Survey on 2-Step Security for Authentication in M-Banking

Salve Anup (Corresponding Author)
Department of Computer Engineering,
AISSMS College of Engineering, Pune -411001
University of Pune, India
Tel: +91-9689950004 E-mail: sanupsalve@gmail.com

Kashid Suraj
Department of Computer Engineering,
AISSMS College of Engineering, Pune -411001, University of Pune, India
Tel: +91-9762309579 E-mail: surajiphone@gmail.com

Patil Rahul
Department of Computer Engineering,
AISSMS College of Engineering, Pune -411001, University of Pune, India
Tel: +91-9579578784 E-mail: patilrahul.sangli@gmail.com

Dhamane Harshad
Department of Computer Engineering,
AISSMS College of Engineering, Pune -411001 University of Pune, India
Tel: +91-8793111782 E-mail:hdhamane@gmail.com

Abstract

Technologies drive the need in every sector and enterprise needs to understand changing need of customer. Financial sector has also no exception. In order to satisfy financial need for customer banks are taking help of new technology such as internet. It is called as e-banking. But problem remain over e-banking is security.

Over the e-banking, the potential use of mobile devices in financial applications such as banking and stock trading has seen a rapid increase. The aim of this work is to provide a secure environment in terms of security for transaction by various ways. In this paper we focus on 2-step security for authentication. For this system we use m-banking. Propose the use of "steganography" as means to improve the communication channel. Task of enhancing security include construction of formula for both data encryption and for hiding pattern and also provide system based on biometric information. i.e., face recognition.

Keywords: decryption, encryption, face recognition, security, steganography

1. Introduction

The Internet is an integral part of our daily lives, and the proportion of people who expect to be able to manage their bank accounts anywhere, anytime is constantly growing. As such, Internet banking has come of age as a crucial component of any financial institution's multichannel strategy. Internet banking is vast, which is why this type of banking is becoming more and more popular in recent years. Convenience is the one advantage that most people will list first when online banking is mentioned. Not having to go to the bank and wait in line is something that appeals to most banking customers. Other advantage of online banking is the automatic payment of bills; internet banking is to have paycheck automatically deposited into our account.

But, the biggest disadvantage of internet banking is security. Customer should be sure that he has a secure connection that is protected before you attempt to bank online. To overcome the drawback of internet banking and security issue new technology is developed known as mobile banking or M-Banking. In the e-Banking the client need the computer machine and internet connection. Some rural areas are not aware of internet. And it is also not possible to everyone to use the internet. To overcome the drawback of e-Banking the new concept of m-

Banking is introduce. The importance of improving M-Banking is beneficial to both the customer and the bank. Mobile banking gives opportunity to everybody for easy banking activities sustainably increasing the interaction between user and bank. It has enabled to increase financial access for in rural areas and paved the way for integrating rural people into the mainstream financial system.

Mobile Banking basic Functionality Offered:

I. Account Information
   (a) Balance Overview
   (b) Account Details
   (c) Transaction History
   (d) Account Statements
II. Transfers
   (a) Transfer Between Own Accounts
   (b) Transfer to same Bank Accounts
   (c) Transfer to Other Bank Clients
III. Cards
   (a) Card Details
   (b) Card Statements
   (c) Card Payments
IV. Payments
   (a) Utility Payments
   (b) Bill Payments
   (c) Government Payments
   (d) Group and Payroll Payments
   (e) Mobile top-ups

However, the amount of transaction money through mobile banking has led to attract criminal attention. Security concerns are important for customers and banks. Finding from studies in e-Banking also have application in the wider field off transaction security for e-Commerce activities. Bank log-in security has to be strong and supervised as banks are integral part of the defense against money laundering [1].

The main reason that Mobile Banking scores over Internet Banking is that it enables “Anywhere, Anytime Banking”. Customer do not need to access computer terminal to access bank account. Now customer can access his bank account anytime, anywhere such as waiting for bus to work, travelling or when waiting for orders to come through in a restaurant.

Serious operational risks and potential liabilities are associated with security breaches in the transfer of fund over the Internet. Concern about security has led to major barrier for mobile banking adoption by several banks [1].

