Mini Review
Volume 13:9, 2022

Journal of Biometrics & Biostatistics

ISSN: 2155-6180

Open Access

Steganography-Based Biometric Authentication System for the Cloud Computing Environment

Mikei Lorei*

Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh

Abstract

Starting from the primary randomized control preliminary of aortic valve substitution by a trans catheter approach is the field of interventional cardiology has seen a transformation in negligibly obtrusive cardiovascular consideration. Thorough examinations have validated its utilization in an undeniably more extensive exhibit of patients, and the U.S. Food and Medication Organization as of late supported the primary huge imminent randomized preliminary of trans catheter aortic valve substitution (TAVR) in okay patients. It is turning out to be increasingly more vital to foresee, deduced, which patients will benefit with which TAVR systems, and imaging is best situated to make this possible. Two-layered and 3-layered echocardiography and cardiovascular registered tomography angiography (CTA) have become fundamental symptomatic parts in the assessment of patients, who might be possibility for TAVR, during the TAVR methodology itself, and for trail behind TAVR,

Keywords: Steganography • Authentication • PPS-BAS

Introduction

Cloud computing (CC) has recently piqued the interest of both businesses and individuals. Security and privacy are regarded as the primary problem with CC, despite the substantial advantages it offers. Due to its stable and high recognition rate, biometric authentication has attracted the attention of numerous researchers. It is frequently used for authentication purposes. The fingerprint is considered to be one of the best biometric authentication models for achieving privacy and security. In addition, image steganographic techniques are utilized to enhance biometric data security. The data embedding that is typically carried out by the most advanced biometric data hiding methods typically takes place in a region that does not include important biometric features [1-3].

Literature Review

With this inspiration, this paper presents a protection safeguarding steganography based biometric validation framework (PPS-BAS) for cloud conditions. The PPS-BAS model's objective is to transmit the encrypted fingerprint image to the cloud within the eye retina image, which serves as the cover image. The cover image is split using the multilevel discrete wavelet transform (DWT) method in the proposed PPS-BAS model to locate the pixel. In addition, the continuous pigeon inspired optimizer (CPIO) algorithm is used to select the cover image's ideal pixel points. A Q-learning method is used to simultaneously extract the tiniest details from the fingerprint image and conceal them in the cover image's optimal pixel locations. The stego image is encrypted using the double-logistic chaotic map (DLCM) model before being sent to the cloud server for further protection. The Scaled Conjugate Gradient (SCG) based back propagation neural network (BPNN) model is used for the biometric recognition process following the reconstruction of the original fingerprint image (the secret image).The proposed PPS-BAS model's improved outcomes are highlighted in a comprehensive simulation analysis, and the comparative results analysis ensured that the PPS-BAS model outperformed the most up-to-date biometric authentication systems. Due to its inherent advantages, biometrics-based detection systems have recently received a lot of attention. It effectively provides cloud users with privacy protection and data security on the cloud server. As a result, the current development focuses on addressing cloud data integrity, growth management, and user privacy issues. This method plays a significant role in the CC's data management, preserving users' privacy and processing data with integrity. Biometric data security and privacy have been improved through the development of effective and cutting-edge techniques over the past few decades. In addition, biometrics based recognition frameworks were likewise extraordinarily examined, which give client confirmation by verifying the individual. One method of consistent and common access control is biometric authentication, which is becoming a standard feature in smartphones. For the purpose of matching subsequent biometric templates, this application necessitates the safe storage of biometric features in digital databases. As a result, secure storage of this sensitive data necessitates the use of efficient encryption. Steganography is used to make the biometric validation scheme more private when it transmits encrypted data. These measures could be embedded biometric data in carrier objects, like facial images, whether or not the user authentication is involved. Along with other personal information, biometric data has the potential to be used by cybercriminals for identity theft, and its value makes it a commodity that is exported in underground markets like the dark web. There is a hidden network of websites on the dark web that can be accessed by a particular browser and provide an anonymizing feature to assist in obfuscating client recognition.

