Review Article

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Engineering Survey
ISSN 2476-2105

2021
Vol. 9 No.1:18

Biometric Authentication in Mobile Banking

ASM Muntaheen* and Mohammad Abdus Shaker

Department of ICT-GIS Division, Institute of Water Modelling (IWM), Dhaka, Bangladesh

***Corresponding author:** ASM Muntaheen, Department of ICT-GIS Division, Institute of Water Modelling (IWM), Dhaka, Bangladesh, E-mail: muntaheen.mist@gmail.com

Citation: Muntaheen ASM, Shaker MA (2021) Biometric Authentication in Mobile Banking. Am J Comput Sci Eng Surv Vol. 9 No. 1:18.

Abstract

In present day world, mobile banking has emerged as a winner among various banking services. The major concern for mobile banking is its security. Since present authentication methods such as passwords, OTPs do not offer high level of security, there is always a risk of fraudulent attacks. To avoid this risk, reliable authentication procedures must be used. Biometric serves the purpose of reliable authentication mechanism. The paper gives the overview and quantitative comparative analysis of various physiological and behavioral biometric techniques that can be used in mobile banking. Various criteria that have been used for analysis are uniqueness, universality, permanence, circumvention, performance, and collectability and acceptability.

Keywords: Biometric; Quantitative analysis; Authentication; Mobile banking

Received: January 11, 2021; **Accepted:** January 25, 2021; **Published:** February 01, 2021

Introduction

Mobile banking is a service provided by a financial institution that allows customers to conduct financial transactions, such as electronic bill payments and funds transfers, using a mobile device and software provided by the aforementioned institution. While mobile banking has its upsides, security of financial transactions is a very important issue that needs to be addressed very carefully, as online banking is one of the most sensitive tasks performed by general user [1]. Although many traditional banks offer mobile baking with peace of mind [2], one should note that there is not a silver bullet providing a user with 100% security guarantee. Mobile banking in Bangladesh continues to grow fast, scaling a new height last year with 53 percent growth year-on-year. In 2015, the industry saw Tk 157,773.31 crore in transactions through mobile phones, the amount being more than half the country's national budget, according to a report of Bangladesh Bank. In 2014, the mobile banking industry saw Tk 103,155.37 crore in transactions. People are becoming increasingly comfortable with the banking platform, analysts said. The average monthly transactions made through mobile phones stood at more than Tk 13,147.77 crore last year, rising from Tk 8,596.28 crore in 2014 [3]. Transaction *via* Mobile Banking in BD is shown in **Figure 1**.

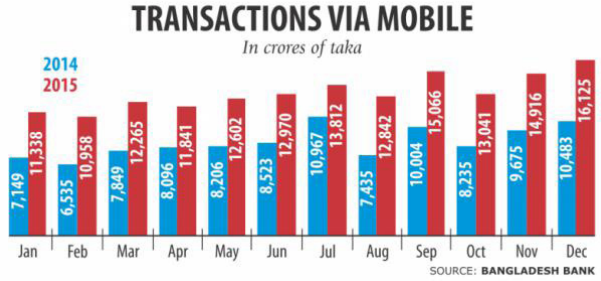

Figure 1: Transaction *via* mobile banking in BD.

There is no doubt that mobile banking has proven to be most convenient way of using banking services. But, along with various benefits, mobile banking exposes itself to various types of security risks. Major concern for mobile banking is to prevent unauthorized access. Considering the increasing number of financial frauds, a reliable authentication system must be incorporated. Biometric systems are known to be most reliable authentication systems, because they have the potential to solve many security problems. "Biometrics" is defined as "the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioral traits" [4]. Biometrics is widely used across various fields like forensics, ATMs, incellular phones, smart cards, PCs, in workplaces, and computer networks. But apart from its wide usage it is still not implemented in mobile banking. **Figure 2** shows proportion of using biometrics in different operations.

