binary

by E L

Submission date: 30-Mar-2022 12:46PM (UTC+0530)
Submission ID: 1796773857
File name: final.docx (246.55K)
Word count: 2166
Character count: 11689

Biometric Authentication Systems

Name
[Email address]

Table of Contents

Table Of Figures

Introduction

We always come across the situations where we must authenticate ourselves and validate that we are the intended users and can get required access. Usually, we use the old process of using passwords or Pin numbers to verify the identification. Biometric authentication was introduced to automate the verification process and provide the result effectively and at a faster rate. It is a process of using a part of physical body to verify the access to the given person. It can be done using any feature of an individual that makes them different from others. The main purpose of biometric authentication is to avoid unauthorized access to the data by using the unique identity of every individual for verification. (Din, 2021)

In biometric authentication, the physical characteristic is mapped to the username and is used for taking the decision for authentication. Some of the most used biometric techniques are Fingerprint recognition, Facial recognition, Voice verification, Retinal Identification and so on. Biometrics is getting incorporated into day-to-day activities like fingerprint recognition in smartphones, Facial recognition in airports and voice recognition in assistant devices.

Block Diagram of biometric methods

The below diagram shows the block structure of biometric methods.

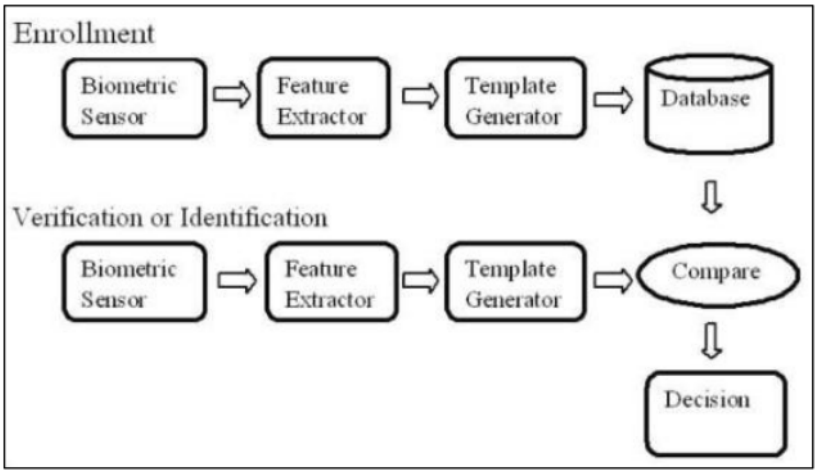

Figure 1 block structure of biometric methods (Anil K. Jain, 2004)

During the enrollment phase the data of individual is collected using biometric sensors. Required features are extracted from the data and passed to template generator to get the data in the required format. This data is stored in the database and is used for verifying the identity of the user. Now whenever a user comes for getting access to the system his data is verified using the sensors and the features are extracted. It is then generated into required template and compared with the data in the database. If both are templates are matched, then the user is an authorized user and if the given data is not matching with the stored data, then the user is an unauthorized user.

Working

The identification of an individual is taken and saved in the system. Sensors like fingerprint reader, voice recognizer or retina scanner are used for capturing the biometric data. These sensors capture the data and compare with the stored data. This data is provided by the user for validating him for getting access to the system. The data is encrypted and stored in a remote server to add another layer of protection and is matched with the visitor to approve or deny the access to system. A biometric device consists of three main parts. A reader or a scanner to capture the user data, a technological process to convert the given data and compare it with saved data and a database for storing the data (Anil K. Jain, 2004).

Biometric Authentication

There are many types of biometric authentication.

