

2018

Usability, Efficiency and Security of Personal Computing Technologies

Nancy Carter

College of William and Mary - Arts & Sciences, njcarter@starpower.net

Follow this and additional works at: <https://scholarworks.wm.edu/etd>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Carter, Nancy, "Usability, Efficiency and Security of Personal Computing Technologies" (2018).
Dissertations, Theses, and Masters Projects. Paper 1550153977.
<http://dx.doi.org/10.21220/s2-rtc-4157>

This Dissertation is brought to you for free and open access by the Theses, Dissertations, & Master Projects at W&M ScholarWorks. It has been accepted for inclusion in Dissertations, Theses, and Masters Projects by an authorized administrator of W&M ScholarWorks. For more information, please contact scholarworks@wm.edu.

Usability, Efficiency and Security of Personal Computing Technologies

Nancy J. Carter

Williamsburg, Virginia

Bachelor of Science, University of Maryland College Park, 1981
Master of Science, Naval Postgraduate School, 1992

A Dissertation presented to the Graduate Faculty
of The College of William & Mary in Candidacy for the Degree of
Doctor of Philosophy

Department of Computer Science

College of William & Mary
January 2019

APPROVAL PAGE

This Dissertation is submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy



Nancy J. Carter

Approved by the Committee August 2018




Committee Chair

Professor Qun Li, Computer Science
College of William & Mary



Associate Professor Gang Zhou, Computer Science
College of William & Mary

Associate Professor Pieter Peers, Computer Science
College of William & Mary

Assistant Professor Adwait Jog, Computer Science
College of William & Mary

Associate Professor Jennifer A. Stevens, Psychological Sciences
College of William & Mary

COMPLIANCE PAGE

Research approved by

Protection of Human Subjects Committee (PHSC)

Protocol number(s): PHSC-2015-05-21-10424-qxlixx

Date(s) of approval: 2015-05-27

ABSTRACT

New personal computing technologies such as smartphones and personal fitness trackers are widely integrated into user lifestyles. Users possess a wide range of skills, attributes and backgrounds. It is important to understand user technology practices to ensure that new designs are usable and productive. Conversely, it is important to leverage our understanding of user characteristics to optimize new technology efficiency and effectiveness. Our work initially focused on studying older users, and personal fitness tracker users. We applied the insights from these investigations to develop new techniques improving user security protections, computational efficiency, and also enhance the user experience. We offer that by increasing the usability, efficiency and security of personal computing technology, users will enjoy greater privacy protections along with experiencing greater enjoyment of their personal computing devices.

Our first project resulted in an improved authentication system for older users based on familiar facial images. Our investigation revealed that older users are often challenged by traditional text passwords, resulting in decreased technology use or less than optimal password practices. Our graphical password-based system relies on memorable images from the user's personal past history. Our usability study demonstrated that this system was easy to use, enjoyable, and fast. We show that this technique is extendable to smartphones.

Personal fitness trackers are very popular devices, often worn by users all day. Our personal fitness tracker investigation provides the first quantitative baseline of usage patterns with this device. By exploring public data, real-world user motivations, reliability concerns, activity levels, and fitness-related socialization patterns were discerned. This knowledge lends insight to active user practices.

Personal user movement data is captured by sensors, then analyzed to provide benefits to the user. The dynamic time warping technique enables comparison of unequal data sequences, and sequences containing events at offset times. Existing techniques target short data sequences. Our Phase-aware Dynamic Time Warping algorithm focuses on a class of sinusoidal user movement patterns, resulting in improved efficiency over existing methods.

Lastly, we address user data privacy concerns in an environment where user data is increasingly flowing to manufacturer remote cloud servers for analysis. Our secure computation technique protects the user's privacy while data is in transit and while resident on cloud computing resources. Our technique also protects important data on cloud servers from exposure to individual users.

TABLE OF CONTENTS

Acknowledgements	v
Dedication	vi
1 Introduction	2
1.1 User-Device Interaction Challenge	3
1.2 Problems	5
1.2.1 Graphical Password Authentication System	6
1.2.2 Personal Fitness Tracker Usage Analysis	7
1.2.3 Phase-aware Dynamic Time Warping Analysis	8
1.2.4 Secure and Efficient Computation of Private Sensor Data	9
1.3 Contributions	9
1.3.1 Graphical Password Authentication System	10
1.3.2 Personal Fitness Tracker Usage Analysis	10
1.3.3 Phase-aware Dynamic Time Warping Analysis	11
1.3.4 Secure and Efficient Computation of Private Sensor Data	11
1.4 Dissertation Organization	12
2 Related Work	13
2.1 Graphical Password Authentication System	13
2.2 Personal Fitness Tracker Usage Analysis	15
2.2.1 User Activity Models	17
2.2.2 Initiation Phase	17
2.2.3 Utilization Phase	18
2.2.4 Utilization Phase – Social Engagement	19
2.2.5 Abandonment Phase	20
2.3 Phase-aware Dynamic Time Warping Analysis	21
2.3.1 Similarity Evaluation	21
2.3.2 Complexity Reduction	22
2.4 Secure and Efficient Computation of Private Sensor Data	23
2.4.1 Privacy Preserving Computation	23
3 Graphical Password Authentication System	25
3.1 Background	25

3.2 System Design	28
3.2.1 Design Motivation.....	28
3.2.2 Design Components.....	30
3.2.3 Entropy Analysis	32
3.2.4 Image Database.....	38
3.2.5 Target Image Selection Tool	41
3.3 Usability Study Design	44
3.3.1 Study Procedures.....	45
3.4 Usability Study Evaluation Results	48
3.4.1 Recall Performance.....	48
3.4.2 Authentication Timing.....	51
3.4.3 Individual Image Selection Timing.....	53
3.4.4 User Input Device Modality	55
3.4.5 Training Benefits	57
3.4.6 Personal Image Sequence Selection Timing	58
3.4.7 Guessing Study.....	59
3.4.8 Image Pattern Effects	60
3.4.9 Text Password Comparison	62
3.5 Graphical Password Extension to Smartphones	64
3.6. Conclusion	69
 4 Personal Fitness Tracker Usage Analysis	 70
4.1 Background	70
4.1.1 User Activity and Behavior Model	73
4.1.2 Personal Fitness Device Hardware, Software, and Social Forums	73
4.2 Motivation	76
4.3 Data Collection Methodology	77
4.3.1 Product Reviews	79
4.3.2 Blogging Websites	79
4.3.3 Image Sharing Websites.....	81
4.3.4 Social Networks	81
4.3.5 Fitness Infrastructure	83
4.4 User Data Analysis.....	86
4.4.1 Initiation Phase analysis.....	86

4.4.2 Exercise Phase Analysis	89
4.4.2.1 Reliability Analysis	89
4.4.2.2 Step Activity Analysis	90
4.4.2.3 Ownership Duration Activity Analysis	100
4.4.2.4 Social Engagement Analysis	101
4.5 Limitations	106
4.6 Conclusion	107
 5 Phase-aware Dynamic Time Warping Analysis	 108
5.1 Background	108
5.2 Dynamic Time Warping Technique	111
5.3 Phase-aware Dynamic Time Warping	115
5.3.1 Phase Identification	116
5.3.2 Phase Agreement Blocks	117
5.4 Performance Evaluation	118
5.5 Limitations	119
5.6 Conclusion	120
 6 Secure and Efficient Computation of Private Sensor Data	 121
6.1 Privacy-Preserving Protocol Workflow	122
6.2 Cryptographic Tools	124
6.2.1 Homomorphic Encryption	124
6.2.2 Oblivious Transfer	124
6.3 Private Squared Euclidean Distance	125
6.4 Private Matrix Filling	127
6.5 Private Minimal Finding	127
6.6 Batched Matrix Filling Optimization	128
6.7 Performance Evaluation	129
6.7.1 Comparison to Previous Work	132
6.7.2 Performance on Smartphone-Laptop Configuration	133
6.7.3 Performance on Gesture Recognition Data	133
6.8 Performance Optimizations	134
6.8.1 Performance Optimization via Early Abandon	134
6.9 Conclusion	135

7 Conclusion and Future Work	137
7.1 Future Work	138
7.1.1 Graphical Password Authentication System	139
7.1.2 Personal Fitness Tracker Usage Analysis	140
7.1.3 Phase-aware Dynamic Time Warping Analysis	141
7.1.4 Secure and Efficient Computation of Private Sensor Data	142
Bibliography	143

ACKNOWLEDGEMENTS

I wish to gratefully acknowledge my appreciation to my advisor, Dr. Qun Li, for his endless patience, guidance and thoughtful criticism during these projects. Thank you also to my committee members, Dr. Gang Zhou, Dr. Pieter Peers, Dr. Adwait Jog, and Dr. Jennifer A. Stevens of the Psychological Sciences Department for your thoughtful feedback and advice.

I am grateful to my current and past research group members for their support and contributions towards this work: Dr. Ed Novak, Dr. Zhengrui Qin, Dr. Shanhe Yi, Cheng Li, Zijiang Hao, and Lele Ma.

Finally, I wish to thank the faculty, Chair Dr. Robert Michael Lewis, and staff of our Computer Science Department who have supported my investigations into the intimate world of human-computer interactions. Vanessa Godwin, Jacquelyn Johnson, and Dale Hayes of the administration team have been a wonderful support during my research.

This dissertation is dedicated to my supportive and patient husband, Wayne Hay,
and to my family, who have lived this long journey of exploration with me.

“Not all those who wander are lost”....J. R. R. Tolkien

Usability, Efficiency and Security
of Personal Computing Technologies

Chapter 1

Introduction

New personal computing technologies such as smartphones, personal fitness trackers and portable computers continue to emerge and enjoy wide adoption among users in every part of human society. Many of us have enthusiastically adopted these technologies and embraced learning to use these devices in our daily lives. But not everyone has such an easy time adopting new technology. Users sometimes find technology challenging, it is important for technology designers to study and understand user physical, cognitive and behavioral attributes so that technology can be optimized to the user. Conversely, thorough understanding of user patterns opens opportunities for new technology optimizations. As always, security is important, and it shouldn't be burdensome for users to maintain good security practices as they go about their daily lives. Frequently the "technology smart" among us are asked by struggling relatives and friends to provide help with getting their devices to work. Our belief is that the time has come for increased efforts to adapt to user characteristics and behaviors, instead of the other way around. Our research reveals that careful study of human traits not only provides clues towards more user-friendly technology designs but also rewards us with ideas for optimizing long-standing algorithms.

The convenience of personal devices provides users with access to an ever-growing array of online services, and also gathers increasingly intimate personal activity measurements, wherever the user is located. As society moves more services online, the user population wants to take advantage of these services,

and they want to use them securely and efficiently. The reality is that not all can easily take advantage of technology due to psychological or physiological differences. While users wish to protect their personal information from compromise, they may use insecure designs because there are no better options available. User frustrations with technology lead to inefficiencies, and may ultimately lead a user to opt-out, accepting the subsequent withdrawal from online society.

Our work focused on improving usability, efficiency, and security through four projects. Our first project is a new authentication system that empowers older user populations by leveraging their long-term memories, and just requires touches on a touchscreen panel to execute. The second project collected and analyzed personal fitness tracker user data to develop an understanding of actual user activities, behaviors and social interaction patterns while wearing these devices. Thirdly, we applied awareness of important user movement activity patterns to improve efficiency of existing dynamic time warping similarity comparison techniques. Lastly, we created a new data privacy protection technique for use in remote data similarity comparisons. This was done by combining dynamic time warping and secure computation techniques. The result is user data privacy protection while engaged with online cloud services.

1.1 User-Device Interaction Challenge

Our vision is that personal computing technologies should be viewed as a combined user-device system. For optimum user experience and system efficiency, each side of the user-device paradigm should leverage knowledge of

the other. A model of our user-device concept is shown in Fig. 1.1. It shows important components of the human user, and interacting technology that define the complete technology interaction in service to a higher goal. Humans consist of the mind and body; hence they can be described by terms and concepts defined in psychology [2] and physiology [3]. By focusing on the user's inherent psychological and physiological traits, effective improvements may be designed for personal computing devices. Effective user experiences are defined in terms of **usability** [1], the degree to which a user can easily learn, and use personal computing technology. When the technology is usable, the user has a satisfying experience that provides benefit to their lives. When a technology is not usable, the user is frustrated or delayed. Technology developers of unusable devices have wasted considerable effort and assets that could have been put to better use. Good technology is described in terms of efficiency and security. **Efficiency** [141] is the degree to which the personal computing technology is optimized to serve the user well. Users wish to obtain the benefits of their personal computing technology quickly, and without wasted effort or time. Efficiency is also the speed with which the overall task at hand is accomplished. A technology design that is not well-designed is inefficient and will take a longer time to accomplish. Efficiency is measurable, allowing the quantified comparison of personal computing technologies in meeting user needs. **Security** [142] is essential to protect the user from harm, and also to protect the user's data from exposure to unauthorized parties. A secure computing experience is a necessary part of an effective and satisfying user experience. Users do not want to worry about their data becoming

exposed to view of unauthorized parties. Often users must implicitly rely upon the built-in security features of their technology to protect their personal information. If the built-in security features are not usable or efficient, either the user will abandon the technology, or they will risk compromise of valuable private data.

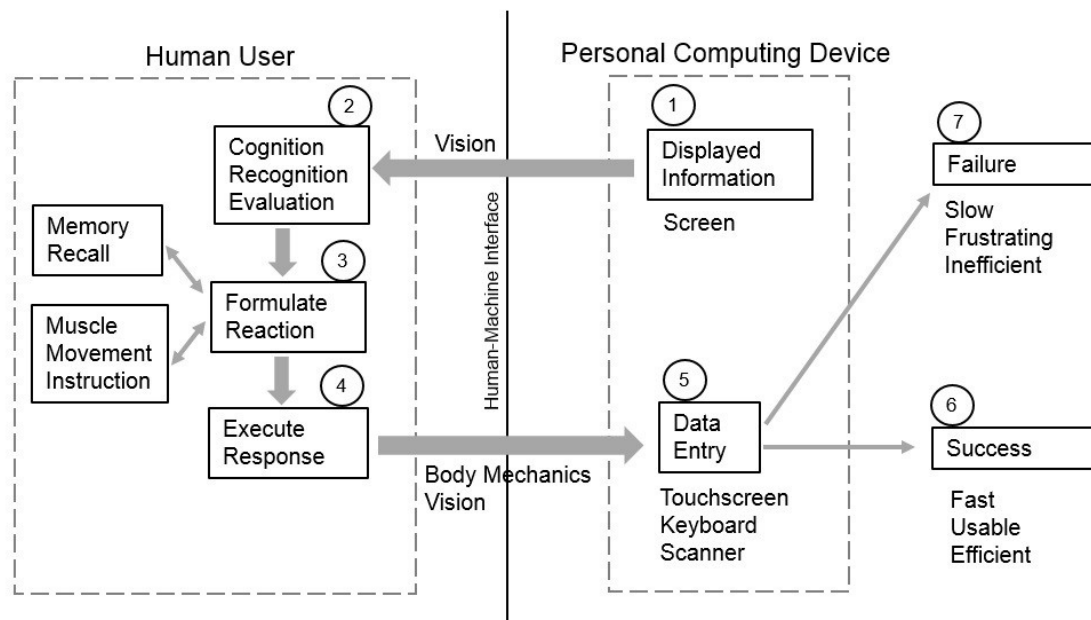


Figure 1.1: User-device interaction model.

1.2 Problems

Our four projects revolve around carefully studying users, with the goals of understanding actual user characteristics and designing appropriate usability, efficiency and security enhancements. We seek to improve the usability and security of user services, and also leverage user characteristics to create a more efficient computational algorithm. The benefit to the user is an improved and easier

user experience. The benefit to the system designer is greater efficiency in processing and space utilization.

1.2.1 Graphical Password Authentication System

Our first project is a new authentication mechanism based on graphical passwords, an alternative to hard-to-remember text passwords. Our interview study with older users revealed that text passwords were hard to recall, keys were hard to see, and motor skill impairment made accurate keyboard entry tough. These are typical health experiences of older age. Often older volunteers reduced or eliminated their use of the computer and internet services due to the difficulties of carrying out password authentication. Their feedback provided motivation to create a more usable authentication method tailored for older computer users. Some existing graphical password systems required hard-to-memorize or hard-to-see abstract sequences such as emoji, icons or text-image pairs. Other techniques relied on precisely redrawing digital lines on a video display, challenging for those with manual dexterity issues such as Parkinson's or palsy. We sought to empower older users by leveraging their long-term memories to create a secret password based on familiar images from each individual's personal past. We make password sequence entry physically easy through placement of a finger on a touchscreen, or clicking a mouse on an image target. Our Graphical Password system allowed each user to select a sequence of personally recognizable black and white facial images for use as a password. To authenticate, each user selects their sequence of images displayed randomly within a larger screen of similar looking decoy facial images. The use of facial images leverages the unique cognitive and neural

abilities that humans have for processing and recognizing faces. Compared to existing password techniques, this method possesses entropy superior to short PINs and comparable to short text passwords. Our usability study demonstrated that users could quickly and easily use this system, and importantly, they found it was fun!

1.2.2 Personal Fitness Tracker Usage Analysis

Our second project studied the highly popular personal fitness tracker devices. They are wristband style devices that measure personal movement, heart rate, and sleep patterns. Unfortunately, there is an absence of validated data regarding the efficacy of these devices because manufacturers have not submitted their trackers for independent testing as is typically done for health care devices. Our goal was to collect and analyze publicly accessible user data to understand actual user activities, behaviors and social interaction patterns. This baseline is important to support the goals of improving user fitness and health by providing users with knowledge of utilization patterns. Developing a baseline understanding of fitness tracker utilization forms a basis for user healthcare and fitness decisions, along with future tracker development work.

This project focused on the popular Fitbit family of personal fitness trackers. This device has altimeters to count stair climbing, and records pulse rate with a skin sensor. The user's private data is stored on the device until relayed through a personal computer or smartphone, ultimately to reside on either the user's laptop, or within the manufacturer's data storage service. Higher level data such as "steps-per-day" or "calorie expenditure" is derived from sensor measurements. We

believe we are the first to study user activity patterns to include participation levels in social fitness forums. Our efforts result in a realistic picture of user experiences with this device.

1.2.3 Phase-aware Dynamic Time Warping Analysis

Our third project had its genesis in our second project. Fitness tracker users take their devices everywhere, they also enjoy comparing their activity patterns with others for fun and competition. The field of time series similarity comparison relies on the Dynamic Time Warping (DTW) [154] algorithm. DTW complexity is $O(n^2)$ which is costly for long time series. Historically, small duration time series have recorded short discrete activities such as handwritten words, or hand gestures. Longer datasets will be required to capture lengthier activities such as periods of walking or running. Traditional DTW of long time series sequences becomes computationally infeasible. Our observations noted that certain classes of human movement patterns can be cyclical, and also limited within naturally constrained physical envelopes. We can take advantage of this class of sinusoidal movement patterns to improve simulation comparison efficiency. These movement patterns are often experienced by certain sports participants, and transport vehicles traveling through constrained natural and geographic travel routes. We demonstrate that adding an activity phase state descriptor to the time series data similarity comparison results in improved computational efficiency, and more effective space utilization, thereby enabling similarity comparison of longer activity sequences with existing technology resources. Our phase-aware algorithm provides a practical means of comparing longer human movement patterns than

was possible with conventional techniques. Our example demonstrated an 80% improvement over traditional DTW technique.

1.2.4 Secure and Efficient Computation of Private Sensor Data

Smart mobile devices, such as fitness trackers with onboard sensors, have spawned many cloud-based data analysis applications. These services provide valuable information to users, but require users to upload their private sensor data to remote cloud servers. The uploaded data is then compared to stored templates in a data library to identify user activity patterns. Unfortunately, the user loses control of their private sensor data after it is transferred to the cloud-based server. Often, data analysis services use this sensor data for other purposes, unknown to the user. Users wish to protect their private data, which often contains locating information, personal activity records, health profiles, handwritten signatures, speech utterances, and hand gestures. Such information may be immediately sensitive, or may be exploited to extract sensitive information. Our fourth project presents a privacy solution that protects private user sensor data while still obtaining similarity comparison services from a cloud-based server. Our solution also protects the cloud-based server's data template library from exposure to individual users.

1.3 Contributions

This work presents our efforts to adapt technology to human traits and patterns. We reject the notion that users must struggle, or learn “how the computer works” in order to obtain benefit from personal technology devices. Technology should adapt to the human user, awareness of human patterns should be leveraged to

improve technology efficiency. The following four projects reflect our efforts to improve usability, efficiency and security while considering inherent traits of the human user, or leveraging inherent aspects of human activity patterns. Our results in these projects illustrate that investigating and designing new techniques are effective and rewarding, furthering user adoption of improved personal computing technologies. And importantly, users find these improved technologies fun and rewarding to use!

1.3.1 Graphical Password Authentication System

Our first project addressed the problem of older users decreasing or abandoning personal technologies because of difficulties with traditional text password authentication. Our interview study revealed that accessing resources via text authentication was just too hard and frustrating. Users accepted a reduced participation in technological society as the price of avoiding text passwords. We created a new graphical password system based on the selection of images of familiar faces. Our usability study showed that our technique was easy to remember and fast to use. Our study participants actually found it fun to use, a marked contrast to the past when they dreaded having to use text passwords. Additionally, our technique is easy and fast for the physically disabled to use, they just have to select faces on a touchscreen.

1.3.2 Personal Fitness Tracker Usage Analysis

Our project on user fitness tracker behavior patterns revealed many aspects of user motivations to acquire and use these popular personal fitness tracking devices. Previously, there was an absence of knowledge in this area because

tracker manufacturers decline to reveal important information about user behavior patterns with their products. We were able to quantify user engagement patterns discriminated by age, gender and length of device ownership. We believe we are the first to present statistics on personal fitness tracker user behaviors in the context of social fitness forums.

1.3.3 Phase-aware Dynamic Time Warping Analysis

The third project extends current DTW technique to improve efficiency for certain longer time series data sequences that capture “sinusoidal” human activity patterns within constrained activity envelopes. With knowledge of this class of user movement patterns, we define an activity “phase” descriptor as an adjunct to the time series sequence itself. Leveraging the phase state is the basis for our “phase-aware” dynamic time warping technique. This technique provides improved space and computational efficiency over previous DTW algorithms with no loss of data accuracy. We present an example comparison in a simulated use case, verifying decreased complexity over previous methods.

1.3.4 Secure and Efficient Computation of Private Sensor Data

Our fourth project modified the DTW technique to incorporate secure computational primitives that provide user data privacy protections during similarity comparisons with remote data analysis services. This project builds on the secure computational primitives, Homomorphic Encryption (HE) and Oblivious Transfer (OT). Our algorithm protects private user sensor data, and the private data templates stored on the remote cloud-server. Until recently, HE and OT were computationally intensive, limited to servers and laptops. Modern smartphones

now have increased processing power and space. Lab studies with a smartphone and laptop demonstrated our secure processing technique, and demonstrated time and communication load efficiencies during similarity comparison of user time series data sequences.

1.4 Dissertation Organization

We believe that studying and applying knowledge of the user is a worthwhile endeavor to improve the user experience, efficiency and security. Our efforts towards this goal are presented as follows. A review of the literature regarding our human-machine interaction investigations and projects is provided in Chapter 2. We present a novel graphical password authentication system designed specifically for older computer users, who may have physical disabilities, in Chapter 3. Following this we investigate the use of popular commercial fitness tracking devices, quantifying user activities, user population trends, and fitness social interaction patterns in Chapter 4. Leveraging our awareness of the unique data patterns and constraints generated during human activities, we present our extension of dynamic time warping similarity computation techniques in Chapter 5. Finally, we further extend the dynamic time warping technique to formulate a secure computation method to preserve user sensor data privacy in Chapter 6. Our conclusions and future work are provided in Chapter 7.

Chapter 2

Related Work

2.1 Graphical Password Authentication System

The Graphical Password Authentication System provides an easy-to-recall, and easy-to-manipulate technique for older persons to gain access to computing resources. Previous graphical password work has been categorized as either recall-based, recognition-based, or cued-recall. *Recall-based* systems such as Draw A Secret (DAS) and Background Draw A Secret (BDAS) [6] require the user to recreate a previously produced digital drawing. GridMap [7] requires precision finger touching along a series of points on a map presentation. DAS, BDAS and GridMap would be challenging for a user with hand or finger disabilities. *Recognition-based* systems require the user to memorize sequences of abstract images such as emoji, icons, or anonymous faces [4][8]. These sequences are later chosen from amid larger displays containing similar decoy images. *Cued-recall* systems such as Passpoints [9], require the user to memorize a set of specific points within an image and to later accurately re-select the same point sequence. All of these tasks require significant manual dexterity and drawing skills, and significant memorization of abstract patterns. Biddle's survey [10] reveals none of the previous works were implemented with solutions personalized to the history of each individual older user.

Komanduri and Hutchings [11] proposed a system requiring the matching of pictures with accompanying text, both shown simultaneously on a display screen. Users transcribe text shown below their assigned images using the keyboard to

form the password. Entropy is a comparative factor describing the robustness of a particular authentication system to attack. While Komanduri and Hutchings's system achieved an entropy superior to theoretical text password entropy, transcription poses an additional cognitive task, and challenges those with vision or hand-finger impairments.

Users in previous work created written notes describing image, drawing or icon password sequences. Anyone with access to the note could then execute the described password sequence [12]. User notes describing the subjects in the Graphical Password personal sequences are not immediately useable. Attackers with access to the note would have to recognize the subject names and their corresponding images in order to match displayed images with the written description.

In practice, users often simplified their text [13] and graphical passwords, resulting in a reduction of the practical entropy level of the system. Bonneau and Preibusch [14] note that Passfaces [8] results showed predictable user image choices. Passfaces users often chose faces of self-similar race or gender, or chose faces of those deemed especially beautiful. DAS, BDAS and GridMap users tended to make simple, symmetric, or centered pattern choices. Florencio and Herley [13] showed that users also often reduce the practical entropy of their text passwords by choosing simplified text passwords. The Graphical Password design re-randomizes image placement at each presentation and requires all images to be unique within a personal sequence, eliminating the possibility of entropy reduction.

Passfaces [4] required users to navigate multiple screen displays, choosing one facial image on each display. This additional cognitive task requires the user to remember current logical position within a sequence of displays. The Graphical Password design presents all image information on a single display screen.

Older users are open to creative computing opportunities [15] and have shown they perform better at memorizing age-appropriate materials [12]. The Graphical Password system is personalized to the older user, with a large selection of images available in the database reflecting notable individuals from the prime working years of the over-60 user.

Vision and manual dexterity impairments may render the keyboard challenging to use, resulting in higher errors with such techniques as tap re-authentication [16], and video interpretations of external virtual keyboards [17]. The Graphical Password system enables use of the mouse and touchscreen. Both devices are faster than the keyboard for selecting sequences. The touchscreen has been shown to speed up older adult movement tasks by 35% when compared to the mouse [18].

2.2 Personal Fitness Tracker Usage Analysis

Previous work with PFTs has been scattered in nature, relying on easy-to-obtain public data that provides a limited view into PFT user patterns. Previous work proposed numerous models of user activity and behavior, each narrowly focused within an aspect of personal informatics. A user activity and behavior model was developed as a more holistic and organized depiction of the PFT user experience.

Previous work is categorized under the three stages of PFT user activities as shown in the User Behavior and Usability Model in Fig. 2.1. This model encompasses the user's decision to acquire a PFT, utilization of the device, and eventual device abandonment. The three stages are called the Initiation Phase, Utilization Phase, and Abandonment Phase. The Initiation Phase covers the motivating impulse by the user to acquire a device, including making a needs assessment, shopping for a desirable PFT model, activating the device software, and user account, and then learning to use the device. The Utilization Phase incorporates normal wear, tracking, reliability and socialization activities as the user goes about their normal daily routine. Finally, the Abandonment Phase addresses the user's decision to stop using the PFT. Previous work has largely focused on the Abandonment phase, and portions of the Initiation phase. This work describes important aspects of user behavior in the Initiation phase and emphasizes the quantitative assessment of user activities and behavior in the Utilization phase. This work is the first to extensively address socialization by PFT users in fitness forums. Several previous works have extensively studied the Abandonment phase. The Abandonment phase is included in the User Activity and Behavior Model for completeness. It is not expanded further in this work.

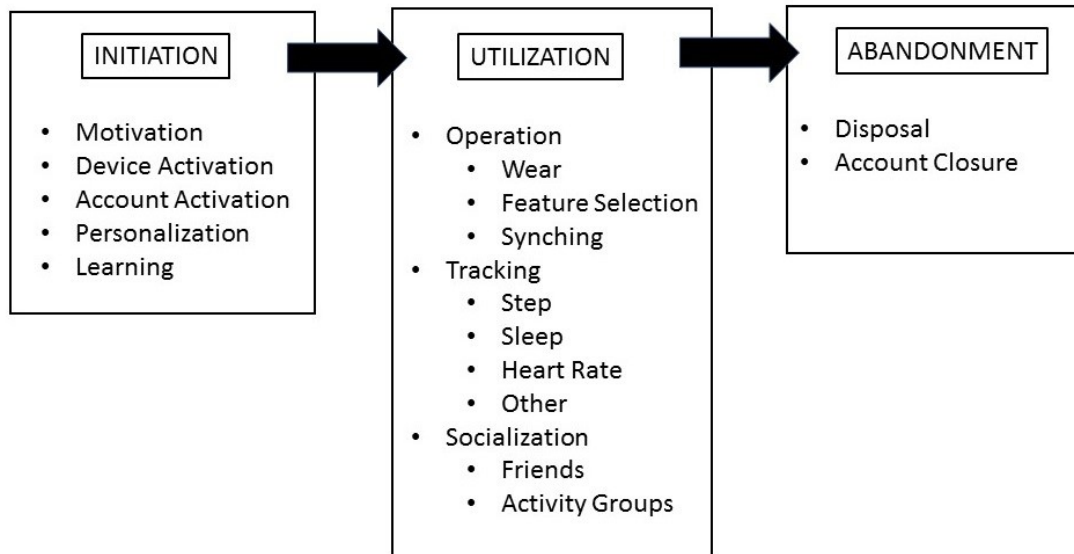


Figure 2.1: User activity and behavior model.

2.2.1 User Activity Models

Previous work with user models has been more narrowly focused on user self-reflection, and informatics derived from user surveys and interviews. Li et al presented a five-stage model comprising the user's preparation, collection, integration, reflection and action stages [29]. Epstein et al [24] proposed a user behavioral change, four-stage model comprising "deciding to track," "selecting tools," "tracking & acting," and "lapsing." Our three-stage User Activity and Behavior Model is described by information gathered from user-posted comments, activity levels, and social connections.

2.2.2 Initiation Phase

Previous work has been focused on user concerns, and level of understanding regarding discrete topics such as device accuracy. Interviews with small groups of subjects, or video analysis were used as the basis for these works. Shin [19]

interviewed a small group to understand intrinsic and extrinsic motivations, noting an initial presence of the Quantified Self (QS)-motivated user. Yang [27] has analyzed user product reviews from a large online marketplace and interviewed a small group of subjects to identify user awareness and technical concerns regarding PFT measurement. Oh [28] analyzed user reviews on a QS community website to identify important user QS tools and experiences. Li [29] has further studied the types of questions users have about their data to support user tool development. Whooley [21] analyzed videos of fitness tracker users to understand user lifestyle goals. In contrast, our work quantified actual user motivations and concerns exhibited by thousands of PFT users. User data was obtained from a wide variety of data sources. An additional understanding of the varying characteristics of data sources was developed.