Authentication problems issues are related to the transfer of information over the insecure communication channel as shown in Fig. 1.

Insecure Information Exchange

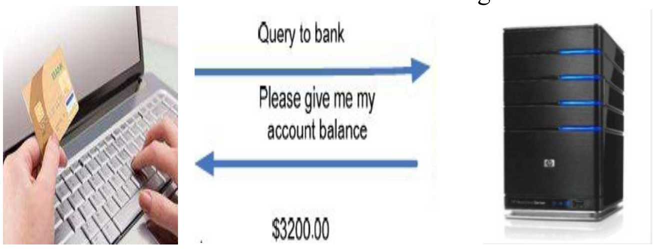


Fig. 1 Insecure Communication channel

Confidential data like password are broken by malicious code. Phishing spoof web page imitating of the user’s online bank is designed and used to encourage the user to enter bank details in this fake page. The data entered is cyber crooks.

Recent increases in online fraud have encouraged banks to think about some different multiple factor solutions for their authentication procedure [1]

In this paper we focus on 2-step security for authentication process using mobile banking for transaction purpose.

Here we make use of different formula i.e., for steganography, for encryption and for session/request id. Only single key is sent along with image used in steganography (cover image) and all formulae in interdependent manner. Key is variable i.e., changed every time and transferred in coded format in stego image. So that it becomes very difficult to get data even if key is found.

In the second step of authentication, we use biometric information. In the biometric information we use face recognition system. In face recognition, image is capture on client and send to server database for validation.

2. Risk associated with e-Banking

I. Interest Rate Risk: Internet rate risk is the risk to earnings or capital arising from movements in interest rates. Interest rate risk arises from different between the timing of rate changes and timing of cash flows.

II. Credit Risk: Credit risk is the risk to earnings or capital arising from an obligator's failure to meet the terms of any contract with the bank or otherwise to perform as agreed

III. Price Risk: Price risk is the risk to earnings or capital arising from changes in the value of traded collection of financial instruments.

IV. Foreign Exchange Risk: Foreign Exchange risk is present when a loan or portfolio of loans is dominated in a foreign currency or is funded by borrowings in another currency.

M-Banking Security measures

I. Debit and Credit cards coupled to a specific phone number of consumer for supplementary transaction security.

II. Transfer channel of SMS can be used with encryption by mobile payment applications to defend data integrity and security.

III. Accomplishment of secure PIN for transactions for fund transfer.

3. Designed System

Our designed system is 2-step authentication process. In the first step of authentication we use steganography and at second step we use biometric information to enhance security over insecure channel.

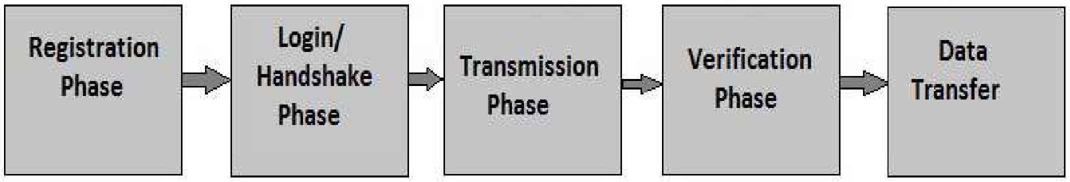
In steganography technique, we hide the user ID and password of client in particular image. We send this image to server for verification.

Biometric information is of two types. In physlogical information it contain face, hand, Iris, DNA, finger print etc while in Behavioral information it contain voice, keystroke, signature etc.

Biometric characteristics such as universality, distinctiveness, collect ability, permanence, performance, acceptability, circumvention cannot be lost or forgotten and are very difficult to copy, share and distribute. For authentication purpose using biometric information person physically present as in real life. This kind of security can enable clients to use their bank ID and biometric to log the bank server remotely to access their account [1].

3.1 Authentication Process

The following fig shows the general authentication procedure in designed technique:



The detailed authentication process is as follows:

I. Registration Phase

By client's mobile the registration phase can be performed remotely or personally. At registration following steps are performed.

