**Table of Contents**

**CERTIFICATE 02**

**DECLARATION 03**

**ACKNOWLEDGEMENT 04**

**CHAPTER 1. INTRODUCTION ………05**

1.1 **PROJECT SUMMARY** 05

1.2 **PROJECT AIM** 05

1.3 **OBJECTIVE** 06

1.4 **SCOPE** 06

1.5 **PROBLEM DEFINITION** 07

**CHAPTER 2. LITERATURE SURVEY 09**

2.1 **VCS for Secret Image Retrieval** 09

2.2 **Progressive VCS and RST Attacks.** 09

2.3 **Extended Visual Cryptography** 10

2.4 **IMAGE WATERMARKING** 10

2.5 **Hybrid Page Layout Analysis** 11

**CHAPTER 3. WORK PROPOSED …………………………………………………12**

3.1 **BLOCK DIAGRAM OF REGISTRATION PAGE** 12

3.2 **BLOCK DIAGRAM OF LOGIN PAGE** 13

3.3**MODULES** 13

3.4**TOOLS** 14

**CHAPTER 4. UML DIAGRAMS …………………………………………………..15**

4.1 **BLOCK DIAGRAM** 15

4.2 **ACTIVITY DIAGRAM** 16

4.3 **ADMIN USE-CASE DIAGRAM** 17

4.4 **USER USE-CASE DIAGRAM** 18

**CHAPTER 5. RESULTS 20**

**CHAPTER 6. CONCLUSION………………………………………………………20**

**REFERENCES 21**

**APPENDIX 22**

**1. INTRODUCTION**

**1.1 PROJECT SUMMARY**

SAFEPASS is the easier, safer way to unlock your digital world. It’s an application you can download on all your devices to remove the hassle of passwords. Get started by logging in to the SAFEPASS app using unique factors such as your IMAGE as a password or a device you own.

From there, the app works quietly in the background to make your current passwords stronger, remembers them and instantly logs you in – so you don’t have to. The SAFEPASS app offers customizable security so you can log in with the factor for fast access, or combine multiple factors together for added security – you decide.

**1.2 PROJECT AIM**

Master password is the easier, safer way to unlock your digital world. It’s an application you can download on all your PC to remove the hassle of passwords. Get started by logging in to the Master password app using unique factors image. From there, the app works quietly in the background to make your current passwords stronger, remembers them and instantly logs you in so you don’t have to.

The app offers customizable security so you can log in with one factor for fast access, or combine multiple factors together for added security you decide. Phishing means is the attempt to gain sensitive information of a user such as usernames, passwords, and credit card details, by impersonating as a credible entity in Internet logins.

In this project we have proposed new approach for secure online login system using Visual Cryptography and Steganography. In this Visual cryptography is applied on confidential data such as username and password image from which two shares are generated. One share is saved at the server site and second Share is steganography with reCHAPTCHA image or User Define image. Whenever user want to login, they will produce username and image or reCHAPTCHA and if authentication is done then login will successfully if two try is wrong then notification is send to user mail.  Master Login respects your privacy. Your passwords belong only to you accessible only by you. We never share or sell your data.

**1.3 OBJECTIVE**

This web application is designed to save your time, simplify your life and keep your private information safe. This app’s innovative features distinguish it from other password managers.

Speaking of handy features, one of our favourites is being able to instantly log into our sites whenever we need to, even on mobile devices. There aren’t many things that are more annoying than typing passwords over and over just to encounter the “invalid password” message time and time again. We know the drill; you enter your password, an error message appears, you check that caps lock is off, re-enter your password - this time, typing each letter individually to make sure to hit all the correct letters - just to go back to square one.

With this app, you can add a new Login, edit an existing Login and instantly sign into your sites all within the browsers on iOS and Android devices.

**1.4 SCOPE**

Here's how we keep your information secure:

* Your passwords and wallet items are encrypted on your own device using AES-256, the strongest encryption available.
* Only you have access to your information. We verify it's you using things that are unique to you (A password image generated, a Trusted Device, or a Master Password that is only known by you). The more factors you have and use, the stronger your SafePass profile becomes - you'll be prompted for at least one factor (in addition to using a Trusted Device) whenever you log in for stronger security.
* No readable password or wallet information is sent over the Internet – not even to our servers.
* We've also put many other measures in place to make sure no one can access your information, including secure data centres with advanced network security systems, continuous real-time security monitoring, secure coding practices and third-party security reviews.
* In addition, we provide multiple security controls so that users can decide how to configure the SafePass app based on their needs. You can use our Password Generator to create strong passwords. Turn on auto-lock. And you can set up the app to always ask for your Master Password.
* This application will work on your favourite phones, tablets, and computers. The platforms we are preparing for includes:
  + **Operating Systems:** Mac OS X, Windows, Android &iOS  
    **Browsers:** Chrome, Internet Explorer, Microsoft Edge, Firefox, Safari  and Chrome (for iOS)

**1.5 PROBLEM DEFINITION**

* **Is it safe to keep all your passwords in one place?**
* It can seem a bit scary to put all your passwords in one place. However, it's almost impossible to follow password 'best practices' like using long, unique passwords for every single online account without one.
* The SafePass app includes a strong password generator, so it's easy to create the strong, lengthy passwords that security experts recommend for protecting your online accounts. This is important because if you use the same password and username for multiple accounts and that information is stolen, it can be tested against other sites and apps - putting much more than just that one account at risk.
* After helping you create more secure passwords, this app protects them with the strongest security available
* **So, you’ve created a profile on the application, and we’ve asked you to add a Master Password. Welcome! Maybe you’re wondering what a Master Password is or what it does?**
* First things first. What is a Master Password? A Master Password is the only password you’ll ever need to remember now that you’re using the True Key app. The entire premise of a password manager is to eliminate the hassle of passwords and let the app store, safeguard and type your passwords for you.
* That’s where your Master Password comes in. Although you can choose not to enable additional biometric factors, the app allows you to verify yourself using things that you have (your devices), unique thing (image as a password), and things that only you know (your Master Password). When you log into a new device for the first time, we use the Master Password as the primary authentication factor before letting you customize your login preference on that device. Once you do log in, don’t forget to add another factor just in case you ever forget your Master Password (we know, it happens) so you can verify other things about yourself to reset it.
* In the case that you do forget your Master Password, your additional factors will let you reset it. Without an extra factor, you won’t be able to access your profile, and you’ll have to contact our Support team to go through the steps of recreating your profile which means you’ll lose all your saved data, as there is nothing we can do to access or keep it.
* Let’s start by adding another security factor because it is so easy and important. You just need to go to your True Key profile and select which factors you want to add from the list. You can even choose between two security levels (Basic and Enhanced) for the Face feature; the basic level lets you sign in quickly, and the Enhanced version offers increased security.
* Now let’s get back to the basics. If you’re looking to create a Master Password, make it complicated and jumbled with symbols, numbers, upper-case, and lower-case letters. Always remember the golden rule of creating strong passwords: Never make it easy to remember, because a password that’s easy to remember is also likely to be easily guessed. A good password strategy is to think up a mix of random, memorable phrases and incorporate a blend of symbols and numbers. For example, **“iL0vePUPPIES&allofthethingsfloral!”** is a good bet. Once you made your passphrase, don’t forget to take note of it and stow it somewhere ultra-safe preferably tucked away deep inside your brain.