2.2.3 Utilization Phase

Previous work sought to understand a single aspect of user practices. Fritz [20] interviewed a small group to identify user practices and benefits in fitness-oriented social networks. Rooksby [23] conducted an interview study to understand user practices that interweave PFTs into everyday life activities. Choe [22] analyzed QS videos to understand existing and emerging user practices. Bentley [26] has designed a system to identify health related user activities. Motti and Caine [140] analyzed user reviews of wearable devices in Amazon and found that most interaction problems are attributed to platform issues (e.g., tracking accuracy, usability issues, synchronization, and battery), which contribute to frustration and interruption and may result in abandonment. Epstein [34] has developed data

visualization techniques to show the locations and goals behind specific PFT user movements. Shin [77] interviewed a small group to understand intrinsic and extrinsic motivations, noting an initial presence of the QS-motivated user. Whooley [21] analyzed videos of fitness tracker users to understand user lifestyle goals. Epstein [24] and Li [25] have formally defined models of QS personal tracking activities. In contrast to previous work developing behavior models, this project sought to understand and describe the quantity of actual user exercise practices based on large amounts of post facto user-posted data.

2.2.4 Utilization Phase – Social Engagement

Previous work sought to understand specific aspects of PFT user habits in a social fitness context. This project developed a quantified understanding of the degree and extent of fitness social networks, and variance in user fitness patterns. Consolvo has designed and tested an app to share user step data among friends [35] and further studied the user reasoning behind data sharing decisions [36]. Tsubouchi [37] has used PFT movement data to detect close working relationships among PFT users. Newman [38] has studied user motivations behind sharing health information on social networks. Burke [39][40] has studied the benefits to social well-being of sharing information on social networks. PFT users have embraced the use of existing social networks to share their fitness achievements and receive peer support. PFT manufacturers have developed dedicated social communities for their users. Work is beginning on understanding the characteristics of Tumblr (Chang [41]), Instagram (Hu [42]), and Flickr (Kennedy [43]). Ugander [44] has focused on Facebook's social network structure, and

defined average user characteristics within the network. Park [45] has mined large quantities of Twitter updates from MyFitnessPal users, to discern qualitative characteristics of persistent users versus short-lived users.

2.2.5 Abandonment Phase

Much effort has been devoted to understanding the rationale behind user abandonment of PFT use. Van Berkel [30] has identified obstacles to long term QS-data collection. User PFT sales advertisements were analyzed by Clawson [31], and Lazar [32] conducted interview-style surveys to understand user abandonment. They found users often did not understand the data produced by PFTs or found the devices difficult to manage. Hansel [33] has investigated the user challenges posed by large quantities of health data. Epstein et al. [24] focused on abandonment by studying not only the reasons why people abandon their devices, but also how their lives change after the abandonment. They noted reasons such as: cost of data collection and management, discomfort with information, and data accuracy concerns. After abandonment, some users were indifferent, but some felt guilt and frustration with their failure to accomplish their tracking goals. It was also noted that some users felt a feeling of freedom as they were no longer using bothersome trackers, yet they continued to use knowledge they acquired from the experience of tracking.

2.3 Phase-aware Dynamic Time Warping Analysis

2.3.1 Similarity Evaluation

Dynamic time warping has proven valuable as a technique to compare time series datasets containing measurements of human activity patterns. Human generated time series data sets often vary in length between two individuals performing the same action. Important data features may occur at different offsets within the data even though the two persons performed similar actions. The benefit of DTW technique is enabling comparison of reference datasets of varying temporal qualities and lengths. With DTW, it is possible to compare time series data sequences of discrete human activities with libraries of stored reference data templates. Matching a new data sequence with a similar reference dataset provides identification of the submitted activity sequence. Originating in the speech recognition community, DTW is important in gesture recognition, handwriting recognition, sign language interpretation, and gait analysis [143][144][85], [103][104][105][117][121][122] . Bartolini's work illustrates the use of DTW in retrieving shapes from image databases [152]. Other work uses gestures as pattern passwords to replace traditional text passwords [106][118][119]. Barbon recognizes short speech segments [120]. The uWave [85] authenticates users through their hand-writing signature movements with smartphones. uWave argues that memorizing gesture passwords is less difficult than traditional passwords. WiFinger [107] has utilized multi-dimensional DTW for similarity calculation between channel state information patterns and gesture patterns. Other work uses DTW as a way to use touching movements to authenticate users [108][109]. As

new applications move forward to compare user time series sequences of increasing lengths, time and space requirements increase quadratically.

2.3.2 Complexity Reduction

There has been strong interest in reducing the quadratic time and space complexity of the classic DTW algorithm. These approaches tend to either constrain the populated cells in the distance matrix, or create an approximate warp path solution through use of data down sampling, or use of the mean of aggregated data sample groups. Sakoe & Chiba, and Itakura proposed limiting distance computations to a diagonal band or parallelogram [143][144]. The restricted space in the distance matrix reduces the number of required computations, restricts the warp path construction and increases the potential for missing the optimal warp path solution [143][144]. FastDTW was designed to approximate DTW through a multi-level approach that has linear time and space complexity but at a loss of resolution that loses fine-grained detail about human activities [146]. Coarse-DTW reduces the complexity of DTW through down sampling of datasets with resultant loss of fine-grained details in the dataset [151]. SparseDTW relies upon similarities between two sequences, re-quantizes the data samples to lower-resolution bins, then creates sparse matrices to formulate the optimal warp path [149]. Keogh devised a Piecewise Aggregate Approximation technique by windowing the data and utilizing the mean value within each window in the DTW calculation [145][147]. Optimizations of the DTW algorithm will be necessary to improve efficiency [148]. Approximation techniques such as FastDTW [124], Lucky Time Warping [125], and Zhu's work [126] may not prove accurate enough to discriminate between a

server's "somewhat similar" data template library population accurately. PrunedDTW is not an approximation but an exact technique to eliminate DPM cells that cannot lead to the optimal warp path solution [127]. Constraint techniques risk omitting the true optimal warp path solution in favor of a solution within the constrained distance field. Approximation techniques lose a degree of data granularity, an important difference from the Phase-aware technique.

2.4 Secure and Efficient Computation of Private Sensor Data

Related work for the traditional DTW may be found in Section 2.3.1. That work relied on a single distance matrix, usually located at a server to hold the intermediate and final data products of the similarity comparison of two time series data sequences. This project strives to keep user data and server data private from each other, and therefore requires a two-part distance matrix. The user keeps their private sensor data within their part of the distance matrix. The server keeps their data template private within their server. Privacy-preserving applications and tools such as Homomorphic Encryption, and Oblivious Transfer are the building blocks of our project. The similarity comparison product is constructed through exchange of encrypted values for use as components in homomorphic computations.

2.4.1 Privacy Preserving Computation

Earlier privacy-preserving application techniques such as profile-matching on social networks [110], authentication through biometric data matching [111], wireless network data aggregation [112], have relied upon additive homomorphic

computations [87]. Huang has identified practical performance issues with placing privacy-preserving applications on Android smartphones [83]. Atallah's [113] work utilized a split distance matrix to privately compute edit-distance between sequences held by two parties, however it cannot hide the optimal path from the other party. Zhu et al. [87], presented a privacy-preserving DTW protocol based on homomorphic encryption that suffers from poor scalability with increasing time series length due to the use of dummy data. Zhu's method sacrifices security for improved performance by using 64-bit homomorphic encryption. Our work explores performance obtainable on a smartphone with stronger 512, 1024, and 2048 bit encryption. Compared to the state-of-the-art, our Secure Computation project shows that improved security through use of computations with stronger encryption on a smarthone are achievable.

Chapter 3

Graphical Password Authentication System

3.1 Background

User authentication through keyboard entry of text passwords is a daily activity for most users. Yet not all portions of the user population find this to be an easy task. After interviewing a group of older volunteers about their human-computer interactions, it was confirmed that creating, recalling, and managing strong text passwords were very challenging tasks [4][5], and motivated the design of a new password authentication mechanism specifically for older users, a system that would be cognitively and physically easy to use, and also foster feelings of user well-being and competence. The Graphical Password System enables a user to choose a personally meaningful set of black and white facial images as their personal password sequence, known as the target image set [46]. A set of unfamiliar, yet similar images, known as the decoy image set, are appended to the user's target image set to form the displayed image set. The complete set of displayed images are randomized for each presentation to the user. The image identifier numbers associated with the target and decoy images constitute the graphical password definition within the computing system. An example of a sixteen-image display is shown on the right in Fig. 3.1. The numbered grid cells on the left of Fig. 3.1 indicate this user's correct image selection sequence to successfully authenticate, for this instance of the randomized user display presentation.

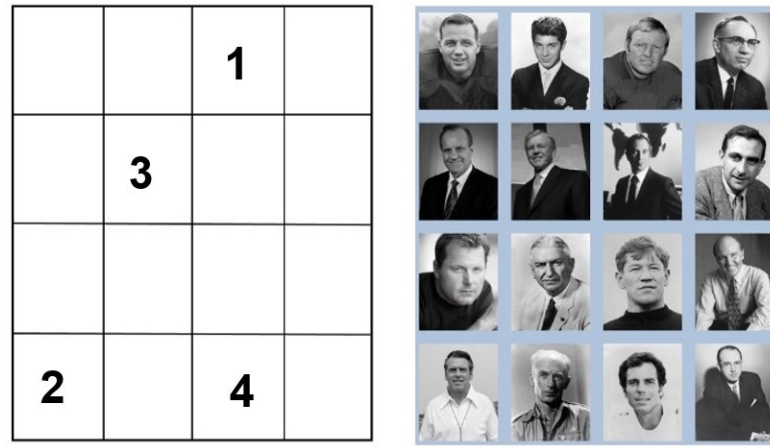


Figure 3.1: Graphical password example.

The Graphical Password technique leverages the unique cognitive and neural abilities that humans have for processing and recognizing faces. The Fusiform Face Area (FFA) in the temporal region of the brain is dedicated to the processing of faces [47], beginning from infancy [48]. The neural processing of faces in the FFA has been extensively documented via MRI studies [7][49][50]. The built-in human ability to recognize faces from an individual's personal past history is an easier cognitive task than recollecting memorized sequences of text, symbols or anonymous facial images [51][52].

The U.S. population is aging, and having difficulty using computer technology. By 2030, more than 20% of the U.S. population will be 65 and older, contrasting with 13% in 2010 [53]. In 2013, 41% of U.S. adults aged 65 and older did not use the internet and one-third of these felt that the internet was not very easy to use [54]. Among users aged 77 or older, fully 62% do not use the internet [55]. As

more of society's functions move online, it is important to study and facilitate older user engagement with computing and the internet [56][57].

During our interview study, volunteers indicated that typing strong text passwords was physically challenging because text passwords require good vision to search computer keys for required letters and symbols. Finger, hand, and arm mobility issues can also impair fine motor skills needed for successful typing. The Graphical Password system eliminates the need to enter text entirely. Each user recognizes and selects their personal target image sequence from within the randomized display using either the mouse or applying their finger directly to the touchscreen.

The password strength or entropy of the Graphical Password system is comparable to short text passwords and superior to PINs. Increasing the entropy of the system is possible by increasing the number of images on the display, and increasing the number of images in the user's chosen target sequence. Increasing entropy potentially results in increased authentication time, and reduced recall performance as users search among a larger set of images or strive to recall a longer personal sequence.

Previous work and volunteer interviews revealed that users often kept written notes of text passwords to aid recall. Unfortunately, loss of the note constituted an immediate password compromise. Written descriptions of the graphical password sequences are not literal physical descriptions. User notes may cite subject names or occupations. Such information may not be recognizable to an adversary gaining possession of the note. Users of the Graphical Password system can create

personalized sequences of images that are very meaningful. Some of the interview volunteers shared that they did not need to keep notes because their chosen sequences had strong personal associations, making them hard to forget.

A usability study was conducted to measure recall and timing performance of the Graphical Password design. We first assembled a database of 550 black and white images, each image coded as to physical attributes, and occupation of the image subject. An image sequence selection tool was created so users could efficiently browse the database based on occupation of the image subject. In the usability study, each volunteer chose three personal target image sequences in lengths of four, seven, and ten images. A series of authentication exercises was created to measure recall rates and elapsed password sequence selection times with varying display image densities, password image sequence lengths, image arrangement patterns, and input device modalities. Additional exercises measured text entry time using the keyboard for comparison purposes. Exercises were repeated at one week or longer intervals to measure user improvement through training experience.

3.2 System Design

3.2.1 Design Motivation

An open-ended interview-style technology survey was conducted with twenty-six (n=26) computer users over the age of 60. The goals were to understand their computing concerns and motivations, and identify technology areas for enhancement germane to this older user population. Strong text password creation, management, and recall emerged as a major user issue. Some older volunteers deliberately chose to limit their use of technology in order to avoid

accumulating more passwords. Other volunteers only used one or two passwords at multiple internet sites. Representative volunteer comments obtained during interviews are listed in Table 3.1.

Nineteen of the interview-style study participants answered more detailed questions focusing on password creation, management, and recall strategies. None of the nineteen personally used strong passwords meeting the classic definition of a series of characters including upper/lower case, numbers, and symbols, without personally meaningful text sequences. All but one of the volunteers prepared text passwords containing character sequences with strong personal associations such as a child's name, previous phone number, pet name, or spouse's birthdate. Such information may be easily findable by an adversary using the internet.

All but two of the volunteers routinely wrote down passwords, making them available to anyone with access to the written record. Two volunteers refused to use more than two passwords, and accepted the resulting lifestyle limitations on internet and computer use.

Our motivation was to design a new password mechanism specifically for older users, a system that would be physically easy to use, and foster feelings of well-being by enabling user competence, and relatedness to their past memories [51]. By relying on personally meaningful images, it is hoped that the tendency to write down explicit password descriptions will be lessened. It would be hard for users to hand draw accurate image reproductions to make a personal note. If a user does write down a list describing image subjects, an attacker must understand the

description to make a match possible to an image subject name. As an example, a music fan may choose images of Kate Smith, Glenn Miller, Dizzy Gillespie and Louis Armstrong for his password sequence images. The attacker finding the list of names “Kate, Glenn, Diz and Louis” will have to understand the names and research each person’s appearance before attempting their attack.

Using a single display screen for the entire authentication process reduces the need for users to remember selections from previous screens, and reduces the number of hand and finger actions.

Table 3.1: User interview comments

User comment	Comment topic
It is annoying to create passwords, it is an extra effort and hard to memorize.	Password creation
It is hard to make a password that is halfway safe.	Password creation
I only use one password in order to keep life simple.	Password usage

3.2.2 Design Components

The Graphical Password system design components consist of a collection of black and white images, software for user selection of target images forming personal user sequences, software to facilitate selection of user decoy images, laptop computer equipped with touchscreen and mouse, and usability study software. The usability software displayed a sequential series of displays with varying configurations of images. The user applied input from the touchscreen or

mouse. The usability study software recorded user results and the elapsed times of user actions.

Each graphical password is formed from the user's target image set and their decoy image set as shown in Fig. 3.2. Each image has a unique image identifier number. The complete graphical password is formed by the set of target image identifier numbers in correct sequence appended to their personalized set of decoy image identifier numbers. Each user's personal target image sequence, chosen based on strong personal memories from the past, forms a "secret key," unique to each individual. Only the user recognizes their personal sequence when viewing all the images on the display.

The complete graphical password is stored by the computer in association with the user's account username, comparable to storage of a traditional text password. The user authentication software would access an image database to retrieve the correct images for display and selection by the user. The image database could be installed locally or accessed from a web service over the internet via a secure channel. User amenities such as password hints and password reset features could also be adapted for use with graphical passwords.

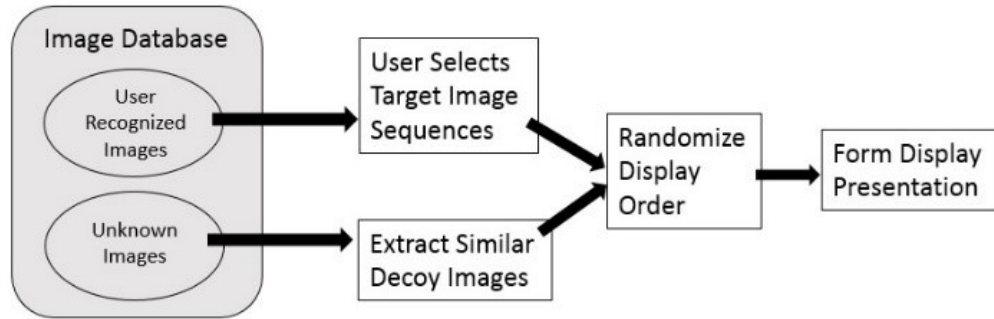


Figure 3.2: System display design.

3.2.3 Entropy Analysis

A goal of the Graphical Password design is to achieve a level of entropy, or password strength, comparable or superior to traditional text password or PIN code systems [58]. Entropy is characterized as the strength of a password system, or the unpredictability of possible values in a password sequence. A password system with higher entropy is more resistant to guessing or brute force attacks, but may become harder to memorize or recognize due to increased symbol complexity, increased password sequence length, or increased user display density. Higher entropy configurations in the Graphical Password system may increase user authentication time as users search for more password sequence images from among higher density displays.

The entropy of the Graphical Password approach is described from three perspectives. First, the information entropy of the symbol set formed by the image database is characterized. Second, the password strength of the system from the perspective of an attacker with direct access to a user system is described. Third,

the entropy of a client-server Graphical Password configuration is described from the perspective of an outside attacker emulating a user. For comparison purposes, equal length text and image password sequences are assumed in each description.

Information entropy is defined as the \log_2 of the number of possible passwords, provided that each symbol in the password is independent [58]. A random password's entropy H , is defined

$$H = L (\log_2 N),$$

where N is the number of symbols available to form the password, and L is the password symbol length. A text password consisting of case-sensitive alphanumeric symbols a-z, A-Z and 0-9 has 62 possible symbols available to be chosen for each password character. Given a password length of eight characters,

$$H_{\text{text}} = 8 (\log_2 (62)) = 47.6 \text{ bits}$$

In the Graphical Password approach, each image is represented by a unique image number that constitutes one symbol in the password sequence. A graphical password image sequence that does not permit repeating images will have as many possible images available for the first password image as there are images available for selection. In the usability study there are 550 images in the database. One less image is available for each subsequent choice. For the eighth image,

there will be 543 possible image choices. The binary log of the number range 543 to 550 is rounded and represented as 9.1 in the comparison. Given a Graphical Password equal length sequence of eight images,

$$H_{\text{graphical}} = 8 \times 9.1 = 72.8 \text{ bits}$$

$H_{\text{graphical}}$ is a 53% improvement over H_{text} .

The second perspective is that of an attacker with direct access to a user's personal computer. Faced with attempting to enter a four-character text password, there are N^M possible combinations where $N = 62$ possible valid text characters and $M = 4$ choices to be made. To exhaustively try all possible text combinations will take $62^4 = 14,776,336$ attempts. Facing a Graphical Password display of sixteen images and choosing the correct permutation of four images will take $N! / (N-M)! = 43,680$ attempts. In this case, exhaustively trying a text password, at three attempts per minute before a system-imposed timeout of ten minutes, it will take 111 days of non-stop attempts to exhaust all possibilities. For comparison, a four-digit numeric PIN offers 10,000 possible combinations. A common touch screen password mechanism requires the user to select the correct symbol sequence from a grid of identical static symbols such as dots. A configuration requiring the user to select the correct sequence of four non-repeating symbols from a grid of sixteen symbols would have an entropy of 43,680 possible variations. Since the correct symbol sequence does not vary in location, a smudge pattern could develop on the touchscreen surface that could aid an attacker. The Graphical

Password approach eliminates the possibility of a smudge pattern by randomizing each display presentation.

The third perspective is that of an attacker attempting to log into a user account on a website from the attacker's personal computer. In this scenario, if a user had a valid four-character text password already stored at the website, the attacker must submit a correct four-character password. As described previously in the second perspective, there are $62^4 = 14,776,336$ attempts to be made by the attacker to exhaust all possible combinations. With the Graphical Password design implemented in a client-server configuration, website servers would already possess a pre-existing record of all sixteen images forming the user's display along with a record of the user's valid four image sequence. Each authentication attempt with the Graphical Password system requires the attacker's client to submit to the server, via a secure channel, sixteen symbols representing the chosen image numbers of the user-selected sequence along with the unchosen decoy images. An attacker with no knowledge of any of the images in the user's display must submit the correct combination of sixteen image numbers in addition to the correct permutation of four image numbers forming the user's chosen target sequence. Assuming the attacker knows that the database is currently limited to 550 images, there are 2.69×10^{30} possible combinations of the sixteen images that must be attempted, *each* combination with 43,680 possible four image permutations.

The entropy of the Graphical Password design may be increased by either increasing the number of images in the display or increasing the length of the

password image sequence. The usability study was designed to measure the effects of increasing entropy on user authentication success and timing.

Fig. 3.3 illustrates many of the configurations that were implemented in the usability study described in Section 3.4. Fig. 3.3 shows the four and ten image sequences, along with the fifteen, sixteen, twenty-five, thirty-six, and seventy image density displays. The effects on user recall and elapsed time as entropy increased, were measured and captured. Results of the usability study are presented in Section 3.5.

Fig. 3.4 provides a comparison of the Graphical Password entropy under six configurations of password sequence length and display image density. Each configuration is denoted within Fig. 3.4 by GP-xxfmyy where xx is the sequence length and yy is the display density. Entropy levels of varying PIN, text, and actual text [13] systems are also plotted along with notable graphical password systems described in the literature review of Section 2. Entropy is expressed as the bit strength or binary log of the number of possible guessing attempts for the listed password system configuration. While the four-image configuration is comparable to short text passwords and superior to four-digit PINs, the client-server design implementation offers the potential for higher entropy than traditional text passwords of length eight characters.

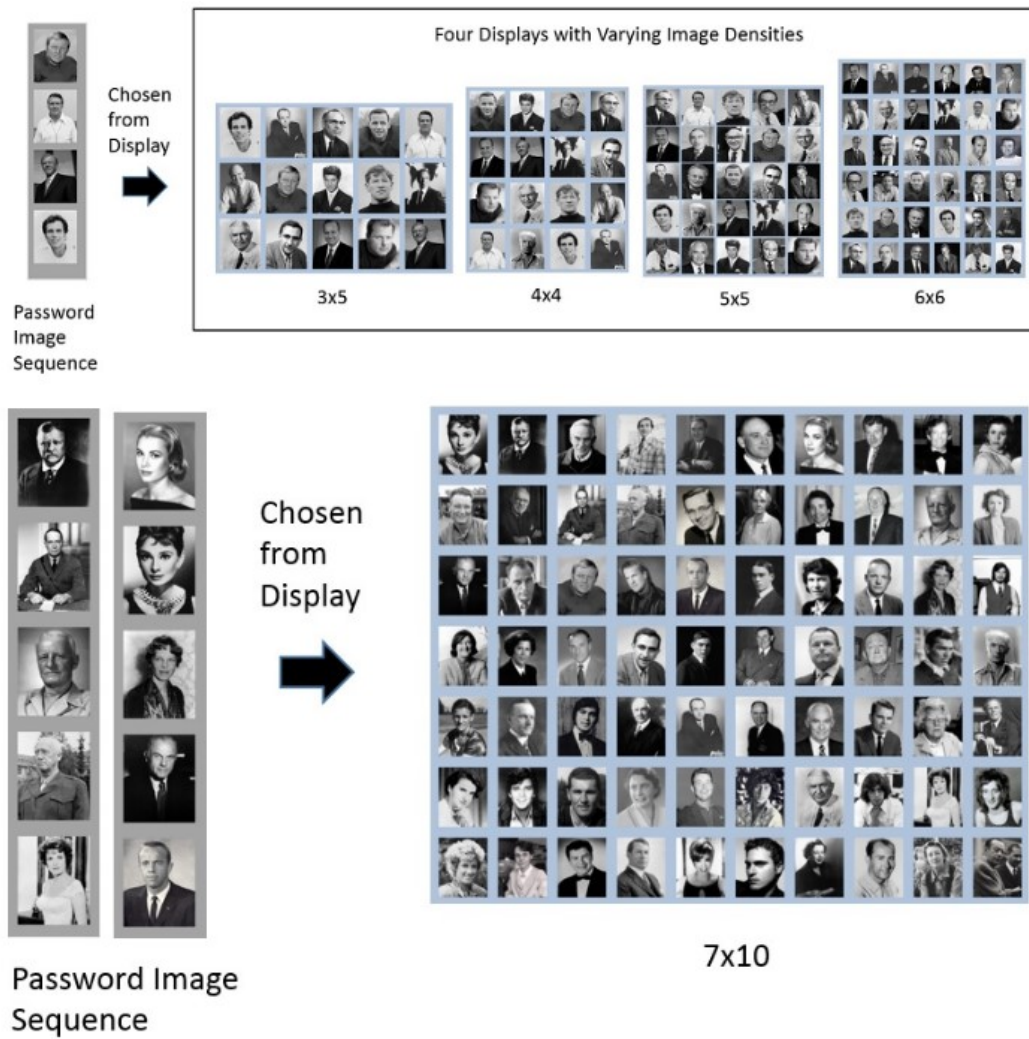


Figure 3.3: Configuration examples.

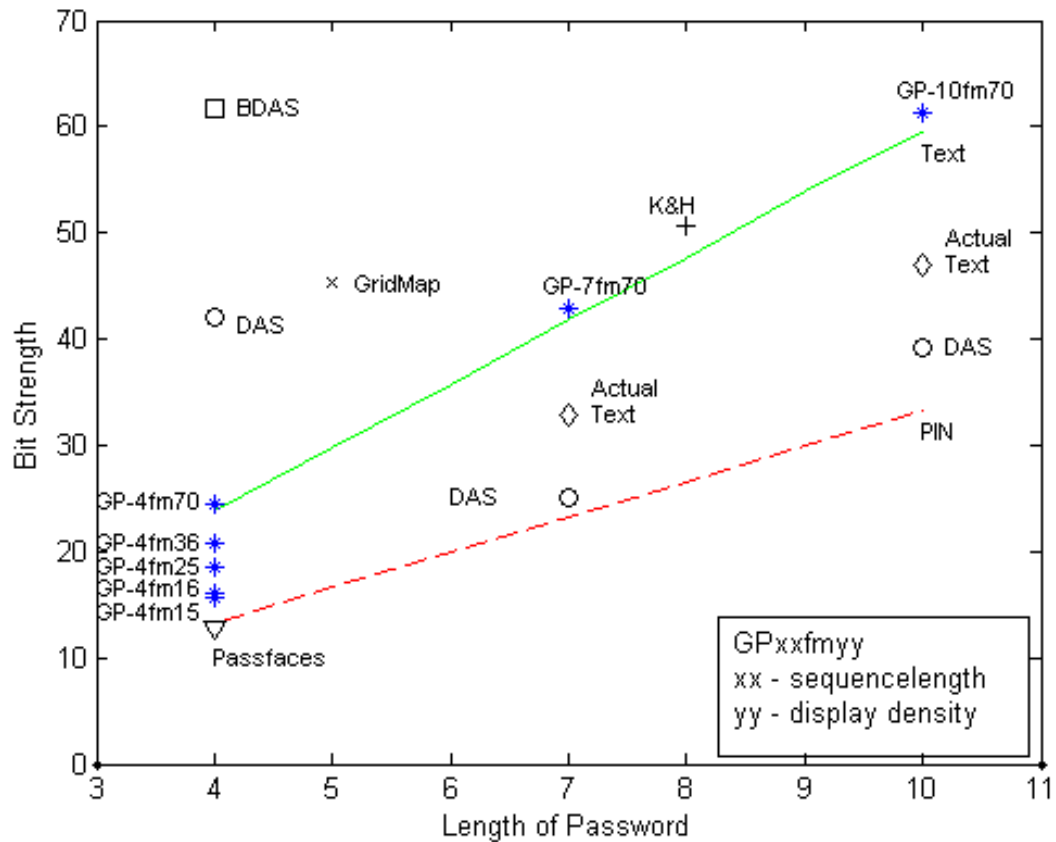


Figure 3.4: Entropy comparison with previous work. Blue asterisks denote varying configurations of Graphical Password sequences.

3.2.4 Image Database

550 black and white facial images of notable figures from the past were collected, processed, and coded. These subjects were prominent in many areas of U.S. culture during the early-to-mid working years of the over-60 user. While the Graphical Password system could be used by those of any age or cultural background, a deliberate decision was made to choose images familiar to older U.S. study volunteers to leverage the cognitive advantages offered by the FFA. For future work, a production version of the Graphical Password system could

permit the user to identify their age and cultural heritage, and then offer candidate target images that are likely to resonate with the user's cultural background.

It is important that images appear to be similar on the screen to defend against shoulder surfing attack. All collected images were converted to black and white. Images were then digitally manipulated to remove noticeable identifying team logos, military insignia or corporate markings from clothing and backgrounds. Prominent features noticeable from a distance such as large jewelry or boutonnieres were also digitally removed. Images were cropped down to one of three sizes: head and shoulder, head to waist, and full body.

Each image has been coded as to subject body size, sex, race, gaze direction, attire, image foreground color, background color, and brightness level. Attire codes indicate if image subjects are wearing glasses, hats or notable accessories. Foreground and background coloring is coded as white, black or gray. Gaze direction indicates if the image subject is looking straight ahead into the camera or to the right or left. Brightness level is a description of the overall image tone and is coded as light, medium or dark. By selecting decoy images similar in appearance to target images, an attacker is challenged to guess the password sequence based on gross visible image attributes. Attackers must be physically close to the display to discern finer differences in image details. For future work, color profiles and brightness levels may be quantified through image spectrum analysis and serve as inputs to a decoy image selection model.

For the Graphical Password technique to be effective, it is necessary that decoy images be unfamiliar to the usability study subjects. To assess the suitability of the image collection to serve as a source for decoy images, volunteers were asked to evaluate the images for familiarity. Sixteen older (over-60, average age 71.9 years) volunteers and five younger (under-60, average age 37.2 years) volunteers manually reviewed each image. Volunteers assigned image recognition ratings from a 5-point scale. The scale ranged from 1 = Do Not Recognize to 5 = Know Well.

Fig. 3.5 illustrates the results of this review with over-60 users shown in red and the younger group shown in blue. A mean of greater than 50% of images were rated as “not recognized” by both groups. This provided evidence that the database has enough images to form strong decoy image sets. Fig. 3.5 also illustrates the younger (blue) user rate of non-recognition of images is 19.2% higher than older (red) users, and younger users strongly recognized 14.4% less than older users. This provides evidence that this set of images is more recognizable by the target population of over-60 people.

