Honours Project
(CSI 4900)

Cancelable Biometrics: Analysis and Implementation of a Fingerprint Template Transformation Method

By

Arman Kompany Zare

Project Supervisor: Dr. Carlisle Adams

Faculty of Engineering

School of Electrical Engineering and Computer Science (EECS)

University of Ottawa

Fall 2023

Abstract

In this report, we analyze, implement, and verify a specific cancelable biometric method from a 2018 research paper (Yang, Hu, Wang, & Wu, 2018), which is used for transforming fingerprint templates. Our implementation of this method has been solely developed on Python over the course of three months with the help of some open source python libraries. The implementation closely follows the given algorithms on the paper and bears certain advantages in comparison such as improved runtime performance using GPU utilization (powered by NVIDIA CUDA), and all tools involved being fully open source and free to use. The verification of the paper's results was done by running the implementation on the same FVC fingerprint datasets used on the paper and other datasets, using the same parameter configurations as indicated in their different test cases. Similar outcomes to those on the paper were achieved as a result, which further proved the security and accuracy of this method for fingerprint matching.

Keywords:
Fingerprint, Cancelable Biometrics

Implementation Software and Tools:
Python 3, Anaconda, Numba, TensorFlow, Nvidia CUDA

Acknowledgement

First and foremost, I would like to thank Professor Carlisle Adams for suggesting this particular research subject, and his continued support and supervision on it. I also appreciate Professor Wencheng Yang, and the other authors of the 2018 paper, for responding to my inquiries regarding their work with helpful explanations and answers. Full credits and acknowledgement goes to the developers and maintainers of the Python libraries used within this project.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In today's world, biometrics play a greater role than ever in preserving our digital security and privacy. Some of the reasons that most people and organizations choose biometrics over static or variable string-based passwords are: Uniqueness, Convenience, and Complexity. However, there is one specific weakness involved with biometric methods, which will be discussed further ahead (under Section 1.2). There exist numerous methods for resolving this weakness which generally fall under the term: Cancelable Biometrics. In this report a specific method (Yang et al., 2018) which is used for fingerprint biometric data, will be discussed and analyzed, along with a documentation on its implementation, yielded results and performance comparison.

1.1 Advantages of Biometric Data

The Uniqueness advantage comes from the fact that when it comes to biometrics, especially fingerprints, almost no two individuals possess the same biometric information. So there are no overlaps in case of comparisons. On the other hand, there is a slim chance that two people in the world would coincidentally share the same static password for their applications or accounts, which would lead to security issues if one of their passwords gets compromised.

Regarding Convenience, it is obvious that biometric information do not necessarily need to be remembered by a person, and are perfectly portable since they are literal parts of that person's own body. On the other hand, complex passwords may be difficult to remember and

misinputs could occur while entering them in. Even sometimes, said complex passwords or hashes are so large in data size that they need to be carried around by flash or external drives.

Naturally, the data complexity of a single fingerprint or piece of biometric data surpasses the complexity of an average static password by a great margin. As it will be discussed further later in this report, approximately 2.5 Megabytes worth of data is required for representing a single encoded fingerprint template. Meanwhile an average static password (32 characters) is represented by a mere 32 Bytes of data. At first glance, there may be a space cost disadvantage, but in return the exponentially increased complexity will make it near impossible to reconstruct biometric data through exhaustive search.

1.2 The Problem: Irrevocability

In spite of the advantages mentioned above, static passwords hold at least one important advantage over biometric data, and that is their revocability. In case of a credential leak, the exposed user can easily revoke their password and have it replaced by a new one, and as a result, the leaked password will hold no leverage in future compromises on the same user.

On the other hand, if biometric data, such as a fingerprint get compromised, it will be forever exposed and there will be no way to have it revoked and replaced like a static password. Additionally, the risk for the biometric data to be used in future attacks will remain indefinitely.

1.3 The Solution: Cancelable Biometrics

Fortunately for us, there are a plethora of methods which cover the irrevocability weakness. These solutions fall under the category of Cancelable Biometrics. In general, the method converts a fingerprint into a certain data structure referred to as a template, which represents the fingerprint's minutiae data with great accuracy. Then the method transforms the template using a public key into a transformed template. Afterwards, the transformed template and its respective public key are saved to a database. In case the database gets hacked into, the attacker wouldn't be able to retrieve the original template through the public key and the transformed

template. In addition, the transformed template and its respective public key are revocable. Meaning that the exposed data could be easily removed from the database, and be replaced by a new public key from which another completely different transformed template could be generated.

