**“Cancelable Fingerprint Template Protection Scheme Based on LTTS Security and Randomly Relocate Bloom Filter”**

Md Sabuj Khan

**Abstract:**

**Key Words:**

**1. Introduction:**

**1.1 Related Work**

**1.2 Motivation and Contributions**

**2. Preliminaries**

**2.1 Locality Sensitive Hashing**

**2.2 Bloom Filter**

**3. Methodology**

**3.1 Fixed Length Binary Vector**

**3.2 Random Security Matrix**

**3.3 Bloom Filter**

**3.4 Matching of the Bloom Filter**

**4.Experiments**

**4.1 Performance of EER**

**4.2 Same Key and Different Key Performance**

**4.3 Time Efficient and Complexity**

**5.1 Privacy & Security Analysis**

**5.1.1 Irreversibility Analysis**

**5.1.2 Revocability Analysis**

**5.1.3 Likability Analysis**

**5.2 Security Analysis**

**5.2.1 Brute Force Attack Discussion**

**5.2.2 False Accept Attack Discussion**

**5.2.3 Birthday Attack Analysis**

**6.Conclusions**

**Abstract:**

**Key Words:** Cancelable Biometric, Fingerprint Template Protection, LTSS, Random Security, Bloom Filter

1. **Introduction**

Fingerprint recognition is one of the most widely used biometric technologies in various applications, including access control, forensics, and financial transactions. However. The widespread use of fingerprint recognition system has raised serious concerns about the security and privacy of individuals, particularly with respect to the protect their biometric data. Fingerprint Template, which represent the unique characteristic of an individual’s fingerprint , are vulnerable to attack that can compromise the security of the entire system. In ordered to safeguard security and privacy, biometric vendors typically store biometric templates which are representations of the original raw biometric data (such as a fingerprint image), rather than storing the raw biometric data itself within their system [1].

Cancelable biometric is a promising approach to addressing these security and privacy concerns. It involves transforming the original biometric data into a new representation that is unlinkable to the original data, and can be canceled or regenerated if the original data is compromised. During the enrollment phase, it is common for biometric data to be stored in its raw, unsecure from the database server [2]. Cancelable fingerprint template protection is a specific area of research within the field if cancelable biometrics that’s aims to protect fingerprint template being misused by an attacker. Biometric system requires security measures to prevent cross-matching and maintain interoperability between applications, for example if a biometric trait, such as a fingerprint in a social media photo, is copied or spoofed, it can compromise the security level of all applications that rely on the trait [3]. Cancelable biometrics has been proposed as a solution to this problem. Cancelable biometric refers to the process of transforming the biometric template a new, unique template that is no longer recognizable as the original. This scheme can provide better security and privacy protection for biometric template, as the transformed template can not be revers-engineered to recover the original biometric data. Our paper aims to provide a comprehensive proposed of the state-of-the-art- techniques in cancelable in fingerprint template protection, as well as their strengths and limitations. The cancelable fingerprint template protection satisfies the following criteria [4]:

Irreversibility: Obtaining the original biometric template from an individual’s protected biometric template should be computationally challenging.

Revocability: If the feature template is compromised, it is possible to generate a new instance of the cancelable template from the original features.

Unlikability: It should be challenging to determine computationally whether multiple instances of a protected biometric template were obtained from the same biometric trait of a user.

Performance: The effectiveness of the template protection technique should not be compromised in the terms of its performance.

The rest of the paper is organized as follows: Section 2 provides a brief overview of related work is cancelable biometrics. Section 3 presents the proposed cancelable fingerprint template protection scheme. Section 4 present the experimental results and analysis. Finally, Section 5 concludes of the paper.

Reference:

1. [Mai, Guangcan, et al. "Secureface: Face template protection." IEEE Transactions on Information Forensics and security 16 (2020): 262-277.](https://scholar.google.com/scholar?hl=fr&as_sdt=0%2C5&as_ylo=2019&q=SecureFace%3A+Face+Template+Protection&btnG=#d=gs_cit&t=1674872791135&u=%2Fscholar%3Fq%3Dinfo%3AFlKoLUX2mYEJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Dfr)
2. Bansal, V., & Garg, S. (2022). A cancelable biometric identification scheme based on bloom filter and format-preserving encryption. Journal of King Saud University-Computer and Information Sciences
3. [Bernal-Romero, Juan Carlos, et al. "A review on protection and cancelable techniques in biometric systems." *IEEE Access* (2023).](https://scholar.google.com/scholar?hl=fr&as_sdt=0%2C5&as_ylo=2019&q=A+review+on+protection+and+cancelable+techniques+in+biometric+systems&btnG=#d=gs_cit&t=1674726553589&u=%2Fscholar%3Fq%3Dinfo%3AD7cyLSQE7DEJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Dfr)
4. Nandakumar K, Jain AK (2015) Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process Mag 32(5):88–100