

Preventing phishing using visual cryptography

- A.Harsha vardhan
- IMT2016101

PROJECT SCOPE:-

This project starts by defining phishing, discussion of problems caused by phishing and prevention methods for phishing which uses visual cryptography followed by analysis with a case study.

Project objective:-

The main objective of this project is to discuss how phishing can be detected and methods that can prevent it.

Background:-

Phishing is an endeavour by an individual or a gathering of people to steal individual private data, for example, passwords, credit card information from different users and systems for gaining money and other fake activities. There are many measures to detect phishing and various methods to prevent phishing. One such method is Visual Cryptography.

Visual cryptography is a method of encryption which needs human eyes to decode it. The fundamental point of visual cryptography is to protect the security of picture captcha by deteriorating the first picture captcha into two shares that are put away in isolated database servers with the end goal that the first picture captcha can be revealed only when both are simultaneously available, the individual share doesn't reveal the character of the first picture captcha which was created already. When the unique image captcha is found to be the same, then that image captcha can be utilized as a secret password for identifying phishing by the client.

Corporations and organizations routinely use online voting to choose officers and Board individuals and for other intermediary decisions. Internet casting a ballot alludes to both the electronic methods for making a choice and the electronic methods for arranging cast a ballot. Casting a ballot framework with Visual Cryptography has been used for an efficient authentication of users to cast vote for confidential internal corporate decisions. Voters who sidestep verification or have just cast a ballot are denied access to the vote. One-vote-per-voter is ensured by storing the vote in a single transaction and marking the electors as voted. The election is held in full confidentiality by applying security measures that allow the voter to vote for any candidate. Only if the candidate logs into the system by entering the correct password which is generated by merging the two shares using Visual Cryptography scheme.

Literature survey:-

Phishing:- Trades in perspective on the Internet ended up being astoundingly essential nowadays. With the extension in online trades, even computerized attacks in light of online

trades extended exponentially. A standout amongst the most well-known and effective assault depends on phishing

The related approaches for phishing detection system are the email-based approach, blacklist approach, visual clue-based. The aggressors are being inventive for each ambush. Similarly, the measures to curb these phishing attacks should be effective and hard to break. It can be executed from numerous point of views. A standout amongst the most widely recognized methods for phishing is to send an email with adjusted URL of the site. The phoney URL comprises the cloned site. For an untrained eye, it is difficult to differentiate. At the point when the client enters the accreditations, the aggressor takes them. To avoid Internet phishing, clients should have knowledge of various types of phishing techniques.

Cryptography:-

The best-known techniques to protect data is the use of cryptography. Cryptography is the process of encryption and decryption. Encryption converts the data into ciphertext. Decryption converts the ciphertext to data. Encryption and Decryption happen with a key. Without the key, the ciphertext can't be converted back to data and ciphertext alone will be meaningless.[5]

Visual cryptography:-

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used.[1]

The credibility of the user is a major concern in present day internet application. This is more prominent in areas like the banking sector where online operations involve a financial transaction. One of the oldest and most used authentications is password based. But due to the exponential growth of computing power of modern devices and attacks like brute force, hash table attacks, phishing, hacking of databases, etc makes password not so secure anymore. To address this issue many solutions have been proposed. One such solution is CAPTCHA based Visual Cryptography. This method generates a unique solution to address the security issue. This method generates a CAPTCHA image for users which is divided into two parts. One part is stored in a database of banks. The other part is stored with customer share. Without the two parts, the original CAPTCHA image can't be recovered. The system is unbreakable as long as both layers do not fall in the wrong hands. When one of both layers is intercepted it is impossible to retrieve the encrypted information.

The system is the web-based application so that it can be accessed by any authorized person anywhere in the world through the internet. Firstly, the textual password image is converted into black and white images based on RGB (red, green, blue). we have to map that to a single number giving a grayscale value. This average method will simply average the values

$$(R + G + B) / 3$$

Each pixel in the monochrome image, the pixel will be divided into 4 sub-pixels depending on the colour of the pixel and thus, increasing the size of the whole image. There are 6 possible permutations to divide a pixel into 4 sub-pixels (2 black and 2 white) [3]

Images	White pixel						Black pixel					
Share 1												
Share 2												
Stacking result												

Figure 1. All possible combinations of sub-pixels

If the colour of the pixel is white, then one of the possible sub-pixels is a white pixel.[3]

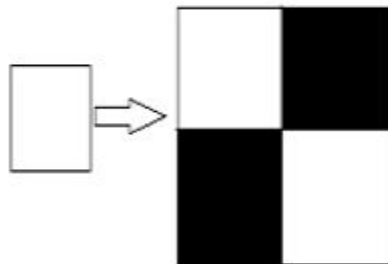


Figure 2. White pixel

If the colour of the pixel is black, the subpixel is a black pixel.[3]

