Prevention of Phishing Attack in Online Voting System by using Visual Cryptography

Vaibhavi Vitthal Kulakarni
Department of Computer Science and Engineering,
AIET, Mangalore, India

T S Kusuma Sri
Department of Computer Science and Engineering,
AIET, Mangalore, India

Asst prof. Tahir Naquash H B
Department of Computer Science and Engineering,
AIET, Mangalore, India

***Abstract* - As per the survey conducted only few people go for voting because of their tight schedule. There are many reasons, few may be everyone has to go to voting center, they have to stand in a long queue, they will be tired because of their tight schedule. So we have proposed an online voting system that make use of internet, the possibility of cheating/threats has been increasing day by day. One such problem is phishing attack which can create problems in authentication. So, we have implemented secured online voting system using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions.**

Keywords—Authentication, cryptography, image captcha, phishing, integer linear program, online voting.

I. INTRODUCTION

Due to rapid increase in the of internet usage, sharing of information on the internet has started, however they are unaware that the network on which they are sharing files is secure or not. So information security becomes a very important issue nowadays [1]. Phishing is identified as a major security threat identified is phishing [2-4] every moment a new technique for doing fraud is being increased. Thus, the security in these cases should be elevated and should not be easily controllable with implementation. Now a days, most applications are safe with their underlying system. Phishing is identified as identity theft that steals password and personal information of people [5]. Many information security techniques have been developed to protect information from hackers that include Steganography, Cryptography and other encryption techniques .Steganography techniques can be applied on any type of digital media such as text, video, audio or images. Visual cryptography and Secret Image Sharing are cryptography techniques that are used for secured encrypting of the information like written materials, textual images, and handwritten notes etc.

II. RELATED WORK

Link manipulation: it is a technique where an email is sent by the attacker with a link in it. The anchor text of the link appears to be legitimate but upon clicking, it takes us to a site that looks exactly similar to the original one. For example the link http://www.abccorporation.com may appear to be the original website address of ABC Corporation but it doesn’t take us to the legitimate site. [6]

In the existing system of phishing detection [13] there is also an approach where the visual cryptography is used. In this approach when the user first registers at the bank server, then at the time of registration itself an image is selected which is divided into two shares. One share of image is stored at the server and user gets another share which he keeps with him. When the user wants to initiate the transaction with merchant server he sends his UID code to the merchant server. Merchant server then sends his sys Id & password along with user’s UID to the bank server. When bank server gets this request he first verifies if the merchant is registered merchant.

If so, he fetches the share of image associated with the specific UID code and sends it to the merchant server which then sends it to the user. When user gets the share of image he combines it with his share. If user gets the original image which was selected at the time of registration, then he gets to know that the merchant is authenticated, and the user can now proceed the transaction

One-time passwords are passwords that are used once and only valid for one login session or transaction. Banks, governments and other security based industries deploying OTP system where user may have many passwords and use each password only once. OTPs can avoid a number of shortcomings that are associated with traditional passwords which are valid for many transactions as users are reluctant to voluntarily change passwords frequently. Since OTPs are only valid for single use, an attacker has a smaller window of time to gain access to resources guarded by such a password because any previously stolen passwords will likely have become invalid[14].

III PROPOSED SYSTEM

As per the related study we could find the gaps in the existing system that is the online voting system has been affected due to phishing attacks so we are developing an efficient system using visual cryptography that would detect the phishing attacks and prevent the system from them using the algorithm for Share generation, distribution and result reconstruction that is Image Captcha Algorithm, The secure multi-party computation.

Objectives of this would be

- For the people who are working outside the native country as well as for the people who are physically disabled and very old people can vote irrespective of their places.
- Proposed system provides voting system only for authorized people.
- Only one person can cast one vote

IV. METHODOLOGY

1. VISUAL CRYPTOGRAPHY

The best known technique to safe evidence is cryptography. The art of forwarding and collecting encrypted messages that can be decrypted only by the forwarder or the collector. Encryption and decryption are proficient by using algorithms in such a way that the intended receiver can decrypt and he can read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as an easy and safe way to allow the secret sharing of images without any cryptographic problems.

