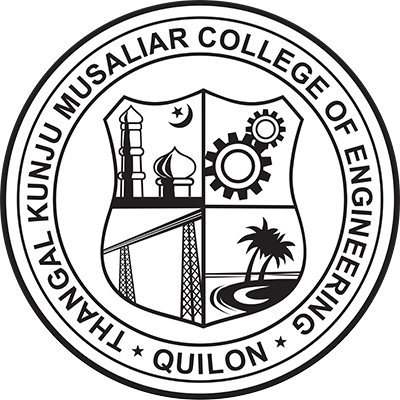
# **ANTI-PHISHING BASED ON** VISUAL CRYPTOGRAPHY

**Department of Computer Science and Engineering**

T.K.M College of Engineering, Kollam

December 2022



# ANTI PHISHING BASED ON VISUAL CRYPTOGRAPHY

Project Phase II Report

Submitted By

**ANAGHA P SANTHOSH (TKM19CS015)**

**EMIL JOJI (TKM19CS022)**

**JISHNU M (TKM19CS030)**

**PRANAV K (TKM19CS049)**

to

*APJ Abdul Kalam Technological University*

*in partial fulfillment of the requirements for the award of B.Tech Degree*

*in Computer Science and Engineering*

# DECLARATION

We undersigned hereby declare that the project report on Anti-Phishing Based On Visual Cryptography, submitted as part of the course, Project Phase I, under APJ Abdul Kalam Technological University, Kerala is a bonafide work done by us under supervision of Dr. Dimple A Shajahan, Professor of Computer Science & Engineering Department, TKMCE, Reena Mary George, Assistant Professor, TKMCE. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the Institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place : Kollam

Date :

Anagha P Santhosh

Emil Joji

Jishnu M

Pranav K

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**T.K.M COLLEGE OF ENGINEERING, KOLLAM**

****

# CERTIFICATE

This is to certify that the report titled **Anti-phishing based on Visual Cryptography** submitted by **Anagha P Santhosh, (TKM19CS015), Emil Joji (TKM19CS022), Jishnu M (TKM19CS030), Pranav K (TKM19CS049)** to the APJ Abdul Kalam Technological University in completion of the requirements for the award of Bachelor of Technology Degree in Computer Science and Engineering during 2022 – 2023 is a bonafide record of the **Project Phase II** carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Project Coordinators Head of the Department

External Examiner

# 

# ACKNOWLEDGEMENT

We take this opportunity to express our deep sense of gratitude to the Almighty and sincere thanks to all who helped us to complete Project Phase I successfully.

We express our sincere gratitude to **Dr. T. A. Shahul Hameed**, Principal, TKMCE, for providing us with all the necessary facilities and support for doing the seminar.

We are extremely grateful to **Dr. Dimple A Shajahan**, Project Coordinator and Head of Department, Department of Computer Science and Engineering, **Prof. Reena Mary George**, Assistant Professor, Department of Computer Science and Engineering, and **Prof. Nisa A K**, Associate Professor, Department of Computer Science and Engineering, for their constructive guidance, advice, constant support and technical guidance provided throughout the preparation of this project. Without their intellectual support and appropriate suggestions at the perfect time, this project would not have been possible.

We extend our immense gratitude to all faculties and technical staff in the Department of Computer Science and Engineering, for their help and necessary facilities to complete the seminar. Our humble gratitude and heartiest thanks also go to our parents and friends, who have supported and helped us on the course of this work.

**Ms. Anagha P Santhosh**

**Mr. Emil Joji**

**Mr. Jishnu M**

**Mr. Pranav K**

# ABSTRACT

Email is a global service used by over a billion people. Flexibility, reliability and convenience make email a popular communication service. Despite its advantages, email can also serve as a vector for cyberattacks, phishing being only one of them. Phishing is the act of sending emails containing the website links which mirror some actual websites. The email will prompt the recipient to provide confidential information, such as account information, PINs, or passwords and the website's owners will use the details to commit fraud. As a security precaution against phishing an anti-phishing technique based on Completely Automated Public Turing Test to Tell Computers and Humans are Apart(CAPTCHA) employing multiple secret sharing has been developed. The suggested method provides five levels of security. The first layer determines whether or not the consumer is a certified customer. The website only allows signed-in users who have been authenticated. The second layer shields the client's system from potential keylogger and screen loggers. The third layer verifies if the client's information is related to the picture captcha. Human users alone can solve the image captcha. No machine-based client can therefore decipher the secret word or any other personal information of the client using captcha strategy. The picture captcha in the fourth layer is made by stacking the shares of the end user and the server and it cannot display the original image captcha for that specific user, who is attempting to log in to the site if the website is phishing. Additionally, the client may easily keep track of how many transactions have already been made using this method, adding a fifth layer of protection. Various evaluation parameters like Precision, F-Measure, Specificity, Balanced Classification Rate (BCR) or Area Under the Curve (AUC) between the original image and secrets, generated by stacking the shares, has comparable value making the proposed approach suitable for preventing phishing attacks.

