VISUAL STEGNOGRAPHY SCHEME FOR SECURE M- BANKING

REVIEW -1 BATCH-C-13

Yaswanth.M	(18C11A05H8)
Goutham kumar.K	(19C15A0502)
Kotesh.P	(19C15A0503)
Ravi Kumar.P	(19C15A0507)

Under the guidance of

Mr. M.RAMBABU(Asst.Professor)

CONTENTS

- ABSTRACT
- INTRODUCTION
- OBJECTIVE
- PROBLEM STATEMENT
- EXISTING SYSTEM
- PROPOSED SYSTEM
- ANALYSIS
- LITERATURE
- IMPLEMENATION SPECIFICATION
- REFERENCES

ABSTRACT

- Now a days, the overwhelming use of sensible banking applications and also the extraordinary growth of web users worldwide for all of our wants are necessary currently each day.

- The security challenges are varied amounts of cash flowing across shoppers and banking. Banks are searching for differing kinds of choices to safeguard users' privacy against many attacks.

- We have a tendency to target secure banking by providing identity verification for authenticated users, i.e. secret data can be represented as username, password and face recognition.

- The utilization of varied ways of every way choosing stegnography to enhance the protection of the hacker detection.

INTRODUCTION

OBJECTIVE

- Smart phones of the new era area unit will perform all the operations that our notebook computer can do. In each sector and company, technology drives the requirement to grasp dynamical client wants.

- In general, a safety of phone devices is achieved by setting a high level restriction. This reduces the acceptance of users for applications and satisfaction factors.

- Only 1 key and also the image employed in the stegnography (cover image) .The server detects that formula to use to decipher username and countersign. Then the server initiates the request to start out the camera on a mobile device.The camera user takes his/her image and sends it and matches the face with the offered information.

PROBLEM STATEMENT

- It’s unlikely that the straight forward implementation of knowledge security standards in server domains with mobile devices is effective for banks and users. Therefore, the amount of security on good phone devices isn't clear from the banking purpose.

- In general, a safety of phone devices is achieved by setting a high-level restriction. This reduces the acceptance of users for applications and satisfaction factors. Stegnography is a better medium for sending secret message sharing.

EXISTING SYSTEM

- Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer.

- The existing systems addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies.

Drawbacks:

- Security shortfall by using weaker cryptography techniques.
- Security loses due to password guessing attacks.
- There are no face recognitions methods for authenticated user’s even compromised login credentials.

PROPOSED SYSTEM

The proposed method is safer and secure using with LSB stegnography and face recognition methods. This system shows secure and invisible communication in M-banking.

It is first encrypting user name and password using of *AES* encryption algorithm and then this encrypted information is processed to hide into an image.

Then system can extract encrypted information from the picture by revise method of LSB stegnography, later decrypt the encrypted information.

The server matches the image to the accessible information with associate KNN algorithmic rule for face recognition.

Advantages:

Providing data security using Cryptography and Stegnography methods.
Encrypted data hidden in the Image for preventing eavesdropping attacks.
Providing Face Recognition.

ANALYSIS

LITERATURE SURVEY

1. **Secure OTP and Biometric Verification Scheme for Mobile Banking:**
   Authors: Chang-Lung Tsai Chun- Jung Chen, Deng-Jie Zhuang.

- The straightforward implementation of knowledge security standards in server domains with mobile devices is effective for banks and users.

- M-banking is thus become more convenient, effective through the new mobile communication systems. In order to raise the security of M-banking, some banks adopt the one-time password (OTP) to remedy the possible M-banking stealing risk. In the past, the OTP is sent to personal mobile phone.

IMPLEMEMATION SPECIFICATIONS

- **Software Requirements:**

Operating System	: Windows family
Technology	: Python 3.6
IDE	: PyCharm
Front-End	: PyQt5
Back-End	: MySQL5.5

HARDWARE REQUIREMENTS:

Processer	:	Any Update Processer
Ram	:	Min 4 GB
Hard Disk	:	Min 100 GB

MODULE DESCRIPTION

User Registering:

In this system, users need to register with name, user name, password, and email. In this process initially using the AES algorithm, we can encrypt user name and password, later using the LSB steganography mechanism this system embedded encrypted results into the image. For the second authentication purpose, we need to store user profile pictures also into the database.

User Login:

In the login verification process, the user enters his/her user name and password and the login request sent to the database server then the server can get all steganography images one by one and retrieve the encrypted results from steganography image by performing the LSB technique. These encrypted user names and passwords can be decrypted and comparison with user credentials, if matched they go for the second authentication with Face detection mechanism. If users authenticated with both cases then they can able to login into the system,otherwise, they denied accessing the system.