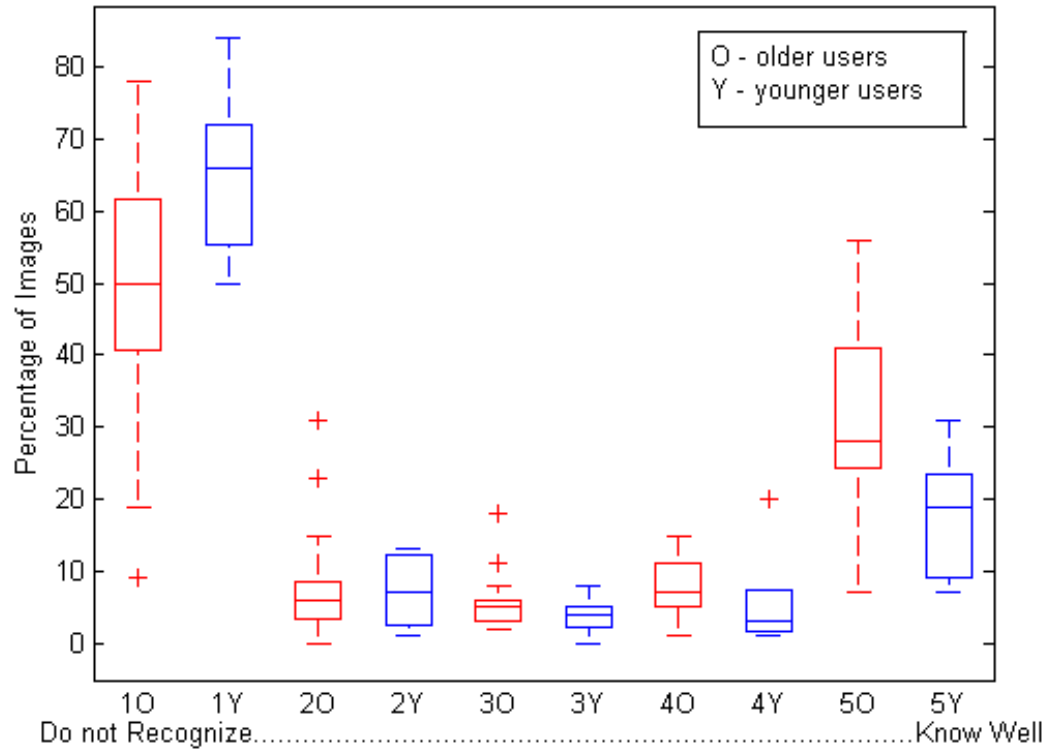


Figure 3.5: User image recognition.

3.2.5 Target Image Selection Tool

The MATLAB image selection software tool enables older users to efficiently select personally meaningful images based upon their unique personal interests. As shown in Fig. 3.6, the user interface presents a series of radio buttons enabling selection of a specific category of images based on image subject occupation. Some examples of occupations are actors, football, golf, writers, and Presidents. Users could choose their personal image sequences from just one category or choose each image from a separate category. Image categories reflect a wide range of U.S. cultural interests such as sports, entertainment, journalism, politics, industry, etc. Relying on images from a single category to form a personal sequence increases the risk of an attacker successfully performing a thematic

analysis on the images in the display presentation. A security policy to address this risk could require users to select images from more than one occupational category.

Users form their personal target password sequences by browsing among the thirty-three categories of images. Users cycle through each category by using the “Go Back” or “Go Forward” buttons shown on the right side of Fig. 3.6. Once the user has selected an image for their personal sequence, that image was displayed at the bottom of the screen in the order chosen. The tool allows users to change selected images if desired. The tool measured level of effort expended by users in choosing their personal images by capturing elapsed time to choose each image and number of images examined by each user. For the study, each user chose three sequences of length four, seven, and ten images. Longer sequences were built upon shorter sequences. As an example, a user’s seven image sequence consisted of their four-image sequence with three additional images appended. During the usability study, it was observed that each user enjoyed the image sequence selection experience, often reminiscing about personal associations as familiar images appeared on the screen. Each user was careful to choose images with strong personal associations.

The decoy images that accompany the target images are chosen based on the user’s unfamiliarity with subjects within each decoy image. As discussed in Section 3.2, volunteers previously evaluated each image in the database as part of the effort to ensure that a sizeable pool of unrecognized images were available for the study. For the purposes of the usability study described in Section 3.4, project

personnel selected decoy images that were unknown to the user and possessed physical characteristics similar to the user's target images. As an example, a user selecting images of blond women for their personal target password sequence will find that the decoy images are also of blond women. The coding in the image database facilitated the identification of suitable decoy images. If all of the user target images featured subjects wearing light clothing on a dark background shown from the waist up, the coding facilitated the selection of decoy images with similar image composition. During the usability study we observed that volunteers strongly preferred some occupational categories over others. For future work, a production version of the Graphical Password system could automate the decoy selection process by having users identify specific occupations with no personal associations, thereby enabling the software tool to automatically draw decoy images from those unfamiliar occupational categories.

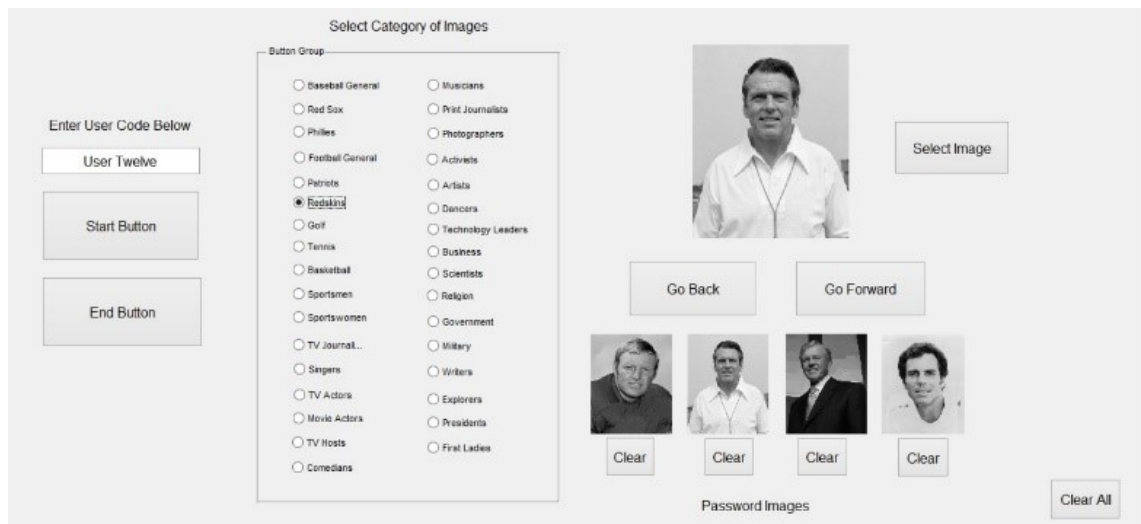


Figure 3.6: Image selection tool.

3.3 Usability Study Design

The usability study software displayed varying screen configurations of increasing image density during a series of exercises. Each exercise accepted user inputs in the form of touchscreen or mouse image selections, recorded user action elapsed times, and authentication success/failure. The usability configurations ranged from a 3x5 display of fifteen images to a 7x10 display of seventy images. Success was defined as user selection of their target image sequence in the correct order. If the user is unsuccessful at selecting their correct sequence, then the authentication request is considered a failure, the failure is recorded, and the display is refreshed with a re-randomized display of images. The image arrangement re-randomizes with each display presentation to include screen refreshes. A casual onlooker will not observe a static placement pattern in the location of any images. Re-randomizing the arrangement of images also defends against smudge attacks [59] by ensuring that all portions of the screen will be touched by the user's finger. A security policy invoking a lock-out interval upon three successive failures or screen refreshes provides further defense against brute force attacks.

The cognitive challenge presented is that while longer password sequences result in greater entropy, they add to the user memorization, recall, and visual search burden. A goal of this work was to measure the time needed to find and select target password images within surrounding decoy images as screen image density increases. The probability of choosing correct images in incorrect order also increases with personal sequence length. Increasing the number of images on the display to achieve higher entropy forces each image to be smaller, and

therefore harder to see and discern image details. Several questions arise that the usability study seeks to answer. How do users search the displayed images? Do users consciously adopt specific search patterns looking for their target images? Does peripheral vision aid in speeding up the search for the target images? Do users remember the current locations of subsequent target images encountered while searching for the initial members of the target image set? Do target image sequences become too long for effective recall and search? Can display screens have too many or too small images for effective search?

3.3.1 Study Procedures

Nineteen volunteers (n=19) were recruited, all over the age of 60, from the local community. After signing the consent form, volunteers were provided information about study goals, definition and benefits of strong passwords, and a description of the tasks they would be expected to perform. In contrast to previous work, individual meetings were set up with volunteers at convenient off campus locations. This strategy ensured that all volunteers completed the exercise sessions. The most popular locations were in volunteer homes or at local coffee shops. While meeting outside the lab environment was not as time efficient, it had the advantage of putting volunteers at their ease in familiar settings.

During the initial session, each volunteer utilized the Graphical Password software tool to browse the database of images and select their target image sequences. Volunteers often shared that they developed a mental story or acronym to aid recall of their image sequences in the correct order. The mental

story was formed from the user's previous personal association with the subjects in the images.

Volunteers were contacted at least a week after choosing their images, to perform a series of authentication exercises. In total, 74 sessions, each consisting of 44 individual exercises were held that lasted from an hour to an hour and a half each. Each exercise consisted of two screens. An introductory screen provided brief instructions and allowed the user to indicate when they were ready to proceed to the exercise displayed on the second screen. The purpose of the introductory screen was fourfold: allow the user to control the pace of the exercises, provide a small break to allow the user's short-term memory to clear from the previous exercise, provide an opportunity for the user to ask questions without adversely affecting exercise timing, and clearly delineate the start time of each exercise. Many of the volunteers described themselves as not comfortable or confident using computers. The introductory screen was deliberately intended to foster user confidence by providing the user with control over the pace of exercise activity.

The second screen consisted of the images displayed in a grid pattern similar to Fig. 3.1. An adjacent space was dedicated to hold selected images. Each user chose their image sequence and then selected the "OK" button to signify exercise completion. Immediate feedback was presented via a success or failure message in a text box. The user then acknowledged the feedback before proceeding to the next screen. If the password sequence was incorrect, the display screen reloaded with a re-randomized image pattern and the user tried again. If the password sequence was correct, the introductory screen for the subsequent exercise

appeared. After the last exercise, elapsed times were displayed for the user. This prompted much discussion with volunteers who were curious about the processes running behind the scenes, and the techniques used to interpret timing information. User comments were recorded, and specific questions were asked regarding conscious visual search techniques and ease of finding target images. Volunteer comments are listed in Table 3.2.

It should be noted that throughout this study, participants were permitted to keep personal notes about their chosen password sequences. Personal notes were not permitted to be consulted during volunteer sessions. This is consistent with their current widespread practice of keeping written records of personal text passwords.

The suite of forty-four exercises consisted of thirty-five exercises requiring selection of a personal password image sequence and nine exercises requiring the typing of given text passwords for comparative performance analysis. Personal password sequences varied among lengths of four, seven, and ten images. Display screen image densities ranged from 5x3, 4x4, 5x5, 6x6 to 7x10. Sequences of length four were chosen from all display densities. Sequences of length seven, and ten were chosen only from the 7x10 display densities, as lesser densities did not provide sufficient display space to conceal target images among the decoy images. Volunteers went through the exercises initially using the mouse and repeated the exercises using the touchscreen to allow analysis of performance differences between the two input modalities.

To investigate volunteer search patterns, eight of the exercises were designed with images deliberately either clustered together or arranged in a linear pattern.

User images close together in specific patterns enables analysis of peripheral vision effects on image recognition. The intuition was that clustering may speed up image recognition and reduce search time.

Five exercises employed “pseudo-random” image placement patterns to enable analysis of visual seeking patterns constant across all volunteer sessions. All remaining exercises were true random arrangements generated at each exercise invocation. Volunteers were not provided any information about specific pattern arrangements before their exercise sessions.

Varying image sizes and densities permit analysis of the effects of image size on visual search and perception of image details. The intuition was that smaller images may be more challenging to view by an aging user population, resulting in increased elapsed authentication times and increased recall error rates.

Varying image attributes such as differing or similar foreground and background colors may affect speed of recognition. The intuition was that some images will prove harder to find, increasing sequence selection times. For future work, a formal definition of an optimal facial image may facilitate image usability, and be a valuable reference in a decoy image selection model.

3.4 Usability Study Evaluation Results

3.4.1 Recall Performance

Nineteen volunteers completed a total of 995 discrete exercises selecting personal password sequences from varying display image densities. Thirty errors were recorded in the 995 exercises for a successful recall rate of 97%, superior to all but two previous works (see Table 3.3). This was especially notable given that our

work is the only project with participants over the age of 60. Seven of the thirty errors occurred with the touchscreen. The remaining twenty-three errors occurred using the mouse. The reduced error rate with the touchscreen may be a result of either the ease and immediacy of directly touching the screen with the finger, or a result of the ordering of exercises. Touchscreen exercises always followed mouse exercises. The mouse exercises could have served as memory reinforcement, and equipment and procedural training for the subsequent touchscreen exercises. The sources of errors are shown in Table 3.4 presented in order of frequency of occurrence.

Errors associated with memory, such as recall, transposition and omission were few. Some volunteers offered comments that they used mental stories or mnemonic sequences to aid recall. One individual chose a chronologically ordered sequence of U.S. Presidents. Another chose eastern major league baseball team coaches. A third created a mnemonic of the last names of their image subjects.

Errors recorded due to inadvertent equipment issues included pressing too hard and registering a “double click” on an image without intending to select that image twice in a row. The test software did not allow the volunteer to “backspace” to correct such errors which were frequently recognized immediately. After disregarding the ten errors originating in equipment issues, the recall rate becomes 97.4%. The demonstrated recall rate is comparable to the best previous work, yet the Graphical Password system also makes the challenging task of password entry easier and fun for older users.

Table 3.2: Usability study comments.

User comment	Comment topic
It was interesting. Very advantageous for seniors, young people wouldn't recognize images from earlier times.	Overall opinion
I memorized those people before I got home, and I live close by."	Memorization
It was interesting.	Overall opinion
It was fun.	Overall opinion
I have to think, but it's easy thinking.	Recall
It was easy to quickly recognize my chosen images because I have followed the careers of those individuals all my life.	Recall
It has been a week and I cannot forget my password image sequence.	Recall
I was mentally saying the names in my head.	Memorization
I can remember my image sequence easily after a week and I cannot normally remember my passwords or the cell phone numbers of friends.	Recall
My finger got ahead of my brain and I touched my third image instead of my second image.	Recall
I can visualize these photographs, I like the people, they are like friends.	Recall
The seventy-image display took too long to hunt through and would not be practical in real world application.	Searching for images
I was struck by the sports guys shown on the display so I chose them.	Thematic analysis during guessing attack

3.4.2 Authentication Timing

Median authentication times with four-image password sequences at varying screen densities are shown in Fig. 3.7. Blue asterisks indicate results from 324 exercises with the mouse, black diamonds indicate results from 285 touchscreen exercises, and red triangles denote percentage performance improvement of the touchscreen over the mouse. Overall results show median time improvement of 32% using the touchscreen versus the mouse. Median time to select a four-image password image sequence at a low density was about ten seconds. This is less time than many volunteers would take to look up a text password in their personal notes. As screen density increased, time needed to select a four-image sequence increased. Many volunteers commented that searching the 7x10 screen displays took too long, ranging from 30 to 35 seconds.

Table 3.5 compares the time ranges taken to perform a successful authentication versus previous work. The minimum recorded time to use the system was 7.4 seconds, better than half of the other systems. The maximum time was 33 seconds, substantially longer than other systems. It must be mentioned that the other systems all conducted usability studies with predominantly young, college age participants. Our usability study was conducted entirely with participants over the age of 60, some significantly over 60 with minor physical disabilities, some with no ability to touch type.

Table 3.3: Password recall comparison.

Password System	Technique	Recall	Ages of Volunteers		
			18-30	31-59	60+
Passhint	Art, Object	97.5%	✓		
Graphical Passwords	Facial Images	97%			✓
Passhint	Mikon, Doodle	95%	✓		
DAS #2	Drawing	95%	✓	✓	
BDAS #2	Drawing	95%	✓	✓	
Gridmap, two weeks	Map Points	83%	✓	✓	
Passhint Original	Mikon	71%	✓		
Passhint Original	Doodle	66%	✓		
Pictures	Pictures	67%	✓	✓	
Gridmap, one week	Map Points	61%	✓	✓	
DAS #1	Drawing	57%	✓		
Passhint Original	Art	55%	✓		
BDAS #1	Drawing	50%	✓		
Characters	Characters	50%	✓	✓	

Table 3.4: Error categories.

Description of Error	Count
Selected incorrect image due to incorrect recall	8
Selected incorrect image due to equipment issue, e.g. inadvertent double-click or double-touch	10
Transposed valid images	6
Omitted valid images	6
Total errors	30

Table 3.5: Authentication timing comparison.

Password System	Time Range
Graphical Password System – mouse select four from sixteen	7.4 to 33 seconds
Passhint [20]	13 to 17 seconds
Pictures [19]	13.7 seconds
Characters[19]	10.5 seconds
DAS [27]	4.5 to 7.5 seconds
DAS Disappearing Stroke [27]	5.3 to 9.6 seconds
DAS Line Snaking [27]	5.9 to 12.4 seconds

3.4.3 Individual Image Selection Timing

Fig. 3.8 shows the separate individual image selection timing for the same volunteer exercises whose median time results are shown in Fig. 3.7. At each screen density (with one exception) median time needed to find a subsequent

image always decreased. Some volunteers commented that they noted the locations of later images in each sequence during the process of searching for earlier images in their sequences, a form of “drive by” recognition. Variance in finding and selecting images increased significantly as screen density increased, reflecting the increased effort needed to search among more images.

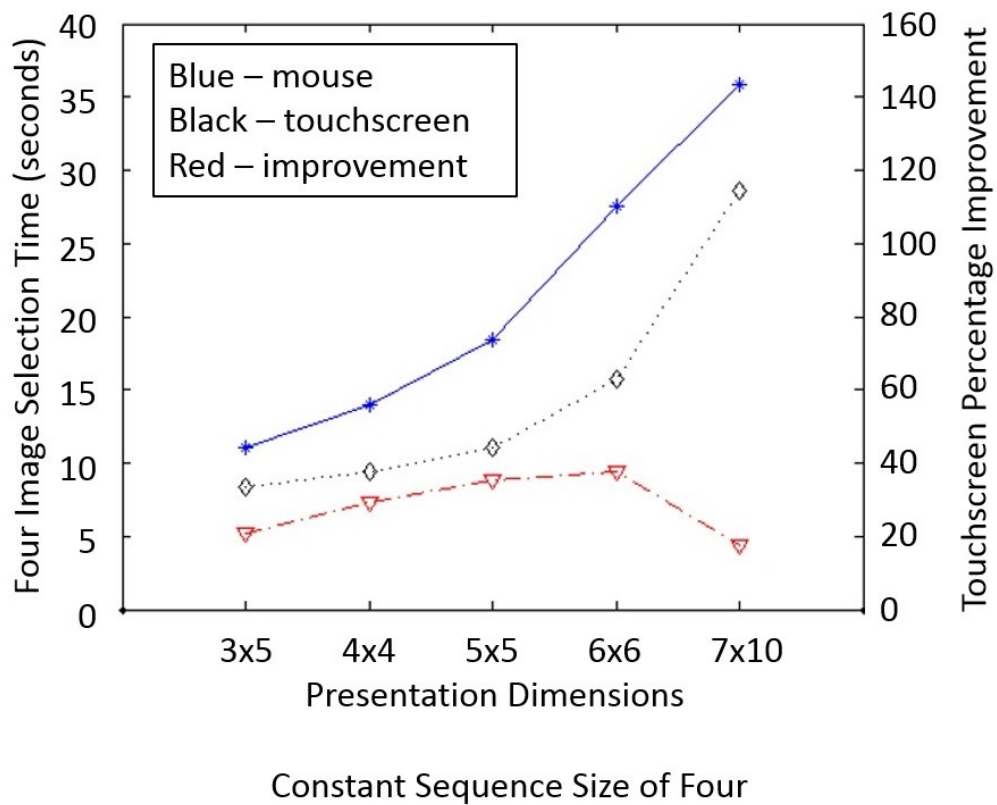


Figure 3.7: Median authentication timing with constant sequence size and varying input device modality.

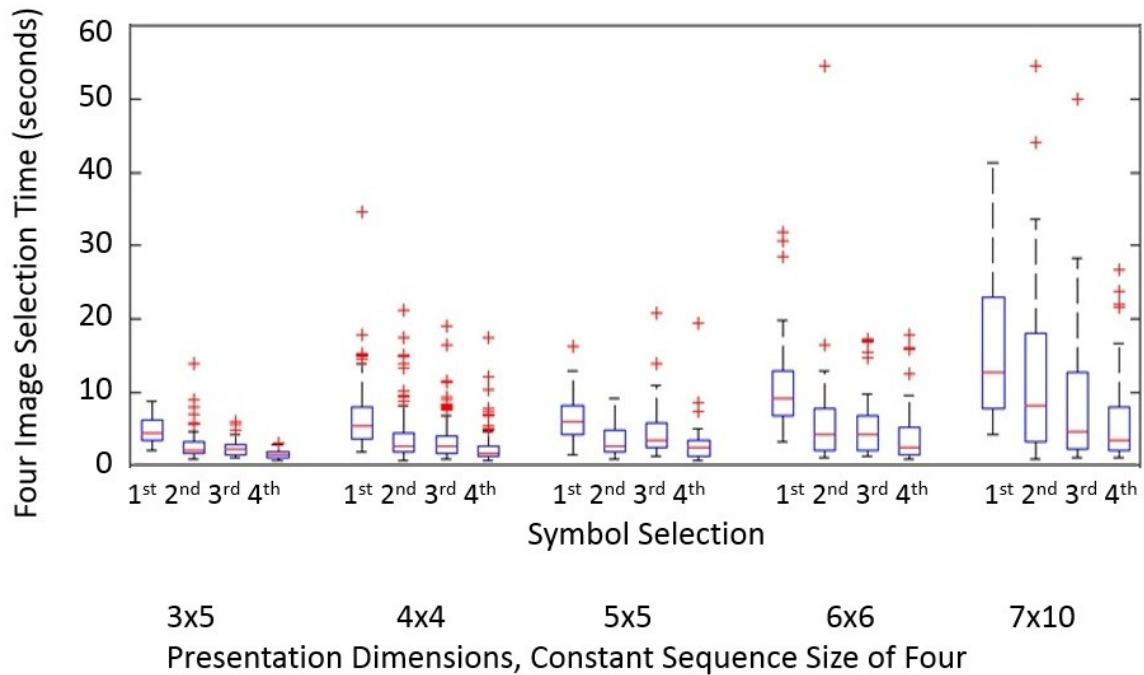


Figure 3.8: Individual image selection timing.

3.4.4 User Input Device Modality

Fig. 3.9 shows median authentication timing data for varying user input devices. Volunteers selected varying length personal image sequences from a constant image display density of seventy. Volunteers performed 82 mouse (blue bars) and 75 touchscreen exercises (red bars). For all three personal sequence lengths, touchscreen use improved sequence selection timing.

One interesting study goal was understanding the impact of using a touchscreen versus using a mouse. Many older persons have no touchscreen experience, or may have disabilities that limit arm and finger movements needed to reach out and accurately select images. Fig. 3.7 and Fig. 3.9 show that these concerns were

unfounded as use of the touchscreen significantly improved median timing by 32%. As shown by the bottom curve in Fig. 3.7, use of the touchscreen increasingly improved performance times as screen image density increased until reaching the densest display, 7x10. This suggests that some other factor overcame the advantage provided by the touchscreen. The usability study volunteers repeatedly commented that the 7x10 screen had too many images which took too long to search.

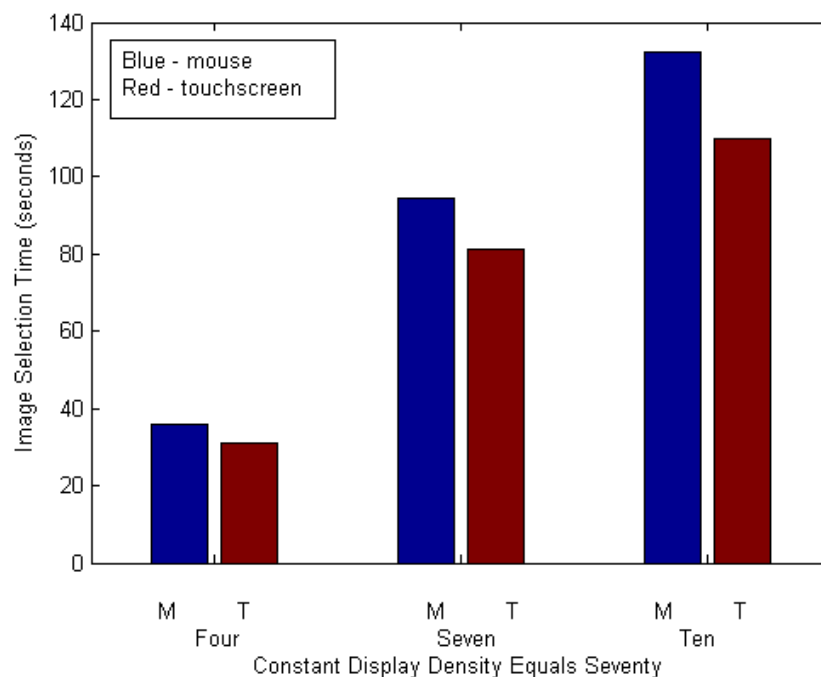


Figure 3.9: Median authentication timing with varying sequence sizes and varying input device modality.

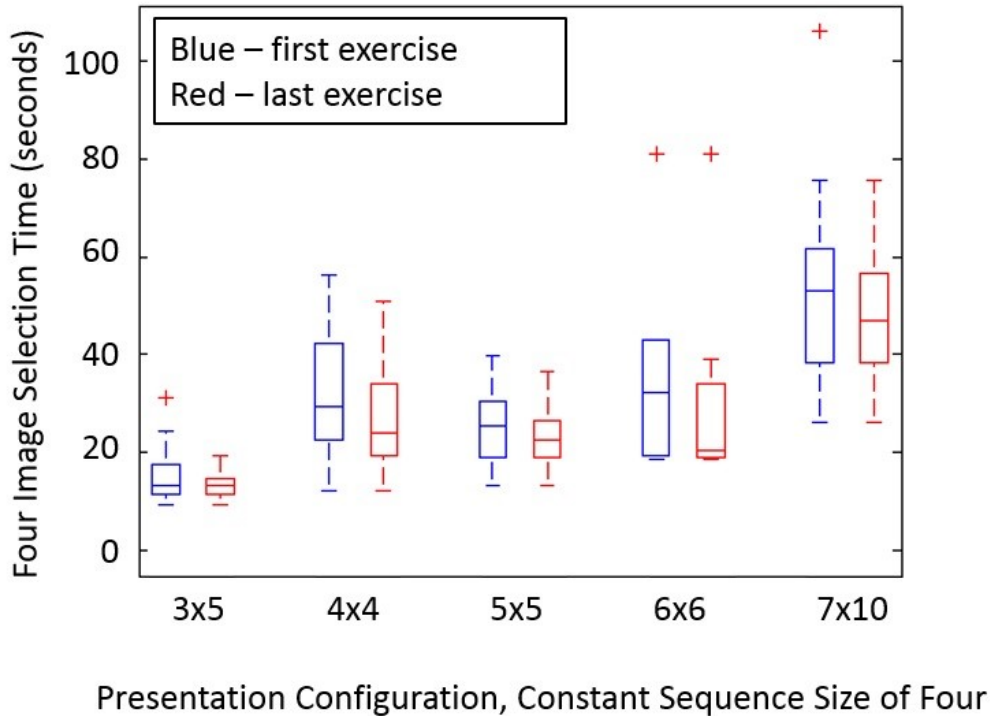


Figure 3.10: Authentication training effects

3.4.5 Training Benefits

A goal was to understand any training benefits resulting from repeating exercises at similar sequence lengths and display image densities. Previous work noted the challenge of getting volunteers to return for subsequent exercise sessions in the lab environment [7]. The increased effort made by going to each volunteer made it possible to observe and measure repeated exercise sessions. Through observation it was noted that initial exercises were often encumbered by volunteer unfamiliarity with handling the equipment and operating the software. Fig. 3.10 provides a comparison of the median timing differences of first attempts versus last attempts at repeated identical exercises using the mouse. Blue data identifies

the first exercise. Red data identifies the last exercise. Results show that the median performance improved, and variance decreased, reflecting user improvement with practice.

3.4.6 Personal Image Sequence Selection Timing

At the start of the study, each volunteer was asked to carefully select personal images important to them. Appropriate selection was key to a successful and efficient password image sequence. Volunteers were instructed to take their time and find meaningful password images. Table 3.6 provides a comparison of the time taken to decide upon and select each user's personal four image password sequence from the database of 550 images. Many volunteers found the image selection experience enjoyable, relating stories about their personal associations with the subjects in the images. Those users enjoying the selection process took markedly longer to complete their image sequence selection than other users. The faster users selected their image sequences in a comparable timeframe to the Passhint system. Through observation it was noted that volunteers often consciously decided on a strategy of selecting images based on occupational category, or era of professional fame, before beginning their image selections. The minimum time for a volunteer to select four images was 52.2 seconds, less than the 55 second mean of the Passhint system, showing that the Graphical Password system can be a practical alternative to Passhint for password creation.

3.4.7 Guessing Study

A guessability study was conducted with a subset of the usability study participants. The intuition was that attackers of comparable age to the volunteers would have a greater chance of recognizing the display images and discerning any themes that might provide hints to actual password images. Five participants were asked to view the 6x6 display screens of five other participants and then guess which four images formed the “victim’s” personal password image sequence. Guessers were told only the sex of the password owner and reminded that the password owner was over sixty years old. None of the guessers were successful at guessing a correct sequence. Guessers did choose at least one of the four images making up each sequence, ineffective for a successful attack. The best guesser chose three of the four correct images, in incorrect order, by performing a thematic analysis on the displayed images. A security policy requiring user selection of target images from multiple categories would thwart this type of adversary analysis.

Table 3.6: Password selection timing comparison.

Password System	Selection Time Range
Passhint [20]	55 to 58 seconds
Graphical Password System – four images	52.2 to 401 seconds

3.4.8 Image Pattern Effects

A goal was to learn if peripheral vision could play a role in target image recognition. Some exercises placed target images in deliberate patterns. As shown in Fig. 3.11, a random arrangement could result in the placement of images anywhere, whereas a block pattern puts the four target images immediately adjacent to each other. A linear pattern places the four images in a line on the display. The results for nineteen volunteers selecting four images from a display of twenty-five images with the mouse and the touchscreen are shown in Fig. 3.12. With both mouse and touchscreen, the block pattern resulted in improved median timing performance. The linear arrangement achieved comparable median timing performance to the random pattern with the touchscreen and improved median performance with the mouse. This provides evidence that users recognize nearby target images more quickly.

It was a goal to learn how the volunteers approached performing the exercises given that this was a completely new technique. After each exercise session, volunteers were asked about any consciously adopted image search strategies.

Some volunteers stated they just allowed their eye to generally roam about the screen display with no conscious direction. Other volunteers adopted “search left to right by row” or “search up and down by column” strategies.

