Visual cryptography in internet voting for extended security

Archana P.S, Ambily O.

Department of computer Applications, K.V.M college of engineering&IT,INDIA

archanaps92@gmail.com

Abstract— India has an asymmetric federal government, with elected officials at the federal, state and local levels. At the national level, the head of government, Prime Minister, is elected by members of the Lok Sabha, the lower house of the parliament of India. The elections are conducted by the Election Commission of India. All members of the Lok Sabha, except two who can be nominated by the President of India, are directly elected through general elections which take place every five years, in normal circumstances, by universal adult suffrage and afirst-past-the-post system.] Members of the Rajya Sabha, the upper house of the Indian parliament, are elected by elected members of the legislative assemblies of the states and the Electoral college for the Union Territories of India.

2015 general elections involved an electorate of 863,500,000 people {including all peoples above 18 years } (larger than both EU and US elections combined). Declared expenditure has trebled since 1989 to almost $300 million, using more than one million electronic voting machines. The size of the huge electorate mandates that elections be conducted in a number of phases (there were nine phases in the 2014 general election). It involves a number of step-by-step processes from announcement of election dates to the announcement of results paving the way for the formation of the new government.

This paper named “Visual cryptography in internet voting for extended security” as the name indicates is a visual cryptography implementation which aims in automating the voting process so that the user can vote from his/her home ,office or anywhere without any geographical restrictions. To ensure secrecy the paper in cooperates the advantages of steganography and visual cryptography together. The secret password is embedded inside an image which is split into two shares.User on entering both the shares correctly can go for voting. Another feature is that the complex tasks going behind the project is hidden from the user so that the system becomes so user friendly.

Keywords----– Biometrics**,** Internet Voting System (IVS),I-voting, Visual Cryptography (VC*)*,E-voting,2-2 visual cryptography scheme- n-k visual cryptography

INTRODUCTION

Elections are conducted in small scale organizations, corporate institutes and on a larger scale, in parliaments too, for appointing board members of that organizational body. These elections restrict the voters to be present at that voting location thus causing inconvenience. This causes an alarming need to bring remote voting systems to effect. Internet voting system using visual cryptography fulfills this need of being able to vote from anywhere without causing security concerns. Almost all fields of life are now automated. But still people have to wait in long queues to do their fundamental right voting. This paper aims in making the voting more secure and effective at the same time making it available for people from any geographical location.

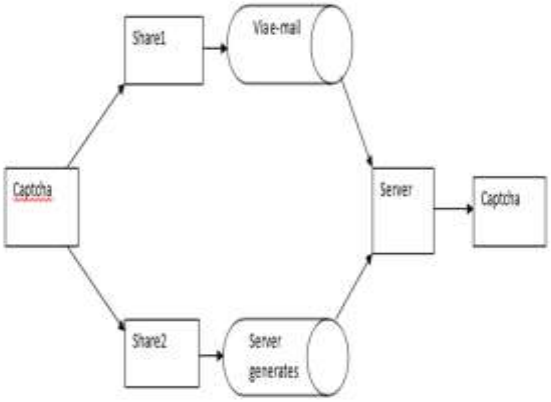
1.1 Internet Voting System

Internet voting system enables a voter to vote over the internet while providing accuracy and security. Internet voting system can be of two types-Poll-site and remote voting. Poll-site voting enables the voter to vote over the internet, at a voting poll. Remote voting enables the voter to vote from anywhere around the globe thus removing geographical restrictions .

1.2 Visual Cryptography

Visual cryptography is an encryption technique that encrypts data using secret key. The encrypted data can be decrypted using human visual system. Thus decryption can be done by someone without the knowledge of cryptography and does not require any decryption algorithm .

Pixel colour	Original pixel	Share 1	Share 2	Share1 + Share 2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■



MATERIALS AND METHODS

II. INTERNET VOTING SYSTEM USING VISUAL CRYPTOGRAPHY

There are number of visual cryptography schemes as follows.

