Abstract of the Thesis

Name: Ayeshabanu Sibgatulla Shaikh

Enrollment No.: 179999913028

Faculty: Engineering

Discipline/Branch: Computer/IT Engineering

Title of the Thesis: Privacy Preserving Fingerprint Authentication Based on Cancelable Biometrics

Abstract

The IT security paradigm has evolved from secret-based to biometric identity-based. Biometric identification has become gradually more popular in recent years for handheld devices. Privacy preservation is a key concern when biometrics are used in authentication systems in the present world. Nowadays, the declaration of biometric traits has been imposed not only by the government but by many private entities as well. There are no proper mechanisms or assurances that biometric traits will be protected by these entities. The encryption of biometric traits to avoid privacy attacks is a giant problem. Biometric authentication systems have become more popular nowadays because of mobile and other handheld devices since they eliminate the need for a password or pin to remember. The usage of the internet and other handheld smart devices promotes the theft of users' biometric traits, which frequently results in a loss of privacy. If an intruder hacks biometric traits, there is no way to change the biometric traits of any person because they are permanently attached to them. The biometric traits are not replaceable like passwords; hence, the key research area is privacy preservation. To stop such biometric traits from being stolen or used improperly, secure technology solutions must be developed. Protecting biometric template data is essential for preventing the loss of user privacy and identification. An effective and efficient approach that focuses on the security and privacy issues of biometric traits is required. The prime threat associated with biometric authentication is identity theft. Any attack that recovers the biometric template may have a serious impact since users cannot change their biometric traits. Hence, biometric templates must be protected to thwart any leakage, as biometric traits are extremely susceptible to change. In privacy-preserving biometric authentication systems, the biometric data is stored in a secure form, which transforms the data into a distorted version and matches the trait in the transformed domain at the time of recognition.

The study investigates the fundamental and applied problem of security and privacy of biometric traits. There is a need for secure and non-invertible privacy-preserving biometric authentication systems to address the limitations by developing novel methods of cancelable biometrics using discrete cosine transformation and index of max hashing for securing biometric traits. In the proposed method, index of maximum hashing offers robust concealment of biometric traits, thereby strengthening the non-invertibility guarantee and enhancing overall template security. In this study, we present a cancelable template generation approach based on index of max hashing, the fast fourier transform, the hadamard product, and speeded-up robust features-based feature extraction. Both theoretical analysis and empirical evidence demonstrate that index of maximum hashing effectively preserves accuracy by maintaining rank correlation properties. The proposed method also satisfies non-invertibility requirements for template protection. Furthermore, with appropriately calibrated parameters, it exhibits strong resistance to several prevalent security and privacy attacks.

In recent years, deep learning algorithms have emerged as some of the most successful artificial intelligence approaches for feature extraction tasks. Among various deep learning methods, convolutional autoencoders have been adopted and have demonstrated substantial performance in the biometric domain. This research proposes methods for non-invertible cancelable biometrics based on convolutional autoencoder to secure biometric traits and address the problem of privacy preservation. All the proposed techniques have been carefully thought out and tested on FVC2002 datasets. The hyperparameters of the models are tuned and thoroughly tested. The outcomes of the suggested procedures are compared with those of the other traditional techniques.

This research contributes to the biometric research community by providing effective mechanisms to address privacy and security challenges associated with biometric traits. By introducing robust non-invertible and cancelable template protection techniques, the proposed approach enhances resistance to unauthorized reconstruction and misuse of biometric data, thereby supporting the development of secure and privacy-preserving biometric systems.

List of Publications:

1) Ayesha S. Shaikh, Dr. Vibha D. Patel, Significance of the Transition to Biometric Template Protection: Explore the Future", International Journal of Image and Graphics, Vol. 21, No. 2, 2021

2) Ayesha S. Shaikh, Dr. Vibha D. Patel, Fingerprint Template Protection: Cancelable Biometrics", International Journal of Computational Vision and Robotic, Vol. 16, No. 4, 2026

3) Ayesha S. Shaikh, Dr. Vibha D. Patel, Privacy Preserving Fingerprint Authentication Based on Cancelable Biometrics", Multimedia Tools and Applications, Springer, Vol. 85, No. 457, 2026