# CONTENTS

1. INTRODUCTION 9
2. MOTIVATION 10
3. LITERATURE SURVEY 11
4. OBJECTIVES 12
5. PROPOSED DESIGN 13

5.1 REGISTRATION PHASE 14

5.2 LOGIN PHASE 14

1. PROPOSED METHODOLOGY 15

6.1 REGISTRATION PHASE 15

6.2 LOGIN PHASE 15

1. COST ESTIMATION 17
2. EXPECTED OUTCOMES 18
3. TIMELINE 19
4. IMPLEMENTATION
5. RESULT
6. SOFTWARE AND HARDWARE REQUIREMENTS 22
7. CONCLUSION AND FUTURE SCOPE
8. ABBREVIATIONS 23
9. REFERENCES 24

# LIST OF FIGURES

| Figure | Title | Page no |
| --- | --- | --- |
| 5.1 | Registration Process |  |
| 5.2 | Login process |  |
| 10.1 | Registration page |  |
| 10.2 | User’s share |  |
| 10.3 | Login page |  |
| 10.4 | Face recognition |  |
| 10.5 | Captcha verification |  |

# LIST OF TABLES

| Table No | Title | Page no |
| --- | --- | --- |
| 11.1 | Comparison of OpenCv vs Haar Cascade Method |  |
| 11.2 | Comparison of OpenCv with TensorFlow/ Keras Based and Haar CascadeMethod |  |

# 

# 1. INTRODUCTION

Email is a global service used by over a billion people. Flexibility, reliability, and convenience make email a popular communication service. Despite its advantages, email can also serve as a vector for cyberattacks, phishing being only one of them.

Phishing is a cyber attacking technique that uses deceptive emails, messages, or websites to trick individuals into revealing sensitive information like passwords or financial details. It often mimics trusted entities, aiming to exploit human vulnerabilities and gain unauthorized access to personal data or commit fraud. Vigilance and caution are crucial in combating phishing threats.

Anti phishing refers to the set of measures and techniques employed to prevent and protect against phishing attacks. Anti phishing methods include email filtering, user education and awareness, website authentication, multi-factor authentication, and the use of security technologies like anti-phishing software and browser extensions. The goal is to detect and prevent phishing attempts, safeguard user information, and maintain online security.

Anti Phishing based on visual cryptography is a security approach that utilizes the principles of visual cryptography to combat phishing attacks.Visual cryptography is a cryptographic technique that involves encrypting a secret image into multiple shares, which are distributed among participants. The shares themselves do not reveal any information about the original secret image, but when superimposed or combined, the secret image can be visually revealed without the need for complex computations. It involves encrypting sensitive information, such as login credentials or personal data, into multiple shares using visual cryptographic techniques. By distributing these shares across different visual elements, it becomes difficult for phishers to extract the original information. Visual cryptography enhances the security and resilience of authentication processes, providing an effective defense against phishing threats.

An approach to prevent phishing based on visual cryptography has been proposed which includes two phases,Registration phase and Login Phase.

In the Registration phase, the user is prompted for photograph and user name along with the necessary information required by the website. The server links the username to the randomly generated group of words, and a CAPTCHA image is generated. Using the MultiSecret Sharing Scheme, the processed secret picture is divided into 2 shares: one for the user and others for the server. Additionally, the user can imprint his/her share on a physical transparency and it serves as the user's share during the login stage for later confirmation. The original CAPTCHAs are stored in the server's database.

In the Login phase, when attempting to log into a website, a user must enter the username. When the client enters a username, the server activates the webcam so it may examine the user's face. Here, the server uses the user's original photo stored in the server and compares it to the user's face. If a match is made, the end user is a real customer and as a result, the server can verify the legitimacy of the user. After that, the server displays its digital share on the user's screen. Since the shares in our suggested solution are in different modes (one is in digital mode and the other is in physical mode), the secret is revealed by virtual stacking of the shares. The user prioritizes his physical share over the server's digital share. The secret revealed i.e, the CAPTCHA is entered and if it matches with one of the captchas stored in server login succeeds else fails.

# 

# 

# 

# 

# 

# 2. MOTIVATION

Online abuses have been rising quickly as a result of cutting-edge web improvements. The most well-known abuses committed by online criminals today are phishing scams. Theft of confidential information from electronic correspondence, such as client names, passwords, and Visa information, is a crime. It's a form of deception with the intention of gaining money and engaging in other fictitious activities. It makes use of fraudulent websites that look like legitimate ones. Links to websites that are infected with malware may be included in phishing communications.Visual Cryptography has become widely popular and preferred recently. It is a data security method that permits effective and efficient secret sharing between a number of trusted parties.

