NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE WIRELESS UBIQUITOUS SURVEILLANCE TESTBED

by

LeRoy P. Dennis III

and

Michael K. Ford

March 2003

Thesis Advisor:	Alex Bordetsky
Second Reader:	Randy J. Hess

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: The Wireless Ubiquitous Surveillance Testbed **6. AUTHOR(S)** LeRoy P. Dennis III and Michael K. Ford	**5. FUNDING NUMBERS** **$95,000**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Homeland Security	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

This thesis research examines the emergence of surveillance and biometrics technologies as a sensible baseline for building a ubiquitous surveillance testbed for the Naval Postgraduate School. This thesis also defines what ubiquitous surveillance is, employs biometric applications and technical strategies to build a working testbed, and addresses developmental issues surrounding the hypothesis for a ubiquitous surveillance testbed. The authors conducted several evaluations of the testbed using different scenarios and recommend emerging biometric and surveillance technologies to promote the maturation of the testbed into a premier ubiquitous habitat.

14. SUBJECT TERMS Testbed, Surveillance, Biometrics Technologies, Ubiquitous Surveillance, Wireless, Senor Technology	**15. NUMBER OF PAGES** 126
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE WIRELESS UBIQUITOUS SURVEILLANCE TESTBED

LeRoy P. Dennis III
Lieutenant, United States Navy
B.S., United States Naval Academy, 1997

Michael K. Ford
Lieutenant, United States Navy
B.S., University of Southwestern Louisiana, 1982

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2003

Authors: LeRoy P. Dennis III

Michael K. Ford

Approved by: Alex Bordetsky
Thesis Advisor

Randy J. Hess
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The thesis research examines the emergence of surveillance and biometrics technologies as a sensible baseline for building a ubiquitous surveillance testbed for the Naval Postgraduate School. This thesis also defines what ubiquitous surveillance is, employs biometric applications and technical strategies to build a working testbed, and addresses developmental issues surrounding the hypothesis for a ubiquitous surveillance testbed. The authors conduct several evaluations of the testbed in using different scenarios. We recommend emerging biometric and surveillance technologies can promote the maturation of the testbed into a premier ubiquitous habitat.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to acknowledge and thank the following people and organizations:

My wife, Henretta Dennis, for her unwavering support during my academic endeavors at the Naval Postgraduate School. The thousands of hours of reading, writing, studying and research during this 18 month experience was made easier by her love and understanding. I could not have done it without you.

To my Mother, Jessie Mae Young, my son, Michael K. Ford Jr., and my daughter, Sandrelle V. Ford, for their continued support and understanding.

To our Thesis Advisor, Professor Alex Bordetsky, for his enthusiastic support during the development of the Testbed.

To our Associate Thesis Advisor, Randy Hess, for his methodical and comprehensive reviews from the proposal to the final version. His guidance and analytical appraisal throughout the entire thesis effort helped make our thesis a more rewarding learning experience.

To Nancy Sharrock for ensuring that our chapters were always in the proper format.

To Jason Close for all of his insight on managing the operation of the ID-2000 software.

To the staff of the Dudley Knox Library for their support in research assistance and literature resource.

To all the staff at the Naval Postgraduate School, thank you for the honor and privilege to attend this prestigious and historic academic institution.

I. INTRODUCTION

A. BACKGROUND

The thesis research examines existing and emerging surveillance and biometrics technologies as a pragmatic baseline supporting a proposed concept testbed for a national ubiquitous surveillance and biometrics system. LCDR Richard Makarski and LT Jose Marrero explored a broad range of surveillance and biometric technologies for improving homeland security in their thesis entitled "A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security."[1] Their thesis scrutinized surveillance/biometric techniques, strategies, and prevailing present day applications. It contrasted the evolving requirements for improved security with sensitivity toward society's need for balanced consideration on civil liberties and privacy. Major Brandon Johnson USMC also helped conduct experiments on the network management side of the project.

The primary emphasis of this thesis is on developing a testbed and using it for limited experiments as they apply to homeland security. The goals are to develop an advanced experimental environment, laboratories, and operational experiments for training civil and military units in integrating and operating collaborative sensor-decision maker environments that are critical for Homeland Security (HLS). For example, the Journal of Homeland Security states, "For terrorist events in general, modern and robust communications systems will play a key role in successful consequence management."[2] Also, "The innovative use of collaborative planning techniques to foster 'Net-Centric Warfare' could well be applied to the various elements involved in Homeland Defense."[3] The studies of such data sharing and communication environments have just started. The commercial-off-the-shelf (COTS) collaborative networking platforms enabling interagency data sharing, emergency site management, and ubiquitous surveillance have yet to be developed. There is also a recognized lack of expertise among the civil and

[1] (Makarski, Richard E. and Marrero, Jose A., "A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security", Master's Thesis, Naval Postgraduate School, September 2002.

[2] The Journal of Homeland Security, December 10, 2002, p. 5.

[3] The Journal of Homeland Security, October 26, 2001, p. 21.

military personnel in handling such mission critical mobile collaborative environments. This means that training and experimentation would be critical for bridging the gap between the emerging collaborative grid and human expertise.

B. PURPOSE

This thesis focuses on the development of the Ubiquitous Surveillance Testbed (UbiSurv) utilizing a wireless network, multi-layered sensors and situational awareness tools and applications. The testbed will be in a secure location and available for data analysis, decision maker support, and follow-on study. The testbed ultimately serves as a tool for surveillance data analysis, wireless network integration, a facility for exploring a ubiquitous habitat, and decision maker implementation of the Global Information Grid as it applies to homeland security.

C. RESEARCH TASKS

The main goals of this thesis are to:

- Set up the biometric sensors and facial recognition surveillance environment.
- Set up collaboration and data sharing environment across the ubiquitous surveillance network.
- Enable peer-to-peer collaboration, collaborative data mining and information fusion with HLS agencies.
- Coordinate identity and profile checking with legacy systems and HLS agencies via agent wrappers, facilitators, and other elements of the intelligent agent grid.

D. SCOPE OF THESIS

Ubiquitous surveillance holds promise for the strategy of Homeland Security. If one cannot control the actions of others, one can at least monitor them and be prepared to respond with intelligent and deliberate countermeasures. The idea of "ubiquitous surveillance comes from the concept of ubiquitous computing—a term coined by the father of Ubiquitous Computing, Dr. Mark Weiser."[4] The term "ubiquitous" means being or seeming to be everywhere at the same time. Ubiquitous surveillance can alert

[4] W eiser, Mark Dr., Xerox Palo Alto Research Center (PARC), 2001, Available Online, [http://www.parc.xerox.com/parcgo.html], ubiq.com, September 2001.

authorities to take corrective actions, capture a perpetrator, intercept a disaster in the making, and save lives.

We want to build a wireless ubiquitous surveillance testbed that is so pervasive and efficient that the subjects will be unaware that they are being watched, screened, observed, or protected. The key to success in the ubiquitous surveillance testbed is that the sensing and data collection technology is complementary to everyday life and unobtrusive to human daily activities. Currently there are no available networks at the Naval Postgraduate School to perform the functions of the proposed test bed.

This thesis will feature a wireless ubiquitous surveillance network testbed utilizing multi-layered sensors and multiple intelligent agents. The testbed will be in a secure location and be available for data analysis, decision maker support, and follow on study. The testbed ultimately serves as a tool for surveillance data analysis, wireless network integration, a facility for exploring a ubiquitous habitat, and decision maker implementation of the Global Information Grid as it applies to homeland security.

