Biometric Identification: Comparative Analysis of Current Methods

Grigoryan Grigor*

Faculty of Finance, Armenian State University of Economics, Yerevan, Armenia.

Abstract: As the world transforms and becomes more digital, the number of passwords people manage also increases, thus making them difficult to store and manage. Financial institutions should take steps to implement relatively safe, secure, and easy-to-use biometric authentication technologies. One such technology is biometrics, which is the measurement and statistical analysis of unique physical and behavioral characteristics of people. For those financial institutions that use digital banking services, the issue of security and efficiency is paramount. These issues make the implementation of biometric authentication technologies critical for institutions to satisfy their customers' secure and convenient use of digital services, at the same time trying to differentiate and stay ahead of competing companies.

Keywords: Biometric identification, banks, digital banking, latest technologies.

With the rapid development of the Internet and mobile devices, authentication systems have also become widespread and developed, protecting user equipment, personal data, accounts, and more. Over time, it became more difficult for users to remember and use many passwords. For this reason, studies began to be carried out in the direction of identifying users using biometric data. Especially in recent years, in-depth studies have been carried out in the direction of new systems development and implementation that work with biometric data identification technology.

Currently, there are many systems working with biometric verification technology in the world. As a result of their implementation and use, the work of companies has become faster and easier, the customer experience has been transformed, etc. Among such technologies, the most widely used ones are based on voice, iris, fingerprint, palm print, and features.

Despite the fact that there are already many studies on biometric authentication in the world, some of them have been mainly done for one specific software environment, that is, a study of one technology has been done, rather than a comparative analysis of widely used technologies. Of course, the implemented technologies have both their positive and negative sides, but in this article we will analyze in detail the critical importance of such technologies in the conditions of comparison of several technologies.

First of all, it is necessary to understand how biometric technologies work, to imagine the structure of work and how they can be used in the banking system. Biometric systems work by using a person's biometric data, based on which special algorithms select characteristic features and create a biometric prototype. Created prototypes are stored in databases. The system can then verify the person's identity within seconds by comparing the obtained characteristics with prototypes in the database.

Biometric authentication technologies can be applied in banking system in several directions, including:

1. Identity verification: Biometric verification technologies may be used to verify a person's identity and open an account.
2. Authorization: Biometric verification technologies may be used before giving access to a customer's account or performing a transaction. Here may be used fingerprint, facial, voice or other authentication technologies.
3. Counterfeit prevention: Biometric verification technologies can be used to detect and prevent fraud before transactions are allowed.
4. Customer service: Biometrics can be used to improve the customer experience by allowing customers to use their voice or facial features to authenticate themselves, as opposed to traditional methods such as passwords or PIN codes.
5. Know your customer (KYC): Biometric data may be used as part of the KYC process to verify the identity of the customer and ensure compliance with regulations.

Studies show that, despite the importance of the main features characterizing biometric systems, they have not been given much attention when designing existing systems. While studying such solutions used in the Republic of Armenia, however, no detailed studies were found, which would characterize the strengths and weaknesses of the used technologies, features characterizing the level of reliability, etc. Since there is a lack of such literature and other sources of information in RA, we will try to perform a qualitative analysis to understand which of the existing technologies is

*Address correspondence to this author at the Faculty of Finance, Armenian State University of Economics, Yerevan, Armenia; Tel: +37455444220; E-mail: grigrig1997@gmail.com

the most favorable both for banks and customers to implement and use in RA, with the main emphasis on the accuracy, usability, efficiency, security and privacy of data systems.

It is commonly accepted to divide biometric authentication into two parts: identification based on physiological characteristics and behavioral characteristics: Physiological features include fingerprints, facial features, iris, palm, and finger vascular structures, and behavioral features include voice, signature, keystrokes, etc.

In practice, various biometric authentication frauds are used in a unique way for each technology. For example, when identifying with facial features, user data can easily become available to fraudsters through the Internet, especially social networks, where there are a large number of personal photos and videos. Having access to such data, fraudsters will not have much difficulty in deceiving the system as well.

Using a high-end optical camera, it is possible to gain access to the image of the user's iris, thanks to which it is possible to cheat an iris-based identification system, but such spoofing is usually expensive, since the cost of such an optical camera is also high.