**2. LITERATURE SURVEY**

**2.1 LITERATURE TITLE: Reversible Image Secret Sharing**

**PUBLICATION DATE: 2020**

**METHODOLOGY/ALGORITMS:**

*Algorithm 1:* The Proposed (k, n) Threshold Reversible Image Secret Sharing

*Algorithm 2:* The Recovery in the Proposed Reversible Image Secret Sharing for the (k, n)-Threshold.

**SUMMARY:**

The secret image is losslessly decoded by a modular operation, and the original cover image is recovered by a binarization. operation, exhibiting the features of n cover images, no pixel expansion, low recovery operation, lossless recovery and share comprehensibility.

**2.2 LITERATURE TITLE:** **Secure Authentication using Image Processing and VC for Banking Applications**

**PUBLICATION DATE: 2008**

**METHODOLOGY/ALGORITMS:**

*Algorithm 1:* Increasing Intensity of the Image through Pre-processin

*Algorithm 2:* Creation of Shares for 2 out of 2 Scheme

*Algorithm 3 :* Stacking the Shares for 2 out of 2 Scheme

*Algorithm 4 :* Calculate Correlation Coefficient

**SUMMARY:**

In the image protection method, the image in need of protection is set access rights on blocks to generate the corresponding encrypted image and authentication information. They used different public keys and private keys built on RSA**.**

**2.3 LITERATURE TITLE:** **Privacy-Preserved Image Protection Supporting Different Access Rights**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

*Algorithm 1:* Key Generation Algorithm.

*Algorithm 2:* Image Protection Algorithm

*Algorithm 3:*ImageMap and Authentication Information Generation Algorithm.

*Algorithm 4:* Coding Algorithm.

*Algorithm 5:* Image Encryption Algorithm

**SUMMARY:**

In the image protection method, the image in need of protection is set access rights on blocks to generate the corresponding encrypted image and authentication information.

They used different public keys and private keys built on RSA.

**2.4 LITERATURE TITLE:** **Visual Cryptography Technique to Share Two Secrets**

**PUBLICATION DATE:2020**

**METHODOLOGY/ALGORITMS:**

*Step 1:* Take the two secret images A and B.

*Step 2:* Apply (2, 2) VC technique on image A and generate two shares, share 1 and Share 2.

*Step 3:* Flip the share 2 horizontally

*Step 4:* Select any three subpixel patterns.

*Step 5:* One by one check the pixels in the secret image B.

*Step 6*: Check the corresponding subpixel pattern from share 1.

**SUMMARY:**

This technique has an advantage of sharing two secret images of different dimensions using only two shares. The proposed technique Is applied on different class of binary images and results show that the technique works well for all class of images.

**2.5 LITERATURE TITLE:** **A VC-Based Watermarking Approach for the Detection and Localization of Image Forgery**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

*Algorithm 1:* Shares Construction Phase

*Algorithm 2:* Image Forgery Verification Phase

**SUMMARY:**

This paper, we proposed an approach to detect and localize forgeries in images based on a visual cryptography watermarking scheme. The CASIA V 1.0 and SIPI datasets were used to test the robustness and efficacy of this approach.

**2.6 LITERATURE TITLE:** **Cryptography Based Watermarking approach for the detection and localization of image forgery.**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

Walsh transform, a local binary pattern and a discrete wavelet transform.

**SUMMARY:**

In this paper, an approach to detect and localize forgeries in images based on a visual cryptography watermarking scheme. It provides a good alternative approach for images forgery detection and localization, and it can be used for image copyright protection.

**2.7 LITERATURE TITLE:** **A Review on Visual Secret sharing schemes for binary, gray and color Image.**

**PUBLICATION DATE:2020**

**METHODOLOGY/ALGORITMS:**

1)Boolean Matrix based.

2)Threshold based VCS using Hadamard Matrices.

3)GAS based VC algorithm

**SUMMARY:**

Today’s fast-growing world of the internet is acquiring more attention of people. They exchange multimedia data over the internet thus there is need of data confidentiality integrity and availability. Visual secret sharing(VSS) schemes capable to handle the problem related with sharing of visual data.

**2.8 LITERATURE TITLE:** **Improving the visual Quality of Size invariant visual cryptography for grayscale images.**

**PUBLICATION DATE:2019**

**METHODOLOGY/ALGORITMS:** An analysis by Synthesis(Abs)Approach.

1)ABS-based probabilistic VC.

2)ABS-based vector VC

**SUMMARY:**

Aiming at improving the visual quality of the reconstruction secret image in size-invariant visual cryptography we propose an ABS framework to push the reconstruction error to high frequency band. This framework is flexible in that it can be used in any threshold VC algorithm to improve the visual quality, without sacrificing security.

**2.9 LITERATURE TITLE:** **A privacy preserving biometric recognition system with visual cryptography.**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

Novel feature recognition method

**SUMMARY:**

We construct a meaning VCS, where HVS(Human Visual System) can print shares on transparencies and recover secret images. We propose a secure storage .

**2.10 LITERATURE TITLE: Visually meaningful image encryption based on universal embedding model.**

**PUBLICATION DATE:2021**

**METHODOLOGY/ALGORITMS:**

1)EM based VMIE(visually meaningful image encryption)algorithm.

2)Simulate VMIE for different numbers of embedded bits.

**SUMMARY:**

In this paper, we have proposed a UEM(Universal Embedding Model) based VMIE algorithm. The host domain is divided into the four embedded domains, which are first embedded by using general embedding formula and then adjusted by the correction operation**.**

**2.11 LITERATURE TITLE:** **Design and implementation of a visual cryptography application**

**PUBLICATION DATE:2020**

**METHODOLOGY/ALGORITMS:**

Visual cryptography

2 and 4 shares

**SUMMARY:**

Work with input data image or text on BW and color VISUAL CRYPTOGRAPHY.

Future work using images to hide information, instead of additional information.

**2.12 LITERATURE TITLE:** **Improved schema and evaluation method for progressive visual cryptography**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

Progressive visual cryptography,

information evaluation method

**SUMMARY:**

Evaluation methods for PVC are subjective or difficult to execute without the knowledge of basis matrices. evaluation methods for PVC are subjective or difficult to execute without the knowledge of basis matrices. The method can also confirm the achievement of a forementioned requirements and can be easily executed. by PVC users. future works for the development of PVC.

**2.13 LITERATURE TITLE:** **Online Fraud transaction prevention system using extended visual cryptography and QR code.**

**PUBLICATION DATE:**

**METHODOLOGY/ALGORITMS:**

Extended cryptography

QR code

**SUMMARY:**

This method to prevention using extended visual cryptography and QR code techniques.it

provides better security in preventing phishing attack compared to visual cryptography.

