



VC Technology in Internet Voting System

Sumit Jagtap¹, Smitesh Vichare², Alpa Vaidya³, Mangesh Jogdand⁴, Prof. Shivani Sthapak⁵

UG Students, Dept. of Information Technology, Dhole Patil College of Engineering, Pune, Maharashtra, India^{1,2,3,4}

Assistant Professor, Dept. of Information Technology, Dhole Patil College of Engineering, Pune, Maharashtra, India⁵

ABSTRACT:For the effective Taxi business we developed the fleet management system based on GPS which is important tool, as well as its useful to provide information to taxi driver for earning profit by mining the historical GPS path of the projectiles. In the literature, distance between current place and recommended place, time for next passengers and exact fare of trip these three factors provide the similar objective have been considered in different work. In this paper, in addition to this factor we added one more factor that is based on driver's experience which is most likely locations to pick up the passenger given the current passenger drop off location .the one location and another location graph model referred to as OFF-ON model is worked for define the relation between the get off location and next passengers get on location. To estimate the expected fare for a trip started at a recommended location we adopted an ON-OFF model. A real world dataset from CRAWDAD is used to evaluate the proposed system. A simulator has been developed for the simulate journey behavior of taxis in database. Our proposed system still effective on recommending better profitable cruising location.

KEYWORDS: About four key words separated by commas.

I. INTRODUCTION

THIS corporate companies, elections are conducted to elect President, Secretary and other board members. Candidates may be working across the world and it is therefore difficult for them to vote from there. A web based polling system assists the process, with security measures by which they can vote confidentially from any part of the world. In the 2001 general election in Washington State, 69% of votes cast were cast by mail. This Internet voting system provides them good solutions with security using Visual Cryptography [1, 2].

A. Internet Voting system refer as online voting system in that user's client server can connect to server system. Hence there is three way implement voting system over the internet: Kiosk, Remote, and poll-site voting. Each of these three ways has its own particular security requirements. In remote voting a third party, or the voter himself (rather than election officials) has control over the voting client and operating environment. In Kiosk voting, the voting client may be installed by election officials, but the voting environment is out of election officials control. In Poll-site voting, election officials have control over the voting client and the operating environment. The visual cryptography system develop for the mainly remote internet voting its nothing prevent being poll-site or kiosk voting, depending on the security requirements. Visual cryptography system having ability to carry out small and large-scale election procedures, or even surveys where strong security may be less of a concern. It is not unreasonable to ask that remote Internet voting be as secure as voting by mail. The authors note that although remote internet system has make large amount of attacks that may not be applicable to poll-site or kiosk Internet voting, it at least reduces the threat of insider attacks and allows less trust to be placed in the election officials.

B. To encrypt written material like printed text, hand written notes, pictures, etc. used Visual Cryptography. The decoding is done by the human visual system directly (By stacking share one over the other). For a set P of n participants, a secret image S(voter password) is encoded into n shadow images called shares, where each participant in P receives one share [5, 6]. To retrieve the image back all the participants share has to be place one over another then the image is got. VC in IVS aims at providing the voters a facility to cast their vote for the elections that are conducted. They can vote from any place without them coming to the place where the elections are conducted by using the features that are provided by VC that are implemented in IVS. The election will go on with good security measures because the voter can only vote for the candidate only if he logs into his login by entering the correct password getting by merging two blocks. IVS with 2-out-of-2 VC for an efficient authentication voting system. If hacker get one block of password for the login then he will not able to access second block as second block send on users Email-id. Thus our IVS provides two way securities to the voting system.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

II. LITERATURE SURVEY

User There are number of visual cryptography schemes in Existence. A selection are described below.

A. 2 out of 2 Visual Cryptography Scheme

In that scheme visual cryptography system can secret image will be divided in two blocks. This easiest way of kind of visual Cryptography. In these scheme we focus on security of voting as we using two share one of the get to user at the election time and second share will be send on users email id. To reveal the original image, these two shares are required to be stacked together. Table 1 represents the division of black and white pixel in this scheme [8].

















Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black				
Black				
White				
White				

Table I. THE PIXEL PATTERN FOR 2-OUT-OF-2 VC [9]

B. n out of k Visual Cryptography

In that scheme allow for divide secret image into k numbers of shares. For example, In 3 out of 6 VC scheme, any 3 shares out of 6 shares are sufficient to reveal the secret data. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption.

C. k out of k Visual Cryptography

Here original secret is divided into k number of shares and

For reconstruction of the secret, all k shares are necessary. For example, in 6 out of 6 VC scheme, Secret is revealed only after stacking all the 6 shares, where k= 6. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity.

