ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

USING BIOMETRICS SYSTEM IN MOBILE BANKING

Mushtaque Ahmed [*1]
[*1] School of Information Science and Engineering, Central South University, Changsha, Hunan, P.R CHINA

ABSTRACT

In these days in this global world mobile technologies are growing very fast and another way world has lots of security problems, that's why everyone wants to move on biometrics side. Because this is the only secure system for communication and verification function. So in this paper we are using graphical passwords on the first phase then we are using biometric features like as Face, Iris, and palm, Vein acknowledgement for verification function and safe transaction for the Mobile Banking.

Keywords:
The DAS(Draw A secret), 2DFLD, NND.

Cite This Article: Mushtaque Ahmed, Dr. Zhang Zuping, Mansoor Ahmed Khuhro, and Preeyaphat Amornngamprasert, "USING BIOMETRICS SYSTEM IN MOBILE BANKING" International Journal of Research – Granthaalayah, Vol. 4, No. 3 (2016): 119-123.

1. INTRODUCTION

Nowadays transformation of money is very necessary in world and it's more important to transfer money in secure system and this is why we are using ATM, western union service, money gram, Mobile Banking PayPal, Credit cards, etc. are obtainable in this growing world. These all technologies are really very useful but Mobile Banking is very better and easy to transfer from one source to another destination. In this Paper we are describing about the safety system of the Biometric system and current impression and assessment of the proficiencies which are utilized in the recent systems in segment. We are going to suggest verification device for the mobile banking during using the several verification constituents of biometrics for further vigorous verification in segment. And we are trying to more exploration some of the troubles in the communication stage of the info and present the use of coding for safe communication.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

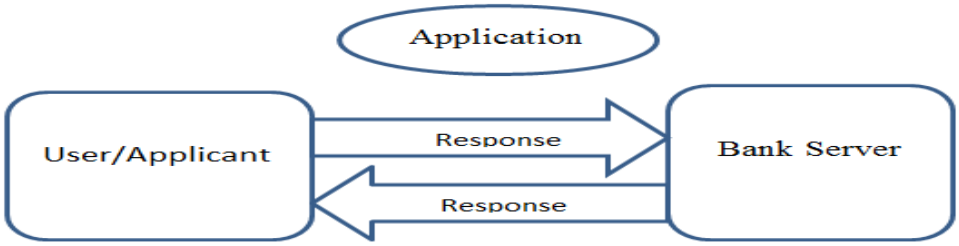


Figure 1: Unsafe Transmission Channel

SUGGESTED SYSTEM

In this article we are going to introduce verification method. The verification is a safety certification demanding the authentication of dissimilar modes of verification mechanisms and affords heightened safety. We are also suggesting combining biometrics safety with cryptography to attract safety over uncertain network. And here it is the fig. Exemplify the overall validating.

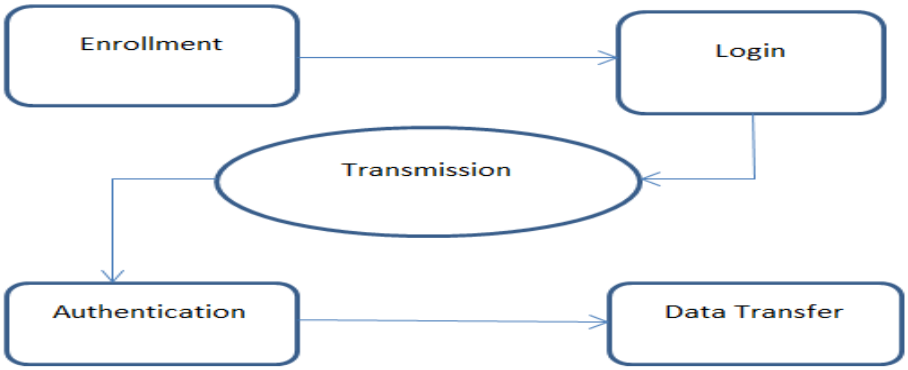


Figure 2: Verification Method

2. VERIFICATION PROCEDURE

The whole verification model is conversed below and instance.

ENROLLMENT

User can be enroll personally or using by mobile as well. During the entrance stage these two executed by the bank server.

1. The biometric info of the user is taken, preprocessed and types are removed. The feature models are shaped stocked as enrolled patterns. These stored patterns are mentioned during the authentication stage. Biometrics examples are captured in our system for suggest for the final pattern stowage in the user catalog.
2. The user has also specified eID and password separately from (i) as an extra parameter for individuality.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

LOGIN

While user wants to login he must have to enter his eID and password.

Server executes the subsequent earliest steps ;(i). Server will try to T current time impression of the user's device. (ii). The ID and given password.

GRAPHICAL PASSWORD

This kind of password is very easy to memorize for the account holder and commonly lexicon assails on graphical passwords are impracticable, the possibility of the suggested system is enhanced. Further, they told the suggested system can hold the play back attack, the password-file concession attack, the rejection of service attack, the expectable n attack, as well as insider attack. Especially the suggested system is correction able/Repairable. Keep in mind this method is safe under the premise that the simply to memorize DAS(Draw A Secret) password is robust. (iii) If the previous data is enrolled is perfect, the user is conveyed to the biometrics confirmation page and then user is requested to start audio as well as video transmission by mobile.

COMMUNICATION

This stage is only for taking care to the communicating info by the internet like we have not command over the unsafe channel.