In the case of (2, 2) VCS [1], each pixel P in the original images encrypted into two sub pixels called shares. Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using individualistic random choices. When the two shares are stratified, the value of the original pixel P can be determined. If a determined P is a black pixel, we will get two black sub pixels; if a determined P is white pixel, we will get one black sub pixel and one white sub pixel.

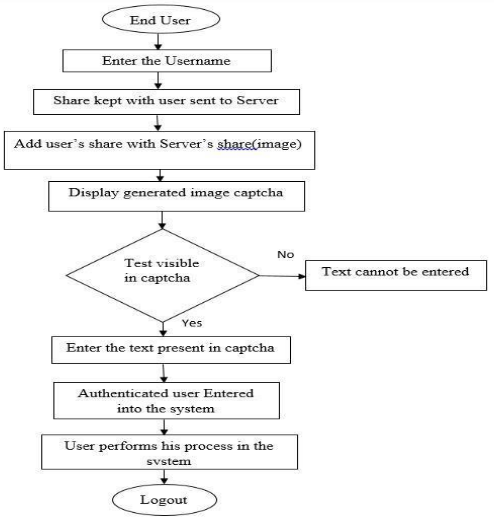

End User
Enter the Username
Share kept with user sent to Server
Add user's share with Server's share(image)
Display generated image captcha
Test visible in captcha
No
Text cannot be entered
Yes
Enter the text present in captcha
Authenticated user Entered into the system
User performs his process in the svstem
Logout

Figure 1. Proposed Online Voting System

1. REQUIREMENTS

Operating System: Windows XP, Windows8

Technology: JSP, Servlet, JDBC, JDK 1.4

Middleware: Tomcat 5.5
Back End: My-SQL 5.0

2. SYSTEM ARCHITECTURE

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology uses visual cryptography and it is based on the Anti-phishing Image Captcha authentication scheme. It prevents password and other unique information from the phishing websites. The proposed system can be divided into two phases one is Registration phase and other one is Login phase.

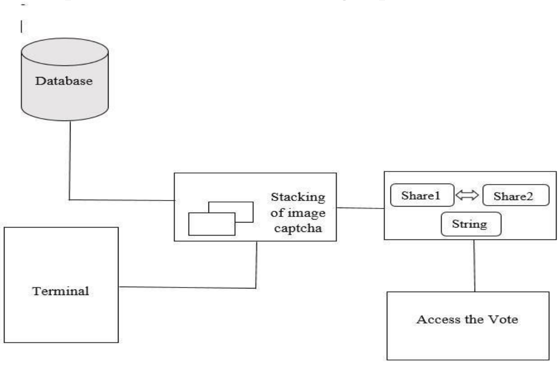


Figure 2: System Architecture

A. REGISTRATION PHASE

In the registration phase, a key string (password) is asked from the user at the time of registration for the safe website. The generated key string can be a combination of alphabets and numbers to provide more secure environment. This string is progressed with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the share is sent to the voter email Id and the other share will be in the voting system itself. The image captcha is also stored in the actual database of any personal website as quiet data. After the registration, the user can change the key string when it is needed.

B. LOGIN PHASE

When the user logs in, then the user is first asked to enter his username (user id).Then the user is asked to enter his share which is sent to his registered mail id before the election process. 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 merged together to produce the image captcha. The image captcha is displayed to the user or voter when two shares are merged. Here the voter or user can check whether the displayed image captcha matches with the captcha created at the time of registration by admin. The voter is required to enter the text displayed in the image captcha which is generated by merging two shares and this can serve the purpose of password and using this, the user or voter can log in into the website. Using the username and image captcha generated by merging 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.