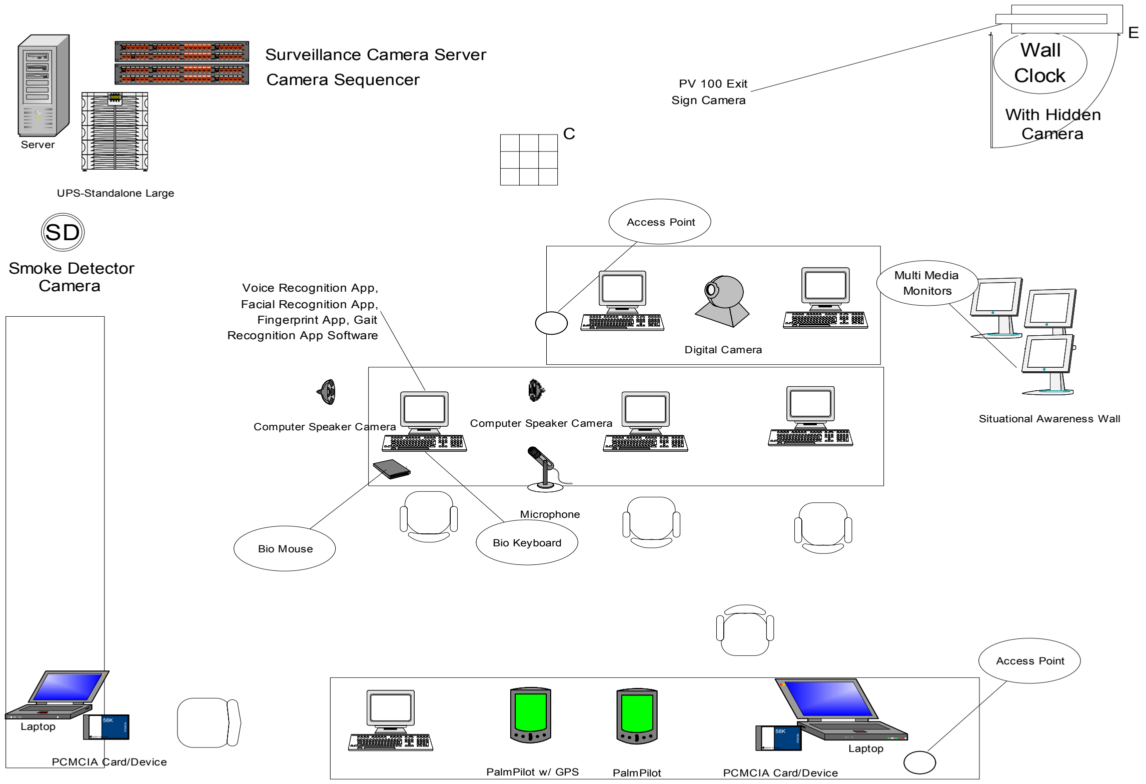


Figure 1.1. The Building Blocks of the Ubiquitous Surveillance Testbed.

The UbiSurv will utilize biometric sensors. The biometric sensors that will be researched are facial, fingerprint, iris, voice and gait recognition. The testbed is installed in the Giga Laboratory in Root Hall at the Naval Postgraduate School with plans to expand campus wide in follow-on projects in this or related fields. The intended use of the finished product is to serve as a testbed to provide Naval Postgraduate School and Department of Defense students' in-depth training on the latest Biometric Ubiquitous Surveillance Network.

The concept of the UbiSurv is to utilize surveillance equipment and biometric technologies embedded in a wireless network. Our thesis research will explore different methods of providing access control and surveillance via a multi-modal system, list the capabilities and limitations of each, and provide reasons for the selected products. Other questions we intend to answer during our research are:

- What defines a ubiquitous environment?
- How viable are current Biometrics?
- What facial recognition techniques best suit Ubiquitous Surveillance?
- What is the security problem associated with different types of sensors and the wireless network?
- What kind of environment optimizes the decision maker and Ubiquitous Surveillance system?

E. METHODOLOGY

The methodology to be used in this thesis research will consists of the following:

- Performing literary reviews of books, magazines, newspapers, and Internet sources that are pertinent to access control and surveillance utilizing biometric sensors and wireless networks
- Examine emerging Department of Defense concepts of Global Information Grid/Force Net, NICCI Habitat, CoAB and how to link the testbed into these initiatives
- Visiting sites with preexisting biometric surveillance systems
- Examining capabilities and limitations of the different testbed products, both, software and hardware
- Selecting the most compatible products to build the testbed
- Building and testing the testbed

- Examine wireless capabilities and limitations

F. ORGANIZATION OF STUDY

- Chapter II discusses the definition of an Ubiquitous Surveillance Habitat and the purpose of the UbiSurv
- Chapter III discusses various biometrics technologies and sensor rich environments. A thorough examination of physiological, behavioral, and various emerging biometrics technologies
- Chapter IV discusses wireless LAN standards, security issues and work environment suitable for wireless networks
- Chapter V provides an in-depth analysis, comparison of expected and actual results, lessons learned and possible upgrades.
- Chapter VI is the summary of the thesis research, recommendations and follow-on thesis topics.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE UBIQUITOUS SURVEILLANCE SYSTEM

A. DEFINITION OF UBIQUITOUS SURVEILLANCE

An ubiquitous surveillance system can be comprised of a network of sensors that can detect personal activity, chemical, biological, and nuclear agents; seismic activity, radar, IR, electro-optical, acoustic, etc. "These sensors are connected to a node (notionally a computer, but perhaps in the future a purpose built device) and collectively they monitor a particular, limited geographic area."[5] Projects such as Smart Dust introduce the concept of self organizing wireless sensor networks. Smart Dust is designed to filter out raw data and relay pertinent information. TinyOS, TinyDB, and Tiny application software is used to facilitate a self organizing network. TinyOS is the framework for building up the operation system capabilities needed for the sensor network-the networking capabilities, localization and support for applications. TinyDB then aggregates the data at the next layer up.

In a deployed scenario, there would likely be multiple nodes (network elements), covering multiple limited geographic areas, feeding into a central monitoring and/or command environment (Ubiquitous Surveillance Network Operations Center [USNOC]). For example a ubiquitous surveillance system could be set up on the battlefield to enable soldiers to see around corners, sense the threat of chemical and biological weapons. The majority of these sensors will use organizational organic equipment as their interface, management, and integrity would need to be guaranteed. This would not preclude the inclusion of potentially trusted second party sensors as long as their status as such was known (e.g. tying in to allied forces camera network).

In order for a system or network to be defined as a Ubiquitous habitat in the works of Kris Pister, the CEO head of Robotics at the University of California, Berkeley, it must meet the following characteristics:

- "pervasive—it must be everywhere, with every portal reaching into the same information base
- embedded—it must live in our world, sensing and affecting it

[5] Johnson, R. Collin, Advanced Technology, "Companies Test Prototype Wireless-Sensor Nets", January 29, 2003, Available Online, [http://www.eet.com/at/news/OEG20030128S0028].

- nomadic—it must allow users and computations to move around freely, according to their needs
- adaptable—it must provide flexibility and spontaneity, in response to changes in user requirements and operating conditions
- powerful, yet efficient—it must free itself from constraints imposed by bounded hardware resources, addressing instead system constraints imposed by user demands and available power or communication bandwidth
- intentional—it must enable people to name services and software objects by intent, for example, "the nearest printer," as opposed to by address
- eternal—it must never shut down or reboot; components may come and go in response to demand, errors, and upgrades"[6]

B. OTHER UBIQUITOUS ENVIRONMENTS

Researchers at MIT are currently working on a ubiquitous environment called Project Oxygen. The goal of Project Oxygen is to replace the PC with ubiquitous-often invisible-computing machines. Project Oxygen integrates different technologies into its system in its effort to pursue its pervasiveness. One of those technologies is Cricket which provides information about location, orientation, and geographic spaces. It works indoors, where access to GPS satellites is unavailable and electronic equipment may interfere with traditional magnetic compasses. Cricket beacons, mounted on walls or ceilings, transmit ultrasound and RF signals; compact listeners, attached to mobile or static devices, use the difference in signal arrival times to determine where they are. Cricket allows users and applications to discover their locations without tracking them; its operation and administration are completely decentralized.