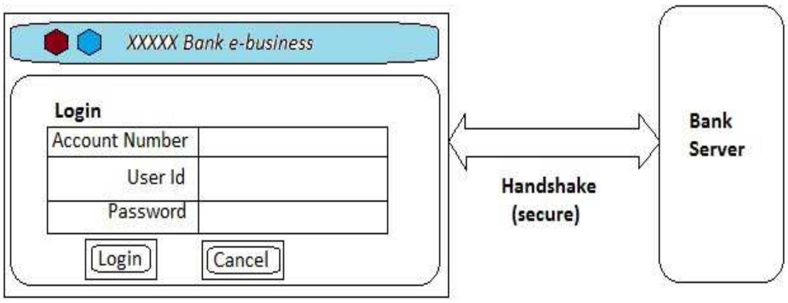
(a) In the first step, the client is also given an e-ID as well as password for processing through his identity. This is first level of authentication.

(b) In the second step, the biometric data i.e., face image is captured, preprocessed and features are extracted. The featured templates are formed and stored as enrolled templates. These saved templates are referred during verification phase. This is second level of authentication.

II. Login Phase

At the login time in bank account he is required to enter his e-ID and password.
The server performs the following preliminary steps:

(a) Checks T is the current time stamp of the user’s machine.
(b) Verifies initial login details i.e. the ID and password.
(c) If the prior information entered is correct, the user is redirected to the biometrics authentication page and the user is asked to start image transmission through the mobile.



III. Transmission Phase

This phase takes care of the transmitting information through the internet as we have no control over the insecure channel.

(a) In order to avoid the interruption of hackers and intruders we propose to hide the text data into some images related to normal life or otherwise which when encountered by the hacker can be ignored and transmission can be preceded safely.
(b) Even if the transmitting data is suspected by the hacker he cannot extract the secret data.

IV. Verification Phase

Upon receiving the login information and the stego file, the authentication server performs the following steps:

(a) The server applies the reverse of the embedding secret data procedure to recover the biometric information from the stego file.
(b) Checks the validity of time stamp with the current date and time T 'and T . The server rejects the login request of the user otherwise accepts the request. Here T denotes the expected valid time interval for transmission delay and T ' denotes the receiving timestamp of login attempt by the user.
(c) Once the biometrics is successfully derived from the stego file, the face recognition takes places as discussed in section 3.4 and the suitable candidate is matched from the database.
(d) Computes T '' and s T from the MAC sent from the server for confirmation. If T then the user rejects this message otherwise calculates the MAC hash function using his private key.

After receiving the response message from server user compares the two hash values calculated from MAC and the original value. If the two are equal the server gets authenticated otherwise the operation is terminated.

V. Data Transfer

The data can be transfer once the user is authenticated then the users are allowed to transfer the data.

3.2 Data Encryption and error checking

I. Encryption and Decryption

A process of translating a message, called the Plaintext, into an encoded message is called encryption. It helps to protect the original data from unauthorized access.

Decryption is process of translating encoded message back to plain text.

Before embedding the data into image using steganography technique, data is first encrypted either by using simple technique like 0 converted to 1 or any standard algorithm. Such encrypted data is then used for steganography.

II. Error checking

Error checking means checking consistency of data in image after receiving by receiver. Because, if random changes are made in the image then resultant extracted data from image may get changed.

This can be achieved by carious ways. We can make use of simple techniques such as parity code or any other standard techniques. Data which is required for error checking should also be added to image along with original data [2].

3.3 Steganography

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. Now days there are many forms of steganography that use many different mediums to transmit hidden information. Steganography can use essentially any other form of media to transmit a hidden message, though techniques vary from cover type to cover type.

Steganography was around long before computers were invented. As long as people have desired to communicate in secret; steganography has been there, allowing them to at least attempt to do so. The term "Steganography" dates back to 440 BC and derives from a Greek word meaning "covered or hidden writing." This word was used to refer to practices of leaders hiding messages sent to other leaders.

Steganography came to what is now the United States as early as the Revolutionary War, during which it took the form of secret message drops, code words, and invisible inks used for communications between General George Washington and a group of spies It continued in use through additional wars, including World War I and II. Following the tragedy of September 11, 2001, investigations revealed that Al'Queda terrorists may have transmitted images containing hidden messages via Usenet. Evidence exists primarily in the form of Islamic extremist websites that provide information on how to embed data in images. Though the use of steganography in planning 9/11 was not confirmed, the possibility of its use sparked new interest in steganography, and led to further research into its use and its prevention [3].