We are focusing on shielding the client's system from potential keylogger and screen logger's assaults by providing only minimal information through the user’s console. Other functionalities involve testing the authenticity of the user and website’s originality..Our main motivation for choosing this topic is because of its relevance and computational simplicity. We believe that a website built with the proposed schemes can protect users from phishing attacks and provide a more secure environment for online transactions.

# 

# 3. LITERATURE SURVEY

With the cutting-edge improvement of the web, online abuses have been increasing rapidly. Phishing is the most widely recognized abuse performed by digital crooks nowadays. It is an activity to steal private data (for example, client names, passwords and Visa data) in an electronic correspondence. It is a sort of fraud with the end goal of monetary benefit and other fake exercises. It utilizes phony websites that resemble genuine ones. Phishing messages might contain links to sites that are contaminated with malware. In the referenced paper, ‘‘an anti-phishing approach using a multi secret sharing scheme" is implemented as an answer to this problem. Here, Dynamic Image CAPTCHA based verification using multi secret sharing is performed. Image CAPTCHA is divided into two pieces called shares. Multiple secret pictures are revealed by overlapping the same set of shares at different angles. In the proposed approach, shares are of different modes i.e., user’s share is imprinted on a physical transparency while server’s share is in digital mode. By using the proposed approach, websites and end clients can cross confirm their identity.

In the referenced paper the approach used has two phases: Registration phase and Login Phase. In the Registration phase, the user is prompted for photograph and user name. The server links the username to the randomly generated group of words, and a CAPTCHA image is generated. To prevent pixel growth in the generated shares, the generated image CAPTCHA has undergone pre-processing. The algorithm used to pre-process secret images has received input from many secret images. Using the MultiSecret Sharing Scheme, the processed secret picture is divided into two shares: one for the user and one for the server.The user’s which the server prints on a physical transparency and gives to the user. Additionally, it serves as the user's share during the login stage for later confirmation. The additional link and original picture CAPTCHAs are stored in the server's database.

In the Login phase, the user enters the username when attempting to log into a website. The server activates the webcam so it may examine the user's face. Here, the server fetches images stored in the database to compare it to the user's face. If a match is made, the end user is a real customer and as a result, the server can verify the legitimacy of the user. After that, the server displays its digital share on the user's screen. Since the shares in our suggested solution are in different modes (one is in digital mode and the other is in physical mode), the secret is revealed by virtual stacking of the shares. The user prioritizes his physical share over the server's digital share. The secret revealed is compared to the CAPTCHA image created during registration. The exact match between the resultant image and the original secret kept by the server allows the user to login to the website.

Haar cascade and LBP are popular techniques in the field of computer vision and image processing.Haar cascade classifiers are based on Haar-like features, which are rectangular image filters used to detect specific patterns or features. In the context of facial recognition, Haar cascade classifiers are commonly used for face detection. They work by training a classifier on a large number of positive and negative face samples to identify facial features such as eyes, nose, and mouth. Once the face is detected, it can be further processed for recognition or analysis. LBP classifiers, on the other hand, are based on the concept of Local Binary Patterns. LBP is a texture descriptor that characterizes the local structure and texture patterns in an image. In facial recognition, LBP is often used for face representation and feature extraction. It works by comparing the central pixel value with its neighboring pixels and encoding the comparisons into binary patterns. These patterns can then be used as features for face classification or recognition.The combination of Haar cascade and LBP classifiers is a common approach in facial recognition systems. Haar cascade is used for face detection, while LBP is used for feature extraction and recognition. This combination leverages the strengths of both techniques to achieve accurate and efficient facial recognition.

Face recognition using OpenCV involves several steps. First, a face detection algorithm is applied to locate faces in an image or video stream. OpenCV provides built-in face detection algorithms like Haar cascades and deep learning-based models.Once the faces are detected, facial features are extracted from each face, such as the position of eyes, nose, and mouth. These features are used to create a unique representation of the face, often referred to as a face embedding or face descriptor.To recognize a face, a comparison is made between the face embeddings of the detected faces and a set of known face embeddings stored in a database. Various techniques can be employed for face matching or identification, such as Euclidean distance, cosine similarity, or machine learning-based classifiers.OpenCV can also be used for training a face recognition model. This involves collecting a dataset of labeled faces, extracting their features, and training a machine learning algorithm to create a model that can identify new faces. Face recognition using OpenCV has diverse applications, including access control systems, surveillance, human-computer interaction, and social media tagging. It provides a reliable and efficient way to automatically identify individuals from images or video streams.