D. Traditional voting systems

With traditional poll site voting, voters authenticate themselves by providing identification or an affirmation to a trusted poll worker; Internet-based voting offers great convenience, but does not offer such obvious authentication methods. Today, remote voting in governmental elections is done through absentee ballots that offer little security, and are slow and expensive to tabulate, and remote voting is becoming increasingly accepted and Popular [10].

III. PROPOSED SYSTEM

In With traditional voting, most voters are willing to accept this because they believe the poll workers are trustworthy. With remote voting, stronger measures are required, and it is important that the existence of those measures is clearly conveyed to voters in a way that establishes an appropriate level of trust [11].

This system has two user sessions namely Admin Session & User (Voter) Session. As soon as we run this system the home page will be displayed with the following links one for the admin session and the other for the user session The working of the system is as shown in the Fig 1.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

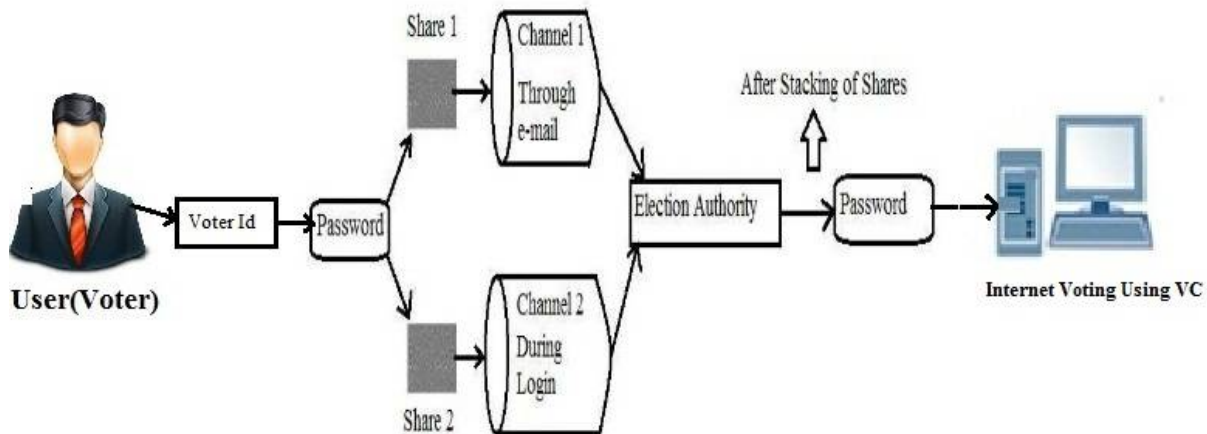


Fig. 1 Process Overview

The admin home page has the following links: User Details, Election Details, Candidate Details, Image Details, Set Password, Election Report, Change Password and Sign Out. When the admin clicks the user details link a page is displayed with the user details in a grid like having the headings as user id, user name, date of birth, cell number, address, email id etc. It consists of a button called “Add User” when admin wants to add a new user he has to press this button. Once admin has filled the relevant details he has to press command button by name register. It will check for user id validation & other validations if all the validations pass, a new user will be inserted in m_user table. When cancel is given the user is not deleted. The table used in this module is m_user. When the admin clicks the election details link a page is displayed with the election details in a grid like having the headings as election date, election name, election remarks, start time & end time. It consists of a button called “Add Election Details” when admin wants to add a new election detail he has to press this button. It will check for validations & if all the validations are correct, a new election detail will be inserted in m_election_master table. When admin presses OK button the election is deleted & admin will get the Message. When cancel is given the user is not deleted. The Table used in this module is m_election_master. When the admin clicks the candidate details link a page is displayed with the candidate details having the headings as candidate image, election details, edit & delete. In the election details column there are some more fields like name, post name, age & remarks. It consists of a button called “Add Candidate Details” when admin wants to add a new candidate detail he has to press this button. It will check for validations & if all the validations are correct, a new candidate will be inserted in m_election_candidate table. When cancel is given the candidate is not deleted. The table used in this module is m_election_candidate. When the admin clicks the image details link a page is displayed with the image details in a table like having the fields as image, image details & delete button. Under image details we have the word & the file name. It also consists of a button called “Add Image Details” when admin wants to add a new Image; he has to press this button. Another link is the set password link when this is clicked a window is displayed with two command buttons called “Set Password” & “Reset Password”. After the completion of this process set password the share 1 image will be sent to user’s email id & Click reset password button to reset the password to all the users. When the images are less than the user & we try to set the images to the users then it displays a message showing that “total images less than users or password set to all the users”. Before an election, the election officials need to generate and mail image transparencies to eligible voters. To generate them, they need a random number. The election officials generate n random voter passwords, where n is the number of eligible voters. A transparency is generated for each voter, using the result of Visual Cryptography. In addition to the image, the transparency includes the password in a human-readable and type able format. An address list of eligible voters to a third party who sends each eligible voter a randomly selected transparency along with a voter information packet including voting instructions. We rely on the integrity of the E-mail as does absentee ballots. Anyone intercepting a transparency in the mail could cast an extra vote, but there are already well-established severe penalties for e-mail tampering to deter this. As the old upset ballots method there is no prevent voters to sell our vote. A one voter can sell his own vote to other voter, who can use this vote for desire vote. In the voting process without

