Biometric Cryptosystems: A New Biometric Key Binding for Fingerprint Minutiae-Based Representation

> Shivam Verma (2020CS50442)

1. Description of the Problem

Biometric cryptosystems aim to securely generate, store, or release cryptographic keys using an individual's biometric data, such as fingerprints. However, integrating biometrics with cryptography presents several challenges:

1. **Intra-User Variability:** Biometric data (e.g., fingerprints) can vary across captures due to factors like sensor noise, finger placement, or environmental conditions. This variability makes it difficult to directly generate consistent cryptographic keys from biometric data.

2. **Template Protection:** Unlike passwords or PINs, biometric templates cannot be replaced if compromised. If a stored template is stolen, it poses a permanent security risk. Hence, protecting biometric templates is critical to prevent misuse.

3. **Security-Performance Tradeoff:** Existing methods, such as Fuzzy Commitment and Error-Correcting Codes (ECC), face a tradeoff between security and performance. Larger key sizes can reduce the key release rate, while simpler schemes may be vulnerable to attacks.

4. **Vulnerability to Attacks:** Traditional key-binding schemes, like Fuzzy Commitment, are theoretically sound but have been shown to be susceptible to specific attacks, such as brute-force or correlation attacks.

5. **Computational Overhead:** Minutiae-based fingerprint representations, particularly fixed-length templates, involve high computational costs due to exhaustive calculations for feature extraction (e.g., histograms of triangular features).

These challenges highlight the need for a robust and efficient biometric key-binding scheme that ensures template security, accommodates biometric variability, and maintains high performance without relying on ECC.

2. Methodologies to Solve the Problem

The proposed solution addresses the above challenges by combining cancellable biometrics with an ECC-free key-binding scheme, inspired by the chaffing and winnowing technique. The methodology is divided into two phases:

A) Key Binding Phase

Input: A binary cryptographic key k is provided as input.

Template Encoding:

- For each bit 1 in k, the system encodes the bit using the true biometric template (derived from the user's fingerprint).
- For each bit 0, the system encodes the bit using a synthetic template (e.g., generated from impostor data or other biometric modalities).

Cancellable Transforms:

- Both true and synthetic templates undergo cancellable transformations to ensure irreversibility.
- The transform involves a permutation process and Graph-based Hamming Embedding (GHE) to secure the minutiae representation.
- Each template uses a different transformation seed, enhancing security against reverse engineering.

B) Key Release Phase

Query Processing: During authentication, the user presents a new fingerprint sample.

Cancellable Query Instances: The system applies m cancellable transforms (where m is the key size) to the query data, generating m transformed query instances.

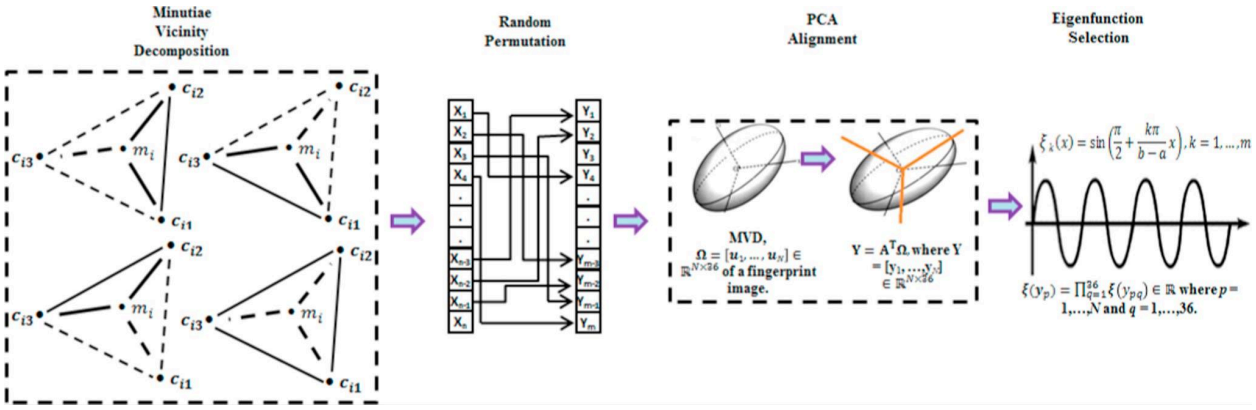
Matching: Each transformed query instance is matched against the stored cancellable templates.

Decision Rule:

- If the matching score for a template exceeds a predefined threshold, the system releases a bit 1.
- Otherwise, it releases a bit 0.
- The original key k is reconstructed if the majority of bits match the enrolled key.

3. Cancellable Transform Used

The proposed cancellable transform protects fingerprint templates through a two-step irreversible process. First, it applies **random permutation** to shuffle rows of the **Minutiae Vicinity Decomposition (MVD)** matrix, ensuring template uniqueness. Next, it employs **Graph-based Hamming Embedding (GHE)**, a non-invertible mapping that converts permuted features into binary codes while preserving geometric relationships. The transform uses eigenfunctions of a weighted Laplacian operator to generate discriminative binary representations. Crucially, even with knowledge of the transformed template and parameters, recovering original minutiae remains computationally infeasible. The scheme supports **cancellability** – compromised templates can be reissued by changing permutation seeds. Unlike error-correction-dependent methods, it accommodates **variable-length biometric features** and works with advanced matchers. Experimental validation on FVC datasets confirms its accuracy matches state-of-the-art systems while resisting privacy attacks like **ARM** and **SKI**.



4. Advantages of the Proposed Scheme

1. **ECC-Free Design:** Eliminates the need for error-correcting codes, resolving the security-performance tradeoff.

2. **Cancellability:** The use of irreversible transforms ensures template protection. Even if the database is compromised, the original biometric data cannot be recovered.

3. **Synthetic Templates:** The inclusion of synthetic templates (e.g., impostor data) confuses attackers, mimicking the chaffing-and-winnowing approach.

4. **Scalability:** The scheme maintains stable accuracy even with larger key sizes, unlike traditional Fuzzy Commitment.

5. Comparison with Fuzzy Commitment

Feature	Fuzzy Commitment	Proposed Scheme
Reliance on ECC	Yes	No
Template Protection	Limited	Strong (Cancellable)
Key Size Flexibility	Low	High
Attack Resistance	Vulnerable	Enhanced

The proposed methodology effectively addresses the limitations of existing systems by leveraging cancellable biometrics and synthetic noise, ensuring both security and usability.

6. Conclusion

The report outlined the challenges in biometric cryptosystems, particularly key binding for fingerprint minutiae, and presented a novel ECC-free scheme combining cancellable transforms and synthetic templates. This approach mitigates security risks, improves performance, and ensures template revocability, making it a promising solution for secure biometric-key integration.

The slides used during the presentation of the paper in the **SIL775** course can be accessed at this link.