**CPSC 525 Group Project Proposal**

|  |  |  |  |
| --- | --- | --- | --- |
| Aron Chan  University of Calgary  Calgary, AB T2N 1N4 archan@ucalgary.ca | Charlie Cheung  University of Calgary  Calgary, AB T2N 1N4 ccheu@ucalgary.ca | Jiashan Li  University of Calgary  Calgary, AB T2N 1N4 jiashan.li@ucalgary.ca | Jie Hu  University of Calgary  Calgary, AB T2N 1N4 jiehu@ucalgary.ca |

**ABSTRACT**

In this paper, we propose a review on the use of hashing functions related to biometric security and the discussion of security concerns in implementing biometric identification systems. The review will address the possibility of a compromised database implementing biometric identification systems and the challenges needed to be overcome before the widespread use of biometrics based authentication. We propose a study of the use of hashing fingerprints, irises, and facial images that can be used to authenticate users. Our research will take an in depth look into the development of biometric usage in security including early designs and implementations of such security systems, the current technology and algorithms used, and possible future implementations that could resolve current challenges. These methods will be reviewed through our study and we anticipate to find the best approaches to securing biometric authentication. This paper will also discuss the limitations of current biometric security and the beneficial uses of hashing for authentication and access control.

**CCS Concepts**

E.m [**Data**]: Miscellaneous – *biometrics, security, hashing.*

**Keywords**

Authentication; Biometrics; Hashing; Security; Privacy.

# INTRODUCTION

The use of biometric systems can already be seen in various applications in our daily lives. As the use of these systems escalates, there are increasing concerns about the security and privacy of this technology. The uniqueness of biometrics provides a high level of security, however, the common weakness is the need for a template database. If the biometric authentication is compromised, there is no way to assign a new template. Therefore, storing biometric templates should be avoided in the event of an attack. For our term project, we would like to research securing the use of biometric data through hashing so that it is impossible to reconstruct the original template and the original biometric is safe and never compromised. The significance of this research is to ensure that future uses of biometric security are reliable and trustworthy, securing the identity of users even after the event of an attack. To do this, we will introduce the concept of biometric hashing and its development as technology advances. Our study will describe the motive behind the need for biometric security and ways to implement it so that it is noninvertible. This paper will document our approach to reviewing this research problem and construct our expected results at the conclusion of our research.

# MOTIVATION & CONTEXT

Biometric systems must first gather data that can later be verified for authentication, which we will call the enrollment process [5]. Typically in authorization, a person is asked to reproduce their biometric information to be matched with the record stored in the database. Certain characteristics will be compared for similarity, and given that they meet a certain threshold, the verification process will succeed (and fail in other cases).

In present day, the use of biometrics for identification and authentication has become widespread and are commonly used in many ways. These systems collect data that are unique to the user, their own human characteristics. Since it is extremely difficult for one to lose these traits, they can be reproduced for verification without much trouble, unlike some instances where one might forget their password. These benefits have their own shortcomings which we will explore the issues at hand and examine possible solutions.

# METHODS

## Research Problem

The biometric data collected from a person is stored in a database, which can be vulnerable to an attacker resulting in a loss of integrity. An attacker who wants to gain unauthorized access can replace the template. Although encryption is possible, the persons involved in generating biometric data may find the use of biometrics to be intrusive and may express concern or discomfort in allowing sensitive information about them to be stored in database if it cannot be protected [2]. In addition, there is also the possibility of the decryption process being compromised. Immediately, cryptographic hash functions can be suggested to deal with this issue. A hash function can be considered to be a one-way function. In other words, given a case where the hash values (or hash output) are compromised, it would be impossible to reconstruct the original template.

Due to the nature of scanning biometric data, it is nearly impossible to reproduce the same result each time it is done. Systems establish some sort of threshold for acceptance, so as a comparison, if the system finds that the key points are close enough, then it is considered a match. This threshold cannot be too forgiving however, since accuracy is an important aspect in avoiding false positives or false negatives.

In consideration of biometric verification, we face a technical problem in constructing a hash function which can be successful with factors of threshold acceptance. Many cryptographic hashing algorithms (MD-5, SHA-1) provide completely different outputs even if the input changes slightly, which is a major concern when trying to incorporate it in biometrics [3]. Suppose the recorded data during the enrollment process is hashed and each time the user seeks verification by presenting their biometric, that data is also hashed before it is compared to the stored biometric. The challenge is that in many times the system will reject the user because the hash values do not match, even if it is the correct person. This is a result of biometric reading, for example each time the user uses a scanner to scan their fingerprint, the position or the angle will very likely be different in each instance, or the scanner does not read the fingerprint properly. Since the recorded data would be at least slightly different from the data in the database, their hash values would be vastly different if a “traditional” cryptographic hash function is used.