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

identify authentic based, it is unlikely that vote selling can be prevented. In our system we provide transparency in voting so no any voter can sell his own vote to another voter. This property could be guaranteed by requiring an open process. For instance, the placing of transparencies in envelopes could be conducted in public where voters could observe that the transparencies are selected randomly. A voter visits the election web site and enters the type able username. The election web site maintains a list of the username used to create transparency and check entered key is match with two shares or not (extensions that would allow a voter to change a previously cast vote are possible but not considered here). If the entered username is valid, the election server can calculate the corresponding transparency image. The election server then generates a random string to use as a password, and generates an image containing that string rendered as a bitmap image. The complementary image to the password image for the voter's transparency is generated and displayed on a webpage returned to the voter. After the web server displays the corresponding image generated from username, the voter combines both the transparency to reveal the password as shown in Fig 2. The user can login with the combined two shares in that one share will be generate at the time voting and second share will be already send on users Email id

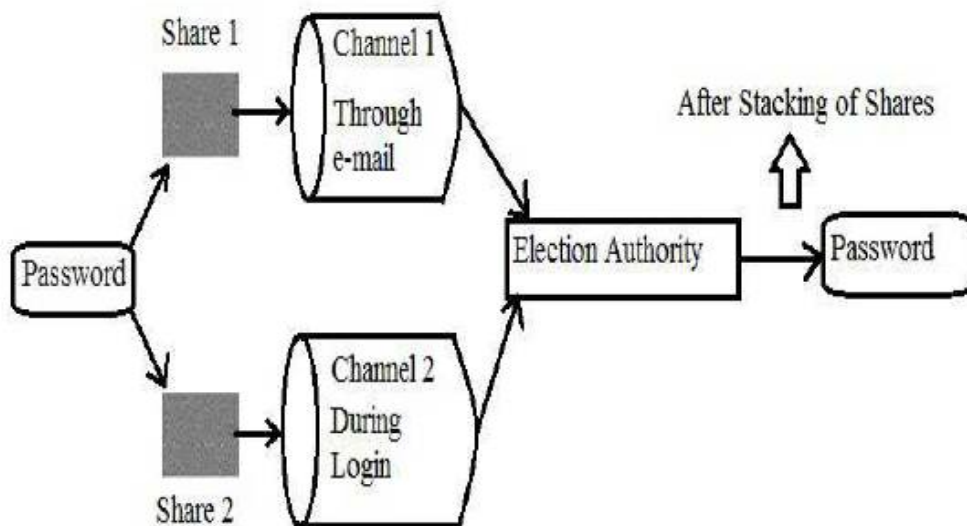


Fig 2. System Architecture

To continue the voting process, the voter enters the revealed Password. This protocol serves to both authenticate the voter to the election server and the election server web site to the voter. Only someone with the correct username transparency could decode the password in the generated image; only something with knowledge of the transparency sent to the voter could generate a sensible password image. In addition, we suspect from anecdotal evidence (but no scientific user studies yet) that nearly everyone will find the process of revealing a secret by holding a transparency up to an image on a monitor to be a satisfying and reassuring experience. previous studies have analysed how much a user needs to know in order to make rational decisions in the security of computer services, and the users showed they did not have a solid grasp on the security aspects of the system. With our system, voters do not need to understand how visual cryptography works, but are directly involved in performing the decryption in an intuitive and physical way. Our authentication scheme ensures that the voter cannot continue with the voting process without also verifying the server is legitimate. The admin is only responsible for creating the users by using the add user option, he has the right to edit the information of any users that are created & also he can delete the users from a list of users that have been created. The access rights for the admin are for the following links. The links are user details, election details, and candidate details, image details, set password, election report, change password and sign out. These links can only be accessed by the admin and none other person. The admin can view and alter the details of user, election, candidate and the images that

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

are used. Admin has the option to set the password for the users and also change the password; Admin can view the election details.