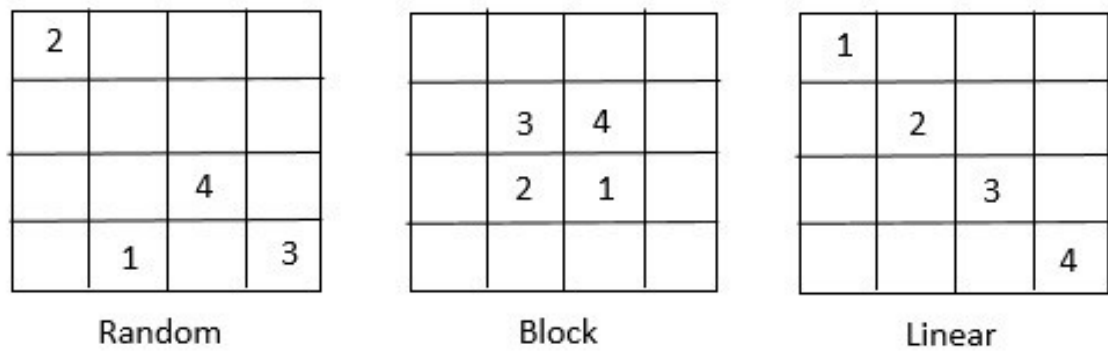


Figure 3.11: Image arrangement examples.

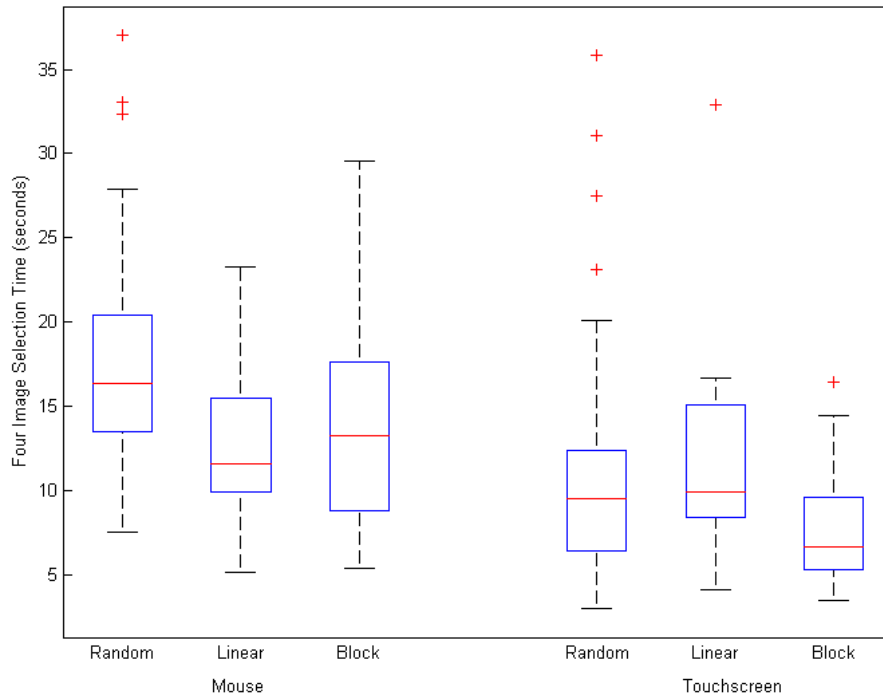


Figure 3.12: Timing effects of varying image arrangement patterns.

3.4.9 Text Password Comparison

A goal was to measure the elapsed time differences between entering a graphical password sequence and typing a text password. Fig. 3.13, from left to right, illustrates the median timing to enter a four-image password sequence with the mouse, then the touchscreen, typing a four-character strong text password, then a seven-character strong text password and finally a ten-character strong text password. Volunteers were asked to mentally create each strong text password for themselves. They were timed solely on typing of the text. The volunteers were observed putting significant effort into typing even the short four-character text password. Often, they were challenged by finding unfamiliar keyboard symbols or they were very slow typists. The median time to enter a four-image sequence with

the mouse was 14.2 seconds, less than the 15.7 second median time needed to type a four-character strong text password. Entering the four-image sequence with the touchscreen was faster yet with a median time of 9.9 seconds, a 37% improvement over text entry. The wider variance shown with the text entry may be attributable to the wide range of typing skills demonstrated by the volunteers. Further observations showed that the over-60 volunteers enjoyed selecting the image sequences and felt that typing a strong text password was not enjoyable because of the effort needed to find correct keys and unusual symbol characters.

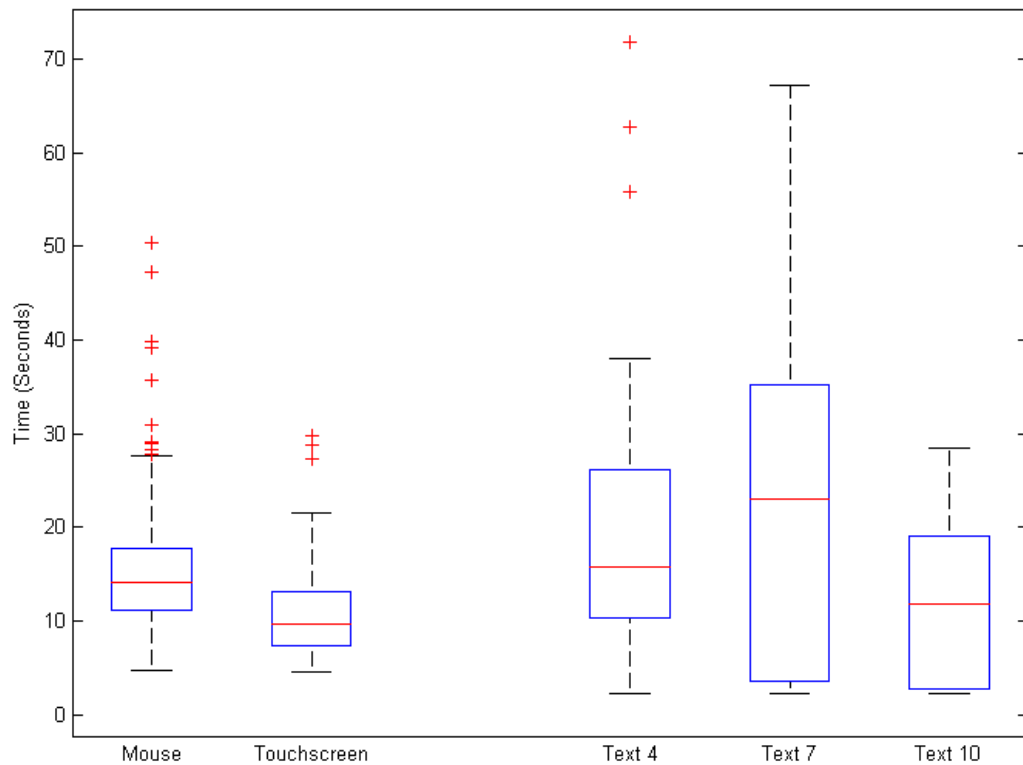


Figure 3.13: Timing comparison between image and text-based password sequences.

3.5 Graphical Password Extension to Smartphones

Older persons have significantly lagged younger generations in adopting modern technology [54] but are now quickly embracing smartphones. 64% of those 65 and older owned smartphones in 2015, reflecting an 8% increase in a single year [60]. Since smartphones are designed as inherently touch-based devices, and users spend up to 9% of their smartphone-engaged time unlocking their devices [61], the Graphical Password technique would seem appropriate for the smartphone platform. As a group, older persons have visual, mobility, and orthopedic disabilities which limit hand or finger use, lengthen visual search processes, adversely affect the ability to perceive small icons, and compromise their ability to move arms, hands and fingers smoothly and continuously” [62]. These physical characteristics can render some current phone unlock mechanisms difficult and frustrating to use. The Graphical Password technique can turn unlocking into an engaging and fun experience, key to maintaining a positive user experience [51] that discourages users from disabling security unlock mechanisms.

With a view toward widespread smartphone adoption by older persons the graphical password technique was compared with many common “phone lock” mechanisms in use today. Our survey methodology was to examine the online descriptions of the first twenty-five “phone lock” apps found in the Amazon Android [63], Apple iPhone [64], and Google Play Android [65] app stores. The most common “phone lock” apps included:

- Slider – slide finger along indicated path to unlock smartphone
- Zipper – slide finger along image of a zipper to unlock smartphone

- Numeric PIN – select four-digit (or higher) PIN from numeric keyboard display
- Alphanumeric Password – select text password from ten-digit keyboard display
- Pattern Swipe – swipe finger across display pattern connecting pre-entered symbols
- Voice Phrase Match – utter a passphrase into the smartphone microphone
- Drawing Match – swipe finger across display creating a drawing that must match pre-entered drawing
- Smartphone Shaking – hold an unlocked phone against a locked phone and shake them together to pass the unlocked state [66]
- Fingerprint Scanner (fake) – hold finger to target to unlock phone
- Fingerprint Scanner (real) – hold finger to target for scanning and match to pre-entered fingerprint scan

The survey analysis considered smartphone physical icon size, unlock technique entropy, ability to replace compromised unlock code, accessibility, touchscreen smudge-resistance, and capacity for personalization. The results are shown in Table 3.7. Each technique was rated using a scale from None (N), Low (L), Medium (M) to High (H) in terms of suitability of each attribute.

Physical size of finger target icons displayed on the smartphone touchscreen is very important. As described by Fitt's Law, the time taken to touch a target is a function of icon size and distance [67][52]. Larger finger targets are easier to see and touch. The complexity of each technique was reviewed in order to gauge resistance to brute force attacks. Many of the apps devolved to simple slider switches which anyone with physical access to the smartphone could unlock the device. More complex techniques such as PIN, pattern and password entry required users to locate and touch very small target characters or icons. Users with vision impairments would benefit from enlarging portions of the screen to make

viewing and touching easier. Attempts to enlarge the on-screen keyboard displays were unsuccessful. Any unlock apps providing screen enlargement capability also adds significant task functional complexity measurable through Goals, Operators, Methods, and Selection (GOMS) analysis of enlargement and scroll motions necessary for successful unlocking [68]. As an example, a user able to directly view and select an icon would be able to successfully select the desired icon in one step. A user needing to enlarge a section of the screen would need to select the screen area to be enlarged, make a zoom gesture and then select the desired icon, a minimum of three steps.

Unlock codes may become compromised and require replacement. In such cases PINs, passwords, and the graphical password technique enable easy replacement of the unlock coding. Other techniques such as real fingerprint scans or facial photo matching are limited to the user's ten fingerprints or single facial image. Once available biometric data is exhausted the user must seek an alternative unlock technique. Fingerprints may become less effective as users age, due to thinning skin. Accessibility in design enables those with disabilities to successfully utilize the unlock technique. Unlocks requiring matching of line drawings are challenging for those with shaky hands drawing on the touchscreen. Both the hand holding the smartphone and the hand with the drawing finger add variation to the executed drawing. Smudge patterns are created on touchscreens executing repeated swipe patterns on static symbol grids. Lastly, unlock techniques providing some user personalization features assists with unlock pattern recall.

As shown in Table 3.7, the graphical password technique, in the 3x3 or 4x4 configuration, provides large target size, good complexity, smudge-resistance, and a high degree of personalization. A ten-digit keypad displayed on a Droid Maxx running Android 4.4.4 was measured. Each character measured 0.25 by 0.25 inches. The same screen with a 4x4 graphical password presentation provides 0.6 by 0.6 inches for each image, more than twice the target space of the ten-digit keypad. The large target size facilitates users with vision, finger and arm mobility impairments. As older users more widely adopt smartphones, the graphical password technique will continue to be beneficial.

In recent times, password managers have come into use as repositories of passwords for users. In a manner similar to text passwords, graphical passwords may be stored and retrieved from an appropriately modified password manager able to handle the list of image identifiers forming the password sequence.

Table 3.7: Smartphone “phone unlock” technique comparison.

Technique	S	C	DR	A	SR	P	Note
Graphical Password System	H	H	H	H	H	H	Assuming choose four images from sixteen images, randomized display.
Slider	H	N	N	H	N	N	Anyone with physical access may unlock the smartphone.
Zipper	H	N	N	H	N	N	Anyone with physical access may unlock the smartphone.
Numeric PIN	L	H	H	L	M	N	Assuming four (or greater) digit PIN.
Alphanumeric Password	L	H	H	L	M	M	Assuming four (or greater) alphanumeric character password.
Pattern Swipe	M	H	H	L	L	L	Assuming four (or greater) dot swipe pattern on a nine (or greater) dot grid.
Voice Phrase Match	L	H	H	M	H	H	Physical size is not relevant to the voice recording quality. Button touches needed.
Drawing Match	H	H	H	L	H	H	Challenging for shaky hands to recreate line drawings consistently.
Smartphone Shaking	L	H	N	L	H	N	Physical size is not relevant to the quality of the shake pattern reproduction. Button
Fingerprint Scanner – fake	H	N	N	H	N	N	Also known as “prank scanner.” Simple touch and hold of finger on large target
Fingerprint Scanner – real	L	H	L	H	H	H	Limited current availability for Samsung, Apple iTouch and Android 6+ smartphones.

H – High

M – Medium

L – Low

N - None

S – Physical Size.

C – Complexity.

DR – Data Replacement.

A - Accessibility

SR – Smudge Resistance

P – Personalization

3.6 Conclusion

Our work on this project has transformed a challenging authentication process for older users into an enjoyable technique that will facilitate continued engagement with technology by older users. Our interview-style study of older computer users revealed challenges with the creation, recall, and management of strong text passwords. Our investigation of the inherent facial recognition capabilities within each user enabled us to create a Graphical Password system based on the selection of familiar facial images from the past personal history of the individual older user. In effect, users were able to rely on memory secrets within themselves to build their personal password sequence. Our usability study with nineteen volunteers demonstrated a 97% recall success rate, faster password selection than many previous graphical password systems, and faster performance than traditional text password entry with a keyboard. Our technique is naturally usable, easy-to-recall, and easy to execute. By enabling use of mouse or touchscreen image selection, a faster password entry mechanism was created that facilitates the manually impaired user. We have shown that the entropy of the Graphical Password technique is comparable to four-character text passwords, and superior to four-digit PINs, a viable security alternative to commonly used authentication systems. Additionally, we are rewarded to know that our technique is enjoyable to use and provides a supportive and positive user experience.

Chapter 4

Personal Fitness Tracker Usage Analysis

Over twenty-five million U.S. adults have purchased personal fitness trackers (PFTs) to pursue their health and fitness goals [69][70][71] and made them a key part of their lifestyle [135]. It has been shown that seventy percent of U.S. adults track some aspect of their health, while seven percent use an app or mobile device as a part of their personal health data tracking program [72]. With so many users wearing PFTs every day, it is important to investigate user activity patterns as a basis of comparison with manufacturer provided information. Manufacturers have not tested their devices in the context of health appliances, nor have they released detailed scientific information about the health aspects of utilizing their devices. It is essential for the user to have this baseline information in order to have an efficient health and fitness improvement program. This project gathered extensive data from many sources to develop a quantified picture of user activity, behavior, and fitness social network patterns.

4.1 Background

PFTs are small devices, unobtrusively worn either on the wrist or clipped to the body with the primary fitness goal of counting user steps. Additional functions include counting stairs climbed, estimating calorie burn, measuring heart rate and recording sleep patterns. Avid PFT users have integrated these devices throughout their daily lives, increasing awareness of fitness activity levels, and receiving motivations to achieve their goals for healthy living [73]. Users may rely upon their PFTs to not only inform important decisions about lifestyle choices and

health behaviors, but also to connect to others in fitness-related social groups for mutual motivation, social benefit and goal reinforcement. This important surge in user self-measurement and analysis has been dubbed the Quantified-Self (QS) [74] movement.

Unfortunately, there is limited public information about current user practices available to inform the user of product efficacy. Manufacturers do not publish user activity statistics for public consumption. Manufacturers have declined to undergo the rigorous independent US FDA and HIPAA testing processes [75] that inform consumers of device effectiveness and durability. Consumer information consists of user reviews in popular journals and web forums, manufacturer technical information, and user-contributed postings to fitness related social media. It is important to understand PFT usage patterns because employers and insurance companies are moving to obtain user tracking data to identify and address individual insurance risks [130].

Previous studies on PFT user patterns enrolled small groups to characterize usage patterns without addressing gender or age differences. Other work was limited to college age participants [76][134][136] or medical patients [133]. There is an identified need to study more diverse PFT user groups [136]. Many studies were the results of interviews or video analysis. Our project captured real-world user data to quantitatively describe usage patterns among typical users.

Previous work based on interview-style user studies, user surveys, and analysis of user experience videos have developed themes important to understanding PFT usage but do not attempt to quantify user activity levels of the diverse PFT user

population. Some studies compensated participants with money, providing an external motivation to continue PFT use, or creating a feeling of obligation to perform well that may skew results [136]. Researcher coding of interviews, surveys and videos may introduce error through incomplete understanding of user intentions. Users may also introduce error in the form of inaccurate recall or a desire to give the researcher pleasing answers. This project's data is collected post-facto from publicly available, user-posted data. There was no opportunity to motivate user participation with a stipend or recognition prior to data collection.

The project goal was to develop a quantified portrait of “in the wild” PFT usage by mining publicly accessible user data postings to popular social media, reviews on websites, and activity data shared among consenting user fitness groups. The importance of user postings has grown as 79% of Americans engaged online in 2016 [128]. A recent fitness tracking study has noted that half of their participants also engaged on social networks [134]. It was possible to mine detailed information about daily activities from users who were open to engaging with other users. This accumulated data enabled measurement of significant gender and age differences in fitness social network group composition and user activity levels. It was possible to identify important fitness trends based on type of social media forum. It is believed this is the first project to use data from real-world PFT users, and the first to quantify the PFT user experience in fitness social forums.

While mining the dataset of user records, it was discerned that a device manufacturer's user URL coding mechanism was strongly correlated with user

ownership onset date. This knowledge enabled characterization of step activity levels as a function of device ownership duration.

Even as PFTs are enjoying wide adoption, and evolving in exciting ways, their functionality is being incorporated into smartwatches, providing users with access to phone functionality directly from the user's wrist [71][129]. PFT and mobile phone functions directly interact together to create a beneficial and personalized user experience.

4.1.1 User Activity and Behavior Model

A holistic model of user activity and behavior defined user activities in three stages is shown in Fig. 2.1. The Initiation phase encompasses the user steps taken to acquire and begin to utilize the PFT. The Utilization phase incorporates normal wear, activity, reliability and socialization activities as the user goes about their normal daily routine. The Abandonment phase addresses the user's decision to stop using the PFT. The project data collection and analysis effort focused on the Initiation and Utilization phases of user activities.

4.1.2 Personal Fitness Device Hardware, Software, and Social Forums

There is a broad array of PFT devices available in the marketplace. This work focuses on wrist-worn PFT products. Fig. 4.1 shows two popular and representative PFTs collocated on a user's left wrist. On the left is a Fitbit Charge alongside an Apple Watch. The user motivation results revealed in Table 4.1, that users are highly interested in product appearance, and wrist band comfort. As personal devices typically worn for much, if not all day, users desire an attractive

band and display. Both models normally have a darkened screen until awakened with a tap or swing of the wrist up to the face. The Fitbit Charge has a single LED screen display and one button to click through user information displays. The Apple Watch has a larger screen with many tap selectable activity displays. Like most models, these devices not only track user steps but also floors climbed on stairs, distance traveled, calories burned, heart rate, active minutes of exercise and more.

PFTs pair using Bluetooth to relay collected activity data via the user's mobile phone or personal computer dongle. That data is then viewable on PFT manufacturer websites, user apps and personal computers. Users frequently view PFT data and change PFT settings via their phone app. Fig. 4.2 shows a representative Fitbit Surge app display showing the PFT model name, number of steps taken that day, resting heart rate, calories burned, floors climbed and other useful information. Images of user app screens can be easily posted to social networking sites for sharing with friends.

Users have access to a wide array of manufacturer or independent apps to assist with data analysis, and foster participation in web-based social forums. As in traditional social networks, PFT users "friend" other PFT users and join groups with similar motivational goals. The forums provide users motivational feedback in the form of achievement "badges" at specified step activity levels and "friend" comments. Group members can "see" the activities of other group members if allowed by individual user account settings. The manufacturers also host

“challenges” whereby small groups of users can track their step activity for short periods of time such as a week or a weekend.

Several popular models of personal fitness trackers and smart watches were identified as desirable targets for gathering internet-posted data. The focus was placed on devices with major market share, specifically Jawbone UP, Garmin, Samsung, Fitbit Charge HR, Fitbit Surge and Apple Watch.



Figure 4.1: Fitbit Charge and Apple Watch



Figure 4.2: Fitbit Surge User Daily Activity Display on Mobile Phone

4.2 Motivation

Users typically wear their PFTs all day, and transmit their data off-device for subsequent storage and use within a wide array of personal fitness apps or device manufacturer websites. Users are relying upon their devices to not only inform important decisions about lifestyle choices and health behaviors but also to connect to others in fitness-related social groups for mutual motivation and goal reinforcement. This work brings together user-posted records from a wide array of sources to achieve a quantified understanding of current fitness activities and extent of fitness related social interactions.

4.3 Data Collection Methodology

English language user product reviews, performance data, social network data and demographic information were collected. Product reviews consist of user comments regarding motivation, PFT performance issues, and reliability. User performance data contained the numeric quantity of steps achieved on the day the user posted information onto a website. Only user-posted information was collected which clearly came from a single PFT user as judged from context, content and user self-identification. Data posted by commercial organizations, professional consumer electronics reviewers, professional journalists or online publications was excluded. Demographic data consisting of age and gender was collected from performance and social group postings as presented by each user fitness account. Performance and social group postings without viewable gender and age information were not included in this study. User social group data consisted of the size and composition of the user's fitness social group. Data was deliberately collected from a variety of online sources to minimize potential effects of site editorial bias, and to enable observation of varying user motivations by data source. Data was collected in the form of screen scrapes (html files), screen grabs (jpg), or manual transcription of displayed screen data. Individual users were tracked by the user-chosen nickname associated with each review or data posting.

This work brings together user-posted step activity records from a wide array of sources including social groups on PFT manufacturer social forums. User-posted fitness data screenshots placed on popular image-sharing venues such as Yahoo, Instagram, Tumblr and Flickr, display actual numbers for notable user step

achievements. Each record displayed specific activity levels from one or more users. Individual record sources may be biased due to editorial policies or user group mutual interests. The project gathered data from multiple sources to develop a more complete spectrum of user motivations and concerns. Social groups and other online forms of online communications have been studied for a long time [132]. Evidence suggests that users may feel most comfortable expressing themselves through internet postings [131]. This lends support to these sources as accurately reflecting PFT user activities and behaviors.

User accounts offer privacy controls regarding public visibility of user information. All website-posted information was explicitly open to public viewing as set by the data owner. No attempt was made to circumvent any security or privacy controls. User data was analyzed statistically with Matlab© software.

PFTs automatically upload user data to manufacturer websites when an authenticated and paired connection is established. This supports data reliability as users cannot directly modify their step activity data. Potential limitations of this work are that users may have mis-represented their gender or age on websites, users may have posted activity information that was actually performed by a different person. It is believed these limitations are minimized by the large set of data collected, and the randomness of the data sources selected. The result of this project is the first fine-grained insight into the real-world usage patterns of PFT technologies.

4.3.1 Product Reviews

Retailers, manufacturers and fitness bloggers provide forums for purchasers to post PFT product reviews and comments. User product reviews consist of the user's comments in text form describing personal experiences with the PFT. These comments include user primary motivations, and reliability issues encountered with the PFT. Retailer sources consulted were amazon.com, bestbuy.com, target.com, walmart.com, rei.com, bhphotovideo.com, verizon.com and att.com. Manufacturer sources consulted were Apple, Fitbit, Garmin, Jawbone and Samsung. Resellers such as eBay and Craigslist were intentionally omitted as their users have the explicit goal of completing a sale and may bias their writing with a positive slant. It must be noted that manufacturer and retailer forums may be curated, as PFT manufacturers have a vested interest in presenting a positive product image. The presence of negative reviews was noted on all websites. Collected reviews were analyzed thematically to discern user purchase motivations and reliability issues.

4.3.2 Blogging Websites

Thirty independent fitness-oriented blogs were identified which focused on the use and performance characteristics of PFT devices. Bloggers posted screenshots of their Fitbit and Garmin fitness activity to support their writing. Tumblr is a microblogging service supporting users posting about personal interests. Tumblr users typically posted an image followed by a short comment along with appended search tags. As an example, by searching on hashtags such as #jawboneup posted fitness data for ten Jawbone PFT users were obtained. Fig. 4.3 shows a

representative Tumblr posting containing a screenshot of a user app screen. The top portion of the screen indicates this user has moved 12,681 steps, burning 1,741 calories. The bottom of the screen shows the user-added text indicating their pride in achieving over 12,000 steps despite encountering bad weather. This user's text also provides evidence of their motivation to lose weight. The user text added to Tumblr postings provided interesting insights into user behavior patterns and motivations. One Jawbone user posted for ten days, recording an average cardio workout of 1 hour 24 minutes and an average walk of 31 minutes per day. Another poster provided information about device idle settings and personal motivation *"My up idle alert is set to 30mins so if I don't move for thirty minutes and get that buzz I've decided to get up and do 10 squats."*

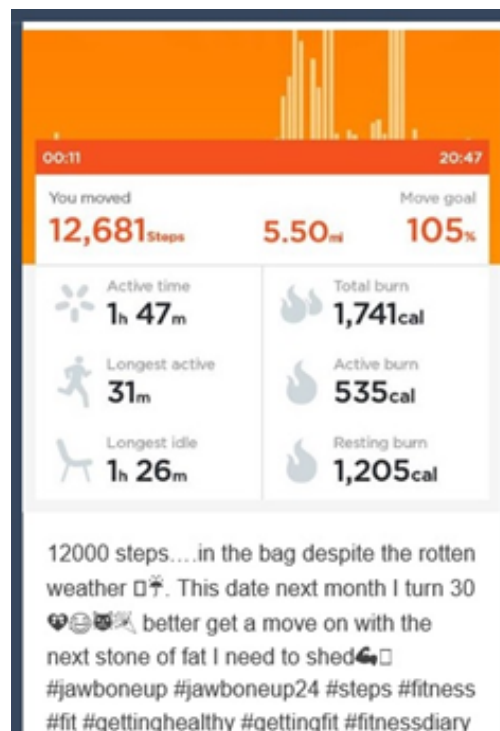


Figure 4.3: Tumblr posting from Jawbone UP user

4.3.3 Image Sharing Websites

Users enjoy sharing screenshot images of their fitness achievements with friends on the image sharing websites Flickr, Instagram and Yahoo. Searching with the terms “fitbit dashboard,” “fitbit activity,” “fitbit steps” or tag “#fitbit” resulted in a large number of resulting images. Users will post a screenshot of their mobile phone PFT app display to celebrate a notable step activity achievement. Often there is accompanying text reflecting pride in their achievement. It is hypothesized that the step activity numbers shown in these screenshot images are often “personal bests,” an upper fitness bound, and are posted to let friends know about user achievements.

4.3.4 Social Networks

Screenshots posted to Facebook were collected by searching with terms “fitbit dashboard,” “fitbit chargehr” and similar terms. It was possible to measure user engagement with online fitness networks by examining the Fitbit online community. Many major PFT device manufacturers maintain websites to support their respective user communities. Individual PFT users may view their personal fitness data and engage in social activities with other device users. Formal groups of Fitbit users within the Fitbit Community are organized into “Activity Groups.” Individual users who join a group are called “friends.” Individual user step activity records were collected from thousands of users on the Fitbit website. Users may establish and/or join activity groups matching their personal interests, fitness goals, occupation, age, geographic location and other focus areas. Data was collected from groups of younger (20s) and older (60s) users. Upon viewing the public profile

of each user, it was often possible to identify the user's gender based upon the provided image and name. When the presented user name or image was not clear as to gender then that user's data was excluded from the gender-based activity statistics in this study.

Just as social networks have become a significant part of society, PFT manufacturers have created fitness-focused social networks to foster social relationships between PFT users. These relationships are a source of motivation to improve fitness and a means of friendly competition with family, friends and others. Fig. 4.4 shows a representative mobile phone Fitbit app screen with the 7 Day Step Total for one user and five of her friends who are also using Fitbit PFTs to record step activities. The display is in a "leaderboard" style format, meaning the five friends with the highest current step totals will be shown on this display.

It is possible to view the personal data of the friends of each device user if the friends have their privacy settings set to permit public view. Users may have varying numbers of friends, up to eight of which are visible in the user data Friends screen on a personal computer. Only six friends are viewable on one Friends screen of a mobile phone. Through analysis of the publicly visible data, it is possible to characterize the quantities and gender of friends linked with each user. By capturing Friend data, a portrait can be developed of the degree of socialization within the group, and between genders.

The screenshot shows a mobile app interface titled "Friends" with a teal header. Below the header is a section labeled "7 Day Step Total". A list of six users is displayed, each with a rank number, a profile picture, a name, and a step count with a right-pointing arrow. The users are ranked from highest to lowest step count.

Rank	Profile Picture	Name	7 Day Step Total
1		You	100,970
2		Jim	75,048
3		Monica	71,669
4		Nat	61,295
5		michael	45,584
6		Patrick	44,504

Figure 4.4: Fitbit Friends Display

4.3.5 Fitness Infrastructure

During the course of collecting user data from the Fitbit community website, we discerned that a unique coding mechanism was assigned to each user account public Uniform Resource Locator (URL) by this manufacturer. Each URL contained an alphanumeric sequence unique to each user. It was also observed that many users had left their personal profile “Join Date” open to public viewing. Correlating the publicly viewable “Join Dates” with user alphanumeric codes confirmed that user codes were assigned in a strictly increasing pattern. Given an ample collection of unique join-date-code-sequence pairs, it was possible to construct a reference list of the range of assigned code sequences assigned for each month/year since the Fitbit was first introduced. Knowing the duration in months of PFT ownership for all users in the collected data enabled further analysis of popular device purchase timeframes, and persistence of PFT usage over time. The

data collection phase was completed in December 2015. It was possible to estimate the number of users joining the Fitbit community in each of the months preceding the data collection effort. As shown in the upper plot of Fig. 4.5, 20-year-old users exhibited large spikes in onset of PFT use at 12 and 24 months prior to December 2015. This implies that large quantities of younger users are beginning PFT use during the North American holiday season. As shown in the lower plot of Fig. 4.6, older users exhibited significant onset of PFT use during the same holiday seasons. Older users also exhibited a significant spike in user onset at the beginning of the immediately previous North American summer season in 2015. There was no corresponding summer onset bump for younger users.