Implementing steganography

Steganography literally means "covered writing." Steganography has been used throughout history for secret communications. Instead of making use of some previous techniques of steganography, such as LSB method which are easy to detect, it uses two mathematical formulae. To make use of steganography appropriate image format should be selected such as loss less image formats.

The general overview of steganography technique is shown in Fig 4.

Cover serves as medium to hide the message being sent. Making use of graphical images as cover solve many problems readily such as large availability of images, various formats of images and variation in size of image.

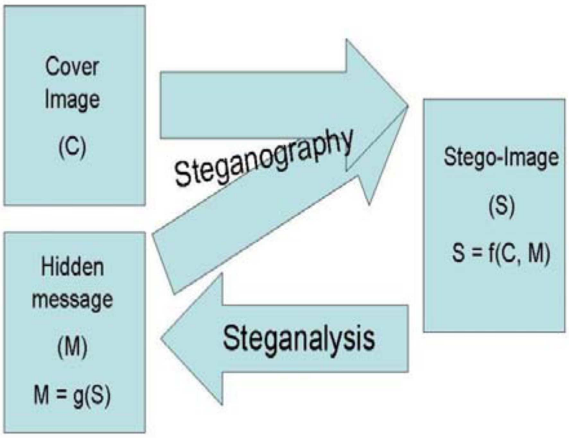
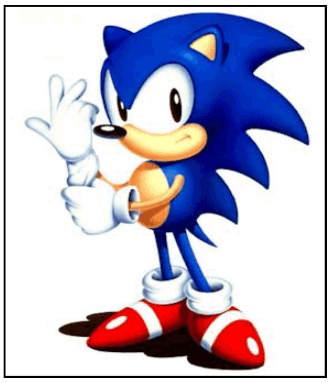


Fig. 2 Steganography and Steganalysis

Both server and end user application will communicate only by sending the cover image and then extracting data from it [2].

Here we make use on two mathematical formulae. First formula will generate series of pixel number in which data will hide. Second formula will generate the bit number for ‘n’ bit pixel in which one bit of data will hide. Using these formulae data will be randomly distributed in image instead of sequential and data hiding bit is also changed every time. Using custom images created by the owner (in this case bank) will help to avoid the comparison of the image.

Before Data Hiding



After Data Hiding

From these results, we see that the image appear completely unaltered to the naked eye, and are statistically quite similar as well, making it very difficult for either a human with both images or a computer with only one image to detect something amiss.

The beauty of randomly generated images is that a user can continue to generate images until one is found with satisfactory statistics or looks, and this often takes only a few iteration to accomplish [3].

3.4 Face recognition

Face recognition has received considerable interest as a widely accepted biometric, because of the ease of collecting samples of a person, with or without subject's intension. Face recognition refers to an automated or semi automated process of matching facial images. This type of technology constitutes a wide group of technologies which all work with face but use different scanning techniques. Most common by far is 2D face recognition which is easier and less expensive compared to the other approaches [4].

There are four steps in face recognition as given below:

I. Acquiring a sample: In a complete, full implemented biometric system, a sensor takes an observation. The sensor might be a mobile camera. In our system, 2D face picture will be supplied manually to server.

II. Extracting Features: For this step, the relevant data is extracted from the predefined captured sample. The outcome of this step is a biometric template which is a reduced set of data that represents the unique features of the enrolled user's face.

III. Comparison Templates: For identification purposes, this step will be a comparison between a given image for the subject and all the biometric templates stored on a server database. For verification, the biometric template of the claimed identity will be retrieved (either from a database or a storage medium presented by the subject) and this will be compared to a given image.

IV. Declaring a Match: The face recognition system will return a client match from image database server match.

Faces in the test images taken using the DROID phone can be of different sizes. Correlating with a standard template size didn't give good results. So, we correlated the image with templates of different sizes (scale ratios from .6 to 1.8) and compared the correlation values. This technique worked well in detecting faces of different sizes.