Another method of fraud is using fingerprints and palm images. Many artificial materials are currently used to obtain a fake image of a hand, and obtaining a fingerprint or an image of a palm is not that difficult, because people touch many objects during the day, from which forgers can collect the necessary information.

Voice-based authentication systems are also easily vulnerable, since in an open space sound travels in all directions, and by recording it and later fraudulently using it in the authentication process, it is very likely that the system can be fooled.

In order to avoid the above mentioned risks, preventive measures should be applied, such as keeping sensitive information in a safe place, using multi-step authentication systems, *etc*., but we also need to know that not all attacks can be avoided through preventive measures. After studying the works of many authors in this direction, we came to the idea that in order to evaluate the best biometric authentication technology, the following factors need to be considered: accuracy, efficiency, usability, security and privacy.

In order to give an assessment of accuracy, it is necessary to define standards according to which the degree of accuracy of the given technology should be assessed. Accordingly, we can distinguish the following:

- False Acceptance Rate (FAR), which means identifying the forger as a legitimate user.
- False Rejection Rate (FRR), which means identifying a legitimate user as a fraudster.
- Equal Error Rate (EER), when the error acceptance rate is equal to the error rejection rate. Usually, the lower this percentage is, the more accurate the given technology is.

As the main indicator characterizing the efficiency, we can accept the time during which the system is able to perform the identification of the person. It includes the time of data collection, processing, separation of features, as well as the time to make a decision.

When looking at usability, a number of features should be explored which include:

- Universality (UV), which means that all users must have the specified identifier to be able to use the given authentication technology.
- Uniqueness (UQ), which means that the characteristics of any two persons are different.
- Permanence (PM), which means that the characteristic features do not change over time.
- Acceptability (AC), which means that it is acceptable for a large number of users to collect characteristics using a given identification technology.
- Extra Equipment (EE), which refers to the availability of additional special equipment through which the characteristics must be collected.

As we mentioned, biometric verification systems are quite vulnerable to a number of attacks, therefore, it must have the ability to withstand attacks, that is, the collected data must be impossible or extremely difficult to falsify, and according to the level of falsification difficulty, security standards are defined. If, however, the system has been attacked, it is usually accompanied by a data leak, which is a breach from a privacy perspective.

The studies were mainly conducted from the following three sources:

- From the professional literature, collecting and evaluating the obtained experiments and results,
- From the Internet,
- From personal experience, which was formed by combining professional work experience and existing scientific results.

As a result of the conducted studies, we have identified 2 main branches of biometric authentication. The first branch is based on static characteristics that remain unchanged or undergo very little change over time, such as face, fingerprint, iris, etc., and the other branch is based on dynamic characteristics such as sound, keyboarding style, etc.

In order to understand which of the identification technologies working on the basis of static and dynamic characteristics are the best in comparison from the point of view of use in RA, we will study the works done by different authors and try to separate them according to the factors listed above, giving Low (L), Medium (M) or High (H) grades. According to the obtained results, we will try to classify the identification methods.

As a result of studies, we have separated the main methods of identification, which are shown in Table **1**.

Identifying people based on facial features is quite common, as each individual has unique features. In general, we can say that the shape of the face is the same for all people, that is, the eyes, mouth, nose, etc. are part of the shape of the

face, but their contours, the distances of certain points from other parts of the face, and the angles that make up the face are mostly different, by which also depends on the specifics of the given technology and the formula of the work. At the same time, we should note that these characteristics change over time, and as a result of changes in the characteristics, the technology may not identify the person. It turns out that this technology has high usability from the point of view of universality, while we can give it a low rating from the point of view of uniqueness and permanence.

In recent years, a number of interesting research have been carried out on the identification of people based on facial features. In Table **1**, we will separate the main research results according to different criteria, giving Low, Medium, High grades (in case of absence, "-").

Table 1. Results of identification methods performed by different researchers.