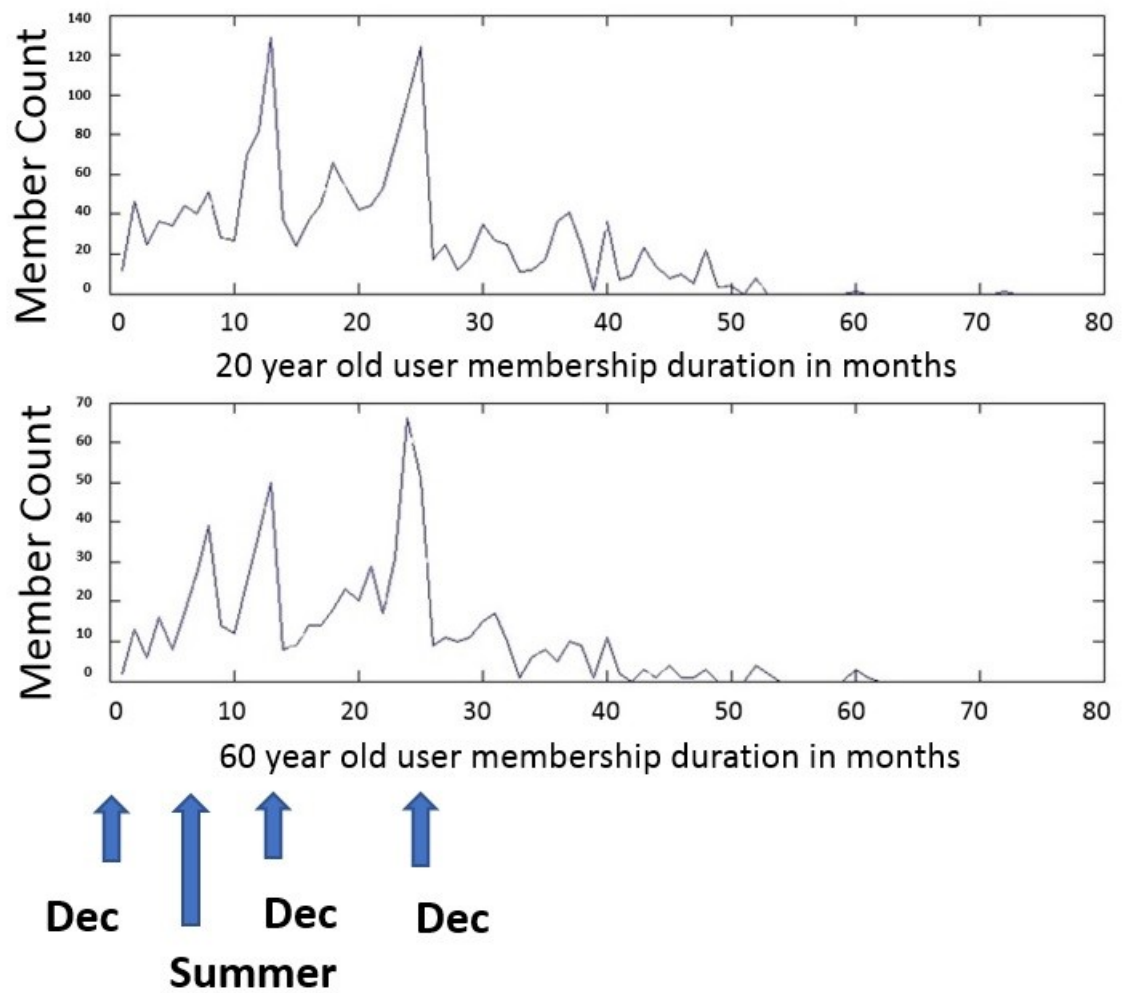


Figure 4.5: Device ownership onset. Upper plot reflects 20-year-old device owners. Lower plot reflects 60-year-old device owners. X-axis is number of months of ownership. Y-axis is number of devices initially activated during the month

4.4 User Data Analysis

4.4.1 Initiation Phase Analysis

PFTs are designed to track multiple aspects of user fitness activities. Users may choose to use one, several or all the available modalities of their device depending upon their personal goals and interests. To understand actual user motivations for acquiring and utilizing PFTs, user comments were gathered and thematically analyzed the text of user-posted product reviews on manufacturer and retailer websites. User PFT reliability concerns were also captured through the same means. A total of 2,461 user-posted product reviews were collected. Each review was evaluated to determine if motivational or product reliability content was present. Examples of motivational statements were “step activity tracking”, “sleep tracking” or “heart rate tracking.” Examples of reliability statements were “synching was easy,” “step tracking was inaccurate,” or “battery charging was a concern.” A review such as “It’s only been a couple of weeks, but so far I really like the Fitbit Charge HR. It keeps really great track of my steps, monitors my heart rate well, and I like the added feature of having a watch on, which I haven’t worn one for years. I haven’t quite learned how to understand the sleep data, but it is definitely monitoring that too. I’m still learning, but so far really like it” provides relevant insight into this user’s interest in multiple current modes of self-tracking, step activity and heart rate. Other reviews such as “I love this item. It’s fantastic” or “It worked as advertised” provide no specific motivational or reliability insight and were not considered further. Reviews commenting solely on PFT pricing, availability and shipping were also not considered further. From the original set of reviews, 1,613 (66%) contained relevant statements meeting the study goals.

Often, user product reviews contained more than one relevant statement. The collection of user product reviews with relevant content contained 3,114 individual statements, an average of 2 relevant comments contained within each qualifying relevant user product review. An example of a user review with multiple relevant statements is “I love my Fitbit Charge HR! It is very accurate, easy to use and a lot of fun. I love that it syncs automatically to my phone. The heart rate feature is great. The band is comfortable to wear and not too big. The clasp is very secure. The battery will last about 4 days and it charges quickly. I am glad I waited for this product!!” Reviews with compound statements were parsed into multiple individual statements. The previous example counted towards the topics of device syncing, heart rate tracking, wrist band comfort and battery capacity.

Table 4.1 lists the ten most significant motivational themes identified in this study. While step tracking is the dominant use, the next most prominent theme stressed the physical appearance of the PFT, more so than the heart rate tracking and sleep tracking user applications. It was theorized that since dedicated PFT users often wear their devices all day, they wish the PFT to be visually attractive, and compatible with their attire.

Table 4.1: PFT User Motivation Themes. Each row indicates the raw count, and proportion of user reviews.

Statement Count	Motivation Theme
409 (27%)	Step activity tracking
305 (20%)	Product looks good or is stylish
283 (19%)	Heart rate tracking
212 (14%)	Sleep tracking
121 (8%)	Motivates to exercise more
70 (5%)	Calorie tracking
59 (4%)	Ability to customize appearance
26 (2%)	Stair tracking
24 (2%)	Received as a gift
21 (1%)	Enjoy social features, friends and challenges

During this study, it became evident that the currently emerging class of wearable devices called “smart watches” is making a big impact with fitness tracking users. The extensive and enthusiastic user comments on smart watches motivated the expansion of the study to take a first look at this next generation of fitness trackers. Smart watches build on the functionality of PFTs by adding functions traditionally associated with mobile phones. Table 4.2 lists the four user motivation themes associated solely with smart watches. Smart watch themes reveal that the convenience of pairing a wrist worn PFT with a mobile phone is a highly valued technical capability. Smart watch advertising, and user product reviews comment that these devices eliminate the need for a user to locate and extract their mobile phone from a pocket or purse to review texts, caller ids, or even initiate phone

calls. It is suggested that as smart watches gain in user functionality they will become a dominant part of the wearable consumer market.

Table 4.2: Smartwatch User Motivations.

Statement Count	Smartwatch Motivational Themes
294 (49%)	Text, caller id, and email notifications displayed on PFT
194 (32%)	PFT acts as an extension of user mobile phone
84 (14%)	Phone calls are made from PFT on the wrist
28 (5%)	PFT voice command recognition was good

4.4.2 Exercise Phase Analysis

4.4.2.1 Reliability Analysis

Table 4.3 lists the seventeen reliability themes represented by more than 1% of the user review statements. Themes reflect the user's assessment regarding the capability of their PFT, and related app software. Themes were categorized as positive or negative from the user's perspective. Positive themes convey that the user is pleased with the performance described in their review. An example of a positive theme is "Wristband is comfortable." Negative themes reflect user dissatisfaction with an aspect of PFT or app performance. An example of a negative theme is "Synching PFT was not easy" reflecting users challenged by unsuccessful attempts to synch their PFT with their mobile phone or computer. It is noteworthy that ten of the seventeen themes were actually positive *and* negative user perception pairs regarding only five reliability themes: app experience, battery life and charging, synching, wristband comfort, and setup and learning. For all five

of these themes, the amount of positive user reviews exceeded the number of negative user reviews.

4.4.2.2 Step Activity Analysis

Step activity tracking was shown earlier in Table 4.1 as the principal user motivation. Yet there remains no consensus on the actual amount of step activity occurring among active users. An obstacle to understanding step activity in the general population is the absence of a centralized, and publicly accessible point for capturing the degree and extent of PFT use by the general PFT user population. In order to gauge the level of step activity, user-reported step activity levels were gathered from a variety of data sources. Step activity data was extracted from a large number of user-posted fitness app screen shot images. It was also possible to capture a large number of user step data records that were automatically uploaded into the Fitbit community website. Through analysis of these step activity numbers we gained a quantified understanding of average user daily step activity levels among currently active users of PFTs.

Numeric data records of step activity levels posted by individual users from seven data sources were gathered. Table 4.4 lists these data sources and corresponding mean user daily step levels. Four of the seven data sources revealed a close correlation in mean user daily step activities. Data from images posted to Flickr, Tumblr, Yahoo, independent bloggers, and Facebook all reported a mean daily step activity level in the narrow range between 11,690 and 12,750

steps per day. It is suggested that their collective daily median of 12,213 steps may be a reasonable reference number to assume for the general population of *motivated* PFT users who went to the extra effort of maintaining a blog, accumulating and keeping a group of followers, or placing their information into a public forum. The Instagram daily average of 15,138 steps is notably higher. This may be reflective of a younger, more active user demographic. Instagram has been shown to be attractive to young adults, 55% of 18 to 29-year olds use Instagram, more than any other social media website [19].

Table 4.3: PFT User Reliability Themes. Each row indicates the raw count and proportion of user reviews. The Bias column indicates the positive or negative nature of each theme.

Statement Count	Reliability Theme	Theme Bias
220 (14%)	App experience positive and met needs	Pos
151 (10%)	Battery life and charging a concern	Neg
101 (7%)	Hardware was broken	Neg
99 (6%)	Battery life and charging not a concern	Pos
93 (6%)	Synching PFT was easy	Pos
92 (6%)	Setup and learning were easy	Pos
88 (6%)	Inaccurate step counting	Neg
80 (5%)	Setup and learning were not easy	Neg
76 (5%)	Synching PFT was not easy	Neg
75 (5%)	Wristband was comfortable	Pos
66 (4%)	Clasp slips and opens	Neg
64 (4%)	Wristband was uncomfortable	Neg
63 (4%)	App experience was negative and did not meet needs	Neg
59 (4%)	Inaccurate heart rate tracking	Neg
51 (3%)	Required to have mobile phone nearby	Neg
32 (2%)	Inaccurate sleep tracking	Neg
24 (2%)	Screen display readable and clear	Pos

A large amount of step activity data from groups of users within the Fitbit social community were gathered. As shown in Table 4.5, step data was extracted from three groups of sixty-year olds, and three groups of twenty-year olds for a total of 2,483 data records. Their mean daily step level was 7,607 steps, the lowest of the data sources and substantially below the well-known 10,000 steps per day goal set by the American Health Association [73]. Examination of mean daily step

values from all the data sources revealed two trends. The first trend observed was that as the degree of data collection automation increased, average daily step value decreased. The second trend noted was potential social reach, and posting effort increasing as average daily step value increased. Fig. 4.6 illustrates these trends in a plot of the mean steps per day from the seven data sources.

The automated data upload mechanism created by Fitbit makes it very easy for active users to keep online data records updated. It also may reduce data entry errors by removing human transcription and personal editorial concerns from the process of recording daily step activity values. Fitbit user data records are updated in an automatic and unattended manner when a user's PFT is within range of a synch point such as a mobile phone or computer dongle. Often, users may not even notice when a data synch is occurring.

Table 4.4: Comparison of mean daily step values. Numbers in parentheses indicate collected number of data records.

Data Source	Mean user daily steps
Instagram Postings (100)	15,138
Flickr Images (100)	12,732
Tumblr Postings (100)	11,959
Yahoo Images (100)	11,875
Blogger Images (28)	11,799
Facebook Postings (150)	11,694
Fitbit Community (2,483)	7,607

Table 4.5: Data from Fitbit Activity Groups

Activity Group Name	Quantity Friends Records	Mean Daily Steps
Over 60 Group One	107	7,431
Over 60 Group Two	34	10,260
Over 60 Group Three	586	7,873
20s Group One	99	7,214
20s Group Two	240	6,682
20s Group Three	1,417	6,182
Total Records	2,483	7,607

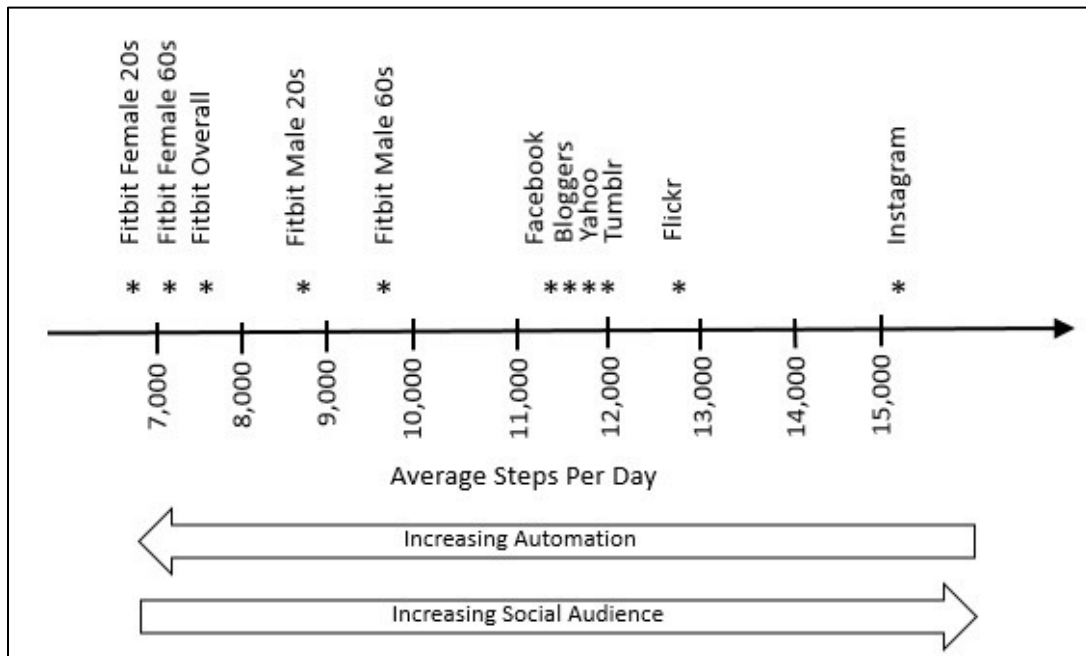


Figure 4.6: Step activity trends from varied data sources as a function of automation and social audience

Websites with a large social audience may enable *already-motivated* users to publicize their step activity achievements. Instagram users can potentially reach millions of viewers. Independent bloggers are known to reach many thousands of readers. The observations of Facebook and Fitbit are that their friend populations are much smaller. In the case of sites such as Instagram and Flickr, the effort required to create a user posting is more significant than the automated Fitbit data upload. Instagram and Flickr users must take explicit action to post step activity screen shot images, select associated tags, and supply accompanying narratives to continue a communication stream with their readers. Their higher degree of motivation to set up and maintain a blog may reflect a higher commitment to increased fitness through increased step activity.

The large group of data records collected from the Fitbit activity groups enabled further analysis of step activity based on gender and age. As shown in Tables 4.6 and 4.7, a large set of records was collected from users self-identifying with ages in their twenties and sixties. The viewable user profile data was utilized to determine gender. In those cases where gender was unclear, the user data record was excluded from further gender analysis.

Table 4.6: Fitbit Activity Group Records by gender and age

Age	Male User Count	Group Percentage Male	Female User Count	Group Percentage Female
20s	292	17.2	1,406	82.8
60s	247	35.5	448	64.5

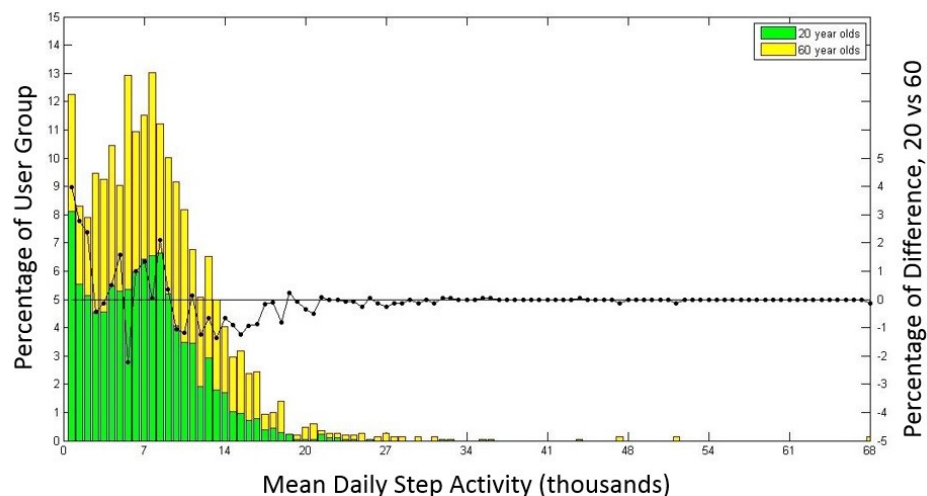
Table 4.7: Step activity by gender and age

Age	Male Mean Daily Steps	Female Mean Daily Steps	Gender Step Delta
20s	8,626	6,913	1,713
60s	9,582	7,238	2,344

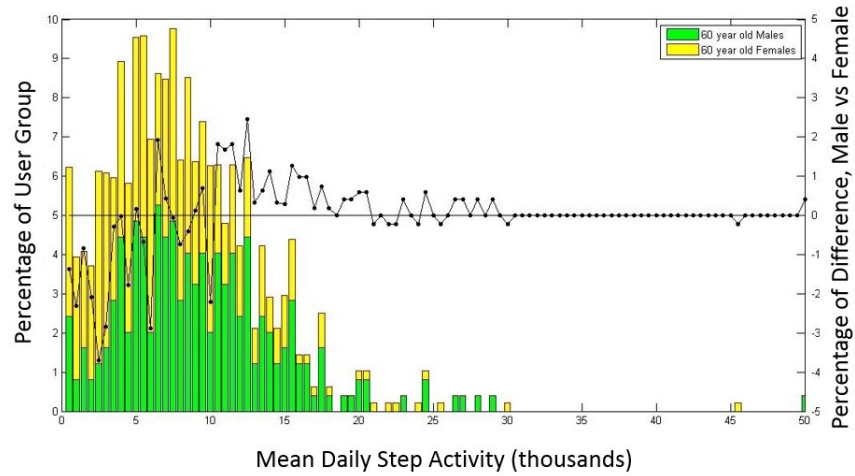
The user membership described in Table 4.6 was largely female, particularly in the younger age group, the 20s. As shown in Table 4.7, the male PFT users recorded significantly higher daily step counts than the female members in both age groups. The male users exceeded Meyer's counts of 7,500-8,500 steps, female users recorded lower activity levels [133]. All four gender-sex user categories recorded daily step averages below the 10,000 steps per day goal.

The five plots in Fig. 4.7 compare normalized mean daily step counts by gender and age groups as recorded over one full month, averaged to a daily step quantity. Fig. 4.7 (a) shows that both age groups display a skewed right normal distribution of step activity with the exception of 20-year olds at the lowest step activity levels.

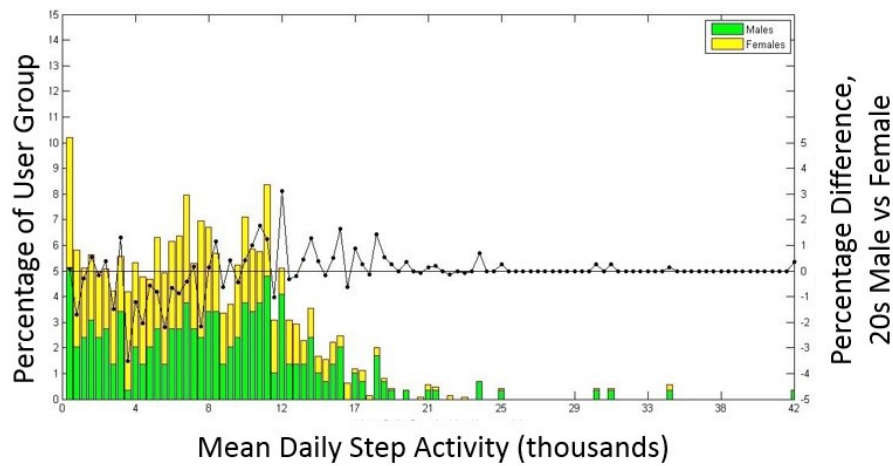
Fig. 4.7 (b) reveals a normal step activity distribution pattern for the older user group except for increased quantities of females at the very lowest activity levels. Fig. 4.7 (c) compares 20-year-old users of both sexes. The overall distribution appears skewed right normal. Displaying male data in green and overlaying female data in yellow, the results are bimodally distributed, reflecting lower step activity levels by female PFT users. Figs. 4.7 (d) and 4.7 (e) compare normalized step averages of same-gender users to illustrate age differences in performance. Fig, 4.7 (d) shows young male users dominant at the lowest activity levels, older male users dominant in the mid-range, and no clear dominance at higher step levels. Fig. 4.7 (e) compares female user step activity for both age groups. The results appear closer to skewed normal distribution pattern though again, younger females dominate the lowest activity levels to a lesser degree than the younger males in Fig. 4.7 (d). From this information, it was observed that relatively significant populations of younger users are exercising very little.



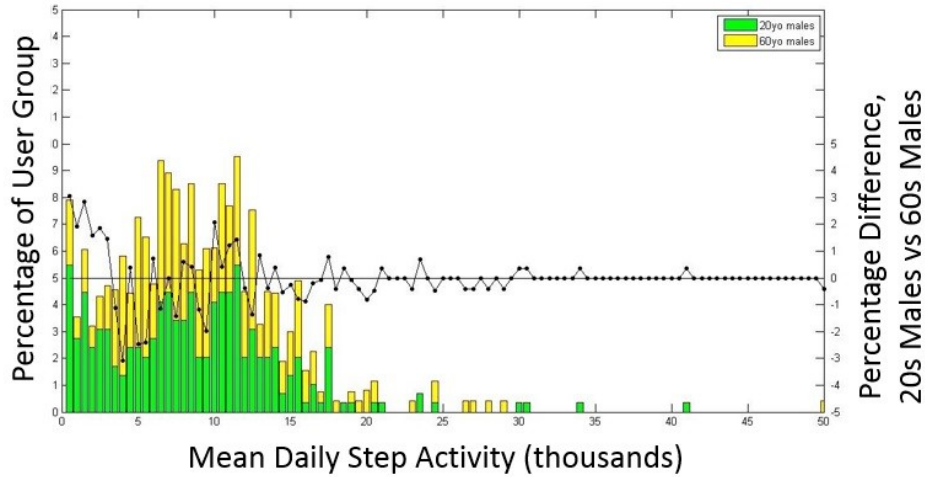
(a) All gender, 20-year olds (green) and 60-year olds (yellow). Delta values of 60-year olds over 20-year olds is plotted in black



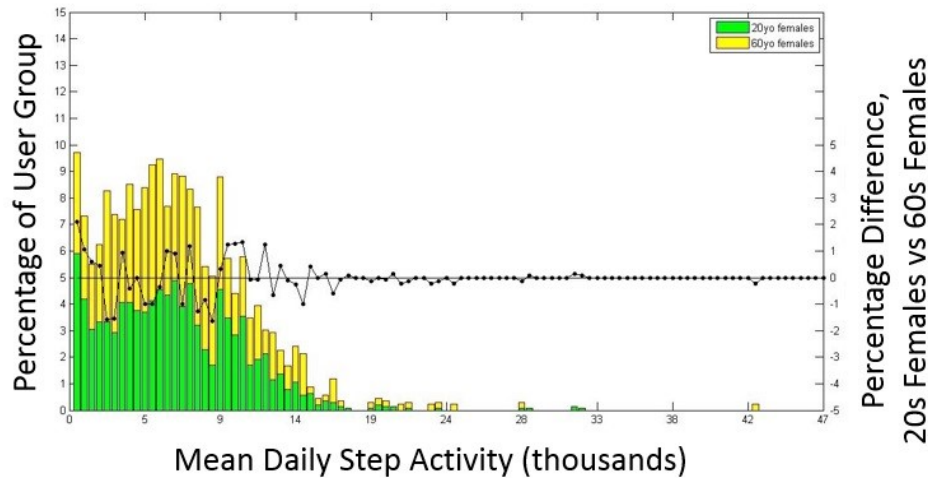
(b) 60-year-old users, both genders. Males (green) and females (yellow). Delta values of 60-year olds over 20-year olds is plotted in black



(c) 20-year-old males (green bars) and females (yellow bars). Delta values of 60-year olds over 20-year olds is plotted in black



(d) Male users, 20-year olds (green) and 60-year olds (yellow). Delta values of 60-year olds over 20-year olds is plotted in black



(e) Female user, 20-year olds (green) and 60-year olds (yellow). Delta values of 60-year olds over 20-year olds is plotted in black

Figure 4.7: Normalized step activity performance level comparisons between 20 and 60-year-old Fitbit users. X axis is increasing mean daily step count averaged over one month. Y axis in parts (a), (b) and (c) reflects percentage of the group population. Y axis in difference plots of parts (d) and (e) reflects magnitude of group difference with 60-year-old data negative and 20-year-old data positive.

4.4.2.3 Ownership Duration Activity Analysis

The average user daily activity level as a function of duration of device ownership was analyzed. Fig. 4.8 illustrates activity levels recorded in November 2015 for devices acquired in the past. Initial speculation was that the longer the user had the PFT, the higher the current activity level would become as user fitness improved. By fitting a line to each data set through application of the Least Squares technique [138], it is possible to confirm overall improving trend of user performance for a subset of users.

The equations used to fit the line were

$$m = \frac{\bar{x}\bar{y} - \overline{x_l y_l}}{(\bar{x})^2 - \overline{x^2}} \quad (1)$$

$$b = \bar{y} - m\bar{x} \quad (2)$$

Where

m = line slope,

b = line y-intercept,

\bar{x} = mean of set of ownership duration values,

\bar{y} = mean of set of average steps per day,

l = element identifier within duration data set.

The slope of the 20-year-old user line is 0.1263. The slope of the 60-year-old user line is 0.1772. This provides evidence that while both user populations achieve increasing step activity levels with increasing duration of ownership, the older user group is increasing their step activity levels more than the younger group. Some of the devices in longest use are observed recording the highest step

activity levels. This could be evidence of very committed users exercising at high levels. It could also be evidence that some users are in occupations with a lot of walking. It has been estimated that approximately 2,000 steps are taken during each mile of activity [139]. This number will vary depending upon the individual user's stride length. It is estimated that the users logging 40,000 steps of daily activity are running or walking in excess of 20 miles per day.

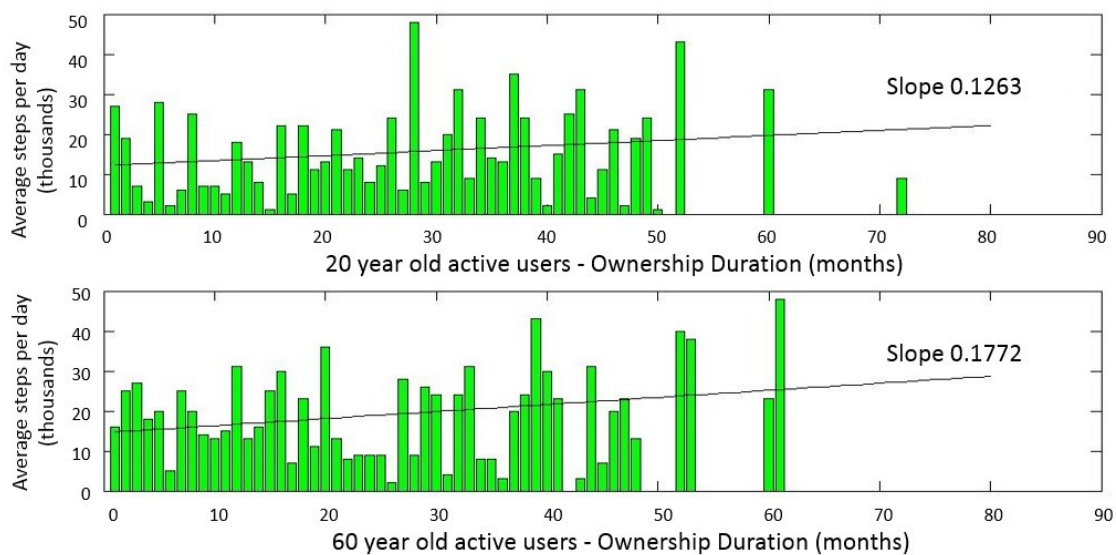


Figure 4.8: Average daily step activity level as a function of duration of device ownership. Upper plot reflects 20-year-old device owners. Lower plot reflects 60-year-old device owners.

4.4.2.4 Social Engagement Analysis

Table 4.8 shows that the mean number of friends for the three activity groups of 60-year olds is less than the mean number of friends for the three activity groups of 20-year olds. From this, it can be inferred that the older group is less interested in socializing with other PFT users.

Table 4.8: Friends per viewable user record.

Activity Group Name	Quantity Viewable Friend Records	Mean Quantity Friends Per User
Over 60 Group One	60	3.95
Over 60 Group Two	20	5.0
Over 60 Group Three	391	3.58
20s Group One	83	5.05
20s Group Two	203	5.29
20s Group Three	1051	5.43

The collected data provided further insights into the distribution of friends per PFT user participating in the fitness-related social network. The quantity of friends serves as a metric for degree of user socialization in fitness social networks. Table 4.9 presents the percentage of users versus quantity of friends. Friend quantities are classified into three categories. “Very Few Friends” was defined as two or less friends. “Few Friends” was defined as four or less friends. “Many Friends” was defined as those with six or more friends. As reflected in Table 4.8, younger users had a significantly higher proportion of members with “Many Friends” than the older group. Younger users had a significantly lower proportion of users with “Very Few Friends” than the 60-year olds. Older males appear to be the group with the smallest social networks. Younger users all showed strong interest in social activities with younger females only slightly edging out younger males.

Table 4.10 provides more detailed results describing the quantity of PFT users with social networks of increasing size, from 0 to 8+ Friends. As an example, there are twelve male 20-year-old PFT users who have zero friends. It must be noted that the fitness device app is set up to show no more than eight friends for each user. There is a strong trend within both age groups to have exactly six friends. This may be a result of the screen size limitations of the mobile phone. It is notable that among females in their 20s, 134 (12.2%) have formed friend groups of at least eight or larger. From this it can be inferred that the younger females are more interested in socialization than males or older females. A group of 42 male device users in their 60s have no friends at all. This is 23.7% or nearly one quarter of that group. Quantitatively the older males socialize the least in this social forum sample.

