# Biometrics for Mobile Banking

B. Kiran Bala

*Department of Computer and Communication Engineering*
*M.A.M College Of Engineering, Tamil Nadu*
*Email: kiran.it2010@yahoo.com*

***Abstract*** **- Now a day the growth of mobile technology is like lightning speed as well as insecurity is also growing with the same speed to overcome this insecurity we are moving for biometrics as secure path to communicate and authentication purpose. In this paper for the mobile banking we are using password as graphical password is the initial stage then we are using biometrics like (Face, Eye Palm Vein recognition) for authentication purpose and secure transaction.**

***Keywords*** **- The important keywords are DAS(Draw A secret), 2DFLD, NND**

## 1. INTRODUCTION

Money Transaction is necessary in this world it is more important to transact in secure way for that we are having ATM, Mobile Banking, Credit cards etc.. are available in this electronic world. Mobile Transaction is very easy to transact easy to carry from on place to another compare to another technlogies. In this paper we discuss about the security of today's electronic banking systems and present an overview and evaluation of the techniques that are used in the current systems in section. We propose an authentication mechanism for mobile banking using multiple authentication components of biometrics for more robust authentication in section. We further try to explore some of the problems in the transmission phase of the information and present the use of steganography for secure communication.

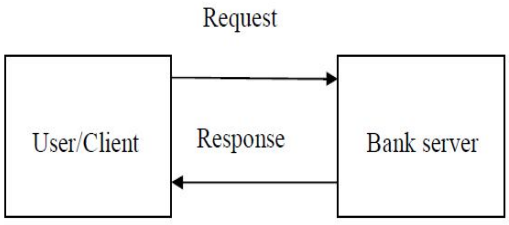



**Figure 1. Insecure Communication Channel**

## 2. PROPOSED SYSTEM

In this paper we will use authentication approach. The authentication is a security solution requiring the verification of different modalities of authentication components and provides enhanced security. We also propose to combine biometric security with steganography to enhance security over insecure channel. The following fig. illustrates the general authenticating

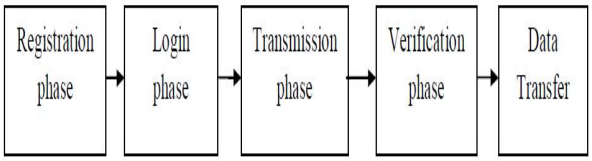



Figure 2. Authentication Approach

### 2.1 Authentication Process

The complete authentication model is discussed below and illustrated .

### A. Registration phase

The registration can be performed either personally or remotely using the mobile by a user. During the registration phase the following steps are performed by the bank server:

1. The biometric data of the user is captured, preprocessed and the features are extracted. The feature templates are formed and stored as enrolled templates. These saved templates are referred during the verification phase. Biometrics samples are taken in our scheme for the purpose for final template storage in the user database.
2. The user is also given an eID as well as a password apart from (i) as an additional parameter for a small processing identity

### B. Login / Handshake Phase

When the user wants to login into the server or account, he is required to enter his eID and password. The server performs the following preliminary steps: i. Checks T is the current time stamp of the user's machine. ii. Verifies initial login details i.e. the ID and password.

### Graphical Password

As graphical password are easy to remember for the user and conventionally dictionary attacks on graphical passwords are infeasible, the practicability of the proposedscheme is improved. Next, they showed that the proposed scheme can withstand the replay attack, the password- file compromise attack, the

denial-of-service attack, the predictable n attack, and the insider attack. In particular, the proposed scheme is easily reparable. Note that this method is secure under the assumption that the easy to remember DAS(Draw A Secret) password is strong. iii. If the prior information entered is correct, the user is redirected to the biometrics authentication page and the user is asked to start video and voice transmission through the mobile

**C. Transmission Phase**

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

i. In order to avoid the interruption of hackers and intruders we propose to hide the video and audio data into some images or videos related to normal life or otherwise which when encountered by the hacker can be ignored and transmission can be proceeded safely.

ii. Even if the transmitting data is suspected by the hacker he cannot extract the secret data.

**D. Verification phase**

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

i. The server applies the reverse of the embedding secret data procedure to recover the biometric information from the stego file.

ii. 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.