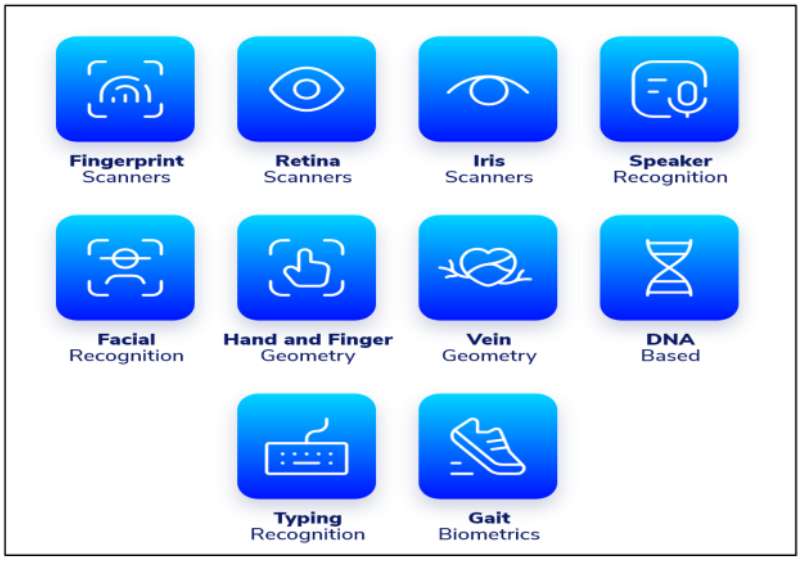

Figure 2 Biometric authentication methods (Din, 2021)

The working structure of few of the popular ones are as follows:

Fingerprint authentication

In this type of biometric authentication one among the three types of fingerprint scanners namely optical, capacitive and ultrasound is being used.

Optical scanner takes the image of the finger, matches, and compiles it for identification. In capacitive scanner electric signals are sent between finger and scanner. The prints in the finger create electrical current while the valleys create the air gaps forming a unique pattern. This type of scanners is being used in laptops and smartphones. Ultrasonic scanners work similar to capacitive scanners but instead of electrical signals they emit the ultrasounds that reflects back to the scanner. These scanners will be used in the coming generation of smartphones. Hacking the fingerprint scanners is a very difficult task as the attacker will need to have a high-quality image of the fingerprint pattern. (Roy, 2022)

Iris authentication

Iris is a part of the body whose structure remains same throughout the lifetime. So, it is considered as a good biometric for identifying an individual. The major advantage of Iris scanner is that the information of individual is not leaked in any form, and it remains unchanged and does not fade away or get eroded. Iris authentication is the best of biometric authentication as it has very low margin for errors and uses high quality photograph of one or both irises of the eyes. The process of verification involves capturing the clear image of the iris. The boundary of the iris is located capturing the center of the circular iris. The iris region is then shadowed by covering the portions of eyelids and reflective areas. The image is then converted into biometric templates which contain the encrypted features of the iris. (Mostafa, n.d.) Iris authentication has the best speed for searching the data from the database and is capable of handling large amount of data. Big enterprises and industries also use iris authentication as one to many searches mode is the fastest when compared with other authentication method. This type of authentication is being used in banks for fast authentication and in healthcare industry for high accuracy and ease of use.

Retina authentication

Retina is considered as one of the most reliable part for biometric authentication as it remains unchanged during the lifetime of every individual. Retinal scan uses infrared light to project the blood vessels in a person's eye. Similar to the fingerprints, the retinal patterns are also unique for all people. (R. Manjula Devi, 2022)

Voice authentication

In this type of authentication, the voice of the user is captured and used to validate the identification. Software is used to break the words into frequency bundles called formants. These formants include the tone of the user and form the voiceprint (Meng, 2020). Voice authentication can be text-dependent or text-independent. The main disadvantage of this method is the voice of the user can easily be recorded and reproduce it get unauthorized access (Hoy, 2018).

Facial Recognition

The different features of the face like eyes, nose, distance between lips and nose, skin texture is being extracted and compared with the image to authorize the user. The face reader captures the projections of the face including the skull bones and saves the accurate information. Facial features are converted into mathematical values and matched with the image. (Dalton Cole, 2021)

Flow diagram of biometric authentication

The below flow diagram describes the process of biometric authentication for face and voice recognition.

