# Security of Teleoperated and Haptic Cyber-Physical Systems

Junjie Yan

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2018

Reading Committee:

Howard J. Chizeck, Chair

M. Ryan Calo

Radha Poovendran

Franziska Roesner

Program Authorized to Offer Degree:
Electrical Engineering

University of Washington

**Abstract**

Security of Teleoperated and Haptic Cyber-Physical Systems

Junjie Yan

Chair of the Supervisory Committee:
Professor Howard J. Chizeck
Department of Electrical Engineering

In teleoperated robotic applications such as robotic surgery, search and rescue robotics, bomb disposal, remotely operated aircraft and underwater vehicles, robots primarily serve as extensions of people. Human operators, often geographically distant, interact with robots through a communication network that may consist of diverse components. It is expected that these teleoperated robotic systems will generate immediate relief in scenarios where it is inappropriate or too dangerous for a human operator to fulfill in person, or simply because there is no experienced operator locally.

The benefit of having geographically distant teleoperators comes, however, with a new set of problems that are not present in traditional settings. In many envisioned scenarios, including under-developed rural areas, disasters, and battlefields, network infrastructure may be limited. We may have to resort to a communication channel consisting of several components, including publicly available wireless or satellite networks, or even UAV-based ad hoc networks to exchange audio, video and other sensory information between the operator and robot. The open and relatively uncontrollable properties of these networks make teleoperated robotic systems more vulnerable to various kinds of attacks. Moreover, the uniqueness of teleoperated robotic systems introduces a tension between security and usability, which potentially makes existing techniques inapplicable.

Therefore, it is crucial to develop specific tools and techniques for the teleoperated cyber-physical systems to make them secure without affecting their usability. In doing so, in this work, we focus on the human component in a teleoperated cyber-physical system and investigate the way to

use the uniqueness of how each human user interacts with the teleoperated cyber-physical system in order to enhance security and reliability.

In doing so, we focus on following two tasks:

1. **Initial Authentication**: Authenticate user's access to the teleoperated system. Minimize the probability of spoofing forgery passwords getting authenticated.

2. **Continuous Authentication**:

    i Guarantee it is the authenticated user who is operating the teleoperated system without affecting the system usability.

    ii Allow the detection of any abnormal action that caused by attacks.

These tasks are fulfilled in the context of *Haptic Passwords* and *Continuous Operator Authentication for Teleoperated Systems*.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# GLOSSARY

ANN: Artificial Neural Network

CPS: Cyber-Physical System

DTW: Dynamic Time Warping

DWT: Discrete Wavelet Transform

HMM: Hidden Markov Model

HSMM: Hidden semi-Markov Model

JIGSAWS: JHU-ISI Gesture and Skill Assessment Working Set

MODWT: Maximal Overlap Discrete Wavelet Transform

PCA: Principal Component Analysis

ROC: Receiver Operating Characteristic

SVM: Support Vector Machine

UAV: Unmanned Aerial Vehicle

# ACKNOWLEDGEMENTS

After 5 years of graduate school study at the University of Washington, today is the day for me to write this finishing touch on my dissertation. It has been a wonderful period in my lifetime, during which I learned a lot, both in how to do a good research and how to be a better man. I am grateful to all the people who have supported and helped me so much throughout this period.

First, I would like to express the deepest appreciation to my adviser, Professor Howard Chizeck, for his continued guidance and advise throughout my research development and analysis. I would also like to thank all my Dissertation Committee, Professor Ryan Calo, Professor Radha Poovendran and Professor Franziska Roesner. Thanks so much for the extensive help and suggestions you offered on my research.

Thank you also to all BioRobotics Lab member and alumnus. Especially, I want to thank Professor Blake Hannaford, for his great questions and comments that have significantly enhanced my work. Also to Tamara Bonaci, it has been a great pleasure for me to collaborate with her and I have learned tremendously throughout this collaboration. Many thanks to Kevin Huang, Kyle Lindgren, David Caballero and Danying Hu, for their help on setting up the teleoperation experiment environment as well as all the insightful discussion and collaboration we had, and to Yangming Li, for all his great advice on my career path.

Lastly, I would like to thank my parents, whose love and guidance are with me in whatever I pursue. Most importantly, I wish to thank my lovely and supportive wife, Anqi, and our cute little fur baby, Toffy. Thanks so much for all those love and companion you offered. I will not be able to reach this far without you.

# DEDICATION

To my dear wife Anqi and our fur-baby Toffy.

Words cannot express how much I love you all.

# Chapter 1

# INTRODUCTION

In telerobotic applications such as robotic surgery, search and rescue robotics, bomb disposal, remotely operated aircraft and underwater vehicles, robots primarily serve as extensions of people. Human operators, often geographically distant, interact with robots through a communication network that may consist of diverse components. It is expected that these teleoperated robotic systems will generate immediate relief in scenarios where it is inappropriate or too dangerous for a human operator to fulfill in person, or simply because there is no experienced operator locally.

## *1.1 Teleoperated Robotic Systems*

As depicted in Figure 1.1, a teleoperated robotic system can be defined as a system where a human operator interacts with a local control console in order to send the command through a communication channel to control a remote robot that is inaccessible or in a dangerous environment at a distance. Typically, the remotely teleoperated robot consists of one or more robotic arms and end effectors controlled by a human operator to fulfill certain tasks.

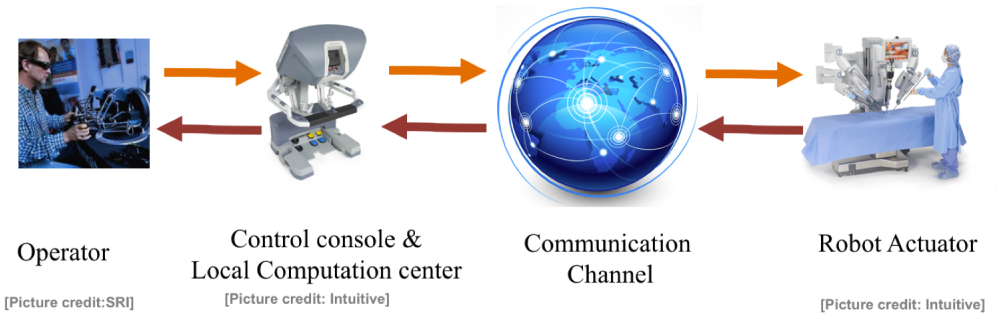


Figure 1.1: Teleoperated Robotic System

Today, teleoperated robots are being widely used in many fields, including bomb disposal, space and underwater exploration, search and rescue in disasters and robotic surgery. There are many benefits of using teleoperated robots. The ability to be operated at distance make it possible for a human operator to fulfill the tasks that can not be done in person, either because it is too dangerous for a human operator to act in person, such as in radioactive and chemical environments and disaster scenarios, or when there is no appropriate personnel available locally. Additionally, with different size and format of teleoperated robots, they also allow us to perform the operation in inaccessible areas, as well as in extremely small or large areas.

### *1.2 Problem:Teleoperated Robots Security*

The benefit of having geographically distant teleoperators comes, however, with a new set of problems that are not present in traditional settings. In many envisioned scenarios, including under-developed rural areas, disasters, and battlefields, basic infrastructure may be limited. Remote robots are expected to operate in harsh and challenging conditions. We may have to resort to a communication channel consisting of several components, including publicly available wireless or satellite networks, or even UAV-based ad hoc networks, to exchange audio, video and other sensory information between the operator and robot. Under these conditions, we recognize two feasible attack modes[11]:

1. **Endpoint compromise**: Either an operator's control console or a remote robot is compromised;

2. **Communication-based attacks**: An attacker intercepts the existing network traffic, inject new malicious traffic, or both.

Endpoint compromises are less interesting, as the physical accesses to both operator and robot sides are most likely strictly monitored. Therefore, communication-based attacks are more feasible to compromise the system. Moreover, the open and relatively uncontrollable properties of networks in many envisioned scenarios makes teleoperated robotic systems more vulnerable to

various kinds of attacks. Due to the uniqueness of teleoperated robotics system, mitigating and preventing these attacks is likely to be challenging. In this dissertation, we will focus on developing tools and techniques to detect and mitigate attacks against teleoperated robotic systems through communication channels.

### *1.3 Attack Models*

Based on whether the commands from human operators are modified or not, we classify possible attacks on teleoperated robotics systems into two categories:

1. Passive attacks,

2. Active attacks.

**Passive attacks** occur when an attacker intentionally jams or interrupts the communication channel between the operator and the remote-controlled robot in order to cause communication latency, packet delays and losses or even devices failures. These attacks include denial-of-service (DoS) attacks and delay attacks. They are relatively easy to launch and may severely degrade the usability of the teleoperated robotic system.

**Active attacks** occur when an attacker acts in an intermediary role between the operator and the remote robot and is able to modify the information transferred between the benign parties. A typical example of this type of attack is a man-in-the-middle (MitM) attack. In the case of MitM, an attacker is able to modify the operator's intended actions by altering his/her command messages while packets are in-flight, and the operator has no control over them. An attacker can also corrupt the sensory feedback data in order to mislead the operator. Since the feedback is assumed to be valid, an operator may unintentionally harm the environment or even people under this kind of attack. Most severely, an attacker can hijack the robot, making it completely ignore the intention of an operator, to perform some other actions follow the commands from an attacker.

## *1.4 Related works*

### *1.4.1 Teleoperated robotics system security*

Recently, motivated by the Raven II extreme operation experiments [42][30], researchers have recognized the importance of teleoperated robotics system security and several attempts to enhance system security have been made. K. Coble et al. developed a lightweight software tool to verify the robot-side code [16]. G. S. Lee et al. propose the use of the Transport Lay Security (TLS) protocol to ensure confidentiality, authentication, and authorization of the Interoperable Telesurgery Protocol (ITP)[41].

### *1.4.2 Preventing passive attacks*

In order to prevent and mitigate the effect of passive attacks, especially DoS attacks, there are some existing preventing methods, including:

1. Intrusion Detection Prevention Systems(IDPS) [70]
   Intrusion Detection Prevention Systems (IDPS)-based approaches require a known attack 'signature' in order to be able to stop the attack. These attack's signatures are normally obtained by analyzing a packet's content and network behavior as features of interest. However, by simply capturing one legitimate message between operator and robot, an attacker is able to flood the network with multiple copies of that message. Moreover, IDPS is unable to prevent distributed DoS, since the attack task is spread over a large number of computers.

2. Blackholing [53]
   The strategy of blackholing is to reroute all the traffic from an attacking network entity to a non-existent server, which is referred to as the "black hole". However, the problem of the blackholing approach is when rerouting all the traffic from an attacking network entity, legitimate traffic may be rerouted as well thus blocking the communication between an operator and a remote robot.

3. Pipes cleaning [4]

   In the pipe cleaning approach, all the traffic is passed through a "pipe" where all the packets are inspected and only legitimate ones can pass through the pipe. The major problem with this approach is that it will cause communication delays. This can not meet the real-time requirement for the teleoperated robotic systems.

### *1.4.3 Preventing active attacks*

While preventative strategies for teleoperated robotic system against active attacks have been less explored, it has been shown that some types of attacks against networked control systems can be mitigated by relying on the system's dynamics[13][45]. In [14][45][44], the authors showed that by using an optimal controller and a Kalman filter, the desired probability of detecting attacks, such as replay, false data injection and integrity attacks, can be guaranteed given a certain model under the linear dynamic assumption. However, the linear dynamics assumption may not hold in most teleoperated robotic systems and thus these techniques may not be readily applicable to prevent attacks against teleoperated robotic systems.

## ***1.5 Prior Work***

In our prior work [11][12], we conducted an experimental study to identify and evaluate the effects of various types of attacks, based on an evaluation of a real technology, the *Raven II*, an advanced teleoperated robotic surgery system. For each type of attack, we assessed the level of impact on a surgical process through a series of human subject experiments.

We quantitatively analyzed the impact of delay and DoS attacks against teleoperated robotic surgery by introducing Fitts' law as a novel way to quantify the impact of attacks on cyber-physical systems. Moreover, we also demonstrated that some of the existing cryptographic methods may be applicable to mitigate the effect of intent modification and hijacking attacks, without negative impacts on system performance and real-time operation requirements.

This work also exposes a security challenge that is unique to the teleoperated robotic sys-

tem, namely the tension between security and usability. The real-time operation constraints of teleoperated robotic systems render many existing security techniques infeasible.

Therefore, the specific problem of teleoperated robotic systems is: *How to secure teleoperated system without affecting its usability?*

### *1.6 Specific Solution for a Teleoperated Robotic Systems*

In order to develop specific techniques that meet the requirements described above, we focus on the uniqueness of teleoperated robotic systems. The fundamental difference between classic cyber systems and teleoperated robotic systems is the human component (operator) in the loop. Human users (operators) have a unique way of interacting with a cyber-physical system. It has been recently shown that users have a unique way of interacting with haptic-based and touch-based devices[84]. The users' unique traits and ways of interacting with a system can be used to identify and authenticate the user and thus increase the system's security, privacy and usability properties.

Therefore, in this work, we investigate ways to use the uniqueness of how each human user interacts with the teleoperated cyber-physical system in order to enhance the security and reliability of teleoperated cyber-physical systems.

In doing so, we focus on following two tasks:

1. **Initial Authentication**:
   Authenticate user's access to the teleoperated system. Minimize the probability of spoofing forgery passwords getting authenticated.

2. **Continuous Authentication**:

   (1) Guarantee it is the authenticated user who is operating on the teleoperated system without affecting the system usability.

   (2) Allow us to detect any abnormal action that caused by attacks.

These tasks are fulfilled in the context of *Haptic Passwords* and *Continuous Operator Authentication for Teleoperated Systems*.

## *1.7 Haptic Passwords*

Most existing cyber-physical systems rely on the use of passwords to identify and authenticate human users [80]. For most kinds of passwords systems, there are three concepts to authenticate the user, based on 1) what you know, 2) what you have and 3) who you are. Existing identification and authentication methods can broadly be classified into those that depend on alphanumerical passwords (what you know), and those that use classical biometric properties of a user (who you are), such as fingerprints, voice data, and iris recognition. Alphanumerical passwords are most widely used since they are easy to implement and the updating process is simple. However, there are drawbacks to the use of alphanumerical passwords. Alphanumerical passwords have a limited possible password space and thus are vulnerable to dictionary and brute-force search attacks [36][82]. Additionally, users often struggle to find a good tradeoff between security and memorizability when dealing with the alphanumerical passwords. People tend to: (1) use overly simplistic passwords that are easy to memorize, but also easy to break; (2) reuse their passwords across different systems; (3) not update their passwords regularly[2][47]. On the other hand, biometric passwords release the burden of memorizing password from users since they are physically a part of the user. However widely used biometric passwords, such as fingerprint and iris recognition, have shortcomings including (1) potential privacy issues that may arise from the use of these passwords; (2) relatively low accuracy rates; (3) limited ability to update[56]. There are also recent concerns about the security of some biometric passwords. For example, there are reports showing that it is simple to break the iPhone fingerprint verification system with just a photo of a fingerprint on a glass surface[1].

These drawbacks motivate the creation of new password systems. Therefore, we propose a novel identification and authentication system which is based on the haptic interaction. In Chapter 2, we develop the novel haptic interaction based password system - *Haptic Passwords*[84][83], which uses both ‘what you know’ and ‘who you are’ to authenticate the user. We demonstrated that each individual user interacts with a force feedback (haptic) device in a unique way, which can be used as a basis for a new type of biometric identification and authentication. We also showed that the extra force (haptic) information helps generate better authentication performance compared to solely use

position and orientation information. It significantly increases the space of possible passwords, making the dictionary and brute force attacks much harder to accomplish. In addition, unlike other biometric-based identification and authentication methods, haptic-based passwords can be updated if the need arises.

Based on our experimental analysis on multiple platforms, we demonstrated that the proposed password system is secure and user-friendly. The advantages of our proposed haptic password system over conventional password systems are that: (1) it is easy to memorize; (2) there are no privacy concerns; (3) the space of possible password (haptic alphabet) is significantly larger than in alphanumerical passwords, so it cannot be guessed and dictionary search attacks will not work; and (4) it is resistant to forgery attacks (5) the authentication process is fast.

Partial content of Chapter 2 has been published in [84] and [83].

### *1.8 Continuous Operator Authentication for Teleoperated Systems*

Teleoperated robots have been playing an increasingly important role in many scenarios including search and rescue in disasters[48], deep underwater[68] and outer space[34] exploration. Additionally, many researchers[43][28] have envisioned that teleoperated surgical robots will emerge which will offer huge medical relief in battlefields, disasters, and rural areas. However, due to the lack of basic network infrastructure in many envisioned scenarios, the teleoperated robots will be expected to use a combination of existing publicly available networks and temporary ad-hoc wireless and satellite networks to send video, audio and other sensory information between operators and remote robots[43]. The open and uncontrollable nature of these communication channels makes these teleoperated robotic systems under these scenarios vulnerable to a variety of possible cyber attacks. The communication between surgeon and robot can be interrupted or even taken over[12]. In most cases, such as teleoperated surgery and disaster search and rescue task, any abnormal operation or discrepancy between the authorized operator and the robot received command will cause severe negative outcomes.

Therefore, to guarantee the security of teleoperated robotic procedures, we need to be able to realize continuous operator authentication. In Chapter 3, we propose a novel approach to

continuously authenticate human operator when using teleoperated systems based on the analogy between speech recognition and the operator gesture recognition. We use a Hidden Markov Model to model operator's gestures and applied the Token Passing Algorithm [85] to concatenate gesture models to obtain recognition of operator's gesture sequence and continuous operator authentication.

In Chapter 3, we build a simulated VR environment using an HTC Vive and PhantomOmni. It allows the user to fulfill a simulated teleoperation task with haptic feedback, which offers the user both visual and tactile sensation during the operation process. In order to explore the performance of the proposed continuous authentication method, we conducted a human subject experiment with 5 subjects. The performance of the model is evaluated based on the continuous (real-time) classification and authentication accuracy. The results suggest that our proposed method is able to achieve 77% continuous classification accuracy with as short as 1 second sample window.

### *1.9 Contributions*

Focusing on the human component in the teleoperated cyber-physical systems, this work makes the fundamental contribution towards developing mitigation and prevention strategies which are based on the uniqueness of human component within a cyber-physical system to enhance the system security. Specific contributions of this work are:

1. **Haptic Passwords - novel biometric-based approach to identification and authentication for teleoperated cyber-physical systems:** In Chapter 2, we propose a novel biometric technology, based on human operator's interaction with a haptic (force sensitive) device. Our technique uses wavelet-based analysis to extract operators' unique haptic interaction features. The extracted features are then further analyzed and then classified to perfors operator identification and authentication. Our experimental results show that the proposed haptic-based authentication system has a high identification accuracy and that it is resistant to forgery attacks.

2. **Continuous Operator Authentication - novel monitoring and detection technique for teleoperated cyber-physical systems:** In Chapter 3, we utilize an analogy between speech

recognition and operator gesture recognition. We use a Hidden Markov Model to represent an operator's gesture and apply the Token Passing Algorithm [85] to concatenate gesture models to realize operating sequence recognition and continuous operator authentication. This approach is based on the assumption that each operator interacts with a teleoperated robotic system in a unique way, thus generating a unique biometric (signature), which can be extracted and used for authentication. We built a simulated VR teleoperation environment with haptic feedback and conducted a human subject experiment on it. The experimental results show that the proposed continuous authentication method is able to generate above 77% accuracy rate with as short as 1 second sampling window.

# Chapter 2

# HAPTIC PASSWORDS

## *2.1 Authentication Techniques for Cyber-Physical Systems*

Existing cyber and cyber-physical systems largely rely on the use of passwords to identify and authenticate human users [80]. Most password-based systems rely on some combination of following concepts to authenticate an user: 1) what you know, 2) what you have and 3) who you are. Current identification and authentication methods can broadly be classified into those that depend on alphanumerical passwords (what you know), and those that use conventional biometric properties of a user (who you are), such as fingerprints, facial recognition, voice data, and iris recognition. Alphanumerical passwords are most widely used since they are easy to implement and the updating process is simple. However, there are drawbacks to the use of alphanumerical passwords. Alphanumerical passwords have a limited possible password space and thus are vulnerable to dictionary and brute-force search attacks [36][82]. Additionally, users often struggle to find a good tradeoff between security and memorizability when dealing with such password systems. More specifically, people tend to: (1) use overly simplistic passwords that are easy to memorize, but also easy to break; (2) reuse their passwords across different systems; (3) not update their passwords regularly[2][47]. On the other hand, biometric passwords release the burden of memorizing password from users since they are physical parts of the user. Nonetheless most widely used biometric passwords, such as fingerprint and iris recognition, also have limitations including: (1) potential privacy issues that may arise from the use of these passwords; (2) relatively low accuracy rate; (3) limited ability to update[56]. There are also recent concerns about the security of some biometric passwords. In [66], the authors suggest that smartphones can easily be fooled by fake fingerprints digitally composed of many common features found in human fingerprints.