**2.14 LITERATURE TITLE:** **Enhancing security of image Steganography using visual cryptography.**

**PUBLICATION DATE:2021**

**METHODOLOGY/ALGORITMS:**

Steganography,

RGB color images,

visual cryptography

**SUMMARY:**

We have worked on steganography. Process and security for making this system much robust. For steganography operation, we have focused on LSB method and RGB.

Creating this robust tool in proper and perfect way is our future work and to make it happen we will add some features and upgrade it.

**2.15 LITERATURE TITLE:** **An Overview of visual cryptography**

**PUBLICATION DATE:2021**

**METHODOLOGY/ALGORITMS:**

Visual cryptography pixel

**SUMMARY:**

Work with input images using encryption technique to decompose image multiple shares.

Future work is Pixel expansion for image or text.

**2.16 LITERATURE TITLE:** **Enhanced visual cryptography : An Augmented model for image security.**

**PUBLICATION DATE:2020**

**METHODOLOGY/ALGORITMS:**

Visual Cryptography; Secret key; transformed pixel; (3,3) – EVS;(2,3)- VCS.

**SUMMARY:**

Our methods require no overhead and less time for computation. During the decryption process. The secret share is encrypted by dividing it two 3 shares depending on scheme. imposed. Using 2-out-of-3 scheme for transmission will certainly reduce the time required to decrypt the image for recipient.

**2.17 LITERATURE TITLE**: **A new secure transmission scheme**

**between senders and receivers using HVCHC without any loss**

**PUBLICATION DATE:2019**

**METHODOLOGY/ALGORITMS:**

Transmission, Visual cryptography, Hill cipher, medical images, Character conversion

**SUMMARY:**

This proposed method of encryption provides double encryption, the minimum execution time of encryption and decryption, reduces the size from the original after the encryption process, 100% perfect reconstructions, provides better performance against hacker/third parties/attackers.

**2.18 LITERATURE TITLE: XOR-Based (*n*, *n*) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

Secret sharing scheme; visual cryptography; XOR; meaningful shares; pixel expansion

**SUMMARY:**

The theoretical analysis and experimental results showed that both of our schemes can completely recover the original secret image using the XOR operation and that they are secure. Our method can be applied to more situations than the existing schemes, most of which deal. With binary images. We believe our technology can lay the foundation for the future.

**2.19 LITERATURE TITLE: Embedded Extended Visual Cryptography Schemes**

**PUBLICATION DATE:2011**

**METHODOLOGY/ALGORITMS:**

Secret sharing, Embedded extended visual cryptography scheme.

Gray scale, computational modeling

**SUMMARY:**

Comparisons on the experimental results show that, the visual quality of the share of the proposed embedded EVCS is competitive with that of many of the well-known EVCS’s in the literature.

**2.20 LITERATURE TITLE: Flip Extended Visual Cryptography for Grayscale and Color Cover Images**

**PUBLICATION DATE:2022**

**METHODOLOGY/ALGORITMS:**

FL flip visual cryptography (FVC); meaningful shares; error diffusion halftoning

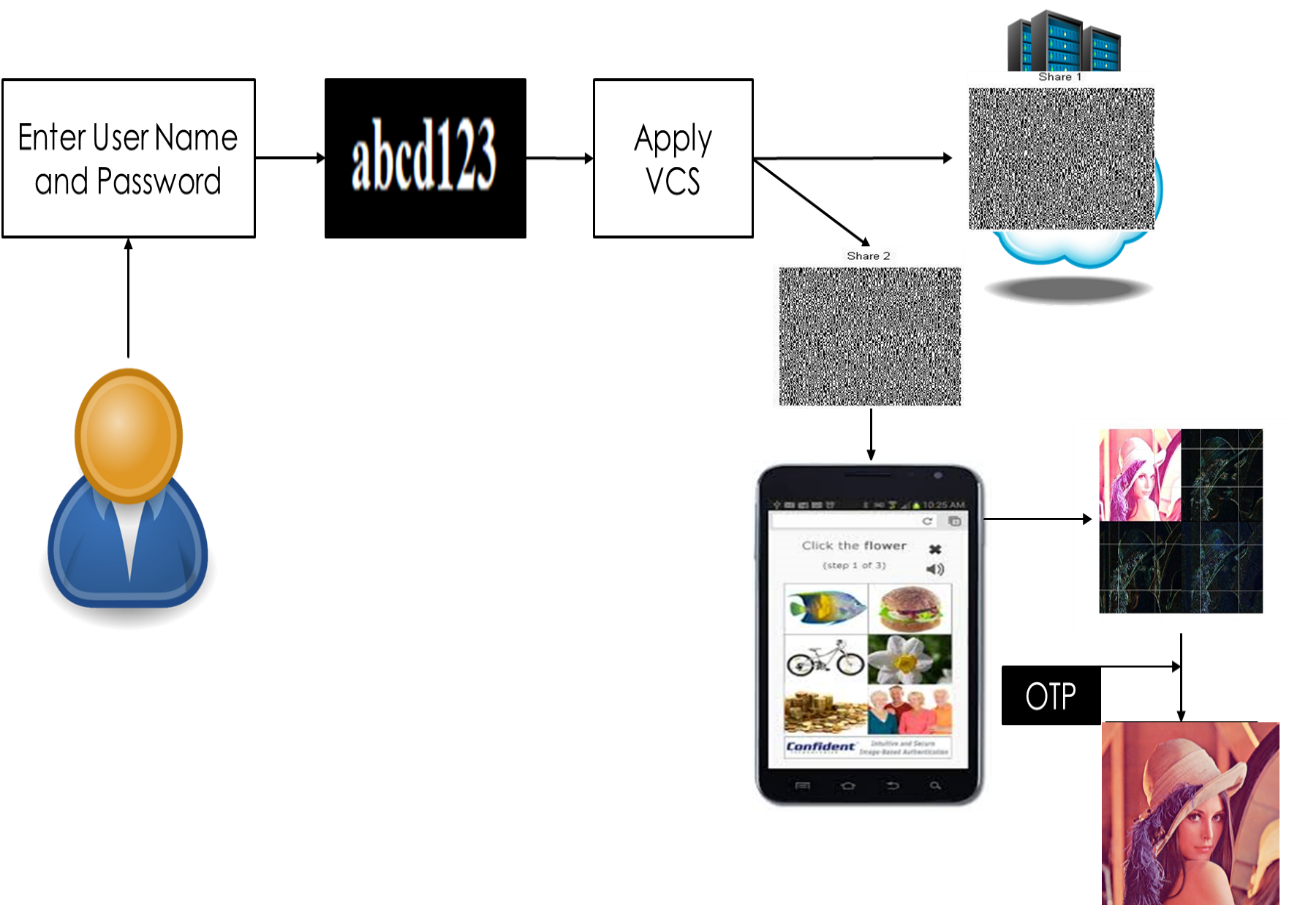
**SUMMARY:**

Our work also demonstrates that joint VC encrypting and

halftoning is promising in improving the visual quality of the share images.