2.1 Two out of two visual cryptography scheme

In this type of Visual cryptography scheme, the secret image is divided into two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with IVS that uses 2 out of 2 Visual secret sharing schemes for authentication purpose. To reveal the original image, two shares are required to be stacked together.

2.2 n out of k visual cryptography scheme

This type of visual cryptography scheme divides a secret image into k number of shares. Then the secret image can be revealed from any n number of shares among k. 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 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

2.3 k out of k visual cryptography scheme

In This type of visual cryptography scheme secret is divided into k number of shares and for reconstruction of the secret image, all k shares are required. 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.

A voting system should be fair enough for both political parties and voters. There are some characteristics of voting system that are as follows-

Authentication: Only authorized voters should be able to vote.
Uniqueness: No voter should be able to vote more than once.
Accuracy: Voting systems should record the votes correctly.
Integrity: Number of casted vote must not be modified.
Verifiability: Possible to verify that votes are correctly counted in the final tally.
Auditability: Reliable and demonstrably authentic election records.
Reliability: Systems should work robustly, even in the face of numerous failures.

This system is developed with due attention to secrecy. User once registered is verified by the admin on validating his ADHAAR CARD.The step by step procedure can be shown as

1.USER REGISTERS

2.ADMIN VIEWS USERS APPLICATIONS

3.HE CROSS CHECKS IT WITH THE IDENTITY PROOF SUBMITED BY USER.

4. IF FOUND VALID HE/SHE IS APPROVED FOR VOTING

5 USER LOGS IN WITH HIS/HER PASSWORD AND USER ID

6.USER DOWNLOADS SECURITY IMAGE

7.USER DOWNLOADS SECURITY IMAGE SEND TO HIS/HER EMAIL ID

8.UPLOADS BOTH SHARES

9.ADMIN CHECKS WHEATHER THE IMAGE SHARES ARE CORRECT(VISUAL CRYPTOGRAPHY)

10.USER MAKES HIS/HER VOTE

12.USER IS NOT ALLOWED TO VOTE AGAIN

13.USER LOGS OUT AND CAN VIEW THE RESULT ONCE IT IS PUBLISHED

AADHAAR

Aadhaar is a 12 digit individual identification number issued by the Unique Identification Authority of India(UIDAI) on behalf of the Government of India. Each individual needs to enroll only once which is free of cost. Each Aadhaar number will be unique to an individual and will remain valid for life. Aadhaar number will helps to provide access to services like banking, mobile phone connections and other Government and Non-Government services. Biometric data like fingerprint, iris and palm geometry face is stored in database of Aadhaar. This number will serve as a proof of identity and address, anywhere in India. Any individual, irrespective of age and gender, who is a resident in India and satisfies the verification process laid down by the UIDAI, can enroll for Aadhaar.

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who make it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to undertake this project. We have a great pleasure in presenting the paper “visual cryptography in internet voting for extended security” under the guidance of Miss:Ambily O.A and for giving us an opportunity to work on this topic. Her encouraging words went a long way in providing the patience and perseverance, which were needed to complete this project successfully. Also her true criticism towards technical issues provided us to concentrate on transparency of our project. We would like to express our gratitude to DR.SV Murugadas, Principal of K.V.M College of Engineering & IT and Prof.S Nagarao, Head of Department of computer applications for their support and guidance.Finally we express our sincere thanks to our parents and all those who helped us directly or in directly in many ways in completion of this paper.

CONCLUSION

The designed system is used in election processes in clubs, corporate organizations, government elections etc in various forms. The system uses two way authentication as the authentication process is performed on the server side as well as the client side thus providing greater security. The electronic voting system has several advantages like allowing remote voting which removes geographical restrictions to the voter. The encryption technique that is used in our system is visual cryptography which makes use of encrypted shares and decryption is done by human visual system which reduces difficulties in decryption.