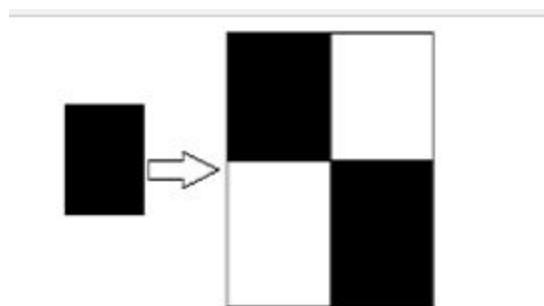
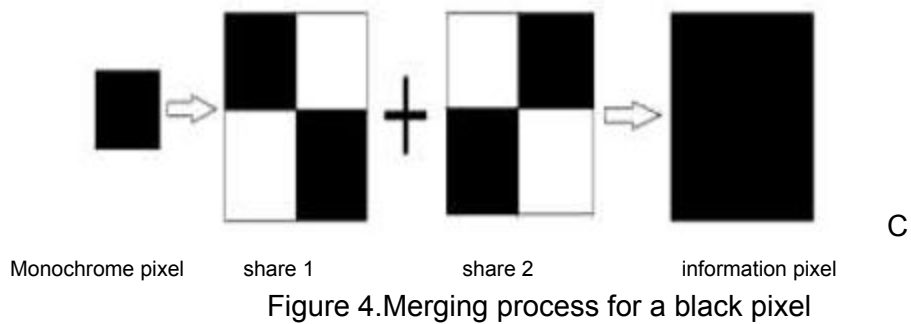
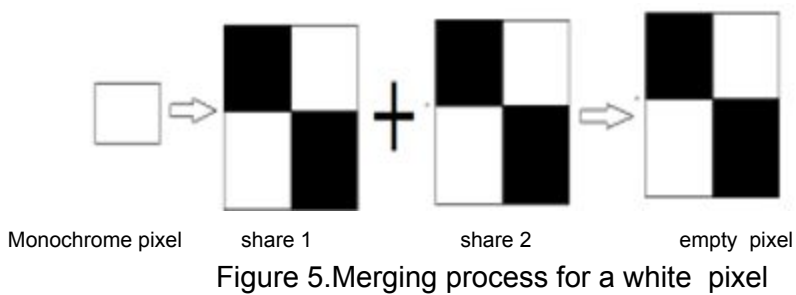


Figure 3.Black pixel

White pixel is called as an empty pixel and black pixel is called the information pixel [3]. If the source pixel in the monochrome image is black, then the subpixels in share 1 and share2 will be inverted as



If the source pixel in the monochrome image is white, then the subpixels in the share1 and share 2 will be identified as [3]



The result of the overall process after merging the two shares is an image containing the textual password which will be represented by information pixels (black pixels) as

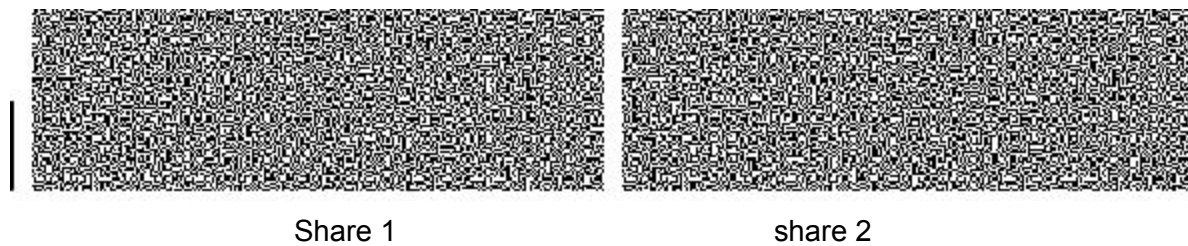


Figure 6. Share 1 + share 2 (can be used for password)

Source for the above shares:

<https://www.semanticscholar.org/paper/A-Visual-One-Time-Password-Authentication-Scheme-C-how-Susilo/6ea94a2b646c08f74ac9f6babe18ea3f5aaff965/figure/0>

Methods to detect phishing:-

There are many ways to detect phishing attacks such as email-based approach, blacklist approach visual clue-based approach, information flow based approach and website feature-based approach.

Current System:-

In the existing system of phishing detection [1], there is additionally an associate degree approach wherever the visual cryptography is employed. In this approach the user first registers at the bank server, then at the time of registration itself, a picture is chosen that is split into two shares. One share of the image is kept at the bank server and also the user gets another share that he keeps with him. Once the user desires to deal with a merchant server he sends his UID code to the merchant server. Merchant server then sends his system Id & password along with user's UID to the bank server. Once bank server gets this request he first verifies if the merchant is registered, merchant. If so, he fetches the share of the image related to the particular UID code. And sends it to the merchant server that then sends it to the user. Once the user gets the share of the image he combines it with his share. If the user gets the initial image that was selected at the time of registration, then he gets to know that the merchant is authenticated, and also the user will currently proceed with the transaction[4]