Project Oxygen also uses multimodal systems to enhance vision and voice recognition. The Speech Builder utility supports development of spoken interfaces. Person tracking, face, gaze, and gesture recognition utilities support development of visual interfaces.

> Systems that understand sketching on whiteboards provide more natural real-time object tracker uses range and appearance information from a stereo camera to recover an object's 3D rotation and translation. When

[6] Johnson, R. Collin, Advanced Technology, "Companies Test Prototype Wireless-Sensor Nets", January 29, 2003, Available Online, [http://www.eet.com/at/news/OEG20030128S0028].

> connected to a face detector, the system accurately tracks head positions, thereby enabling applications to perceive where people are looking.[7]

Project Oxygen also uses a person-tracking system consisting of stereo, camera and a computer. The cameras are arranged to view an entire room and continually estimate 3D-point clouds of the objects in the room. The system clusters foreground points into blobs that represent people, from which it can extract features such as a person's location and posture. "Synthetic profiles are used to recognize people by their gait. In constraint-free environments, where users move freely, this kind of view-independent identification is crucial because no particular pose of a user can be presumed."[8]

C. SUMMARY OF CHAPTER

The UbiSurv could benefit by implementing Smart Dust and the person-tracking systems from Project Oxygen. What makes the UbiSurv unique is its implementation of Biometrics. Biometrics makes the UbiSurv nomadic, embedded, pervasive, and adaptable. The first biometric application to be installed in the UbiSurv is facial recognition utilizing the ID-2000 facial recognition software application. Other biometric applications such as fingerprinting, gait recognition, iris and retina scan can also be installed in the future. Future advancements of the testbed also involved combining biometric applications with various systems and ubiquitous habitat.

[7] Brown, Eric S., An MIT Enter5prise Technology Review, "Project Oxygen's New Wind"' December 20, 2001, Available Online, [http.www.technologyreview.com/articles/wo_brown122001.asp].

[8] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INCORPORATING BIOMETRICS IN A UBIQUITOUS NETWORK

The use of biometrics has been around for a little over 20 years and has recently experienced a remarkable increase in popularity and employment as a result of the attack of the World Trade Center Towers and the Pentagon, September 11, 2001 and the beginning of the War on Terrorism. The choice of using biometrics in the UbiSurv was simple. It is due in part to the fact that biometric technological advances have increased tremendously and have proven beneficial. The use of biometrics affords the opportunity to eliminate passwords, personal identification numbers and combinations. The type of UbiSurv we are designing drives us towards biometrics. The challenge that we currently face is how to make the UbiSurv as unobtrusive to users as possible. The use of biometrics will assist tremendously towards that effort.

Biometrics is defined as 'the science of using digital technology to identify individuals based on the individual's unique physical and biological qualities.'[9] Although there are many different aspects of biometrics, "biometrics is basically divided into two classifications: physical and behavioral."[10] After carefully examining the different biometric sensors we will examine the different products available, select the biometric sensors to be implemented into the UbiSurv network, and elaborate on the inherent security and privacy issues of using biometrics for identification and surveillance purposes.

A. THE GROWING USE OF BIOMETRICS

For over 20 years, the use of biometrics have been basically confined to the Department of Defense (federal and state), the military and law enforcement agencies. The most prevalent use of biometrics in the earlier days was limited to fingerprinting. The primary use of fingerprinting for law enforcement was a way of identifying a convicted criminal, whereas the military and government agencies used fingerprinting as a method of checking or granting security clearances to personnel. The only other use of

[9] Page, Douglas, High Technology Careers Magazine, Feature Presentation, "Biometrics: Facing Down the Identity Crisis". Available Online, [http//www.hightechcareers.com/doc198/biometrics198.html], August 28, 2002.

[10] Ibid.

biometrics was that normally found on the big screens where the technological advances of biometrics were brought to the forefront.

Today, the use of biometrics has grown tremendously, especially since 9/11, from the previously mentioned agencies to include big business and industries. It is no longer confined to basic fingerprinting. The use of biometrics has shifted from basic fingerprinting to methods of access control, identification, verification, authentication and surveillance. The following list provides you with a better picture of some organizations using biometrics:

- "The County of Los Angeles has implemented a system for all criminal justice agencies
- The United States Department of Justice, implementing a biometric system using hand-geometry in all federal prisons
- The 1996 World Olympics in Atlanta used hand-geometry as a mean of checking and tracking the athletes."[11]
- The Connecticut Department of Social Services has implemented a biometric system in the public school system used by students receiving lunch
- The one receiving the most notoriety was the ubiquitous system installed for the NFL "Super bowl XXXV in Tampa, Florida. The system was used to survey the crowd for known or suspected terrorists."[12]
- Automobile dealerships are installing ubiquitous systems in their Finance and Insurance offices to monitor or survey the transactions of car buyers while in the process of signing their final contracts. This method tends to eliminate or be able to identify fraudulent activities.

> Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening our national borders, in travel documents, visas and in preventing ID theft. Congressional offices and different Government agencies are addressing the important role that biometrics will play in identifying and verifying the identity of individuals and protecting national assets.[13]

[11] Page, Douglas, High Tech Careers Magazine, Feature Presentation, "Biometrics: Facing Down the Identity Crisis," Available Online [http://www.highcareers.com/doc198/biometrics198.html], August 28, 2002.

[12] Woodard, Jr., John D., Super Bowl Surveillance, "Facing Up to Biometrics "Rand, Arroyo Center, October 2001.

[13] The Biometric Resource Center Website, "Legislation", Available Online, [http://www.itl.nist.gov/div895/biometrics/legislation.html], downloaded August 28, 2002.

B. CLASSIFICATIONS OF BIOMETRICS

1. Physiological

Physiological biometrics involve the physical characteristics of an individual that includes facial features, hand-geometry, eye patterns (to include iris and retinal), and fingerprint. The fingerprint is the biometric feature that is most widely used; however, growing emphasis is placed on the use of facial recognition and eye patterns.

a. Fingerprint

The art of fingerprinting individuals as a means of identification has been used by law enforcement agencies, to include local, state and federal, for nearly a century. Law enforcement agencies fingerprinted individuals when arrested on misdemeanor or felony crimes. When arrested it was mandatory to take the fingerprints of all 10 fingers. What started out as a totally manual task has now emerged as a sophisticated and semi-automated process.

Fingerprints were taken using inkpads. The fingerprints were placed on a fingerprint card, read or compared with the naked eye or with the assistance of a magnified glass then stored in a file for safekeeping and later retrieval. As time passed and technological advances have been made the fingerprinting process has also changed.

The templates are still taken using inkpads and now, the more technically advanced digitally scanned templates. Regardless of the technique utilized, the ability to quickly retrieve the data and match the prints to the subjects have tremendously improved. The process of identifying fingerprints takes the following techniques into considerations: Minutae-based and Correlation-based.

- “A fingerprint match or determination using the Minutae-based technique first find Minutae points and then map their relative placement on the finger
- Correlation-based techniques require the precise location of a registration point and are affected by image translation”[14]

Figure 3.1 depicts a typical fingerprint, fingerprints with Minutae and the comparison of Minutae points between two fingerprints.

[14] Fingerprint Identification, Available Online, [http://biometrics.csu.edu/fingerprint.html], March 16, 2003.