Table 4.9: Quantities of friends

	Very Few Friends (<3)	Few Friends (3 or 4)	Many Friends (>4)
20s males	10%	27%	70%
20s females	8%	21%	74%
60s males	36%	53%	40%
60s females	32%	48%	46%

Table 4.10: Size of friend group versus age of user

Number of Friends	0	1	2	3	4	5	6	7	8+
Male 20s	12	13	11	15	14	8	132	7	31
Female 20s	32	54	49	38	54	58	632	43	134
Male 60s	42	21	11	8	11	14	67	0	3
Female 60s	52	25	22	24	17	18	126	4	6

The collected data enabled analysis of the gender ratios of friends within the social-fitness network. Each of the friend records was examined for gender identity but not age. As shown in Tables 4.11 and 4.12, PFT users in both age groups were more likely to have friend relationships with females than with males. The friends of the users shown in Tables 4.11 and 4.12 were not further categorized as to age. As shown in Table 4.11, among younger users, females were the most likely to

have female friends and the least likely to have male friends. As shown in Table 4.12, among older users, older males were most likely to have female friends, and least likely to have male friends. Table 4.13 shows the gender ratios of male to female friends for each gender-age category of users. If users had equal amounts of friends from each gender, then the friend gender ratio would be equal to one. As shown in Table 4.13, young males had the highest ratio of male to female friends. Older females had the lowest ratio of male to female friends. Tables 4.11, 4.12 and 4.13 quantify the PFT user propensity to make female friends to a greater degree than male friends. These results are consistent with the general public's participation on social media, specifically Facebook, younger users participate more than older users, females more than males [137].

Table 4.11: 20-year-old user friend-gender likelihood.

20-year-old PFT Users	Friends	Ratio (friend/users)
243 males	425 males	1.8
243 males	731 females	3.0
1,094 females	1,660 males	1.5
1,094 females	3,760 females	3.4

Table 4.12: 60-year-old user friend-gender likelihood.

60-year-old PFT Users	Friends	Ratio (friends/users)
294 males	241 males	0.8
294 males	861 females	2.9
177 females	182 males	1.0
177 females	412 females	2.3

Table 4.13: Gender ratio of friends to device users

PFT Users	Ratio Male/Female
20s males	0.58
20s females	0.44
60s males	0.44
60s females	0.28

4.5 Limitations

This project collected data from thousands of active PFT users in order to quantify user activity, behavior and fitness social network patterns. It must be recognized that this group may not be a large percentage of all active users and may therefore not be an accurate representation of the population of all users. Additionally, anecdotal evidence is that a large percentage of users give up using their PFT after six months. There is no feasible way to capture data from the inactive user group without access to historical activity records from the manufacturer's storage facility.

4.6 Conclusion

Our project gathered a large amount of data regarding PFTs in order to illustrate the nature of motivations and activity levels across the range of typical PFT users. We were able to describe user patterns based on age, gender, and duration of PFT ownership. We believe we are the first to describe user behavior patterns in fitness social forums. This baseline knowledge will inform users as to the realistic benefits to be expected from their PFT devices, along with describing typical and usual user behaviors. Understanding current PFT utilization should facilitate effective future device modification, and foster more effective fitness social forums.

Chapter 5

Phase-aware Dynamic Time Warping Analysis

5.1 Background

Human movements can be measured and analyzed with the goals of enabling automatic pattern recognition, improving movement efficiency and increasing speed. Dynamic time warping has been shown to be an ideal technique to quantify and compare temporal patterns of varying speed and length. A class of sinusoidal movement patterns was defined that captured complex human motions of sports participants and transport vehicles within constrained sinusoidal travel paths. The DTW technique was adapted to take advantage of those constraints by reducing ineffective computations in the DTW distance matrix based on activity phase agreement. Our Phase-aware algorithm provides a practical means of comparing longer human movement time series data sequences than was possible with conventional dynamic time warping comparison techniques. The performance example demonstrated an 80% improvement over traditional DTW technique.

Many aspects of human activity can be measured and recorded in the form of time series data sets. Comparing datasets is advantageous in that it allows assessment of a human action through comparison of a newly captured measurement dataset with a library of reference dataset templates. Matching the new dataset to an existing, known dataset identifies the new human activity. Short datasets record short discrete activities such as individual handwritten words or hand gestures. Longer datasets capture longer activities such as brief periods of walking or running which can be described in sinusoidal terms. Increasing the size

of the measurement sample dataset records longer activities but creates the need for more memory space and processing capacity. The Phase-aware comparison technique leverages some inherent constraints in sinusoidal human movement patterns to reduce complexity and space requirements for longer movement datasets. This project is the first to describe these constraints and apply them to reduce complexity of DTW analysis.

Equal length time series sequences can be compared with Euclidean distance evaluation between corresponding points in each sequence. Considering that human activities are rarely identical, or even equal in length, the Euclidean distance technique cannot provide an accurate measurement of the differences between two human activity sequences without adjustment of sampling rate and resultant loss of data fidelity to the original activity. Euclidean distance comparison has no temporal flexibility, similar events that are offset in time cannot be matched as identical events. Dynamic time warping (DTW) has been shown to accommodate temporal variability in patterns and can be used to compare datasets of varying length. Initial work with DTW was used to compare and identify individual speech sounds [1], handwritten words [17], and hand movement gestures [18][19]. Expanding the ability of DTW to compare longer sequences will enable sequence similarity comparison in new realms of human activities.

The Phase-aware technique is specifically tailored to enable assessment of human activities well-described and constrained by sinusoidal patterns. Non-sinusoidal patterns such as hand gestures or handwriting move unpredictably in 360 degree spherical or planar field around a locus of action such as the hand or

the pen. Constrained activities such as walking on a sidewalk limit the body movements to the rectangular envelope of the sidewalk dimensions. Sinusoidal human activities follow natural or human-defined constraints within the natural or geographic world. Examples are: bobsledders and skiers going down mountain tracks, planes traveling through navigational air lanes, ships cruising in shipping lanes, and vehicles traveling on interstate highways. In each case the body in motion cannot leave the defined activity envelope but can wander within the envelope boundaries. The freedom of motion within the activity envelope results in some bodies moving faster or more efficiently than others towards meeting their goals. Analyzing these patterns will identify the most efficient or fastest body to either improve energy utilization or identify the winner in sports competitions. The Phase-aware technique takes advantage of the natural sinusoidal constraints to reduce the complexity of the DTW algorithm with no loss of underlying data fidelity.

Capturing basic human movement patterns such as walking is achievable with sensor sample rates of 20Hz, faster sports activities require sensor sampling rates of 100Hz [10][150] to meet the Shannon-Nyquist criteria [155]. Faster sampling rates result in larger datasets requiring greater storage capacity and improved analysis techniques for efficient similarity comparison. Olympic athletes are very competitive, top finishers in the sledding and alpine skiing events are only separated by a second or less [20]. These athletes are very interested in any analysis that provides a performance advantage. Sampling skier velocity rate within each foot of a 3 mile downhill skiing event will result in a 16,000 sample dataset for skiers moving at typical speeds of 70 to 90 miles per hour. Longer

movement patterns result in larger datasets. As an example, ships traversing trans-oceanic routes must maneuver to avoid natural obstacles, bad weather, and other ships during journeys of thousands of miles. Sampling position, velocity or fuel utilization at high resolution will provide insights into efficient ship operation but will result in a very large dataset. Traditional DTW can compare large sequences but quadratic complexity challenges space and computation resources as data sequences grow larger.

5.2 Dynamic Time Warping Technique

DTW optimally aligns two time sequences finding the minimum cumulative distance between aligned sample pairs. Fig. 5.1 illustrates the DTW alignment between two time series sequences, A and B. Both sequences have similar features, yet these features are not strictly aligned in time. DTW computes the optimal alignment with the minimum inter-series distance. The resulting distance metric defines the two series comparison.

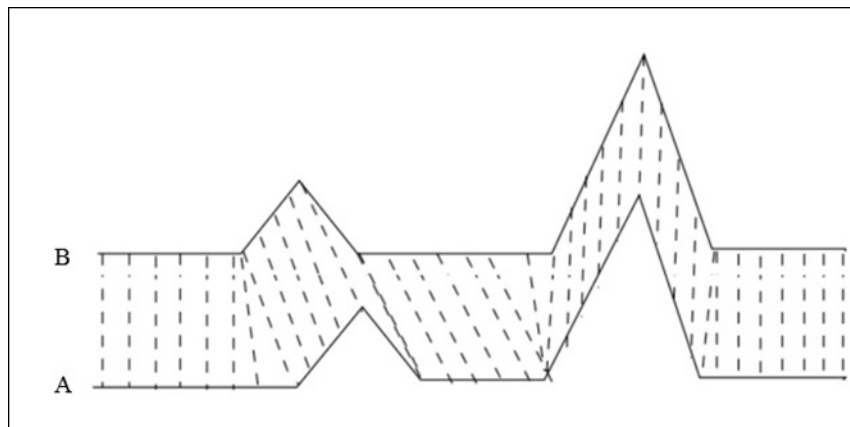


Figure 5.1: Dynamic time warping between two time series [15].

The DTW algorithm is comprised of two steps. The first step is creating the distance matrix listing all distance measurements between all possible sample pairs. A representative distance matrix is shown in Fig. 5.2. The second step is to dynamically compute the minimum cumulative distance warp path from the distance cell of the last data samples in both data sequences, and working back to the distance cell between the first data samples of both data sequences. The minimum warp path is shown in the green shaded cells in Fig. 5.2. The distance value for each cell in the distance matrix is defined as:

$$D(i, j) = |n(i) - m(j)|^2 \quad (1)$$

*for time series $n = n_1 \dots n_N$
and $m = m_1 \dots m_M$*

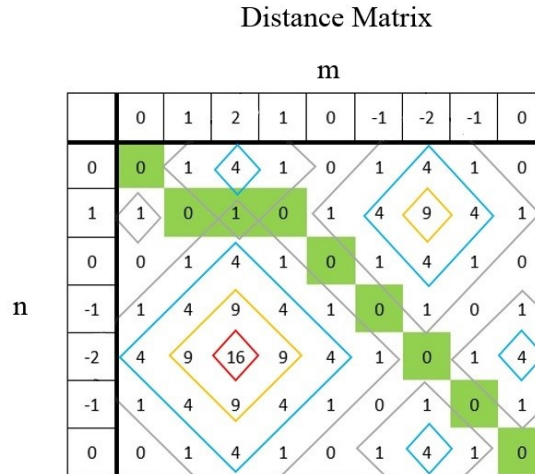


Figure 5.2: Distance matrix for data sequence $m=[0 \ 1 \ 2 \ 1 \ 0 \ -1 \ -2 \ -1 \ 0]$ and $n=[0 \ 1 \ 0 \ -1 \ -2 \ -1 \ 0]$. Minimum cumulative warp path is shown in green shaded cells. Cumulative warp distance for this example is 1.

Use of Squared Euclidean Distance (SED) enhances the differences between values in the data sequences under comparison. As can be seen in Fig. 5.2, the minimum distance warp path routes away from the highest distance values,

intuitively running through the valleys in the data avoiding the high points. The dynamic programming algorithm to calculate the minimum value warp path is:

$$D(i, j) = \min \left\{ \begin{array}{c} D(i, j - 1) \\ D(i - 1, j) \\ D(i - 1, j - 1) \end{array} \right\} + d(m_i, n_j) \quad (2)$$

Intuitively, the algorithm begins at the lower right distance cell of Figure 5.2, and compares blocks to the left, diagonally up, and directly up to find the neighbor cell with the minimum cumulative warp distance from the distance matrix origin. The reader is referred to [116] and [123] for implementation details. DTW complexity is $O(MN)$ due to the requirement to populate the distance matrix with values for all possible data sample pair combinations. Fig. 5.3 illustrate previous efforts to reduce DTW complexity by limiting the number of cells in the distance matrix that are populated and contribute to the warp path construction. Risk of inaccuracy occurs if the actual warp path deviates outside the green shaded areas of Fig. 5.3.

Restrictions on DTW are:

- each data sample from the first sequence must be matched with one or more samples from the second sequence and vice versa;
- the first data samples from both sequences must be matched together;
- the last data samples from both sequences must be matched together;
- the mapping must proceed in a monotonically increasing manner, in that the matching pattern cannot “double back” upon itself.

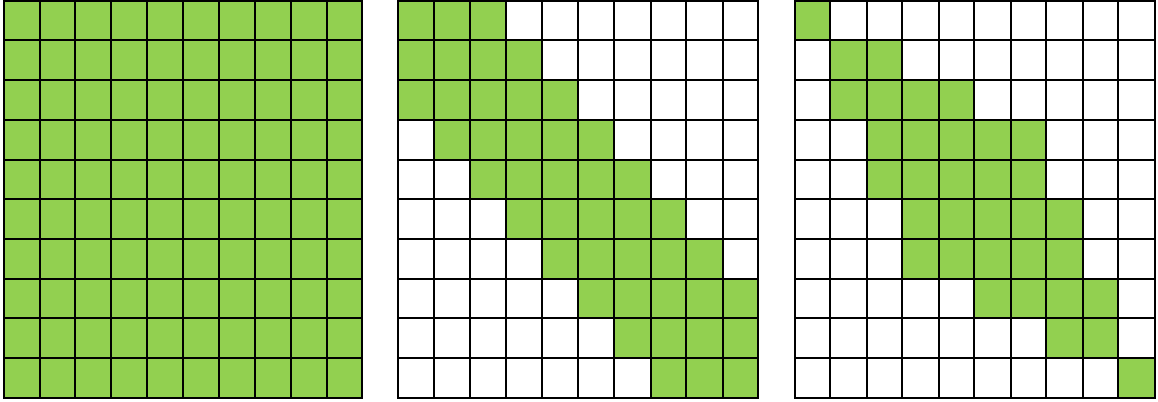


Figure 5.3: Different distance matrix constraints. From left to right: green shaded cells illustrate populated distance cells utilized in traditional DTW, Sakoe-Chiba, and Itakura techniques [143][144].

Fig. 5.4 illustrates a representative human activity situation suitable for application of the Phase-aware DTW technique. The plot illustrates a notional sports activity field with a ski slope defined as running from left to right. The black lines define the physical limits of the ski slope trail with skiers free to traverse the area between the lines in any manner they see fit. In this instance the velocity samples from two skiers were recorded at each indicated location. Red crosses represent the locations with data samples from skier one. Blue stars represent the locations with data samples from skier two. The two skiers traverse the same ski slope along different paths. Using the Phase-aware technique it is now possible to quantitatively compare the performance of multiple skiers throughout the distance of the skiing route. Detailed insights gained as skiers traverse difficult sections of the course will assist in developing improved skier technique. Without this detailed comparison technique, skiers will be left with only overall elapsed time to provide relative performance information. Historically, elite athletes study video that is annotated to report split times at specified locations [156]. This is time consuming

and error prone as trainers make manual transcription mistakes. Through the use of accelerometers and GPS recorders, a detailed record of athlete performance throughout the event is now available for analysis and comparison.

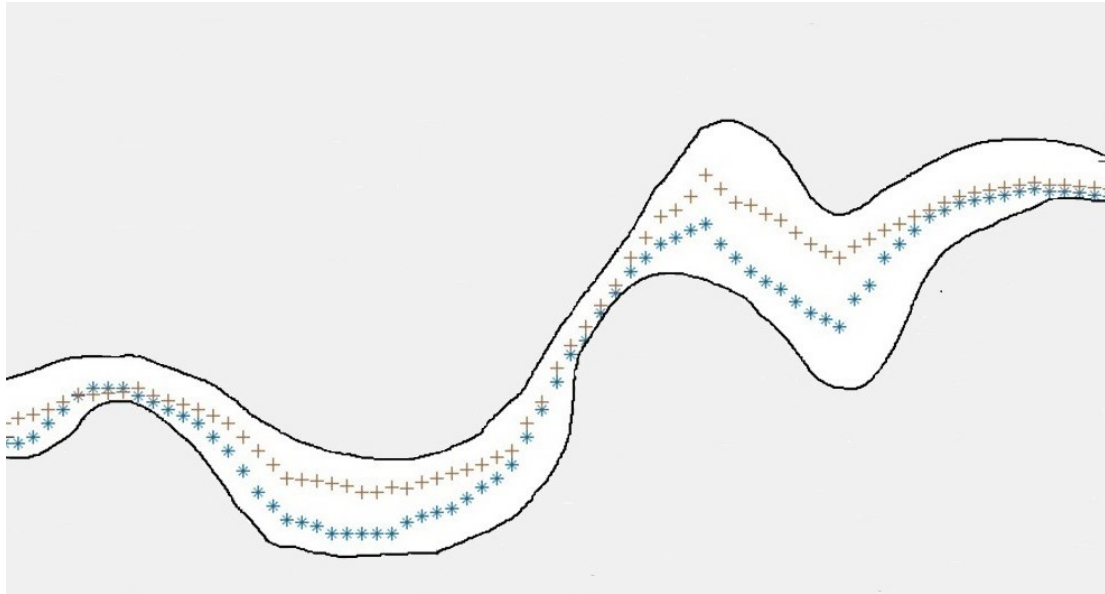


Figure 5.4: Example plot showing time series data collection locations from two persons proceeding from left to right within constraint envelope defined by black lines.

5.3 Phase-aware Dynamic Time Warping

With Phase-aware DTW attention is focused on human activities that are best described through sinusoidal patterns captured in the data sample sequences. Fig. 5.5 illustrates two sinusoidal data patterns, the red line is a weaker magnitude pattern at a higher frequency, the blue line is a stronger magnitude pattern at a lower frequency. They are similar in shape reflecting the same activity performed by two individuals. The activity was performed in the same physical space envelope. The Phase-aware DTW technique has three components. First is

identification of the phase changes in the data sequence. Second is population of the distance matrix only for sections where both sequences are in phase agreement. Third, construction of the optimal warp matrix in the traditional manner. The warp path will run through the populated areas of the distance matrix, augmenting with additional cell computations as needed. Intuitively, the distance matrix is constrained by the phase pattern agreement reflecting the human movement activity envelope. Recall that Phase-aware DTW is designed for sinusoidal environments. An empirical example is provided below.

5.3.1 Phase Identification

Successive data sample pairs in the same sequence that are increasing in value are defined as in positive phase. If they are decreasing in value they are defined as in negative phase, steady state otherwise. Please note in Fig. 5.5 that both lines begin in a positive phase, then disagree in phase as the red line begins to decrease in value. For the example in the figure, the two lines go in and out of phase as the activity is conducted. The first step in Phase-aware DTW is to define the phase associated with each data sample in the two sequences under comparison.

Phase agreement is defined as:

Data Condition	Phase Coding	Data Trend
$m(i + 1) - m(i) > 0$	1	Increasing
$m(i + 1) - m(i) = 0$	0	Locally Constant
$m(i + 1) - m(i) < 0$	1	Decreasing

An example is:

Time series $m = \{0\ 1\ 2\ 1\ 0\ -1\ -2\ -1\ 0\}$

Phase(m) = $\{1\ 1\ 1\ -1\ -1\ -1\ -1\ 1\ 1\}$

Time series $n = \{0\ 1\ 0\ -1\ -2\ -1\ 0\}$

Phase(n) = $\{1\ 1\ -1\ -1\ -1\ 1\ 0\}$

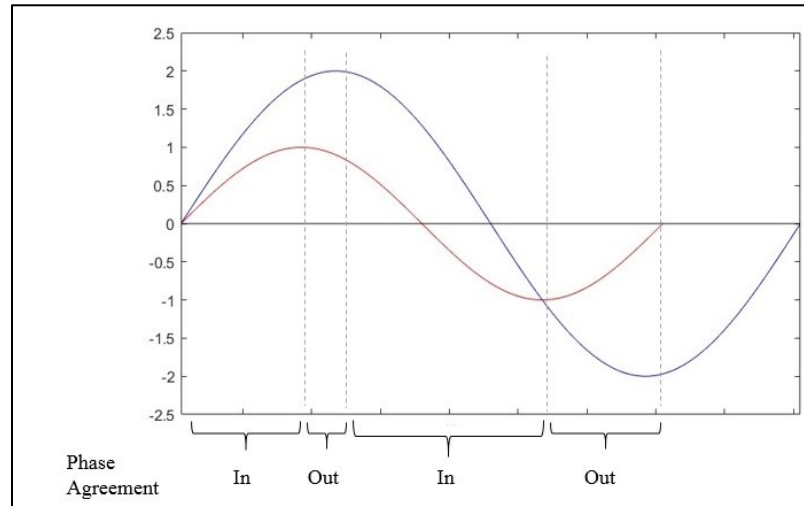


Figure 5.5: Illustration of phase agreement between two sinusoid time series.

5.3.1 Phase Agreement Blocks

The distance matrix is subdivided into phase agreement blocks. As shown in Fig. 5.6, the two data sequences are in agreement in blocks of cells. Intuitively this is because the two original human movement activities are constrained by the same sinusoidal constraint envelope. In blocks with no phase agreement, the two human activity patterns are diverging, so distance is increasing. The optimal warp path

alignment will avoid the higher distance cost cells representing diverging human activity patterns. Steady state blocks are rare and are appended to agreement blocks.

The optimal warp path is constructed in the traditional manner as described in Equation 2. If the warp path strays outside the pre-populated areas of the distance matrix, distance computations will be performed as needed until the warp path returns to the pre-populated areas. The accumulated sum of the warp path distance provides the overall comparison metric.

		0	1	2	1	0	-1	-2	-1	0	m Phase m
		1	1	1	-1	-1	-1	-1	1	1	
0	1	A	A	A	N	N	N	N	N	N	
1	1	A	A	A	N	N	N	N	N	N	
0	-1	N	N	N	A	A	A	A	N	N	
-1	-1	N	N	N	A	A	A	A	N	N	
-2	-1	N	N	N	A	A	A	A	N	N	
-1	1	N	N	N	N	N	N	N	A	A	
0	0	N	N	N	N	N	N	N	A	A	
n Phase n											

Figure 5.6: Phase(m) vs phase(n). Phase agreement between two time series $m=\{0\ 1\ 2\ 1\ 0\ -1\ -2\ -1\ 0\}$ with corresponding phase states $\{1\ 1\ 1\ -1\ -1\ -1\ 1\ 1\}$ and $n=\{0\ 1\ 0\ -1\ -2\ -1\ 0\}$ with corresponding phase states $\{1\ 1\ -1\ -1\ -1\ 1\ 0\}$, A means data sequence is in same phase, or constant at sample time, and distance cell will be populated. N means data sequence is in opposite phase at sample time, distance cells will not be populated.

5.4 Performance Evaluation

The simulated data illustrated in Fig. 5.4 consists of two, 75-element velocity vectors representing the sampled speeds of the two skiers traversing the notional ski trail. The complexity of the Phase-aware technique as measured by populated distance matrix cells, was compared with the traditional DTW technique, and an

Optimal Sakoe-Chiba technique that is just wide enough to encompass the optimal warp path. The results in Table 5.1 showed that the Phase-aware technique had greatly reduced complexity, paving the way for comparative analysis of much longer time series sequences. In the comparison, the number of cells were counted which were initially populated by Phase-aware in addition to the few additional cells that were additionally populated as the optimal warp path was constructed. Phase-aware only needed to further compute 27 distance values in addition to the original 1,110 computed in the phase agreement blocks. For this empirical example, the Phase-aware technique computed 1,110 cells out of the necessary 1,137 for an accuracy rate of 97.6% percent.

Table 5.1: Empirical comparison of DTW techniques

Technique	Distance cells populated	Percentage of All Cells Populated
Traditional DTW 75x75	5,625	100.0%
Sakoe-Chiba	3,273	58.2%
Phase-aware	1,137	20.2%

5.5 Limitations

As described in this work, our Phase-aware technique is suitable for the broad class of sinusoidal human movement patterns. Application of this technique to other types of data without defined phase characteristics in their patterns will not produce optimal results. This work has shown that it can be productive to carefully

study user movement patterns to deduce characteristics that can be leveraged to improve algorithm efficiency and complexity.

5.5 Conclusion

The Phase-aware DTW technique offers a new way to measure and compare human activity patterns in constrained sinusoidal envelopes. Our addition of phase state to each data sample value allowed for consideration of natural constraints without loss of data accuracy. Reflecting the natural and geographic constraints of many types of human movement patterns, Phase-aware offers an opportunity to compare larger time series datasets than traditional DTW computing techniques given limited processing and storage space. Through simulated experiment it was demonstrated that Phase-aware offers an 80% improvement over traditional DTW in space and computing complexity. Phase-aware also demonstrated a 65% improvement over an optimally configured Sakoe-Chiba DTW constraint. With sensors coming into more common use with many types of human activities, Phase-aware offers a new way of thinking about efficient analysis and comparison of human activity patterns.

Chapter 6

Secure and Efficient Computation of Private Sensor Data

A data similarity comparison technique is presented that preserves user sensor data privacy, while also comparing the user's time series data with a library of templates located on a remote cloud server. As was mentioned in Chapter 5, DTW has been widely applied in speech [84][116], gesture [85], and hand-writing signature recognition [86] by comparing a user's individual time series sequence with a library of data templates stored on a server [153]. The result of the similarity evaluation indicates if a match to a known reference template is obtained.

User data transferred from personal computing technologies such as smartphones is vulnerable to privacy leakage. The user's data is uploaded to the remote or cloud servers, with only the comparison result returning to the user's device. While users are given a privacy and data usage agreement before accessing remote services, users frequently just accept agreements without reading them. These agreements may also grant the company permission to retain and utilize private user data for various other purposes [80]. It has been shown that this data could be used to infer the user's gender, personality, emotion, name, and travel locations [78][79]. Little work has been done on enhancing secure function evaluation with personal computing devices, because existing privacy-preserving computation protocols impose too heavy of a processing and space utilization burden. This project has demonstrated the feasibility of this technique in the lab with a smartphone-laptop server configuration. The privacy-preserving time

series recognition protocol applies secure computation techniques to existing traditional unsecure DTW technique described as shown in Table 6.1.

Table 6.1: Mapping of Unsecure to Secure DTW techniques

	Unsecure Computation	Secure Computation
Distance Computation One Cell	Squared Euclidean Distance $ a - b ^2$	Private Squared Euclidean Distance $a^2 - 2ab + b^2$
Distance Matrix Filling	Immediate Fill with SED	Privacy-Preserving Matrix Filling
Finding Minimal Warp Path and Cost	Dynamic Programming	Private Minimal Finding

6.1 Privacy-Preserving Protocol Workflow

Algorithm 6.1 provides a simple description of our protocol. Further details are depicted in Fig. 6.1. In our protocol, the single distance matrix used in traditional DTW is replace by a two-part Dynamic Programming Matrix (DPM). One part of the DPM resides on the user device. The other part of the DPM resides on the server. Encrypted data products are exchanged by the user and server to populate their respective matrices. This data exchange leads to significant communications loading, a concern for a resource-limited device such as a smartphone.

Algorithm 6.1 Dynamic Time Warping using SED

```

1: procedure DTW( $A[n_a], B[n_b], M[n_a][n_b]$ )
    where  $A$  is the user's time series dataset
            $B$  is a server's data template
            $M$  is the distance matrix
            $n_a, n_b$  are indexes
2:    $M[1][1] \leftarrow d^2(A[1], B[1])$ 
3:   for  $i = 2 : n_a$  do
4:      $M[i][1] \leftarrow d^2(A[i], B[1]) + M[i - 1][1]$ 
5:   for  $j = 2 : n_b$  do
6:      $M[1][j] \leftarrow d^2(A[1], B[j]) + M[1][j - 1]$ 
7:   for  $i = 2 : n_a$  do
8:     for  $j = 2 : n_b$  do
9:        $M[i][j] \leftarrow d^2(A[i], B[j]) + \min(M[i - 1][j - 1], M[i][j - 1], M[i - 1][j])$ 
  
```

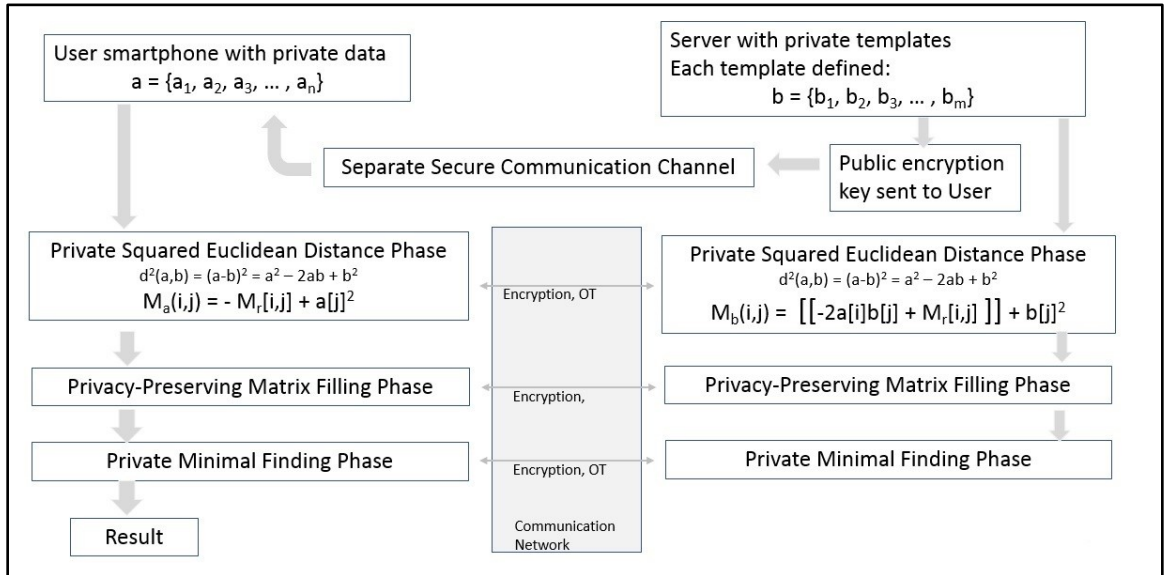


Figure 6.1: Workflow of Secure DTW Computation

6.2 Cryptographic Tools

Key components of our protocol are formed from Homomorphic Encryption and Oblivious Transfer tools.

6.2.1 Homomorphic Encryption

Homomorphic Encryption provides the capability for arithmetic operations to be performed on encrypted data. The result remains in encrypted form and remains concealed privately for further steps in our protocol. We use Paillier encryption [90], relevant arithmetic functionality is shown in Fig. 6.2.

Enables computations on encrypted data

$$\text{Enc}(a) \times \text{Enc}(b) = \text{Enc}(a + b)$$
$$\text{Enc}(a)^{\text{Enc}(b)} = \text{Enc}(a \times b)$$
$$\text{Enc}(a) / \text{Enc}(b) = \text{Enc}(a - b)$$

Ex. If $a = 2, b = 3$ then $\text{Enc}(2) \times \text{Enc}(3) = \text{Enc}(5)$

Figure 6.2: Homomorphic Encryption

6.2.2 Oblivious Transfer

Oblivious Transfer(OT) protocol is a key building block in many secure computation applications. OT allows one party, the receiver Bob, to secretly retrieve one or more values of its own choice from another party, the sender Alice, while no other information is disclosed during the protocol [91]. In this project the chooser and the sender are the user and the server respectively. The chooser will not know the other values held by the sender, while the sender has no idea which values are taken by the chooser. If the chooser is selecting one value out of two

values from the sender, the term is called a 1-out-of-2 OT, denoted as 1-2 OT. A example OT workflow is provided in Fig 6.3. OT-Extension [93] is a promising technique to reduce the high costs of OT. It extends a small number of base OTs to a very large number of OTs using simpler symmetric functions. Similar to hybrid encryption which uses a relatively expensive public key encryption scheme to exchange a secret key, and then uses the secret key for relatively cheap symmetric encryption. Recent optimizations [94][95] have shown that efficient implementation of OT-Extension can reduce communication complexity.

