FINGERPRINT AUTHENTICATION ALGORITHM AND METHODS OF ITS IMPROVEMENT

Javlonbek Bahodir ugli Uralov
Graduate student of TATU Urganch Branch named after Muhammad al-Khorazmi
uralovjavlonbek0001@gmail.com

Kamola Erkinovna Saurova
Graduate student of TATU Urganch Branch named after Muhammad al-Khorazmi
kamolaerkinovna@gmil.com

ABSTRACT

The main goal of this article is to study the algorithm of the fingerprint authentication method, which is one of the widely used biometric authentication methods today, and to determine ways to improve it.

Keywords: biometric, authentication, identification, deep learning, verification.

АННОТАЦИЯ

Основной целью данной статьи является изучение алгоритма метода аутентификации по отпечатку пальца, который на сегодняшний день является одним из широко используемых методов биометрической аутентификации, и определение путей его усовершенствования.

Ключевые слова: биометрия, аутентификация, идентификация, глубокое обучение, проверка.

INTRODUCTION

Biometric authentication refers to the use of unique biological characteristics, such as fingerprints, facial recognition, iris patterns, or voice recognition, to authenticate or identify individuals. It is a secure method of authentication because biological characteristics are difficult to replicate or forge, and they are unique to each individual. Biometric authentication is widely used today in various applications, including access control, time and attendance tracking, banking and finance, and law enforcement.

The use of fingerprints as a means of identification can be traced back to ancient Babylon, where fingerprints were used on clay tablets for business transactions. However, it wasn't until the

late 19th century that the scientific study of fingerprints, known as dactylography, was developed.

The credit for the modern use of fingerprints as a means of identification goes to Sir Francis Galton, a British scientist who was interested in using fingerprints for forensic purposes. In 1892, he published a book titled "Fingerprints," which presented a comprehensive study of the subject and proposed a classification system that is still used today. Around the same time, another British scientist named Edward Henry developed a fingerprint classification system that was based on Galton's work but was simpler and more practical. This system, known as the Henry Classification System, became widely adopted by police agencies and is still used in some countries today.

The use of fingerprints in criminal investigations became more widespread in the early 20th century, and by the 1920s, most major police agencies had established fingerprint bureaus. Today, fingerprints remain one of the most important means of identifying individuals in law enforcement, and fingerprint technology has advanced significantly, with the development of digital fingerprint scanners and sophisticated computer algorithms for matching fingerprints. [3]

FINGERPRINT ALGORITHM

The process of matching fingerprints is typically done through an algorithm that analyzes various features of the fingerprint and compares them to a database of known fingerprints. Here is a simplified overview of the algorithm used for fingerprint recognition: [1]

Image acquisition: A digital image of the fingerprint is captured using a scanner or other imaging device.

Pre-processing: The image is cleaned and enhanced to improve the contrast and clarity of the fingerprint ridges and valleys.

Feature extraction: The algorithm identifies specific features of the fingerprint, such as ridge endings, bifurcations, and ridge direction, and generates a set of numerical values that represent these features.

Template creation: The set of numerical values is used to create a unique digital template that represents the fingerprint.

Matching: The template is compared to a database of known fingerprints to find a match. The database may contain hundreds of thousands or even millions of fingerprints.

Verification: If a match is found, the algorithm performs a verification process to confirm that the fingerprint belongs to the

individual in question. This may involve comparing the fingerprint to additional images or using other biometric data, such as facial recognition, to confirm the individual's identity.

Decision: Based on the results of the verification process, the algorithm produces a decision, indicating whether the fingerprint matches a known record and whether the individual's identity has been confirmed.

Fingerprint recognition algorithms are constantly evolving, with researchers working to improve accuracy, speed, and reliability. Some newer algorithms incorporate machine learning techniques to improve performance and adapt to new types of fingerprints and imaging devices.[5]

FINGERPRINT AUTHENTICATION ALGORITHM PROBLEMS

While fingerprint recognition technology is generally considered reliable, there are several problems associated with relying solely on fingerprints for identification. Here are some of the main problems of fingerprint recognition:

False positives: In some cases, the algorithm may match a fingerprint to the wrong individual, resulting in a false positive identification.