Method	References	Accuracy	Efficiency	Usability	Security	Privacy
Facial Recognition	[1]	L	-	M	L	-
	[2]	M	M	M	H	-
	[22]	L	-	M	-	-
	[3]	M	H	M	H	L
Iris Recognition	[4]	H	-	M	M	L
	[6]	H	-	M	M	-
	[5]	H	-	M	M	-
	[13]	H	-	M	H	-
	[23]	H	L	M	M	L
	[24]	M	-	M	M	-
	[25]	H	M	M	M	-
Fingerprint/Palm Recognition	[26]	-	-	H	M	-
	[9]	H	H	H	-	-
	[10]	H	H	H	-	-
	[11]	H	-	M	H	-
	[7]	-	-	M	H	-
	[12]	M	M	M	H	-
	[8]	M	-	M	H	-
	[13]	M	-	M	H	-
	[24]	H	-	H	L	L
	[25]	H	-	H	L	M
ECG Signals	[16]	-	-	M	H	-
	[14]	M	-	M	H	-
	[15]	H	-	M	H	-
Voice Recognition	[17]	L	-	H	H	-
	[18]	M	-	H	L	-
	[19]	L	-	H	H	-
Keystroke/Touch Dynamics	[20]	H	-	L	M	-
	[21]	M	-	L	M	-
	[22]	M	-	M	M	-

(L = Low, M = Medium, H = High)

We can highlight Gonzalez-Jimenez and Alba-Castro's research using 2D images [1]. During the analysis, various identification methods were applied using 2D images, changing the positions of the received images, angle degrees, different facial movements, etc. As a result, the accuracy level of the technology was 30%, which, should be noted, is not a high indicator, moreover the technology was not able to distinguish the emotional state of a person, that is, if the person was smiling, sad or with a different facial expression when receiving the image. As a result, the accuracy of the technology was rated as low, usability as medium, security as low, but privacy and efficiency were not discussed in the research.

Some time later, Queirolo and several other co-authors conducted research, but this time with 3D scanning [12]. The results were satisfactory because, unlike the previous study, this time the accuracy level of the system was 96%, and the false acceptance rate (FAR) was 0.1%. The authentication process took between 1.5 and 3.1 seconds, and excluded the fact that counterfeiters could use photos during 3D scanning. Considering the above circumstances, this method has been rated as medium for accuracy, medium for efficiency, medium for usability, high for security, but privacy has not been discussed.

Identification of people using FaceID became more popular in recent years, when one of the major companies, Apple, began to use it for its mobile devices as well [3]. The technology is based on machine learning, and the company has further improved the technology. As a result, before identifying the customer, the system is able to understand whether the received data is not fake (liveness detection), and customer identification is done when the customer is looking directly at the phone's lens, thus giving its consent to be authenticated. Overall, this system is rated as medium in accu-

racy, high in efficiency, medium in usability, high in security, and low in privacy.

Iris authentication is considered a non-contact biometric feature like facial features, which makes it more advanced. From the point of view of acceptability (AC), we can note that it is less widely accepted than identification based on facial features, but from the point of view of uniqueness (UQ) and permanence (PM) it is very high. As for universality (UV), it also does not show high indicators.

As a result of Pillai's research, an algorithm was put forward, which was based on identifying a person using distorted images of the iris [4]. As a result of the research, experiments with deliberately false data were also carried out, but the system was able to distinguish false experiments. As a result, it was able to record a high level of accuracy of 99%, medium level of usability, medium security and low privacy, and no study has been conducted on the effectiveness.

Thavalengal, along with a number of other researchers, investigated the hypothesis that the concentration of pixels in smartphone cameras is too low, which limits the process of iris identification by mobile devices [5, 6]. Considering the above circumstances, they were able to come up with several business strategies, where the accuracy rate of iris biometric identification exceeded 98%, the usability and security were rated as medium, but no results were obtained from performance and privacy results.

Some researchers claim that repeated attacks on systems can be prevented by using an iris authentication system. According to the above idea, Pacut and Czajka conducted a research and presented 3 solutions on how to distinguish fake and real iris during identification. As a result of the research, it was reported that the mentioned method has high accuracy, medium usability and high security, but the efficiency and privacy of the system have not been discussed in the work.

Czajka and a number of other researchers presented a biometric smart card that can be used for multiple authentication systems. As a result of the studies, the accuracy of the system was rated high, usability - medium, efficiency - low, security - medium, privacy - low.

The evaluations of several other publications and studies are summarized in Table **1**.