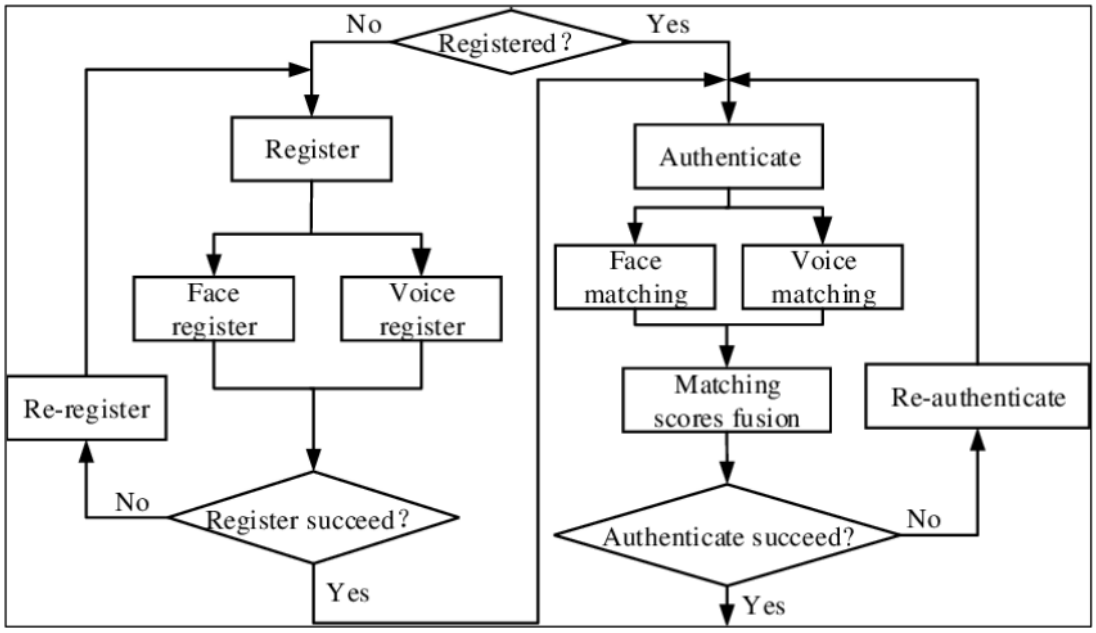

Figure 3 Flow diagram for Biometric Authentication (Xinman Zhang, 2020)

If the user is new to the system, then he must register face and voice into the system. If the registration is not succeeded it will prompt the user to register again.

Once the registration is successful it will store the data and authenticate it. If the saved data and given data are not matching, then the system will ask for re-authentication.

If the values of stored data matches with the user data, then the user is provided the access into the system. The access is denied until the user matches his identity with the saved data.

Applications

Biometric authentication can be implemented in almost all the fields requiring the authentication and avoiding unauthorized access of data. It can be

- In government agencies it can be used for identification of the user before permitting access to work location or highly sensitive areas.
- In airports biometrics can be used to match the person with the digital image of the person's passport.
- In hospitals biometrics can be used to easily track the patient's data separately and avoid medical errors.
- In offices biometric can be used in a combination of access control system and attendances log system ensuring the employees maintains certain time in the offices (Muravskyi, 2021).

Advantages

- The major advantage of biometrics is that the chance of unauthorized access is very less as the hacker cannot hack it from the remote place and must be physically present in order to get the details and there are chances that he might get caught red handed.
- Biometric authentications are easy and secure and are hard to duplicate since it uses unique characters for identification. By using the traditional approaches like password or pin number there are chances that it might be noticed by other person and get easily get hacked which cannot be done in case of biometrics. (Margit Sutrop, n.d.)
- They are a faster way of authentication when compared with traditional methods.
- Biometric authentication requires its input is present upon authorization. We cannot transfer or share a physical biometric digitally – the only way to utilize most biometric authentication systems is with a physical application.
- Unlike other security measures, users cannot forget or loose biometrics and are difficult to be hacked.
- Biometrics add additional protection and ensures greater security. Password authentications are time consuming and can lead to vulnerabilities.

