Secure Online Voting System Using Visual Cryptography

Prof S.H. Dinde1, Himani Hemant Jain2, Prachi Deepak Vernekar3, Julia Sanjay Yadav4, Neha Ramesh Tejwani5, Aishwarya Sanjay Khanjire6

1Assistant Professor, Computer Science and Engineering Department Sanjay Ghodawat Group of Institutions, Atigre, Kolhapur, India.

2,3,4,5,6 UG Scholars, Computer Science and Engineering Department Sanjay Ghodawat Group of Institutions, Atigre, Kolhapur, India.

Abstract

Visual cryptography is a technique of encrypting the image in such a way that the original image can be obtained if correct share is provided. Visual cryptography enables security to the system. Share is generated by selecting random pixels from original image. The share is generated in such a way that original image cannot be predicted. Visual cryptography enables security and privacy to the system. Visual cryptography in online voting system provides simplicity in voting process. It is easy and efficient to handle. Voting can be done from any place. Election will be conducted online with security. id and password are needed to login into account. User can login into account any time and make changes into account details; Only during voting process user must upload secret security share which is received during registration. Only if correct share is uploaded then vote can be casted. System will allow voter to vote only once Hence visual cryptography in voting system enables security and authenticity which enables secure and easy-to-use interface to users.

Index Terms—Visual cryptography, security share, voting system.

1. INTRODUCTION

Elections are conducted everywhere, but voters must go to polling booth to caste vote. Election process is very complex and requires a lot of things to be done prior to voting. There are a lot of arrangements to be done. It includes a lot of manual work. Elections are conducted area wise in government elections. To caste vote, voter must be present at voting site. This may decrease voter participation Online voting makes this task easy. visual cryptography adds security in voting. It is important to implement such systems. this will reduce manpower, make voting easy to use and efficient. People must be present on site to cast vote. Visual cryptography is a technique of encrypting image. In this system, user will be asked to upload a security image during registration. User will receive security share of security image via email. This share will be in encrypted format. User can login to system any time to edit voter details. Only during voting, user must upload security share. If share is incorrect, voting cannot be done. Since security share is generated by using random pixels, the actual image cannot be predicted. Also, the share cannot be obtained by any other user or unauthorized person since it will be securely sent through email. Voting will be successful only if correct share associated to that user is uploaded.

2. SURVEY OF PREVIOUS WORK

A. Visual cryptography for gray-level images

A (*k*, *n*)-threshold visual cryptography scheme is proposed to encode a secret image into *n* shadow images, where any *k* or more of them can visually recover the secret image, but any *k*−1 or fewer of them gain no information about it. The decoding process of a visual cryptography scheme, which differs from traditional secret sharing, does not need complicated cryptographic mechanisms and computations. Previous efforts in this topic are almost restricted in processing binary images, which are insufficient for many applications. Instead of using gray sub pixels directly to construct shares, a dithering technique is used first to convert a gray-level image into an approximate binary image. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The overall effect of the proposed method is the achievement of visual encryption and decryption functions for gray-level images only.

B. Visual Cryptography Scheme for General Access Structure

In (k, n) visual cryptography scheme, all n shares have equal importance. Any k out of n shares can reveal the secret information. It may compromise the security of system. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information. But the main disadvantage of this scheme is that it takes lot of memory to store the all shares.

C.Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of b bits is distributed among n shares of size at least b bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most 1/k bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is nearly100%.

D.Multiple Secret Sharing Scheme

All the previous researches in visual cryptography were focused on securing only one image at a time. This visual cryptography scheme is to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by rotating A by 90 degrees anti-clockwise. This scheme has multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares.

E. Extended Visual Cryptography Scheme

In traditional visual cryptography scheme, shares are created as random patterns of pixel. These shares look like a noise. Noise-like shares arouse the attention of hackers, as hacker may suspect that some data is encrypted in these noise-like images. So, it becomes prone to security related issues. It also becomes difficult to manage noise-like shares, as all shares look alike. An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

F. Progressive Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, it is not possible to recover the secret image though one less than k shares are available. In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases. K. Region Incrementing Visual Cryptography Scheme In traditional visual cryptography scheme, one whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So, it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply same encoding rule to all pixels. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion.

3. PROPOSED SYSTEM

A. METHODOLOGY

The proposed system has Admin, Officer and User Session. Once we install this system and run this system the home page will be displayed having links as login and registration.
The working of user session is shown in fig.1

The proposed approach consists of three modules which are:

a. User Module

There are two users as candidate and voter. There are different Candidates who stand for the election from different areas and are selected by the admin. If a candidate wants to stand for election he can register into the system and create his profile. The details are further verified and validated and then added to the system. There are two phases using which the voter interacts with the system.