IV. EXPERIMENTAL RESULTS

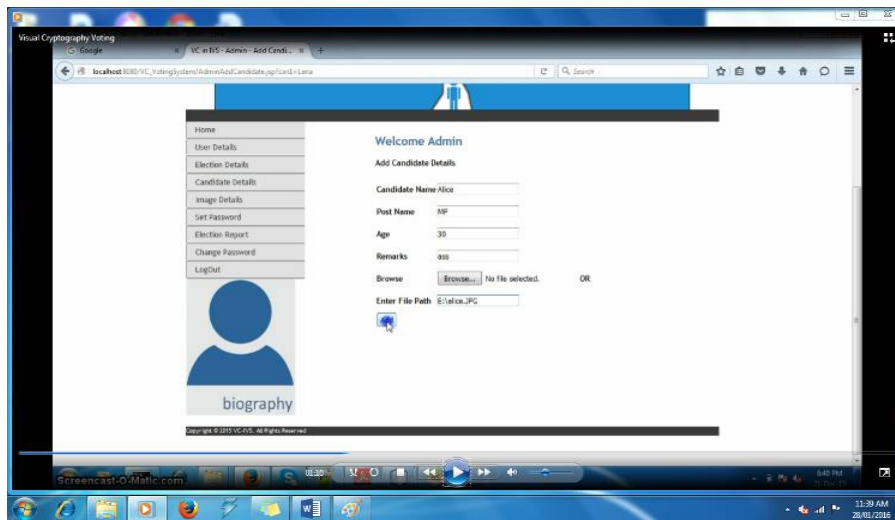


Fig 3. Candidate Registration

Admin can registered the Candidate details and add the image.

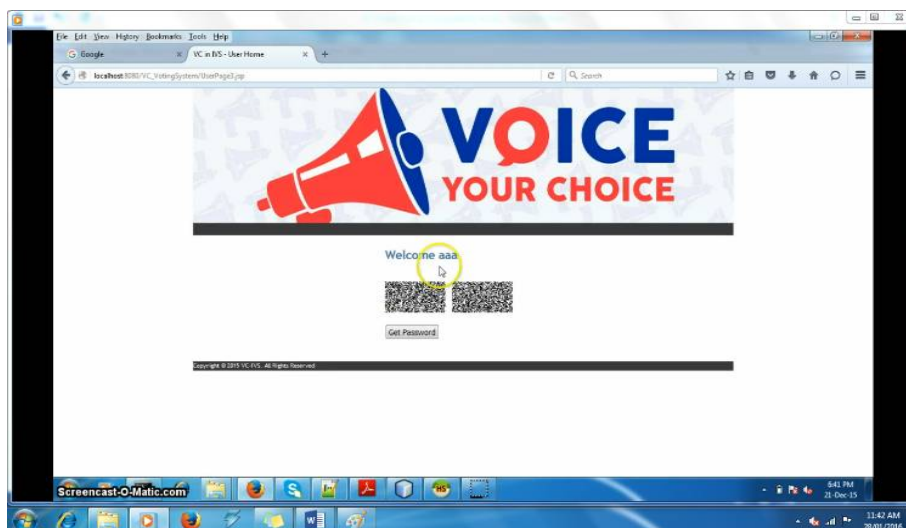


Fig 4. Add Image

In image first image will be send on mail and user get second image.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