REFERENCES:

[1] Rajendra A B and Sheshadri H S, Visual Cryptography in Internet Voting system, *IEEE*, 2013 ,
Arti Bhise, 2Namrata Borate ,3Aarti Garje,4Yogita Karkal,Secure internet voting,IJES

[2] Anusha MN Srinivas B K., Remote Voting System for Corporate Companies using Visual Cryptography*, International Journal of Advanced Research in Computer Science and Software Engineering Research, Volume 2*, Issue 6, June 2012

[3] Puja Devi Rana, Anita Singhrova, Suman Deswal Design and Implementation of K-Split Segmentation Approach for Visual Cryptography, *International Journal of Scientific and Research Publications*, *Volume 2*, Issue 8, August 2012

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi, Online Voting System Powered By Biometric Security Using Steganography, *IEEE*, 2011

[5] J. Alex, Halderman Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer1 Drew Springall,
Security Analysis of the Estonian Internet Voting System, May 2014

[6] Kohno, Tadayoshi, et al. "Analysis of an electronic voting system." *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*. IEEE, 2004.

[7]http://newindianexpress.com/states/andhra_pradesh/Maoists-strike-fear-make-off-with-poll-papers-in-agency/2013/07/15/article1684243. ece

[8] Executive Summary of "Genesis and Spread of Maoist Violence and Appropriate State Strategy to Handle it", Bureau of Police Research and Development, Ministry of Home Affairs, New Delhi

[9] Dill, David L., Bruce Schneier, and Barbara Simons. "Voting and technology: who gets to count your vote?." *Commun. ACM* 46.8 (2003): 29-31

[10] Jefferson, David, et al. "Analyzing internet voting security." *Communications of the ACM* 47.10 (2004): 59-64.

[11] Evans, David, and Nathanael Paul. "Election security: Perception and reality." *IEEE Security & Privacy Magazine* 2.1 (2004): 24-31.

[12] Agarwal, Himanshu, and G. N. Pandey."Online voting system for India based on AADHAAR ID." *ICT and Knowledge Engineering (ICT&KE), 2013 11th International Conference on*. IEEE, 2013.

[13] Zissis, Dimitrios, and Dimitrios Lekkas. "Securing e-Government and e-Voting with an open cloud computing architecture." *Government Information Quarterly* 28.2 (2011): 239-251.

[14] Agarwal, H., & Pandey, G. N. (2013). Impact of E-Learning in Education.*International Journal*.

[15] SusheelKumar, K., Vijay Bhaskar Semwal, Shitala Prasad, and R. C. Tripathi. "Generating 3D Model Using 2D Images of an Object." *International Journal of Engineering Science and Technology (IJEST)* 3, no. 1 (2011): 406-415.

[16] Castillo, Jose Miguel, et al. "Prospecting the future with AI." *International Journal of Interactive Multimedia and Artificial Intelligence* 1.2 (2009).

[17] SusheelKumar, K., Vijay Bhaskar Semwal, Shitala Prasad, and R. C. Tripathi. "Generating 3D Model Using 2D Images of an Object." *International Journal of Engineering Science and Technology (IJEST)* 3, no. 1 (2011): 406-415.

[18] Vishwanath Bijalwan,Vinay Kumar, Pinki Kumari,Jordan Pascual," KNN based Machine Learning Approach for Text and Document Mining" International Journal of Database Theory and Application Vol.7, No.1 (2014), pp.61-70.

[19] Pinki Kumari and Vikas Pareek, RAKSHITA- A Novel web based Approach for Protecting Digital Copyrights Using Public Key Digital Watermarking and Human Fingerprints" International conference on methods and models in computer science (ICM2CS-2010).

[20] K. S. Kumar, V. B. Semwal and R. C. Tripathi, "Real time face recognition using adaboost improved fast PCA algorithm", arXiv preprint arXiv:1108.1353, (2011).

[21] K. S. Kumar, S. Prasad, S. Banwral and V. B. Semwal, "Sports Video Summarization using Priority Curve Algorithm", International Journal, vol. 2, (2010).

[22] K. S. Kumar, V. B. Semwal, S. Prasad and R. C. Tripathi, "Generating 3D Model Using 2D Images of an Object", International Journal of Engineering Science, (2011).