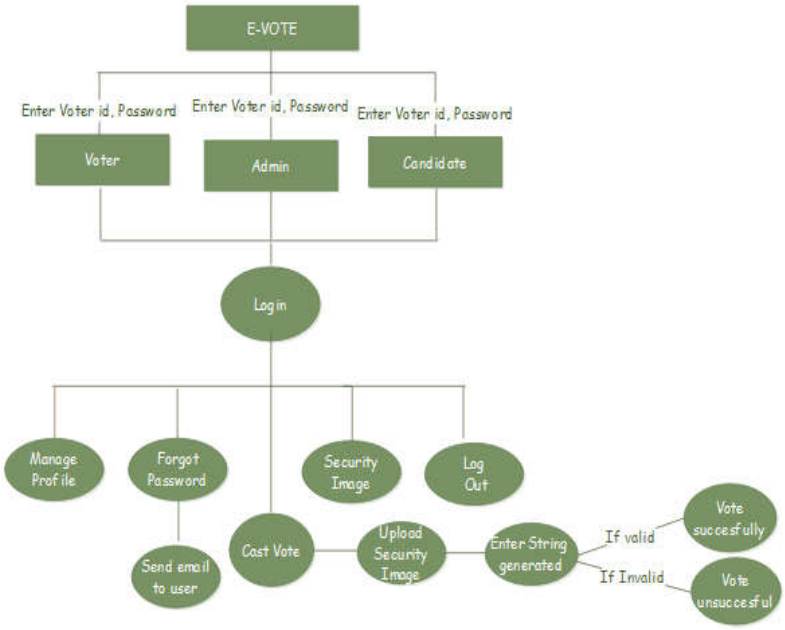

Fig 1: Data Flow of the system

.

i. Registration Phase

The user first must register and fill his personal details like Name, Address, city, state, pin code, profile photo, Date of birth, unique voter id along with his email-id and password. To be eligible for voting, the user must be above 18 years of age. The user is first validated and then details are stored in the database. Then the user is asked to upload his security image. A random string is added to the image and then the image is divided into shares such that one share is send to the user's email-id and original image is kept in the server database along with random text. The voters share is sent to the voter via his/her registered email id which is used for later security purpose during voting.

ii. Login Phase

The user can log in by entering his voter-id and password. The User has the right to log into the system anytime to see his profile or change personal details. The vote button will be active only during voting period using which the user can cast his vote. During the voting procedure, the user must first upload his share which was send him during registration phase on his registered email-id. After the share is uploaded, it is checked and compared with the original image stored in database for that user. The image along with text stored in the database for that user is displayed to the user. Here the end user can verify whether the displayed image matches with the image uploaded at the time of registration. The user is required to enter the text which is displayed on the image and this can serve the purpose of password and using this, the user can cast his vote.

b. Admin Module

The Admin can log into the system by entering correct voter-id, password and see his profile. The admin home page consists of following links: Link to add, remove and edit voter, Link to Add, Remove and edit officer, Link to add, remove and edit candidate, link to add the election details. The details about election is published by admin. Admin can add candidates and in case if fraud is found remove candidates. Displaying the results by counting the votes will be done by admin and respective officer. The admin can add election details by clicking on election details link where he must add the election name, name of the candidates, name of the city, state, country and date of election. By selecting remove election, admin can even delete an election which is old. The admin can add candidate details by clicking on candidate details link where he must add the candidate name, name of the election, name of the city, state, country and date of election. After validating and checking the details it can be added to database. Voter is added by admin by using add voter option, he can also change the details of voter if voter edits his profile he can also remove the voter from the list of voters created.

c. Officer module

Officer is responsible for conducting the region wise election so that the election will be conducted in ease. Each city will have an officer who is responsible for conducting and dealing with the elections held in that area. Officer manages the candidates and voters of that region. Admin handles all the officer and is responsible for adding and removing them. Officer dashboard will have links as add, remove and edit candidate. Link to add, remove and edit voter. Link to add, edit and remove election.

B. VISUAL CRYPTOGRAPHY FOR SECURITY IMAGE:

The voter uploads his security image during the registration phase, which is then sent to server. At server side, first a random string is embedded in the image and then the system generates share of the image by selecting random pixels from X and Y axis of original image using a random number generator. The random string is also stored in the database. The generated share is sent to the voters registered email id which will be used as a security image by voter to casts his vote.