**3. WORK PROPOSED**

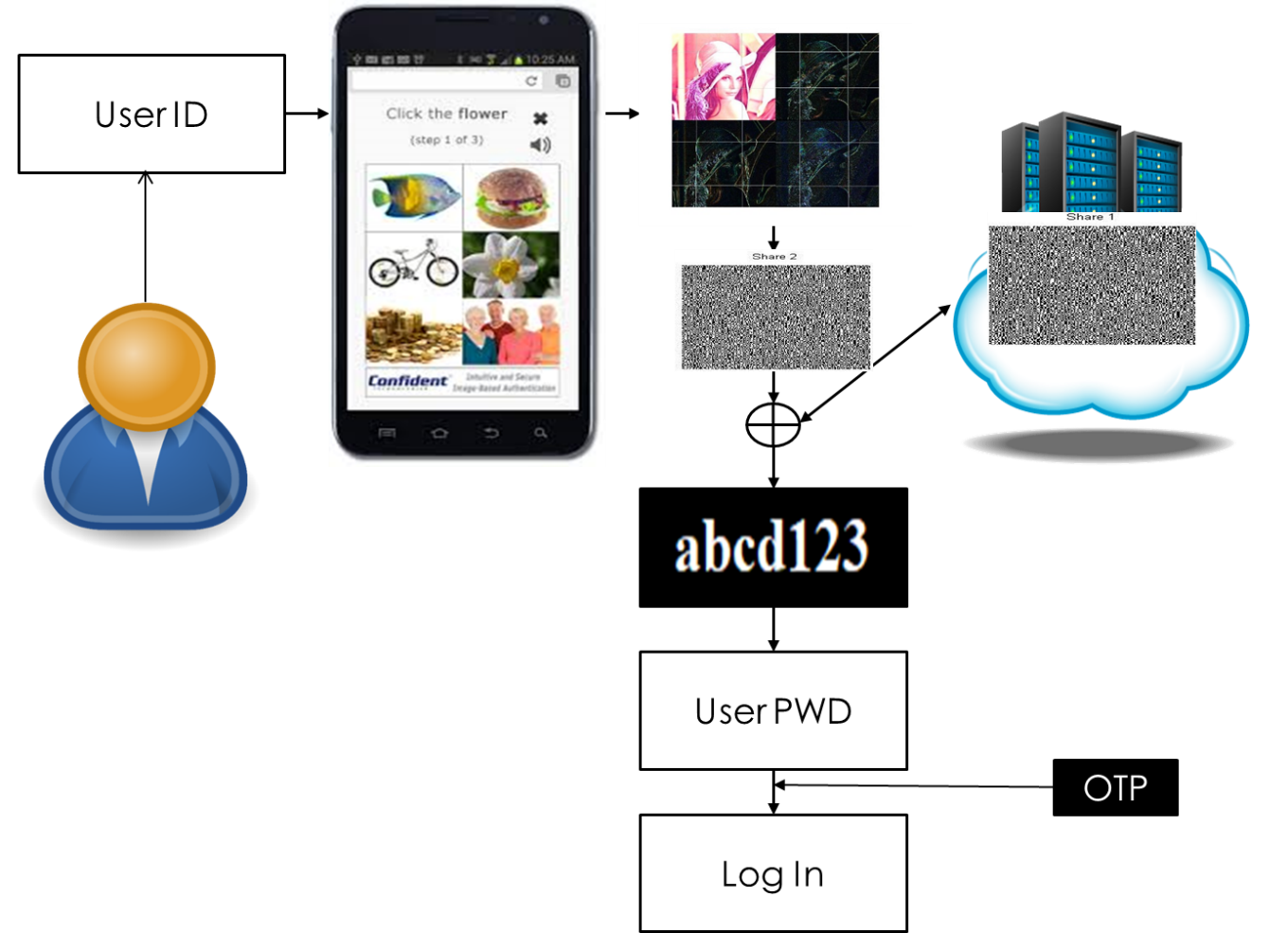
**3.1 BLOCK DIAGRAM OF REGISTRATION PAGE**

****

**3.1.1 DESCRIPTION**

In our project Registration block diagram shows the registration procedure. Firstly, the user has to enter his/her user name/id and password. As the user enters the username and password he/she will be asked to upload an image. As soon as the image gets uploaded VCS will be applied and the image will be divided into two shares i.e., share 1 and share 2. Share 1 will be at server side and share 2 will be at user side. Thereafter re-capcha will get generated and user must select re-capcha and then the image will get saved and registration procedure gets completed.

**3.2 BLOCK DIAGRAM OF LOGIN PAGE**

****

**3.2.1 DESCRIPTION**

In our project Login block diagram shows the login procedure. User has to enter his/her username/id that has been generated while registration procedure. As the user enters the id, he/she will be asked to browse the image. After browsing, ex-or gate functionality will occur between the users share and server-side share so as to check whether both share matches or not and as both shares get checked and accepted user gets logged into the account.

* 1. **MODULES**
* **N-USERS**: A person who ultimately uses or is intended to ultimately use a product.
* **ADMIN**: The one who is administrator of any organisation.
* **TEXT TO IMAGE**: Converting the text into binary code.
* **IMAGE TO TEXT**: Converting the binary code into text.
* **VISUAL CRYPTOGRAPHY**:  It’s a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.
* **DATA-EMBEDDING**: Known as digital watermarking. It should embed information transparently, meaning that the quality of the host signal is not degraded perceptually by the presence of embedded data.
* **DATA EXTRACTION**: Data extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration).
* **NETWORK ATTACK**: It can be defined as any method, process, or means used to maliciously attempt to compromise network security. There are a number of reasons that an individual(s) would want to attack corporate networks.
* **ATTACK RECOVERS**: Attack occurred on any of the account can be recovered by some of the recovery tools.
* **RE-CAPTCHA GENERATION**: re**-**CAPTCHA is a CAPTCHA-like system designed to establish that a computer user is human (normally to protect websites from bots) and, at the same time, assist in the digitization of books.
* **ALERT NOTIFICATION**: It alerts the user by sending mail and messages related to their account.

**3.4 TOOLS**

**Python:**

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms and can be freely distributed. Anaconda is a distribution of the Python.