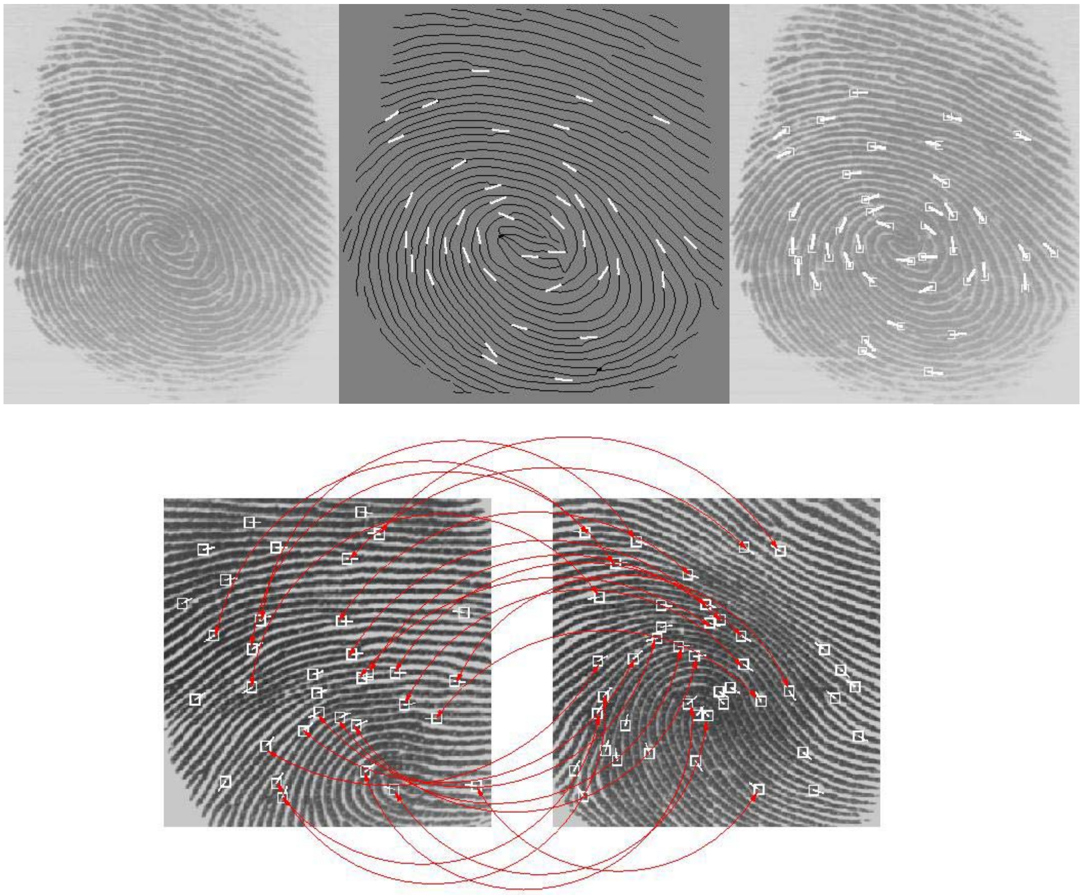


Figure 3.1. Depicts Basic Fingerprints, Fingerprints with Visible and the Comparison of Minutae (From: Two Different Prints. Fingerprint Identification, Available Online, [http://biometrics.csu.edu/fingerprint.html], March 16, 2003).

Some of the disadvantages of using fingerprints to positively identify a subject are that just as technology is forever changing so as the techniques of the criminals. Criminals have been known to use leather gloves, plastic gloves, just enough material to cover the prints and on occasions other prints. "Minutae-based techniques are difficult to extract points from low level quality. The correlation-based technique requires the precise location of a registration point and are affected by image translation and rotation."[15]

The fingerprint technology will benefit the UbiSurv because it requires a very small sample size or database and the user is affected only one time, for the initial

[15] Fingerprint Identification, Available Online, [http://biometrics.csu.edu/fingerprint.html], March 16, 2003.

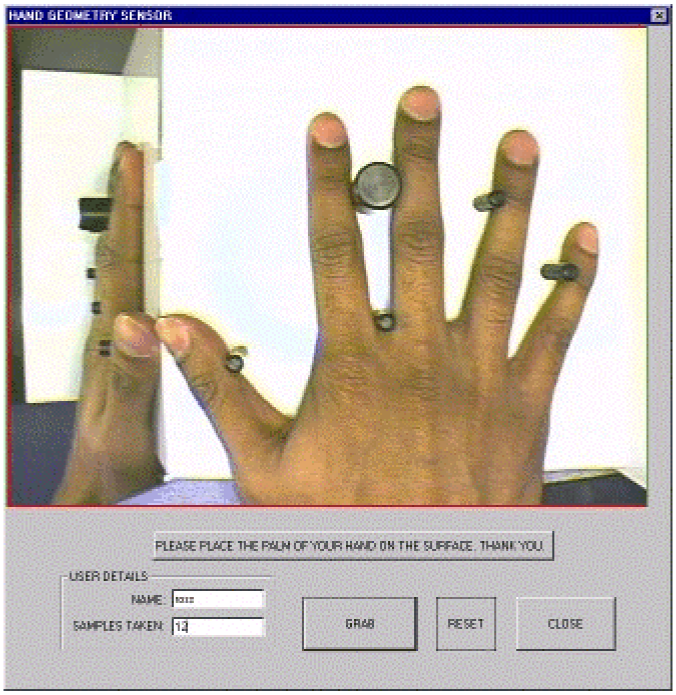
enrollment. Adding fingerprint technology would result in a multi-modal testbed and could be used as a means of access control.

b. Hand Geometry

The art of identifying individuals by hand geometry predates the use of fingerprints by many years. Identification via the hand posed different problems than fingerprinting because it is not as exact as fingerprinting, therefore, the actual term should be verification rather than identification. An individual's identity is verified from the geometric characteristics of the hand, the size, width, and thickness. Additionally, hand geometric measurements include the length and contour or curvature of the fingers.

The use of identifying individuals biometrically through hand geometry has grown significantly. Most hand geometry identification measures have been implemented as a means to grant access control and to keep track or monitor the movement of individuals. A hand geometry security device was implemented in the 1996 World Olympics in Atlanta, GA in order to keep track of the athletes. Airports around the world and federal prisons have begun using hand geometry biometrics in their security system as a means of access control and surveillance.

There are several hand geometry measuring devices that offer outstanding products that could be tailored to meet the needs. Some of the leading vendors in Hand Geometry are Recognition Systems, Inc., Prevent and Dermalog. Of the three vendors Recognition Systems is the worldwide leader in access control, time and attendance and personal identification. Hand Geometry is advantageous due to the fact that implementation of a hand geometry security system is easy and requires approximately 30 seconds of an individual's time to receive and archive an accurate template. Additionally, Hand Geometry is the number one selling biometric product in terms of access control and time and attendance markets, capturing 46% of the market. Figure 3.2 illustrates the ease with which a template can be taken using the image acquisition system by placing the hand firmly on the flat surface comprising a mirror, camera and a lighting intensity control with five pegs. Figure 3.3 illustrates dimensions that are extracted, the width and length, at various points on the hand that are taken into consideration when determining the verification of individuals.



PLEASE PLACE THE PALM OF YOUR HAND ON THE SURFACE. THANK YOU.

USER DETAILS

NAME: xxx

SAMPLES TAKEN: 12

Figure 3.2. Capturing Hand Images. A Hand Geometry – Based Verification System, (From: "Capturing Hand Images and Extracting Features," Available Online, [http://biometrics.cse.msu.edu/hand_proto.html], August 30, 2002).