In recent years, fingerprint-based identification technologies have been widely adopted and applied not only at the academic level, but also in practice. Since fingerprint recognition technology is easy enough to implement and relatively stable, identifying a person using it is also easy enough to implement. It has medium universality (UV) and high levels of uniqueness (UQ), permanence (PM) and acceptability (AC). As a result, fingerprint technology has been widely adopted and used in large volumes, for example almost all mobile devices have fingerprint identification technology installed.

Fingerprint-based authentication technologies are not limited to fingerprints. Studies were also done by Kumar and Ravikanth in the direction of identification with images of the back of the finger [9]. The results were quite promising, with an error rate of 1.39%. The authentication process took approximately 530 milliseconds. Sometime later, Prasad made improvements in palm recognition technology based on discrete wavelet transform [10]. As a result, the level of accuracy was 98.63%, and the total process was 622 milliseconds. Despite making such attempts, no other parameters were touched here except the authentication technology to make the security and privacy of the system clear, as users could cheat the system with fake images, and data leakage would occur. As a result, the system was rated high for accuracy, efficiency, and usability, while no ratings were given for security and privacy.

In the above-mentioned studies, the criteria that would be possible to distinguish whether the given fingerprint is real or not were missing. Currently, fingerprint authentication is the most common biometric authentication technology for mobile devices. Later research were conducted where an attempt was made to understand whether the fingerprint/palm is fake or real. Such an example is Pavešić's research, where the principle of multiple verification was developed based on thermal images of the palm surface [11]. After testing 29 real and 56 artificial thermal images, a 0% error rate was reported. Although this method has high accuracy, it was necessary to have an additional camera on mobile devices to check thermal walls, due to which the level of usability is estimated as medium, and also the person cannot be sure of the privacy of personal data, so we cannot estimate the level of privacy, and from the point of view of security, this method has a high level.

In another study done by Judhav and Nerkar, they claim that human finger vein identification system is better because it has low falsification rate [12]. According to this approach, their experiments achieved 97% accuracy with a 3% error rate, and the process took only 2 seconds. As a result, accuracy, usability and effectiveness were reported as medium, safety as high, but the research did not mention anything about privacy.

In another study, Ferrer put forward the idea of tissue identification [13]. For the experiment, a high pixel accuracy camera was used for 154 subjects. As a result, the error rate was 3.29%. Here, the level of accuracy, applicability, and safety was rated medium, and no study was conducted on effectiveness and privacy.

The above-mentioned studies were connected with static characteristics. The dynamic characteristics, which refer to the behavioral characteristics of a person, will be discussed below. Key static features include ECG signals, voice recognition, keystroke/touch dynamics, etc., which we will cover in more details.

Carreiras conducted research focusing on the uniqueness feature [14]. The study was performed based on 618 subjects, recording an error percentage of 9.01, and it was also recorded that the percentage of errors does not increase with the increase of subjects.

Keshishzadeh and Rashidi proposed 2 different ways to apply ECG signals [15]. For each selected signal, four additional artificial features were created, which were further classified according to different features. During the trial testing, the identification with the mentioned methods recorded 99.38% accuracy.

In a number of other studies, the idea is put forward that over time the prices of various sensors will decrease rapidly and systems based on ECG signals can be attached to mobile equipment, such as bracelets, through which the authenticity of the identified person can be verified. However, this method still has low usability and high security, and privacy-preserving studies are still lacking [16].

One of the dynamic forms of biometric verification is identification using voice recognition technology. Since almost all current mobile devices have a microphone, and almost everyone has the ability to speak, except for people with speech problems, the acceptability, uniqueness, universality and permanence of this technology are high, that is, this method has high usability.

Jayamaha, along with a number of other researchers, developed a voice recognition system based on HMM (Hidden Markov Model) [17]. Previously, this technology was used for speech recognition, but here they used it in a slightly different way, trying to separate certain features from the voice and use them to identify the person. In pilot testing, this method recorded 86% accuracy, receiving a low rank. From the point of view of security, it had a high level, because it was possible to falsify only 2 out of 150 tests, but there were no discussions about privacy in this work.

Galka and a number of other researchers conducted research on access authorization, again using the Hidden Markov Model [18]. Here, the percentage of error was 3.4%, which ensures high accuracy, and no studies were conducted with the rest of the criteria.

