Opinion
Volume 14:2, 2023

Journal of Biometrics & Biostatistics

ISSN: 2155-6180

Open Access

Biometric Encryption: Securing Identity with Unique Biometric Keys

Dutifa Yalam*

Department of Biostatistics, Science and Technology of New York, New York, USA

Introduction

Biometric encryption represents an innovative approach to enhancing the security and privacy of sensitive information. By combining the strengths of biometric data and encryption techniques, biometric encryption offers a robust and unique method of protecting identity-related data. This article explores the concept of biometric encryption, its underlying principles, applications, and the advantages it brings to the field of information security. Biometric encryption involves the integration of biometric data and encryption algorithms to secure sensitive information. Unlike traditional encryption methods that rely on passwords or keys, biometric encryption leverages the unique physiological or behavioural characteristics of individuals as encryption keys. Biometric traits such as fingerprints, iris patterns, or voiceprints are used to generate encryption keys specific to each individual. These keys are then employed to encrypt and decrypt data, ensuring that only authorized individuals with the matching biometric traits can access the protected information [1].

Description

Biometric encryption relies on two fundamental principles: key binding and template protection. Key binding is the process of creating a cryptographic key that is uniquely derived from an individual's biometric data. This key serves as the basis for encryption and decryption operations. Template protection, on the other hand, involves transforming the biometric template into a non-invertible or irreversible form. This ensures that even if the encrypted data or the transformed template is compromised, the original biometric data cannot be derived from it. Biometric encryption offers several significant advantages over traditional encryption methods. Firstly, it eliminates the need for individuals to remember and manage passwords or keys, reducing the risk of unauthorized access due to weak or compromised credentials. Biometric traits, being inherent to individuals, cannot be easily forgotten or misplaced. Additionally, biometric encryption provides a higher level of security as biometric data is unique and difficult to replicate. Even if an attacker gains access to the encrypted data, they would still require the corresponding biometric key to decrypt it. This adds an additional layer of protection against unauthorized access and strengthens data security. Moreover, biometric encryption offers greater convenience and user experience. Users can seamlessly authenticate themselves using their biometric traits, eliminating the need for complex authentication processes. Biometric traits are more user-friendly and natural, improving the overall usability and acceptance of security systems [2,3].

Biometric encryption has diverse applications across various sectors. It is particularly valuable in protecting sensitive data in areas such as financial transactions, healthcare records, personal identification, and access control systems. For example, in financial transactions, biometric encryption enhances the security of digital payments by encrypting transaction data with the user's biometric key, ensuring that only the authorized individual can access and decrypt the data. In healthcare, biometric encryption helps safeguard patient records, ensuring privacy and preventing unauthorized access to sensitive medical information. Biometric encryption can also be employed in access control systems, securing physical and digital environments by allowing only authorized individuals with matching biometric keys to gain entry [4,5].

Conclusion

Biometric encryption offers promising advantages; there are challenges and considerations to address. Ensuring the protection and privacy of biometric data is of utmost importance, requiring robust security measures for its storage, transmission, and usage. Additionally, careful attention must be given to issues such as system accuracy, scalability, and interoperability to ensure seamless integration and user acceptance. Biometric encryption represents a powerful approach to securing identity-related data. By combining the strengths of biometric traits and encryption algorithms, it offers enhanced security, convenience, and privacy protection. Biometric encryption eliminates the need for passwords and provides a more reliable and user-friendly authentication method. Its applications in financial transactions, healthcare, personal identification, and access control systems showcase its potential to strengthen data security in various sectors. By addressing challenges, ensuring privacy protection, and fostering responsible use, biometric encryption can play a significant role in enhancing the security landscape and protecting individuals' identities in the digital age.

Acknowledgement

We thank the anonymous reviewers for their constructive criticisms of the manuscript. The support from ROMA (Research Optimization and recovery in the Manufacturing industry), of the Research Council of Norway is highly appreciated by the authors.

Conflict of Interest

The authors declare that there was no conflict of interest in the present study.

References

1. Khalil-Hani, Mohamed, Muhammad N. Marsono and Rabia Bakhteri. "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm." *FGCS* 29 (2013): 800-810.

2. Moi, Sim Hiew, Nazeema Binti Abdul Rahim, Puteh Saad and Pang Li Sim, et al. "Iris biometric cryptography for identity document." *IEEE* (2009):736-741.

3. Cavoukian, Ann and Alex Stoianov. "Biometric encryption." *Biom* 15 (2007): 11.

4. Moradi, Masoud, Masoud Moradkhani and Mohammad Bagher Tavakoli. "A real-time biometric encryption scheme based on fuzzy logic for IoT." *J Sens* 2022 (2022).

5. Gobi, M. and D. Kannan. "A secured public key cryptosystem for biometric encryption." *IJCSNS* 15 (2015): 49.

Address for Correspondence: *Dutifa Yalam, Department of Biostatistics, Science and Technology of New York, New York, USA, E-mail: yalam93@edu.in*

Received: 27 March, 2023, Manuscript No. jbmbs-23-101640; **Editor assigned**: 29 March, 2023, Pre QC No. P-101640; **Reviewed:** 12 April, 2023, QC No. Q-101640; **Revised:** 17 April, 2023, Manuscript No. R-101640; **Published:** 25 April, 2023, DOI: 10.37421/2155-6180.2023.14.159

How to cite this article: Yalam, Dutifa. “Biometric Encryption: Securing Identity with Unique Biometric Keys.” *J Biom Biosta* 14 (2023): 159.