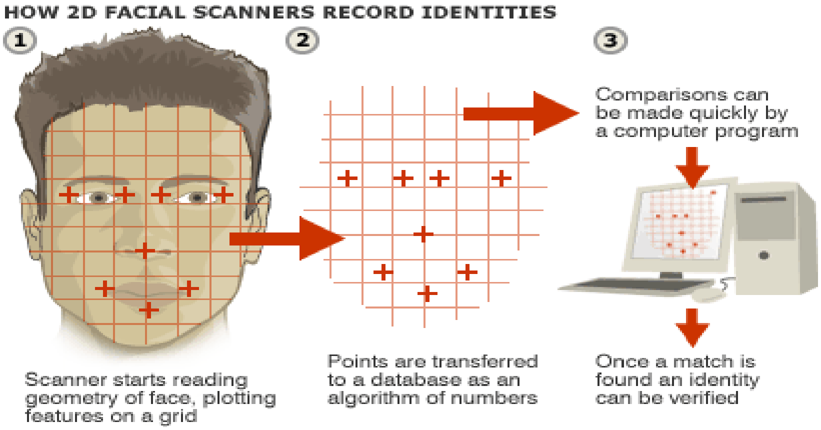
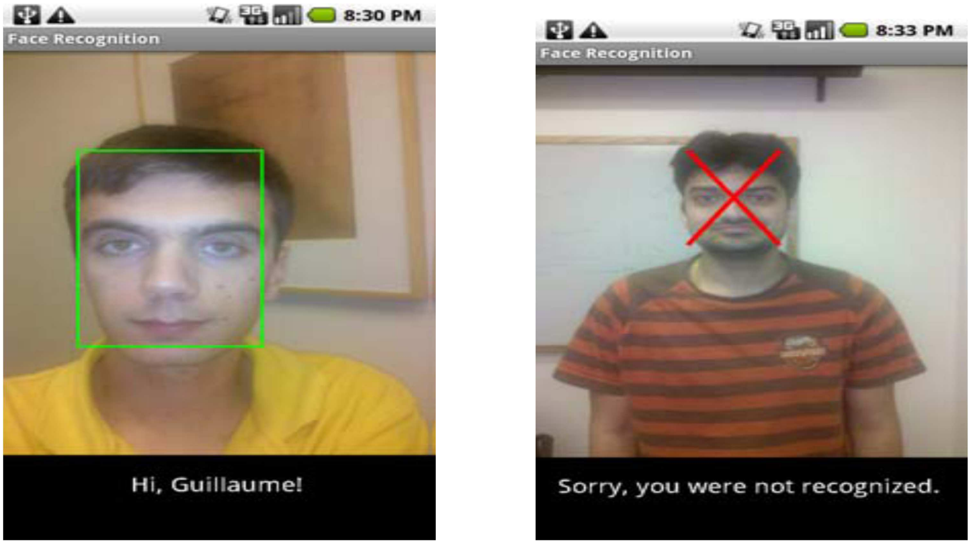

HOW 2D FACIAL SCANNERS RECORD IDENTITIES
1
2
3
Comparisons can be made quickly by a computer program
Scanner starts reading geometry of face, plotting features on a grid
Points are transferred to a database as an algorithm of numbers
Once a match is found an identity can be verified

Fig.3 Face Recognition

For the face recognition technique we use most popular Eigenvector algorithm.
In face recognition security srep if any fake request is send to server from Android application, server will easily detect the fake request. It shows the error message and does not allow the transaction to hacker.



Hi, Guillaume!

Sorry, you were not recognized.

Fig. 4 Result of the Face Recognition application for Android. (a) Client correctly recognized, (b) Client correctly rejected [5]

3.5 Custom session ID and request ID

In computer science, a session identifier, session ID or session token is a piece of data that is used in network communications (often over HTTP) to identify a session, a series of related message exchanges. Session identifiers become necessary in cases where the communications infrastructure uses a stateless protocol such as HTTP.
The request information object contains all request-local information and server as the vessel for most forms of intercommunication. A Request ID object is born when an incoming request is encountered, and its life expectancy is short, as it dies again when the request has passed through all levels of the module type calling sequence.