In their work, Yan and Zhao developed a new format for voice authentication, which consisted of 3 main levels: user, third party, and authenticating party [19]. Due to the multi-level security used here, the system is able to provide a high level of security, but from the point of view of accuracy, it has a low level, as the identification accuracy is only 80.6%, and efficiency and privacy are not discussed in the work.

Saevanee and Bhattarakosol note that touch dynamics provide more accurate information than keystroke dynamics [20]. But to check the dynamics of the touch, a sensor must be installed on the device so that the touch signals can be collected. Identification using dynamic keystrokes usually occurs with 2 classifiers, positive and negative, and by collecting the mentioned information, the system can identify the person. Then Antal and Szabo carried out research on improving the accuracy of the system, which was able to work with both one-class and two-class algorithms at the same time [21]. That is, when working with negative information it was not possible to collect information with the help of a binary classifier, then the system can identify a person using a single-class algorithm.

Since mobile devices no longer use pressure-sensitive sensors in recent years, researchers have begun to conduct studies based on touch dynamics [22]. Servada et al. conducted a study based on behavioral characteristics to determine the error rate of a system and concluded that chronological information about the occurrence of errors can help solve this problem.

However, over time, with the development of mobile devices and fingerprint sensors, the latter method has largely given way to emerging and widely usable methods such as fingerprint and facial recognition methods.

Research Results

Exploring the research done by the above-mentioned authors, let's try to classify the identification methods and find the method that best suits the participants of the RA banking system.

Since several criteria have been set for the research: accuracy, efficiency, applicability, security and privacy, we will try to find the best method according to those criteria. Despite the fact that the presented criteria are closely related to each other, banks that are going to introduce biometric identification technology, depending on their business strategy, can define the priorities of the given criteria. In theory, banks that are completely new to digital banking will focus on usability when choosing a biometric authentication method, so that a relatively large number of people can use their digital banking services, followed by accuracy, with the aim of ensuring that the technology works relatively flawlessly. Security, privacy, and efficiency can already follow these standards accordingly.

Banks that already have digital banking services in place, a stable customer base, and want to transition to customer engagement and service through biometric authentication can focus on security first to avoid customer data leaks, customer dissatisfaction, and other negative circumstances. After the security standard is met, according to the business strategy, the degrees of importance of the other standards can be set, with the aim of ensuring a high level of all other standards.

In order to understand which of the above-mentioned methods is the best choice, a number of researches were studied, the trends and perspectives of current technology development were taken into account.

Based on the data in *Table 1*, we can conclude that the usability of Keystroke Dynamics is medium to low, which means that fewer users can use this technology compared to other technologies. The number of researches in the direction of this method is not so much, so the information serving as a basis for the conclusion is not fully substantiated, but by combining the results of the existing researches with our own experience, we can come to certain results. In terms of security and accuracy, the system is rated medium, but there are no analyzes on efficiency and privacy. However, we think that we can give privacy a medium level rate, because trying to have access to such information by means of hardware would require additional efforts, use of embedded hardware in user equipment, etc. In general, we can give it a medium level for implementing this method, but from the point of view of implementing it in the RA banking system, it is not very appropriate.

Voice recognition technology has a high level of applicability, as microphones are already installed on almost all devices, which makes this method easy to apply. From the obtained results, we can conclude that security records average indicators, and from the point of view of accuracy, it is below average. Although serious work has been started in the direction of this technology recently, we can state that the

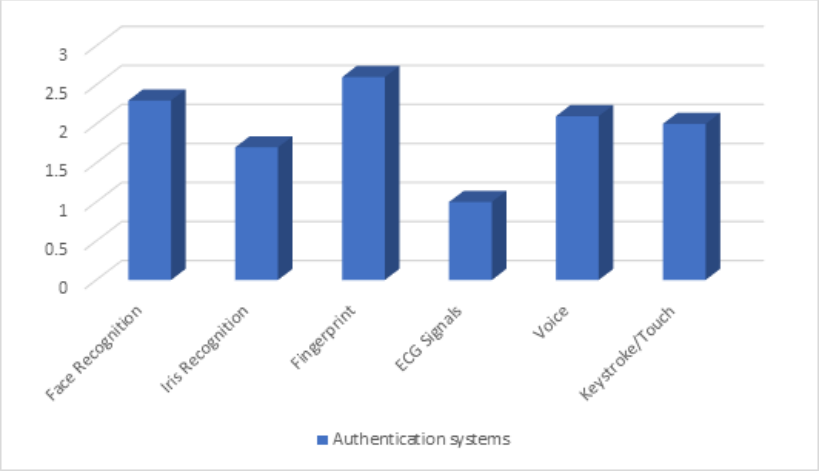

Chart 1. Ratings of Identification Systems According to Our Findings.