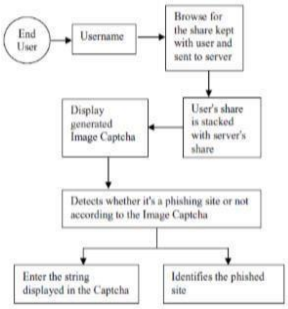

End User
Username
Browse for the share kept with user and sent to server
User's share is stacked with server's share
Display generated Image Captcha
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the Captcha
Identifies the phished site

Figure 3. When user attempts to log in into site

V. IMPLEMENTATION

In the registration phase the most important part is the creation of shares from the image captcha where one share is sent to voter or user mail id before the election and other share can be kept with the server. For login, the user needs to enter a valid username in the given field. Then he has to browse his share and process in the server side, every pixel from the secret image is encoded into multiple sub-pixels in each share image using a matrix to determine the color of the pixels.

1) Binary Secret Image Sharing Method: A binary image is an image that has only two possible values for each pixel. Two colors used for a binary image are black and white. Each pixel is stored as a single bit 1 or 0. For binary image, in order to use the proposed scheme, the grayscale level (k) should be taken as 2. The rest of the procedure is same for construction of shares and revealing phase to recover the secret image. Fundamental Concepts of binary Image Sharing Process

- Successively take the pixels of a binary image of h x w dimension. For every pixel, determine whether it is black or white.

- Now for every pixel, we use a random function to choose a set of pixels from the codebook which gives two set of pixels for every chosen pixel, one corresponding to share-1 while other corresponding to share-2 of the image. At the end of this step, two shares of size h x 2w are generated. Reconstruction Process • Collect both the shared images to reconstruct the original binary image.

- Taking the corresponding pixels from both the shared images we generate a new pixel by performing the following operation: ~ (A+B) Where, A is the pixel from share-1, B is the pixel from share-2, + represents the binary OR operation, and ~ represents the binary negation (NOT) operation.

2) Grayscale Secret Image Sharing Method: The process of share construction phase and image reconstruction phase of secret image sharing scheme for grayscale image are as follows: Share construction:

- get scrambled image PA by using a key to generate a permutation sequence to permute the pixels of A.

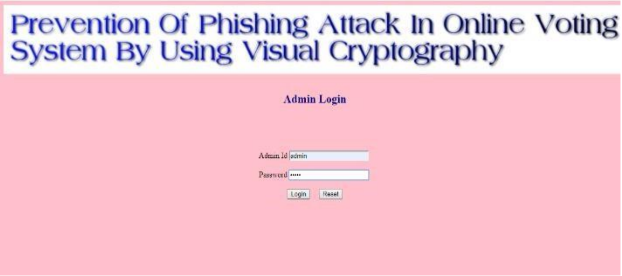
- generate n-1 random matrices R1,……,Rn1, each of which has size h x w and element be {0,…..,k-1} for an image with k grayscale levels. • compute Rn = (kJ - R1 …….- Rn-1)mod k, where J is unit matrix with size hxw. • compute Si = (Ri + PA)mod k, where " + " means matrix addition and i ϵ {1,….,n-1}.

- compute Sn = (Rn + kJ - (n-2)PA)mod k, where " - " means matrix subtraction. Image Reconstruction: • PA'= (S1 +….+ Sn)mod k.

- apply inverse-scrambling operation to PA' to get the reconstructed image A'.

3) Color Secret Image Sharing Method: For color image, any desired colors can be obtained by mixing primitive colors red (R), green (G) and blue (B). In true color system, R, G and B are respectively represented by 8 bits which can represent 0-255 variation of scale. To extend the proposed schemes for grayscale image to color image, three steps are needed. Firstly, decompose the color image into three components of R, G and B, each of which can be seen as grayscale image. Then perform the proposed scheme for grayscale image to each component R, G and B. Finally, compose R, G and B components to generate shares. In the revealing phase, again take the decomposed RGB components of the shares and perform the proposed scheme separately. Finally merge the generated RGB components to recover the secret image At the server side the user's share is combined with the share in the server and an image captcha is generated. The user has to enter the text from the image captcha which is generated by merging two shares in the required field in order to log in into the website. The different cases.