# 4. OBJECTIVES

Phishing attacks are on the rise as a result of the increased use of the internet for online shopping, financial transactions, and e-learning. The attackers create websites that are exact replicas of other websites and they steal client's confidential information to profit financially or to harm the client by leaking it publicly. As a security measure against phishing, an anti-phishing mechanism based on Image CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans are Apart) using Multiple secret sharing has been proposed. In the proposed mechanism, the website cross confirms its identity and demonstrates that it is a trustworthy and authenticated website for various online transactions before the end users. This system utilizes the ideas of image processing, visual cryptography and multi secret sharing.

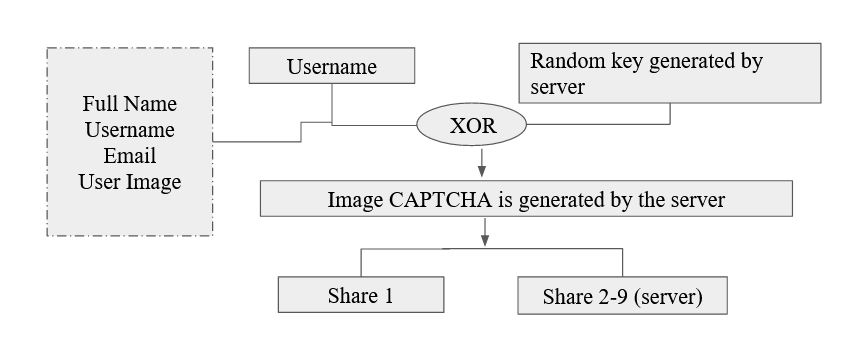
# 5. PROPOSED DESIGN

An anti-phishing approach based on image CAPTCHA by utilizing the Multi Secret Sharing Scheme is proposed in our project.

It has two phases

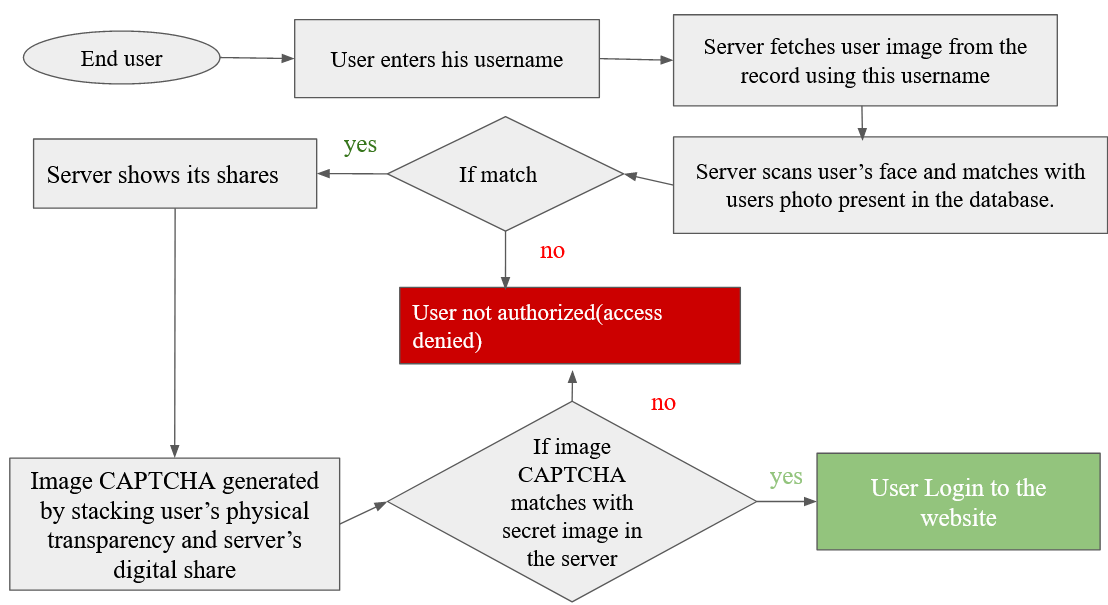
1. Registration Phase
2. Login Phase

## **5.1 REGISTRATION PHASE**

****

5.2 Registration Process

## **5.2 LOGIN PHASE**



5.3 Login Process

# 6. PROPOSED METHODOLOGY

## **6.1 REGISTRATION PHASE**

In the Registration phase, the user’s name, username, email and image are asked from the user. Username can be any combination of alphabets and numbers and it's unique for each user . Username along with random key generated by server is XOR-ed to generate Image CAPTCHA. Image CAPTCHA may be a different combination of letters and digits from 0 to 9. The processed secret image i.e, Image CAPTCHA is splitted into 9 shares. One for the user and the rest 8 shares for the server. The users’ share is imprinted on a physical transparency and will be given to the user. It additionally serves as the user’s share for later confirmation during the login stage. The other shares and original image CAPTCHAs are kept in the database of the server. The common user’s share is stacked with one of the server shares to obtain CAPTCHA. The captcha generated is unique for each user and cannot be reused for other users.The stacking of shares each time generates a CAPTCHA which matches one of the 8 CAPTCHAS listed by server. Algorithm of Registration phase takes Username as an input and generates shares. Image captcha (IC) is produced as a result of XOR operation on username and randomly generated string (RK). Then, multiple secret images of this Image CAPTCHA are generated.