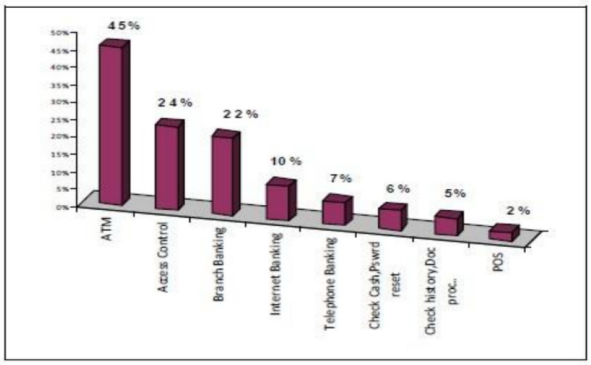

Figure 2: Proportion of using biometrics in different operations.

Authentication Schemes in Mobile Banking

In mobile banking, there are mainly two types of authentication schemes used i.e. single factor authentication and multi factor authentication [5].

Single factor authentication

Single factor authentication refers to the use of authentication credentials i.e., user name and password. Disadvantage of this scheme is that the passwords can easily be guessed and stolen by using different algorithms [5].

Multi factor authentication

Multi factor authentication makes the use of mainly two different factors i.e. something you have and something you know. It involves combination of two factors i.e., static passwords and one-time passwords generated by small devices. Although this scheme provides higher level of security than single factor authentication, but it is not reliable. There is always a risk of unauthorized access to mobile devices so the OTPs can be easily stolen [6].

Considering the shortcomings of single factor and multi factor authentication schemes, it is concluded that more reliable authentication mechanism must be incorporated in mobile banking. In this context an analysis of various biometric techniques is required so that best of them can be used for the authentication system.

An Overview of Biometric Modalities

Figure 3 shows Biometric Modalities. Biometric identification methods can be achieved on mobile devices either through its built-in biometric sensors, attaching portable biometric hardware to it *via* a USB cable, or through a Wi-Fi connection. Here are a few biometric authentication methods that banks are already taking advantage of:

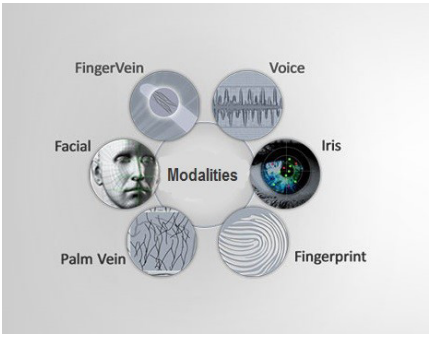

Figure 3: Biometric modalities.

Iris scan

Iris scanning biometrics measures the unique patterns in the colored circle of your eye to verify and authenticate your identity. Contactless, fast and renowned for its accuracy, biometric iris recognition can operate at long distances, with some solutions that leverage the modality requiring only a glance from a user [7].

This mode contains more than 200 unique points of data that are stored in the institution's database. Many biometric experts believe that the iris scan is the most reliable way of authenticating a user's identity (**Figure 4**) [8].

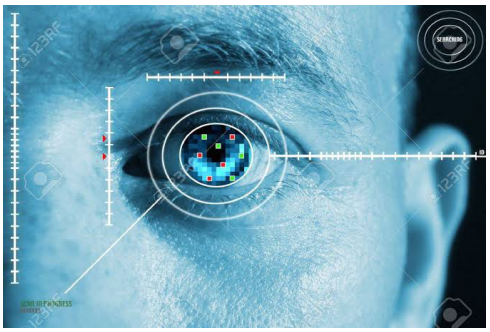

Figure 4: Iris scan.

Voice recognition

In this method, voice signals are converted into electrical signals and then compared with database. These systems operate with user's knowledge. However, wrong voices cannot always be avoided. Biggest drawback of this scheme is that the system may be hacked with prerecorded voice messages (**Figure 5**) [9].

Figure 5: Voice recognition.

Facial recognition

Facial recognition can authenticate users at ATMs, as well as online and mobile banking. This type of authentication is dependent on the user's environment such as the lighting or positioning of the face, making it a less effective security option [8].

It has a relatively low cost (i.e., it can be carried out using standard cameras) and is one of the least intrusive biometric modalities available, since it does not require physical contact like fingerprint recognition or retina scanning (**Figure 6**) [10].