False negatives: In other cases, the algorithm may fail to match a fingerprint to the correct individual, resulting in a false negative identification.

Fingerprint alterations: Fingerprint recognition can be affected by changes to the fingerprint due to injury, age, or other factors, which can make it more difficult to accurately identify an individual.

Security vulnerabilities: Fingerprint recognition systems can be vulnerable to hacking or other forms of tampering, which can compromise the security of the system and result in false identifications.

Privacy concerns: The use of fingerprints for identification raises concerns about privacy, as individuals may be reluctant to have their fingerprints collected and stored in a database.[4]

To address these problems, many fingerprint recognition systems now incorporate additional biometric data, such as facial recognition or iris scanning, to reduce the likelihood of false identifications. Additionally, strict security protocols and regular maintenance of fingerprint recognition systems can help ensure accuracy and prevent fraud or hacking attempts. Finally, it is important to carefully consider the privacy implications of using fingerprints for identification and to ensure that appropriate safeguards are in place to protect individuals' privacy.

METHODS OF IMPROVING THE FINGERPRINT AUTHENTICATION ALGORITHM

Improving the algorithm of fingerprint recognition is an ongoing area of research, and there are several approaches that have been proposed to improve accuracy and performance. Here are some ways that the algorithm of fingerprint recognition can be improved:

Using deep learning: Deep learning algorithms have shown promise in improving the accuracy of fingerprint recognition. By training a neural network on a large dataset of fingerprints, the algorithm can learn to identify patterns and features that may be difficult for traditional algorithms to detect.

Incorporating additional biometric data: Combining fingerprint recognition with other biometric data, such as facial recognition or iris scanning, can improve accuracy and reduce the likelihood of false positives or false negatives.

Enhancing image quality: Improving the quality of the fingerprint image can improve the accuracy of the algorithm. This can be done through image enhancement techniques, such as noise reduction or contrast enhancement, or by using high-quality imaging devices.

Dealing with damaged or partial fingerprints: Some individuals may have damaged or partial fingerprints, which can be difficult for the algorithm to match. Newer algorithms are being developed that can handle these types of fingerprints more accurately.

Optimizing parameters: Fine-tuning the parameters of the algorithm, such as the threshold for matching, can improve the accuracy of the algorithm. This can be done through extensive testing and optimization on large datasets of fingerprints.

Overall, improving the algorithm of fingerprint recognition requires a combination of advanced technology, careful analysis, and testing. With ongoing research and development, the accuracy and performance of fingerprint recognition algorithms will continue to improve, making this technology even more reliable and useful in a variety of applications.

CONCLUSION

In conclusion, fingerprint recognition is a powerful biometric technology that is widely used today in various applications, including law enforcement, access control, time and attendance tracking, border control, and banking and finance. Fingerprint recognition

algorithms have evolved significantly in recent years, incorporating machine learning and other advanced techniques to improve accuracy and performance. However, there are still challenges associated with relying solely on fingerprints for identification, such as false positives, false negatives, and privacy concerns. As a result, many systems now use a combination of biometric data to reduce the likelihood of errors and enhance security. With ongoing research and development, fingerprint recognition technology will continue to improve and be an essential tool for many industries in the years to come.

REFERENCES

1. Biometrics Institute: https://www.biometricsinstitute.org/
2. National Institute of Standards and Technology (NIST): https://www.nist.gov/topics/biometrics
3. International Biometrics+Identity Association (IBIA): https://www.ibia.org/
4. IEEE Biometrics Council: https://ieee-biometrics.org/
5. Fingerprint Recognition -An Overview: https://www.sciencedirect.com/topics/computer-science/fingerprint-recognition
6. Nitin Kaushal, Purnima Parashar Kaushal - Human Identification and Fingerprints: A Review, January 2011, Journal of Biometrics & Biostatistics 2(4)