These drawbacks motivate the creation of new password systems. Therefore, we propose a

novel identification and authentication system which is based on the haptic interaction. In [84], we demonstrated that each individual user interacts with a force feedback (haptic) device in a unique way, which can be used as a basis for a new type of biometric identification and authentication, namely *haptic passwords*. We also showed that the extra force (haptic) information helps generate better authentication performance compared to solely use position and orientaion information. Haptic passwords use both 'what you know' and 'who you are' to authenticate the user. They significantly increases the space of possible passwords, making dictionary and brute force attacks much harder to accomplish. In addition, unlike other biometric-based identification and authentication methods, haptic-based passwords can be updated if the need arises.

In [83], relying on recent technologies, such as force sensitive touchscreens on smartphones and tablets, we built our haptic passwords system on an iPhone 6s. We performed a study with 29 participants of mixed demographics. All subjects enrolled their signatures as their passwords. We then developed a maximal overlap discrete wavelet transform (MODWT)[79] based feature extraction and combined it with a customized classification strategy to fulfill the authentication task. We also developed an adaptive template update scheme to accomodate user's variation over time. We tested our authentication technique and collected detailed data on the authentication accuracy and how different writing postures (i.e. hand and device position), and day-to-day variation affects the system performance. We simulated skilled forgery attacks and tested the proposed system's vulnerability to such attacks.

The contributions of the haptic passwords work in this dissertation are:

1. The development of a haptic passwords system that combines 'what you know' (user's signature or user defined pattern) and 'who you are' (user's unique way to haptically interact with the touch screen) to realize the user identification and authentication.

2. Demonstration that this haptic password system is forgery-resistant and robust over time.

3. Demonstration that haptic passwords are user friendly. It is easy to memorize and update the password and the authentication process is fast.

## *2.2 Related Work*

Chiasson et al.[15], Jablon et al.[36] and Wiedenbeck et al.[80] proposed to use graphical based password systems to authenticate users. The main idea of these systems is to let the user click on a few chosen regions of an image and, based on the clicked location, to authenticate the user. Such systems provide benefits over alphanumeric and biometric passwords. In general, users are able to better memorize graphical passwords. Additionally, the possible graphical passwords space is much larger than that of alphanumeric passwords. One major concern, however, is that graphical passwords are still vulnerable to forgery attacks (i.e. shoulder surfing attacks) [40].

To overcome this issue and increase the possible password space, several studies have been done to authenticate the user by implementing haptic-based information. Bianchi et al. [8][9] proposed authentication schemes that combine both visual and haptic/audio cues, such as vibration or specific sound effect, as password input. There are two major limitations in their work. They rely on extra hardware, such as a tactile wheel or earphones, to generate cues. Moreover, the authentication speed is relatively low (more than 10 seconds). Krombholz et al. [39] developed a force-PINs technology that enhances traditional 4-digits or 6-digits PINs with tactile features using pressure sensitive touchscreens as found in modern consumer hardware. Besides 0-9 for each digit, they enrich the password information with force pressure. While their approach offers an "invisible" force layer to the password, the possible password space is limited as the force is discretized into "deep" and "shallow" press only. If an attacker learns the PIN, such as through shoulder-surfing, the password can be hacked through brute-forcing. Additionally, the haptic channel introduced in both aforementioned work adds extra memorization burden on the user.

Another way to authenticate the user is through their graphical signature[19][31][49][50]. With the development of force sensing technology, not only the position information about the signature but also the ‘hidden’ haptic (force) information can be captured. This extra dimension of data enhances the security of these systems. Currently, most signature verification algorithms are based on dynamic time warping (DTW) to realize user identification and authentication[35]. For an input signal and a template of different lengths, the DTW algorithm is able to find the best matching path,

in terms of the least global distance, based on dynamic programming (DP)[69]. However, DTW has several drawbacks when applied in online signature verification. First, DTW is a computationally expensive algorithm[20]. This is because the DTW performs non-linear warping on the entire signal. The computational cost is proportional to the square of the signal length[69]. Second, the DTW algorithm is required to store the raw signature signal as a template to fulfill the matching process for a test signature signal. In case the malicious party hacks the database, the malicious party will be able to obtain complete information of each user's signature. Aware of this issue, in [33] [51][52][6] [67], global statistical properties such as mean, variance, correlation of the recorded signature data[33] [51][52][6] and histogram of trajectory direction and location [67] were used as password features to classify the user. The drawbacks of the aforementioned techniques are the loss of signature transient properties in the feature extraction process.

In [24], a continuous authentication based on how a user interacts with the touch screen is proposed. The author investigated the user's touch actions during navigation maneuvers to continuously authenticate the user. The major limitation of this work is that it requires a relatively long enrollment period and the experimental evaluations disqualify this method as a stand-alone authentication mechanism for long-term authentication.

In [3] [18], the discrete wavelet transform (DWT) is implemented to extract features from the user's signature in order to realize user authentication. The key benefit of the DWT is that it captures both frequency and localized (in time) information. However, there is a constraint for DWT that the length of the signal has to be a multiple of a power of two. We had to resample the signature to meet this requirement. This requirement inevitably alters the original properties of the given signature signal and potentially increases the similarity between genuine signatures and forgeries (since the length of genuine signatures and forgeries is most likely different, while after resampling, they will be the same).

Additionally, in most prior works, conventional classification algorithms, such as neural network, support vector machine or random forests, are implemented. One major limitation of these classification algorithms in signature verification applications is that in the training phase, they heavily rely on the choices of both positive and negative samples. Although the choices of positive

samples are straightforward as we can use the genuine signatures, *how to choose negative samples to train the classifier is a tricky problem*. First, using forgeries (as in [38]) as negative samples to train the classifier is not applicable in the real-life scenario, since the forgeries require extra effort to generate. On the other hand, although using different subjects' signatures or predefined patterns as negative samples is feasible, this may lead to the classifier under-estimate the difficulty of the classification problem, since different signatures can easily be classified graphically while it is more challenging to classify genuine signature and its forgery. One major contribution of this dissertation is to develop a customize classification strategy to train the classifier with only positive samples.

Another limitation of the conventional classifiers is a lack of adaptivity. Galbally et al. [25] demonstrated that the dynamic property of a human's signature may vary over time. Therefore, in order to achieve reliable long-term use of the signature based password system, it is crucial to develop a mechanism to account for this variation. However, for these conventional classifiers, a new training set has to be reconstructed to address the signature variation over time and the entire training process for the classifier needs to be performed again.

Recently, Harbach et al. [29] conduct a detailed real-world study of the smartphone unlocking and provide a benchmark of current smartphone authentication mechanisms. In their study, it is shown that on average, participants unlock their phones more than 40 times per day. Also according to the subjective survey, most participants put high emphasis on the authentication speed of unlocking the system. These results indicate that in practical applications, the time needed to fulfill the authentication process is a critical factor regarding the usability of the password system.

## *2.3 Problem Statement and Challenges*

### *2.3.1 Problems*

Problem 1: Forgery attacks.

The general structure of a biometric authentication system is depicted in Figure 2.1[81]. Various types of attacks can be launched to compromise the system at different stages.

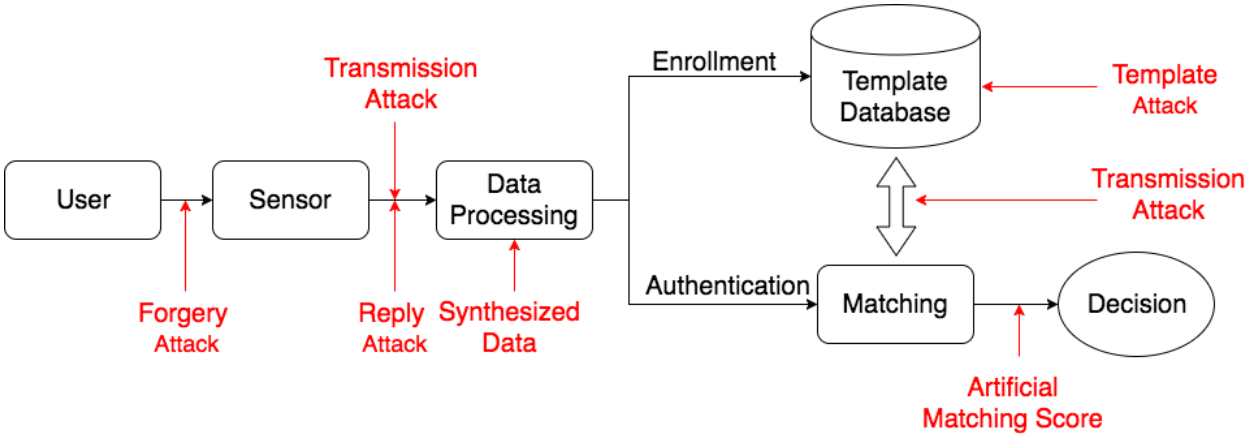


Figure 2.1: Attacks on biometric authentication systems

In this work, we focus on demonstrating that our proposed haptic password system is resistant to various forgery attacks. The haptic information, such as force and velocity, is able to classify and authenticate user and prevent forgery attack. Our proposed feature extraction technique can mitigate template attacks. As discussed later, the feature extraction process is non-invertible, so even if the template is hacked, a malicious party still has no information about the genuine password.

Problem 2: The lack of negative samples to train the classifier.

During the classifier training phase, only positive samples (genuine password from the user) are available, thus conventional classifiers, whose training procedures depend on both positive and negative samples (forgeries), are not appropriate for this application. Customized classifiers need to be developed to classify different users while achieving forgery attack resistance.

Problem 3: Randomness of Haptic Interaction.

The randomness of a human during haptic interaction also introduces extra challenges to the authentication system. First, during the enrollment phase for each user, the system must be trained based on the training set of the given user and generate a template database. However, there potentially will be 'bad' or 'inconsistent' training sets in the enrollment phase. Moreover, the dynamic properties of how a human haptically interacts with the device may vary over time [25]. It is crucial to develop a method to adaptively update the template database to accommodate the variation over time so that the authentication system does not become stale.

In order to solve the problems mentioned above, we pursued a series of projects as follows.

## *2.4 Haptic Password System on Haptic Interface Device*

In this project, we implement the haptic password approach on a haptic interface device (the Sensable PHANToM Omni). We mainly deal with Problem 1: forgery attacks. We propose a novel haptic password approach which uses a discrete wavelet transform-based feature extraction technique in conjunction with an artificial neural networks classifier as a secure haptic password system. The advantages of our proposed haptic password system over alphanumerical passwords and classic biometric passwords are that: (1) it is easy to memorize; (2) there are no privacy concerns; (3) the space of possible passwords (haptic alphabet) is significantly larger than in alphanumerical passwords, thus complicating guessing and dictionary search attacks will not work; (4) it is resistant to forgery attacks.

### *2.4.1 Discrete Wavelet Transform*

The discrete wavelet transform (DWT) is a modified wavelet transform for which wavelets are discretely sampled to deal with discrete signals. The main idea of the DWT is to represent a time series as a linear combination of a set of functions generated from a mother wavelet. The weighting parameters are called wavelet coefficients. A key benefit of the DWT is that it captures both frequency and localized (in time) information. This facilitates the feature extraction process later on [77].

The DWT coefficient of signal $x$ is calculated by passing it through a series of filters generated from a mother wavelet filter. The mother wavelet filter $g$ is a low-pass filter that satisfies the standard quadrature mirror condition [71]

$$G(z)G(z^{-1}) + G(-z)G(-z^{-1}) = 1 \tag{2.1}$$

where $G(z)$ denotes the z-transform of the filter $g$. Its complementary high-pass filter can be obtained as

$$H(z) = zG(-z^{-1}) \tag{2.2}$$

These mother wavelet filters are then used to generate the series of filters of increasing width

$$H_{i+1}(z) = H(z^{2^i})G_i(z) \tag{2.3}$$

$$G_{i+1}(z) = G(z^{2^i})G_i(z) \tag{2.4}$$

with initial condition $G_0(z) = 1$. Equivalently, these filters can be expressed in the time domain as

$$h_{i+1}(k) = [h]_{\uparrow 2^i} \times g_i(k) \tag{2.5}$$

$$g_{i+1}(k) = [g]_{\uparrow 2^i} \times g_i(k) \tag{2.6}$$

where the notation $[\cdot]_{\uparrow m}$ denotes upsampling by a factor of $m$. Figure 2.2 shows the block diagram of the DWT process.

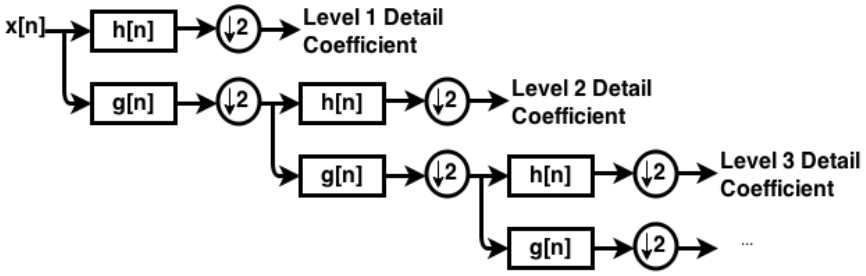


Figure 2.2: DWT sub-band decomposition

At each level in the above diagram, the signal is decomposed into low and high frequencies. The high frequency component of each level is regarded as the detail coefficient of that corresponding level. In this work, we use the DWT as the first stage of real time analysis of the haptic signal generated by a user. This is then used as the basis of the password.

### *2.4.2 Haptic Password System*

There are three main parts of our haptic password system: data collection, feature extraction and classification, as shown in Figure 2.3.

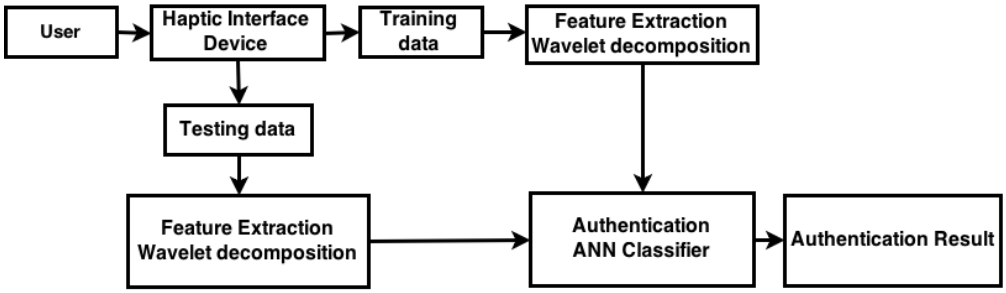


Figure 2.3: Haptic Password System on PHANToM Omni

*Data Collection*

In our haptic-based identification and authentication system, we collect the following data:

1) Position of the pen tip in virtual environment $(x, y, z)$

2) Applied forces $(f_x, f_z)$

3) Stylus orientation $(\theta_{pitch}, \theta_{roll}, \theta_{yaw})$

The state vector is constructed as $v = (x, y, z, f_x, f_z, \theta_{pitch}, \theta_{roll}, \theta_{yaw})$. All data is recorded at a 30 Hz sampling rate. The software starts recording data when the pen tip makes contact with the virtual paper and stops when no more contact is detected.

*Feature Extraction*

Feature extraction is the next step in the classification problem. The choice of elements in the feature vectors significantly affects the performance of classifier. Because the recorded haptic signals contain transient and localized features, the DWT is chosen to extract the feature vector because it, like all wavelet methods, can capture signal frequency properties while conserving its local features. The feature vector for each trial is obtained in the following steps [37]:

1. The position data $(x, y, z)$ is differentiated to obtain the velocity data$(v_x, v_y, v_z)$.

2. The data set of each trial is resampled to 128-point length (i.e. for each trial the data size is $8\times128$, where 8 is the dimension of the data). This resampling makes the data amenable to the discrete wavelet transform process.

3. The DWT is applied to each channel separately. The mother wavelet is the Duabechies Wavelets order-4. For each channel, seven levels of detail coefficients, $D_1 \sim D_7$, are obtained

4. For $D_1 \sim D_5$, the following statistical features are used to represent the time frequency distribution:

- Maximum of the wavelet coefficients in each level.
- Minimum of the wavelet coefficients in each level.
- Mean of the wavelet coefficients in each level.
- Standard deviation of the wavelet coefficients in each level.

Since the length of $D_6$ and $D_7$ are 2 and 1 respectively, they are inserted into the feature vector directly. Therefore, the feature vector of each dimension is $f_i = [v_1, v_2, v_3, v_4, v_5, D_6, D_7]$, where $v_i = [max(D_i), min(D_i), mean(D_i), std(D_i)]$. The length of $f_i$ is 23. Then the feature vector of each trial is obtained by combining all 8 vectors together. $F = [f_1, f_2, ..., f_8]$. The length of F is $23\times8$=184.

*Classification*

Based on the obtained feature vector, an artificial neural network is implemented to complete the classification task. This includes an ANN with 184 inputs, one hidden layer with 500 neurons and $N$ outputs for the user identification, where $N$ is the number of users. The output $O$ is a vector with length $N$. Each element of the output vector is between 0 and 1, where a zero-value $i^{th}$ element indicates that the data is least likely to be generated from user i, while a value of 1 means the data is most likely from user i. We use a scaled conjugate gradient backpropagation supervised learning method to train the network. All training parameters used default settings. In order to obtain satisfying training results, the stop criterion is set to minimize the mean square error before validation failures reach 100 or the performance gradient is less than $1 \times 10^{-10}$.

### *2.4.3 Experimental Setup*

*Experiment Environment*

In this part, our haptic-based method is evaluated in an experiment where human users interact with a virtual 3D environment via a 3 degree of freedom haptic device, the Sensable PHANToM Omni. As shown in Figure 2.4, the user interacts with the haptic device to manipulate the configuration of a virtual pen in order to write on a virtual paper. It is depicted visually and force feedback rendered haptically, thus allowing subjects both to see and feel the virtual paper. The virtual paper is slightly tilted (15 degrees) towards the user. In this environment, the user's pen tip position is visually rendered as a red cursor and a shadow is used to represent the projection of the pen tip on the paper.

*Experiment Task*

Before each experiment, subjects were asked to explore the environment and get used to the haptic device and the sensation of its force feedback. There are 4 different tasks. There are:

- L-shaped pattern
- Word *'SEAHAWK'* (all in uppercase)

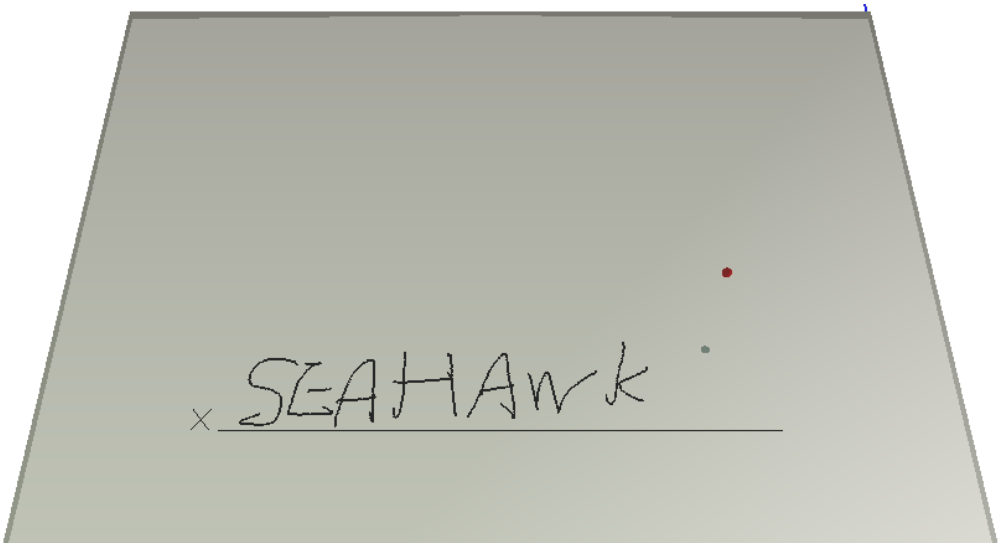


Figure 2.4: Haptic Password System Virtual Environment

Figure 2.5: L-shape Pattern

- The subject's own signature
- Forging a pre-defined signature

Subjects were given a practice period before each task type in order to gain sufficient proficiency, and to limit learning effects. After practice, then each task was repeated 10 times per user.