Steganography:

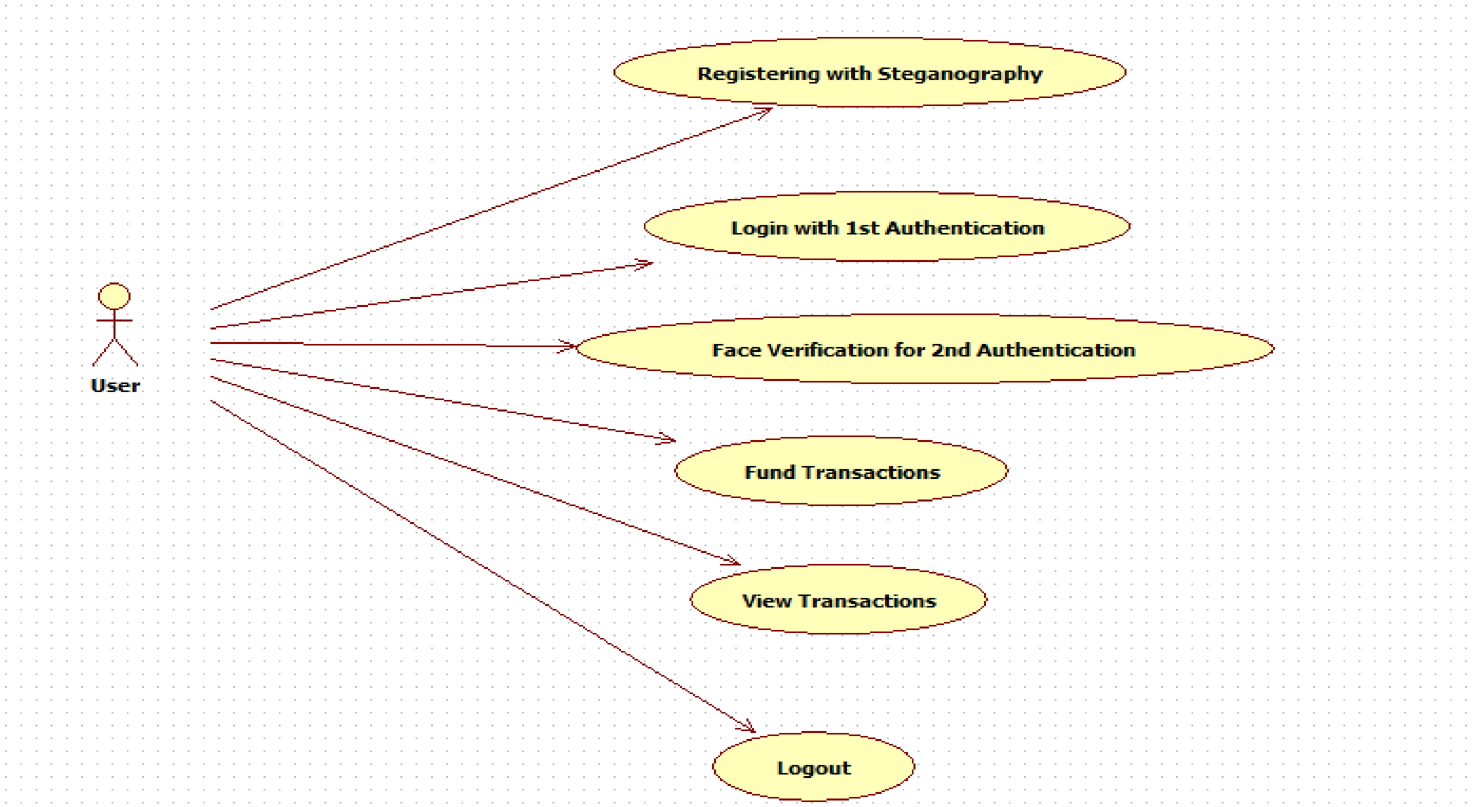
In general, a safety of banking system is achieved by setting a high level restriction. This reduces the acceptance of users for applications and satisfaction factors. Steganography is a better medium for sending secret message sharing. In this system we implementing Least Significant Bit (LSB) algorithm.