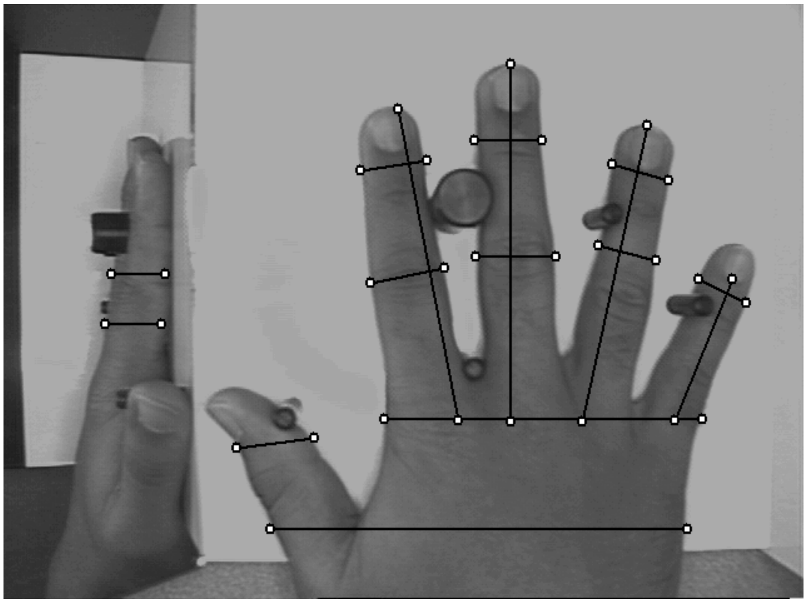


Figure 3.3. Extracting Features. A Hand Geometry – Based Verification System, (From: "Capturing Hand Images and Extracting Features," Available Online, [http://biometrics.cse.msu.edu/hand_proto.html], August 30, 2002).

Although, the geometric features of the hand do not undergo a significant change over time it is not an exact science, therefore, only able to use for verification purposes only. Additionally, the use of hand geometry does not infringe upon the privacy rights of individuals such as fingerprints. The best method for using the hand geometry biometric feature is when used in the multi-modal sense. In order to use for identification purposes hand geometry should be incorporated with fingerprints or facial recognition.

The goal for this biometric feature in the UbiSurv is to eventually manage access control in the Giga Lab and serve as a multi modal feature with facial recognition for positive identification.

c. Eye Patterns

Of all physiological biometric features used for identification purposes, the eye patterns, retina and iris are by far the most accurate and most reliable. This holds true because certain aspects of the eye patterns are formed early and remain basically unchanged throughout a person's life. Figure 3.4 illustrates a depiction of the composition of the iris and retina.

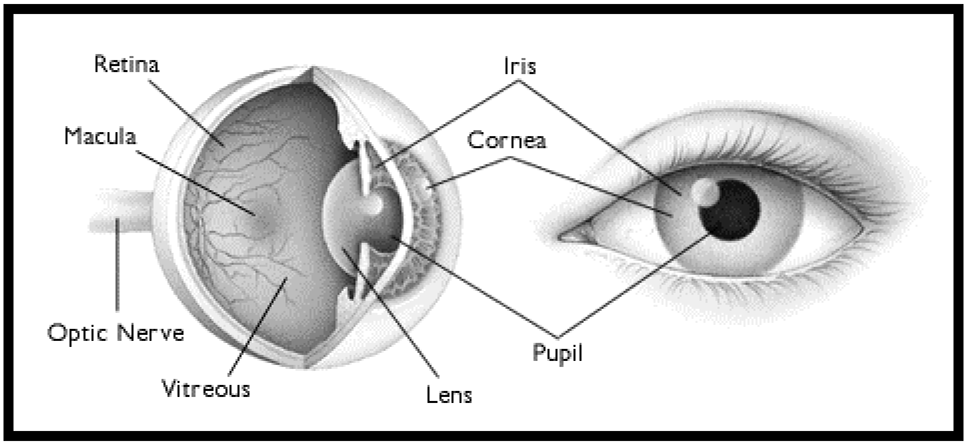


Figure 3.4. Composition of Retina and Iris, (From: Retina Scan Technology, Available Online, [http://www.retina-scan.com/retina_scan_technology.htm], October 28, 2002).

Although eye pattern is the most reliable and accurate biometric means of identification, it is considered the most intrusive to individuals. The retina is comprised of eccentric network of blood vessels located at the rear of the eyeball and has been identified in the early 1930's as being a unique identifier of an individual. One of the primary functions of the retina is to regulate the amount of light that enters the eye. Although formulated prior to birth, first hand experience proved that the vessels change slightly over time. “With the exception of some types of degenerative eye diseases, or cases of severe head trauma, retinal patterns are stable enough to be used throughout one's life.”[16]

One of the primary reasons that the iris is an outstanding form of biometric identification is that the iris is continuously exposed to surveillance systems. A good recognition system could be as far as three feet from the subject and can render a positive match. Of the eye patterns, the retina and iris, a part of the iris called the trabecular meshwork is formed during the eight month of gestation and remains virtually unchanged throughout the life of an individual. Another reason iris recognition is preferred is due in part that the eye is constantly exposed to the public. The composition of the eye are: trabecular meshwork, rings, furrows, freckles and the corona. As in the fingerprint, the exposed visual aspects of the iris are needed in order to form a template or an IrisCode. Figure 3.5 depicts an individual IrisCode. Additionally, the accuracy of the iris recognition system far surpasses that of the retina and fingerprint. Thus, it sets the benchmark for all biometric identification systems to emulate.

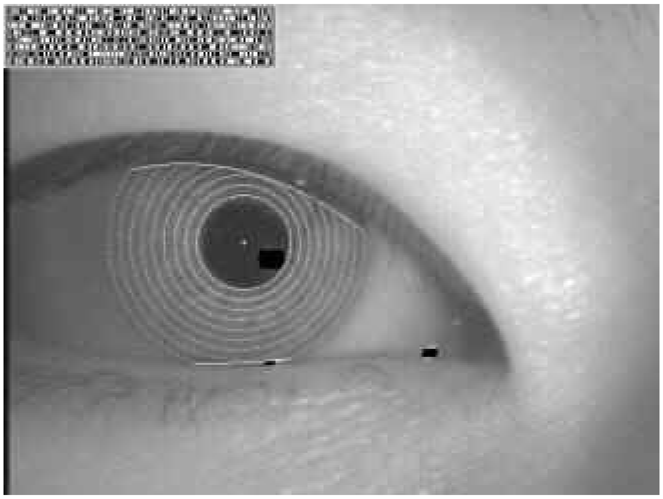


Figure 3.5. IrisCode. Nanavati, Samir, Thieme, Michael, (From: “Biometrics: Identity Verification in a Networked World,” John Wiley and Sons, Inc., U.S.A., 2002).

The accuracy of the iris recognition system far surpasses that of any other biometric systems to the point that it has the capability to distinguish the difference

[16] Retina Scan Technology, Available Online, [http://www.retina-scan.com/retina_scan_technology.htm], October 28, 2002.

between identical twins. "No two irises are alike. In fact, the iris is said to be more individual than a fingerprint. According to the patent holder and manufacturer, IriScan of Mt. Laurel, New Jersey, no other biometric technology can rival the combined attributes of mathematical certainty and non-intrusive operation offered by iris recognition. The probability that any two irises could produce the same pattern is one in 10 to the 78th power--the entire population of the earth is roughly 5.8 billion."[17]

The primary disadvantage of the eye pattern is that it is not unobtrusive to the subjects. It requires a cooperative subject and is easily hampered by donning a pair of dark sunglasses.

d. Facial Recognition

Facial Recognition is often considered the biometric system receiving the greatest acceptance from the general public and is clearly ubiquitous in nature. The need for government, private and public organizations, as well as private citizens to protect their homeland, property and most importantly their families and American citizens, justifies a growing need for facial recognition systems as a means of access control and surveillance. Facial recognition systems compares and individual's features and the geometric measurements between them.

As a result of 9/11, facial recognition systems are becoming omnipresent primarily because of an ease of installation, the increased terrorist threats to homeland security, and its unobtrusiveness to individuals. The installation of this type of system is relatively inexpensive in comparison to other types of recognition systems and considered a reliable means of identification. The growing acceptance to the facial recognition system can be attributed to the fact that it requires minimal interaction between the system and the public.