**6.2 LOGIN PHASE**

At the time of login to a website, a user is needed to enter the username. The server then fetches the user’s image which was uploaded during the registration phase using the username. The server switches on the user’s webcam so that the server can scrutinize the user's face. Here, the server matches the user’s face with the user’s photograph fetched from the database. If a match happens, the end user is a genuine client. From that point onward, the server shows its digital share onto the screen before the user. The user can stack its share printed on physical transparency on the top of the share displayed,this would reveal a captcha. This captcha is then entered by the user. If it matches one of the captchas stored in the server the user is granted access to the website else login fails. In this proposed approach, the shares are in various modes (one is in digital mode and other is in physical mode), and virtual stacking of shares happens to uncover the secret i.e, captcha. The revealed secret is compared with the CAPTCHAs formed at the registration time. At the time of stacking of user’s share and the server’s share, a new image CAPTCHA will be revealed every time. In the proposed scheme, the user's share is imprinted on physical trans-parency. The server's share is digital in nature which will be displayed on the screen at the time of login. The user has to stack his physical transparency onto the digital share displayed on the screen. The exact match between the resultant image and the original secret kept by the server allows the user to login to the website. As server’s and user’s shares are of different modes, then it will surely improve the security of the system. Moreover, if a user lost his physical transparency that is found by some X user. Somehow X also got the original user’s username and tries to login to the system, then the server scans his face through the webcam of his computer system and matches it with the photograph extracted from the QR Code. There will be an obvious mismatch and user X is not allowed to login to the system.

Face recognition typically involves two main steps: face detection and face identification/verification. Here face recognition is done with the help of OpenCV. The user’s photograph is stored in the server under the username and when the user enters his username the corresponding photo is fetched. Through a webcam the user's face is detected and then verified. If the face matches with the photograph, this layer of security is fulfilled, as face recognition is a biometric technology that involves identifying or verifying individuals based on their facial features.

# 

# 

# 

# 

# 7. COST ESTIMATION

The project estimates the cost using the **COCOMO Model.** Based on the size, experience and knowledge of the team, a *semi-detached* mode was chosen.

Hence,

* a = 3.0
* b = 1.12
* c = 2.5
* d = 0.35

The following parameters were calculated:

* *KLOC* (Expected) = 7
* *Effort* = *a(KLOC)b* = 25.523 Person-Month
* *Development Time* = *c(Effort)d* = 7.87 Months
* *Average staff required* = *Effort* / *Development Time* = 4 Persons

The approximate expenditure for the given requirements are calculated as:

* + Windows: Free
  + Python: Free
  + Google Slides: Free
  + DJango : Free
  + VSCode : Free

# 8. EXPECTED OUTCOMES

The proposed approach gives multiple layers of safety:

1. It determines if or not the customer is a registered customer as the server can ensure the authenticity of the user by matching his photo and his face through the webcam of the user's framework.
2. It shields the client's system from potential keylogger and screen logger's assaults as only less information is entered through the console.
3. It verifies whether the client is associated with the image captcha.
4. Only human clients can read the CAPTCHA.
5. Generates multiple captcha
6. It confirms the website's originality.

# 9. TIMELINE

| **NOV** | **DEC** | **JAN** |
| --- | --- | --- |
| Topic Selection | Research on already existing techniques | Implementation of methods to generate image shares |
| Paper Selection | Comparison of methods | Comparison of results generated |
| Paper Study | Brainstorming the project ideas | Creating a layout for research paper |
| Understanding the methodology | Finalizing the idea for first implementation | Accumulating information for paper |
|  | Discussion with guide for approval |  |
|  | Researching already existing projects |  |
|  | Fixing the tech stack to be used |  |
|  | Studying the tech stack |  |
|  | 40% of implementation of the project |  |

| **FEB** | **MAR** | **APR** | **MAY** |
| --- | --- | --- | --- |
| Keeping record of the current method | Completion of Login phase | Draft 2 of paper | Final draft |
| Completion of registration phase  : 60% implementation | Complete implementation | Result analysis | Final presentation |
| Creating first draft of paper | Start individual performance analysis |  |  |
|  | Documentation of results |  |  |
|  | Combined performance analysis |  |  |