## Approach

To combat our problem, a hash function must be designed such that close inputs would give the same, or similar hash value, and inputs that are not close would give completely different hash values. This way, using hashing to properly secure biometrics can be done practically without severely impacting the enrollment and verification process.

Our approach involves reviewing different algorithms that use biometric data hashing and comparing their results for successes and errors. We will also look into the accuracy of each of the algorithms as they compare and identify the biometrics of different users. There are databases containing biometric data used for research studies we plan to use when comparing the *False Acceptance Rate (FAR)* and *False Rejection Rate (FRR)* of the hashing functions we will study. The results of the *FAR* and *FRR* can be used for not only fingerprints but facial recognition as well [4]. The challenges we find will be approached in a way that considers variation when authorizing with the use of biometrics identification and guided by the research and studies done on the topic.

# EXPECTED RESULTS

From our research, we expect to see the results of various methods of hashing biometrics and how they deal with the challenges brought upon the need of template security. The results should also show that biometric authentication can be just as viable as passwords for identification, authentication, and authorization. For the possible attacks that could compromise a biometric identification database, we expect to find a solution that can manage the attack while maintaining user security. Issues with biometric hashing should be identified and address issues of scalability, security, and collision-freeness. As our research develops over the course of the semester, we hope to develop more in depth questions and discussions relevant to hashing biometrics which will be added to our final report.

# PROJECT RELEVANCY

Pertaining to this course, the study of biometric hashing is relevant to our discussion of access control. The uniqueness of biometrics grants possible advantages to authenticating users and authorizing their level of access [1]. Through the study of biometrics we will also be looking into the possibilities of errors that occur at the presence of false positive and false negatives. Since biometrics can be used for both identification and authentication and they cannot be lost, stolen, or shared, they are susceptible to many privacy challenges as discussed in class. Further research into biometric identification will continue the discussion brought up in class about this security challenge of biometrics. The concept of using biometrics for security also applies to the notion of access control. There are many vulnerabilities that can arise from using biometric identification, this is especially the case when securing who can access what, in what way, under what circumstance. A study on biometric hashing will look at all of the possible vulnerabilities and review ways to combat threats. As taught in the tutorial sessions, our research of the use of biometric identification will review the principles documented in STRIDE and identify possible threats pertaining to the use of biometrics. Through our research, we will approach each of these threats and review security procedures and approaches to overcome them in an effort to make biometric security viable in the use of daily applications.

# CONCLUSION

In this paper, we proposed the use of biometric hashing to be the core topic of our term project. The use of biometric systems requires a high degree of trust and reliability that can be compromised with the threat of outsider attacks. We can secure fingerprint templates by using hash functions, this method is widely used for any biometric modality. We proposed a study of the evolution of biometric security and technology and a review of the methods that attempt to find a solution to our research problems. Our approach is to compare the success and error rates of various proposed hashing algorithms and evaluate the methods to which they apply the biometrics in an effort to guarantee security. As this is only a proposal of our final project, we hope to uncover more on this topic so we can review biometrics.

# REFERENCES

1. Fong, W.L. Philip. "Authentication." Presentation, University of Calgary, 2016.
2. Pfleeger, Charles P., and Shari Lawrence Pfleeger. *Security in computing*. Prentice Hall Professional Technical Reference, 2002.
3. Sutcu, Yagiz, Husrev Taha Sencar, and Nasir Memon. "A secure biometric authentication scheme based on robust hashing." In *Proceedings of the 7th workshop on Multimedia and security*, pp. 111-116. ACM, 2005.
4. Tulyakov, Sergey, Faisal Farooq, and Venu Govindaraju. "Symmetric hash functions for fingerprint minutiae." In *International Conference on Pattern Recognition and Image Analysis*, pp. 30-38. Springer Berlin Heidelberg, 2005.
5. Tulyakov, Sergey, Faisal Farooq, Praveer Mansukhani, and Venu Govindaraju. "Symmetric hash functions for secure fingerprint biometric systems." *Pattern Recognition Letters* 28, no. 16 (2007): 2427-2436.