In task 4, subjects were shown an image of the signature to be forged, as shown in Figure 2.6. The first three tasks test the performance of different types of haptic passwords in user identification

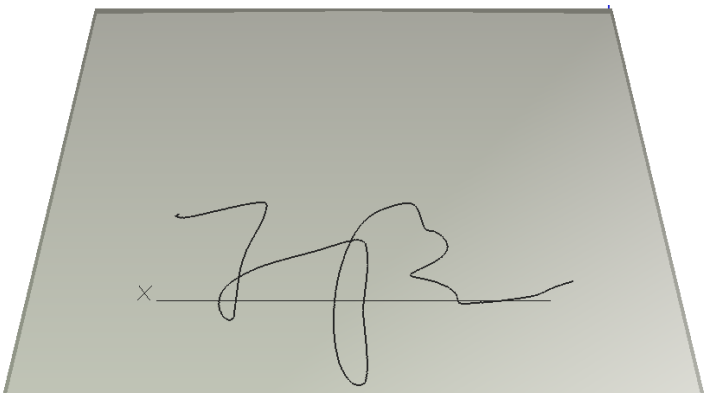

Figure 2.6: Pre-defined Signature

and authentication. The last task simulates a forgery attack and examines the haptic password's resistance to such an attack.

*Subjects Demographics*

Our analysis is based on data collected from experiments involving nine participants. This study was approved by the University of Washington Institutional Review Board approval (#46946 - EB). All of our subjects were undergraduate and graduate students from the Electrical Engineering department, ranging in age from 22 to 35 years. There were eight right-handed participants and

one left-handed participant. Most of the subjects had not used a stylus haptic device prior to the experiments.

For the forgery task, a genuine signature to be forged was provided. Thirty sets of genuine signature data were collected on three different days.

### *2.4.4 Results*

*Relative Password Variation*

To evaluate the performance of the proposed password system, using the collected experimental data, we consider the relative variation of the different types of passwords. The level relative variation for each task is defined as

$$PV_i = \frac{\sum_{j=1}^{N} ||F_{i,j} - \bar{F}_i||_2}{N} \times \frac{1}{\min\limits_{j \neq i} ||\bar{F}_i - \bar{F}_j||_2} \tag{2.7}$$

where

$PV$: Password Variation

$N$: Number of trials

$F_{i,j}$: Feature vector of user i, trial j

$\bar{F}_i$: Mean feature vector of user i.

The relative password variation is the variation of one subject's password relative to the distance to its most similar subject's password. The smaller the variation is, the better identification and authentication (classification) performance will be.

Table 2.1 shows the relative password variation among 9 subjects for the first three tasks. We notice that among these, the signature task varies the least. Probably the main reason for this outcome is that most subjects are familiar with signing their own signatures and the mental effort required to finish the task is lower than the other two. The intra-subject performance and execution of this task is thus more consistent. Therefore, in a password verification scheme, signature data generates better performance than the other two methods examined.

Table 2.1: Relative Password Variation

| Task | subj1 | subj2 | subj3 | subj4 | subj5 | subj6 | subj7 | subj8 | subj9 |
|---|---|---|---|---|---|---|---|---|---|
| L-shape | 1.108 | 1.011 | 0.356 | 0.659 | 0.464 | 1.138 | 0.553 | 0.746 | 0.866 |
| Seahawk | 0.671 | 1.164 | 0.231 | 0.884 | 0.765 | 0.683 | 0.872 | 0.897 | 1.017 |
| Signature | 0.632 | 0.572 | 0.321 | 0.619 | 0.456 | 0.503 | 0.622 | 0.580 | 0.710 |

*User Classification and Authentication*

For user classification and authentication, the ANN network was trained using $M$ trials of each subject while the remaining $10-M$ trials were used for evaluation of the method. All $\binom{10}{M}$ traning and testing sets combinations were examined. Classification performance was obtained by averaging all combinations results.

As mentioned in Section V, the input of the neural network is the feature vector of each trial and the output $O$ is a 9 dimensional vector, with each element representing the likelihood that the data is from a particular subject.

In the classification task, the data is classified as generated by subject $i$ if

$$i = arg\max_j O(j) \tag{2.8}$$

In the authentication task, the data will be authenticated if the likelihood is greater than threshold $t$; that is, if

$$O(i) > t \tag{2.9}$$

The classification performance, when the number of training sets used $M$ varies from 3 to 7 for the first three tasks is shown in Table 2.2. Even for the simplest task, the L-shape pattern, the classifier successfully classified more than 90% of data when 4 or more training sets are used. When the tasks (writing the word *'SEAHAWK'* and the subject's personal signature) becomes more complex and personalized, the method successfully classifies almost all subjects when 4 or more training sets are used.

Table 2.2: Classification Performance

| Task | Number of Training Sets | | | | |
|---|---|---|---|---|---|
| | 3 Sets | 4 Sets | 5 Sets | 6 Sets | 7 Sets |
| L-Shape | 87.35% | 90.24% | 91.26% | 93.29% | 95.46% |
| Seahawk | 93.02% | 96.25% | 97.57% | 98.73% | 98.89% |
| Signature | 99.19% | 99.26% | 99.86% | 100% | 100% |

The ANN classifier training was done on a Macbook Pro with 2.2 GHz Intel Core i7 and 16 GB memory. Matlab R2014b Neural Network toolbox is used. The average training time (in second) for each training setting is shown in Table 2.3.

Table 2.3: Classifier Training Time

| Task | Number of Training Sets | | | | |
|---|---|---|---|---|---|
| | 3 Sets | 4 Sets | 5 Sets | 6 Sets | 7 Sets |
| L-Shape | 2.92s | 5.11s | 5.88s | 8.08s | 9.15s |
| Seahawk | 2.43s | 3.06s | 3.32s | 3.63s | 4.64s |
| Signature | 4.60s | 5.08s | 6.99s | 10.79s | 12.60s |

Figure 2.7 shows the Receiver Operating Characteristic (ROC) curve of the authentication performance for one training and testing set combination (first 7 trials as training set and last 3 trials as testing set). We notice that both the *'SEAHAWK'* and signature task have generated ideal performance and the performance of L-shaped pattern is acceptable.

Our experimental results indicate that even though all subjects used similar looking patterns in task 1 and task 2, they can still be identified and authenticated. It is how the user interacts with the haptic password system, rather than the shape of the password, that makes the user identifiable.

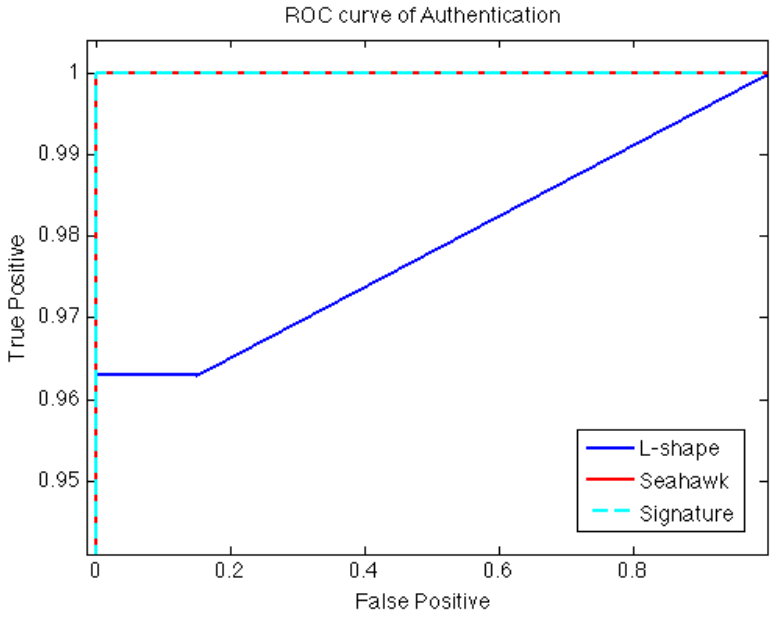


Figure 2.7: Authentication ROC Curve for 3 Tasks

*Forgery Attack Resistance*

Next, the resistance of the haptic password system to forgery attack is analyzed. Subjects were given an image of a genuine signature to simulate a forgery attack. They were then instructed to forge the signature while an image of the genuine signature was presented to them. The network was trained by using all genuine signatures (10 data sets per subject), including the data from the user whose signature was to be forged. The testing data was obtained from forged signatures generated by 9 subjects (10 forged signatures each) and 20 genuine signatures.

In order to explore the attack resistance of the haptic-based identification system, three different feature vector sets were used. The first one is the original data that contains all 8 dimensional features. In the second, only pen tip velocity features ($V_1 = (f_1, f_2, f_3)$) are used. Finally, for the third, only the force and stylus orientation features($V_2 = (f_1, ..., f_5)$) were used. Practically, for a password system, certain levels of false negative (genuine signature regarded as fake) are acceptable (requiring a repeat attempt to authenticate) while false positives (fake signature regarded as genuine)

should be prevented. Therefore, we are focusing on the intercept on the y-axis of the ROC curve.

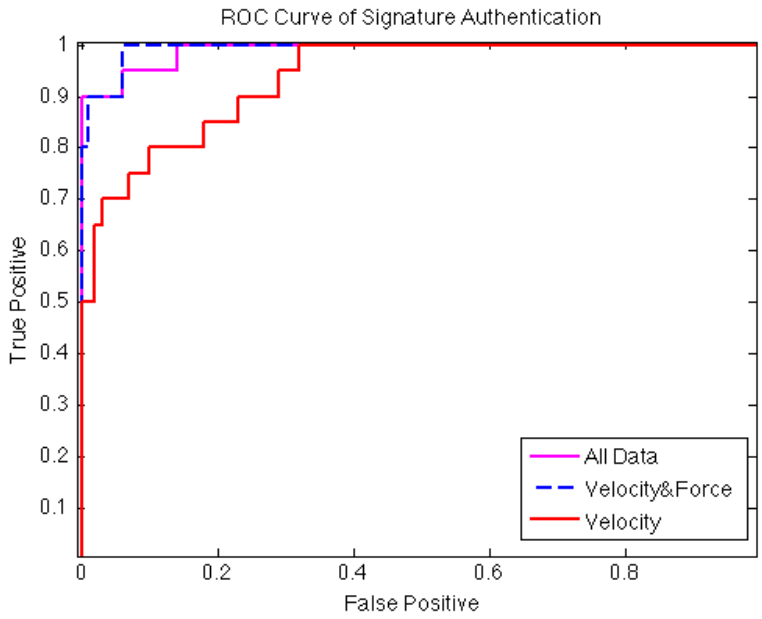


Figure 2.8: Authentication ROC Curve for Forgery Attack

As shown in Figure 2.8, using only velocity data generates the worst performance (50%) while using all of the 8 dimensional data perform the best (90%), which is slightly better than the using velocity and force data only (80%). This demonstrates that extra information obtained from the haptic interaction increases resiliance against forging signatures. With just an image of the victim's signature picture, it is possible for one to forge a signature that is similar looking to the original. However, the latent information of force applied and orientation of the stylus is unique to the user. This provides protection against forgery attacks.

*Handedness Detection*

Although there was only one left handed subject involved in our experiment, we observed an interesting difference between right handed subjects and the left handed subject. We performed principal component analysis (PCA) on stylus orientation features $(f_6, f_7, f_8)$ and extracted first two

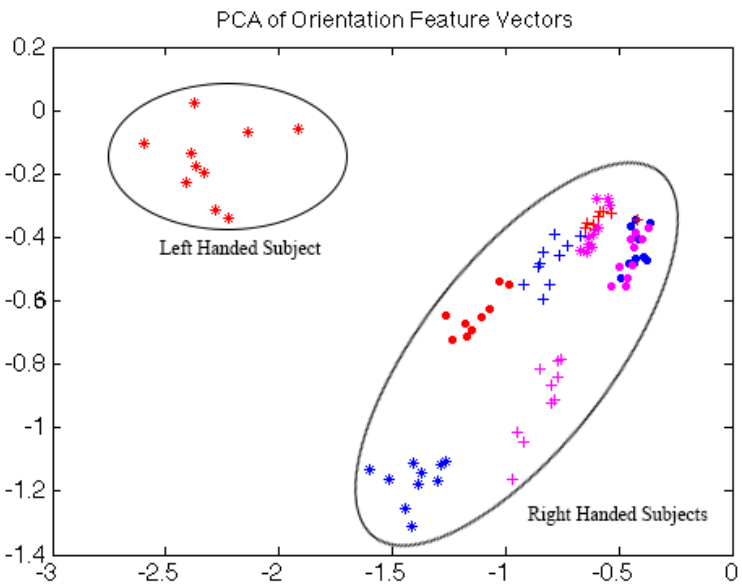


Figure 2.9: PCA of Orientation Feature Vectors

principal components. The result is shown in Figure 2.9, where different color and dots shape are feature vectors obtained from different subjects. The top left red asterisk points are obtained from a left handed subject while all the bottom right points are from right handed subjects.

## *2.5 Haptic Password System on Force Sensitive Mobile Device*

In this section, we extend the haptic password approach and develop the application on a force sensitive mobile device - iPhone 6s. We focus here on the Problem 2: The lack of negative samples to train the classifier, and Problem 3: The randomness of haptic interaction. Moreover, we also quantitatively analyze how the password complexity affects the authentication performance. We propose to use a maximal overlap discrete wavelet transform (MODWT) based feature extraction along with customized classifier and adaptive password update scheme in order to achieve a new secure behavior based haptic password system.

The proposed haptic password system is shown in Fig. 2.10 (training process) and Fig 2.11

(authentication process). The proposed haptic password system consists of three main parts: 1) real-time data collection, 2) feature extraction, and 3) user authentication. In the training process, a user will enter the passoword (i.e. signature) 10 times in order to train the authentication classifier. The mobile app will collect position and force data in real time and extract corresponding features. A classifier will be trained based on the extracted features. In the authentication process, we then use the trained classifier to fulfill the user authentication. We also developed an adaptive template update scheme to accomodate a user's password variation overtime.

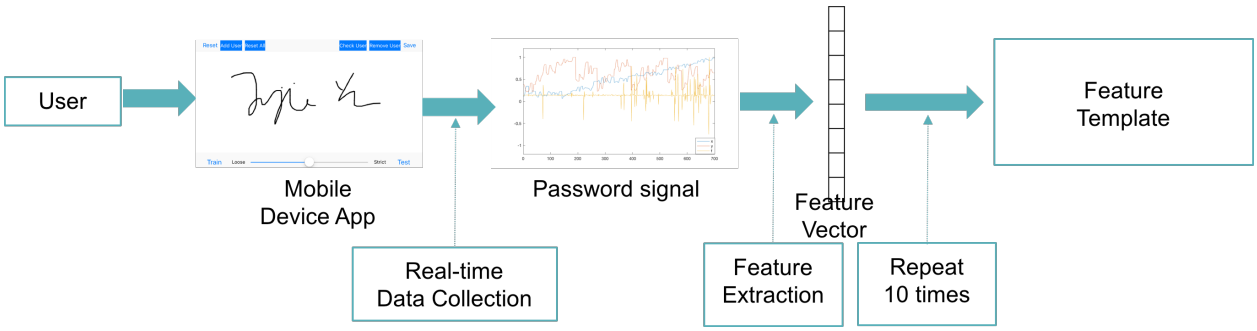


Figure 2.10: Haptic Password System Training Process

### *2.5.1 Experiment and Data Collection*

We conducted human subjects experiments on an iPhone 6s where subjects used their signature as passwords by using their finger to sign on an iPhone (as shown in Fig. 2.12). We also simulated a forgery attack where each subject was asked to forge 4 previous subjects' passwords and tested the proposed system's resistance to such attack.

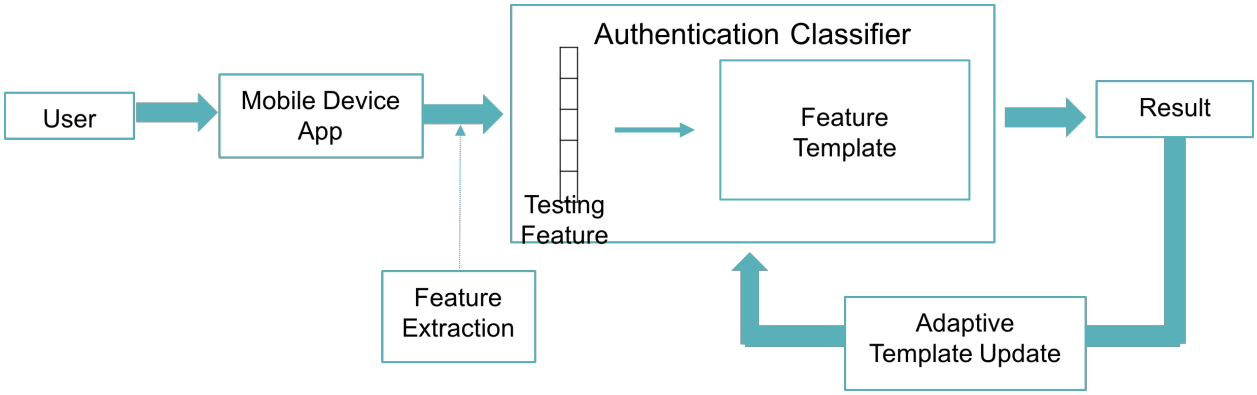


Figure 2.11: Haptic Password Authentication Process

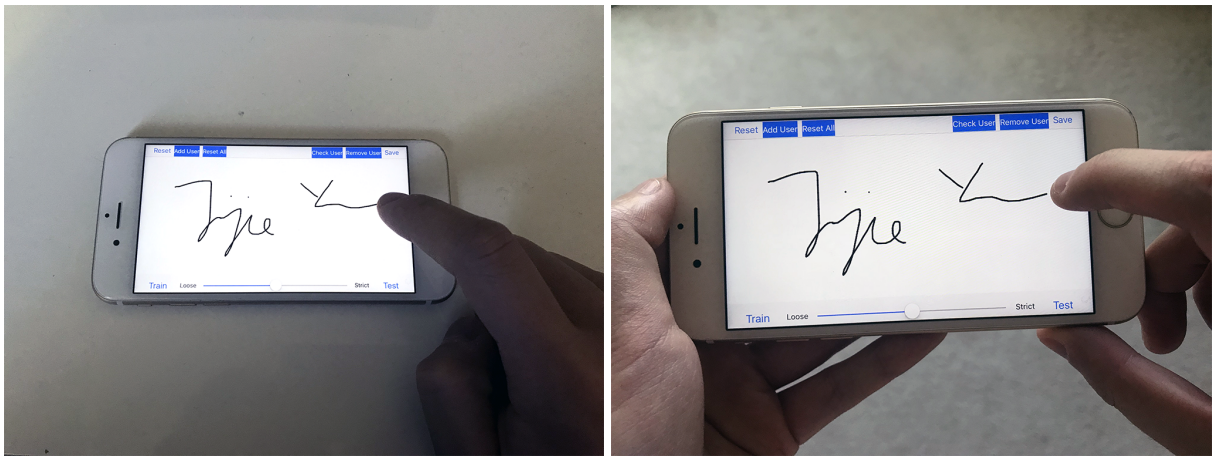

Figure 2.12: Experiment: User Sign Signature in the Static Posture (Left) and the Holding Posture (Right)

*Experiment Setup*

In this experiment, subjects used their signature as a password. First, subjects were asked to explore the app environment and practice their passwords for 5 to 10 times in order to get used to the interface, get rid of the learning effect and generate consistent passwords.

Each subject was asked to fulfill following tasks:

1) Sign the signature with the phone being on the desk (flat surface); (referred as **static signature** in the following context)

2) Sign the signature with the phone being held in hand; (referred as **holding signature** in the following context)

3) Forge other subjects' signatures with the phone being on the desk (flat surface);

4) Forge other subjects' signatures with the phone being held in the hand;

Task 1) and 2) aim to test how different postures affect the authentication results and task 3) and 4) simulate a forgery attack and test system resistant to such type of attack. The detailed attack model will be discussed in the following section.

For each subject, the experiment is completed in two consecutive days to examine the system authentication performance over time. In day 1, the subject completed all tasks listed above, while on day 2, only task 1) and 2) were completed.

*Attack Model*

The goal of attacks against authentication system is to impersonate a specific user. In this work, we mainly focus on the forgery attack where malicious individual pretends to be someone else by providing a forged password of a legitimate user.

**Forgery Attack**: The malicious individual is able to watch how the victim enters the password and generate forgeries based on the observation.

In order to simulate such an attack, all genuine passwords are video recorded in real time. Each subject (simulated 'malicious individual') will be able to watch videos of previous subjects entering

their password and forge those passwords based on the observation. In this way, the simulated 'malicious individual' has access to not only the static and graphical property but also the dynamic property of each password.

.

*Data Collection*

In this experiment, we use an iPhone 6s to collect user haptic passwords data. The 3D touch technology allows us to collect not only the contact position information but also how much force is applied when the users enter their haptic password.

We collect the following data in real time:

1) Position of contact position on screen $(x, y)$;

2) Applied forces $(f)$;

All data is recorded at 60 Hz. The iPhone 6s app starts recording data when the user makes contact with the screen and stops when the user press the 'save' button. Each password signal data is then truncated to the point where the last contact happens.