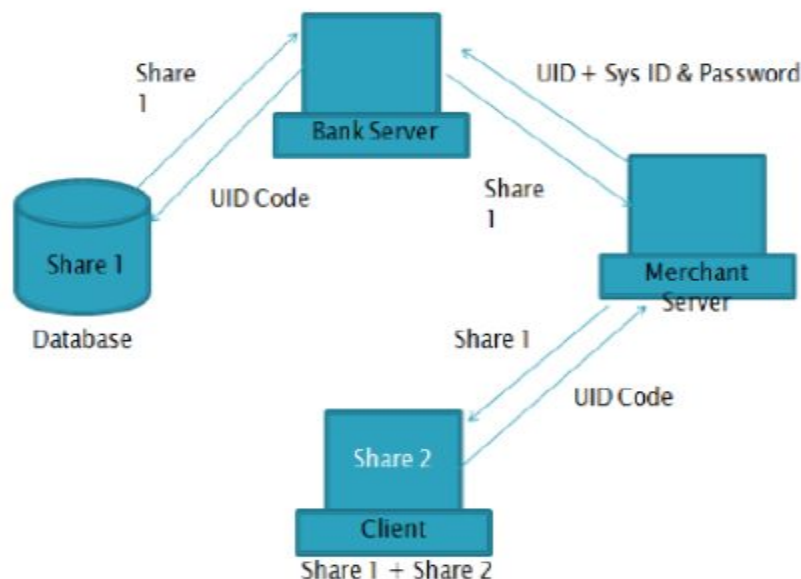


Figure 7. Current system

Drawbacks:-

The main drawback of this approach is each time a user wants to make a transaction, he has to use the same system or carry the share everywhere. So this technique is time-consuming.

Better Approach:-

To overcome the drawbacks in the current system, a new approach was introduced.

The system architecture is divided into two phase's registration phase and the transaction Phase. In the first part, registration starts once the client signs up and enters his/her profile data and send this registration request to the bank server. The bank server when receiving the registration request from client generates a public/private key combination for the client. Then the bank server saves the key pair/user id details within the information. The bank server then informs the general public key to the user and therefore the personal key never leaves the server. Finally, the registration gets completed once the client receives the general public key from the server. The client will amend or update key any time later.[4]

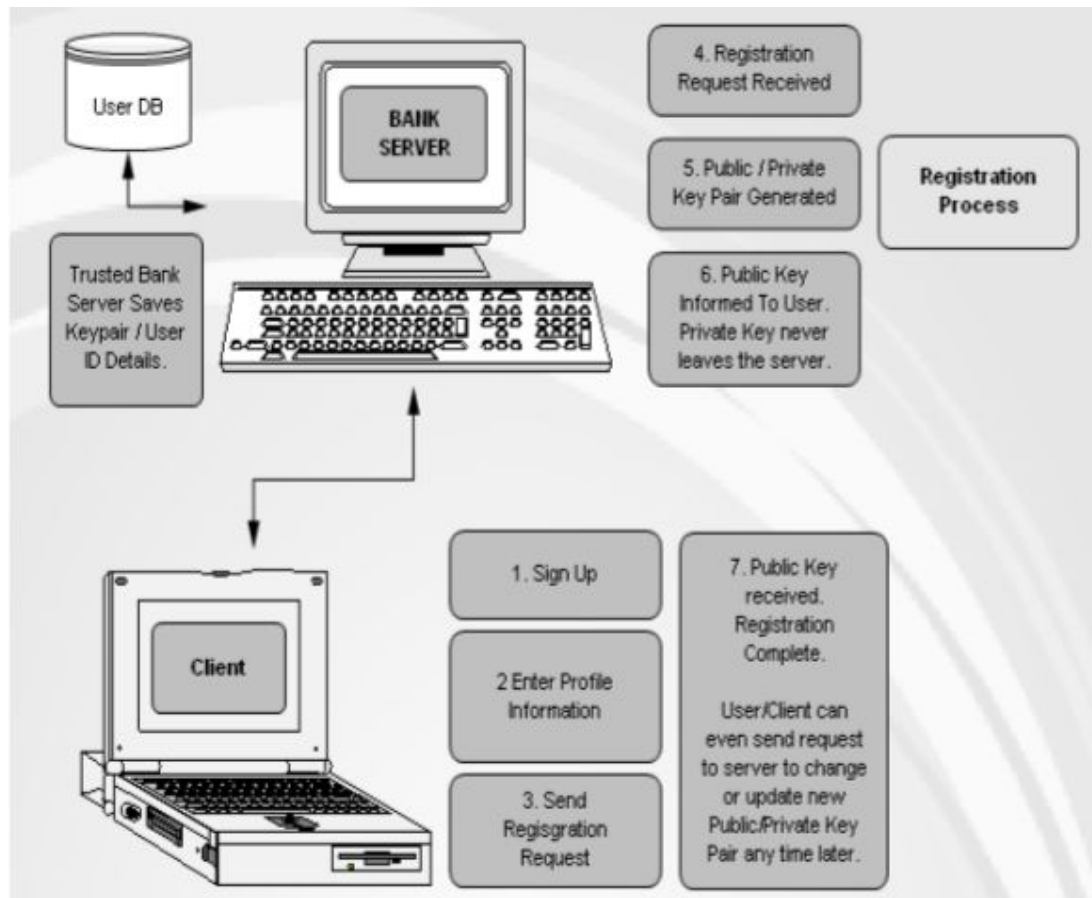


Figure 8. Registration phase

The exchange stage begins after the enlistment stage is finished. For confirming if a vendor server is verified or free from phishing, the client utilizes our phishing detection system. For this,

the client chooses any random image. In the wake of choosing a picture, he then thresholds the picture and divides the picture into two shares using visual cryptography (VC) algorithm

From these two offers, one offer, for example, share1 is encoded using the open key and furthermore, the client at that point transmits this encrypted share1 to the vendor server. The vendor server gets encoded share1 from the client and retransmits the scrambled share1 to the bank server.