- Due to cyber/hackers we can hide the video/audio info in images or videos connected to common life or else when skirmished by the hacker can be rejected and communication can be continued secured.
- If the communicating info is assumed by hacker he cannot extract the underground info.

AUTHENTICATION

On the accepting the login info and the stego file, the verification server will apply the below steps.

- The server performs the opposite of the implanting confidential info process to regain the biometric data from stego file.
- A server will also check the expiry time and date stamp with the present date and time T and T. The server discards the login application of user or accepts. T announce the required the valid time intermission for communication hold and T announces the accepting times stamp of login effort by the user.
- The biometrics is positively developed from the stego file, the face and acknowledgement taken positions are described in section 3.3 and appropriate applicant is correspond as it is in database system.
- Calculate T" and s T from the MAC sent by the server for verification. If it is the T the user will ignore the information otherwise computes the MAC hash purpose by using his personal key. If both are the same then server acquires verified if not the process will be finished automatically.

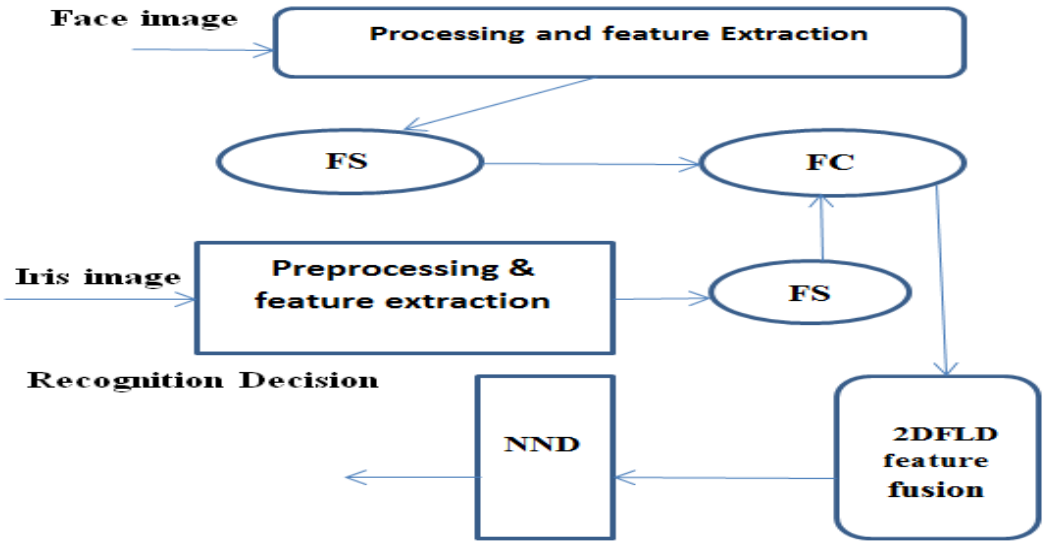
ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

DATA TRANSFER

User cannot transfer before the verification procedure; once user will be verified by the server then the user has to allow transferring the data.

3. FACE AND EYE ACKNOWLEDGEMENT ALGORITHM

Shape of the face and iris feature fusion has exposed initially, face image preprocessing and feature removal are done to achieve face unique feature medium. Then feature correction (FS) is performed to the face innovative feature atmosphere. Temporarily, iris image preprocessing and feature abstraction are understood to improvement iris unique feature matrix, and feature correction is done to the iris unique feature matrix. Then, feature mixture (FC) is utilized to assimilate the face correction matrix and iris adjustment matrix into one matrix and the joint matrix is gotten. Formerly, feature fusion and withdrawal are done to the joint matrix by way of 2DFLD. Temporarily, the optimal sharp estimate matrix is created, and the fusion feature matrix is increased. Lastly, NND is applied in acknowledgment.



4. PALM VEIN RECOGNITION ALGORITHM

The pictures of the vein image are in unsatisfied demarcation due to brightness, and incorporate unbalanced shadow produced by countless widths of skin and bones. Vein design verification needs a regularized and enhanced vein image to authenticate a dependable user. This paper presents a de noising and improvement proficiency based on GSZ – shock filter, which emphases on both sound evaluation and edge sweetening. Various Feature extraction technique extracts hand figure features.

5. IMPLEMENTATION/EXECUTION

The customer must be furnished with a mobile phone with a camera and the ability of browsing the internet through WAP (Wireless Access Protocol). Separately from this a consecrated

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

separate client/server application is needed for the fruitful actualization of transmission between the user and the bank. Nevertheless, the bank must deliver the user with the requirement software. A Java applet for that topic would be the best of explanation.

6. CONCLUSION

In this paper, we have demonstrated failings of some of the former remote user verification systems. That is why originally we are using graphical password using coding is utilized then we are moving the Biometrics verification for that in this paper I have utilized face, iris, and palm vein is utilized to validate the user if the verification is approachable user can transfer their money. As compare to other technologies this system is very and this is totally safe and secure.

7. FUTURE WORK

In future, more practice supervision and using such systems particularly the biometrics within the experimental setting might deliver more naturalistic data, falling the potential rinsing and prejudice of first time use. Programmatic effectuation of the same is also necessary to have a real life environment for more evolution to take place. Usage of biometrics may surely guide to real life physical verification systems. More strong systems for face and voice recognition required to be explored.

8. ACKNOWLEDEMENT

Author would like to thanks all friends those who helped a lot and parents for their prayers.

9. REFFRENCE

[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.