Besides the data collected as shown above, we generate a set of extra information from the contact position data $(x, y)$ at time $t$ as follows:

1) Signature trajectory velocity

$$v_x(t) = x(t) - x(t-1), v_x(0) = 0 \tag{2.10}$$

$$v_y(t) = y(t) - y(t-1), v_y(0) = 0 \tag{2.11}$$

2) Stroke Acceleration

$$a(t) = \sqrt{v_x^2(t) + v_y^2(t)} - \sqrt{v_x^2(t-1) + v_y^2(t-1)}, a(0) = 0 \tag{2.12}$$

3) Trajectory direction

$$\theta(t) = atan(\frac{v_y(t)}{v_x(t)}), \theta(0) = 0 \tag{2.13}$$

4) Trajectory direction change

$$\omega(t) = \theta(t) - \theta(t-1), \omega(0) = 0 \tag{2.14}$$

The state vector is then constructed as $s = (x, y, f, v_x, v_y, a, \theta, \omega)$.

In summary, for each subject, the experimental data collected includes:

1) 30 genuine static signatures (Day 1: 20 sets, Day 2: 10 sets)

2) 30 genuine holding signatures (Day 1: 20 sets, Day 2: 10 sets)

3) 20 static signature forgeries (from 4 different subjects, 5 forgeries per subject)

4) 20 holding signature forgeries (from 4 different subjects, 5 forgeries per subject)

More specifically, for the simulated forgeries attacks, each subject will be asked to watch videos of the previous 4 subjects' genuine signatures, and generate corresponding forgeries. 5 forgeries per subject per posture(i.e. $i^{th}$ subject will forge $(i-4)^{th} \sim (i-1)^{th}$ subject's signatures). In this way, each subject's genuine signatures in each posture will be forged 20 times by 4 different subjects.

*Training, Testing and Evaluation*

Given the experiment dataset, we aim to answer the following questions:

1) How does a user's password day-to-day variation affect the authentication performance?

2) Can we achieve similar authentication performance when the user enters the password in different postures?

3) How resistant is the authentication to forgery attacks?

In order to answer the question above, we divide the dataset into a training set and a testing set.

The first 10 static/holding signatures in day 1 are used to train the corresponding classifiers and tune their parameters.The rest 10 static/holding signatures on day 1 are used as the same-day testing set while 10 static/holding signatures on day 2 are used as the second-day testing set. This allows us to explore the effect of passwords day-to-day variation on the authentication accuracy.

*Subjects Demographics*

Our analysis is based on data collected from experiments involving 29 participants. The detailed demographics of all subjects is shown in Table 2.4. The subject racial and signature language distribution are shown in Fig. 2.13 and Fig 2.14 respectively.

Table 2.4: Subjects Demographics

| | |
|---|---|
| Sample Size | 29 |
| Sex | 14 Females; 15 Males |
| Age Range | 18 to 62 |
| Age (Mean $\pm$ SD) | 26.5 $\pm$ 8.7 |
| Handedness | 4 Left; 25 Right |

### *2.5.2 Feature Extraction*

In order to realize user authentication given the haptic passwords, the first step is to extract features. The choice of elements in the feature vector significantly affects the performance of the classifier. In our previous work [84], we implemented discrete wavelet transform (DWT) to fulfill the feature extraction of the signature signal. The key benefit of the DWT is that it captures both frequency and localized (in time) information. However, there is a constraint for DWT that the length of the signal has to be multiples of a power of two. If we resample the password signal to meet this requirement, this inevitably alters the original property of the given password signal and potentially increases the similarity between genuine passwords and forgeries (since the original length of genuine passwords and forgeries is most likely different, while after resampling, they will be the same). To avoid this problem, in this work, we use the maximal overlap discrete wavelet transform (MODWT)[54], a modified discrete wavelet transform, to deal with the signature signals. Unlike the DWT, MODWT is defined naturally for all signal lengths. This allows us to perform feature extraction on the original

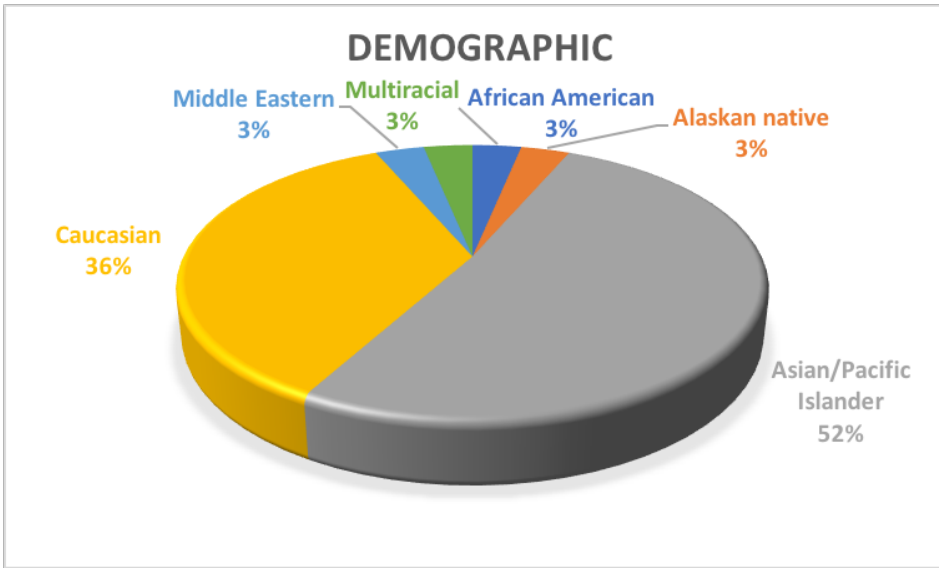


Figure 2.13: Subjects Demographic Distribution

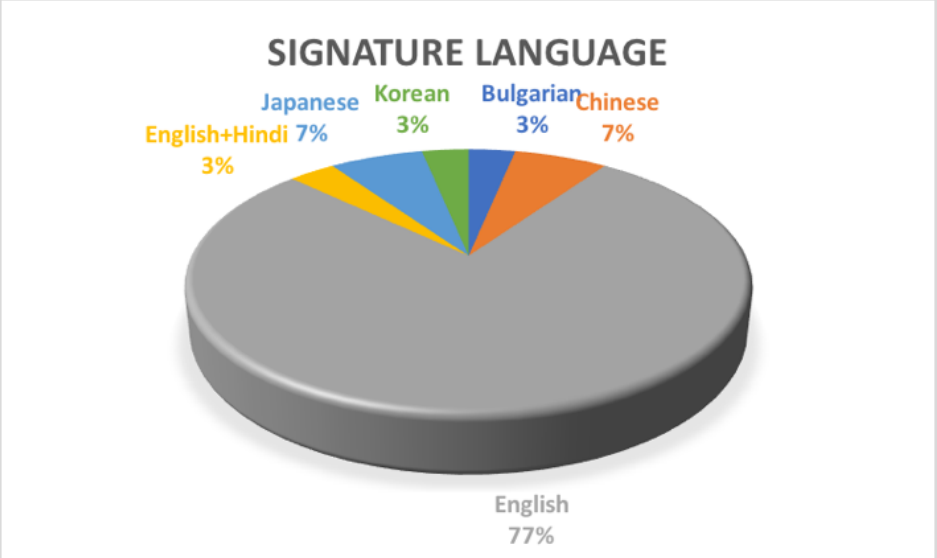


Figure 2.14: Subjects Signature Language Distribution

signature signal without resampling.

Additionally, in order to enhance the stored feature template security, the proposed feature extraction process is non-invertible. In this way, even if the malicious party is able to hack the template database via template attack, it is impossible to reconstruct the original password from the features. This property mitigates the template attack against the proposed haptic password system.

*Maximal Overlap Discrete Wavelet Transform*

In this section, we briefly review the general concept of MODWT. Similar to the DWT, the MODWT coefficient of signal $X$ is calculated by passing it through a series of filters generated from a mother wavelet filter. The mother wavelet filter $g$ is a low-pass filter that satisfies the standard quadrature mirror condition [54][71]

$$G(z)G(z^{-1}) + G(-z)G(-z^{-1}) = 1 \tag{2.15}$$

where $G(z)$ denotes the z-transform of the filter $g$. Its complementary high-pass filter can be obtained as

$$H(z) = zG(-z^{-1}) \tag{2.16}$$

These mother wavelet filters are then used to generate the series of scaling filters $H$ and wavelet filter $G$

$$H_{i+1}(z) = H(z^{2^i})G_i(z) \tag{2.17}$$

$$G_{i+1}(z) = G(z^{2^i})G_i(z) \tag{2.18}$$

with initial condition $G_0(z) = 1$.

Let $h_j(k)$ and $g_j(k)$ be the time-domain representation of $H_j(z)$ and $G_j(z)$ respectively. The MODWT scaling filter $\widetilde{h}_j(k)$ and wavelet filter $\widetilde{g}_j(k)$ are:

$$\widetilde{h}_j(k) = \frac{h_j(k)}{\sqrt{2}} \tag{2.19}$$

$$\widetilde{g}_j(k) = \frac{g_j(k)}{\sqrt{2}} \tag{2.20}$$

Let $X$ be a time series of length $N$. Similar to standard DWT, the MODWT scaling coefficient $\widetilde{V}_j(k)$ and wavelet coefficient $\widetilde{W}_j(k)$ at the $j^{th}$ level is calculated as shown in (12) and (13)

$$\widetilde{W}_j(k) = \sum_{l=0}^{L_j-1} \widetilde{h}_j(l) X((k-l) \ \ mod \ \ N) \tag{2.21}$$

$$\widetilde{V}_j(k) = \sum_{l=0}^{L_j-1} \widetilde{g}_j(l) X((k-l) \ \ mod \ \ N) \tag{2.22}$$

where $L_j$ is the width of $j^{th}$ level filter. Here $L_j = (2^j - 1)(L-1) + 1$, and L is the width of the initial mother wavelet filter. Figure 2.15 shows the block diagram of the MODWT process.

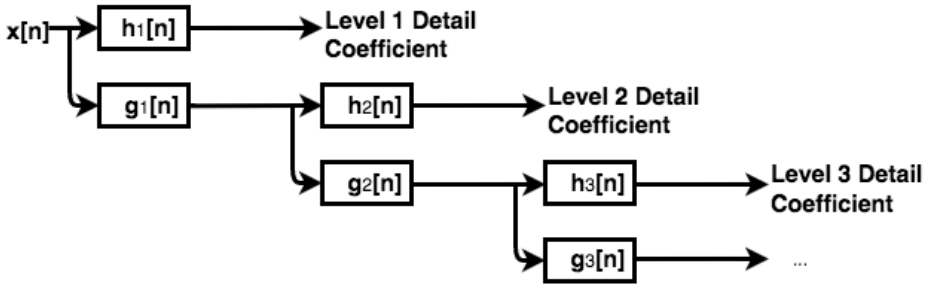


Figure 2.15: MODWT sub-band decomposition

The input signal $X$ is decomposed into high and low frequency components at each level and they are regarded as detail coefficient and approximate coefficient of that corresponding level respectively.

*Feature Vector*

The feature vector for each signature signal is obtained in the following steps:

1. The MODWT is applied to each channel (position, velocity, the force applied, acceleration, direction and direction change) in the state vector $s$ separately. For each channel, 5 levels of

decomposition are accomplished and we obtain 5 levels of wavelet coefficients $W_1 \sim W_5$ and level 5 scaling coefficients $V_5$.

2. The following statistical features are used to represent the time-frequency distribution of the signature signals:

- Mean of the absolute values of the coefficients in each sub-band.
- Standard deviation of the absolute values of the coefficients in each sub-band.
- Maximum of the absolute values of the coefficients in each sub-band.
- Ratio of the absolute mean values of adjacent sub-bands.

More specifically,for $i = 1,2,3,4$,we define

$$v_i = [mean(|W_i|), std(|W_i|), max(|W_i|), mean(|W_i|)/mean(|W_{i+1}|)] \tag{2.23}$$

for $i = 5,6$, we define

$$v_5 = [mean(|W_5|), std(|W_5|), max(|W_5|), mean(|W_5|)/mean(|V_5|)] \tag{2.24}$$

$$v_6 = [mean(|V_5|), std(|V_5|), max(V_5)], \tag{2.25}$$

Therefore, the feature vector of each channel in signature signal $s$ is $f_i = [v_1, v_2, v_3, v_4, v_5, v_6]$. The length of $f_i$ is 23. Then the complete feature vector of each signature signal is obtained by concatenating all 8 channels together as $F = [f_1, f_2, ..., f_8]$. The length of F is $23 \times 8 = 184$.

The statistics of wavelet coefficients in each sub-band are calculated as features for haptic passwords. Our assumption is that the statistical analysis is non-invertible as it is impossible to reconstruct the complete sub-band coefficient from the statistics stored in the feature vector. Therefore, the feature extraction process non-invertible, which means even if the adversary party hack the feature database, they are unable to reconstruct users' original password information. This provides an extra level of security protection against attacks for the haptic password system.

### *2.5.3 User Authentication*

As mentioned in Problem Statement section, in order to realize user authentication, we need to deal with the following three problems: 1) the lack of negative samples to train the classifier; 2) the randomness of the human, and 3) the forgery attacks.

First, we need to develop a classifier to authenticate users based on the obtained feature vectors. However, most classic classifiers, such as support vector machines (SVM), artificial neural networks (ANN) and decision trees, are highly dependent on both positive and negative samples in the training process. On the other hand, in our application scenario, only positive samples (genuine signatures) are available. It is inappropriate to use forgeries as negative samples because it is not feasible to obtain forgeries of each user's signature in the real-life application due to the confidentiality of the users' passwords. Additionally, although using other people's genuine signatures as negative samples is feasible, this will potentially make the classifier underestimate the difficulty of the classification problem and thus be unable to achieve good forgery-proof performance.

Therefore, in this work, we develop an authentication classifier without using negative samples. The authentication result is based on the distance between the testing feature vector and the feature vectors in the template set. The template set is generated in the training process. The authentication process based on two distance metrics, Euclidean distance and Hamming distance, are developed and tested.

#### *Euclidean Distance*

In this section, we propose to calculate the matching score based on the Euclidean Distance between the testing password and the password template.

First, the given user's training password feature set is normalized, and the mean and standard deviation of the training feature set is stored to normalize the testing data. Because the dimensionality of the feature vector is large (23 per channel), simply treating each dimension equally for all different users is not appropriate. We formulate the following optimization problem to find the weighting for each dimension such that for a given user, the signature features in the training set are weighted in

such a way that makes the features most consistent to his/herself.

First, given vector $X = [x_1, x_2, \ldots, x_n], Y = [y_1, y_2 \ldots, y_n]$, we define operation $\otimes$ as $X \otimes Y = [x_1 y_1, x_2 y_2, \ldots, x_n y_n]$. Let the weighting parameter for the $s^{th}$ user be $w_s = [w_{s,1}, w_{s,2}, \ldots, w_{s,n}]$

$$\begin{aligned} \underset{w_s}{\text{minimize}} \quad & \sum_{i=1}^{N} \sum_{j=i+1}^{N} d(w_s \otimes F_{s,i}, w_s \otimes F_{s,j}) \\ \text{subject to} \quad & w_{s,i} \geq 0,\ i = 1, \ldots, n. \\ & \sum_{i=1}^{n} w_{s,i} = 1 \end{aligned}$$

where $N$ is the number of signatures in training set, $n$ is the dimensionality of the feature vector and $F_{s,i}$ is the $i^{th}$ feature vector in the training set of the $s^{th}$ user. $d(X,Y)$ calculates the Euclidean distance between vector $X$ and $Y$.

For the password authentication, we use the passwords in the training set as templates and match the testing password to the templates in order to obtain the matching score $\lambda$. For the user $s$ authentication, given the genuine password template set $\{F_{s,i}\}$ and testing password $F_{test}$, we are able to obtain $d_i = d(w_s \otimes F_{test}, w_s \otimes F_{s,i})$ and $D_E = [d_1, d_2, ..., d_N]$. The distance set $D_E$ contains the Euclidean distance between the testing password and each template password. We can then generate the matching score based on the distance set $D_E$.

However, due to the random changes in human signatures, simply calculating the matching score by summing all the distance together may not be able to generate a reliable result. 'Bad' passwords can be generated during the training process. We anticipate that users may enter poorly in some of the passwords in the training set which is inconsistent with the genuine ones. When calculating the matching score, if we use the entire training set as templates, those poorly entered passwords will potentially increase the matching score of a genuine testing password and degrade the authentication performance.

Therefore, to overcome this issue, we define the matching score as follows. We define operation $Findmin(S,k)$ as find a subset of $S$ that contains $k$ smallest elements in $S$. The matching score $\lambda$ of the given testing password is calculated as in (17)

$$\lambda = \sum Findmin(D_E, k) \tag{2.26}$$

where $k \in [1,2,...,N]$ is a tuning parameter. Smaller $\lambda$ means that the testing password is more similar to the genuine ones in the template set. The testing password will be authenticated when the matching score is below the predefined threshold $T_{D_E}$.

With the tuning parameter $k$, testing passwords will be matched to those 'good' templates. By doing so, we will be able to mitigate the effect of the human's randomness in the training phase.

*Hamming Distance*

In this section, we propose to calculate the matching score based on the Hamming Distance between the testing password and the password template.

Hamming distance between two vectors of equal length is defined as the number of positions at which the corresponding symbols are different. Therefore, in order to use hamming distance, the definition of "different" between features in the testing password feature vector and the password template needs to be defined.

First, the mean and standard deviation of the given user's training password feature set is obtained as $\mu = [\mu_1, \mu_2, ..., \mu_n]$ and $\sigma = [\sigma_1, \sigma_2, ...\sigma_n]$, where $n$ is the dimensionality of the feature vector. We then update the mean and standard deviation in the following ways in order to mitigate the effect of the 'Bad' training password as mentioned in the previous section. We assume that features from those 'Bad' training passwords are outliers. Therefore, for each feature obtained from the $j^{th}$ training password $f_{i,j}$, if $|f_{i,j} - \mu_i| \geq 2\sigma_i$, the corresponding feature is discarded. The updated mean $\hat{\mu}$ and standard deviation $\hat{\sigma}$ is calculated by using the remaining features.

The testing password feature vector $F_{test} = [f_1, f_2, ..., f_n]$ is normalized based on $\hat{\mu}$ and $\hat{\delta}$ as in (2.27)

$$\tilde{f}_i = \frac{f_i - \hat{\mu}_i}{\hat{\sigma}_i}$$
$$\tilde{F}_{test} = [\tilde{f}_1, \tilde{f}_1, ..., \tilde{f}_n] \tag{2.27}$$

If $|\tilde{f}_i| > T_f$, the corresponding feature in the testing password is regarded as different from the password template, where $T_f$ is a pre-defined threshold for feature difference. The Hamming distance $D_H$ between a feature vector of a testing password and the password template set is defined as the number of features that can be regarded as different. The testing password will be authenticated when the Hamming distance $D_H$ is below the predefined distance threshold $T_{D_H}$

*Adaptive template update*

Another issue in the user authentication is the user's password variation over time. In order to address this issue, we developed two adaptive template update schemes for Euclidean distance and Hamming distance based authentication process respectively.

1. Euclidean Distance

The adaptive template update scheme for the Euclidean distance based authentication consists of the following steps:

1) Calculate the matching score $\lambda$ between the given testing password and the password templates as in $(17)$.

2) If matching score is greater than the threshold $T_{D_E}$, reject the given testing password.

3) If the matching score is smaller than the threshold $T_{D_E}$, authenticate the given testing password. Meanwhile, find the password template in the template set that has the largest distance to the current testing password, and replace it with the current new one.

In this way, we will be able to adaptively update the signature template set to accommodate the user's password variation over time.

2. Hamming Distance

The adaptive template update scheme for the Hamming distance based authentication consists of the following steps:

1) Normalize the testing password feature as shown in (2.27) and obtain $\tilde{F}_{test}$. Calculate the Hamming distance $D_H$ between the given testing password and the password templates.

2) If $D_H$ is greater than the threshold $T_{D_H}$, reject the given testing password.

3) If $D_H$ is smaller than the threshold $T_{D_H}$, authenticate the given testing password. Let $\Delta = F_{test} - \hat{\mu}$

4) Update $\hat{\mu}_{new} = \hat{\mu} + \eta\Delta$, where $\eta$ is a tuning parameter that represents the adaptive rate.

By doing so, the template mean is shifted toward the feature that generated from the new authenticated password. This allows us to accommodate the user's password variation over time. We keep the standard deviation $\hat{\sigma}$ unchanged through the adaptive update process because it is obtained from the training set which is generated by the corresponding user within a short period of time and it represents the size of the user's password interval. Our assumption is that the user's password interval will not change over time and thus only the template mean is updated through the process.