The bank server begins the verification method when the receiver gets encrypted share1 and the client id from the dealer server. It checks if the merchant/vendor server under test is enrolled with the bank server. On the off chance that the vendor server is enlisted with bank server, at that point exclusively the bank server decrypted share1 and send it back to the merchant server. The merchant server gets decrypted share1 and retransmits it to the client.

The customer gets decrypted share1 from the vendor. The merchandiser at that point recombines new share1 with the previous share2. On the off chance that the created picture is equivalent to the genuine picture, at that point, the client gets the opportunity to comprehend that the merchant server is verified and he will as of now starting his transaction.[4]

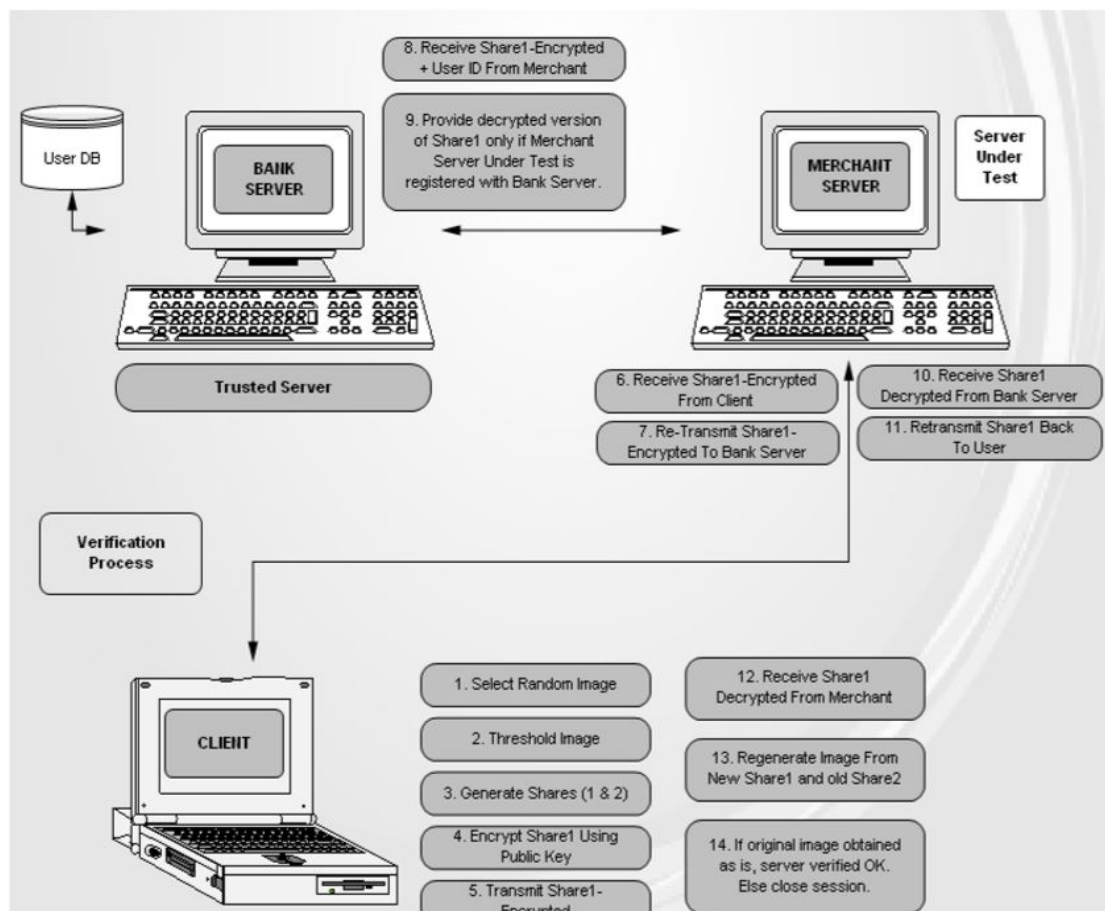


Figure 9. Verification phase

If the merchant server is a phishing site, the session will be closed

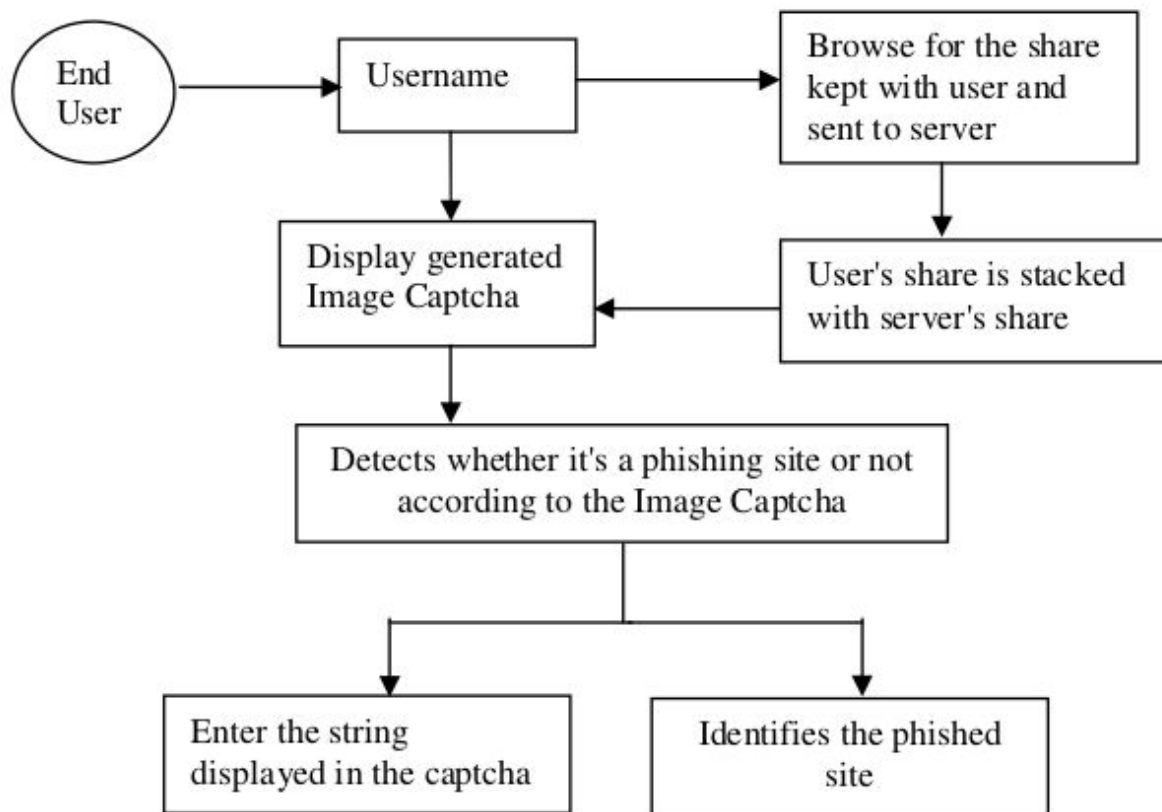


Figure 10. User login phase

ANALYSIS OF ONLINE VOTING (case study):

Preventing phishing in online voting:-

The voting system has evolved from years. They evolved with respect to advancements in technology.

A. Paper ballot system:

The paper ballot system is that the normally used ancient legal system. Its widely used before the introduction of the electronic legal system. Paper ballot system includes casting the vote using the paper and also the stamp. Every voter has a ballot and it can't be shared [1]

The disadvantages of this system are:

- i) time overwhelming
- ii) booth capture

iii) low tally speed

In this type of voting system, there are high chances of rigging. Politicians might use their power to make fake votes or use people to vote many times with different ID's. To avoid such cases and improve elections procedure, the government introduced an electronic voting system.

B. Electronic voting system:

An electronic voting system is a type of voting system which uses an electronic ballot that would allow voters to broadcast their secret vote ballot to election officials over the internet.[1]

The disadvantages of this system are:

- i) people with poor computer knowledge cannot vote properly.
- ii) vulnerable to security.
- iii) power consumption on the polling venue.
- iv) cost

The main disadvantage posed by electronic voting would be the security risk that can potentially undermine the election process. In addition to human error, internet electronic voting is susceptible to a range of threats(phishing), technical glitches, voter impersonation and even system failure.

C. Online voting system:

The online voting system is the latest electronic voting system introduced in which the voted ballot is transmitted over the public internet through a web browser. The voter can directly vote online from anywhere in the world. Security is the major drawback in using this system. The majority of the applications are giving high assurance towards the Password Security and they are not focusing on phishing assaults. By phishing, assailants are legitimately getting the passwords from the client and they can go into the applicable sites with correct passwords.

To overcome the problem we can use visual cryptography to prevent phishing in online voting.

