Multi-modal Biometrics' Template Preservation and Individual Identification

| Conference paper | First Online: 04 October 2023

| pp 805–820 | Cite this conference paper

Inventive Communication and Computational Technologies

(ICICCT 2023)

B. Nithya & P. Sripriya

Part of the book series: Lecture Notes in Networks and Systems ((LNNS,volume 757))

Included in the following conference series:
International Conference on Information, Communication and Computing Technology

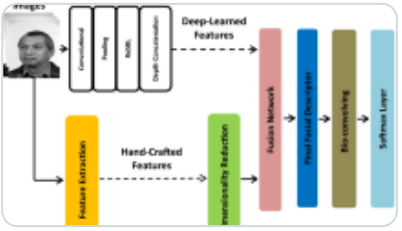
Abstract

We introduce a system that provides multi-modal template security in response to the rising vulnerability to biometric templates. The proposed work aims to provide a multi-modal biometric identification system with protected templates that do not degrade overall recognition performance. The presented shielded technique was compared against an unprotected multi-modal biometric recognition system to prove the above metric. Many criteria are used to determine the success of the recommended system, including training time, testing time, Equal Error Rate (EER), accuracy, and classifier performance. Unique characteristics are acquired using Speeded-up Robust Features (SURFs) and Histogram of Oriented Gradients (HoG) from three biometric modalities (fingerprint, face, and signature). With the aid of the bio-secure template security method, the extracted characteristics have been fused, and templates have been turned into new templates. The generated template can be altered by simply adjusting the seed's random matrix. A virtual database is developed to evaluate the recommended approach. The hybrid feature extraction method is also assessed in addition to the performance of the single feature extraction strategy. Finally, the classifier and deep neural network are trained to predict the provided individual. The findings reveal that the protected approach improves the system's overall recognition performance, and the EER value remains lower at different feature counts. The acquired highest accuracy is 96%, and the lowest EER is 0.07% on the 20 vital hybrid feature points.

Similar content being viewed by others

Biometric Template Protection Using Deep Learning

Chapter | © 2021



Fusion of deep-learned and hand-crafted features for cancelable recognition systems

Article | 13 April 2020

Fingerprint and Face-Based Secure Biometric Authentication System Using Optimized Robus...

Chapter | © 2021

References

1. Sanjekar P, Patil J (2013) An overview of multi-modal biometrics. Signal Image Process: Int J (SIPIJ) 4(1):57–64. https://doi.org/10.5121/sipij.2013.4105

Article Google Scholar

2. Jain AK, Ross AA, Nandakumar K (2011) Introduction to biometrics. Springer, New York, Dordrecht, Heidelberg, London

Google Scholar

3. Jain AK, Flynn P, Ross AA (2008) Book: handbook of biometrics. Springer, New York

Book Google Scholar

4. Argyropoulos S, Tzovaras D, Ioannidis D, Damousis Y, Strintzis M, Braun M, Boverie S, Biometric template protection in multi-modal authentication systems based on error-correcting codes. J Comput Secur 18:161–185. https://doi.org/10.3233/JCS-2010-0369

5. Teoh ABJ, Goh A, Ngo DCL (2006) Random multispace quantization as an analytic mechanism for bio-secure of biometric and random ıdentity ınputs. IEEE Trans Pattern Anal Mach Intell 28(12):1892–1901

Google Scholar

6. Dwivedi R, Dey S (2016) A non-ınvertible cancelable fingerprint template generation based on ridge feature transformation. IEEE 4:1–16

Google Scholar

7. Rathgeb C, Uhl A (2013) A survey on biometric cryptosystems and cancelable biometrics. Eurasip J Inf Secur 3

Google Scholar

8. Sudhi GK, Dharan S, Manjusha Nair S (2021) Review paper on biometric template security. Int J Eng Res Technol (IJERT) 10(06)

Google Scholar

9. Belguechi R, Cherrier E, Rosenberger C (2012) Texture based fingerprint bio-secure: attacks and robustness. İn: 2012 5th IAPR International conference on biometrics (ICB), pp 196–201. https://doi.org/10.1109/Icb.2012.6199808

10. Fatima B, Reda A (2018) Secured multi-modal biometric system. J Multim Process Technol, pp 77–87. https://doi.org/10.6025/Jmpt/2018/9/3/77-87

11. Teoh A, Goh A, Ngo D (2007) Random multispace quantization as an analytic mechanism for bio-secure of biometric and random ıdentity ınputs. IEEE Trans Pattern Anal Mach Intell, pp 1892–901. https://doi.org/10.1109/Tpami.2006.250

12. Topcu B, Karabat C, Azadmanesh M, Erdogan H (2016) Practical security and privacy attacks against biometric hashing using sparse recovery, Eurasip J Adv Signal Process

Google Scholar

13. Talreja V, Valenti M, Nasrabadi NM (2021) Deep hashing for secure multi-modal biometrics. IEEE Trans Inf Forensics Secur 16:1306–1321. https://doi.org/10.1109/Tifs.2020.3033189

14. Sardar A, Umer S, Pero C, Nappi M (2020) A novel cancelable facehashing technique based on non-ınvertible transformation with encryption and decryption template. IEEE Access. https://doi.org/10.1109/Access.2020.2999656

15. Baghel V, Ali S, Prakash S (2021) A non-ınvertible transformation based technique to protect a fingerprint template. IET Image Process. https://doi.org/10.1049/Ipr2.12130

16. Jacob IJ, Betty P, Darney PE et al (2021) Biometric template security using DNA Codec based transformation. Multimed Tools Appl 80:7547–7566. https://doi.org/10.1007/s11042-020-10127-w

Article Google Scholar

17. Bay H, Ess A, Tuytelaars T, Van Gool L (2008) Surf: speeded up robust features. Comput Vis Image Underst (CVIU), pp 346–359

Google Scholar

Funding

This research did not receive any specific grant from funding agencies in public, commercial, or not-for-profit sectors.

Author information

Authors and Affiliations

Department of Computer Science, New Prince Shri Bhavani Arts and Science College, Medavakkam, Chennai, Tamil Nadu, India
B. Nithya

Department of Computer Applications, VISTAS, Chennai, Tamil Nadu, India
P. Sripriya

Corresponding author

Correspondence to B. Nithya .

Editor information

Editors and Affiliations

Department of Electronics and Communication Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India
G. Ranganathan

Department of Computer Science (HUMAIN-Lab), International Hellenic University, Thessaloniki, Greece
George A. Papakostas

Information Systems and Operations Management (ISEG), University of Lisbon, Lisboa, Portugal
Álvaro Rocha

Ethics declarations

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Rights and permissions

Copyright information

About this paper

Cite this paper

Nithya, B., Sripriya, P. (2023). Multi-modal Biometrics' Template Preservation and Individual Identification. In: Ranganathan, G., Papakostas, G.A., Rocha, Á. (eds) Inventive Communication and Computational Technologies. ICICCT 2023. Lecture Notes in Networks and Systems, vol 757. Springer, Singapore. https://doi.org/10.1007/978-981-99-5166-6_54

.RIS .ENW .BIB

DOI
https://doi.org/10.1007/978-981-99-5166-6_54

Published
04 October 2023

Publisher Name
Springer, Singapore

Print ISBN
978-981-99-5165-9

Online ISBN
978-981-99-5166-6

eBook Packages
Intelligent Technologies and Robotics
Intelligent Technologies and Robotics (R0)

Publish with us

Policies and ethics