**Libraries:**

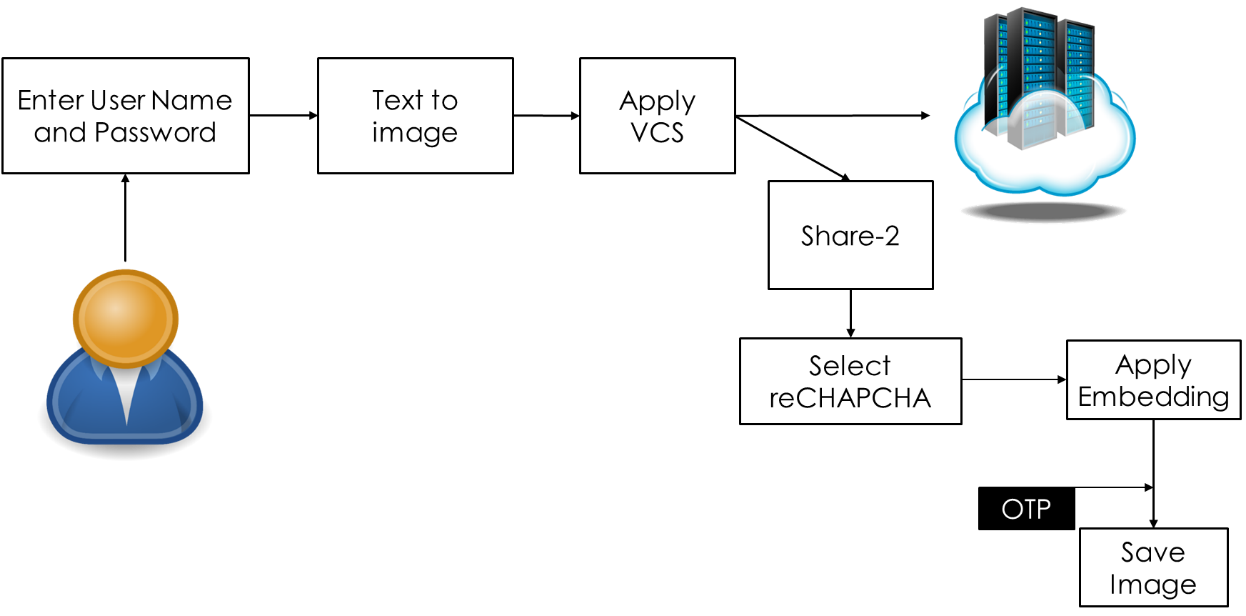
* Pandas
* Matplotlib
* Numpy
* OpenCV
* Streamlit

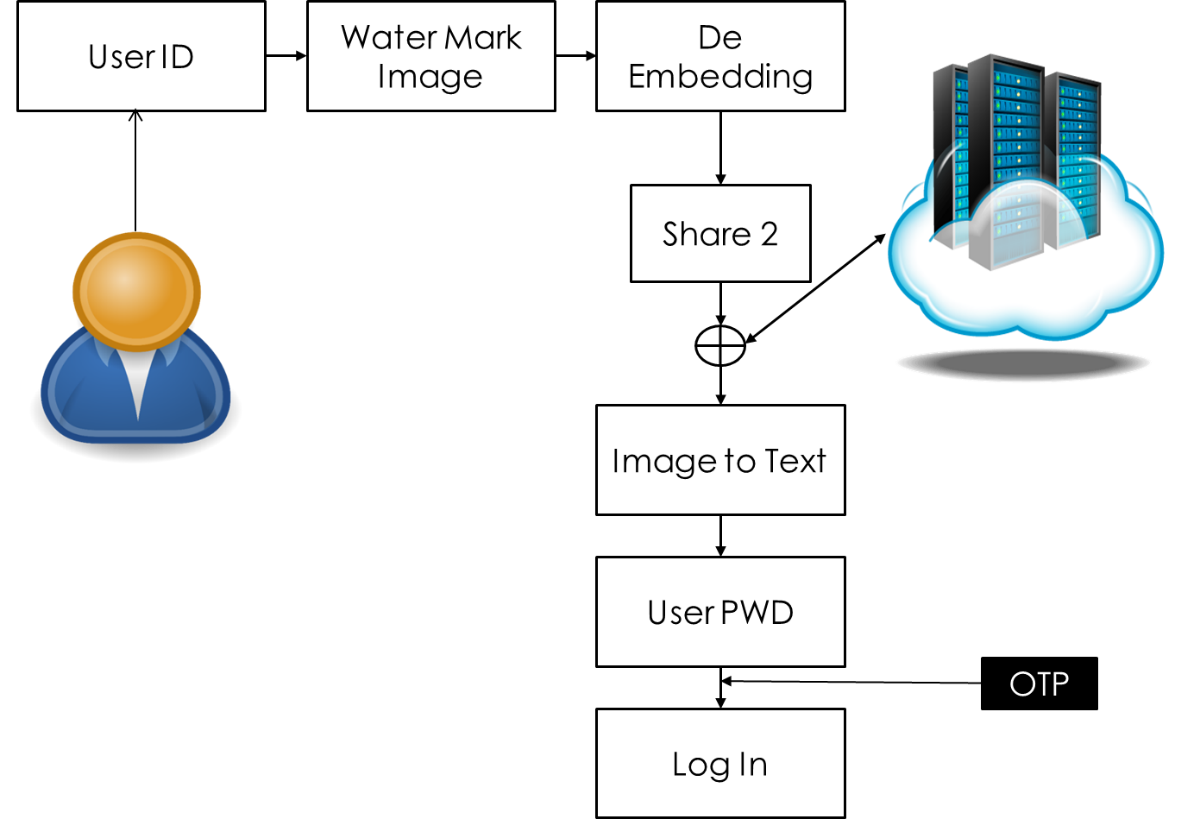
**4. UML DIAGRAMS**

**4.1 BLOCK DIAGRAM:**

A block diagram is a [diagram](https://en.wikipedia.org/wiki/Diagram) of a [system](https://en.wikipedia.org/wiki/System) in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks.[[1]](https://en.wikipedia.org/wiki/Block_diagram#cite_note-SSEV-1) They are heavily used in engineering in [hardware design](https://en.wikipedia.org/wiki/Hardware_architecture), [electronic design](https://en.wikipedia.org/wiki/Electronic_design), [software design](https://en.wikipedia.org/wiki/Software_design), and [process flow diagrams](https://en.wikipedia.org/wiki/Process_flow_diagram).

Block diagrams are typically used for higher level, less detailed descriptions that are intended to clarify overall concepts without concern for the details of implementation. Contrast this with the [schematic diagrams](https://en.wikipedia.org/wiki/Schematic_diagram) and [layout diagrams](https://en.wikipedia.org/wiki/Integrated_circuit_layout) used in electrical engineering, which show the implementation details of electrical components and physical construction.

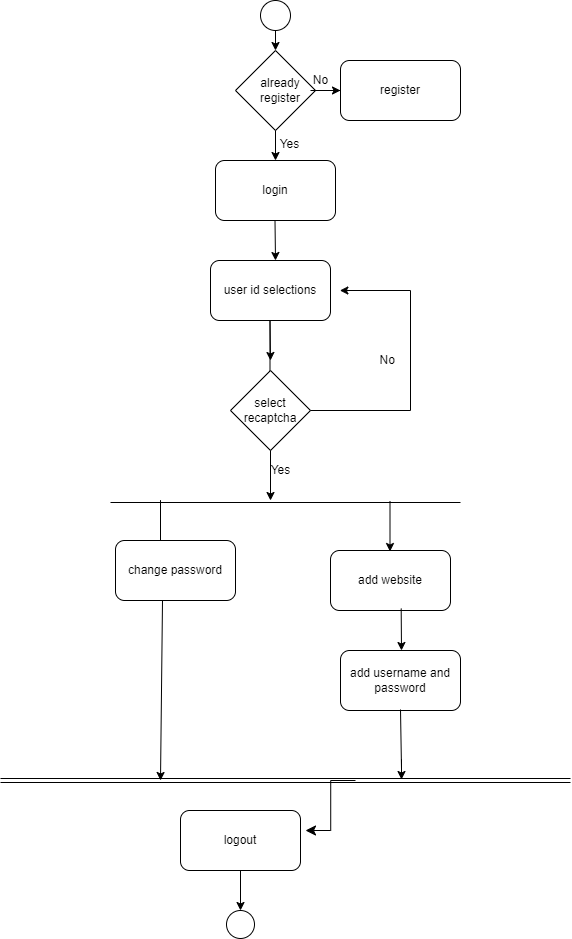


****

**4.2 ACTIVITY DIAGRAM:**

Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system.