# 

# 

# 

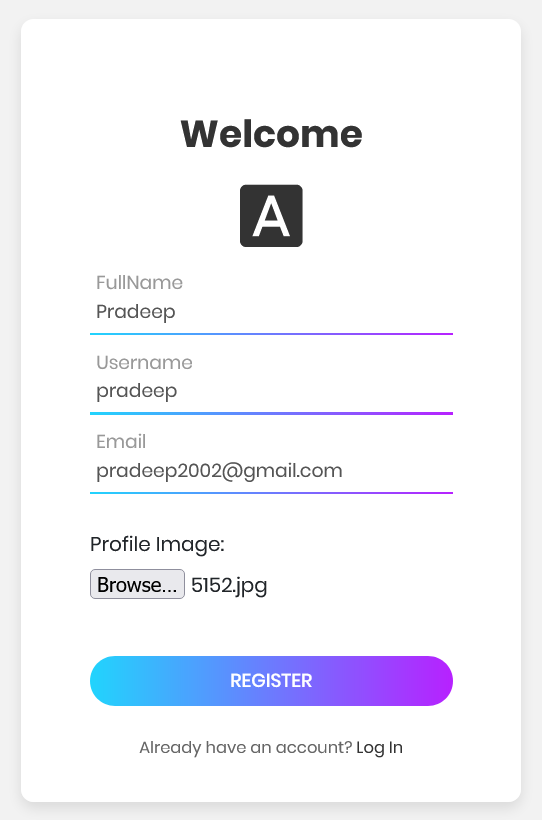
# 

# 

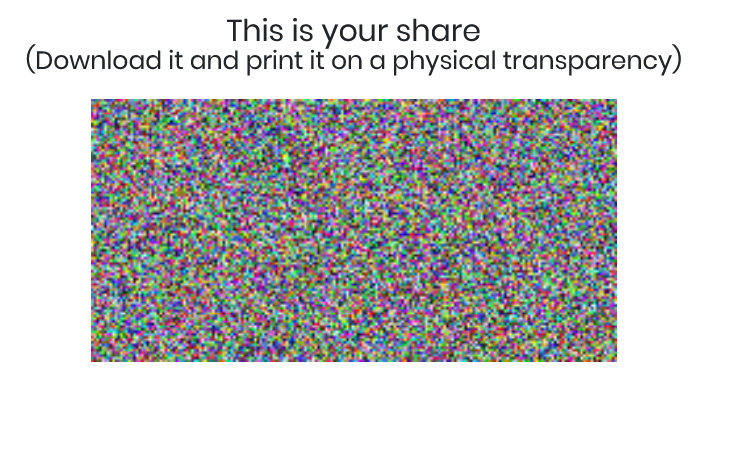
# 

# 

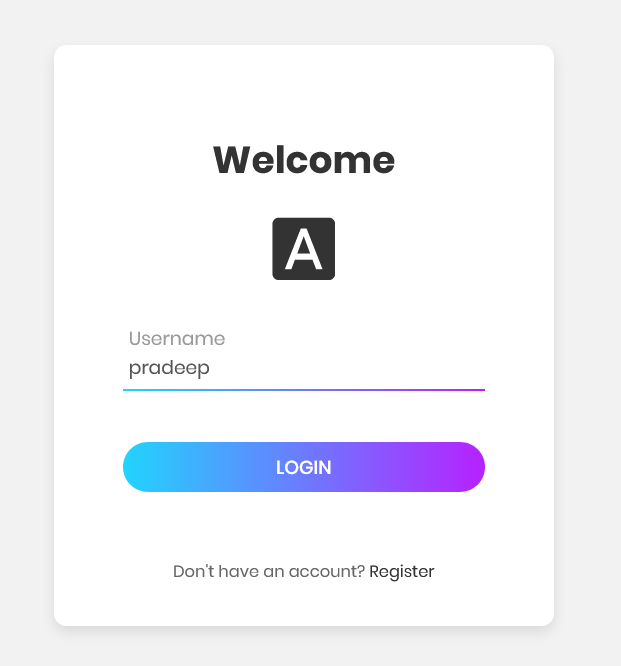
# 10. IMPLEMENTATION



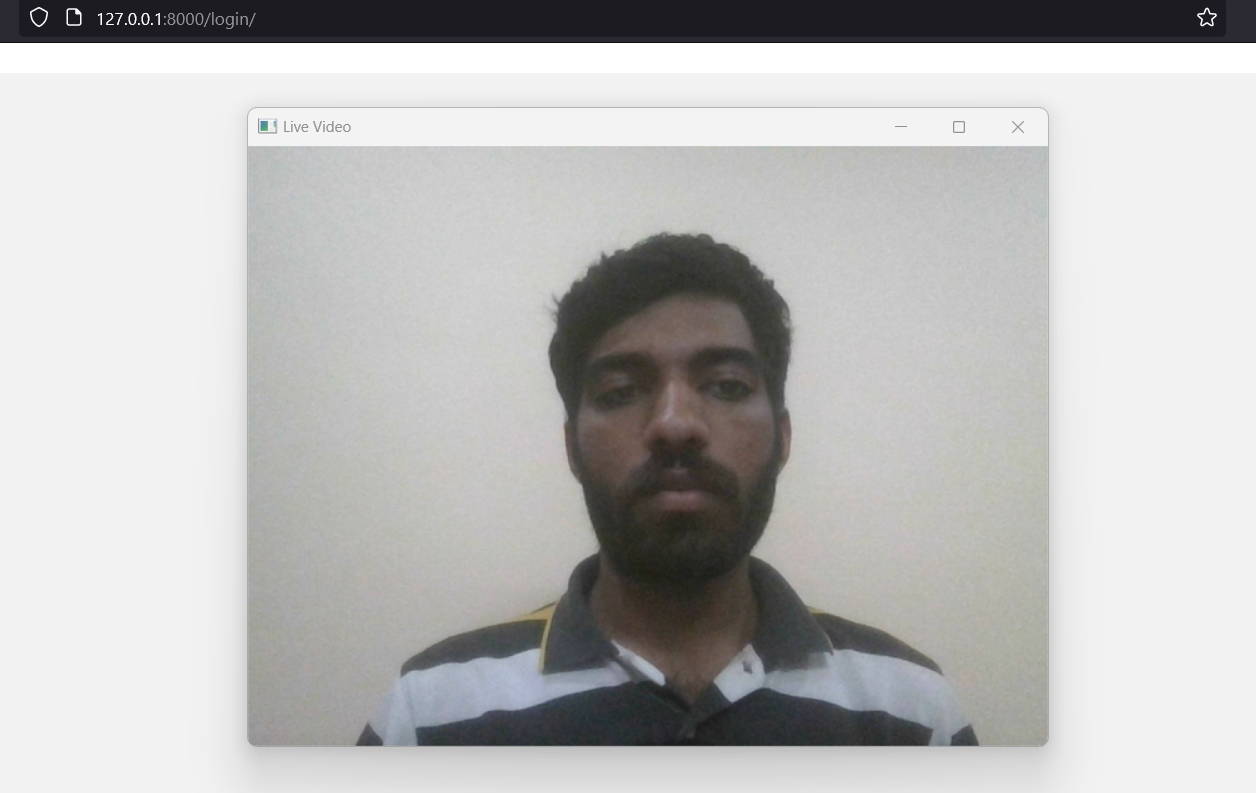
10.1 Registration page



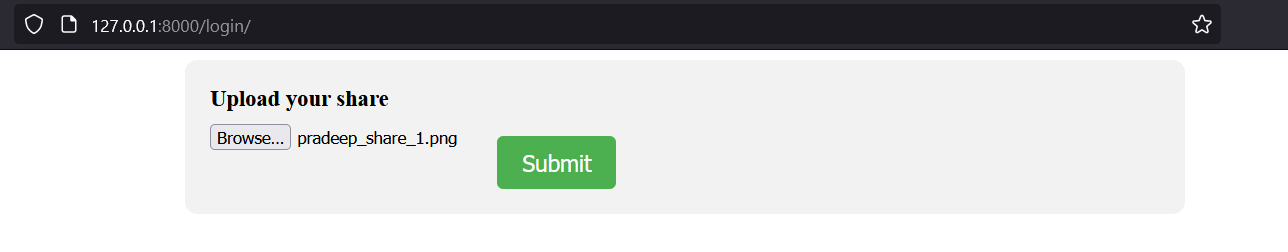
10.2 User’s share



10.3 Login



10.4 Face recognition



10.5 Upload User share



10.5 Captcha verification

# 

# 

# 

# 

**11.RESULT**

| **Metric** | **Haar Cascade Method** | **OpenCV Face Recognition Module** |
| --- | --- | --- |
| Accuracy | 80%-90% | 85%-95% |
| Speed (Frames Per Second) | 30+ | Varies depending on algorithm and hardware |
| False Positive Rate (FPR) | 0.1-0.5 | 0.09-02 |
| True Positive Rate (TPR) | 0.7- 0.9 | 0.8-0.9 |
| Area Under Curve (AUC) | 0.8-0.95 | Varies |
| Mean Average Precision (mAP) | 0.75-0.9 | 0.8-0.9 |
| Execution Time (per face) | 10- 100 milliseconds | Varies depending on algorithm and hardware |
| Failure Rate | 5%-20% | Varies |

# 

# 

# Table 11.1 Comparison of OpenCv vs Haar Cascade Method

| **Metric** | **Face Recognition Library** | **Tensorflow/Keras based** | **HaarCascade method** |
| --- | --- | --- | --- |
| Speed / Processing time | 100 ms per frame | 80 ms per frame | 50 ms per frame |
| Memory usage | 100 MB | 150 MB | 50 MB |
| Model size | 100 MB | 200 MB | No model required |
| Dependencies | Face\_recognition,OpenCV | Tensorflow,Keras, OpenCV | OpenCV only |
| Accuracy | 0.92 | 0.87 | 0.75 |
| Ease of implementation | Simple and straightforward | More complex due to model training loading | Simple straightforward |

# Table 11.2 Comparison of OpenCv with TensorFlow/Keras Based and Haar Cascade Method

# 

# The complexity of searching user’s image for comparing is O(1) as image stored in particular username only is being fetched for comparison

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 12.SOFTWARE AND HARDWARE REQUIREMENTS

For Windows:

● Operating Systems: Windows10 or later (64-bit), x86-64 based.