Figure 6: Facial recognition.

Fingerprint scans

Fingerprint scans are currently the most popular form of biometric authentication used on many mobile devices worldwide [8].

The use of fingerprints for identification has been employed in law enforcement for about a century. A much broader application of fingerprints is for personal authentication, for instance to access a computer, a network, a bank-machine, a car, or a home (**Figure 7**) [11].

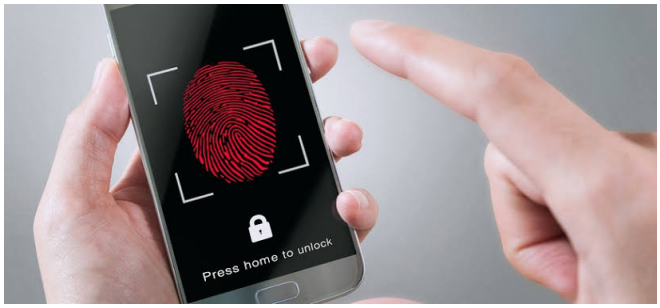

Figure 7: Fingerprint scans.

Vein pattern authentication

Vein pattern authentication relies on the unique pattern of veins in the palm, finger, or eye to identify a user. The vein patterns of the user are as unique as their fingerprints, but not as easy to replicate [12].

Finger vein patterns are unique biometric features, which differentiate from individual to individual, so they are suitable for authentication applications. Systems based on the use of this feature have numerous advantages such as low cost and high accuracy.

General Scheme of a Biometric System

There are three main functionalities of a biometric authentication process which are given below [13]:

Enrollment

Process of acquiring, accessing and storing data in the form of template for later use is called enrollment.

Verification

Verification is the process of matching between stored template and biometric. Matching score is provided between 0 and 100%. Although no system ever reaches to 100%.

Identification

Process of identifying an individual from a number of database values is called identification. Access may be granted to user or the user can also be rejected.

General scheme of biometric system is shown in **Figure 8** [14].

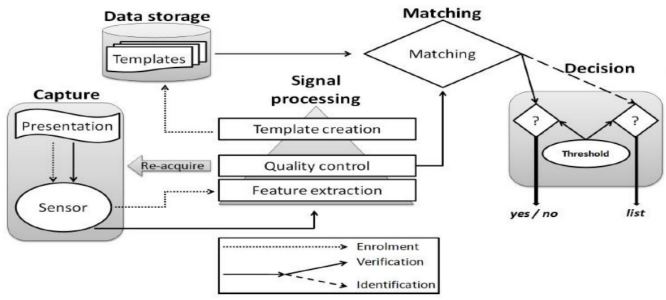

Figure 8: General scheme of biometric system.

Comparison of Biometric Techniques Based on their Properties

Biometric techniques are mostly characterized by seven properties [14,15]. These properties have been used as criteria for comparison.

- Universality: Every individual must have this property.
- Uniqueness: It should be distinct for two different individuals.
- Permanency: it should be preserved for lifetime of an individual.
- Collectability: it should be easily measured.
- Acceptability: it measures the use of a particular biometric system by users.
- Performance: it indicates the achievable accuracy, speed and robustness of the biometric property.
- Circumvention: it relates to ease with which a biometric system can be circumvented or bypassed. **Table 1** shows the comparison of various biometric techniques based on seven criteria [16,17].

Table 1: Comparison of various biometric techniques based on seven criteria.

Biometric technique	Universality	Uniqueness	Performance	Collectability	Acceptability	Resistance to Circumvention	Permanency	Total
Finger print	2	3	3	2	2	3	2	17
Face	3	1	2	2	3	1	2	14
Iris	3	3	3	2	1	1	3	16
Signature	1	1	1	3	3	3	1	13
Voice	2	1	1	2	3	3	1	13
Hand Vein	2	2	2	2	2	1	2	13

Discussion

Table 1 refers to the comparison between six biometric techniques i.e., Fingerprint recognition, Face recognition, Iris Recognition, Signature recognition and hand vein recognition. Comparison is based on seven criteria which are characterized by three levels i.e., Low, Medium and High [14,18]. In order to do quantitative analysis, numerical values have been assigned to these three levels i.e., 1 refers to low level, 2 to medium level and 3 to high level.