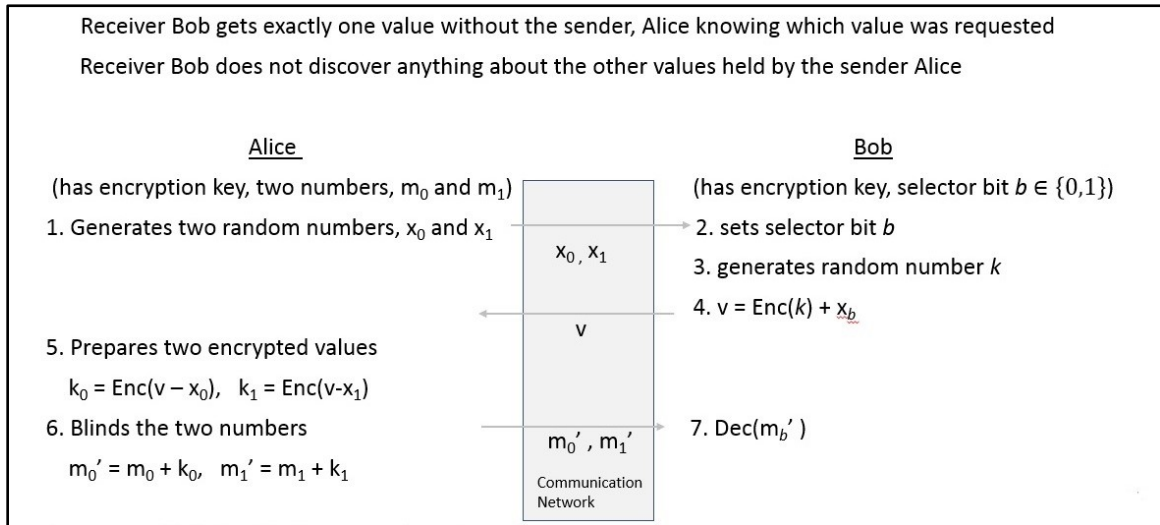


Figure 6.3: Oblivious Transfer Workflow

6.3 Private Squared Euclidean Distance

In order to calculate DTW distance privately, it is necessary to compute squared Euclidean distance $d^2(a, b)$ privately. To compute a squared Euclidean $(a - b)^2 = a^2 - 2ab + b^2$ where a and b are all l bit integers, it is only necessary to obtain the product ab , since a^2 and b^2 can be calculated locally by the user and the server.

The scalar product computation, based on [96], proposes *binHDOT* for secure Hamming distance computation using OT and homomorphic encryption. This technique can be used for scalar product computation, since scalar product is actually equivalent to the Hamming distance when the alphabet is binary. This protocol is extended to implement secure Euclidean distance computation. Due to the inefficiency in homomorphic encryption, Bringer et al. [97][98] have proposed a protocol for Hamming distance computation using only OT and generalized it for several more distance metrics such as Mahalanobis distance, Euclidean Distance and Scalar Product. The core technique enabling use of OT for Hamming distance calculation is the binary representation method. By adopting a similar method to calculate the scalar product of two inputs, this protocol extends from a 1-vs-1 case to a $M \times N$ case. The Private Squared Euclidean Distance workflow is shown in Fig. 6.4.

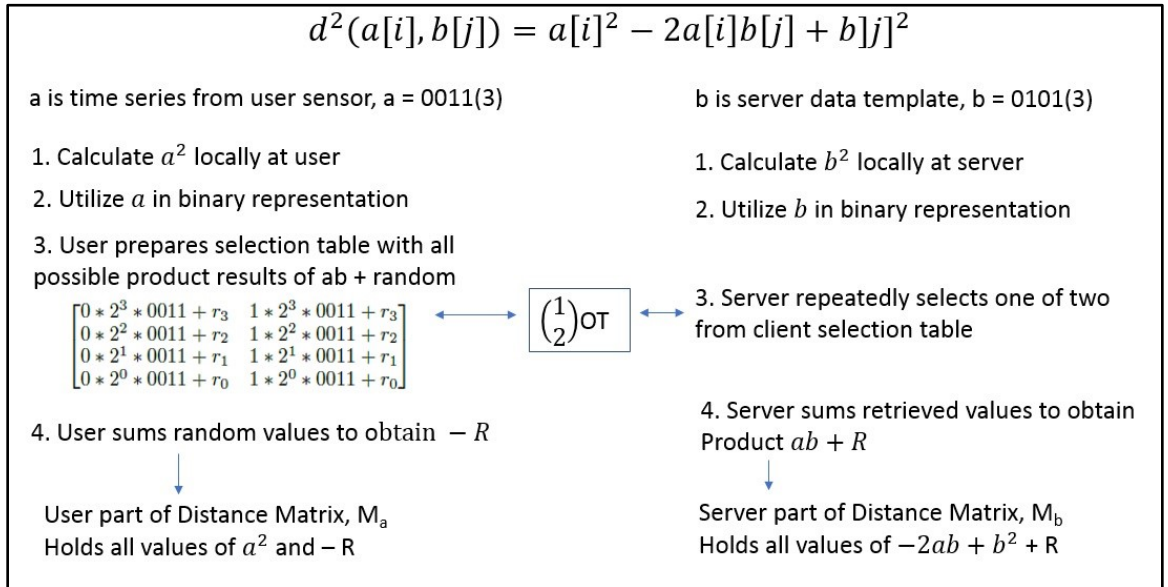


Figure 6.4: Private Squared Euclidean Distance Workflow

6.4 Private Matrix Filling

In order to fill the matrix, the server will send an encrypted triple tuple $[\text{Enc}(M_b^{i-1,j-1}); \text{Enc}(M_b^{i-1,j}); \text{Enc}(M_b^{i,j-1})]$ to the client. Without a secret key, the client cannot decrypt these cipher texts. Through multiplication of cipher texts, e.g. $[[M_a^{i,j}][M_b^{i,j}] = [M_a^{i,j} + M_b^{i,j}] = [a_i^2 - 2a_i b_j + b_j^2]$, the client can get the SED in cipher text. Now the private Dynamic Programming Matrix (DPM) fill has been reduced to the private minimal finding problem of finding the minimal value in a triple tuple of cipher texts. Fig. 6.5 has the workflow for Private Matrix Filling.

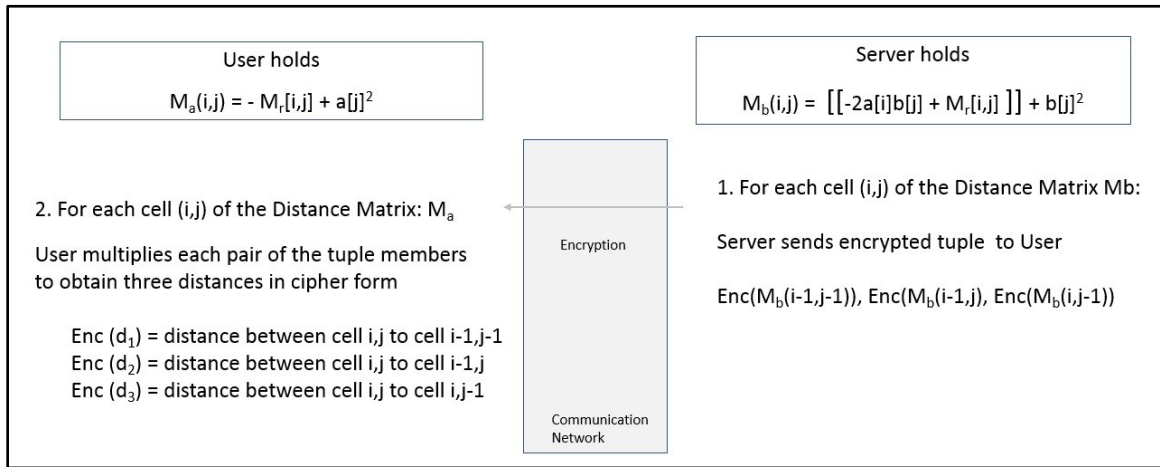


Figure 6.5: Private Matrix Filling

6.5 Private Minimal Finding

In order to find the optimal warp path, it is necessary to use a privacy-preserving protocol for finding the minimum value in a set of distance values adjacent to each cell in the DPM. The detailed workflow of Private Minimal Finding is shown in Fig.

6.6. An illustration of Private Matrix Filling and Private Minimal Finding is shown in Fig. 6.7.

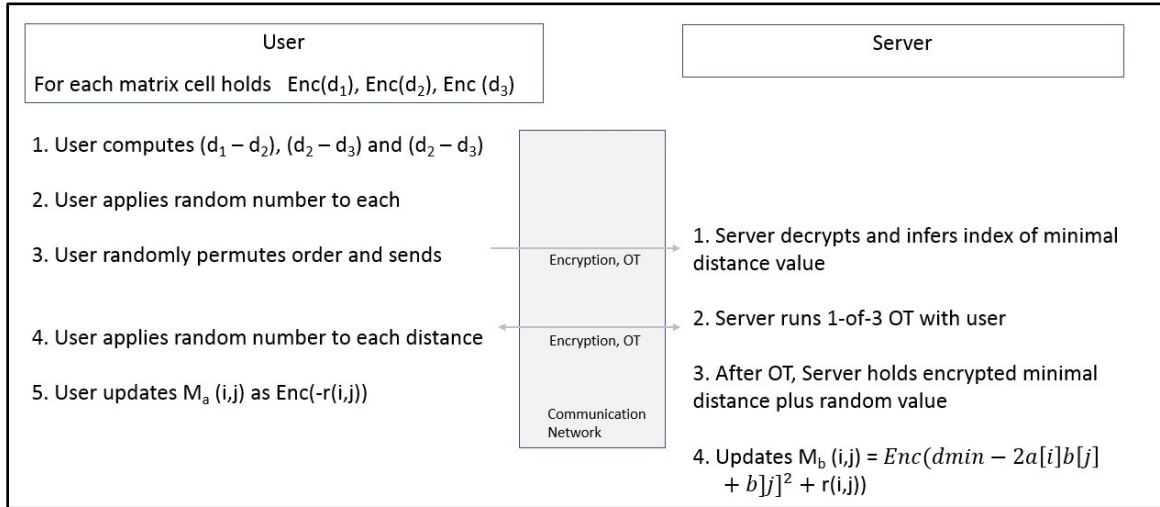


Figure 6.6: Private Minimal Finding

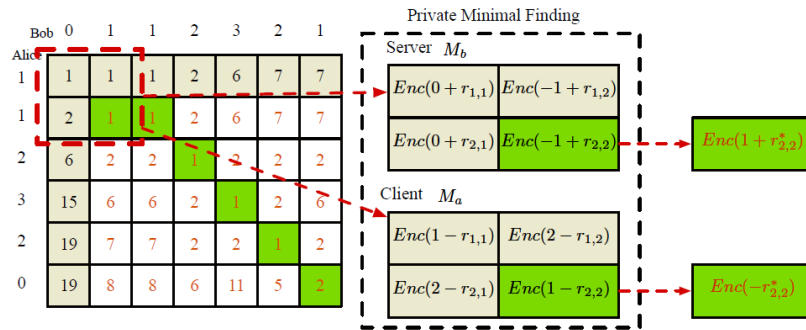


Figure 6.7: Matrix Filling in Privacy-preserving DTW.

6.6 Batched Matrix Filling Optimization

The baseline matrix filling is iterative. Computations supporting each cell filling require individual communications loads between client and server. However, communications overhead may be consolidated by utilizing a batching method. Since the update of each distance cell only depends on three immediately adjacent

cells, an update scheme can be designed as shown in Fig. 6.8, where the cells in the same red dash-line box will be batched together and transmitted in a single network connection. The iteration will follow the direction shown in the figure to ensure correct data dependencies are present for subsequent computations.

By employing a batched method, the number of network connections during the DPM filling has been reduced from $O(mn)$ to $O(m + n)$.

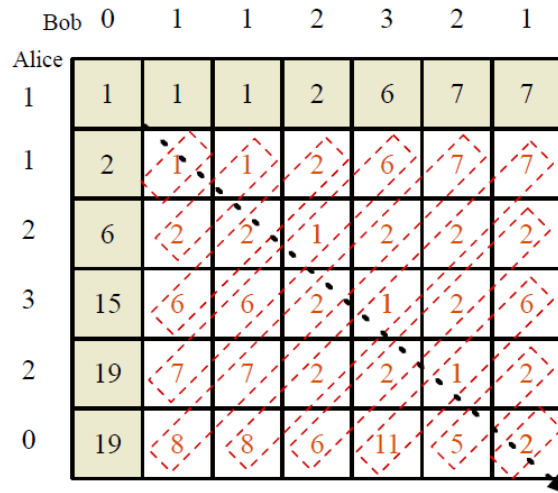


Fig. 6.8 Batched Matrix Filling Scheme in Privacy-preserving DTW.

6.7 Performance Evaluation

This protocol has been implemented in a client-server setup for evaluation. The client runs on a smartphone (Huawei Nexus 6p, 2GHz Qualcomm Snapdragon 810 processor), and the server runs on a remote server (2.2GHz Intel Core i7 MacBook Pro). The OT and OT-Extension protocols used for SED computing

implementations are based on ECC, while the 1-2 OT implementation is based on prime numbers.

Paillier Encryption is carried out on both phone and laptop. However, to evaluate loading on the smartphone, the key length is adjusted from 64 to 2048 bits and resulted are reported in Fig. 6.9 and Fig. 6.10. The left side is the result on the phone, noted as C and the right side is the result at the laptop, noted as S. The results show that the overhead of Paillier encryption is negligible when the key is short, and scales exponentially when the key is longer. Additionally, the homomorphic encryption operations cost only 1 to 2 ms on both devices. This is favorable since most Paillier-related operations at the phone are Add and Mul, low cost operations. The phone only needs the Enc and the server will do both Enc and Dec. Therefore, the chosen key size is 1024, which is a good trade-off between time cost and security.

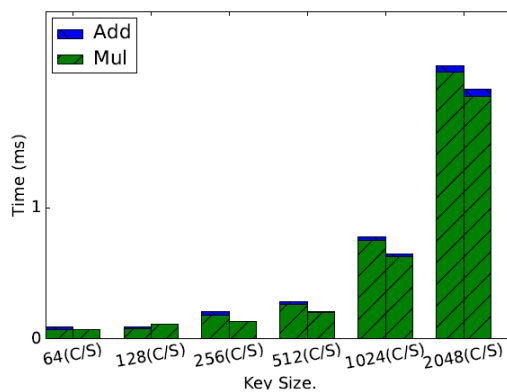


Figure 6.9: Benchmark of Add/Mul on Paillier encryption.

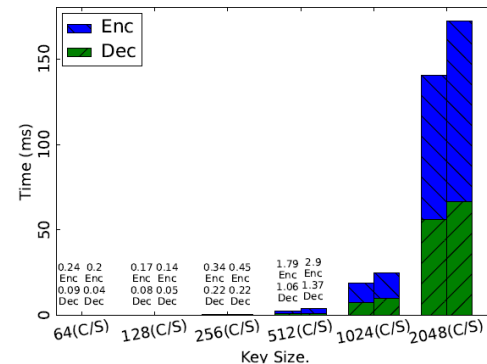


Figure 6.10: Benchmark of Enc/Dec on Paillier encryption.

Comparison of OT and OT-Extension is performed with both ECC-based and Prime-based OT implementation. The benchmark tests on smartphone and laptop with varying input sizes are shown in Fig. 6.11 and Fig. 6.12. The slow ECC implementation, of the underlying crypto library BouncyCastle [101] is illustrated. This benchmark shows that OT-Extension can significantly improve performance. Considering ECC can provide the same level of security with a much shorter key size, the ECC-based OT Extension is chosen for the private scalar product protocol to reduce communication cost. The private minimal finding requires 1-2 OT, in which case the improvement of OT extension technique is limited. Therefore, private minimal finding is implemented with Prime OT to obtain a better balance between time and communication costs.

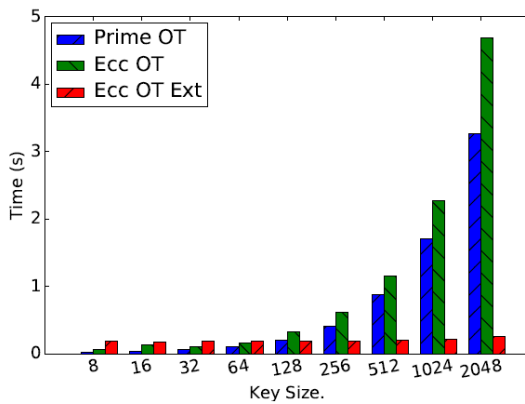


Figure 6.11: OT Benchmark on Laptop.

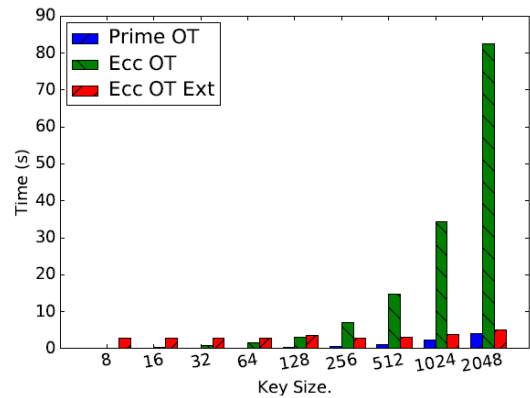


Figure 6.12: OT Benchmark on Smartphone.

6.7.1 Comparison to Previous Work

Previous work by Zhu [87] has built a privacy-preserving time series similarity computing protocol based on homomorphic encryption and a blind-and-insert-dummy method. Due to the number of dummies and corresponding invocations of homomorphic encryption, this scheme is not efficient. Additionally, their implementation of Paillier encryption uses a 64-bit prime number, which is not as secure. Two security enhancements have been made on their implementation in order to make a fair comparison with this approach: 1) adoption of 1024-bit key for Paillier encryption; 2) change of the random number generator from Random to SecureRandom. The two protocols are run on a local laptop with the same parameter setups and compare the time and communication costs. The time and communication cost comparisons are illustrated in Fig. 6.13 and Fig. 6.14, respectively. The x-axis is the input vector length shared by client and server. From the communication cost breakdown in [87], it has been found that all communication loads are on the client side.

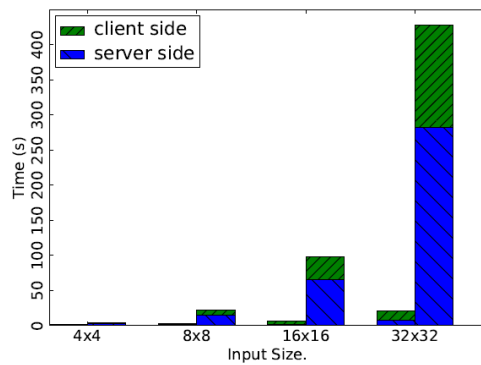


Figure 6.13: Time Cost in seconds. Left bar is the protocol. Right bar is result from [87].

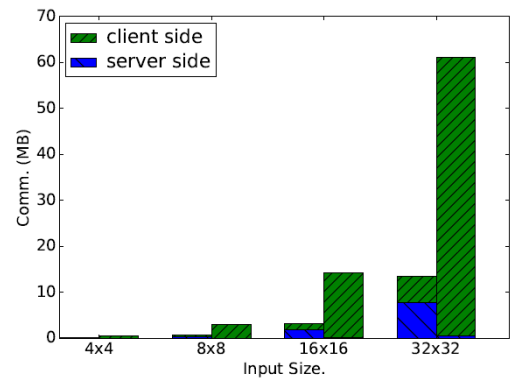


Figure 6.14: Communication Cost in MB. Left bar is the protocol. Right bar is result from [87].

6.7.2 Performance on Smartphone-Laptop Configuration

The protocol has been deployed on a smartphone-laptop configuration with varying input sizes. The time cost breakdowns are shown in Fig. 6.15. The communication loading costs are shown in Fig. 6.16. These indicate that the private minimal finding protocol is very efficient. The high time cost of phase 1 may be attributed to the inefficient ECC implementation in the crypto library. The communication costs are in reasonable range considering current high-speed Internet provided by WiFi and LTE.

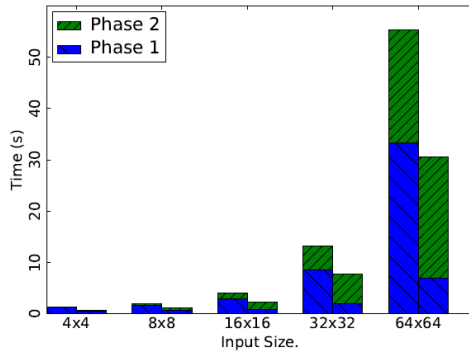


Figure 6.15: Time Cost in seconds. Left bar is client side. Right bar is server side.

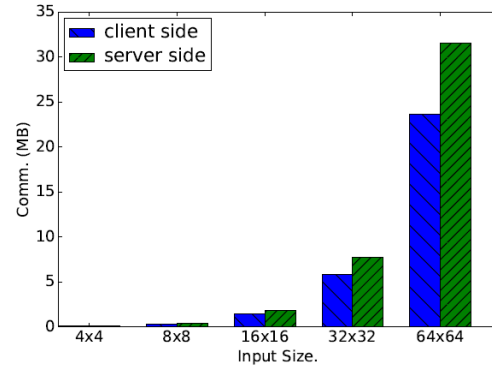


Figure 6.16: Communication Cost in MB.

6.7.3 Performance on Gesture Recognition Data

To assess system performance on realistic time series data, our protocol was applied to the gesture data obtained from [102]. Seven gestures, *check*, *circle*, *delete mark*, *pigtail*, *question mark*, *rectangle*, and *triangle* formed a set of gesture templates. Each gesture time series length varied from 30-90 samples depending on different user drawing speeds. The template sets were tested on gesture *check*, with the results provided in Fig. 6.17. The expected average time savings if Early Abandon (EA) is enabled is also indicated, currently about 30s recognition time

with a smartphone and remote server setup. While orders of magnitude improvement have been achieved compared to previous work, it is acknowledged that this recognition time cost may not meet the smartphone user expectations.

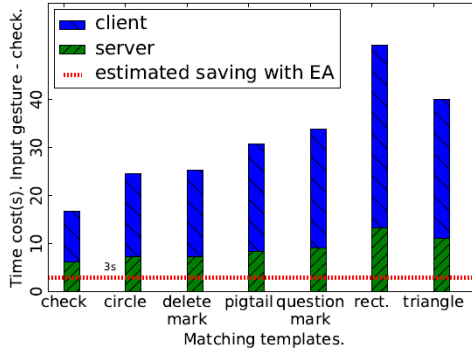


Figure 6.17: Time Cost of matching a check gesture to all seven templates and the expected average time savings with Early Abandon.

6.8 Performance Optimizations

As previously mentioned in Section 5, there are several techniques proposed to improve DTW performance by intelligently applying constraints on the number of filled cells in the distance matrix, hierarchically refining coarse DTW solutions, and aggregating or downsampling data resulting in reduced solution granularity.

6.8.1 Performance Optimization via Early Abandon

Our lab tests implemented an optimization technique called *Early Abandon (EA)*. It tracks the intermediate DTW accumulation, and compares it to the current optimal result. Since the DTW solution is always increasing, the protocol can be terminated when the current DTW accumulation surpasses the *in-hand* optimal result. While there are other Early Abandon schemes based on other lower bounds [99][100], the Euclidean distance-based early abandon is advantageous since the distance can be computed securely. The specifics of Early Abandon is presented

in Alg. 6.2. A simple implementation is to check the interim DTW solution once at the halfway point of each run of each privacy preserving DTW algorithm.

Algorithm 6.2 Early Abandon

- 1: **procedure** EarlyAbandon(d^* , i , j)
 where d^* is the current optimal distance (minimal), i, j is the index of
 client and server input respectively.
 - 2: Client holds $\llbracket R_{ij} \rrbracket$, and key pairs sk, pk .
 - 3: Server holds $\llbracket d_{ij} + R_{ij} \rrbracket$
 - 4: Server prepares a random number a
 - 5: Client computes and sends $\llbracket -R_{ij} - d^* \rrbracket$ to server
 - 6: Server computes and sends $\llbracket a(d_{ij} - d^*) \rrbracket$ to client
 - 7: Client decrypts $\llbracket a(d_{ij} - d^*) \rrbracket$ and checks the sign
 - 8: **if** sign is positive **then**
 - 9: abort, move on to the next input in server's data template library
 - 10: continue the computation on current input
-

6.9 Conclusion

In this project we showed it is possible to preserve the privacy of both the user's personal information, and the remote cloud server's valuable data template library while performing time series data similarity comparisons. We utilized Homomorphic Encryption, Oblivious Transfer and a split distance matrix during DTW to performing similarity comparisons and also preserve privacy of both parties. We demonstrated that it is possible to improve DTW efficiency by adopting an Early Abandon technique midway through the similarity comparison if interim

results exceed the current “best-in-hand” solution. Lastly, we showed that our technique was viable in a smartphone-laptop configuration in our lab environment.

Chapter 7

Conclusion and Future Work

In this dissertation we have described four projects illustrating the usability, efficiency and security benefits realized from strong consideration of user characteristics and behaviors. For our first project we have investigated the concerns of older computer users and created a graphical password authentication system leveraging the inherent ability already within everyone to recognize familiar faces. With our use of touchscreen image selection, and easy-to-recall faces, our technique has eliminated an important barrier to technology use for this population. We conducted a usability study of our graphical password system that demonstrated our technique was fast, easy to use and fun.

We investigated current fitness tracker user motivations and user activity patterns by gathering data from a variety of sources. We were able to develop a quantified description of average personal fitness tracker motivations, reliability concerns, activity levels, behavior and social activity patterns, serving as a basis for user understanding of potential benefits, and a foundation for future device enhancements. We were able to characterize user activity and behavior patterns discriminated by age, gender, and duration of device ownership. We believe we are the first to describe user behaviors in fitness social forums.

For our third project we developed a new time series data similarity comparison algorithm that is optimized for sinusoidal human movement pattern comparison. Through awareness of user movement patterns, study of existing dynamic time

warping techniques and optimization constraints, we were able to define a new phase state field added to user movement time series data samples. Relying on the phase state to focus on optimal comparison regions resulted in improved computational and space efficiency.

Finally, we present a secure technique for similarity comparison of private user sensor data with private data templates on remote-cloud servers. Our protocol protects both the user's data and the server's data from privacy compromise.

Our efforts have shown that rewarding results may be obtained through careful study and assessment of user characteristics. Technology designs that compensate for user disabilities may enable those users to continue participation in technological society. Accurate assessment of personal technology device utilization may allow users to make informed decisions on personal fitness programs. Leveraging knowledge of user movement patterns resulted in optimizations to the dynamic time warping algorithm. Enhancing DTW led to a secure computation technique that protects both user data privacy and cloud-service data templates.

7.1 Future Work

We believe that each of our projects illustrate the need for future investigations in improving the user experience, and leveraging our increased user knowledge in tailoring future technology designs. Our ideas are presented below.

7.1.1 Graphical Password Authentication System

In our Graphical Password project, we have shown the benefits of carefully studying user characteristics and creating a tailored authentication technique. Our current implementation is suitable for a specific cultural group of North American older adults. To expand this project to other cultural groups it will be necessary to add additional familiar images recognizable to those other groups in order to reap the benefits of facial recognition and recall from long-term memory that have been demonstrated here. The advantage to expanding the image database will be that it also has the beneficial effect of increasing password entropy thereby rendering the password sequence more resistant to attack. The image selection tool should be modified to permit users to choose a culturally appropriate image set and timeframe for their personal background.

Future work focusing on the color spectrum and frequency content of the images themselves would be a reasonable avenue to improve user recognition efficiency, and improve resistance to shoulder surfing attack. The set of black and white images are intended to provide a consistency of appearance to a distant observer making it difficult to detect the user's personal sequence from afar. A defined common color spectrum profile applied to all images would be a step towards enhancing uniformity of appearance. The frequency content of images can also be managed to systematize the low frequency content which is recognizable from farther away than the high frequency fine image details. The user is very close to the presented images so is easily able to discern necessary fine image details to recognize their target images. Control and standardization of

image content noticeable from farther away will improve resistance to shoulder surfing attack.

Older users are very interested in using smartphones but their small displays are challenging for those with vision impairments. Additionally, the small areas of the touchscreen are challenging for those with shaky hands or disabled fingers to precisely and accurately target small images. Future work porting this technique to smartphones should focus on the essential parts of the facial image that are necessary to optimize recall and recognition. Images on the smartphone should be as large as screen real estate will permit. Additionally, adoption of a swipe pattern would assist those with arm/finger mobility issues. Use of a swipe pattern selection technique would require target images to be in adjacent proximity to each other each time the screen display is re-randomized.

7.1.2 Personal Fitness Tracker Usage Analysis

It may prove informative to revisit the data sources in this study to quantify the degree of continued active PFT utilization. Such a project would lend insight into the persistence of personal fitness tracker users and the validity of our data sources. Any changes in motivation and reliability trends would reflect the real-world experiences of the maturing personal fitness tracker user population. Understanding current PFT utilization patterns should inform both effective future device modifications, and foster more effective practices within fitness social forums.

7.1.3 Phase-aware Dynamic Time Warping Analysis

Our work with dynamic time warping has shown that it can be productive to carefully study movement patterns to deduce characteristics that can be leveraged to improve algorithm efficiency and complexity. Other types of human activities may prove profitable to similar study. Smartphones often contain a variety of sensors that would be valuable to study. Extension of this technique to the smartphone platform should consider maximum time series size constraints due to space limitation. It would be productive to evaluate smartphone energy savings experienced by implementing the Phase-aware technique as contrasted with conventional dynamic time warping constraint methods.

Longer data sequences are coming into greater use as users adopt personal technologies into their daily lives. Better techniques for similarity comparison of longer user actions, or greater sampling resolution of smartphone sensors, will be needed to smartly choose between multiple possible, yet near-equivalent distance warp paths in the remote server's data template library. The simple example of Fig. 6.4 does not illustrate the complexities of potential warp path routing in larger distance matrices. Some applications may find meaning in characteristic patterns or shapes of warp paths through the distance matrix.

Future work should also consider that more efficient methods of storing and sorting among the remote server's library of stored data templates will be needed. It may be that hierarchical access models of data template selection will be based on categorization by raw distance scores, shapes of warp path subsections, or establishment of distance minimization direction rules when multiple equivalent

minimization directions are present. Optimally, it should not be necessary to compare a user's time series data sequence to every single data template in the server library if additional techniques for template inclusion/exclusion in the similarity comparison can be developed.

7.1.4 Secure and Efficient Computation of Private Sensor Data

Future secure computation work should focus on application to real-world user activities, and implementation on emerging smartphone platforms. Data privacy is important to users and today, users have to accept less-than-secure technologies to obtain personal benefits. Users desire secure features that blend in to their activities seamlessly and conveniently, ideally, they should also be transparent to the user.