1.3.1 Solution Outline

The process behind Cancelable Biometrics methods usually involves two generic stages: Enrolment and Verification. The following is a rough explanation of the whole process and its stages.

Enrolment

In the Enrolment stage, the Target fingerprint which is supposed to be used as reference for future comparisons gets scanned, and we get a grayscale picture of the fingerprint scan as a result. Next, we need to detect all the valid minutiae points on the fingerprint image, and create an Initial Fingerprint Template (IFT) using said minutiae. The IFT is composed of extracted minutiae data under a number of different schemes. From this point on, is where the most crucial process begins to occur. Using a set of algorithms designed for this specific Cancelable Biometric method, we will transform the IFT into an Transformed Fingerprint Template (TFT) using a psudeo-randomly generated Public Key. Finally, the TFT along with its respective Public Key which was used to generate it, will be stored in memory.

Verification

Afterwards, in the Verification stage, our Query fingerprint will be scanned and converted into another IFT using the same schemes and standards based on its minutiae data. Then using the same public key, the IFT will be transformed into a TFT. The Query fingerprint's TFT will then be compared with the Target fingerprint's TFT using a series of comparison methods. Ultimately, using a final score derived from the comparison methods and a predetermined score threshold, we will determine whether the two fingerprints match or not.

1.3.2 Solution Properties

Ofcourse, in order for both security and accuracy to be guaranteed, two main requisites must be met in the design a Cancelable Biometric method. One is the irreversibility of the process, in which the IFT gets transformed into the TFT. The other is the comparability of the Target fingerprint's TFT with the Query fingerprint's TFT, hence the differences in the Target and Query IFT must be somewhat preserved in their respective TFTs.

Irreversibility

In the case of an intrusion, the worst case scenario would be the compromise of the TFT and Public Key pair. In this case, the infiltrator should not be able to obtain the IFT from the TFT and Public Key by any means other than brute force. For a function to guarantee this attribute, it must preferably be a non-injective function (not one to one), and non-invertible. The input element of this function must be also large enough for exhaustive search to be near impossible. For instance a hash function such as SHA-512, is a good example of an irrevertible function.

Comparability

An irrevertible function such as a hash function may seem to be a good candidate for our purpose at first glance. But when it comes to biometric input, the smallest differences in input data could result in very different and incomparable outputs after being put through something such as a hash function.

Therefore we need a function or transformation that could preserve the small initial differences and render the results comparable. In Chapter 2, a few of these functions will be discussed.

Chapter 2

Other Related Works

Before we get to the full analysis of the Yang method (Yang et al., 2018), a number of other previously devised methods in the field of Cancelable Biometrics will be briefly covered from a review paper (Manisha & Kumar, 2019). After a brief discussion of other methods, certain advantages of the Yang method over previous methods will be examined.

2.1 Brief Outlines of Previous Strategies

2.1.1 Random Projections

2.2 The Yang Method

2.2.1 Outline

2.2.2 Advantages

The main contributions of the Yang method compared to the previously mentioned works, are the following advantages:

Reduced Non-Linear Distortion

ARM Attack Invulnerability

Chapter 3

Problem and Algorithm

3.1 Formal Description of Problem

3.2 Design of Algorithm

3.3 Proof of Correctness

3.4 Complexity Analysis

Chapter 4

Evaluation

4.1 Implementation Details

4.2 Experimental Setup

4.3 Results

Chapter 5

Conclusion

5.1 Contributions

5.2 Future Work

References

Maltoni, D., Maio, D., Jain, A. K., & Feng, J. (2022). *Handbook of fingerprint recognition.* Springer Nature Switzerland AG.

Manisha, & Kumar, N. (2019). Cancelable biometrics: A comprehensive survey. *Artificial Intelligence Review*, *2020*, October, 2019, 3403–3446.

Yang, W., Hu, J., Wang, S., & Wu, Q. (2018). Biometrics based privacy-preserving authentication and mobile template protection. *Hindawi Wireless Communications and Mobile Computing*, *2018*, June, 2018.

Appendix A

Code