### *2.5.4 Results*

*Parameter Tuning*

For the user authentication, we first focus on tuning the parameter in both Euclidean distance based and Hamming distance based methods in order to achieve best authentication performance. Therefore, a leave-one-out cross-validation is conducted for both tasks (static signature, and holding signature) by using the training data only for both distance based methods. We use the authentication accuracy when the false acceptance rate (FAR) is 0 % (no forgery is authenticated) as a metric to determine the parameter.

First, for both methods we need to determine which mother wavelet to use in the feature extraction process. Therefore, we tested Haar wavelet, Daubechie wavelet (DB4 and DB8), least asymmetric wavelet (LA8 and LA16) and coiflet wavelet (C6 and C12) as the mother wavelet.

Next, for Euclidean distance based method, the number of nearest template feature set $k$ used (as shown in (17)) is varied from 2 to 9. The corresponding cross-validation results for all 3 tasks are shown in Fig2.16 - 2.17

We notice that for both static and holding signature when we use Coif12 as mother wavelet and

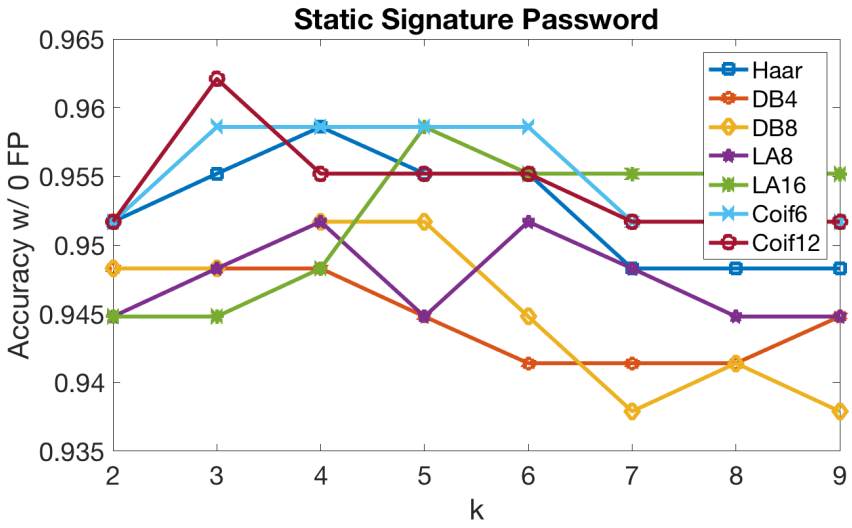


Figure 2.16: Euclidean distance based parameter tuning, Static signature

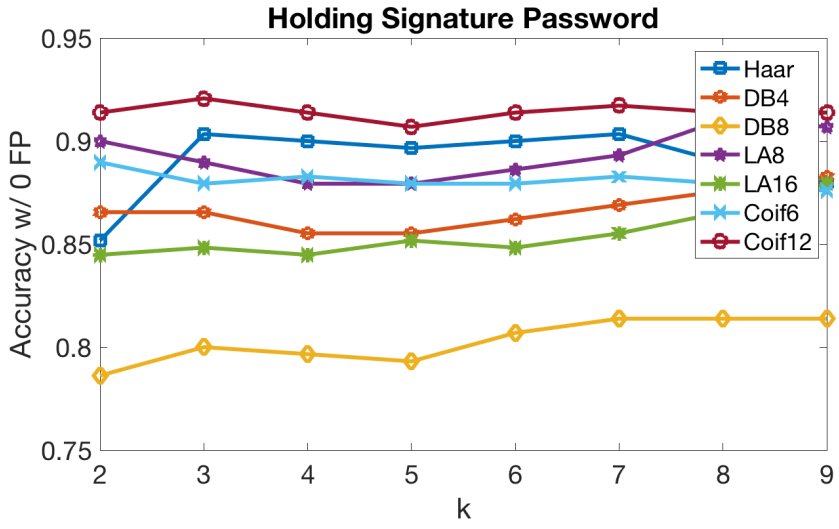


Figure 2.17: Euclidean distance based parameter tuning, Holding signature

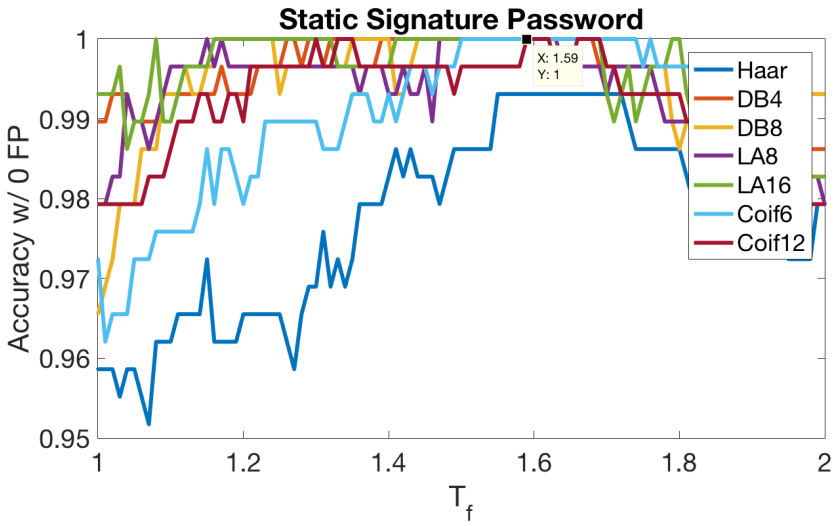


Figure 2.18: Hamming distance based parameter tuning, Static signature

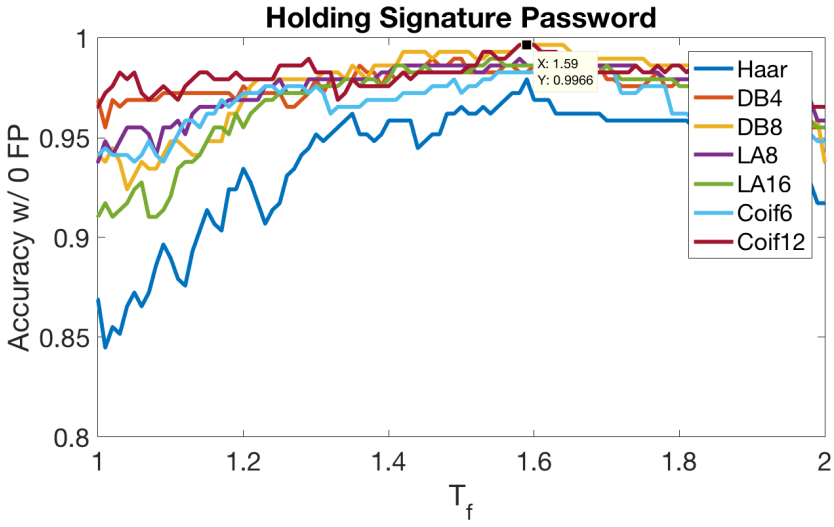


Figure 2.19: Hamming distance based parameter tuning, Holding signature

$k = 3$, the best authentication performance can be obtained as the accuracy rate is largest. Therefore, we keep these settings for both tasks respectively in the remaining context.

For the Hamming distance based method, we also need to determine the threshold $T_f$ to define feature difference. $T_f$ is varied from 0 to 5 and the corresponding cross-validation results (around peak) for all 3 tasks are shown in Fig. 2.18 - 2.19

In this case, we notice that for both tasks, when we use Coif12 as mother wavelet and $T_f = 1.59$, best authentication performance is achieved. Therefore, we keep the setting for Hamming distance based method in the remaining context.

*Authentication performance*

To evaluate the authentication performance, we evaluate on the genuine testing sets and the corresponding forgeries. Our evaluation metric includes the false acceptance rate (FAR), the false rejection rate (FRR), and the equal error rate (EER). FAR is the percentage of the forgeries from malicious individuals that are accepted as genuine passwords by the authenticator. FRR is the percentage of the genuine passwords from a legitimate user that are rejected by the authenticator. In most classification and authentication system, there is a trade-off between FAR and FRR. By adjusting the threshold so that the classifier is more strict and sensitive, one can reduce the FAR since fewer forgeries will be accepted by the system. However, FRR will increase inevitably as more genuine passwords will be rejected due to the strict classifier. Therefore, in order to address this trade-off, we use EER to represent the authentication performance. The equal error rate is the rate at which both FAR and FRR are equal. Additionally, as an authentication system, especially when dealing with life-critical systems, false accepts are far more detrimental than false rejects. Therefore, we also include the authentication accuracy when FAR is 0 as a performance metric. Table 2.5 and 2.6 represent the authentication performance for Euclidean distance based and Hamming distance based method respectively.

First, when no adaptation is applied to the authentication process, the authentication performance in the day 2 session degraded significantly comparing to day 1 session for all cases. This shows that human haptic passwords do vary overtime due to the human's randomness and it is necessary

Table 2.5: Euclidean Distance Based Authentication Performance

| Task | Session Day | W/O Adaptive | | W/ Adaptive | |
|---|---|---|---|---|---|
| | | EER | Accuracy w/ FAR = 0 | EER | Accuracy w/ FAR = 0 |
| Static Signature | Day 1 | 2.07% | 84.83% | 1.38% | 94.14% |
| Static Signature | Day 2 | 5.17% | 45.86% | 2.07% | 87.24% |
| Holding Signature | Day 1 | 3.79% | 81.03% | 2.07% | 90.00% |
| Holding Signature | Day 2 | 8.97% | 40.00% | 4.83% | 74.48% |

Table 2.6: Hamming Distance Based Authentication Performance

| Task | Session Day | W/O Adaptive | | W/ Adaptive | |
|---|---|---|---|---|---|
| | | EER | Accuracy w/ FAR = 0 | EER | Accuracy w/ FAR = 0 |
| Static Signature | Day 1 | 2.84% | 83.79% | 0.96% | 95.86% |
| Static Signature | Day 2 | 6.71% | 60.34% | 3.26% | 88.97% |
| Holding Signature | Day 1 | 4.47% | 78.97% | 2.33% | 90.34% |
| Holding Signature | Day 2 | 9.95% | 43.79% | 6.09% | 77.24% |

to compensate for it. On the other hand, the proposed adaptive template update schemes enhance the authentication performance for both Euclidean distance based and Hamming distance based methods, especially for the day 2 sessions. This outcome demonstrates that the proposed template adaptation schemes for both methods are able to compensate for the user's password variation over time and enhance the system authentication performance.

The Hamming distance-based method generates slightly better authentication performance than Euclidean distance-based method. The reason for this may be because the Hamming distance based method handles the following 2 scenarios better than the Euclidean distance-based method. First, consider a simplified example as shown in Fig. 2.20, where the circle represents the genuine template feature vector from one user, the red cross represents the genuine testing feature vector and the red asterisk represents a forgery feature vector. When using Euclidean distance-based method, since we use the parameter $k = 3$, both the genuine testing feature vector and the forgery testing feature vector will be matched to 3 templates in the top right and similar matching score will be generated. However, intuitively, the genuine testing feature should be considered as more similar to the template feature. On the other hand, by using Hamming distance based method, both dimensions of the genuine testing feature are within the range of $T_f$ so the distance to the template is 0, while the distance between the forgery testing feature and the template is 2 as both dimensions of the forgery feature is outside the range of $T_f$.

Second, Hamming distance based method is less sensitive to a single (or few) dimension of feature that has extremely large offset comparing to the template features. This property well fits the proposed authentication method. Since the wavelet-based feature extraction captures both frequency and localized (in time) information, a feature vector, which has only one (or few) dimension of feature with the large offset to the template, can still be a genuine one, as the user might do something not consistent locally. On the other hand, if multiple dimensions of a testing feature have medium offset, the testing feature is more likely generated from a forgery, since medium offset in multiple dimensions of features implies the global difference. However, when using the Euclidean distance based method, both testing features mentioned above will generate similar matching score as the Euclidean distance between both features and the template features are similar. On the other

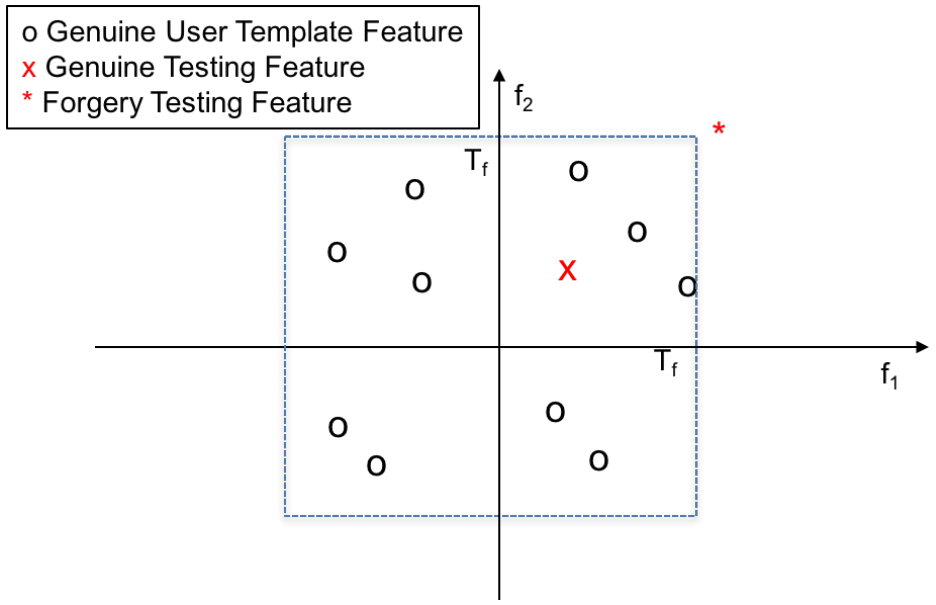


Figure 2.20: Simplified Example

hand, the Hamming distance based method is able to distinguish these two cases. The Hamming distance between the testing feature with a single (or few) large offset and template features is small, while the hamming distance between the testing feature with multiple medium offsets and template features is large. This helps improve the authentication performance.

Lastly, static signatures slightly outperform holding signatures (static means the device is on a flat surface) in authentication accuracy and it is because the phone is less stable when being held by the using during the password entering phase. We observed that user may vary the way how they hold the phone and inconsistency will degrade the authentication accuracy.

*Effect of password complexity*

In this section, how the password complexity affect each individual subject authentication performance is analyzed. Similar to alphanumerical passwords, we anticipate that the complexity of the user's haptic password will affect the authentication performance. Therefore, to quantitatively

evaluate the effect of the password complexity on the performance of the haptic passwords system, the signature complexity $\delta$ of the user $i$ is defined as

$$\delta_i = \frac{s_i}{s_{max}} + \frac{x_i}{x_{max}} + \frac{a_i}{a_{max}} + \frac{d_i}{d_{max}} \tag{2.28}$$

where

1) $s$ represents the average number of strokes in the given user's password in the training set;

2) $x$ represents the average number of trajectory intersections in the training set;

3) $a$ represents the average number of acceleration zero crossings in the training set;

4) $d$ represents the portion of curved trajectory in the password. The reason to add $d$ to the signature complexity is that many subjects in our experiments expressed that it is more difficult to mimic curved lines, compared to straight lines and vertices (i.e. sharp turnings). The portion of curved trajectory in the signature is calculated by averaging the number of medium trajectory direction changes in the training set. The medium trajectory direction change is defined as $|\omega(t)| \in [\pi/6, \pi/4]$;

5) $[\cdot]_i$ represents the corresponding value of user $i$ and $[\cdot]_{max}$ represents the largest value across all users within the same task.

The password complexity $\delta \in [0,4]$, as all 4 metrics listed above are rescaled to $[0,1]$ based on the maximum value in the corresponding metric among all subjects. The larger the complexity is, the more complex the user's signature will be.

Fig. 2.21 shows the complexity histogram of static signature and holding signature tasks.

Intuitively, a simple password is more likely to be forged. In order to prove this intuition, we first define the forging difficulty of each user's password as the smallest Hamming distance any forgery can achieve among all 20 forgeries in the corresponding task. The smaller the forging difficulty is, the more likely the corresponding password can be forged.

Table 2.7 illustrate how the password complexity affects the corresponding forging difficulty. We notice that for both static and holding signature password, the forging difficulty increases when the password complexity increase. Therefore, this result indicates that in order to achieve good

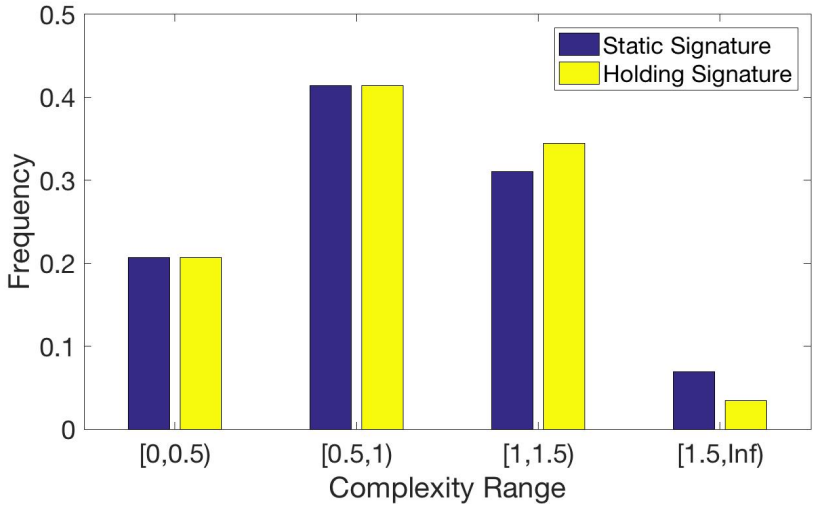


Figure 2.21: Complexity Histogram

Table 2.7: Average Signature Forging Difficulty within Each Complexity Range

| Task | Complexity Range | | | |
|---|---|---|---|---|
| | [0,0.5) | [0.5,1) | [1,1.5) | [1.5,∞) |
| Static Signature | 111.50 | 119.50 | 120.11 | 136.00 |
| Holding Signature | 105.67 | 114.50 | 121.00 | 129.50 |

authentication performance, it is crucial to guarantee that the original passwords in the training set are complex enough. The lack of complexity will increase the probability of the given password being forged. In practical applications, to deal with this issue, if a person's signature is too simple, they could also include writing some numbers, since people do that consistently, in order to increase the password complexity.

*Password Entropy*

The possible password space and scalability is crucial for the password system application. Therefore, in this section, we investigate the password entropy of the haptic password system as an indicator of the system scalability. For a password of Length $L$, the definition of password entropy[22] is shown in (2.29), where $S_i$ is the number of possible symbols at $i^{th}$ location.

$$H = \sum_{i=1}^{L} log_2 S_i \tag{2.29}$$

The haptic password entropy is calculated in the following steps.

1. **Find uncorrelated features to calculate the password entropy.** Since velocity, acceleration, trajectory direction and trajectory direction change as shown in (1) - (5) are generated from the position, we only consider the position and force features. We then calculate pairwise correlation among the selected features and discard those feature with average correlation above 0.3 to obtain uncorrelated features.

2. **Calculate possible symbol size for each uncorrelated feature.** First, for each feature $f_i$, we find the value range $R_i$ among all user as (2.30).

$$R_i = f_{i,max} - f_{i,min} \tag{2.30}$$

We then calculate the standard deviation $\sigma_i$ for each feature $f_i$ for each subject and obtain the largest standard deviation among all the subject as $\sigma_{i,max}$. The possible symbol size $S_i$ for feature $f_i$ is defined as in (2.31)

$$S_i = \frac{R_i}{3\sigma_{i,max}} \tag{2.31}$$

3. **Calculate Password Entropy.** Given the possible symbol size of each feature, the password entropy can be calculated as shown in (20)

By following the above steps, we obtain the haptic password entropy for signature based passwords are 67.45 bits. Compared to the human alphanumerical password with average entropy as 40.54 bits[22], the password entropy of the haptic password is much larger.

### *2.5.5 Discussion*

In this section, we discuss several critical points and limitations in the design of our experiments and study. We also raise possible extensions for the proposed method.

**Cross posture authentication.** As investigated in the previous section, the authentication performance of the signature based password is good within static posture and holding posture. An interesting question is can we generate a unified template that can be used to authenticate users in both postures. However, our analysis shows that when we use the static signature template to authenticate testing holding signature (and vice versa), we are unable to achieve as good an authentication performance as within each posture. The reason for such outcome is two-fold. First, when holding the mobile phone in the hand, the mobile phone position is less stable which makes the signature trajectory deviates from those static signatures. Second, the force applied to the touch screen is different in each posture. For the static signature, the phone is put on a rigid surface while for the holding signature, the phone is held by the user in hand, which can be regarded as an elastic surface. This difference will affect the force applied to the screen as the holding posture will work as a low-pass filter and filter out local force details. Moreover, given the difference between static and holding posture, the proposed adaptive template update scheme might not fit. Nevertheless, however, there is a possible way to overcome this difficulty. With the gyrometer and accelerometer data on the mobile phone, it is relatively easy to determine the posture of the user and the user can be authenticated using the corresponding template based on the posture determined.

