Fingerprint Authentication in Biometric Technology

Shreyas Joshi

Fourth Year B.Tech Integrated, Computer Engineering, NMIMS's MPSTME.

---***---

ABSTRACT: This paper mainly focuses on reviewing biometric technology and its types in detail. It also reviews Sensor technology which is the future of fingerprint identification in biometric technology and security. It also discusses about a multifactor authentication model which provides high grade security with the help of fingerprint, voice as well as face recognition all used in a sequence for better identification. The paper also discusses about an analysis of safety that the fingerprint authentication provides with the help of ECC encryption algorithm.

Keywords: Fingerprint authentication, fingerprint identification, two factor authentication, biometric multimodal, biometrics, biometric technology.

1. INTRODUCTION

1.1 Biometric Technology

Biometrics is how a person's unique physical and other characteristics are identified and recorded by an electronic device or system as a medium of confirming identity. The term "biometrics" originates from the word "biometry" which indicates the statistical analysis of biological observations and phenomena. Since biometric identifiers are unique to selves, they are further reliable in confirming identity than token and knowledge-based techniques, such as identity badges and passwords. Biometric identifiers, or modalities, are frequently classified as either "physiological" or "behavioural". Physiological biometric identifiers are associated to a person's physical traits and incorporate fingerprint recognition, hand geometry, odour/scent, iris scans, DNA, palm print, and facial recognition. Behavioural characteristics are associated with the pattern of behaviour of a person and incorporate keystroke dynamics, gait analysis, voice recognition, mouse use characteristics, signature analysis, and cognitive biometrics.

Biometric technologies are operations or applications that intend to employ biometric data acquired from biometric identifiers or modalities. A biometric system is an automated process that:

- Obtains or captures biometric data via a piece of biometric identification equipment, such as an image scanner for fingerprints or palm vein patterns or a camera to collect facial and iris scans,
- Deduces the data from the substantive submitted sample,
- Analyses the scanned data from those captured for reference,
- Resembles the submitted sample with templates, and
- Determines or confirms whether the identity of the biometric data possessor is genuine.
- Biometric technologies, therefore, consist of both hardware and software. Biometric identification equipment is hardware that gathers, reads, and corresponds to biometric data. Biometric data is a specimen obtained from an individual that is unique to the person. Software installed within biometric technologies includes a biometric engine that processes collected biometric data. The software typically works in tandem with the hardware to operate the biometric data capture process, derive the data, and undertake comparison, including data matching.
- Biometric technologies can also be categorized further according to the variety of biometrics used in the system. These technologies are usually utilized to either identify persons and their characteristics against a database, such as criminal records or to validate the identity of persons to impart them access to computing resources, devices, or amenities.

1.2 Fingerprint Authentication

One of the most ancient and widely practiced biometric technology is fingerprint biometrics. The most traditional fields of usages are:

- Passport
- Aadhar Card (India)
- Electronic Locks

Since fingerprints are unique for each person, they are immensely reliable; no two humans have the same fingerprint pattern. One of the most significant advantages of fingerprints is that they cannot be reconstructed, and they can depreciate only after death.

2. BIOMETRIC MULTIMODAL

Biometric modality implies the use of one person's biological attributes of a person such as a face, voice, and fingerprint, and can be distinguished into 2 varieties:

- Behavioural: Identification accomplished by behavioural characteristics such as keystrokes.
- Physiological: Identification achieved by body parts that have unique attributes such as the face, fingerprint, etc.

Nowadays most of the systems utilize only one type of source of erudition for the determination of authentication. These unimodal are suitable for small level protection but for high-class security, we cannot rely on these unimodal as they are vulnerable such as spoofing and noisy data. The multimodal system is very effective and reliable.

- ***First Step***: Fingerprint authentication is succeeded.
- ***Second Step***: Facial authentication will be needed.
- ***Third Step***: After successful fingerprint and face authentication, the last step will be voice authentication.

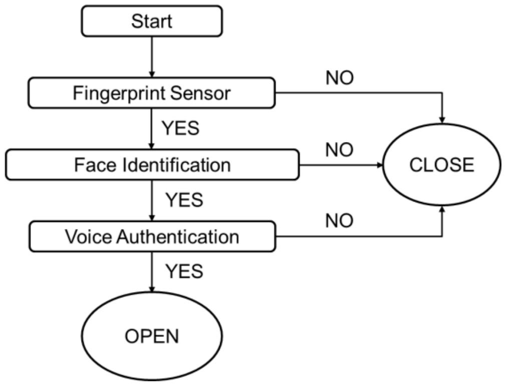

Fig: Biometric authentication multimodal

Only if all the three authentications succeed, we can say that the person is authenticated and he/she will receive the verification. This architecture is more robust, effective, and secure as compared to the two-tier architecture. Since a user goes through three levels of authentication, the possibilities of a wrong person accessing the system are insignificant.