In this study, six biometric techniques which are more applicable to mobile banking have been chosen for analysis. **Table 2** refers to ranking of biometric techniques. Based on total values of seven indicators, Fingerprint recognition is the highest-ranking biometric feature, Iris recognition is second and Face recognition is placed on third rank which is followed by Signature, Voice and Hand vein recognition. Biometric systems require hardware implementation for proper functioning of the system. Fingerprint, Iris and face recognition require scanners for recognition. Since most mobile phones are equipped with these scanners nowadays days so it will be easier for banks to include biometric features in financial transactions. In order to achieve higher level of security, biometric systems can be combined with passwords.

Table 2: Ranking of biometric techniques.

Sr. No	Biometric	Total value
1	Fingerprint	17
2	Iris	16
3	Face	14
4	Signature	13
5	Voice	13
6	Hand Vein	13

Conclusion

Since traditional authentication methods used in mobile banking such as passwords, tokens etc. do not assure high level of security, it is clear that use of biometric system is imperative for security in mobile banking. This paper presents overall quantitative analysis of various biometric techniques so that appropriate technique can be incorporated in mobile banking. From above analysis, it has been inferred that Fingerprint recognition is best among six biometric techniques used for comparison. Future work will focus on studying and analyzing more important features other than above mentioned. Another scope for future work is to analyze various problems and security risks involved with Biometric systems.

References

1. Mannan M, Van Oorschot PC (2008) Security and usability: The gap in real-world online banking. In Proceedings of the 2007 Workshop on New Security Paradigms: 1-14.
2. Lee YS, Kim NH, Lim H, Jo H, Lee HJ (2010) Online banking authentication system using mobile-OTP with QR-code. In 5th Int Conf Comput Sci Converg Info Tech: 644-8.
3. The Daily Star. The dailystar. 2014.
4. Kaur S (2017) Security in mobile banking: A biometric approach. Int J Eng Sci Manag Res 4: 93-8.
5. Parusheva S (2015) A comparative study on the application of biometric technologies for authentication in online banking. Egypt Comput Sci J 39: 116-27.
6. Hayikader S, Binti Abd Hadi FH, Ibrahim J (2016) Issues and security measures of mobile banking Apps. Int J Sci Res Publ 6: 36-41.
7. Biometrics. findbiometrics. 2020.
8. How biometric authentication is shaping the future of security in mobile banking. 2019.
9. Bhatia R (2013) Biometrics and face recognition techniques. Int J Adv Res Comput Sci Softw Eng 3: 93-9.
10. Soldera J, Schu G, Schardosim LR, Beltrao ET (2017) Facial biometrics and applications. IEEE Instru Meas Mag 20:4-30.
11. O'Gorman L (1998) Fingerprint Verification. Biometrics 3: 43-64.
12. Tagkalakis F, Vlachakis D, Megalooikonomou V, Skodras A (2017) A novel approach to finger vein authentication. In 2017 IEEE 14th International Symposium on Biomedical Imaging: 659-62.
13. El-Abed M, Giot R, Hemery B, Rosenberger C (2012) Evaluation of biometric systems: A study of users' acceptance and satisfaction. Int J Biom 4: 265-90.
14. Stavroulakis P, Stamp M, editors (2010) Handbook of information and communication security. Springer Science & Business Media; 2010: 139.
15. Sharma K, Singh AJ (2012) Biometric Security in the E-world. In Cyber Crime: Concepts, Methodologies, Tools and Applications. IGI Global: 474-523.
16. Saini H, Garg K (2013) Comparative analysis of various biometric techniques for database security. Int J Sci Res 2: 45-51.
17. The best and most practical biometric modalities for individual identification. The Cloud Biometric Company. 2016.
18. Hosseini SS, Mohammadi S (2012) Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system. Int J Sci Basic Appl Res 2: 9152-60.