**Long term adaptive template update.** In the proposed experiment study, we were only able to conduct a 2-day experiment. We showed that the adaptive template update compensates users' variation over time on the second day. However, we notice the degradation across days still exists. How users' passwords vary over long-term and can the proposed password adaptive template update scheme accommodate the variation is worth further investigation.

**Different forms of the password.** A possible extension of our work is to investigate other forms of passwords besides signatures. Every user potentially has a unique way of handwriting. Therefore, as long as the person does some writing tasks, such as a word, a series of digits or even a doodle of a cat, frequently so that they are consistent, they can be a password. Extra experiments need to be conducted to examine the password authentication performance of various forms.

### *2.5.6 Conclusion*

In this work, a haptic password system on mobile device platform was developed. We investigated whether and how the way a user haptically interact with a force-sensing touchscreen can serve as a behavioral biometric for user authentication. We designed and conducted a human subject experimental study to collect signature based passwords of 29 subjects. We developed a MODWT feature extraction along with customized classifiers to fulfill the user authentication process. In order to accommodate users' password variation over time, we also developed an adaptive template update scheme. The authentication process is able to achieve robust authentication results for the signature-based password, with equal error rates 0%-5% and 75%-96% accuracy with 0 FAR under forgery attacks depending on the experiment setting. Moreover, we investigated the effect of password complexity on the authentication performance and quantitatively demonstrated that the more complex a password is, the less likely it can be forged. We also showed the good scalability of the haptic passwords as the password entropy is much larger than alphanumerical passwords. The results indicate that the developed method is able to generate robust forgery-proof authentication performance for user authentication on the force sensing mobile devices.

Future work, might involve analysis how users' haptic passwords vary over the long term and exploration of the authentication performance of different forms of haptic passwords.

## *2.6 Summary*

In this chapter, we develop a haptic password system on multiple platforms. By implementing wavelet based feature extraction and authentication algorithm, good performance is obtained. Compared to classic alphanumeric password systems, the possible password space is much larger using the haptic information. Furthermore, this method affords the user a way of intuitively memorable passwords that are also complex, modifiable and secure. Additionally, this haptic password system provides resistance to forgery attacks, which is a problem for other security and authentication systems. The development of adaptive template set update also further enhance the system authentication performance by addressing the user haptic password signal variation over time. With the adaptive template set update method, we are able to achieve good authentication accuracy on the genuine signatures without letting any forgery pass the authentication process.

Our experiment results indicate that this haptic password system is secure and robust. Moreover, this system is practical and user friendly. For both platforms, interaction with haptic device and touch screen devices is intuitive for most users. Additionally, the entire process of obtaining the 'password' took only several minutes per user. This included data collection and feature extraction, and the verification process can be done within seconds.

## *2.7 Acknowledgements*

This work is supported by the National Science Foundation, Grant # CNS-1329751, and support from UW CoMotion and the Amazon Catalyst Program. Any opinions, findings, and conclusions or recommendations expressed in this Chapter do not necessarily reflect the views of the funding agencies.

We thank Kevin Huang, for his help with haptic interfaces, Shen Jiang and Jiwei Wang for their help with the execution of the experiments, and Tamara Bonaci and Trang Tran, and Professors Howard J. Chizeck, Blake Hannaford, for all of their help with experimental design, setup, execution, as well as with experimental data analysis.

Table 2.8: Summary of notation from Chapter 2.

| Symbol | Definition |
|---|---|
| $\delta$ | Signature Complexity |
| $\lambda$ | Matching Score |
| $\theta(t)$ | Trajectory Direction at time $t$ |
| $\omega(t)$ | Trajectory Direction Change at time $t$ |
| $a(t)$ | Trajectory Acceleration at time $t$ |
| $D_i$ | Wavelet: Detail Coefficients of level $i$ |
| $f_i$ | Feature Vector of $i^{th}$ Channel in the Haptic Password |
| $F$ | Feature Vector of the Complete Haptic Passoword |
| $g(n)$ | Time Domain Expression of the Mother Wavelet Filter |
| $G(z)$ | Frequency Domain Expresssion of the Mother Wavelet Filter |
| $h(n)$ | Time Domain Expression of the Complementary High-pass Filer |
| $H(z)$ | Frequency Domain Expresssion of the Complementary High-pass Filer |
| $PV$ | Password Variation |
| $V_i$ | Wavelet: Scaling Coefficients of level $i$ |
| $Var$ | Signature Variation |
| $w_s$ | Weighting Parameter for Subject $s$ |
| $W_i$ | Wavelet: Wavelet Coefficients of level $i$ |

# Chapter 3

# CONTINUOUS OPERATOR AUTHENTICATION FOR TELEOPERATED SYSTEMS

## *3.1 Introduction*

Teleoperated robotic systems have become an emerging and popular technology, largely due to several salient benefits of teleoperation. Critically, teleoperation provides a means to extend human capability to spaces in which humans are unable to fulfill the task. The task may, for example, be too dangerous, such as in radiation and chemical environments and disaster scenarios. The task may be at a scale too large or too small for a human to physically accomplish. Finally, consider the case where a human's particular expertise is required immediately but not within proximity, e.g. a specialized surgeon is needed on another continent. In these cases, the use of a remote robotic proxy controlled at a distance via a human operator provides practical benefits that could not be achieved with humans alone. However, the benefit of having geographically distant teleoperators comes with its own set of problems: *what if the security of teleoperated robotic systems is compromised?* Especially in many envisioned high-reward scenarios, basic infrastructure may be limited. Remote robots may have to operate in a harsh environment. The open and relative uncontrollable nature of the communication link between the operator and the robot potentially makes the teleoperated robotic system more vulnerable to various kind of attacks. Moreover, in our prior work [12][11], we discovered that the tension between real-time operation (usability) and security for teleoperated robotic systems may render many existing security techniques infeasible. Many teleoperated robotic systems deal with delicate or critical tasks. It is therefore crucial to make them secure without affecting their usability. The specific solution we found lies in the fact that there is a human operator in the loop. Human operators have unique ways of interacting with teleoperated robotic system[84], and this unique operating signature can be used to identify and authenticate the operator, thus

enhancing the security and privacy properties of teleoperated robotic systems. In chapter 2, a new password system based on the user's behavior biometric is developed to fulfill the initial login authentication task. However, if the malicious party targets the postauthenticated session, such as through communication channel jamming or 'hijacking', initial authentication may not be sufficient.

Therefore, continuous authentication needs to be developed in order to secure the teleoperated robotic system. Behavior biometric-based continuous authentication has emerged recently to mitigate the security problems and attacks that target the postauthenticated session after the initial login for computer systems[7][76][46] and mobile deivices [24][73][21][10][65]. In these works, instead of authorizing a user through a one-time login challenge, the continuous authentication system continuously examines the user's behavior biometrics (i.e. key stroke/mouse dynamics, touch screen usage, device dynamics etc.) in order to gurantee the identity of the initially authenticated user.

Nevertheless, in the aforementioned work, the authentication results are based on the analysis of relatively simple user actions. In [7] and [76], features of user key stroke action, such as key code, press time and interval time between strokes when a user interacts with a desktop computer, are analyzed. Touch actions on mobile devices, such as tapping, scrolling and flinging, are used for authentication purposes. Due to the simplicity of these actions, using single actions to fulfill the authentication is highly volatile. In most cases, to increase the robustness of the authentication method, multiple consecutive actions are used for the final decision. However, the operator's motions and actions during a teleoperated procedure are far more complex than a single simple action. The methods developed in the above work is unlikely to suit this case. Moreover, in most of the aforemention approaches, conventional classifiers, such as k-Nearest Neighbour, Support Vector Machine, Neural Network or Random Forest, are implemented. The major limitation of these classification algorithms is that they heavily rely on the choices of both positive and negative samples during the training process. Although the choices of positive samples are straightforward in our case, as we can use data obtained from the genuine operator, negative samples are not so easily acquired. It is intractible to let someone imitate every operator and generate the corresponding negative sample as it requires tremendous extra effort. On the other hand, if we suppose that using

different operators' data as negative samples is feasible, choosing the negative samples to train the classifier is in and of itself another issue to solve as it will significantly affect the performance of the classifier.

In this work reported here, by making the analogy between human language and operator motion, we present a Hidden Markov Model (HMM) based method for continuous teleoperator authentication. The HMM can be trained with only the operators data (positive samples)[65] and it has been widely used in speech recognition[32] and human motion modeling [74][72], which fits the teleoperator continuous authentication task well. To determine the feasibility of out approach, we performed an experimental study with 5 participants. All subjects carried out a block transfer task in a simulated virtual reality environment with haptic feedback and virtual fixtures enabled.

In summary, the main contributions of this work are:

1. The development of a continuous teleoperator authentication method that uses Left-Right HMM[86] to model an operator's gestures followed by a Token Passing algorithm [85] that concatenates gesture models.

2. The development and demonstration of a VR simulated teleoperation environment and the experimental user study evaluation with 5 participants.

3. Experimental demonstration that the proposed continuous teleoperator authentication is able to achieve high accuracy and impersonation attack resistance.

### *3.2 Related Work*

HMMs have been extensively used in surgical skill assessment [59][60][61][62][63]. In most of these works, it is assumed that the entire surgical process is generated from a single HMM model while each surgical gesture is represented by a single state in the HMM. In [63], it is assumed that each surgical gesture can be represented by samples from a Gaussian distribution. In [59], Short Time Fourier Transform (STFT) followed by K-Means is used to discretize the surgical process data into gestures (states in HMM). Discrete HMMs are then trained to fulfill the skill evaluation. Linear

discriminant analysis (LDA) is applied to the surgical data to perform dimension reduction in [78] before HMMs are trained. In [75], a Sparse HMM approach is proposed, where a sparse dictionary learning technique called K-SVD[5] is used to model the surgical gesture states in the HMM.

However, representing a surgical gesture by a single state in HMMs potentially has limitations with regard to fully capturing the dynamic and complex properties of each gesture. Moreover, it may not be applicable for continuous surgeon authentication. In all aforementioned work, the analysis is performed offline given the entire kinematic data of the surgical procedure. However, as shown in Fig. 3.1, in continuous authentication, a sample window is used instead and authentication of the operator is based on the analysis of data in that window. In this case, unlike the offline scenario, the data in the sample window will contain only partial gestures. The kinematic properties of a partial gesture are different from the complete gesture. This may cause some problems using a single state in the HMM to represent the operator's gesture.

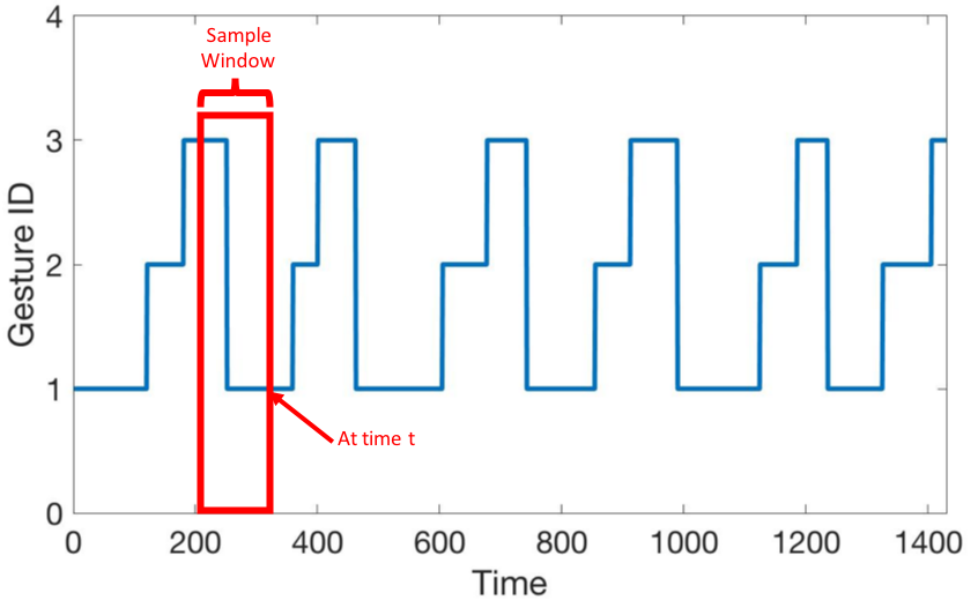


Figure 3.1: Comparison Between Offline Analysis and Continuous Authentication

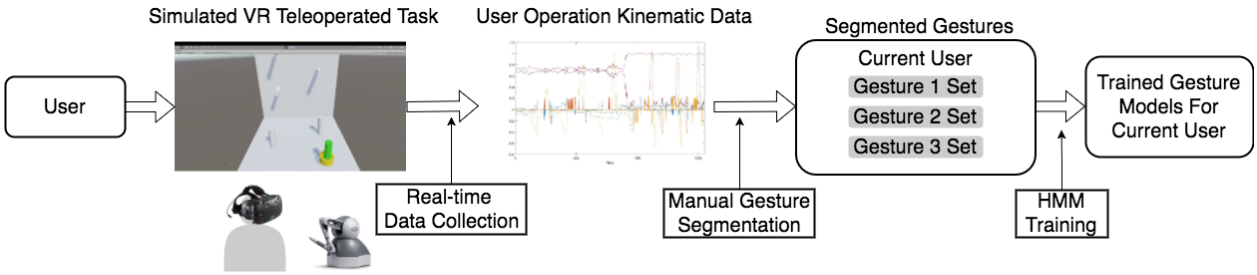


Figure 3.2: Continuous Operator Authentication Training Phase

## *3.3 Continuous Operator Authentication for Teleoperated Systems*

In order to achieve continuous operator authentication for teleoperated systems and overcome the limitations present in existing methods, we developed a novel scheme as shown in Figure 3.2 (training process) and 3.3 (continuous authentication process). In the training phase, a user will perform the simulated teleoperation in the VR environment by using a haptic input device. Real-time kinematic data (i.e. velocity,orientation, and force applied) of the entire teleoperation process is collected. We then manually segment the teleoperation process into several basic gestures. The corresponding user's gesture HMM models are trained based on the segmented gesture pieces. In the testing phase, a user will perform the simulate teleoperation task while we use a moving sample window with width $T$ to collect kinematic data from $t-T$ to $t$ where $t$ is the current time. An HMM likelihood analysis is then performed on the data within the sample window based on the trained operator gesture HMM models and this generates the continuous authentication result.

## *3.4 Experiment*

### *3.4.1 Experiment Setup*

In this work, we first built a VR environment within the Unity Game Engine[17] to let subjects perform a simulated teleoperation task. As shown in Figure 3.4, the user was asked to use the

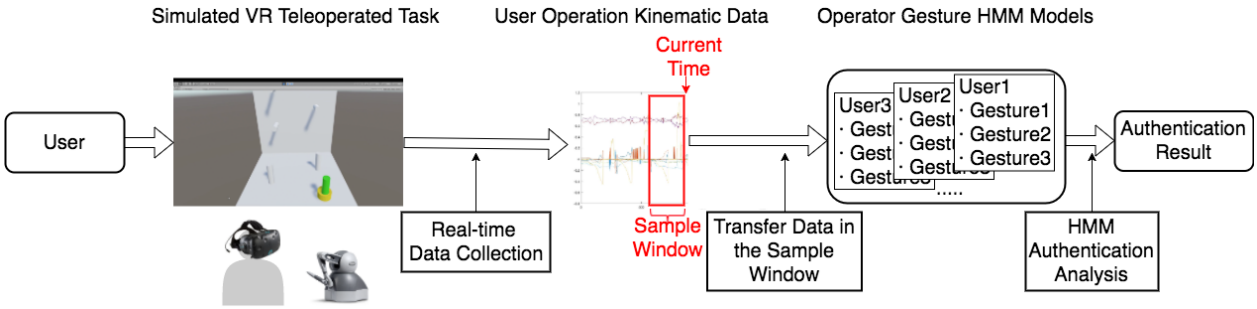


Figure 3.3: Continuous Operator Authentication Testing Phase

Sensable PHANToM Omni[55] to control the 6 degree of freedom (DOF) configuration of a virtual ring in order to transfer it through the virtual pegs on the board in a predefined sequence. In the experiment, each user wore the HTC Vive headset for 3D visual feedback about the VR simulated task. Meanwhile, haptic feedback via virtual fixtures[64] was enabled during the entire operation as the user provided motion commands with the Sensable PHANToM Omni. Two types of virtual fixtures were introduced: 1) Forbidden region around the pegs and base board and 2) Guidance toward the next peg tip. The guidance virtual fixture was only activated when the ring was out of the peg and being transferred toward the next peg. The haptic feedback offers the user a sense of touch and helps improve the operational performance. Moreover, in [84][83], we found that humans have unique ways of interacting with haptic interfaces and that haptic feedback can be used for continuous authentication.

In this experiment, subjects were first asked to explore the VR environment to get used to the interface and practice the simulated teleoperated task 10 to 15 times until they gained enough familiarity with the task. The goal of this process is to eliminate any learning effects to the continuous authentication performance.

Each subject was then asked to perform the task 5 times, while the following data were collected in real-time.

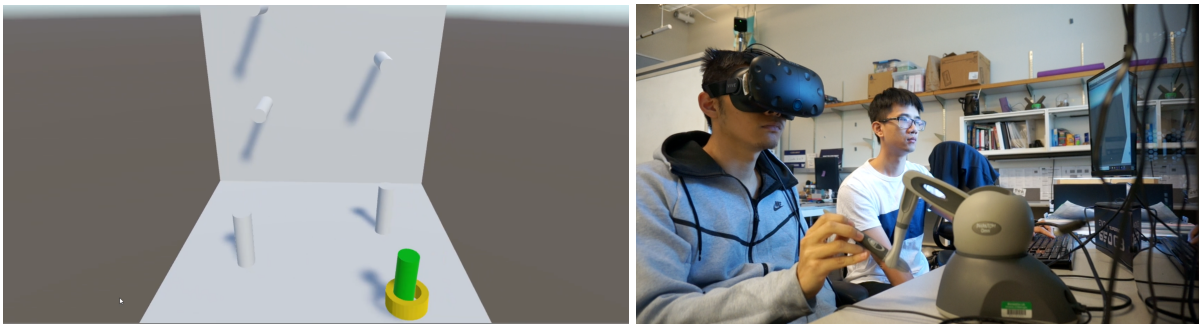

Figure 3.4: Experiment: The VR Environment (Left) and The user and PhantomOmni Controller (Right)

1. Position of the center of the ring $(x, y, z)$

2. Orientation of the ring ($Q_x, Q_y, Q_z, Q_w$, in quaternion)

3. Force applied $(f_x, f_y, f_z)$

All data was recorded at 60 Hz. In each trial, the app starts recording data when the user starts moving the ring and stops when the user pulls the ring out of the last peg.

Since the position and force data is highly correlated due to the influence of the virtual fixtures, we generate extra velocity information from the gathered position data as follow.

$$v_x(t) = x(t) - x(t-1), v_x(0) = 0 \tag{3.1}$$

$$v_y(t) = y(t) - y(t-1), v_y(0) = 0 \tag{3.2}$$

$$v_z(t) = z(t) - z(t-1), v_z(0) = 0 \tag{3.3}$$

The state vecor at time $t$ is then constructed as $s = (v_x, v_y, v_z, Q_x, Q_y, Q_z, Q_w, f_x, f_y, f_z)$.

### *3.4.2 Gesture Segmentation*

In order to make the analogy between human motion and language, we first need to find the 'word' in the teleoperation process, which is the operator's gesture. In this work, we segmented the entire process into 3 basic gestures as listed below.

1) Gesture 1: Transfer the ring toward next peg tip;

2) Gesture 2: Insert the ring;

3) Gesture 3: Pull out the ring.

The segmentation is based on the position of the ring and the corresponding status of the teleoperation process.

### *3.4.3 Subject Demographics*

Our experimental results are based on our study involving 5 participants. The demographics of all participants are shown in Table 3.1.

Table 3.1: Subjects Demographics

| | |
|---|---|
| Sample Size | 5 |
| Sex | 2 Females; 3 Males |
| Age Range | 18 to 28 |
| Handedness | 1 Left; 4 Right |

## ***3.5 Proposed Method***

As discussed in previous sections, there are two major challenges to achieve continuous operator authentication. First, the lack of negative samples to train the classifier makes conventional classification strategies such as SVM, neural networks and random forests inappropriate for this

application. Moreover, unlike offline operator motion analysis, where the entire operation process data are available, we only have partial motion information within the sample window for continuous operator authentication.