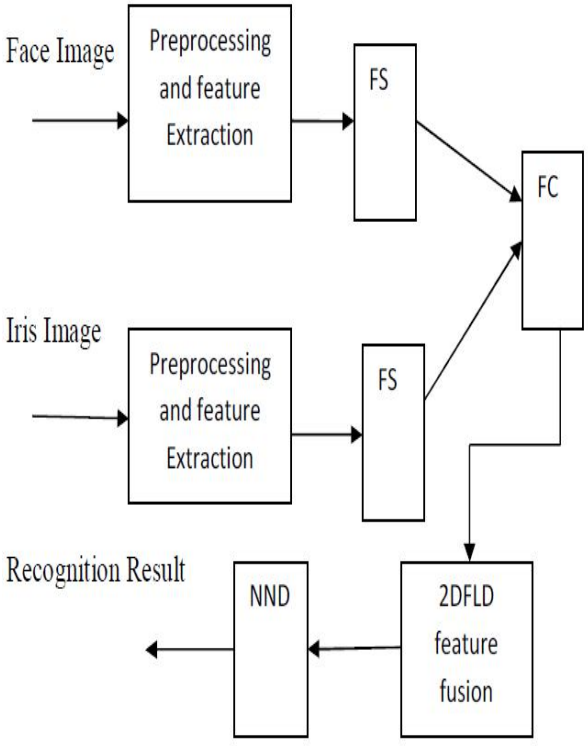
iii. Once the biometrics is successfully derived from the stego file, the face and voice recognition takes places as discussed in section 3.3 and the suitable candidate is matched from the database. iv. Computes *T* '' and *s T* from the MAC sent from the server for confirmation. If *T* then the user 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.

**E. Data Transfer**

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

**2.2 Face and Eye recognition algorithm**

The model of face and iris feature fusion is shown Firstly, face image preprocessing and feature extraction are done to attain face original feature matrix. Then feature standardization (FS) is applied to the face original feature matrix. Meanwhile, iris image preprocessing and feature extraction are realized to gain iris original feature matrix, and feature standardization is done to the iris original feature matrix. Secondly, feature combination (FC) is used to integrate the face standardization matrix and iris standardization matrix into one matrix, and the combined matrix is obtained. Then, feature fusion and extraction are done to the combined matrix by way of 2DFLD. Meanwhile, the optimal discriminating projection matrix is constructed, and the fusion feature matrix is gained. Finally, NND is applied in recognition.




**2.3 Palm Vein Recognition algorithm**

The photographs of the vein image are in poor contrast due to glare, and contains irregular shadow caused by various thicknesses of skin and bones. Vein pattern authentication requires a normalized and enhanced vein image to authenticate a reliable user. This paper presents a de noising and enhancement technique based on GSZ – shock filter, which focuses on both noise elimination and edge enhancement. Multiple Feature extraction technique extracts hand shape features.

## 3. IMPLEMENTATION

The client must be equipped with a mobile phone with a camera and the capability of browsing the internet through WAP (Wireless Access Protocol). Apart from this a dedicated standalone client/server application is needed for the successful realization of communication between the user and the bank. However, the bank must provide the user with the necessary software. A Java applet for that matter would be the best of solution.

## 4. CONCLUSION

In this paper, we have presented weaknesses of some of the previous remote user authentication schemes. For that initially we are using graphical password using steganography is used then we are moving the Biometrics authentication for that in this paper I have used face, iris, and palm vein is used to authenticate the user if the authentication is success user can transact their money. Compare to other technology it is very easy and secure process.

## 5. FUTURE WORKS

In future, more practice handling and using such schemes especially the biometrics within the experimental setting might provide more realistic data, reducing the potential strain and bias of first-time use. Practical implementation of the same is also required to have a real life environment for more developments to take place. Use of biometrics may certainly lead to real life physical authentication systems. More robust techniques for face and voice recognition need to be explored.

## REFERENCES


1. An Enhanced Palm Vein Recognition System Multi-level Fusion of Multimodal Features and Adaptive Resonance Theory 201 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 20
2. A Method for Face and Iris Feature Fusion in Identity Authentication IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006
3. Jadhav, Pawan K. Ajmera in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 13
4. Combining minutiae descriptors for fingerprint matching by Jianjiang Feng in 2008
5. Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems by Dushyant Goyal1 and Shiuh-Jeng Wang 2
6. B. Ives, K.R. Walsh, and H. Schneider, 2004. The domino effect of password reuse. Communications of the ACM 47 (4), 75–78
7. M. Mattila, H. Karjaluoto, and T. Pento, 2002. Internet banking adoption factors in Finland.
8. S. Ranger, 2005. Chip and PIN heads for Cyberspace. Silicon.com Financial Services News, CNET Networks, UK.