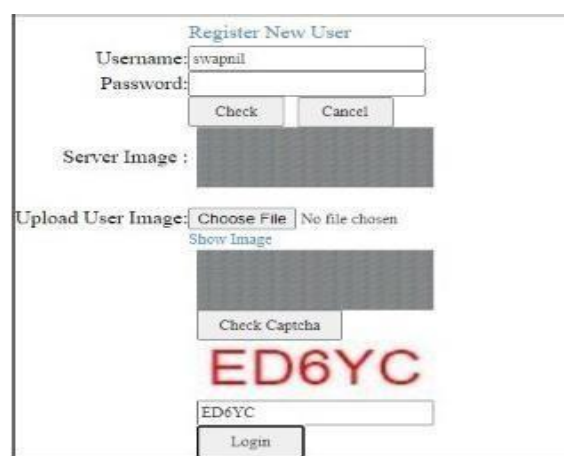


Fig.4 Login Phase(after entering into the login page)

VISUAL CRYPTOGRAPHIC ALGORITHM:

The system involves an automatic segregator of Images which is a step-by-step process of converting any images into the required Visual cryptography formatted images. After getting the original image,

the images will be combine into various shares depends on the access structure.

Fig.5 Otp is send to user mail

ID	Name	Postage	Area	Image	View/Edit	Delete
1	Shahid Kumar	BJP	Thane		View	Delete
2	Chetan Deep	Congress	Mahad		View	Delete
3	Sunil Patil	BJP	Wadh		View	Delete
4	Vijaykumar	BJP	Thane		View	Delete

Fig.6 Administration phase

SHARES CREATION:

Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and the information is obtained . A sender send the secret image which is divided into multiple shares and it holds hidden information. When all of these shares are aligned and stacked together, they expose the secret image information to the receiver.

CONCLUSION

Election plays a crucial role for any democratic country. If this proposal is implemented, then the voting percent is implemented, then the voting percent is often improved further since some percent of our citizens who are working in world- wide , and that they cannot ready to come to their native country at the time of voting. those people as well as people who are physically disabled and very old also can make use of the online voting system Since visual Cryptography Technique is employed , in this we add visual cryptographic algorithm , shares creation and visual scheme(2,2) algorithm for security

purpose so user can ready to determine whether he is in phishing site or not . Proposed online electoral system is extremely effective and it'll useful for voters.

REFERENCES

- [1].<https://jpinfotech.blogspot.com/2012/10/a-novel-anti-phishing-framework-based.html>
- [2] Thiagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE- International Conference on Communications and Computational Intelligence, 2010.
- [3] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.
- [4] Ren-Junn Hwang,"A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).
- [5] Divya James, Mintu Philip, "A novel Anti-phishing framework based on visual cryptography", IEEE 2012.
- [6] M.Naor and A.Shamir,"Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3,No.1, 2012.
- [7] N.P. Singh. "Online Frauds in Banks with Phishing". Journal of Internet Banking and Commerce, vol.12, 2009.
- [8] Juan Chen and Chuanxiong."Online Detection and Prevention of Phishing Attacks". IEEE Communications and Networking, NSFC, 2005.
- [9] Bryan Parno, Cynthia Kuo, and Adrian Perrig. "Phoolproof of Phishing Prevention". Financial Cryptography and Data Security, Springer, 2006.
- [10] PhishGuard.com. Protect against Internet Phishing Scams <http://www.phishguard.com/>.
- [11] M. Jakobsson, and S. Myers: „Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft“ Wiley, 2010.
- [12] M. Naor and A. Shamir, "Visual cryptography," in Proc. Advance in Cryptography (EUROCRYPT'94), 2005, vol. 950, LNCS, pp. 1–12.

- [13] Network Security, https://en.wikipedia.org/wiki/Network_security, accessed on May 2015.
- [14] JoeyPaquet, http://users.encs.concordia.ca/~paquet/wiki/index.php?title=Capability_maturity_model, accessed on May 2015.
- [15] Villafiorita A, Weldermariam K, Tiella R, “Development, Formal verification and evaluation of an e-voting system with VVPAT”, IEEE Transactions on Information Forensics and Security, 2009, p.no. 651-661.
- [16] Abdalla Al-Ameen and Samani Talab, “The Technical Feasibility and Security of E-Voting”, The International Arab Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.
- [17] <https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/>, Phishing attack, accessed on 12.09.2015.
- [18] M. Mounika Reddy and B.Madhura Vani, “A Novel Anti phishing Framework based on Visual Cryptography”, International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 9, Sep 2013, P.No.3434-3436.
- [19] Mayur Patil, Vijay Pimplodkar, Anuja R.Zade, Vinit Vibhute, Ratnakar Ghadge, “A Survey on Voting system techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1, Jan 2013, p.no. 114-117.
- [20] Shyong Jian Shyu, Ming Chiang Chen, “Minimizing Pixel expansion in Visual cryptographic scheme for General Access Structures”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 25, No. 9, Sep 2015.