Therefore, in order to overcome these challenges, we propose the use of a Left-Right HMM[58] to model operators' gestures followed by a Token Passing algorithm [85] to concatenate the gesture models, thus achieving continuous authentication. The major advantage of using HMMs is that in the training phase, only positive samples are required. Also, HMMs are able to capture local dynamic properties of the operator's gestures[65] which serves the purpose of continuous operator authentication. In the following sections, we will briefly review the Left-Right HMM Model and Token Passing Algorithm and demonstrate how we implement them for the proposed continuous authentication task.

### *3.5.1 Left-Right HMM Model*

Left-Right HMMs have been widely used in speech recognition[26][57][86]. Generally, it is assumed that the sequence of speech vectors corresponding to each word (or phoneme) is generated by an HMM model. In the proposed continuous operator authentication method, an analogy between word (phoneme) and gesture is made, by which each gesture from an individual operator is represented by a unique HMM.

The proposed Left-Right HMM structure is shown in Figure 3.5. Each state $i$ is associated with an emission probability distribution $b_i(o_t)$, which defines the probability of generating observation $o_t$ at time $t$. Additionally, the transition probability between each pair of states $i$ and $j$ is determined by transition probability $\{a_{ij}\}$. Furthermore, the entry (first) and exit (last) states of the proposed HMM are non-emitting. These two states are used to facilitate the concatenation between surgeme models as explained in more detail later. The rest states are emitting states associated with emission probability distributions. The transition matrix is $N \times N$, where $N$ is the number of states. The sum of each row will be one except for the last row which is zero since no transition is allowed from the final state.

We assume that for each emitting state $i$ that the emission probability distribution is a Gaussian

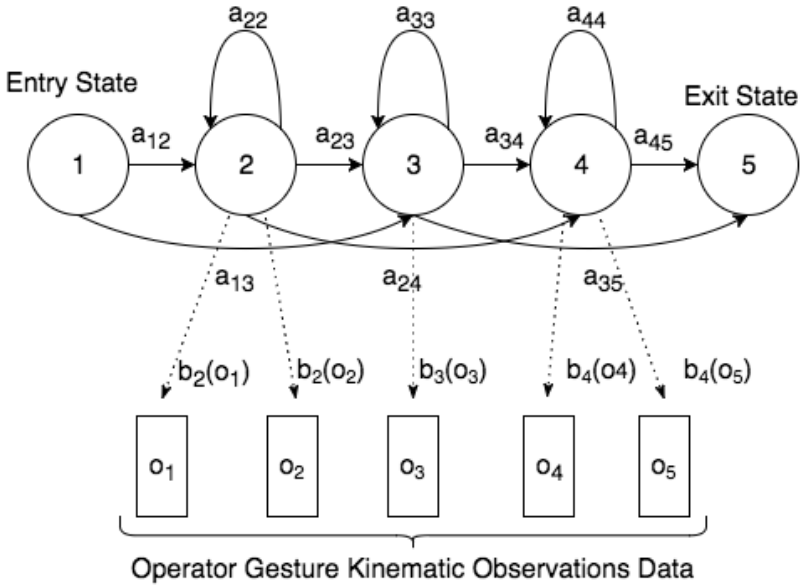


Figure 3.5: Left-Right Hidden Markov Model with Non-emitting State

mixture as shown below. For state $i$, the probability $b_i(o_t)$ of generating observation $o_t$ is given by

$$b_i(o_t) = \sum_{m=1}^{M_i} c_{im} \mathcal{N}(o_t; \mu_{im}, \Sigma_{im}) \tag{3.4}$$

where $M_i$ is the number of Gaussian mixtures in state $i$, $c_{im}$ is the weight of the $m^{\text{th}}$ mixture and $\mathcal{N}(\cdot; \mu_{im}, \Sigma_{im})$ is the probability density function of a multivariate Gaussian distribution with mean $\mu_{im}$ and covariance matrix $\Sigma_{im}$.

In the training phase, Baum-Welch re-estimation [58] is used. Segmented pieces of gesture sequences from each operator (as mentioned in section 3.4.2) are used as ground truth and the Baum-Welch algorithm is applied to obtain the maximum likelihood estimation of the model parameter state transition probability matrix $\{a_{ij}\}$ and emission probability distribution $b_i(o_t)$ for $i, j = 1, ..., N$.

### *3.5.2 Token Passing Algorithm*

Given the observation sequence, to achieve gesture recognition and continous authentication, the first step is to determine the hidden state sequence. This can be done using Viterbi Decoding Algorithm [23]. In this work, an alternative formulation of the Viterbi Algorithm called the Token Passing Algorithm[85] is used. It is able to realize single gesture recognition while simplifying concatenating gesture models for continous operator authentication.

First, for the base case of single gesture recognition, the Token Passing algorithm works as follows. Let $\psi_j(t)$ denote the maximum log likelihood of observing operation signal $o_{1:t}$ and being in state $j$ at time $t$. In the Token Passing algorithm, it is assumed that each state $j$ of a HMM at time $t$ holds a single movable token that contains partial log likelihood $\psi_j(t)$. At each time frame $t$, the following algorithm is executed:

**for** t= 1 **to** T do
  **for each** state $i$ **do**
    Pass a copy of the token in state $i$ to all
    connecting state $j$, incrementing $\psi_j(t)$ by
    $log(a_{ij}) + log(b_j(o(t)))$;
  **end**
  Discard the original tokens;
  **for each** state $i$ **do**
    Find the token in state $i$ with the largest
    $\psi_i(t)$ and discard the rest
  **end**
**end**

In this way, with the gesture piece $O_g = o_{1:T}$, let $\psi_{max}(T|O_s, g_{ij})$ denote the log likelihood held by the remaining token at time $T$ given that the gesture model is from operator $i$ and gesture $j$, the

correpsonding operator $i$ and gesture $j$ can be recognized as

$$(i, j) = arg \max_{i,j} \{\psi_{max}(T|O_s, g_{ij})\} \tag{3.5}$$

Next, in order to realize continuous operator authentication, individual gesture models need to be concatenated. Moreover, similar to human language, there is *grammar* in the teleoperation task as well, which defines how the gestures can be connected. In our proposed simulated teleoperated task, the grammar is shown in Figure 3.6

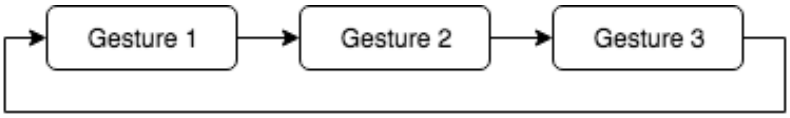


Figure 3.6: Gesture Grammar

The structure of concatenating the gestures based on the grammar is show in Figure 3.7. The non-emitting entry and exit states now work as *glue* to join gesture models together.

For connected gesture recognition, besides overall log likelihood, we also want to know the best matching gesture sequence. Therefore, now tokens are assumed to hold a path identifier as well as the path log likelihood. The path identifier is used to record gesture boundary information which will be called Gesture Link Record (GLR). At each time $t$, extra steps shown as follows are taken in addition to the individual gesture recognition algorithm listed above:

**for each** token entered EXIT state at time t do
  create a new GLR containing;
    <token contents, $t$, identity of emitting gesture model>;
  change the path identifier of the token to point to this new record
**end**

By doing so, potential gesture boundaries are recorded in a linked list, and on completion at time $T$, the path identifier held in the token with the largest log likelihood can be used to trace back

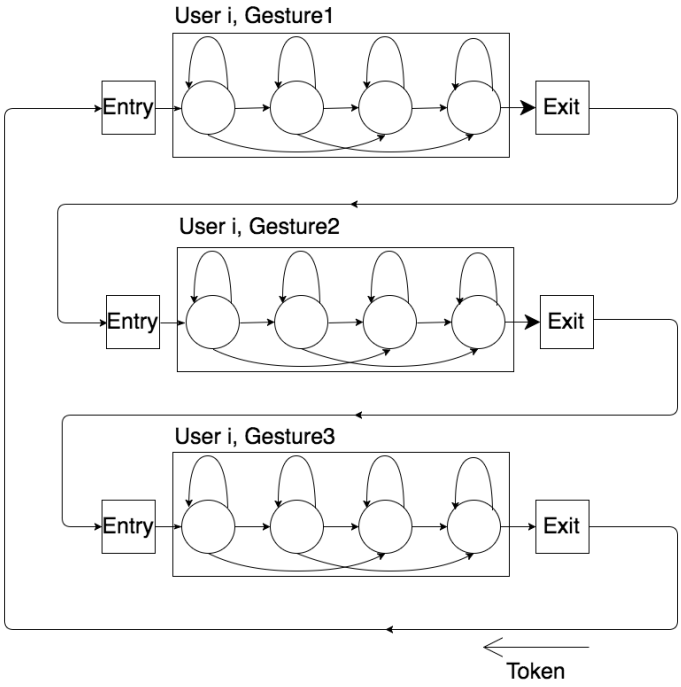


Figure 3.7: Token Passing Algorithm

through the linked list to find the best gesture sequence and the corresponding gesture boundary locations.

### *3.5.3 Continuous Operator Authentication*

In this way we will be able to fulfill the continuous operator authentication as shown. We put an additional constraint on the aforementioned gesture recognition scheme by mandating that consecutive gestures must come from the same operator.

At time $t$, given the observation from the sample window with width $T$ as $O_{t-T:t}$, operator recognition is done by solving $\psi_{max}(t)$ and checking the gesture labeling $l_{t-T:t}$. The observation sequence will be recognized as operated by user $i$ if

$$l_{t_0} \in L_i, t_0 = t-T, ..., t \tag{3.6}$$

where $i$ is the operator ID and $L_i$ is the corresponding gesture label set for the $i^{th}$ user.

## *3.6 Results*

### *3.6.1 Authentication Result*

In this work, we used the leave-one-trial-out strategy to train and test the proposed method.

First, in the training phase, the gesture models from each subject are trained based on the segmented individual gesture pieces in those training trials. In this way, 3N subject gesture models were obtained where 3 is the number of gestures and N is the number of the subjects. We varied the hyperparameters of the HMM to test the corresponding authentication performance. We varied the number of states from 3 to 6 and the number of mixtures in each state from 1 to 3.

In the continuous authentication phase, we also tested moving sample windows with widths of 5 seconds, 3 seconds and 1 seconds. The continuous authentication accuracy rate is evaluated as shown below:

$$Accuracy = \frac{L_{hit}}{L_{tot} - L_{window}} \tag{3.7}$$

where $L_{hit}$ is the number of sample windows in which the subject is correctly recognized, $L_{tot}$ is the total length of the teleoperation process and $L_{window}$ is the size of the moving sample window. The corresponding results are shown in Figure 3.8 to 3.10.

We found that when we choose the hyperparameter of the HMM which models each gesture as 5 states with 1 Gaussian mixture for each state, we were able to achieve the best authentication accuracy, and the result is listed in Table 3.2.

Table 3.2: Continous Authentication Accuracy with Multiple Sample Window Width

| Window Width | 5 sec | 3 sec | 1 sec |
|---|---|---|---|
| Accuracy | 88.47% | 85.27% | 77.26% |

When we used a sample window width of 5 seconds, we were able to authenticate the operator in realtime with almost a 90% accuracy rate, while with a 1-second sample window we achieved

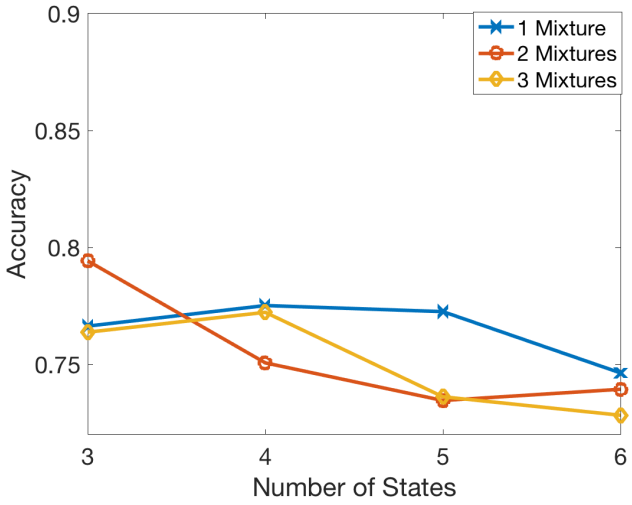


Figure 3.8: Continuous Authentication Accuracy with 1-Second Sample Window

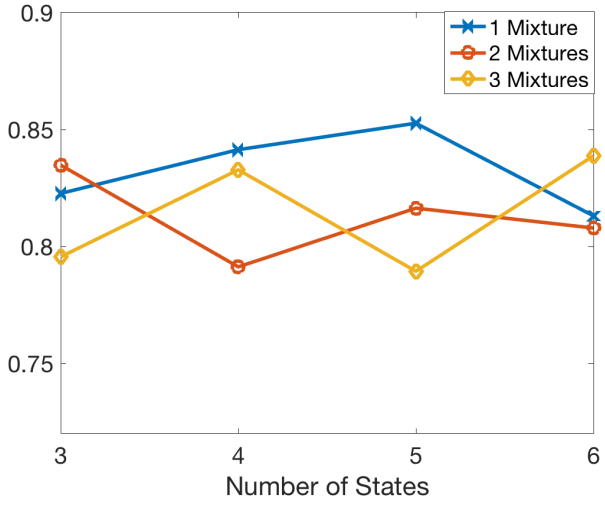


Figure 3.9: Continuous Authentication Accuracy with 3-Second Sample Window

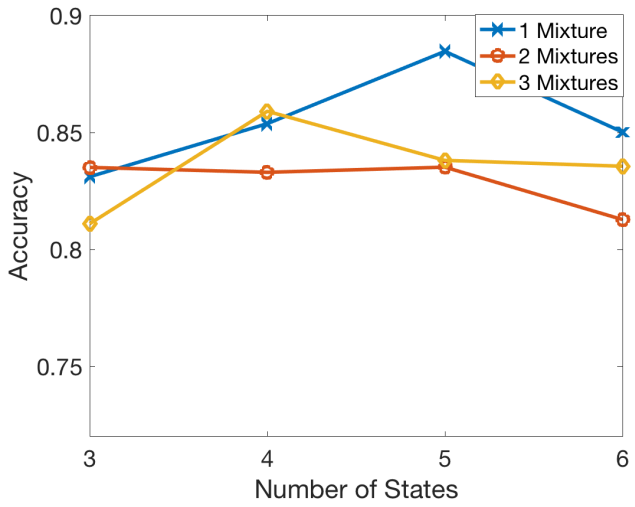


Figure 3.10: Continuous Authentication Accuracy with 5-Second Sample Window

77.26% continous authentication accuracy. This shows that the proposed method works and is promising for continuous authentication performance. We set the hyperparameter as 5 states with 1 mixture in the following sections.

### *3.6.2 Simulated Impersonation Attack Resistance*

In this section, we simulated an impersonation attack in the following steps. First, we picked two subjects (represented as User 1 and User 2 in the following context) and use the leave-one-trial-out strategy to train the model for the gestures of each subject. In the testing phase, instead of using the remaining testing trial to examine the authentication performance, we now split the test trial from User 1 and User 2 into 2 half pieces and connect the User 1's first piece to the User 2's second piece and vice versa. In this way, we generated two artificial teleoperation process observation sequences, where user 2 (user 1) impersonate user 1 (user 2) during the second half of the teleoperation task.

Figure 3.11 shows one of the results in detail. The blue and red lines represent the likelihood that the data within the corresponding sample window is operated by user 1 or user 2 respectively. The orange dashed line is the point where the simulated impersonation attack takes place. First,

the proposed method is able to detect the impersonation attack as the likelihood of the original user drops significantly after the simulated attack launches. Moreover, we notice that with a longer sample window, it is easier to distinguish two operators as the differences between the likelihood of the two users are significantly larger at various points when the size of the sample window increases. On the other hand, the response time for the continous authentication system to detect the impersonation attack increases when the sample window size becomes wider. Denoting the response time as the time between the time of the impersonation attack and the likelihood cross point between two users, the average response time is shown in Table 3.3.

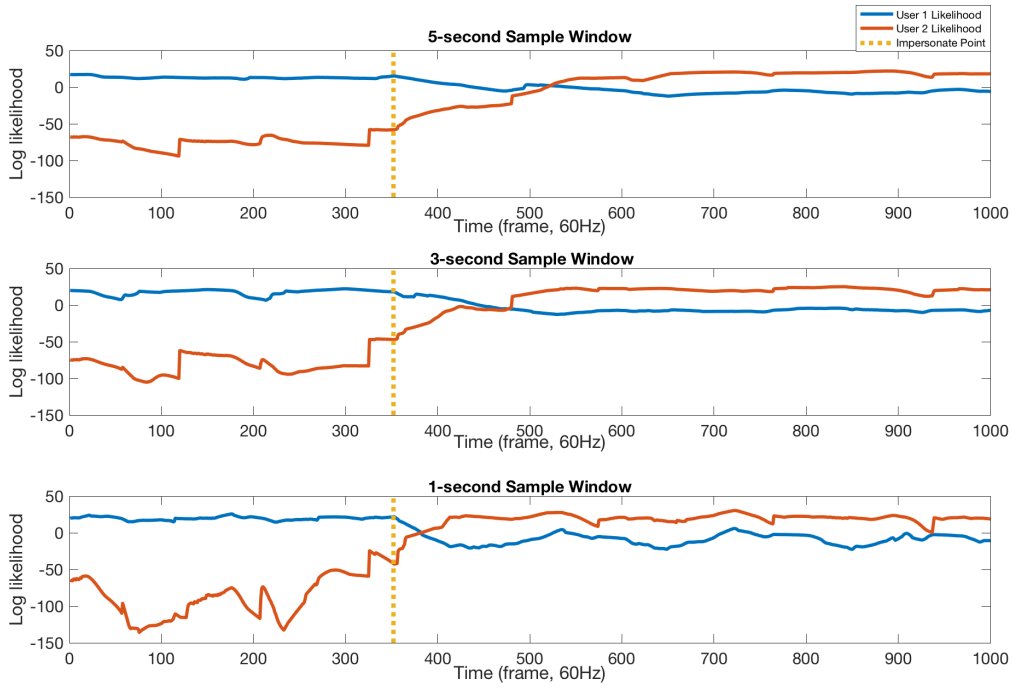


Figure 3.11: Simulated Impersonation Attack

Therefore, when choosing the size of the sample window, there is tradeoff between the accuracy of the continuous authentication and response time to attacks. A wider sample window is able to generate more stable continuous authentication accuracy, however it takes more time to respond to the attack. On the other hand, shorter sample windows offer the ability to react quickly to

Table 3.3: Average Response Time to Impersonation Attack with Multiple Sample Window Widths

| Window Width | 5 sec | 3 sec | 1 sec |
|---|---|---|---|
| Response Time | 2.35 sec | 1.51 sec | 0.49 sec |

impersonation attacks, but the authentication accuracy is less stable.

### *3.6.3 Authentication Performance on Physical Telerobotic Data*

In this section, we tested the continuous operator authentication method on JHU-ISI Gesture and Skill Assessment Working Set (JIGSAWS)[27] and explored the authentication performance of the developed method on a physical telerobotic system. In JIGSAWS, the dataset is obtained through da Vinci Surgical Robot, where subjects were asked to perform several surgery tasks. Data of three basic surgical tasks (suturing, needle passing and knot tying) performed by 8 study subjects are included. Each task was performed 3-5 trials for each subject. Each teleoperation process is manually labeled as a sequence of surgical gestures.

Given the data, for each surgical task, we keep the leave-one-trial-out setting to train and test the continuous operator authentication. In the training phase, we obtain $MN$ gesture models, where $M$ is the number of gesture types and $N$ is the number of subjects. We test the sample window with width as 5 seconds, 3 seconds and 1 second. We use the same setting as discussed in the previous session to evaluate the continuous authentication accuracy. In this section, the grammar of the teleoperation process is simplified that any pair of gestures can be connected during the continuous authentication. We then obtain the following result as shown in Table 3.4.

From these results, we note that even with 1-second observation sequence, the continuous operator authentication accuracy to detect the surgeon is above 80% for all three tasks. This shows that the developed continuous authentication method also works for the teleoperated robotic surgeries.

Table 3.4: Continous Authentication Accuracy with Multiple Sample Window Width

| Task | 5 sec | 3 sec | 1 sec |
|---|---|---|---|
| Suturing | 95.18% | 94.47% | 93.40% |
| Needle Passing | 85.36% | 84.77% | 81.24% |
| Knot Tying | 91.36% | 91.95% | 91.75% |

## *3.7 Disccussion*

In this section, we will discuss several limitations of this project and also raise possible extensions of the proposed method.

