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.

List of Figures

List of Tables

Table of Contents

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.

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 MBs worth of data is required for representing a single encoded fingerprint template, while an average person's static password (32 characters) is represented by a mere 1 KB of data. In first glance, there may be a space cost disadvantage, but in return the exponentially increased complexity will make it near impossible to reconstruct biometric

Figure 1.1: A picture of a gull.

data through exhaustive search.

1.1 Background

In this section, we briefly discuss the history and background of the problem. A detail literature survey is presented in Chapter 2.

The problem we study in this report is an important one. This problem is first proposed in 1990 in the context of graph theory (Manisha & Kumar, 2019). Zhang gives the first algorithm to the problem and applied it to solve several problems in artificial intelligence More recently, a slightly different formulation of the problem is studied independently (Maltoni, Maio, Jain, & Feng, 2022). None of this previous work uses the technique that we propose in this project. Thus, we believe that our algorithm is novel.

1.2 The Problem

In this section, we formally defined the problem. We adopt the definition given by Kovsky

1.3 Our Solution

1.4 Report Organization

Chapter 2

Related Work

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