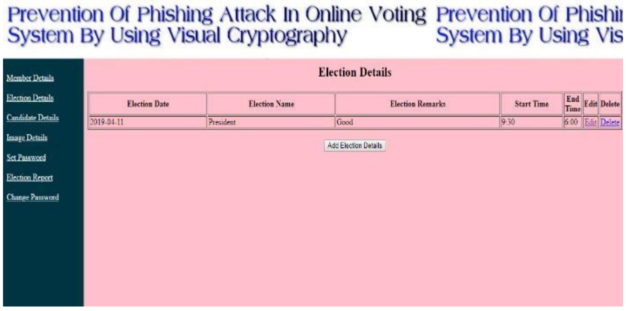
VI RESULT ANALYSIS


Prevention Of Phishing Attack In Online Voting System By Using Visual Cryptography

Admin Login

Admin Id admin
Password *****

Figure 4: Admin Login In this figure 4 the login page is shown where the only admin can login.


Prevention Of Phishing Attack In Online Voting System By Using Visual Cryptography Prevention Of Phishi
System By Using Vis

Election Details

Election Date	Election Name	Election Remarks	Start Time	End Time	Edit	Delete
2019-04-11	President	Good	9:30	6:00	Edit	Delete

Figure 5: Election Details

The figure 5 shows that admin adding users to vote the particular candidates.

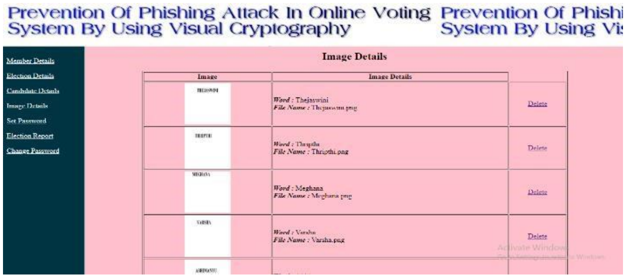
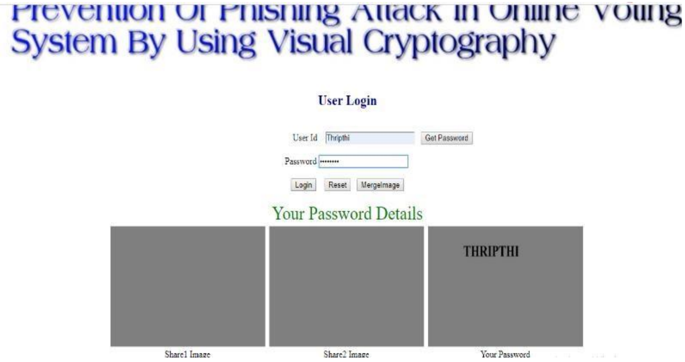


Image Details

Image	Image Details	
THEJASWINI	*Word :* Thejaswini *File Name :* Thejaswini.png	Delete
THRIPTHI	*Word :* Thripthi *File Name :* Thripthi.png	Delete
MEGHANA	*Word :* Meghana *File Name :* Meghana.png	Delete
VARSHA	*Word :* Varsha *File Name :* Varsha.png	Delete
ABHIMANYU		

Figure 6: Image Details

The figure 6 shows the image captcha details that is used for verification which is next divided into two shares.