**Inexperienced Experimental Subjects** In this project, most subjects had never interacted with VR and/or haptic input devices. Although we conducted a training session to familiarize them with the system, we still noticed that there was a learning effect during the data collection, whereby the subject became better in handling and operating the system. Also, in some cases, subjects were less patient towards the end of the experiment, which influenced their motion to deviate from the original model. All these factors might have undermined the authentication performance result in our experiment. However, in most real-life applications, the genuine operators are usually well trained and have sufficient familiarity and experience with the teleoperated system. Therefore, it is more likely that the operator has a unique operating 'pattern' which makes it easier to accomplish the continuous operator authentication.

**Teleoperation Task Complexity** In this work, our experimental results were also based on a relatively simple and straightforward teleoperation task. In real-life scenarios, some teleoperation tasks, such as robotic surgery, are more complex. It would be interesting to explore whether the proposed method are able to achieve good continuous authentication performance in these applications. We anticipate that better gesture segmentation as well as gesture grammar is needed to better generalize the teleoperation process.

### *3.8 Summary*

In this chapter, we develop a continuous operator authentication method by making an analogy between human motion and human language (gesture to word and operation process to sentence). We use HMMs to model each operator's gestures and then concatenate them by using the Token Passing Algorithm based on a predefined operation grammar to achieve continuous authentication. We built a VR simulated environment and conducted a human subject experiment where the subjects conducted a simulated teleoperation task within the VR environment. Our experimental results indicate that the proposed continuous teleoperator authentication method works and is able to achieve above 77% accuracy rate with as short as a 1-second sample window.

### *3.9 Acknowledgements*

This work is supported by the National Science Foundation, Grant #CNS-13292751 and the Amazon Catalyst Program. Any opinions, findings, and conclusions or recommendations expressed in this paper do not necessarily reflect the views of the funding agencies.

Table 3.5: Summary of notation from Chapter 3.

| Symbol | Definition |
|---|---|
| $x, y, z$ | Position of the ring |
| $v_x, v_y, v_z$ | Velocity of the ring |
| $Q_x, Q_y, Q_z, Q_w$ | Orientation of the ring in Quaternion |
| $f_x, f_y, f_z$ | Force applied by the operator $t$ |
| $b_i(o_t)$ | Emission Probability of state $i$ given observation at time $t$ |
| $a_{ij}$ | State transition probablity between state $i$ and $j$ |
| $L_{tot}$ | Total length of the teleoperation process |
| $L_{window}$ | Length of the moving sample window |
| $L_{hit}$ | The number of sample windows in which the subject is correctly recognized |

# Chapter 4

# CONCLUSIONS AND FUTURE WORK

In this dissertation, we focus on enhancing the security of teleoperated system based on the human component in the loop. This dissertation focuses on the security risks that have recently arisen with cyber-physical systems, and propose that the fact every human have a unique way to interact with a teleoperated system can be used to increase the system's security, privacy and usability properties. We have developed several ways to solve the specific challenge in the security of teleoperated systems, which is *the tension between usability and security*. In doing so, this dissertation proposed two methods to authenticate the human operator 1) Initial authentication: Haptic Password and 2) Continuous Operator Authentication.

In Chapter 2, we proposed a new behavior biometric-based password system: *Haptic Passwords*. We experimental tested and analyzed the authentication performance of the Haptic Password System on multiple platforms, including PhantomOmni and mobile devices, such as iPhone. Our results indicate that the proposed Haptic Password System is able to achieve good authentication accuracy (above 90% with 0 FAR). Moreover, we also showed that the Haptic Password is able to generate robust forgery-proof authentication performance as well as good scalability (the possible password space is much larger than the human alphanumerical password).

In Chapter 3, we further developed a continuous operator authentication scheme to focus on detecting any attack that takes place after the initial authentication. We made an analogy between human language and human motion and modify a speech recognition based method to model the operator motion and achieve continuous authentication. Experimental demonstration is conducted through a human subject experiment where subjects were asked to fulfill a simulated teleoperation task in VR environment with haptic feedback enabled. It allows the subject to obtain both visual and tactile sensation during the experiment. The experimental result shows that the proposed method is

able to achieve above 77% continuous authentication accuracy with as short as 1-second sample window. Moreover, the proposed continuous operator authentication method is able to detect a simulated impersonation attack in real time.

In both chapters, operator authentication is based on the operator's behavior biometric and the unique traits that how the operator interacting with the teleoperated systems. These methods offer us a tool to identify the genuine user and detect possible attacks toward the teleoperated systems without affecting the system usability.

Possible next steps to extend this work include:

- Investigation of haptic passwords with long-term performance and various password forms other than the signature.

- Investigation and experimental evaluation of continuous operator authentication on more complicated, practical and physical telerobotic systems, rather than solely in simulation, in terms of its response speed, accuracy, and robustness.

- Investigation and development of mechanisms to prevent and reduce the harm caused by attacks. These mechanisms may lead to the development of methods that involve switching to a temporary autonomous operating mode once any anomaly or malicious activity has been detected.

# BIBLIOGRAPHY

[1] Chaos computer club breaks apple touchid. `http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid`. Accessed: 23 Februry 2015.

[2] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] FA Afsar, M Arif, and U Farrukh. Wavelet transform based global features for online signature recognition. In *9th International Multitopic Conference, IEEE INMIC 2005*, pages 1–6. IEEE, 2005.

[4] Sharad Agarwal, Travis Dawson, and Christos Tryfonas. Ddos mitigation via regional cleaning centers. Technical report, Citeseer, 2003.

[5] Michal Aharon, Michael Elad, and Alfred Bruckstein. Svd: An algorithm for designing overcomplete dictionaries for sparse representation. *Signal Processing, IEEE Transactions on*, 54(11):4311–4322, 2006.

[6] Fawaz Alsulaiman, Jongeun Cha, and Abdulmotaleb El Saddik. User identification based on handwritten signatures with haptic information. *Haptics: Perception, Devices and Scenarios*, pages 114–121, 2008.

[7] Lívia CF Araújo, Luiz HR Sucupira, Miguel Gustavo Lizarraga, Lee Luan Ling, and Joao Baptista T Yabu-Uti. User authentication through typing biometrics features. *IEEE transactions on signal processing*, 53(2):851–855, 2005.

[8] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Spinlock: a single-cue haptic and audio pin input technique for authentication. In *International Workshop on Haptic and Audio Interaction Design*, pages 81–90. Springer, 2011.

[9] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Counting clicks and beeps: Exploring numerosity based haptic and audio pin entry. *Interacting with computers*, 24(5):409–422, 2012.

[10] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. Silentsense: silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 187–190. ACM, 2013.

[11] Tamara Bonaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. To make a robot secure: an experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv:1504.04339*, 2015.

[12] Tamara Bonaci, Junjie Yan, Jeffrey Herron, Tadayoshi Kohno, and Howard Jay Chizeck. Experimental analysis of denial-of-service attacks on teleoperated robotic systems. In *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, pages 11–20. ACM, 2015.

[13] Alvaro A Cárdenas, Saurabh Amin, and Shankar Sastry. Research challenges for the security of control systems. In *HotSec*, 2008.

[14] Rohan Chabukswar, Yilin Mo, and Bruno Sinopoli. Detecting integrity attacks on scada systems. *IFAC Proceedings Volumes*, 44(1):11239–11244, 2011.

[15] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. Graphical password authentication using cued click points. In *Computer Security–ESORICS 2007*, pages 359–374. Springer, 2007.

[16] Kyle Coble, Weichao Wang, Bill Chu, and Zhiwei Li. Secure software attestation for military telesurgical robot systems. In *MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010*, pages 965–970. IEEE, 2010.

[17] Unity Game Engine. Unity game engine-official site. *Online][Cited: October 9, 2008.] http://unity3d. com*, pages 1534–4320, 2008.

[18] Maged MM Fahmy. Online handwritten signature verification system based on dwt features extraction and neural network classification. *Ain Shams Engineering Journal*, 1(1):59–70, 2010.

[19] Marcos Faundez-Zanuy. On-line signature recognition based on vq-dtw. *Pattern Recognition*, 40(3):981–992, 2007.

[20] Hao Feng and Chan Choong Wah. Online signature verification using a new extreme points warping technique. *Pattern Recognition Letters*, 24(16):2943–2951, 2003.

[21] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 451–456. IEEE, 2012.

[22] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[23] G David Forney Jr. The viterbi algorithm. *Proceedings of the IEEE*, 61(3):268–278, 1973.

[24] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1):136–148, 2013.

[25] Javier Galbally, Marcos Martinez-Diaz, and Julian Fierrez. Aging in biometrics: an experimental analysis on on-line signature. *PloS one*, 8(7):e69897, 2013.

[26] Mark JF Gales. Maximum likelihood linear transformations for hmm-based speech recognition. *Computer speech & language*, 12(2):75–98, 1998.

[27] Yixin Gao, S Swaroop Vedula, Carol E Reiley, Narges Ahmidi, Balakrishnan Varadarajan, Henry C Lin, Lingling Tao, Luca Zappella, Benjamın Béjar, David D Yuh, et al. Jhu-isi gesture and skill assessment working set (jigsaws): A surgical activity dataset for human motion modeling.

[28] Tamas Haidegger and Zoltan Benyo. Surgical robotic support for long duration space missions. *Acta Astronautica*, 63(7):996–1005, 2008.

[29] Marian Harbach, Alexander De Luca, and Serge Egelman. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4806–4817. ACM, 2016.

[30] Brett M Harnett, Charles R Doarn, Jacob Rosen, Blake Hannaford, and Timothy J Broderick. Evaluation of unmanned airborne vehicles and mobile robotic telesurgery in an extreme environment. *Telemedicine and e-Health*, 14(6):539–544, 2008.

[31] Kai Huang and Hong Yan. Stability and style-variation modeling for on-line signature verification. *Pattern Recognition*, 36(10):2253–2270, 2003.

[32] Xuedong D Huang, Yasuo Ariki, and Mervyn A Jack. Hidden markov models for speech recognition. 1990.

[33] Rosa Iglesias, Mauricio Orozco, FA Alsulaiman, JJ Valdes, and Addulmotaleb El Saddik. Characterizing biometric behavior through haptics and virtual reality. In *Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on*, pages 174–179. IEEE, 2008.

[34] Takashi Imaida, Yasuyoshi Yokokohji, Toshitsugu Doi, Mitsushige Oda, and Tsuneo Yoshikawa. Ground-space bilateral teleoperation of ets-vii robot arm by direct bilateral coupling under 7-s time delay condition. *IEEE Transactions on Robotics and Automation*, 20(3):499–511, 2004.

[35] Donato Impedovo and Giuseppe Pirlo. Automatic signature verification: the state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 38(5):609–635, 2008.

[36] David P Jablon. Extended password key exchange protocols immune to dictionary attack. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997. Proceedings., Sixth IEEE Workshops on*, pages 248–255. IEEE, 1997.

[37] Pari Jahankhani, Vassilis Kodogiannis, and Kenneth Revett. Eeg signal classification using wavelet feature extraction and neural networks. In *Modern Computing, 2006. JVA'06. IEEE John Vincent Atanasoff 2006 International Symposium on*, pages 120–124. IEEE, 2006.

[38] Edson JR Justino, Flávio Bortolozzi, and Robert Sabourin. A comparison of svm and hmm classifiers in the off-line signature verification. *Pattern recognition letters*, 26(9):1377–1385, 2005.

[39] Katharina Krombholz, Thomas Hupperich, and Thorsten Holz. Use the force: Evaluating force-sensitive authentication for mobile devices. In *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[40] Arash Habibi Lashkari, Samaneh Farmand, Dr Zakaria, Omar Bin, Dr Saleh, et al. Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*, 2009.

[41] Gregory S Lee and Bhavani Thuraisingham. Cyberphysical systems security applied to telesurgical robotics. *Computer Standards & Interfaces*, 34(1):225–229, 2012.

[42] MH Lum, DCW Friedman, HH King, Timothy Broderick, MN Sinanan, J Rosen, and B Hannaford. Field operation of a surgical robot via airborne wireless radio link. In *the Proceedings of the IEEE International Conference on Field and Service Robotics*, 2007.

[43] Mitchell JH Lum, Jacob Rosen, Hawkeye King, Diana CW Friedman, Gina Donlin, Ganesh Sankaranarayanan, Brett Harnett, Lynn Huffman, Charles Doarn, Timothy Broderick, et al. Telesurgery via unmanned aerial vehicle (uav) with a field deployable surgical robot. *Stud Health Technol Inform*, 125:313–5, 2007.

[44] Yilin Mo, Emanuele Garone, Alessandro Casavola, and Bruno Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5967–5972. IEEE, 2010.

[45] Yilin Mo and Bruno Sinopoli. Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 911–918. IEEE, 2009.

[46] John V Monaco, Ned Bakelman, Sung-Hyuk Cha, and Charles C Tappert. Developing a keystroke biometric system for continual authentication of computer users. In *Intelligence and Security Informatics Conference (EISIC), 2012 European*, pages 210–216. IEEE, 2012.

[47] Robert Morris and Ken Thompson. Password security: A case history. *Communications of the ACM*, 22(11):594–597, 1979.

[48] Keiji Nagatani, Seiga Kiribayashi, Yoshito Okada, Kazuki Otake, Kazuya Yoshida, Satoshi Tadokoro, Takeshi Nishimura, Tomoaki Yoshida, Eiji Koyanagi, Mineo Fukushima, et al. Emergency response to the nuclear accident at the fukushima daiichi nuclear power plants using mobile rescue robots. *Journal of Field Robotics*, 30(1):44–63, 2013.

[49] Loris Nanni, Emanuele Maiorana, Alessandra Lumini, and Patrizio Campisi. Combining local, regional and global matchers for a template protected on-line signature verification system. *Expert Systems with Applications*, 37(5):3676–3684, 2010.

[50] Tetsu Ohishi, Yoshimitsu Komiya, Hikaru Morita, and Takashi Matsumoto. Pen-input on-line signature verification with position pressure inclination trajectories. In *Proceedings of the 15th International Parallel & Distributed Processing Symposium*, page 170. IEEE Computer Society, 2001.

[51] Mauricio Orozco, Matthew Graydon, Shervin Shirmohammadi, and Abdulmotaleb El Saddik. Experiments in haptic-based authentication of humans. *Multimedia Tools and Applications*, 37(1):73–92, 2008.

[52] Mauricio Orozco, Behzad Malek, Mohamad Eid, and Abdulmotaleb El Saddik. Haptic-based sensible graphical password. In *Proceedings of Virtual Concept*, volume 56, pages 1–4, 2006.

[53] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki. Distributed denial of service attacks. *The Internet Protocol Journal*, 7(4):13–35, 2004.

[54] Donald B Percival and Andrew T Walden. *Wavelet methods for time series analysis*, volume 4. Cambridge university press, 2006.

[55] Omni PHANTOM. Sensable technologies. *Inc., http://www. sensable. com*.

[56] J Prevost. Biometrics with limited government intervention: How to provide for privacy and security requirements of networked digital environments. *Paper for MIT*, 6, 1999.

[57] Lawrence Rabiner and Biing-Hwang Juang. Fundamentals of speech recognition. 1993.

[58] Lawrence R Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257–286, 1989.

[59] Carol E Reiley and Gregory D Hager. Task versus subtask surgical skill evaluation of robotic minimally invasive surgery. In *Medical Image Computing and Computer-Assisted Intervention–MICCAI 2009*, pages 435–442. Springer, 2009.

[60] Carol E Reiley, Henry C Lin, Balakrishnan Varadarajan, B Vagvolgyi, S Khudanpur, DD Yuh, and GD . Automatic recognition of surgical motions using statistical modeling for capturing variability. *Studies in health technology and informatics*, 132:396, 2008.

[61] Jacob Rosen, Jeffrey D Brown, Lily Chang, Mika N Sinanan, and Blake Hannaford. Generalized approach for modeling minimally invasive surgery as a stochastic process using a discrete markov model. *Biomedical Engineering, IEEE Transactions on*, 53(3):399–413, 2006.

[62] Jacob Rosen, Blake Hannaford, Christina G Richards, and Mika N Sinanan. Markov modeling of minimally invasive surgery based on tool/tissue interaction and force/torque signatures for evaluating surgical skills. *Biomedical Engineering, IEEE Transactions on*, 48(5):579–591, 2001.

[63] Jacob Rosen, Massimiliano Solazzo, Blake Hannaford, and Mika Sinanan. Task decomposition of laparoscopic surgery for objective evaluation of surgical residents' learning curve using hidden markov model. *Computer Aided Surgery*, 7(1):49–61, 2002.

[64] Louis B Rosenberg. Virtual fixtures: Perceptual tools for telerobotic manipulation. In *Virtual Reality Annual International Symposium, 1993., 1993 IEEE*, pages 76–82. IEEE, 1993.

[65] Aditi Roy, Tzipora Halevi, and Nasir Memon. An hmm-based behavior modeling approach for continuous mobile authentication. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pages 3789–3793. IEEE, 2014.

[66] Aditi Roy, Nasir Memon, and Arun Ross. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 2017.

[67] Napa Sae-Bae and Nasir Memon. Online signature verification on mobile devices. *IEEE Transactions on Information Forensics and Security*, 9(6):933–947, 2014.

[68] Roque Saltaren, Rafael Aracil, Cesar Alvarez, Eugenio Yime, and Jose Maria Sabater. Field and service applications-exploring deep sea by teleoperated robot-an underwater parallel robot with high navigation capabilities. *IEEE Robotics & Automation Magazine*, 14(3):65–75, 2007.

[69] David Sankoff and Joseph B Kruskal. Time warps, string edits, and macromolecules: the theory and practice of sequence comparison. *Reading: Addison-Wesley Publication, 1983, edited by Sankoff, David; Kruskal, Joseph B.*, 1, 1983.

[70] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007):94, 2007.

[71] Mark Shensa. The discrete wavelet transform: wedding the a trous and mallat algorithms. *Signal Processing, IEEE Transactions on*, 40(10):2464–2482, 1992.

[72] Guangyi Shi, Yuexian Zou, Yufeng Jin, Xiaole Cui, and Wen J Li. Towards hmm based human motion recognition using mems inertial sensors. In *Robotics and Biomimetics, 2008. ROBIO 2008. IEEE International Conference on*, pages 1762–1766. IEEE, 2009.

[73] Weidong Shi, Jun Yang, Yifei Jiang, Feng Yang, and Yingen Xiong. Senguard: Passive user identification on smartphones using multiple sensors. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on*, pages 141–148. IEEE, 2011.

[74] Cristian Sminchisescu, Atul Kanaujia, and Dimitris Metaxas. Conditional models for contextual human motion recognition. *Computer Vision and Image Understanding*, 104(2-3):210–220, 2006.

[75] Lingling Tao, Ehsan Elhamifar, Sanjeev Khudanpur, Gregory D Hager, and René Vidal. Sparse hidden markov models for surgical gesture classification and skill evaluation. In *Information Processing in Computer-Assisted Interventions*, pages 167–177. Springer, 2012.

[76] Charles C Tappert, Mary Villani, and Sung-Hyuk Cha. Keystroke biometric identification and authentication on long-text input. In *Behavioral biometrics for human identification: Intelligent applications*, pages 342–367. IGI Global, 2010.

[77] Michael Unser. Texture classification and segmentation using wavelet frames. *Image Processing, IEEE Transactions on*, 4(11):1549–1560, 1995.

[78] Balakrishnan Varadarajan, Carol Reiley, Henry Lin, Sanjeev Khudanpur, and Gregory Hager. Data-derived models for segmentation with application to surgical assessment and training. In *Medical Image Computing and Computer-Assisted Intervention–MICCAI 2009*, pages 426–434. Springer, 2009.

[79] Brandon Whitcher, Peter Guttorp, and Donald B Percival. Wavelet analysis of covariance with application to atmospheric time series. *Journal of Geophysical Research*, 105(D11):941–962, 2000.

[80] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1):102–127, 2005.

[81] Qinghan Xiao. Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Computational Intelligence Magazine*, 2(2):5–25, 2007.

[82] Jeff Yan et al. Password memorability and security: Empirical results. *IEEE Security & privacy*, (5):25–31, 2004.

[83] Junjie Yan, Tamara Bonaci, and Howard Chizeck. Your signature is your password: Haptic passwords on mobile devices. *IEEE Transactions on Information Forensics and Security*.

[84] Junjie Yan, Kevin Huang, Tamara Bonaci, and Howard J Chizeck. Haptic passwords. In *Intelligent Robots and Systems (IROS), 2015 IEEE/RSJ International Conference on*, pages 1194–1199. IEEE, 2015.

[85] Stephen John Young, NH Russell, and JHS Thornton. *Token passing: a simple conceptual model for connected speech recognition systems*. Cambridge University Engineering Department Cambridge, UK, 1989.

[86] Steve Young, Gunnar Evermann, Mark Gales, Thomas Hain, Dan Kershaw, Xunying Liu, Gareth Moore, Julian Odell, Dave Ollason, Dan Povey, et al. *The HTK book*, volume 2. Entropic Cambridge Research Laboratory Cambridge, 1997.