Face Detection:

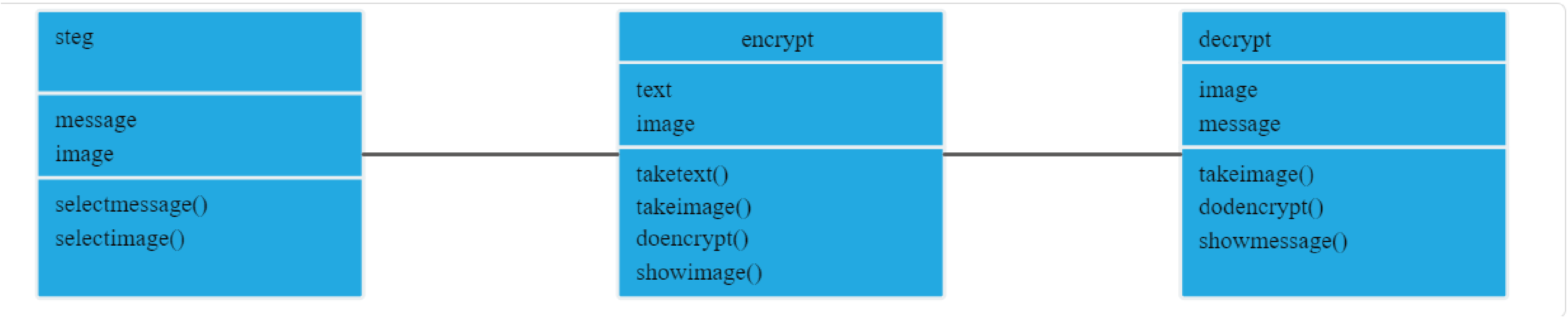
In this system, we are using KNN algorithm for face recognition. Here the server initiates the request to start out the camera on a system.

CLASS DIAGRAM

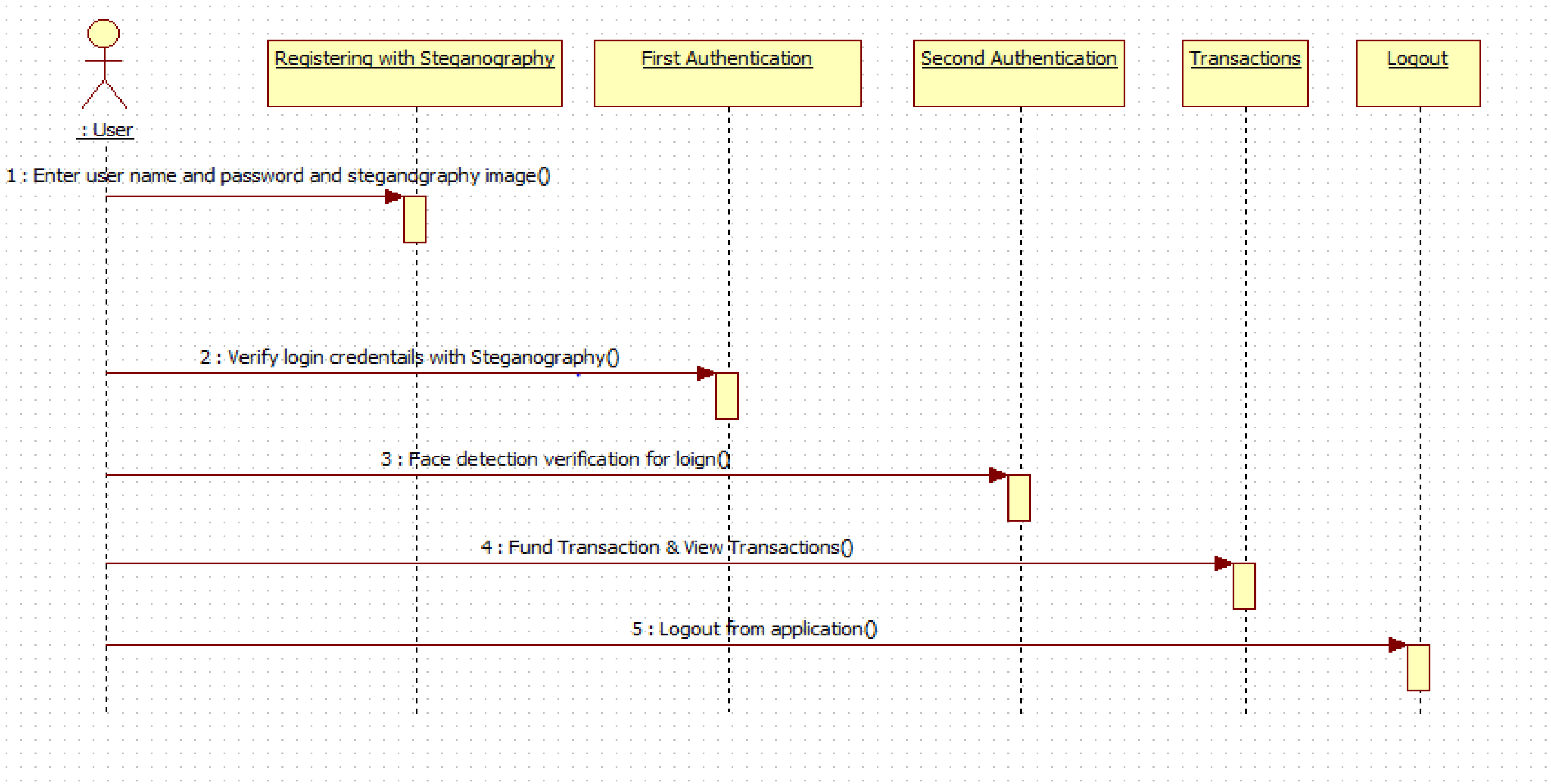
USECASE DIAGRAM


Registering with Steganography
Login with 1st Authentication
User
Face Verification for 2nd Authentication
Fund Transactions
View Transactions
Logout