Permitting several organizations like government and bank agencies, access to biometric templates presented by a central and trusted entity would be beneficial in several features. Initially, it permits organizations that presently have no direct access to a freely available database. Next, this organization doesn't want to invest in the framework needed for enrolling novel users and stores raw biometric databases of their personal. It will decrease the threat of significant data breaches. Lastly, a client should register one time with the confidential entity for accessing services given by several organizations. Singapore's SingPass face authentication and India's Aadhaar project are the 2 current instances, whereas the organization subscribes to the national biometric database for enabling verification service to their user. Biometric access control system provides a security layer nearby safe resources. Steganography techniques employed to the biometric data provide distinct

***Address for Correspondence:** Mikei Lorei, Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh, E-mail: lorie453@edu.in*

Date of Submission: 05 September, 2022, Manuscript No. jbmbs-22-81528; **Editor assigned:** 06 September, 2022, PreQC No. P-81528; **Reviewed:** 18 September, 2022, QC No. Q-81528; **Revised:** 22 September, 2022, Manuscript No. R-81528; **Published:** 29 September, 2022, DOI: 10.37421/2155-6180.2022.13.128

and separate security layers. It has the benefits of combining biometrics with steganography like augmenting the security of sensitive biometric data in transmission, and acceptance in real time application must be continued [4].

Steganography based biometric authentication system

This paper presents privacy preserving steganography based biometric authentication system (PPS-BAS) for cloud environment to hide the fingerprints image (secret image) into the eye retina image (cover image). The proposed PPS-BAS model involves multilevel discrete wavelet transform (DWT) technique with continuous pigeon inspired optimizer (CPIO) algorithm for the identification and optimal pixel point selection in the cover image. Besides, a Q-learning technique is employed for the minutiae extraction from the fingerprint image and is then hidden into the optimal pixel locations in the cover image. Moreover, the double-logistic chaotic map (DLCM) model is utilized for encryption process. At last, the reconstruction of the original fingerprint image (secret image) takes place followed by Scaled Conjugate Gradient (SCG) based back propagation neural network (BPNN) model for biometric recognition. For examining the betterment of the proposed PPS-BAS model, a series of simulations take place on benchmark test images and investigated the outcomes in terms of different measures. This section surveys the existing biometric based authentication systems developed to achieve security [5].

Conclusion

A cancellable biometric architecture depending upon deep learning (DL) method on the cloud. They determine that cloud is a better resolution for biometric system whereas quick response times, intensive computation, and higher accurateness is needed. In Banerjee et al, a novel security method was determined by creating the scheme more secure using steganography together with biometric security.

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. He, Jiang and Paul K. Whelton. "Elevated systolic blood pressure and risk of cardiovascular and renal disease: Overview of evidence from observational epidemiologic studies and randomized controlled trial." *Am Heart J* 138 (1999): (3 Pt 2):211–219.
2. Shaw, Caroline, Tony Blakely, Peter Crampton and June Atkinson. "The contribution of causes of death to socioeconomic inequalities in child mortality: New Zealand 1981-1999." *N Z Medi J* 118 (2005).
3. Deng, Hongtao. "Real-Time monitoring of Athletes' training data based on wireless sensors." *Microprocess Microsyst.* 81 (2021): 103697.
4. Halunen, Kimmo, Juha Häikiö and Visa Vallivaara. "Evaluation of user authentication methods in the gadget-free world" *Pervasive Mob Comput* 40 (2017) 220-241.
5. Quentin, Wilm, Olayinka Abosede, Joseph Aka and Patricia Akweongo, et al. "Inequalities in child mortality in ten major African cities." *BMC Med* 12 (2014): 1-12.

How to cite this article: Lorei, Mikei. "Steganography-Based Biometric Authentication System for the Cloud Computing Environment." J Biom Biosta 13 (2022): 128.