|  |
| --- |
| **Preventing Phishing Attack on Voting System Using Machine Learning** |
|  |
| **A report submitted in partial fulfilment of the**  **requirement** **for the award of degree of**  **BACHELORS OF ENGINEERING**  **in**  **ELECTRONICS AND COMMUNICATION ENGINEERING**  **SECTION-1 GROUP-B**  **SECTION-2 GROUP-A** |
|  |
| **Submitted By** |
| **Rishali rishu 19BEC1108**  **Sushant Kumar : 19BEC1078** |
|  |
| **under the guidance of**  **Dr. O Jeba Shiney** |
|  |
| **Electronics and Communication Engineering** |
|  |



**BONAFIDE CERTIFICATE**

Certified that this project report **Preventing Phishing Attack on Voting System Using Machine Learning** is the bonafide work of **Rishali rishu and Sushant Kumar** who carried out the project work under

My/our supervision.

**SIGNATURE SIGNATURE**

**SUPERVISOR HEAD OF THE DEPARTMENT**

Submitted for the project viva-voce examination held on

**INTERNAL EXAMINER EXTERNAL EXAMINER**

**Table of Contents**

[**Chapter**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013742) **1.** [**Introduction**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013743)

[**Chapter**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013783) **2.** [**Literature survey**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013784)

**Chapter 3. Design flow/Process**

**Chapter 4.** [**Results analysis and validation**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013784)

**Chapter 5. Conclusion and future work …………………………**

**ECE Archives Project Submission Form………………………………**

**Acknowledgment**

I really appreciate that I have such an opportunity to express my great gratitude and respect to people who helped me when I prepared my BE project. Without their supports and encouragements I cannot go so far.

It is difficult to overstate my greatest gratitude to my project **Dr. O Jeba Shiney**, Professor, and ECE Department. First, I would like to thank her for their patient guiding and inspiring throughout my study period. Secondly, I highly appreciate their encouragement and support in my project work, which helped me build confidence and courage to overcome difficulties. Finally, I am grateful for their great insight and suggestions and sharing so much time in project completion. I would have been lost without their support.

I am as ever, truly and deeply indebted to Prof. (Dr.) S. S. Sehgal, Executive Director, Prof. (Dr.) Nikhlesh Kumar Sharma, Director Engineering and Prof. (Dr.) Paras Chawla, Head of ECE Department for their great supports at every stage of my academic life, and longed to see this achievement come true

**Abstract**

Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims our system aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow the casting of votes from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only

**Chapter 1**

**Introduction**

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 centre, 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 makes 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. 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 Phishing is identified as a major security threat identified is phishing 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 days, most applications are safe with their underlying system. Phishing is identified as identity theft that steals password and personal information of people. 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.

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.

**Chapter 2**

**Literature survey**

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 linkhttp://www.abccorporation.com may appear to be the original website address of ABC Corporation but it doesn’t take us to the legitimate site. In the existing system of phishing detection 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. Voting system Using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares using VC scheme. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose ID and password or other authenticating information provided by the network administrator that allows them access to information and programs within their authority. Voting system Using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares using VC scheme. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose ID and password or other authenticating information provided by the network administrator that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password Establishing and maintaining a secure computing environment is increasingly more difficult as networks become increasingly interconnected and data flows ever more freely. In the commercial world, connectivity is no longer optional, and the possible risks of connectivity do not outweigh the benefits. Therefore, it is very important to enable networks to support security services that provide adequate protection to companies that conduct business in a relatively open environment. There are different kinds of threats available in networks irrespective of the types of networks. Internet is the large and global network. There are different kinds of applications and researches emerging every day to satisfy the needs of users worldwide. There are different kinds of applications based on the Internet. One of them is online voting system. The use of new technologies to support voting and is the subject of great debate. Several people advocate the benefits it can bring such as improved speed and accuracy in counting, accessibility, voting from home and as many are concerned with the risk it poses, such as unequal access, violation to secrecy and anonymity and alteration of the results of an election.

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.



**Chapter 3**

**Design flow/Process**

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. Na or 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 ,each pixel P in the original images encrypted into two sub pixels called shares. Neither share 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.

****



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 xw 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-1while 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 there constructed 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 Bare 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.