final appearance of this technology is not yet to the point that it would be appropriate to introduce it into the banking system, but we expect that in the near future there will be such versions of this system that will be able to fully meet the requirements of both users and the organization. At the moment, we can give the method an average rating, expecting that after some time it will become quite a competitive method.

Voice recognition technology has a high level of usability, as microphones are already installed on almost all devices, which makes this method easy to apply. From the obtained results, we can conclude that security records medium indicators, and from the point of view of accuracy, it is below medium. Although serious work has been started in the direction of this technology recently, we can state that the final appearance of this technology is not yet to the point that it would be appropriate to introduce it into the banking system, but we expect that in the near future there will be such versions of this system that will be able to fully meet the requirements of both users and the organization. At the moment, we can give the method an average rating, expecting that after some time it will become quite a competitive method.

As a result of the examination of ECG signals, we can conclude that this method records quite good results from the point of view of safety, but from the point of view of accuracy and usability, it provides an average level. As with the keystroke method, it is difficult to find many studies where both effectiveness and privacy have been studied, and it is difficult to expect any exact results at this time, however, modern trends lead to the fact that the use of this method will also increase in the near future. According to our conclusion, at the moment, it is not advisable to implement this method not only in RA, but also in other countries, because it will be necessary to implement special techniques in already existing mobile and other equipment.

As we can see in Table 1, the accuracy of the iris provides a very high level, but the usability and security are medium. Compared to the previously discussed methods, this method recorded higher than medium indicators, but we should note that we have a medium level of usability. This method is currently not encouraged to be used by banks that aim to attract new customers, as the method is simply not usable for a wide segment of customers.

Almost all of us have come across devices that use fingerprint or facial biometric authentication. In recent years, these 2 methods have been widely used on new mobile devices, which means that the usability data in our table almost completely reflects the real picture. According to the data in our table, we can estimate the accuracy of the face biometric verification method to be below medium, but if we consider that the research data also includes data from 3 and more years ago, we can give at least a medium estimate, taking into account the fact that to improve the accuracy of this method enough efforts have been made in recent years. The level of accuracy of the fingerprint, according to the table we received, is above medium, which is logical to the extent that we hardly encounter cases of fingerprint repetition in real life. Comparing the effectiveness indicators of these 2 methods, we can rate it above medium for both methods. Given the fact that the number of studies on effectiveness is not so great, this estimate can be slightly deviated in both positive and negative directions.

Comparing the usability indicators, we can give it a medium score for face recognition, expecting technology development with modern trends, high score for fingerprint recognition and above medium score for palm image recognition.

From the point of view of security, we can rate facial recognition technology as above medium, but due to the amount of research, this indicator can also fluctuate to a certain extent. In the case of fingerprint, there are enough studies, so the deviation of the rating will not be too big, and we can give it an above medium rating.

Since we do not have a lot of research on privacy either, and the research that has been done gives both of these methods a lower than medium rating, it would be more correct to avoid giving a specific rating.

If we try to evaluate these two methods with the existing standards, we can give the facial biometric verification method an above medium rating, closer to the medium rating, and the fingerprint biometric verification technology - a medium rating, considering that it has relatively high indicators by some standards.

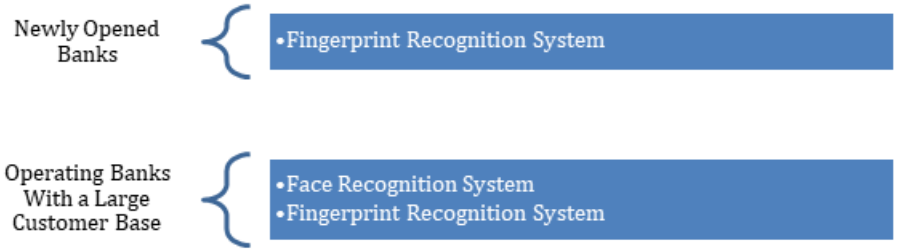

Fig. (1). Recommended Systems for Newly Opened and Operating Digital Banks.