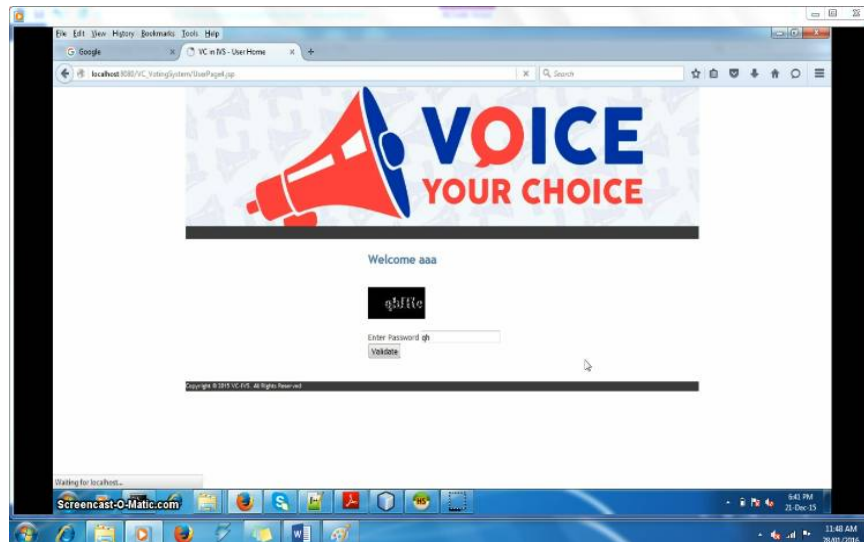


Fig 5. Voting Password

In above image User get password for secure voting

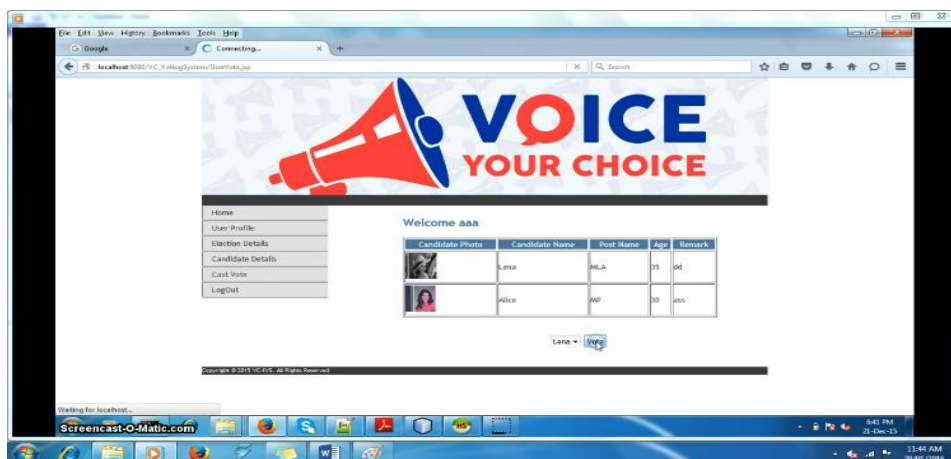


Fig 6. Display candidate details

Display all available candidate details.

V. CONCLUSION

In This system is designed for corporate companies to conduct their elections for different posts such as the presidential election, manager election etc. even companies branches spread in different countries then also all members can voting easily and effectively in a proper manner by using this Internet based voting system using visual cryptography because the voter can vote from the place where he is working by using this system .This can also be used for conducting the elections in Clubs like Country Club, Country Vacations etc. It can be converted for public elections and also parliament elections. Proposed online voting system is very effective and it will be useful for voters and organization in many ways and it will reduce the cost and time. Internet-based voting offers many benefits including low cost and increased voter participation. Voting systems must consider security and human factors carefully, and in particular make sure that they provide voters with reliable and intuitive indications of the validity of



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

the voting process. The system we propose uses visual cryptography to provide mutual authentication for voters and election servers.

REFERENCES

1. Adi Shamir (1979), "How to share a Secret", Communications of the ACM, pp .612-613.
2. M. Naor and A. Shamir (1995), "Visual Cryptography", Advances in Cryptology-Eurocrypt '94 Proceeding, LNCSvol. 950, Springer-Verlag, pp. 1-12.
3. Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, (2012) "Attacking the Washington, D.C.Internet Voting System", In Proc. 16th Conference on Financial Cryptography & Data Security,pp.1-18
4. Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdurrahman Dawood (2012), "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp. 428-434.
5. Adhikari Avishek and Bimol Roy (2007) "Applications of Partially Balanced Incomplete Block Designs in Developing (2,n) Visual Cryptographic Schemes". IEICE Trans. Fundamentals, Vol.E90-A, No.5 ,pp. 949-951
6. Marek R. Ogiela, Urszula Ogiela(2009) "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1,pp. 33-40
7. Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme".pp. 1-28
8. Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471.
9. A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160.
10. Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250-251.
11. Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9
12. 2014 "Electronic Medical Report Security Using Visual Secret Sharing Scheme", IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83

BIOGRAPHY

Mr. Sumit Jagtappursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Mr. Smitesh Vicharepursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Miss. Alpa Vaidypursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Mr. Mangesh Jogdandpursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Prof. Shiwani Sthapakis an Assistant Professor in Department of Information Technology in Dhole Patil College of Engineering, Pune, Maharashtra, India.