**Code**

Image capture:

*"""*

*Created on Mon Apr 4*

*@author: Sush*

*"""*

*import cv2*

*# Take input of the person name*

*name = input("Enter name: ")*

*# Create the videocapture object*

*cap = cv2.VideoCapture(0)*

*while True:*

*# Read each frame*

*success, frame = cap.read()*

*# Show the output*

*cv2.imshow("Frame", frame)*

*# If 'c' key is pressed then click picture*

*if cv2.waitKey(1) == ord('c'):*

*filename = 'faces/'+name+'.jpg'*

*cv2.imwrite(filename, frame)*

*print("Image Saved- ",filename)*

*# if 'q' is pressed then break the loop and exit the program*

*if cv2.waitKey(1) == ord('q'):*

*break*

*# Finally release the camera and destroy ll active windows*

*cap.release()*

*cv2.destroyAllWindows()*

Face Recognition:

*"""*

*Created on Mon Apr 4*

*@author: Sush*

*"""*

*import face\_recognition*

*import cv2*

*import numpy as np*

*import pickle*

*f=open("ref\_name.pkl","rb")*

*ref\_dictt=pickle.load(f) #ref\_dict=ref vs name*

*f.close()*

*f=open("ref\_embed.pkl","rb")*

*embed\_dictt=pickle.load(f) #embed\_dict- ref vs embedding*

*f.close()*

*known\_face\_encodings = [] #encodingd of faces*

*known\_face\_names = [] #ref\_id of faces*

*for ref\_id , embed\_list in embed\_dictt.items():*

*for embed in embed\_list:*

*known\_face\_encodings +=[embed]*

*known\_face\_names += [ref\_id]*

*video\_capture = cv2.VideoCapture(0)*

*# Initialize some variables*

*face\_locations = []*

*face\_encodings = []*

*face\_names = []*

*process\_this\_frame = True*

*while True :*

*# Grab a single frame of video*

*ret, frame = video\_capture.read()*

*# Resize frame of video to 1/4 size for faster face recognition processing*

*small\_frame = cv2.resize(frame, (0, 0), fx=0.5, fy=0.5)*

*# Convert the image from BGR color (which OpenCV uses) to RGB color (which face\_recognition uses)*

*rgb\_small\_frame = small\_frame[:, :, ::-1]*

*# Only process every other frame of video to save time*

*if process\_this\_frame:*

*# Find all the faces and face encodings in the current frame of video*

*face\_locations = face\_recognition.face\_locations(rgb\_small\_frame)*

*face\_encodings = face\_recognition.face\_encodings(rgb\_small\_frame, face\_locations)*

*face\_names = []*

*for face\_encoding in face\_encodings:*

*# See if the face is a match for the known face(s)*

*matches = face\_recognition.compare\_faces(known\_face\_encodings, face\_encoding)*

*name = "Unknown"*

*# # If a match was found in known\_face\_encodings, just use the first one.*

*# if True in matches:*

*# first\_match\_index = matches.index(True)*

*# name = known\_face\_names[first\_match\_index]*

*# Or instead, use the known face with the smallest distance to the new face*

*face\_distances = face\_recognition.face\_distance(known\_face\_encodings, face\_encoding)*

*best\_match\_index = np.argmin(face\_distances)*

*if matches[best\_match\_index]:*

*name = known\_face\_names[best\_match\_index]*

*face\_names.append(name)*

*process\_this\_frame = not process\_this\_frame*

*# Display the results*

*for (top, right, bottom, left), name in zip(face\_locations, face\_names):*

*# Scale back up face locations since the frame we detected in was scaled to 1/4 size*

*top \*= 4*

*right \*= 4*

*bottom \*= 4*

*left \*= 4*

*#updating in database*

*cv2.rectangle(frame, (left, top), (right, bottom), (0, 0, 255), 2)*

*# Draw a label with a name below the face*

*cv2.rectangle(frame, (left, bottom - 35), (right, bottom), (0, 0, 255), cv2.FILLED)*

*font = cv2.FONT\_HERSHEY\_DUPLEX*

*cv2.putText(frame, ref\_dictt[name], (left + 6, bottom - 6), font, 1.0, (255, 255, 255), 1)*