Summarizing these indicators, we can conclude that now the best method that will fit the strategy of a bank with a large customer base is to introduce a biometric verification method using a fingerprint, and for a bank with a strategy to attract customers, it is recommended to introduce a dual method - facial and fingerprint recognition systems. With facial biometric authentication technology, a person can become a bank customer without going to a bank branch, and using the fingerprint authentication method - fill in the gaps that would arise if accuracy, usability and security issues arise in the face identification process.

CONFLICT OF INTEREST

I would like to affirm that there are no conflicts of interest to declare in relation to the research, analysis, or presentation of the findings within this manuscript.

ACKNOWLEDGMENTS

I am deeply indebted to several individuals and organizations whose unwavering support and contributions made this research possible.

To my family, whose constant encouragement, patience, and understanding have been my pillars of strength throughout this journey. Your belief in me has been my driving force, and I am profoundly grateful for your unwavering support.

To my friends, for their camaraderie and understanding during the highs and lows of research. Your encouragement and thoughtful discussions have enriched my perspective and kept me motivated.

I would like to express my heartfelt gratitude to my scientific supervisors, for their invaluable guidance, mentorship, and expertise. Their insightful feedback and dedication to my academic growth have been instrumental in shaping this research. I am fortunate to have had the opportunity to learn from you.

I also extend my sincere thanks to the Armenian State University of Economics and FastBank CJSC for their support and resources. The academic environment and research facilities provided by these institutions have been pivotal in the successful completion of this study. Their commitment to fostering research and innovation is truly commendable.

This research has been a collaborative effort, and it would not have been possible without the collective support of my family, friends, scientific supervisors, and the backing of the Armenian State University of Economics and FastBank CJSC. I am deeply appreciative of the opportunities and assistance that have paved the way for this work.

REFERENCES

https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

https://www.innovatrics.com/glossary/biometric-system/#:~:text=Identification%20System%20%E2%80%93%20ABIS.-,How%20does%20a%20biometric%20system%20work%3F,reference%20to%20the%20biometric%20database.

https://www.researchgate.net/publication/325585048_Securing_Mobile_Healthcare_Data_A_Smart_Card_Based_Cancelable_Finger-Vein_Bio-Cryptosystem

https://www.innovatrics.com/glossary/false-accept-rate-far/#:~:text=False%20Accept%20Rate%20(FAR)%20is,False%20Match%20Rate%20(FMR).

https://www.innovatrics.com/glossary/false-reject-rate-frr/

https://www.innovatrics.com/glossary/equal-error-rate-eer/

H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, ''Recognizing surgically altered face images using multiobjective evolutionary algorithm,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89–100, Jan. 2013.

D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, ''Fake fingerprint detection by odor analysis,'' in Proc. Int. Conf. Biometrics. Berlin, Germany: Springer, Jan. 2006, pp. 265–272.

S. Li and A. C. Kot, ''Privacy protection of fingerprint database,'' IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.

S. Li and A. C. Kot, ''Fingerprint combination for privacy protection,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 2, pp. 350–360, Feb. 2013

W. Yang, J. Hu, and S. Wang, ''A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement,'' IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1179–1192, Jul. 2014.

D. Pishva, ''Spectroscopic approach for aliveness detection in biometrics authentication,'' in Proc. 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol., Oct. 2007, pp. 133–137.

A. Franco and D. Maltoni, ''Fingerprint synthesis and spoof detection,'' in Advances in Biometrics. Berlin, Germany: Springer, 2008, pp. 385–406.

D. Gonzalez-Jimenez and J. L. Alba-Castro, ''Toward pose-invariant 2-D face recognition through point distribution models and facial symmetry,'' IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 413–429, Sep. 2007.

C. C. Queirolo, L. Silva, O. R. P. Bellon, and M. P. Segundo, ''3D face recognition using simulated annealing and the surface interpenetration measure,'' IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 2, pp. 206–219, Feb. 2010.