The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc.



**4.3 ADMIN USE-CASE DIAGRAM:**

UML Use Case Diagrams. Use case diagrams are usually referred to as behaviour diagrams used to describe a set of actions (use cases) that some system or systems (subject) should or can perform in collaboration with one or more external users of the system (actors).

**Secure Master Login**

Server

<<Uses>>

<<Uses>>

<<Uses>>

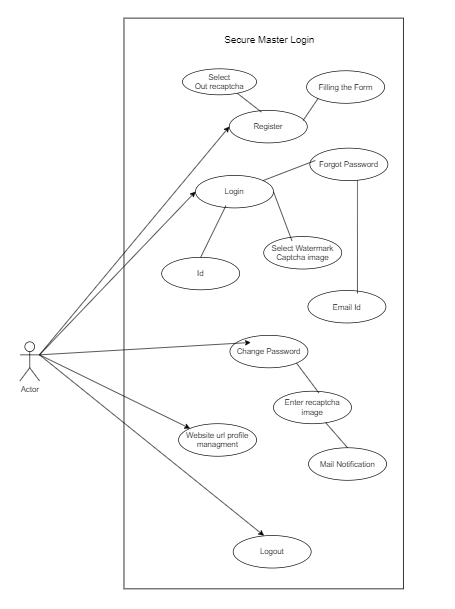
<<Uses>>

<<Uses>>

<<User>>

**4.4 USER USE CASE DIAGRAM:**

In software and systems engineering, a use case is a list of actions or event steps typically defining the interactions between a role (known in the Unified Modelling Language as an actor) and a system to achieve a goal. The actor can be a human or other external system.



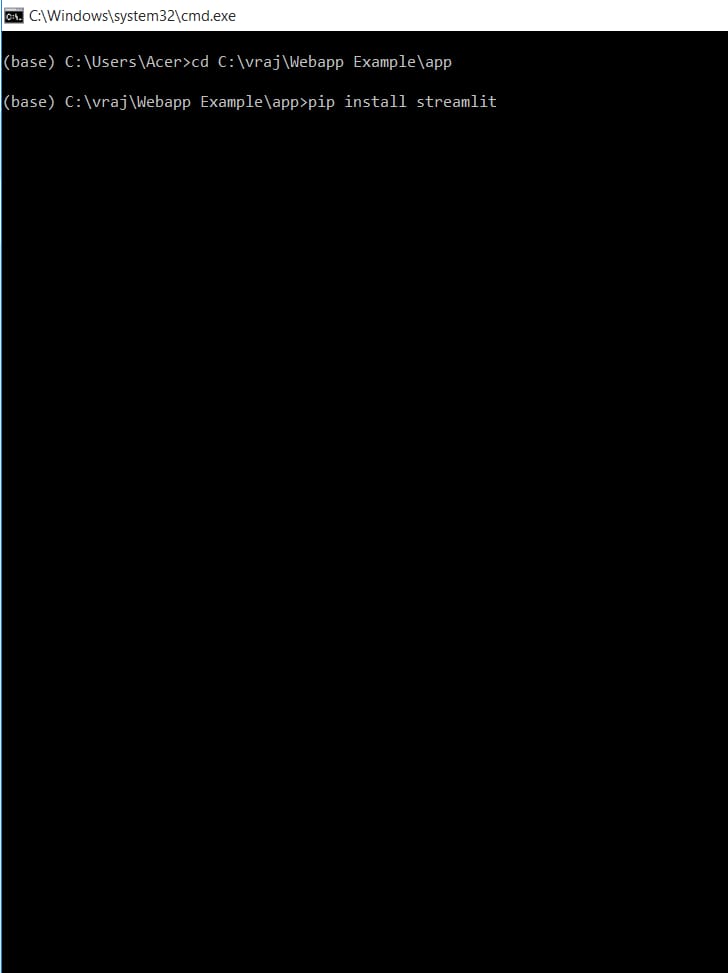
**4.5 DATATYPES:**

|  |  |  |
| --- | --- | --- |
| **VARIABLE** | **TYPE** | **VALUE** |
| FIRST NAME | STRING | 20 |
| LAST NAME | STRING | 30 |
| USERNAME | STRING | 40 |
| PASSWORD | STRING | 10 |
| E-MAIL | STRING | 60 |
| PHONE NO | INTEGER | 10 |
| RE-CAPTHA | IMAGE | LESS THAN 2MB |

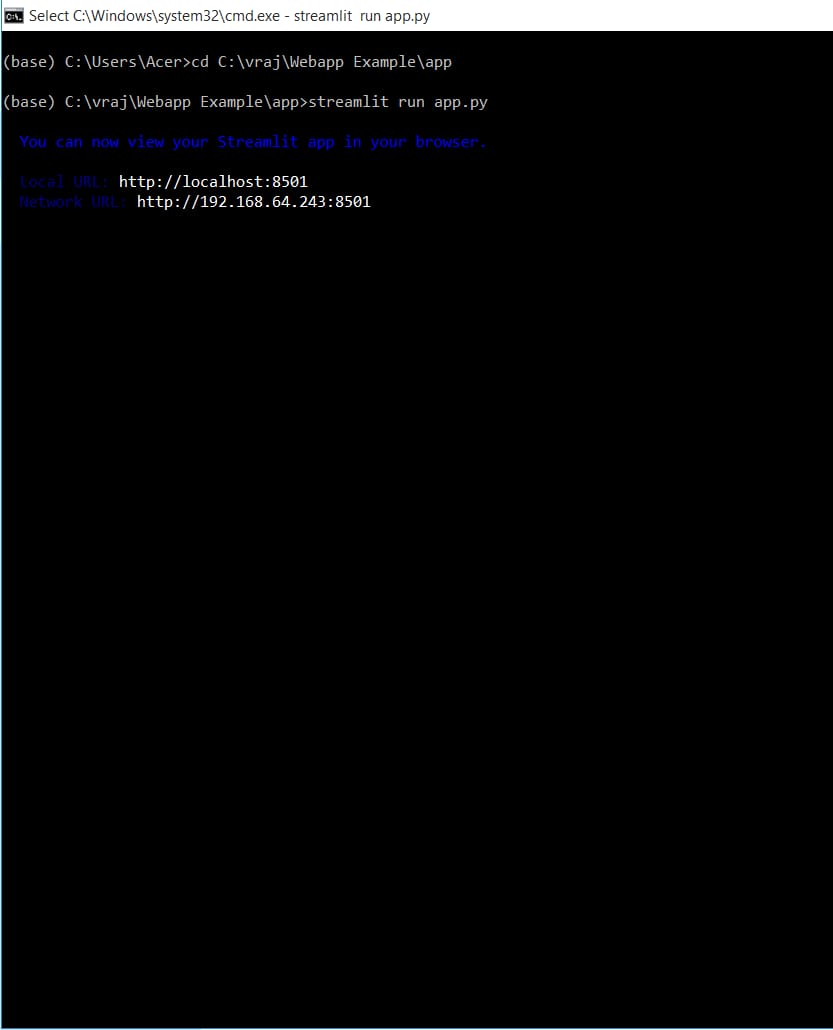
**5. RESULTS**

**5.1 INSTALL STREAMLIT:**

Streamlit is an open source app framework in Python language. It helps us create web apps for data science and machine learning in a short time. It is compatible with major Python libraries such as scikit-learn, Keras, PyTorch, SymPy(latex), NumPy, pandas, Matplotlib etc.