The process of starting a facial recognition system for access control and surveillance requires a photograph and the implementation of a facial recognition system database. There are many vendors of facial recognition products. One of the more popular products is FaceIt, manufactured by Visionics Corp., Minneapolis. FaceIt was

[17] Page, Douglas, High Tech Careers Magazine, Feature Presentation, "The Eyes Have It," Available Online [http://www.highcareers.com/doc198/biometrics198.html], August 28, 2002.

implemented in a “Malaysian airport security firm to develop the world’s first biometrics-based airline passenger and baggage security system. The system will use face recognition technology and other biometric measurements to ensure only ‘true’ passengers are allowed to enter departure lounges and to board aircraft.”[18] Figure 3.6 depicts FaceIt surveillance images, digital images stored in a database and process of determining a match.

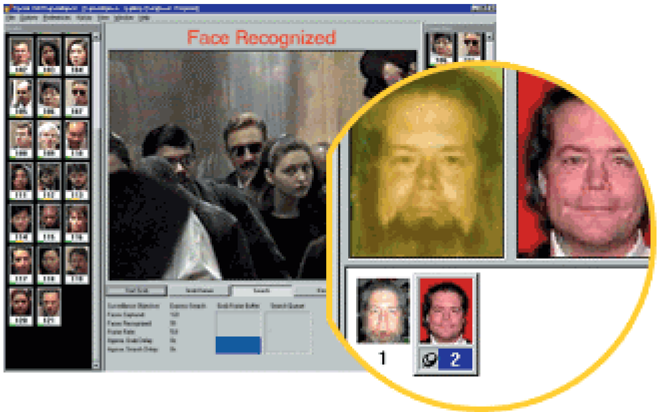


Figure 3.6. FaceIt Image Product. Identix, Empowering Identification, (From: “Facial Surveillance,” Available Online, [http://www.identix.com/products/pro_faceit.html], October 26, 2002).

Technological advances and a determined effort to curtail terrorist activities have yielded outstanding facial recognition systems. There is a system developed for the “University of Southern California, called Eidos”[19] that boasts the ability to identify a person by facial features just as accurately as using the human eye, retina and iris. Additionally, although very few, capturing facial features using 3-dimensional products are emerging. AcSys Face Recognition system produces a 3-dimensional product involved with Holographic Neural Technology (HneT). Neurodynamics has produced such a product, called Tridentity. Tridentity is less restrictive on individuals’ movement and compares not only facial features and geometric distances between them it also takes the bone structure into consideration to determine identification. Figure 3.7 depicts a Tridentity image. “Tridentity offers major advantages

[18] Page, Douglas, High Technology Careers Magazine, Feature Presentation, “Biometrics: Facing Down the Identity Crisis”, p. 5, [http://www.hightechcareers.com/doc198/biometrics198.html.], October 9, 2002.

[19] Ibid. p. 4.

over the two-dimensional approach. Using patterned light to create a full three-dimensional image of the face, Tridentity is able to analyze more subtle features of the face, such as the bone structure around the eyes and nose. In addition, since the information is a true three-dimensional representation of the face, it can be rotated so that it is facing the camera, even if the subject wasn't at the time the image was captured."[20]

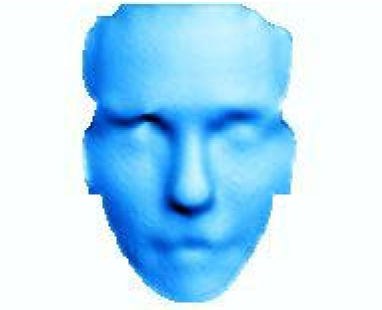


Figure 3.7. 3-D Facial Image. (From: Neurodynamics Home Page, Available Online, from [http://www.neurodynamics.com/BIOMETRICS/biometrics_product_tridentity/], August 28, 2002).

Additionally, the AcSys Face Recognition system produces a 3-dimensional product uses Holographic Neural Technology (HNeT).

The challenge of facial recognition systems is the actual management of large databases. The database manager or system administrator has to determine the subjects to be enrolled, the method of enrollment. Additionally, a strict policy should be implemented to determine the frequency the data will be purged. With all biometric systems, individual identification is greatly improved when coupled with another aspect of biometrics, resulting in a multi-modal system.

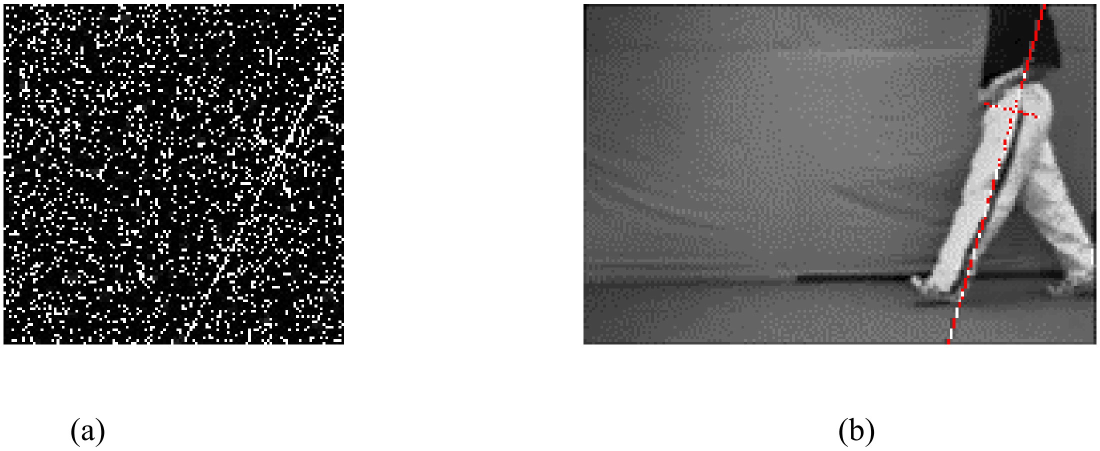
2. Behavioral

Behavioral characteristics of biometrics are considered the uniqueness of an individual. It is the way an individual walk, write and speak. Behavioral traits could only be used for verification purposes. In order to actually identify, it is best to combine a behavioral trait with a physiological trait.

[20] Neurodynamics HomePage, Available Online, [http://www.neurodynamics.com/BIOMETRICS/biometrics_product_tridentity/], August 28 2002.

a. Walk or Gait

Gait signature is that biometric feature involved in the verification of a subject by their walk. This verification method takes a lot of things into consideration, the movement of the torso, the alignment of the hip motion, the bend of the knee and the actual stride. Verifying someone's identity via gait is easier than voice recognition and handwriting due in part that it can and usually is done from a greater distance, thus, requiring no interaction with subject and the process does not have to rely on sound or camera resolution. Figure 3.8a depicts a motion model. Figure 3.8b depicts an extraction from a subject.



(a) (b)

Figure 3.8. a. Motion Model and b. Gait Extraction from Subject, Cunado, David, Dr., (From: Automatic Gait Recognition and Extraction, "Model-based Gait Recognition-Variation in Hip Inclination," Available Online, [http://www.isis.ecs.soton.ac.uk/image/gait/david_cunado/index.php3], August 25, 2002).

> The gait signature is formed from the Fourier description of the thigh and lower leg rotation. Angles of rotation are extracted via temporal template matching across the whole image sequence. Classification is done via the k-nearest neighbor and cross-validated with the leave-one-out rule.[21]

Current research suggests that the identification of a person from gait signature is just as accurate as the identification of a person using the physiological method, eye pattern, facial recognition and hand geometry. In the pursuit of homeland

[21] Yam, Chew Yean; Nixon, Mark S.; Carter, John N., University of Southampton, Fifth IEEE Southwest Symposium on Image Analysis and Interpretation, Santa Fe, New Mexico, April 7-9, 2002, "Performance Analysis on New Biometric Gait Motion Model", Available Online, [http://www.computer.org/proceedings/ssiai/1537/15370031abs.htm].

security defense, the optimum use of gait signature surveillance systems is in and around high value targets such as courthouses, federal buildings, nuclear plants, and water treatment facilities, as well as icons such as Statue of Liberty. Due to the amount of kinetic energy involved in gait, it is extremely difficult for a subject to disguise his walk or run as in the case of facial recognition. Gait signature does not require individual cooperation in order to ascertain identification from large crowds and at great distances.

b. Voice or Speaker Signature

Investments in the research and development of speaker recognition systems are on the rise. Corporations and individuals use voice recognition systems due to the relative ease of installation, added security it provides and the ability to obtain the necessary data (template) needed for a robust system. The most common use of the voice signature is that of access control.