During the voting period, the user has to login into the system using his voter-id and password. The user can see his profile after he logs in successfully. During the voting period, the user first uploads his security image which was sent to his email. After uploading the security image. the server compares that image with original image stored in the database by that voter-id. By using random number, the images are compared and if it is valid, the stored random text will be displayed on that image. The voter must type that text which serves as one-time password to successfully casts his vote. After casting his vote, the image is invalidated in the database of the system so that voter cannot use the same image and casts his vote twice.

In this way, voting can be done in a secure and efficient manner using visual cryptography.

4. ALGORITHM

A. Image Division and text generation:

Step 1: Input the security image uploaded by the user.

Step 2: Create a variable in php to store the final image using image create () with the same dimensions as the user's image.

Step 3: Create a variable to store random text using random_string() function.

Step 4: Add that text to the uploaded image.

Step 5: Generate a random number to skip the pixels to generate a random image.

Step 6: Now scan the original pixel by pixel in a loop by skipping the pixel row wise using the random number generated and get the color to that pixel with imagecolorat ().

Step 7: Set the same color of the new image at the same pixel position using imagesetpixel()

Step 8: After the end of the loop send the new image to the user with email and store the original image with the random number generated

B. Image Compare:

Step 1: Input the part of security image uploaded by the user.

Step 2: Get the stored security image and random number stored while dividing the image.

Step 3: Now scan the original pixel by pixel in a loop by skipping the pixel row wise using the random number generated and get the color to that pixel with imagecolorat ().

Step 4: Compare the percentage of pixels of original image and the uploaded image.

Step 5: If percentage of comparison of uploaded image and original image is greater than 96% then success.

Step 6: If pixel didn't match give error else end.

5. ADVANTAGES OF PROPOSED SYSTEM

User login is safe and secure. Voters can vote from any place. voter can login to account, only during voting, voter must upload security share which is sent to registered email id during registration. If uploaded image is correct, then vote can be casted after entering the text generated on image. in this system, the system is secure, and all user details are confidential a secure It will be easy to keep track of

voters. this system Will allow voters to easily cast their votes this system is efficient to use. It would be easier for those in remote locations to vote.

6. RESULT ANALYSIS

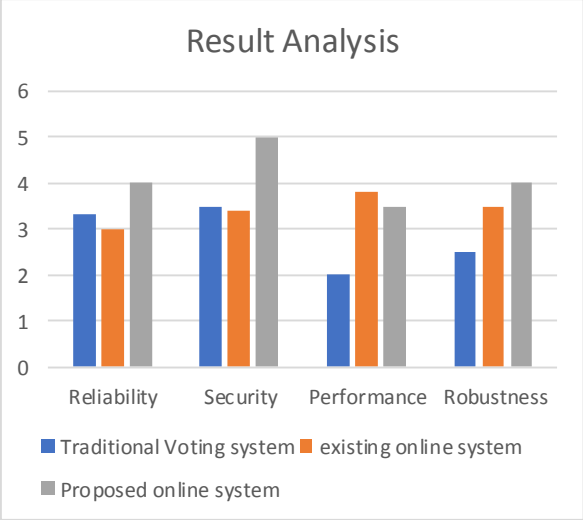

Fig 2: Comparison between Traditional, Existing and proposed system

The system has reasonable short time response. The voter can login and is able to get response for his requests in 2-3 seconds which is robust compared to earlier system. All the passwords that are generated or accepted is stored in database in an encrypted form compared to existing system where it may be stored as it is thus vulnerable to attacks. As the voting is done only if user uploads correct share and thus enter the correct strings which serves as tight security for voting system and provides enhanced security. In election Mode the system is 99% reliable providing high performance. To prevent data loss in case of system failure, the result of votes is polled till then they are saved in database and the system recovers itself from previous crashes and continue the voting process providing high reliability.

7. CONCLUSION

This system enables us to conduct voting process. Various elections can be conducted using this system. This includes various government elections. Area wise voting can be done in easy and efficient manner. Voting can be done from any place. The system enables security through visual cryptography technique. Voting can be done only if correct security share associated to that user is uploaded. Visual cryptography technique adds a layer of security to the voting process.

We access internet almost daily to carry out various tasks, so online voting will enable maximum participation. The proposed system provides security to users. It has several layers of security. User can login only if correct id and password is entered. user can vote only if correct security image associated to that account is uploaded. Text is generated on image which can be entered by end user and voting can be done.

8. 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-Euro crypt '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 .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, Urs zula 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