PROPOSED ONLINE VOTING SYSTEM :

Consider an online polling system for electing a government authority. The mechanism for detecting phishing or preventing phishing can be done using the technique as described in figure 11. At whatever point the election officer or head on account of any private concern who needs to perform casting a ballot to transfer the password image, it needs to move from local system to web server. To divide the password image into two shares, this system proposed the Visual Cryptography procedure. Before separating the image into two shares the image is first changed over into a monochrome picture (for example highly contrasting picture which is a black and white image). Given a secret image S , a set P of n members and a solid access structure, a Visual Cryptographic Scheme (VCS) for General Access Structures (GVCS)

encodes S into n offers of transparencies. Demonstrating of limiting the pixel expansion for a (k, n) - VCS into an integer linear program (ILP), to guarantee that the imperatives for GVCS can be satisfied. The pixel expansion of a GVCS would thus be able to be limited by fathoming the corresponding ILP. The proposed ILP is summed up for (k, n) - VCS. It very well may be connected to develop the basis matrices with the minimum pixel for a GVCS.

The ideal pixel expansion of a GVCS can be gained, particularly for those applications that truly need a GVCS with the smallest shares. After Image is isolated into two shares one share must be sent to the relevant voter through email, for which SMTP procedure is utilized.[1]

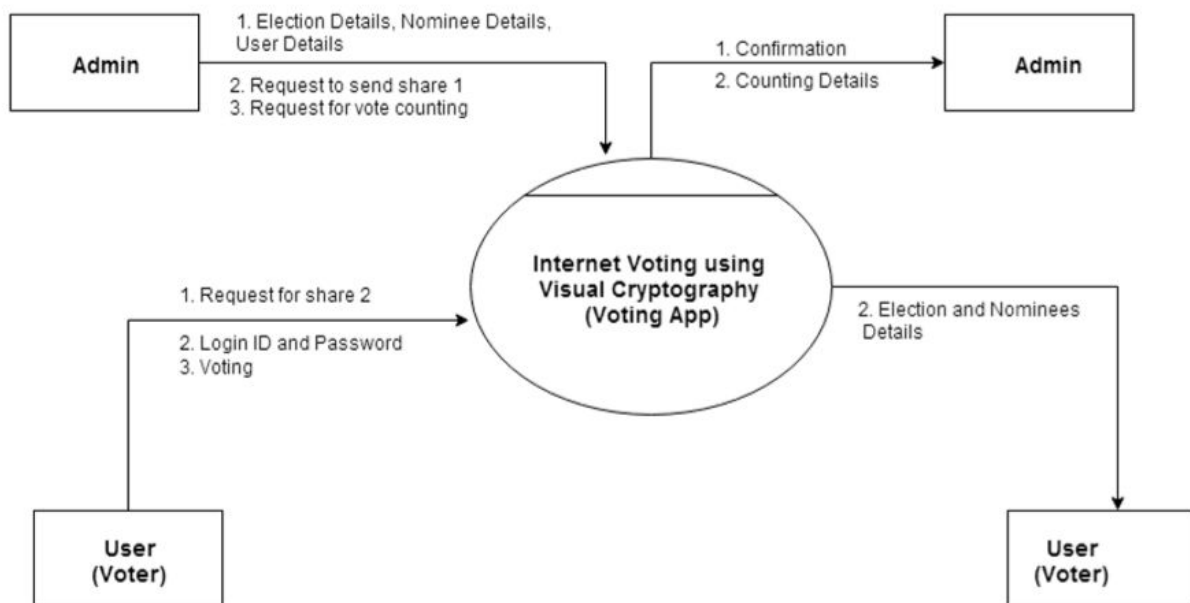






Figure.11.The proposed online voting system using visual cryptography





The image of text captcha is split into two shares namely share 1 and share 2. From figure 12, we can easily recognize three unique types of output. Every pixel of the images is partitioned into smaller squares. There is dependably the same number of white (transparent) and black squares. In the event that a pixel is partitioned into two parts, there are one white and one black square. In the event that the pixel is isolated into four equal parts of, there are two white and two black squares. In case1 and case2, it can be seen that correct images are framed and the

captcha can be reconstructed appropriately though in case3, distinctive offers are utilized and thus the captcha can't be created legitimately.

Case.1

Original Captcha	Share 1	Share 2	Reconstructed Captcha
			

Case 2

Original Captcha	Share 1	Share 2	Reconstructed Captcha
			

Case.3



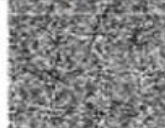
Share 1 of Case1	Share 2 of Case2	Reconstructed Captcha
		

figure .12. Different types of image captcha

If the shares are from the same image then he can continue. After entering the captcha, the user is allowed to cast his vote. In case 3, the two shares are different and thus the output is not the proper image captcha. Hence the user cannot enter the captcha and thus the user is logged out of the system.[1]

For an online voting system, there should be many powerful validations to make the voting successful. Some of them are

- Once the voter completes his polling, he should not be allowed to vote again. We can accomplish this by making his password expire immediately after polling.

- Whenever the voter does his polling and votes to a particular candidate, the total voting count will be increased and also the count for the corresponding candidate will be increased. This will make it easy for evaluating results and to maintain a count of the number of voters left for voting
- Proper authentication should be provided in order that the voters shouldn't have ambiguity about the safety of polling exploitation of a web legal system. this could be achieved by the combined usage of visual cryptography and anti-phishing techniques.