● Disk Space: 1.64 GB (does not include disk space for IDE/tools).

● Tools: Python DevTools

For Unix-Based:

● Operating Systems: macOS Big Sur or later / Ubuntu 16.04 or later

● Disk Space: 2.8 GB (does not include disk space for IDE/tools).

● Tools:. Python DevTools

Programming Standards

● Readable, Maintainable, and Optimized code.

● Must follow indentation.

● Must follow proper exception handling.

● Class names should start with capital letters.

● Intel i5 processor

**13. CONCLUSION AND FUTURE WORKS**

Although the anti-phishing strategy that was adopted, based on Dynamic Image CAPTCHA and Multi-Secret Sharing Scheme, has shown encouraging results, there are still a number of areas that might use better. For upcoming research and development, the following areas can be taken into account:

1. **Enhanced CAPTCHA Generation**: Investigate advanced techniques for generating dynamic image CAPTCHAs that are more resilient to automated attacks. This could involve exploring novel image manipulation algorithms, incorporating machine learning approaches to generate personalized CAPTCHAs, or leveraging additional user-specific information to increase the complexity of the CAPTCHA generation process.
2. **Usability and User Experience**: Conduct user studies to assess the usability and user experience of the implemented technique. Collect feedback from users to identify potential areas of improvement, such as CAPTCHA comprehension, ease of interaction, and overall satisfaction. This feedback can be used to refine the technique and make it more user-friendly, ensuring a seamless and effective defense against phishing attacks.
3. **Integration with Mobile Devices**: Investigate the adaptation of the implemented technique for mobile devices, considering the unique challenges and constraints of mobile platforms. Develop methods to seamlessly integrate the technique into mobile applications and web browsers, ensuring consistent protection against phishing attacks across different devices.
4. **Multi-Secret Sharing Scheme Enhancements**: Further research can be conducted to enhance the multi-secret sharing scheme used in the project. This could involve exploring alternative secret sharing algorithms, investigating the scalability and efficiency of the scheme for large-scale deployments, or considering the integration of cryptographic primitives for stronger security guarantees.
5. **User Awareness and Education**: Recognizing that user awareness plays a crucial role in combating phishing attacks, future efforts can focus on designing educational campaigns and interventions to educate users about phishing risks, detection techniques, and safe online practices. This can complement the implemented technique by empowering users to make informed decisions and actively contribute to their own online security.
6. **Real-world Deployment and Evaluation**: Validate the implemented technique in real-world settings by deploying it in a production environment and evaluating its performance over an extended period. This will provide valuable insights into its effectiveness, scalability, and practicality in mitigating phishing attacks.

By addressing these future research directions, the anti-phishing technique based on Dynamic Image CAPTCHA and Multi-Secret Sharing Scheme can be further improved, strengthened, and adapted to the evolving landscape of phishing attacks, ultimately enhancing the security and protection of users against such threats.

# 14. ABBREVIATIONS

1. VCS- Visual Cryptography Scheme
2. VSS- Visual Secret Sharing
3. EVC - Extended Visual Cryptography
4. HVC - Halftone Visual Cryptography
5. MSS - Multi Secret Sharing
6. LBP- Local Binary Patterns

# 

# 

# 14. REFERENCES

1. Akanksha Arora, Hitendra Garg, Shivendra Shivani,Anti-phishing technique based on dynamic image captcha using multi secret sharing scheme,Journal of Visual Communication and Image Representation,Volume 88,2022.
2. R.G. Sharma, P. Dimri, H. Garg, Visual cryptographic techniques for secret image sharing: a review, Inf. Secur. J.: Glob. Perspect. 27 (2018) 241–259.
3. Peng Li, Jianfeng Ma, Quan Ma,(t, k, n) XOR-based visual cryptography scheme with essential shadows,Journal of Visual Communication and Image Representation,Volume 72,2020.
4. Anirudha B Shetty, Bhoomika, Deeksha, Jeevan Rebeiro, Ramyashree,Facial recognition using Haar cascade and LBP classifiers, GlobalTransitions Proceedings,Volume 2, Issue 2,2021