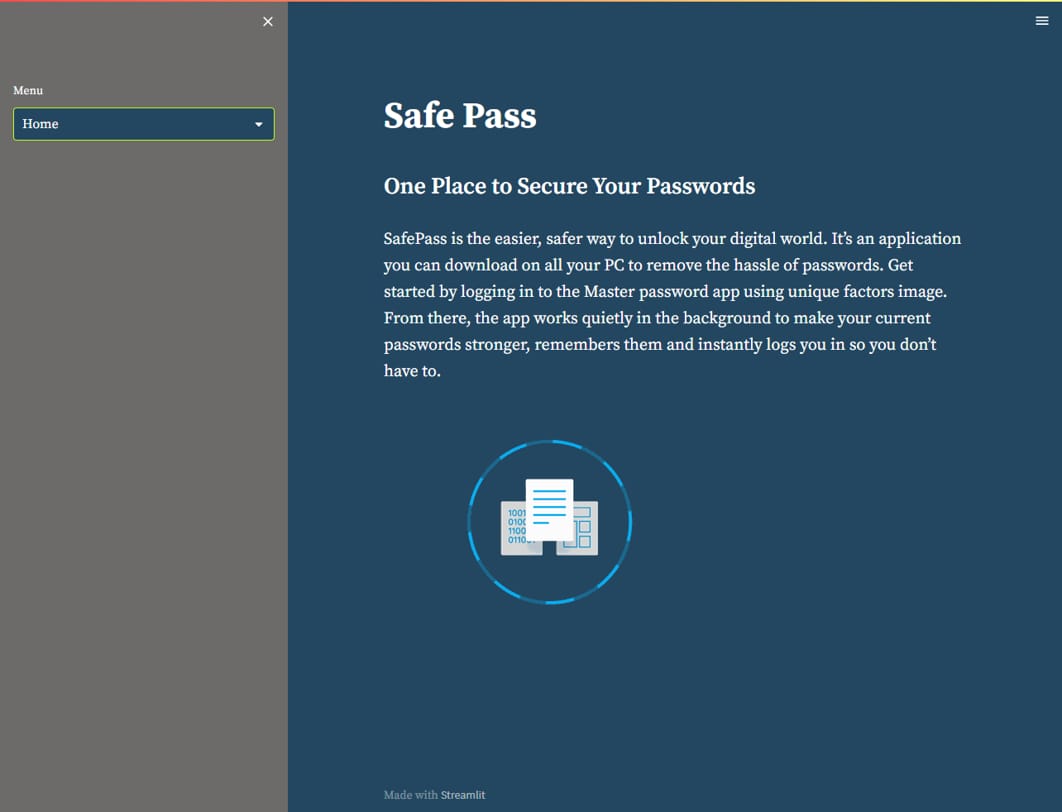
**5.2** **RUN STREAMLIT APP**

Running streamlit app

****

* 1. **HOME PAGE:**

In home page we have used markdown command

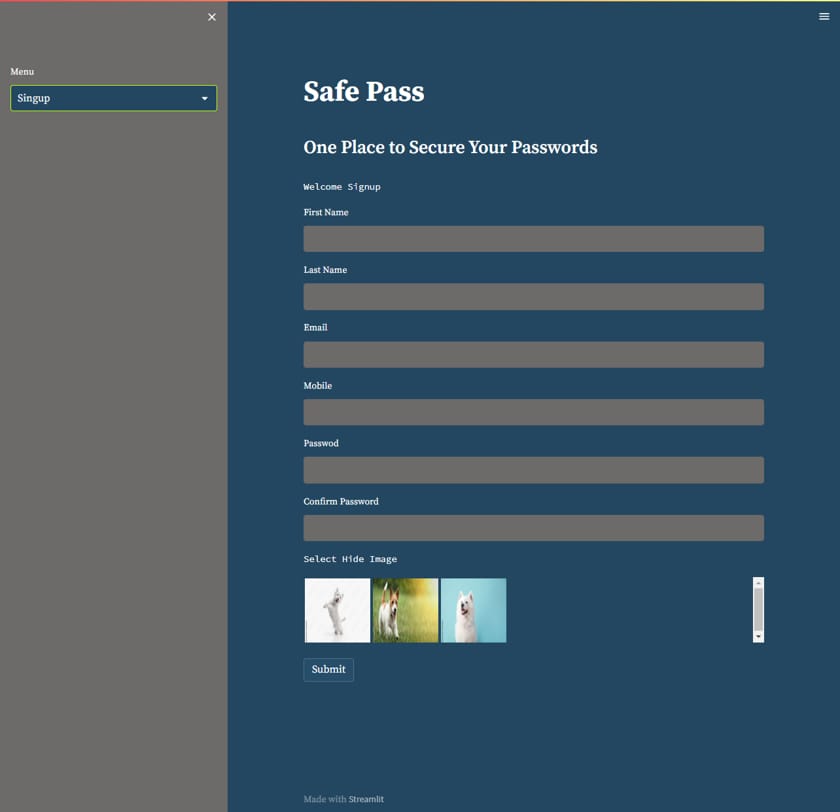
**-**

* 1. **SIGN UP:**

In signup page we have used input box for text input

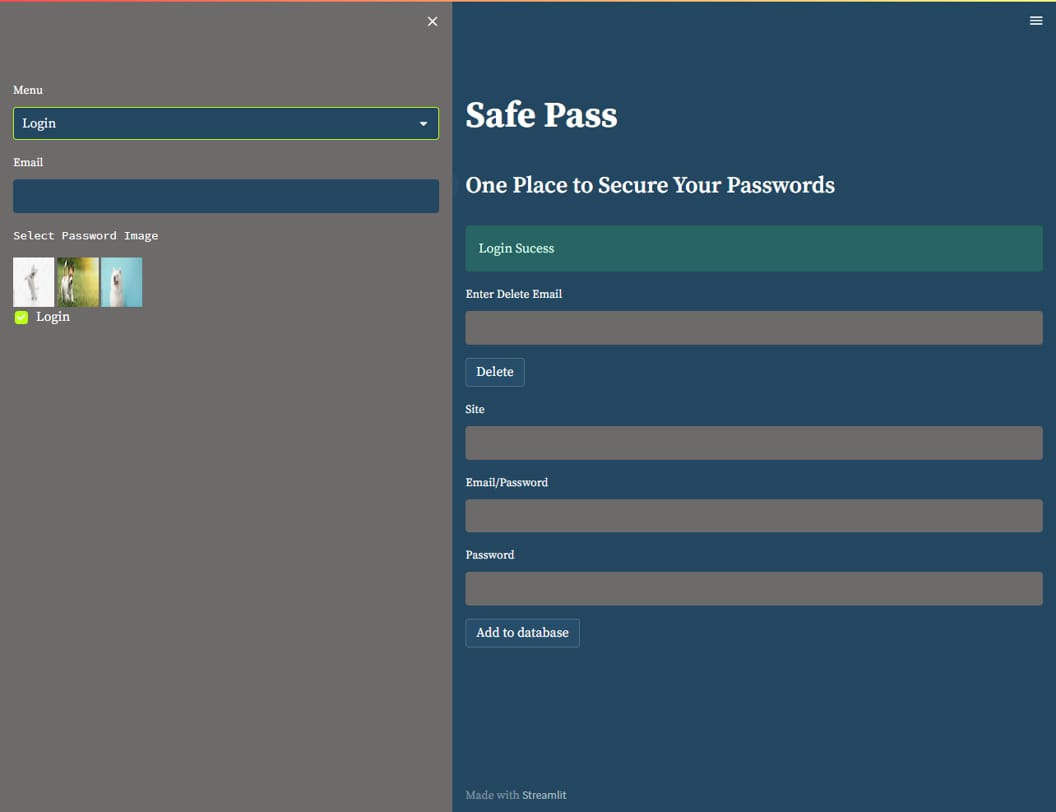
We have used selection box for choosing image

Image-grid library for showing image

****

* 1. **LOGIN DASHBOARD:**

In sidebar we have used image-grid library which contains images

****

**6. CONCLUSION**

Here by in the near future we are expecting to develop SafePass which would be the easier and safer way to unlock your digital world. It’s an application you can download on all your PC to remove the hassle of passwords. Get started by logging in to the Master password app using unique factors image. From there, the app works quietly in the background to make your current passwords stronger, remembers them and instantly logs you in so you don’t have to.

**7. REFERENCES**

[1] B. Le Thanh Thai, H. Tanaka, and K. Watanabe, “Improved scheme and evaluation method for progressive visual cryptography,” Eurasip Journal on Information Security, vol. 2022, no. 1, 2022, doi: 10.1186/s13635-022-00136-7.

[2] P. Anghelescu, I. M. Ionescu, and M. B. Bodea, “Design and implementation of a visual cryptography application,” Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020, pp. 1–4, 2020, doi: 10.1109/ECAI50035.2020.9223191.

[3] S. Khaimar and R. Kharat, “Online Fraud transaction prevention system using extended visual cryptography and QR code,” Proceedings - 2nd International Conference on Computing, Communication, Control and Automation, ICCUBEA 2016, 2017, doi: 10.1109/ICCUBEA.2016.7860061.

[4] M. A. Islam, M. A. A. K. Riad, and T. S. Pias, “Enhancing Security of Image Steganography Using Visual Cryptography,” International Conference on Robotics, Electrical and Signal Processing Techniques, pp. 694–698, 2021, doi: 10.1109/ICREST51555.2021.9331225.

[5] D. R. Ibrahim, J. Sen Teh, and R. Abdullah, “An overview of visual cryptography techniques,” Multimedia Tools and Applications, vol. 80, no. 21–23, pp. 31927–31952, 2021, doi: 10.1007/s11042-021-11229-9.

[6] J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, “Enhanced Visual Cryptography: An Augmented Model for Image Security,” Procedia Computer Science, vol. 167, no. 2019, pp. 323–333, 2020, doi: 10.1016/j.procs.2020.03.232.

[7] S. Almutairi, S. Manimurugan, and M. Aborokbah, “A new secure transmission scheme between senders and receivers using HVCHC without any loss,” Eurasip Journal on Wireless Communications and Networking, vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1399-z.