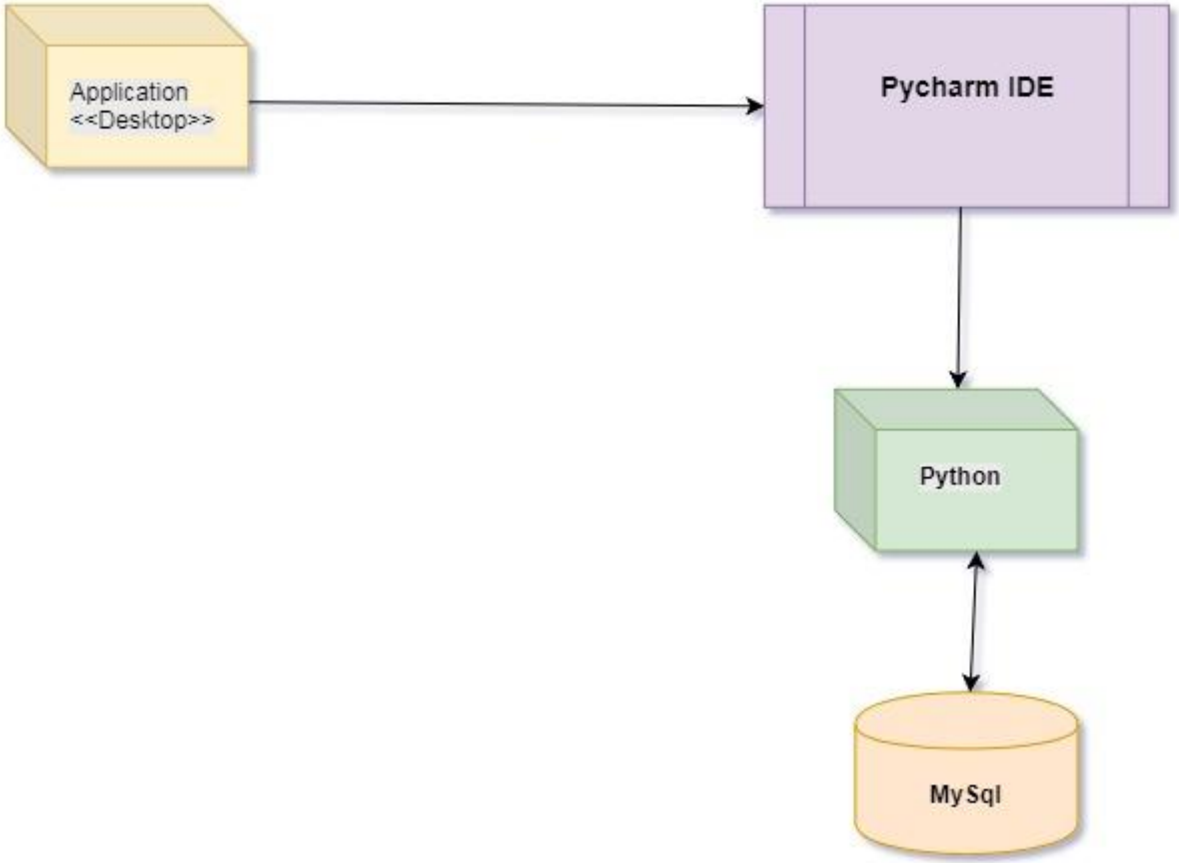
CLASS DIAGRAM



SEQUENCE DIAGRAM


: User
Registering with Steganography
First Authentication
Second Authentication
Transactions
Logout
1 : Enter user name and password and stegandgraphy image()
2 : Verify login credentails with Steganography()
3 : Face detection verification for loign()
4 : Fund Transaction & View Transactions()
5 : Logout from application()

DEPLOYMENT DIAGRAM



REFERENCES

1. Rethink the “Mobile” in Mobile Banking Disruptions and Innovations in Mobile Communications Technology, March 2013.
2. Dushyant Goyal, Shiuh-Jeng Wang, “Stegnographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems” , International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 10, October 2015.

THANK YOU