*font = cv2.FONT\_HERSHEY\_DUPLEX*

*# cv2.putText(frame, last\_rec[0], (6,20), font, 1.0, (0,0 ,0), 1)*

*# Display the resulting imagecv2.putText(frame, ref\_dictt[name], (left + 6, bottom - 6), font, 1.0, (255, 255, 255), 1)*

*cv2.imshow('Video', frame)*

*# Hit 'q' on the keyboard to quit!*

*if cv2.waitKey(1) & 0xFF == ord('q'):*

*# t.cancel()*

*break*

*# break*

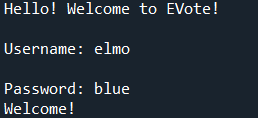
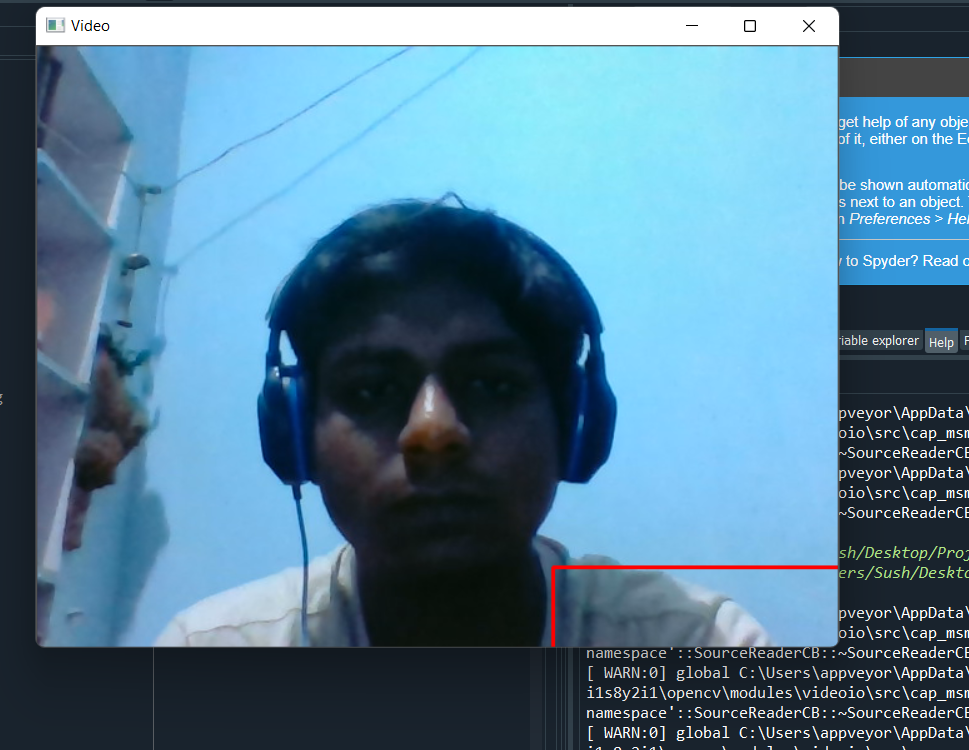
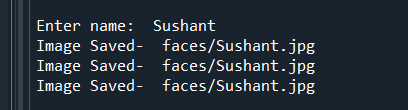
*# Release handle to the webcam*

*video\_capture.release()*

*cv2.destroyAllWindows()*

**Chapter 4.**

[**Results analysis and validation**](file:///U:\Uni%20Project\Sem%205\Final%20Project%20report.docx#_Toc204013784)



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

**ECE ARCHIVES PROJECT SUBMISSION FORM**

Project Code: **CU/ECE/20\_\_\_\_/Sem\_\_\_\_/UID\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (To be filled by Office)**

Project Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and UID of student: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Team Members:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Name** | **UID** | **Semester** | **Contact No.** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| 5. |  |  |  |  |

**Section to be filled by Project Mentor**

**Status (Please tick, whichever applicable)**

|  |  |  |  |
| --- | --- | --- | --- |
| Working |  | Not Working |  |
| **Marks Awarded** | | **60** |  |

Project Mentor Details:

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Employee ID \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sign \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Section to be filled by Project Examiner(s)**

**Status (Please tick, whichever applicable)**

|  |  |  |  |
| --- | --- | --- | --- |
| Working |  | Not Working |  |

Project Examiner Signatures:

Internal \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Employee ID \_\_\_\_\_\_\_\_\_\_\_\_\_\_

External \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Employee ID \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_