[8] Y. H. Chen and J. S. T. Juan, “XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares,” Applied Sciences (Switzerland), vol. 12, no. 19, pp. 1–17, 2022, doi: 10.3390/app121910096.

[9] F. Liu and C. Wu, “Embedded extended visual cryptography schemes,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 307–322, 2011, doi: 10.1109/TIFS.2011.2116782.

[10] L. Wang, B. Yan, H. M. Yang, and J. S. Pan, “Flip extended visual cryptography for gray-scale and color cover images,” Symmetry, vol. 13, no. 1, pp. 1–23, 2021, doi: 10.3390/sym13010065.

[11] X. Yan, Y. Lu, L. Liu, and X. Song, “Reversible Image Secret Sharing,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3848–3858, 2020, doi: 10.1109/TIFS.2020.3001735.

[12] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, “Secure authentication using image processing and visual cryptography for banking applications,” Proceedings of the 2008 16th International Conference on Advanced Computing and Communications, ADCOM 2008, no. Vc, pp. 65–72, 2008, doi: 10.1109/ADCOM.2008.4760429.

[13] Y. F. Chang, W. L. Tai, and Y. T. Huang, “Privacy-Preserved Image Protection Supporting Different Access Rights,” Applied Sciences (Switzerland), vol. 12, no. 23, 2022, doi: 10.3390/app122312335.

[14] A. G. Bhosale and V. S. Patil, “A (2, 2) Visual Cryptography Technique to Share Two Secrets,” Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020, pp. 563–569, 2020, doi: 10.1109/ICICT48043.2020.9112420.

[15] M. Z. Salim, A. J. Abboud, and R. Yildirim, “A visual cryptography-based watermarking approach for the detection and localization of image forgery,” Electronics (Switzerland), vol. 11, no. 1, 2022, doi: 10.3390/electronics11010136.

[16] V. V. Panchbhai, “A Review on Visual Secret Sharing Schemes for Binary, Gray & Color Image,” Bioscience Biotechnology Research Communications, vol. 13, no. 14, pp. 268–272, 2020, doi: 10.21786/bbrc/13.14/63.

[17] B. Yan, Y. Xiang, and G. Hua, “Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach,” IEEE Transactions on Image Processing, vol. 28, no. 2, pp. 896–911, 2019, doi: 10.1109/TIP.2018.2874378.

[18] Y. G. Yang, B. P. Wang, Y. L. Yang, Y. H. Zhou, W. M. Shi, and X. Liao, “Visually meaningful image encryption based on universal embedding model,” Information Sciences, vol. 562, pp. 304–324, 2021, doi: 10.1016/j.ins.2021.01.041.

[19] L. Ren and D. Zhang, “A Privacy-Preserving Biometric Recognition System with Visual Cryptography,” Advances in Multimedia, vol. 2022, no. 1, 2022, doi: 10.1155/2022/1057114.

[20] P. Kashyap and A. Renuka, “Visual Cryptography for colour images using multilevel thresholding,” Proceedings of the 3rd International Conference on Inventive Systems and Control, ICISC 2019, no. Icisc, pp. 567–572, 2019, doi: 10.1109/ICISC44355.2019.9036432.