A. B. Proov, ''Facing the future: The impact of Apple FaceID, '' Biometric Technol. Today, vol. 2018, no. 1, pp. 5–7, Jan. 2018.

J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, ''Secure and robust iris recognition using random projections and sparse representations,'' IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

S. Thavalengal, P. Bigioi, and P. Corcoran, ''Iris authentication in handheld devices—Considerations for constraint-free acquisition,'' IEEE Trans. Consum. Electron., vol. 61, no. 2, pp. 245–253, May 2015.

S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, ''Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones,'' IEEE Trans. Consum. Electron., vol. 61, no. 2, pp. 137–143, May 2015.

A. Pacut and A. Czajka, ''Aliveness detection for IRIS biometrics,'' in Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol., Oct. 2006, pp. 122–129.

A. Czajka, P. Strzelczyk, M. Chochowski, and A. Pacut, ''Iris recognition with match-on-card,'' in Proc. 15th Eur. Signal Process. Conf., Sep. 2007, pp. 189–192.

A. Kumar and C. Ravikanth, ''Personal authentication using finger knuckle surface,'' IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 98–110, Mar. 2009.

S. M. Prasad, V. K. Govindan, and P. S. Sathidevi, ''Palmprint authentication using fusion of wavelet and contourlet features,'' Secur. Commun. Netw., vol. 4, no. 5, pp. 577–590, May 2011.

N. Pavešić, T. Savič, S. Ribarić, and I. Fratrić, ''A multimodal handbased verification system with an aliveness-detection module,'' Ann. Des. Télécommun., vol. 62, nos. 1–2, pp. 130–155, Jan. 2007.

M. Jadhav and P. M. Nerkar, ''Implementation of an embedded hardware of FVRS on FPGA,'' in Proc. Int. Conf. Inf. Process. (ICIP), Dec. 2015, pp. 48–53.

M. A. Ferrer, A. Morales, and A. Díaz, ''An approach to SWIR hyperspectral hand biometrics,'' Inf. Sci., vol. 268, pp. 3–19, Jun. 2014.

C. Carreiras, A. Lourenço, A. Fred, and R. Ferreira, ''ECG signals for biometric applications—Are we there yet?'' in Proc. 11th Int. Conf. Inform. Control, Automat. Robot. (ICINCO), vol. 2, Sep. 2014, pp. 765–772.

S. Keshishzadeh and S. Rashidi, ''Single lead electrocardiogram feature extraction for the human verification,'' in Proc. 5th Int. Conf. Comput. Knowl. Eng. (ICCKE), Oct. 2015, pp. 118–122.

H. P. da Silva and A. Fred, ''Harnessing the power of biosignals,'' Computer, vol. 47, no. 3, pp. 74–77, Mar. 2014.

R. G. M. M. Jayamaha, M. R. R. Senadheera, T. N. C. Gamage, K. D. P. B. Weerasekara, G. A. Dissanayaka, and G. N. Kodagoda, ''Voizlock—Human voice authentication system using hidden Markov model,'' in Proc. 4th Int. Conf. Inf. Automat. Sustainability, Dec. 2008, pp. 330–335.

J. Galka, M. Masior, and M. Salasa, ''Voice authentication embedded solution for secured access control,'' IEEE Trans. Consum. Electron., vol. 60, no. 4, pp. 653–661, Nov. 2014.

Z. Yan and S. Zhao, ''A usable authentication system based on personal voice challenge,'' in Proc. Int. Conf. Adv. Cloud Big Data (CBD), Aug. 2016, pp. 194–199.

H. Saevanee and P. Bhattarakosol, ''Authenticating user using keystroke dynamics and finger pressure,'' in Proc. 6th IEEE Consumer Commun. Netw. Conf., Jan. 2009, pp. 1–2.

M. Antal and L. Z. Szabó, ''An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices,'' in Proc. 20th Int. Conf. Control Syst. Comput. Sci., May 2015, pp. 343–350.

C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, ''Performance analysis of touch-interaction behavior for active smartphone authentication,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 498–513, Mar. 2016.

Received: September 20, 2023 Revised: September 22, 2023 Accepted: September 27, 2023