Disadvantages

- There is no option to remotely change the biometric details as done in case of passwords. Also, there is no way to modify the biometric details as they are for lifetime.
- False positives and inaccuracy – False rejects and false accepts can still occur preventing select users from accessing systems in biometric.
- If the server storing the biometric data is hacked, then important information's can get leaked.

- If the scanning device fails or performs in accurately then it can lead to failure of the entire system resulting in unauthorized person accessing the system.
- In Fingerprint based biometric authentication, certain atmospheric properties (humidity, moisture) affect the response time.
- The system involves complex settings and security programs which are very expensive.
- Businesses and governments that collect, and store users' personal data are under constant threat from hackers. Because biometric data is irreplaceable, organizations need to treat sensitive biometric data with increased security and caution – something that's expensive and technically difficult in order to stay ahead of fraud advancements. If a password or pin is compromised, there's always the possibility of changing it. The same can't be said for a person's physiological or behavioral biometrics.
- if some hacker gets your biometric data somehow, then he can use the data on every biometric system forever.

Why Not Wider adoption:

- The biggest concern on using the biometrics is the storage of the biometric information. The data of every individual is stored in the central database and the people having access to this can misuse the data and can fraudulently use this data for other transactions and get access to private information. (Abdulmonam Omar Alaswad, n.d.)
- The overall process of biometric authentication is expensive since it involves complex processes for verifying the unique patterns. If a person loses part of his hand used in authentication, then it is not easy to change as in case of forgotten password. Many people are unaware of modern technologies and can get frauded by copying the finger patterns. Also fingerprints fade away for aged people.

Conclusion

Biometric authentication is one of the best and secure way for authentication purpose. It is an easy way of verification as they are always with us and there is no need to remember or note any of the passwords. Many organizations use biometric devices to monitor the attendance and track the people. Biometrics are difficult to hack unless the hacker personally gets the physical data from the person. Also, biometrics cannot be stolen or misused as it is unique for every individual.

References

Abdulmonam Omar Alaswad, A. H. M., n.d. Vulnerabilities of Biometric Authentication. *International Journal of Information & Computation Technology,* 4(10).

Anil K. Jain, A. R., 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* Issue 14.

Dalton Cole, S. N., 2021. A New Facial Authentication Pitfall and Remedy in Web Services. *IEEE Transactions on Dependable and Secure Computing*.

Din, A., 2021. *What Is Biometric Authentication? A Complete Overview.* [Online]
Available at: https://heimdalsecurity.com/blog/biometric-authentication/

Hoy, M. B., 2018. Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. *Medical Reference Services Quarterly,* Volume 37.

Margit Sutrop, K. L.-M., n.d. Ethical Implications of Second Generation Biometrics. *Review of Policy Research(RPR),* pp. 10-12.

Meng, Z., 2020. Active voice authentication. *Digital Signal Processing.*

Mostafa, M., n.d. A Novel Similarity Measurement for Iris Authentication. *Informatica ,* Volume 37.

Muravskyi, V., 2021. ACCOUNTING OF WAGES WITH THE USE OF BIOMETRICS TO ENSURE CYBERSECURITY OF ENTERPRISES. *Financial and Credit Activity Problems of Theory and Practice.*

R. Manjula Devi, D. K. P., 2022. Retina biometrics for personal authentication. In: *Machine Learning for Biometrics.* s.l.:s.n., pp. 87-103.

Roy, S. P. C. S., 2022. Emerging Trends in Biometric Authentication. *ICRES 2022.*

Xinman Zhang, D. C., 2020. An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice. *IEEE Access.*

binary

ORIGINALITY REPORT

10%	9%	0%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.miteksystems.com Internet Source	5%
2	heimdalsecurity.com Internet Source	1%
3	Submitted to New Zealand School of Education Student Paper	1%
4	Submitted to Rochester Institute of Technology Student Paper	1%
5	Submitted to Danford College Student Paper	1%
6	Submitted to Study Group Australia Student Paper	1%
7	www.coursehero.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off

Exclude bibliography On