3. FINGERPRINT IDENTIFICATION AND SENSOR TECHNOLOGY

3.1. Fingerprint Identification

At present, fingerprint recognition technology is one of the most mature biological recognition technologies, which is considered as the most stability and uniqueness of the identification technology. The stability can guarantee the long-term effectiveness of user security information. The uniqueness ensures the verification be one to one correspondence between the verifier the stay verifier.

At the same time, fingerprint identification technology has better security, without any burden increase of the system. In addition, the fingerprint acquisition operation is simple, rapid, and fingerprint image processing technology mature. We adopt the compensation algorithm and genetic algorithm as fingerprint matching algorithm. The algorithms not only can identify the fingerprint translation or rotation parameters, but also has strong ability of resisting noise and deformation. So, it realizes the partial fingerprint identification, and then makes the fingerprint identification technology is not entirely dependent on the central regions of the fingerprint, reached the preciseness of fingerprints.

3.2. Sensor Technology

Sensing technology is the most important and basic information access technology, which is wide used in various fields. The proposed scheme tests whether the pulse of the fingerprint extractor in the normal range based on the sensing technology, which to verify whether the fingerprint extractor for living.

4. SAFETY ANALYSIS

The dynamic password and fingerprint sequence of client and server adopt ECC encryption algorithm to decrypt, signature, and verify the signature, which can effectively resist password guessing attack, replay attack, coaxing attacks of identity information, etc.

4.1. Resistance Password Guessing Attacks

Offline and online attacks are two common password guessing attacks. In this scheme, the dynamic password passed between the client and the remote-control centre is encrypted by ECC in the process of identity authentication. Even if an attacker to obtain this information, offline password guessing attacks is invalid because that it unable to get the private key to verify the server password is correct. In order to resist the online password guessing attack by attackers, valves, set up the scheme certification authentication failed more than a certain number of times, the server as illegal users in the online password guessing attacks. So, this scheme can effectively prevent the password guessing attacks.

4.2. Anti-Replay Attacks

Replay attack refers to illegal access of the legitimate users with information used in the past.

This solution can effectively prevent replay attacks.

First of all, this scheme uses dynamic password technology, which makes the user login authentication information are different every time. So, the scheme can effectively prevent the replay attack. Second, this scheme uses random combination of any two fingerprints, where each user input fingerprint sequence is random. This system can bring greater security and effectively prevent the replay attack. Moreover, user authentication uses the fresh value of random Numbers, which makes each time authentication information is different, thus effectively prevent the replay attack.

4.3. Resistance to Coax Attacks

Coaxing attack refers to the pretenders tried to cheat the system counterfeiting legitimate users in the process of transmission through the biological data input port to tamper and steal fingerprint database fingerprint data. First of all, this system uses a trusted third-party personnel identity verification to remote monitoring centre and real fingerprint extraction, thus effectively prevent the pretender fingerprint data input port through the user registration. Second, fingerprint data in the certification database are encrypted with ECC encryption algorithm. In addition to the server, others could not decipher fingerprint characteristic value because that they cannot access to the server for private key. So, the attack for fingerprint database is failure. Moreover, if the attacker impersonating server, the attacker cannot decrypt the message because that it cannot access the private key of the server. Then, the attacker cannot get the new value *k* of user. Therefore, the confirmation message of user authentication server is failure. There are two kinds of circumstances if an attacker impersonates legal identity. The first, an attacker belongs to information intercepted and pretend to be the identity of the attack. The attack is meaningless because that the attacker will fail because of unable to get real fingerprint. Two attackers subdued legitimate users, to extract the real fingerprint of legitimate users, but at the moment of legitimate users due to the state in the excited state, or death, then the system to extract the pulse of the value is not in the normal range, then the system as an exception, will be cut off the user and the server connection, thereby coaxing attacks of the attacker to fail.

5. CONCLUSION

It essentially embraces the various biometric technologies. The paper reviews what biometric technology is, the types of biometric authentications, biometric multimodal, fingerprint identification, sensor technology, and safety analysis.

6. REFERENCES

[1] S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System", International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE, February, 2020.

[2] Manabhanjan Pradhan, Chittaranjan Pradhan. Bhabani Shankar Prasad Mishra, Aditya Kaustav, "Authentication Using 3 Tier Biometric Modalities", International Conference on Communication and Signal Processing (ICCSP), April, 2018.

[3] Qian Xu, Jie Deng, "Identity Authentication System Based on Fingerprint Identification and Pulse Certification", International Conference on Intelligent Networking and Collaborative Systems (INCoS), September, 2016.

[4] Lan Chen, Hai Yang Yin, Tao Wang, He Xu, Mei Song Tong, "An Improved Algorithm for Enhancing Fingerprint Image Quality", Progress in Electromagnetics Research Symposium (PIERS), August, 2018.

[5] Branka Stojanovic, Oge Marques, Aleksandar Neskovic, "A Novel Synthetic Dataset For Research In Overlapped Fingerprint Separation", Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) , December, 2017.