Every voter needs to be provided with a share i.e. one of the image shares, of his password is sent through any of the electronic transfer systems such as email. This mailing system needs to be a properly secured one and needs to have proper authentication. The voters have to make use of the same mailing system for receiving their shares using their mail ID's which are already created by them in the corresponding mailing services.

IMPLEMENTATION OF PROPOSED SYSTEM:

There are two sessions involved in the proposed system. They are Admin session and Voter session

Admin Session:

Admin login to the complete system and can be responsible for managing Login details, Voters details, Election details, Image details (Text images), Nominees details, Setting Voters password, Election reckoning details and alter the password.[1]

- A. Login Details: Using this process, the admin will log in to the entire system.
- B. Voters Details: The list of the voters who are eligible for the voting process can be viewed.
- C. Election Details: The entire details of the elections (if any) present on any particular day can be viewed
- D. Image Details (Text Images): Here we present the password text images that the admin can provide for different voters that keep changing frequently.
- E. Nominees Details: Here the complete details of each nominee are presented clearly to make the work of admin simpler.
- F. Setting Voters Password: The following steps to be taken for setting voters password:
 - Random Number Generator to pick the Image
 - Divide the Image into two shares using Visual Cryptography
 - Sending the First Share through Email using Visual Cryptography
 - Storing the second share in the database
- G. Election Counting Details: Here the admin can actually view the number of votes gained by each candidate contested for elections and declare the results accordingly.

H. Change Password: Here the admin can change the passwords of all the candidates more frequently as per the requirement.

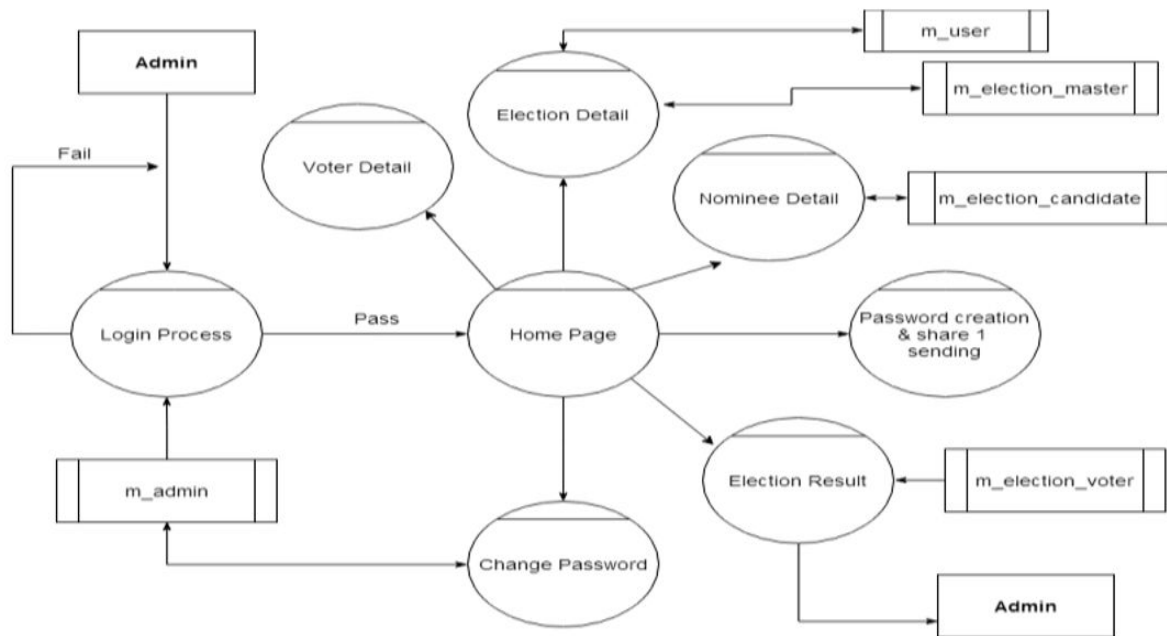


Figure 13.Admin session

Voter Session:

Voter session involves user login with phishing protection, providing a User ID and getting a share from the server, producing captcha image, and user home page whereas the user can select election, display the nominees, and cast the vote.[1]

In the Voters Session, the following processes were involved:

- A. Login Module with Phishing Protection
- B. Providing User ID and getting Share from Server
- C. Producing Captcha Image
- D. Home Page
 - Selecting Election
 - Nominees Display
 - Voting Process

In voter session after merging both shares, the voter will be accessible to ballot his vote. In this process, he can see his details in nominee details. After his voting, his vote is updated and he will be exited from the session. his password will be expired so that we will not be able to vote again.