Prevention Of Phishing Attack In Online Voting
System By Using Visual Cryptography
Get Password
Login
Reset
MergeImage
THRIPTHI
Share1 Image
Share2 Image
Your Password

User Login

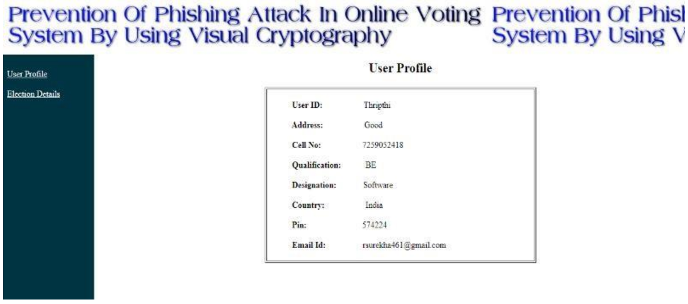
User Id Thripthi

Password ••••••••

Your Password Details

Figure 7: Merging Two Shares

The figure 7 shows the page for merging the two shares which the image is added by the admin and the image split into two shares.


Prevention Of Phishing Attack In Online Voting System By Using Visual Cryptography
Prevention Of Phisl
System By Using V
User Profile
Election Details

User Profile

User ID: Thripthi

Address: Good

Cell No: 7259052418

Qualification: BE

Designation: Software

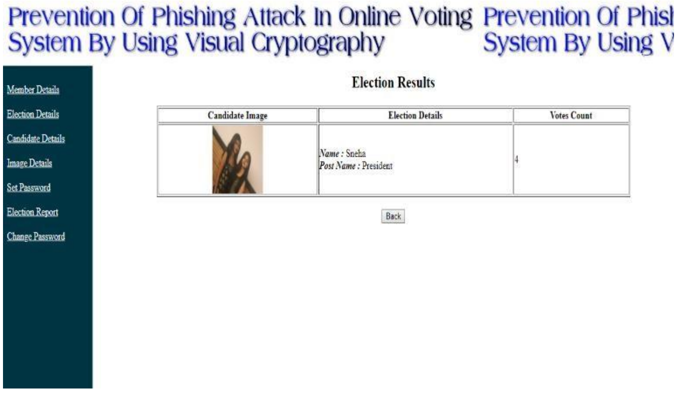
Country: India

Pin: 574224

Email Id: rsurekha461@gmail.com

Figure 8: User Profile

The figure 8 shows the user profile who is voting, registered by the admin



Election Results

Candidate Image	Election Details	Votes Count
	Name : Sneha *Post Name :* President	4

Figure 9: Election Result

The figure 9 shows the votes count, how many voters voted to the particular candidate.

VI. CONCLUSIONS AND FUTURE WORK

Election plays an important role for any democratic country. If this proposal is implemented, then the voting percent can be improved further since few percent of our citizens are working in worldwide and they cannot able to come to native country at the time of voting. For those people as well as for the people who are physically disabled and very old also can make use of the online voting system. Since Visual Cryptography Technique is used, user can able to find out whether he is in phishing site or original site easily. Proposed online voting system is very effective and it will useful for voters.

REFERENCES

[1] Liang H., & Xue Y., “Understanding security behaviors in personal computer usage: A threat avoidance perspective”, Association for Information Systems, 11(7), pp. 394–413, 2010

[2] Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behavior (38), pp. 304–312, 2014.

[3] Yuancheng Lia et al., “A semi-supervised learning approach for detection of phishing web pages”, Optik, (124), pp. 6027– 6033, 2013.

[4] Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007 http://www.antiphishing.org

[5] Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, *NGS Software Insight Security Research.*

[6] Anti-Phishing Working Group, Global Phishing Survey: Trends and Domain name use in 1H2009, 2009Anti-Phishing Working group.http://www.antiphishing.org/.

[7] Core Street, Spoofstick, http://www.corestreet.com/spoofstick/

[8] Dhamija, R. and Tygar, J. D. 2005. The battle againstphishing: Dynamic Security Skins. In Proceedings of the2005 Symposium on Usable Privacy and Security, SOUPS '05, vol. 93, ACM Press.

[9] eBay Toolbar, http://pages.ebay.com/ebay_toolbar/

[10] Evgeniy Gabrilovich and Alex Gontmakher. "The Homograph Attack" (PDF), February 2002, ACM.