Bibliography

- [1] <https://en.wikipedia.org/wiki/Usability>
- [2] <https://en.wikipedia.org/wiki/Psychology>
- [3] <https://en.wikipedia.org/wiki/Physiology>
- [4] Sacha Brostoff and M. Angela Sasse., M. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. *People and Computers XIV-Usability or Else!*. pp. 405-424, 2000. Springer Link.
- [5] James Nicholson, Lynne Coventry, and Pam Briggs. Age-Related Performance Issues for PIN and Face-based Authentication Systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'13, pp. 323-332.
- [6] Paul Dunphy and Jeff Yan. (2007) Do Background Images Improve “Draw a Secret” Graphical Passwords? In *Proceedings of the 14th ACM conference on Computer and Communications Security*, CCS'07, pp. 36-47.
- [7] Nicholas Van Balen and Haining Wang. GridMap: Enhanced Security in Cued-Recall Graphical Passwords. In *International Conference on Security and Privacy in Communications Networks*, SECURECOMM'15, Vol. 152, pp. 75-94. Springer Link.
- [8] Passfaces Corporation. The science behind Passfaces. <http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf>. (Accessed April 2015)

- [9] 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*, Vol. 63(1-2) Issues 1-2, pp.102–127. 2005.
- [10] Robert Biddle, Sonia Chiasson and P.C. Van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys*. Vol. 44 Issue 4, Article No. 19. August 2012.
- [11] Saranga Komanduri and Dugald Hutchings. Order and Entropy in Picture Passwords. In *Proceedings of Graphics Interface 2008*, GI'08, pp. 115-122.
- [12] Soumyadeb Chowdhury, Ron Poet and Lewis Mackenzie. (2014) 'Passhint: Memorable and Secure Authentication. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'14, pp. 2917-2926.
- [13] Dinei Florencio and Cormac Herley. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW'07. pp. 657-666.
- [14] Joseph Bonneau and Soren Preibusch. (2010) 'The password thicket: technical and market failures in human authentication on the web. In *Proceedings of the 9th Workshop on the Economics of Information Security*, WEIS'10.
- [15] Jenny Waycott, Frank Vetere, Sonja Pedell, Lars Kulik, Elizabeth Ozanne, Alan Gruner and John Downs. Older Adults as Digital Content Producers. In

Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI'13, pp. 39-48.

- [16] Zijian Hao and Qun Li. Towards User Re-Authentication on Mobile Devices via On-Screen Keyboard.' In *4th IEEE Workshop on Hot Topics in Web Systems and Technologies*, HOTWEB'16, pp. 78-83.
- [17] Yafeng Yin, Qun Li, Lei Xie, Shanhe Yi, Ed Novak and Sanglu Lu. CamK: a Camera-based Keyboard for Small Mobile Devices. In *35th Annual IEEE International Conference on Computer Communications*, INFOCOM'16.
- [18] Leah Findlater, Jon Froehlich, Kays Fattal, Jacob Wobbrock and Tanya Dastyar. Age-Related Differences in Performance with Touchscreens Compared to Traditional Mouse Input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'13, pp. 343-346.
- [19] Grace Shin, Eun Jeong Cheon and Mohammad Jarrahi. Understanding Quantified-Selfers' Interplay between Intrinsic and Extrinsic Motivation in the Use of Activity-Tracking Devices. In *Proceedings of iConference 2015*, 2015-03-15.
- [20] Thomas Fritz, Elaine Huang, Gail Murphy and Thomas Zimmermann. Persuasive technology in the real world: A study of long-term use of activity sensing devices for fitness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pp. 487–496. ACM.
- [21] Mark Whooley, Bernd Ploderer and Kathleen Gray. On the Integration of Self-tracking Data amongst Quantified Self Members. In *Proceedings of the 28th*

- International BCS Human Computer Interaction Conference*, BCS-HCI'14, pp. 151-160.
- [22] Eun Choe, Nicole Lee, Bongshin Lee, Wanda Pratt and Julie Kientz. Understanding Quantified-Selfers' Practices in Collecting and Exploring Personal Data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'14, pp. 1143-1152.
- [23] John Rooksby, Mattias Rost, Alistair Morrison and Matthew Chalmers. Personal Tracking as Lived Informatics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'14, pp. 1163-1172
- [24] Daniel Epstein, An Ping, James Fogarty and Sean Munson. A Lived Informatics Model of Personal Informatics. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp'15, pp. 731-742.
- [25] Ian Li, Anind De and Jodi Forlizzi. A Stage Based Model of Personal Informatics Systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'10, pp. 557-566.
- [26] Frank Bentley, Konrad Tollmar, Peter Stephenson, Laura Levy, Brian Jones, Scott Robertson, Ed Price, Richard Catrambone and Jeff Wilson. Health Mashups: Presenting statistical patterns between wellbeing data and context in natural language to promote behavior change. In *ACM Transactions on Computer-Human Interaction*, TOCHI 20(5):30, 2013.

- [27] Rayoung Yang, Eunice Shin, Mark Newman and Mark Ackerman. When Fitness Trackers Don't 'Fit': End-User Difficulties in the Assessment of Personal Tracking Device Accuracy, In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp'15, pp. 623-634.
- [28] Jeungmin Oh and Uichin Lee. Exploring User Experience Issues in Quantified Self Technologies, 2015 *Eighth International Conference on Mobile Computing and Ubiquitous Networking*, ICMU'15, pp. 53-59.
- [29] Ian Li, Anind Dey, and Jodi Forlizzi. Understanding My Data, Myself: Supporting Self-Reflection with Ubicomp Technologies. In *Proceedings of the 13th international conference on Ubiquitous computing*, UbiComp'11, pp 405-414.
- [30] Niels van Berkel, Chu Luo, Denzil Ferreira, Jorge Goncalves and Vassilis Kostakos. The curse of quantified-self: an endless quest for answers. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers*, ISWC'15, pp. 973-978.
- [31] James Clawson, Jessica Pater, Andrew Miller, Elizabeth Mynatt and Lena Mamykina. No Longer Wearing: Investigating the Abandonment of Personal Health-Tracking Technologies on Craigslist, In *Proceedings of the 2015 ACM International Conference on Pervasive and Ubiquitous Computing*, UbiComp'15, pp. 647-658.
- [32] Amanda Lazar, Christian Koehler, Joshua Tanenbaum and David Nguyen. Why We Use and Abandon Smart Devices, In *Proceedings of the 2015 ACM*

International Conference on Pervasive and Ubiquitous Computing,
UbiComp'15. pp. 635-646.

- [33] Katrin Hänsel, Natalie Wilde, Hamed Haddadi and Akram Alomainy. Challenges with Current Wearable Technology in Monitoring Health Data and Providing Positive Behavioural Support. In *Proceedings of the 5th EAI International Conference on Wireless Mobile Communication and Healthcare*, MobiHealth'15, pp. 158-161.
- [34] Daniel Epstein, Felicia Cordeiro, Elizabeth Bales, James Fogarty and Sean Munson. Taming Data Complexity in Lifelogs: Exploring Visual Cuts of Personal Informatics Data. In *Proceedings of the 2014 conference on Designing interactive systems*, DIS'14, pp. 667-676.
- [35] Sunny Consolvo, Katherine Everitt, Ian Smith and James Landay. Design Requirements for Technologies that Encourage Physical Activity, In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'06, pp. 457-466.
- [36] Sunny Consolvo, Ian Smith, Tara Matthews, Anthony LaMarca, Jason Tabert and Pauline Powledge. Location Disclosure to Social Relations: Why, When & What People Want to Share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'05, pp. 81-90.
- [37] Kota Tsubouchi, Ryoma Kawajiri and Masamichi Shimosaka. Working-Relationship Detection from Fitbit Sensor Data, In *Proceedings of the 2013*

ACM conference on Pervasive and ubiquitous computing adjunct publication, UbiComp'13 Adjunct, pp. 115-118.

- [38] Mark Newman, Debra Lauterbach, Sean Munson, Paul Resnick and Margaret Morris. It's not that I don't have problems, I'm just not putting them on facebook: challenges and opportunities in using online social networks for health. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, CSCW'11, pp. 341-350.
- [39] Moira Burke, Cameron Marlow and Thomas Lento. Social network activity and social well-being. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'10, pp. 1902- 1912.
- [40] Moira Burke, Robert Kraut and Cameron Marlow. Social Capital on Facebook: Differentiating Uses and Users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'11, pp. 571-580.
- [41] Yi Chang, Lei Tang, Yoshiyuki Inagaki and Yan Liu. What is Tumblr: A Statistical Overview and Comparison, *ACM SIGKDD Explorations Newsletter*, Vol 16, Issue 1, June 2014, pp 21-29.
- [42] Yuheng Hu, Lydia Manikonda and Subbareo Kambhampati. What we instagram: A first analysis of instagram photo content and user types. In *Proceedings of the Eighth International AAI Conference on Weblogs and Social Media*, ICWSM'14, pp. 595-598.
- [43] Lyndon Kennedy, Mor Naaman, Shane Ahern, Rahul Nair and Tye Rattenbury. How flickr helps us make sense of the world: context and content

- in community-contributed media collections. In *Proceedings of the 15th International Conference on Multimedia*, MM'07, pp. 631–640.
- [44] Johan Ugander, Brian Karrer, Lars Backstrom and Cameron Marlow. The Anatomy of the Facebook Social Graph, *Social and Information Networks*, Cornell University Library, 2011, arXiv:1111.4503[cs.SI].
- [45] Kunwoo Park, Ingmar Weber, Meeyoung Cha and Chul Lee. Persistent Sharing of Fitness App Status on Twitter, In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW'16, pp.184-194.
- [46] Nancy Carter, Ed Novak, Cheng Li, Zhengrui Qin and Qun Li. Graphical Passwords for Older Computer Users. In *Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, UIST'15, pp. 29-32.
- [47] Nancy Kanwisher. Functional specificity in the human brain: A window into the functional architecture of the mind. In *Proceedings of the National Academy of Sciences of the United States of America*, PNAS'10, Vol. 107; No. 25; pp. 11163-11170.
- [48] Faraz Farzin, Chuan Hou and Anthony Norcia. Piecing it together: Infants' neural responses to face and object structure. In *Journal of Vision*, Vol. 12, Issue 13, pp. 1-14. 2012.
- [49] Jia Liu, Alison Harris and Nancy Kanwisher. Perception of Face Parts and Face Configurations: An fMRI Study. In *Journal of Cognitive Neuroscience*, Vol. 22, No. 1, pp. 203-211. January 2010.

- [50] Isabel Gauthier, Pawel Skudlarski, John Gore and Adam Anderson. 'Expertise for cars and birds recruits brain areas involved in face recognition. In *Nature Neuroscience*, Vol. 3, No. 2., pp. 191-197. 01 February 2000.
- [51] Rafael Calvo and Dorian Peters. *Positive Computing: Technology for Well-Being and Human Potential*. MIT Press, 2014. ISBN 978-0-262-02815-8.
- [52] Yvonne Rogers, Helen Sharp and Jenny Preece. *Interaction Design*, 4th ed., John Wiley & Sons, Ltd, West Sussex, UK. 2011.
- [53] United States Census Bureau. *An Aging Nation: The Older Population in the United States*. United States. P25-1140. 2014.
- [54] Pew Research Center. *Older Adults and Technology Use*. 2014.
<http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/>
(Accessed 16 May 2017)
- [55] Pew Research Center. *Who's not online and why*. 2013.
<http://pewinternet.org/Reports/2013/Non-internet-users.aspx> (Accessed 16 May 2017)
- [56] Siân Lindley, Richard Harper Abigail Sellen. Designing for elders: exploring the complexity of relationships in later life. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, BCS-HCI'08, Vol. 1, pp. 77-86.
- [57] Norfazlina Haris, Rogayah Majid, Natrah Abdullah and Rozianawaty Osman. The Role of Social Media in Supporting Elderly Quality Daily Life. In *Proceedings of 3rd International Conference on User Science and Engineering*, i-USEr'14, pp. 253-257.

- [58] Password Strength. [online] https://en.wikipedia.org/wiki/Password_strength
(Accessed 26 April 2016).
- [59] Adam Aviv, Katherine Gibson, Evan Mossop, Matt Blaze and Jonathan Smith.
Smudge attacks on smartphone touch screens. In Proceedings of the 4th
USENIX conference on Offensive technologies, WOOT'10, Article No. 1-7.
- [60] Pew Research Center. U.S. Smartphone Use in 2015. 2015.
http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf
(Accessed 16 May 2017)
- [61] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichter, Alexander De
Luca and Matthew Smith. It's a Hard Lock Life: A Field Study of Smartphone
(Un)Locking. In *Proceedings of the Tenth Symposium on Usable Privacy and
Security*, SOUPS'14, pp. 213-230.
- [62] Sara Czaja and Chin Lee. Older Adults and Information Technology
Opportunities and Challenges. In *The Human-Computer Interaction
Handbook*, 2012, Taylor & Francis Group, LLC, pp. 825-840.
- [63] Amazon Appstore for Android. [online] https://www.amazon.com/mobile-apps/b/ref=topnav_storetab_mas?ie=UTF8&node=2350149011 (Accessed
on 15 August 2016).
- [64] Apple iTunes iPhone App Store. [online]
<https://itunes.apple.com/us/genre/ios/id36?mt=8> (Accessed on 14
September 2016).

- [65] Google Play Android App Store. [online]
<https://play.google.com/store/apps?hl=en> (Accessed on 13 September 2016).
- [66] Rainhard Findling, Muhammad Muaaz, Daniel Hintze and René Mayrhofer. ShakeUnlock: Securely Unlock Mobile Devices by Shaking them Together. In Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, MoMM'14, pp. 165-174.
- [67] Alan Dix, Janet Finlay, Gregory Abowd and Russell Beale. *Human-Computer Interaction*, 3rd ed., Pearson Education Limited, Harlow, England. 2004.
- [68] Stuart Card, Thomas Moran and Allen Newell. *The Psychology of Human-Computer Interaction*, Lawrence Erlbaum Associates, Hillsdale, New Jersey, USA. 2004.
- [69] <http://www.consumerreports.org/cro/fitness-trackers/buying-guide.htm>
accessed on 13Jan2015
- [70] United States Quick Facts. www.census.gov/quickfacts/table/PST045215/00.
Accessed 01 May 2018
- [71] IDC Press Release, Apple Debuts at the Number Two Spot as the Worldwide Wearables Market Grows 223.2% in 2Q15, 27 August 2015, www.idc.com/getdoc.jsp?containerId=prUS25872215
- [72] Pew Research, Tracking for Health, January 28, 2013, www.pewinternet.org/2013/01/28/tracking-for-health/
- [73] Fitbit Staff (2010) The magic of 10,000 steps. <https://blog.fitbit.com/the-magic-of-10000-steps/>. Accessed 01 May 2018

- [74] https://en.wikipedia.org/wiki/Quantified_Self
- [75] J.C. Herz. Wearables Are Totally Failing the People Who Need Them Most, *Wired Magazine*, Conde Nast, November 6, 2014, www.wired.com/2014/11/where-fitness-trackers-fail/.
- [76] Rachel Purta, Stephen Mattingly, Lixing Song, Omar Lizardo, David Hachen, Christian Poellabauer and Aaron Striegel/ Experiences Measuring Sleep and Physical Activity Patterns Across a Large College Cohort with Fitbits, In *Proceedings of the 2016 ACM International Symposium on Wearable Computers*, ISWC'16, pp. 28-35.
- [77] Pew Research Mobile messaging and social media. 2015.
<http://www.pewinternet.org/files/2015/08/Social-Media-Update-2015-FINAL2.pdf>. Accessed 19 August 2015.
- [78] Muhammad Shahzad, Alex Liu and Arjmand Samuel. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. MobiCom'13, pp. 39–50.
- [79] Lingjun Li, Xinxin Zhao and Guoliang Xue. Unobservable re-authentication for smartphones. In *Proceedings of the 20th annual Network & Distributed System Security Symposium*. NDSS'13.
- [80] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou. Privacy-preserving public auditing for data storage security in cloud computing. In 2010 Proceedings IEEE INFOCOM, INFOCOM'10, pp. 1–9.

- [81] Ian. Spiro. Motion chain: a webcam game for crowdsourcing gesture collection. In *CHI'12 Extended Abstracts on Human Factors in Computing Systems*, 2012, pp. 1345–1350.
- [82] Shahrivar Amini and Yang Li. Crowdlearner: rapidly creating mobile recognizers using crowdsourcing. In *Proceedings of the 26th annual ACM symposium on User interface software and technology*. UIST'13, pp. 163–172.
- [83] Yan Huang, Peter Chapman and David Evans. Privacy-preserving applications on smartphones. In *Proceedings of the 6th USENIX conference on Hot topics in security*, HotSec'11, pp. 4-4.
- [84] Lindasalwa Muda, Mumtaj Begam and I. Elamvazuthi. Voice recognition algorithms using mel frequency cepstral coefficient (mfcc) and dynamic time warping (dtw) techniques. *Journal of Computing*, Vol. 2, Iss. 3, March 2010. Cornell University Library arXiv preprint arXiv:1003.4083, 2010.
- [85] Jiayang Liu, Lun Zhong, Jehan Wickramasuriya and Venu Vasudevan, uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing*, Vol. 5, Iss. 6, December 2009, pp. 657-675. ScienceDirect.
- [86] Jian Tian, Chengzhang Qu, Wenyan Xu and Song Wang. Kinwrite: Handwriting-based authentication using kinect. In *Proceedings of the 20th annual Network & Distributed System Security Symposium*. NDSS'13.

- [87] Haohan Zhu, Xianrui Meng and George Kollios. Privacy preserving similarity evaluation of time series data. In 17th International Conference on Extending Database Technology, EDBT'14, pp. 499–510.
- [88] Meinhard Muller. *Information Retrieval for Music and Motion*. Springer Science+Business Media, 2007.
- [89] Ahmad Akl, Chen Feng and Shahrokh Valaee. A novel accelerometer-based gesture recognition system. *IEEE Transactions on Signal Processing*, vol. 59, no. 12, pp. 6197–6205, 2011.
- [90] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology—EUROCRYPT'99*. Springer, 1999, pp. 223–238.
- [91] Michael Rabin. How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive, vol. 2005, p. 187, 2005.
- [92] Moni Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*. SODA'01, pp. 448–457.
- [93] Yuval Ishai, Joe Kilian, Kobbi Nissim and Erez Petrank. Extending oblivious transfers efficiently. In *Advances in Cryptology-CRYPTO 2003*. Springer, 2003, pp. 145–161.
- [94] Gilad Asharov, Yehuda Lindell, Thomas Schneider and Michael Zohner. More efficient oblivious transfer and extensions for faster secure computation. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. CCS'13, pp. 535–548.

- [95] Benny Pinkas, Thomas Schneider and Michael Zohner. Faster private set intersection based on ot extension. In *Proceedings of the 23rd USENIX Security Symposium*, USENIX'14, pp. 797-812.
- [96] Ayman Jarrous and Benny Pinkas. Secure hamming distance based computation and its applications. In *Applied Cryptography and Network Security*, ACNS 2009, pp. 107–124. SpringerLink.
- [97] Julien Bringer, Hervé Chabanne and Alain Patey. Shade: Secure hamming distance computation from oblivious transfer. In *Financial Cryptography and Data Security*, SpringerLink, pp. 164-176, 2013.
- [98] Julien Bringer, Hervé Chabanne, Melanie Favre, Alain Patey, Thomas Schneider and Michael Zohner. Gshade: faster privacy-preserving distance computation and biometric identification. In *Proceedings of the 2nd ACM workshop on Information hiding and multimedia security*. IH&MMSec'14, pp. 187-198.
- [99] Eamonn Keogh, Li Wei, Xiaopeng Xi, Michail Vlachos, Sang-Hee Lee and Pavlos Protopapas. Supporting exact indexing of arbitrarily rotated shapes and periodic time series under euclidean and warping distance measures. *The VLDB Journal*, June 2009, vol. 18, no. 3, pp. 611–630.
- [100] Thanawin Rakthanmanon, Bilson Campana, Abdullah Mueen, Gustavo Batista, Brandon Westover, Qiang Zhu, Jesin Zakaria and Eamonn Keogh. Searching and mining trillions of time series subsequences under dynamic time warping. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD'12, pp. 262–270.

- [101] Bouncy Castle. Bouncy castle Crypto APIs. www.bouncycastle.org last accessed 19July2018.
- [102] Jacob Wobbrock, Andrew Wilson and Yang Li. Gestures without libraries, toolkits or training: a \$1 recognizer for user interface prototypes. In *Proceedings of the 20th annual ACM symposium on User interface software and technology*, UIST'07, pp. 159–168.
- [103] G. A. ten Holt, M. J. Reinders and E. Hendriks. Multi-dimensional dynamic time warping for gesture recognition. In *Proceedings of the Thirteenth annual conference of the Advanced School for Computing and Imaging*, vol. 119. 2007.
- [104] Bastian Hartmann and Norbert Link. Gesture recognition with inertial sensors and optimized dtw prototypes. In *IEEE International Conference on Systems, Man and Cybernetics*, SMC'10, pp. 2102–2109.
- [105] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang and Na Ruan. When CSI meets public WIFI: Inferring your mobile phone password via WIFI signals. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS'16, pp. 1068–1079.
- [106] Gradeigh Clark and Janne Lindqvist. Engineering gesture-based authentication systems. *IEEE Pervasive Computing*, vol. 14, no. 1, pp. 18–25, 2015.
- [107] Sheng Tan and Jie Yang. WiFinger: leveraging commodity wifi for fine-grained finger gesture recognition. In *Proceedings of the 17th ACM*

International Symposium on Mobile Ad Hoc Networking and Computing,
MobiHoc '16, pp. 201–210.

- [108] Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister and Nasir Memon. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI'12, pp. 977–986.
- [109] Jingchao Sun, Rui Zhang, Jinxue Zhang and Yanchao Zhang. TouchIn: Sightless two-factor authentication on multi-touch mobile devices. In *IEEE Conference on Communications and Network Security*, CNS'14, pp. 436–444.
- [110] Ming Li, Ning Cao, Shucheng Yu and Wenjing Lou. FindU: Privacy-preserving personal profile matching in mobile social networks. In *Proceedings of IEEE INFOCOM 2011*, pp. 2435–2443.
- [111] Yan Huang, Lior Malka, David Evans and Jonathan Katz. Efficient privacy-preserving biometric identification. In *Proceedings of the 17th conference Network and Distributed System Security Symposium*, NDSS'11.
- [112] Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt and Tarek Abdelzaher. PDA: Privacy-preserving data aggregation in wireless sensor networks. In *Proceedings of IEEE INFOCOM 2007*, pp. 2045–2053.
- [113] Mikhail Atallah, Florian Kerschbaum and Wenliang Du. Secure and private sequence comparisons. In *Proceedings of the 2003 ACM workshop on Privacy in the electronic society*. WPES'03, pp. 39–44.

- [114] Somesh Jha, Louis Kruger and Vitaly Shmatikov. Towards practical privacy for genomic computation. In *Proceedings of IEEE Symposium on Security and Privacy*, SP'08, pp. 216–230.
- [115] Yan Huang, David Evans, Jonathan Katz and Lior Malka. Faster secure two-party computation using garbled circuits. In *Proceedings of the 20th USENIX conference on Security*. SEC'11 Pages 35-35.
- [116] Donald Berndt and James Clifford. Using Dynamic Time Warping to Find Patterns in Time Series, *AAAI Workshop on Knowledge Discovery in Databases*. KDD'94, pp 229-248.
- [117] Bogdan Pogorelc and Matjaž Gams. Detecting gait-related health problems of the elderly using multidimensional dynamic time warping approach with semantic attributes. *Multimedia Tools and Applications*, September 2013, vol. 66, pp 95-114, SpringerLink.
- [118] Tam Vu, Akash Baid, Simon Gao, Marco Gruteser, Richard Howard, Janne Lindqvist, Predag Spasojevic and Jeffrey Walling, Distinguishing Users with Capacitive Touch Communication, In *Proceedings of the 18th annual international conference on Mobile computing and networking*. Mobicom'12, pp 197-208.
- [119] Xin Zhao, Xue Li, Chaoyi Pang, Xiaofeng Zhu and Quan Sheng. Online human gesture recognition from motion data streams, In *Proceedings of the 21st ACM international conference on Multimedia*. MM'13, pp 23-32.

- [120] Sylvio Barbon, Rodrigo Guido, Shi-Huang Chen, S., Viera, L., and Sanchez, F., Improved Dynamic Time Warping Based on the Discrete Wavelet Transform, ISMW 2007, pp 256-261.
- [121] Muzaffar Bashir and Jürgen Kempf. Reduced Dynamic Time Warping for Handwriting Recognition Based on Multi-dimensional Time Series of a Novel Pen Device, *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 2, no. 9, 2008, pp. 1839-1845.
- [122] Jiaon Zhu, Rubén San-Segundo and José Pardo. Feature extraction for robust physical activity recognition. *Human-Centric Computing and Information Sciences* 2017, vol. 7, no. 1, pp. 1-16.
- [123] Wikipedia entry for Dynamic time warping,
https://en.wikipedia.org/wiki/Dynamic_time_warping, accessed 3 June 2018.
- [124] Stan Salvador and Philip Chan. Toward accurate dynamic time warping in linear time and space. *Intelligent Data Analysis*, vol. 11, no. 5, pp. 561–580, 2007.
- [125] Stephan Spiegel, Brijnesh-Johannes Jain and Sahin Albayrak. Fast time series classification under lucky time warping distance. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing, SAC'14*, pp. 71-78.
- [126] Qiang Zhu, Gustavo Batista, Thanawin Rakthanmanon and Eamonn Keogh. A novel approximation to dynamic time warping allows anytime clustering of

- massive time series datasets. In *Proceedings of the 2012 SIAM International Conference on Data Mining*, SDM'12, pp. 999–1010.
- [127] Diego Silva and Gustavo Batista. Speeding up all-pairwise dynamic time warping matrix calculation, In *Proceedings of the 2016 SIAM International Conference on Data Mining*, SDM'16, pp. 837-845.
- [128] Pew Research. Social media usage: 2005-2015. 2015.
www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.
 Accessed 8 October 2015.
- [129] Tim Bruggen. How Apple Watch can gain wearables market share in 2016. 2016. [www.fool.com/investing/general/2016/01/09/ how-apple-watch-can-gain-wearables-market-share-in.aspx](http://www.fool.com/investing/general/2016/01/09/how-apple-watch-can-gain-wearables-market-share-in.aspx) Accessed 01 May 2018
- [130] Parmy Olson. Wearable tech is plugging into health insurance. 2014. Forbes.
[http://www.forbes.com/sites/parmyolson/2014/06/19/ wearable-tech-health-insurance/#2f3117f918bd](http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#2f3117f918bd). Accessed 01 May 2018
- [131] John Bargh, Katelyn McKenna and Grainne Fitzsimons. Can you see the real me? Activation and expression of the "true self" on the Internet. *Journal of Social Issues*, 58(1):33-48. 2002.
- [132] Joseph Walther. Computer-mediated communication: Impersonal, interpersonal, and hyper personal interaction. *Communication Research*, 23(1):3, 1996.
- [133] Jochen Meyer, Merlin Wasmann, Wilko Heuten, Abdallah El Ali and Susanne Boll S. Identification and classification of usage patterns in long-term activity

- tracking. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, CHI'17, pp 667-678.
- [134] Lie Tang and Judy Kay. Harnessing long term physical activity data – how long-term trackers use data and how an adherence-based interface supports new insights. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, IMWUT, 1(2):26. 2017.
- [135] Mary Berglund, Julia Duvall and Lucy Dunne. A survey of the historical scope and current trends of wearable technology applications. In *Proceedings of the 2016 ACM International Symposium on Wearable Computers*, ISWC'16, pp. 40-43.
- [136] Hayeon Jeong, HeePyung Kim, Rihun Kim, Uichin Lee and Yong Jeong. Smartwatch wearing behavior analysis: a longitudinal study. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, IMWUT, 1(3):60. 2017
- [137] Pew Research. Social media fact sheet. 2018.
<http://www.pewinternet.org/fact-sheet/social-media>. Accessed 01May 2018
- [138] Least Squares. <https://en.wikipedia.org/wiki/Least+squares>. Accessed 01 May 2018.
- [139] 10,000 steps a day. www.thewalkingsite.com/10000steps.html. Accessed 01 May 2018
- [140] Vivian Motti and Kelly Caine. Smart wearables or dumb wearables? Understanding how context impacts the UX in wrist worn interaction. In

Proceedings of the 34th ACM international conference on the design of communication, SIGDOC'16, Art No 10.

[141] <https://en.wikipedia.org/wiki/Efficiency>

[142] <https://en.wikipedia.org/wiki/Security>

[143] Hiroaki Sakoe and Seibi Chiba. Dynamic programming optimization for spoken word recognition. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, Vol. ASSP-26. 1978

[144] Fumitada Itakura. Minimum prediction residual principle applied to speech recognition, *IEEE Transactions on Acoustics, Speech and Signal Processing*, Vol. ASSP-23(1), pp. 67-72. 1975.

[145] Eamonn Keogh and Chotirat Ratanamahatana. Exact indexing of dynamic time warping, *Knowledge and Information Systems*. March 2005, 7(3), pp. 358-386. SpringerLink.

[146] Stan Salvador and Philip Chan. FastDTW:Toward accurate dynamic time warping in linear time and space. *Intelligent Data Analysis*, vol. 11, no. 5, pp. 561-580, 2007.

[147] Eamonn Keogh and Michael Pazzani. Scaling up dynamic time warping for datamining applications, In *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD'00, pp. 285-289.

[148] Eamonn Keogh, Kaushik Chakrabarti, Michael Pazzani and Sharad Mehrotra. Locally adaptive dimensionality reduction for indexing large time

- series databases, In *Proceedings of the 2001 ACM SIGMOD international conference on Management of data*, SIGMOD'01, pp. 151-162.
- [149] Ghazi Al-Naymat, Sanjay Chawla and Javid Taheri. SparseDTW: A novel approach to speed up dynamic time warping, In *Proceedings of the 8th Australasian Data Mining Conference*, AusDM'09, vol. 101, pp. 117-127.
- [150] Aftab Khan, Nils Hammerla, Sebastian Mellor and Thomas Plötz. Optimising sampling rates for accelerometer-based human activity recognition. *Pattern Recognition Letters*, vol. 73, no. 1, April 2016, pp. 33-40.
- [151] Marc Dupont and Pierre-Francois Marteau. Coarse-DTW: Exploiting Sparsity in Gesture Time Series, *Proceedings 1st International Workshop on Advanced Analytics and Learning on Temporal Data*, AALTD 2015.
- [152] Ilaria Barolini, Paolo Ciaccia and Marco Patella. WARP: Accurate Retrieval of Shapes Using Phase of Fourier Descriptors and Time Warping Distance, *IEEE Transactions On Pattern Analysis and Machine Intelligence*, vol. 27, iss. 1, January 2005, pp. 142 – 147.
- [153] Paolo Capitani and Paolo Ciaccia. Efficiently and Accurately Comparing Real-valued Data Streams, 13th Italian National Conference on Advanced Data Base Systems. SEBD'05, 2005.
- [154] https://en.wikipedia.org/wiki/Dynamic_time_warping
- [155] https://en.wikipedia.org/wiki/Nyquist_Shannon_sampling_theorem
- [156] Andrew Callaway, Jon Cobb and Ian Jones. A comparison of video and accelerometer based approaches applied to performance monitoring in

swimming. *International Journal of Sports Science & Coaching*, vol. 4, iss. 1, pp. 139-153, 2009

- [157] Neil Davey, Megan Anderson and Daniel James. Validation trial of an accelerometer-based sensor platform for swimming, *Sports Technology*. Vol. 1, Issue 4-5, pp. 202-207, 2008.