> Several large corporations, including AT&T, ITT, GM, Hertz, Texas Instruments, and Martin Marietta, employ voice verification to protect computer, office, lab, and vault access. In addition, several states use voice recognition for parolees on home detention.[22]

The ideal voice recognition will have the ability to take into consideration the entire voice box or vocal tract and pay particular attention to the nostril, nasal cavity, and oral cavity. Due to the complex nature of the vocal tract it is easily subjected to manipulation, especially if an individual has a sincere desire to disguise his or her identity. Figure 3.9 gives a complete diagram of the human vocal tract.

[22] Page, Douglas, High Technology Careers Magazine, Feature Presentation, Biometrics: Facing Down the Identity Crisis, p. 4, Available Online, [http://www.hightechcareers.com/doc198/biometrics198.html], November 5, 2002.

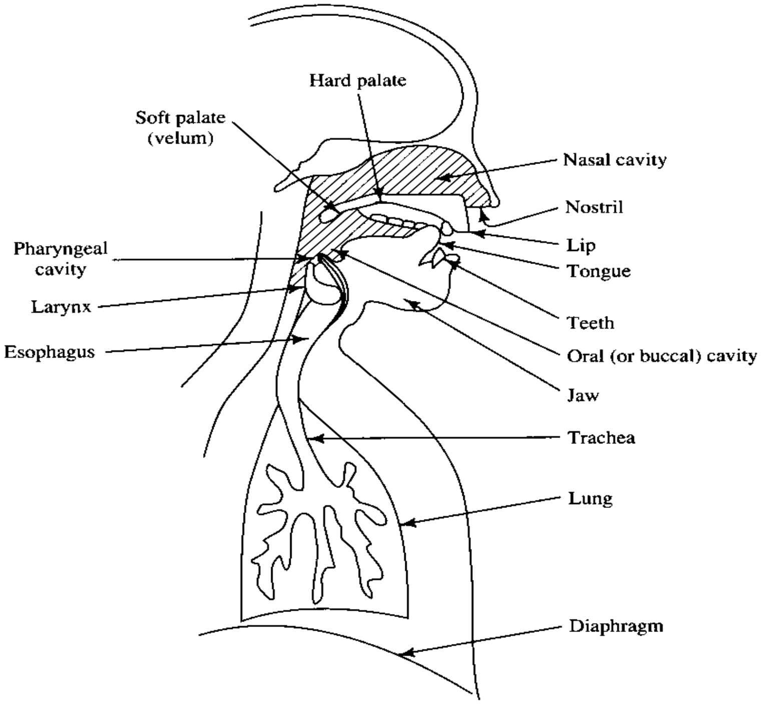
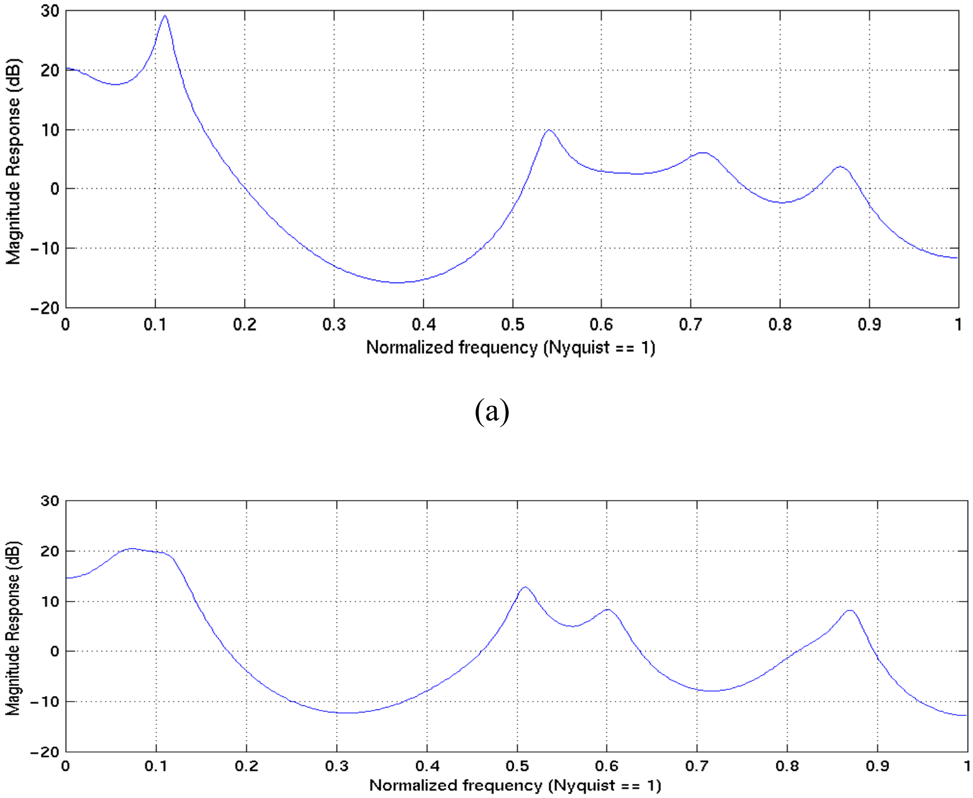


Figure 3.9. Human Vocal Tract, Speech Production System,(From: Speaker Verification, Available Online, From [http://biometrics.cse.msu.edu/speaker.html], November 5, 2002).

The voice template needed to commence the recognition system is easier to obtain than that of fingerprinting and especially of iris scanning. Additionally, it is more receptive among the general public. Once a voice recording is made, it is played back until the system recognizes the voice, the pattern and formulates the actual template. Once the template is made, it is stored for later retrieval in order to compare a set of spoken words or phrases. Figure 3.10a and 3.10b demonstrates a voice analysis of two different voices saying the same phrase. One of the leading voice recognition system vendors is Voice Security System.



(a)

(b)

Figure 3.10. a and b. Demonstrates a Voice Analysis of Two Different Voices Saying the Same Phrase. Voice Analysis,(From: Speaker Verification, Available Online, From [http://biometrics.sce.mdu.edu/speaker.html], November 5, 2002).

The primary advantages of voice recognition systems are twofold, physical contact is not required to formulate a template or extract data and it is relatively inexpensive to implement. Other advantages consist of what it allows the user to do. The voice recognition system allows "voice control to:

- hands free devices, for example car mobile hands free sets
- electronic devices, for example telephone, PC, or ATM cash dispenser
- software applications, for example games, educational or office software
- industrial areas, warehouses, etc.

- spoken multiple choice in interactive voice response systems, for example in telephony
- applications for people with disabilities”[23]

The primary disadvantage of a voice recognition system should be obvious to everyone, especially if the goal is to circumvent the security system or to conceal personal identification. The question that should come to mind is whether or not the system is robust enough to distinguish between an actual voice and taped recording? Additionally, since the vocal tract consist of so many moving parts the actual voice could be affected by an individual having a common cold or something as simple as a blister on the tongue.

c. Handwriting

The verification of an individual’s identity by their handwriting is a physiological biometric trait that is totally dependent on the mannerisms of the individual. Handwriting is a learned skilled and totally dependent upon the motor skills working together at the extremities, the fingertips. The learning process for handwriting commences early in life through trial and error. It is often improved or perfected to individual taste, hence formulating a signature template or individual password.