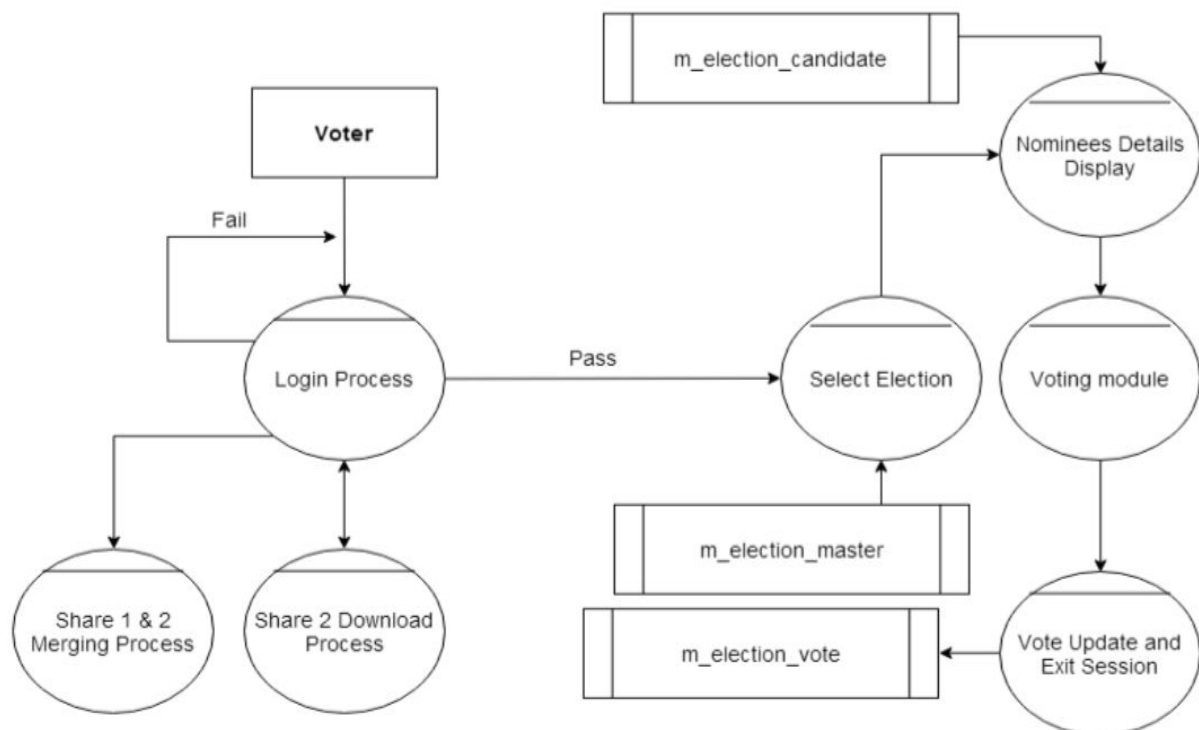


Figure 14. Voter session

JUSTIFICATION AND CONCLUSION :

Voting plays a really crucial role in the future of any democratic country. If the projected model is enforced, then the proportion of choice during an election will increase considerably and not simply voters who reside within the country however conjointly voters of the state across countries can vote for the elections. This process even simplifies the method of choice for disabled people and people who are very old to vote in conventional voting systems. By using the proposed method of Visual Cryptography Technique, a user is able to see whether or not the site which that person is referring to, is a phishing site or a secured site with ease. the proposed online legal system is incredibly effective and it'll be helpful for voters and

organizations in many ways and it will also reduce price and time. Within the present situation, phishing attacks are terribly frequent on a global scale as a result of which capturing and storing users' confidential information will be so simple for hackers. This data is sold for a high price on the dark web or used against users. Preventing Phishing websites can be done by using "Visual Cryptography". The proposed methodology ensures that the confidential information of users is secured using three layers of security.

- the first layer verifies whether or not the web site may be a genuine/secure website or a phishing website. If the web site may be a phishing website (A website that's a fake one also looks the same as a secure website however with very little changes which can be noted only by a trained eye), then in that scenario, the phishing web site will not show the image captcha for that specific user (who needs to log in into the website), thanks to the very fact that the image captcha is generated by the stacking of 2 shares, one is with the user and another one is contained with the secure website only.
- Second layer cross validates image Captcha like the user. The image Captcha can be cleared by human users alone and not by machine users. Only human users accessing the web site will browse the image Captcha and make sure that the site is safe as well as the user is permissible one or not. So, using image Captcha technique, no machine-based user will crack the secret or other confidential information of the users.
- The third layer of security prevents intruders' attacks on the user's account. This technique provides extra security in terms of not letting the intruder log in into the account even when the intruder is aware of the username of a specific user. The proposed methodology is additionally helpful to prevent the attacks of phishing websites on the financial web portal, banking portal and online shopping market.

References :

- [1] Mintu Philip A Novel Anti Phishing framework based on Visual Cryptography in IEEE, 2012.
- [2] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
- [3]<https://ijarcce.com/upload/2017/may-17/IJARCCE%2022.pdf>
- [4]
https://www.researchgate.net/publication/328064154_PHISHING_DETECTION_SYSTEM_USING_VISUAL_CRYPTOGRAPHY
- [5]https://www.researchgate.net/publication/261064429_Visual_Cryptography

Bibliography :

- [1] <https://www.ijsr.net/archive/v2i3/IJSRON2013533.pdf>
- [2]<https://www.ijsr.net/archive/v3i2/MDIwMTM5NTE=.pdf>
- [3] 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.