I. Session ID

A session token is a unique identifier, usually in the form of a hash generated by a hash function that is generated and sent from a server to a client to identify the current interaction session. The client usually stores and sends the token as an HTTP cookie and/or sends it as a parameter in GET or POST queries. Session id will be constant throughout one session. Server will identify the authorized application’s session using session id.

II. Request ID

To communicate with server every message hidden in image should have request id. This id will not be sequential fashion instead it will also be generated by formula. We know that key used in this process is variable i.e. changed every time for every message. So the formula for request id will generate id using key for previous transaction.
At server, if session id found valid then request id is checked. If any request with incorrect request id will not be processed. As request id is not sequential next id will not be after equal interval but interval depends indirectly on key. This avoids the fake request to server [2].

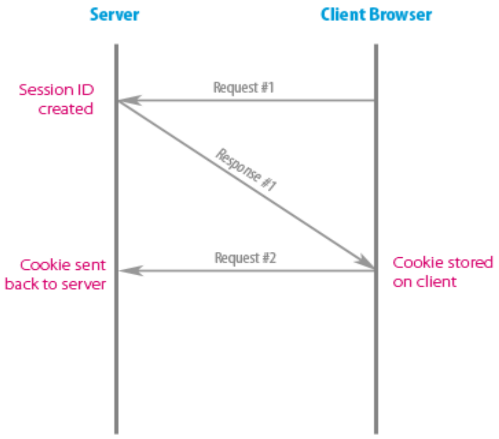


Fig.5 General Overview of Session ID and Request ID

Architectural Model:

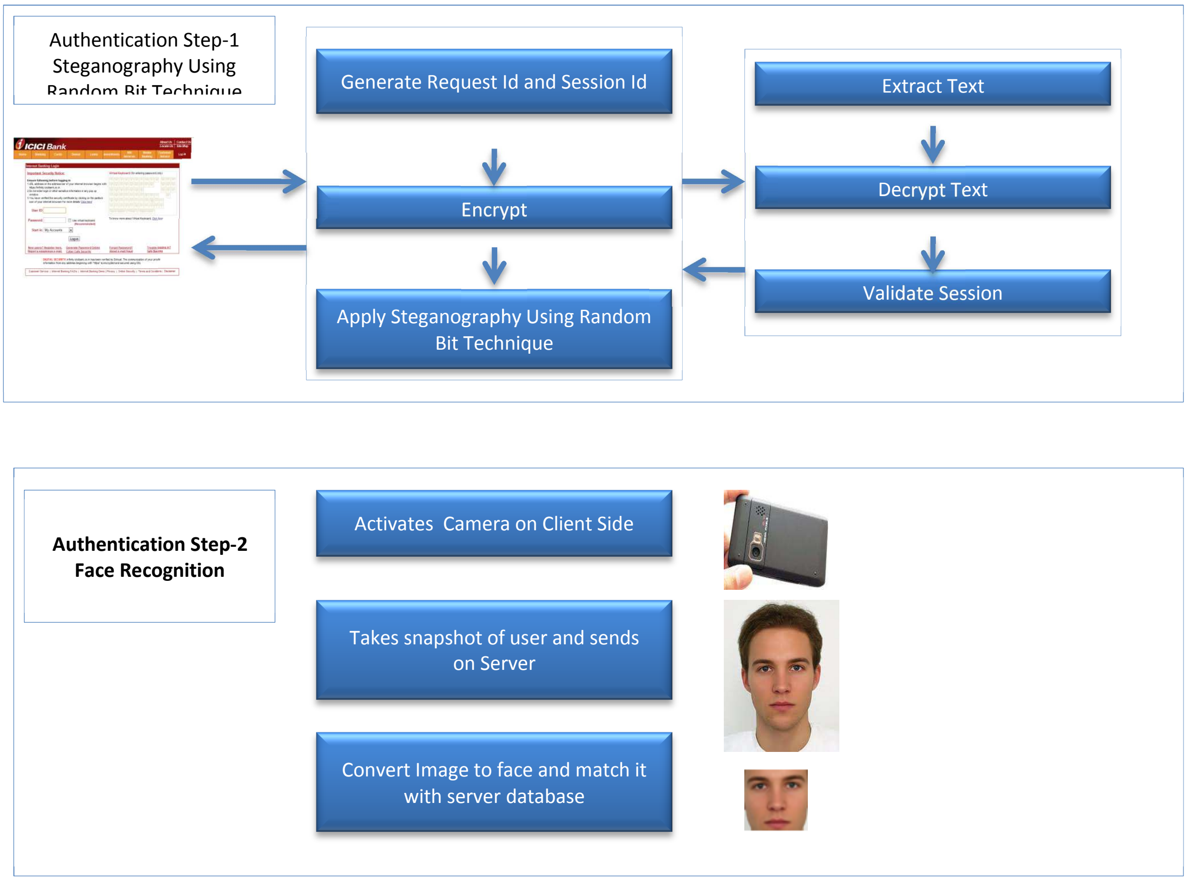

Authentication Step-1 Steganography Using Random Bit Technique
Generate Request Id and Session Id
Encrypt
Apply Steganography Using Random Bit Technique
Extract Text
Decrypt Text
Validate Session
Authentication Step-2 Face Recognition
Activates Camera on Client Side
Takes snapshot of user and sends on Server
Convert Image to face and match it with server database

Fig. 6 Designed 2-step Authentication model

4. Implementation

For implementation of proposed system there must be some requirements are as follows

I. Mobile device of client must be GPRS/Wi-Fi enabled and camera.

II. User must have basic knowledge of internet and mobile.

III. Client server application is needed for successful realization of communication between the customer and bank.

IV. Bank must provide necessary software to client for authentication and transaction process.

V. Speed of the GPR/Wi-Fi data transfer may vary depending on mobile server.

VI. There could not be mobile network problem on client side.

5. Benefits of m-Banking

I. Practical and straightforward alerting services.
II. Low Cost: No additional hardware to buy. Can be deployed on a large scale at a fraction of the cost of traditional authentication solutions.
III. High Security: Unlike our competitors, DIGIPASS for Mobile supports multiple synchronization methods (time-based algorithms in addition to event-based algorithms). Authentication credentials automatically expire either after a configurable time-out or immediately after initial use.
IV. High User Acceptance: End-users will enjoy the freedom of secure banking—anywhere, anytime while conveniently using their very own mobile device.
V. Fully-Customizable User Interface: Banks can fully customize the interface with their own unique branding scheme (menus, messages, icons, logos, fonts, colors).
VI. Password is not exchanged between the server and the mobile. Therefore there is no risk of exposure of user password.
VII. Response time and speed of bank's server increases.
VIII. It is difficult to detect password by intruder because password is stored in any particular Image

6. Conclusion

In this paper, we have surveyed drawbacks of some of the existing system for authentication. To overcome this drawback we proposed 2-level authentication process based on biometric information and Steganographic approach which improves all identified drawbacks and provide more security for real life.

References

Dushyant Goya1 and Shiuh-Jeng Wang (2010), "Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems", High Performance Computing Conference, India
http://www.hipc.org/hipc2010/HIPCSS10/1569358847.pdf
Geeta S. Navale, Swati S. Joshi and Aaradhana A Deshmukh (2010)," M-Banking Security – a futuristic improved security approach", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1,
No. 2
www.ijcsi.org/papers/7-1-2-68-71.pdf
Jessica Codr (2009)" Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide", Washington University in St.Louis, Department of Computer Science & Engineering,
Bryan Hall, Campus Box 1045, One Brookings Drive, St. Louis, Missouri 63130
http://www.cse.wustl.edu/~jain/cse571-09/ftp/stegano/index.html
Noor AlSheala and Hasan AlOdail (2011)," Face Recognition System", KING FAHAD UNIVERSITY OF PETROLEUM AND MINERALS, College of Computer Science and Engineering ICS411 Senior Project Term 082.
http://student.kfupm.edu.sa/s200352870/doc/faceFinal.pdf
Guillaume Dave, Xing Chao and Kishore Sriadibhatla (2010)," Face Recognition in Mobile Phones", Department of Electrical Engineering Stanford University Stanford, USA
http://www.stanford.edu/class/ee368/Project_10/Reports/Sriadibhatla_Davo_Chao_FaceRecognition.pdf