Handwriting takes into account the writing instrument, i.e., pen or pencil, writing surface, angle of the writing surface, and more importantly the inflection of the pen. In spite of the fact that an individual cannot write his or her name twice the same way, there is still enough evidence in the writing to determine if the signature is a match. Forgery or simulating a signature is extremely difficult and requires a great deal of practice. “One reason individuals find it difficult to simulate the handwriting of others is that to do so successfully requires understanding the essence of the writer's motor control program and executing that same program.”[24]

The use of handwriting in biometrics is usually reserved for verification purposes only. This practice has been in existence since the ancient Chinese and

[23] Voice Security System, Voice Command and Recognition Technology, Available Online, [http/www.speechpro.com/eng/technologies/restriction.html], November 5, 2002.

[24] Will, Emily J., Certified Document Examination Page, “Handwriting and Signatures – Some Basic Facts and Theory,” Available Online, [http://qdewill.com/theory.htm], November 5, 2002.

continues today. Federal, state and local agencies use handwriting biometrics in Forensic laboratories around the world in pursuit of justice.

There are companies around the world in pursuit of the perfect pattern recognition technique. One system that is worth mentioning is the Markov Model (MM) – it separates the handwriting into frames and compares the frames with other signatures for match. "The underlying assumption of the MM is that the signal can be well characterized as a parametric random process, and that the parameters of this process can be estimated in a precise, well-defined manner."[25]

Figure 3.11 demonstrates the Markov Model process of extracting observation symbols.

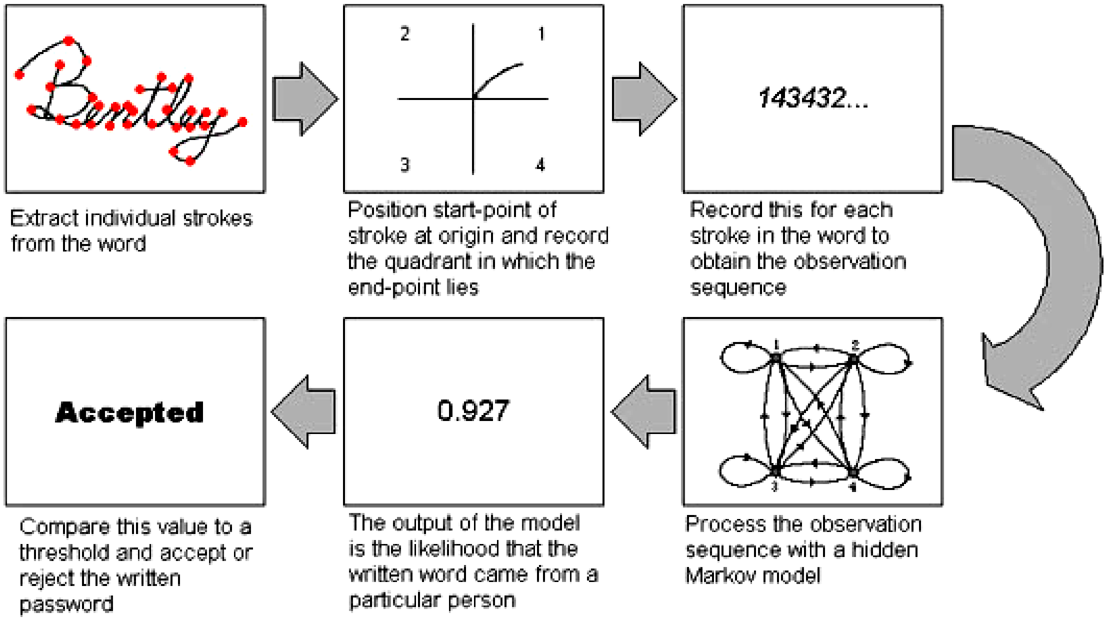

Bentley
Extract individual strokes from the word
2
1
3
4
Position start-point of stroke at origin and record the quadrant in which the end-point lies
143432...
Record this for each stroke in the word to obtain the observation sequence
1
2
3
4
Process the observation sequence with a hidden Markov model
0.927
The output of the model is the likelihood that the written word came from a particular person
Accepted
Compare this value to a threshold and accept or reject the written password

Figure 3.11. Markov Model Observation Process. McCabe, Alan Ph.D. Student," (From: Markov Modeling of Simple Directional Features for Effective and Efficient Handwriting Verification," Available Online, [http://www.cs.jcu.edu.au/~alan/handwriting/], November 1, 2002).

Other methods involved in the verification process include something as simple as someone studying a signature through a microscope. One would suggest that

[25] McCabe, Ph.D. Student, School of Information Technology, James Cook University, North Queensland, "Markov Modeling of Simple Directional Features for Effective and Efficient Handwriting Verification", Available Online, [http://www.cs.jcu.edu.au/~alan/handwriting/], October 28, 2002.

handwriting should be looked at 3-dimensionally and it is the third dimension that attributes to a distinct pattern. A writer pushes, pulls and applies a certain amount of depth or pressure to the writing surface on key words or phrases. Figure 3.12 demonstrates a three-dimension frame.

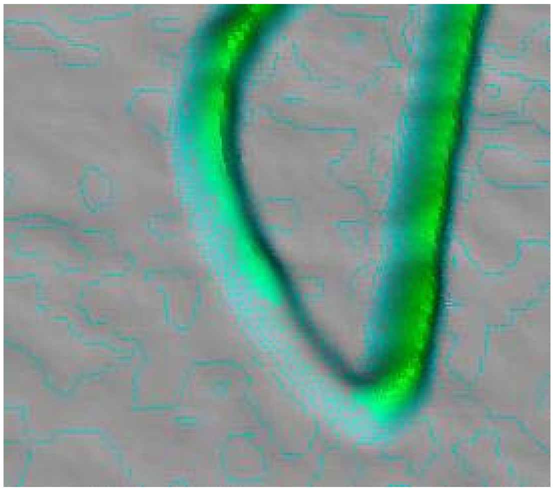


Figure 3.12. Three-Dimension Image. (From: MISC Program Brings 3D Modeling and Mathematical Information to Handwriting Identification and Document Examination, Available Online, [http;//qdewill.com/mics.htm], October 28, 2002).

A more robust verification system is a biometric system used in conjunction with an existing system. Banks have used handwriting signatures as a means of verification for many years. In lieu of the fact that forgery is on the rise and criminals pursue innovative techniques to circumvent the system, a more robust system would use the signature coupled with a Password or Personal Identification Number. The advantages of using Passwords or Personal Identification Numbers with handwriting biometrics are as follows:

- Combines the security of a secret password with the users own unique handwriting style, making forgery very difficult
- Alleviates the need for storage of highly sensitive biometrics data
- High user acceptance rate[26]

[26] McCabe, Ph.D. Student, School of Information Technology, James Cook University, North Queensland, "Markov Modeling of Simple Directional Features for Effective and Efficient Handwriting Verification", Available Online, [http://www.cs.jcu.edu.au/~alan/handwriting/], November 1, 2002.

The overall disadvantages of using handwriting as a means of verification of one's identity are numerous. "Handwriting can also be effected by other factors - injury, illness, medication, drug or alcohol use, stress, the writing surface, the writing instrument, or attempted disguise."[27]

d. Keystroke

The use of keystrokes in the biometric sense is for the verification of an individual's identity and access control. Similar to that of handwriting, keystrokes are learned and require motor skills at the extremities of the fingertips. Keystroke analysis is concerned with the frequency, accuracy, the pause between strokes and the length of time a key is depressed. Sufficient data compiled revealed that keystroke patterns are distinguishable enough for actual identification, thus being able to grant or deny access. "Samir Nanavati, a partner with International Biometric Group said, keystroke dynamics is a viable technology because it requires minimal training and no special hardware. It also inhibits employees from sharing passwords - a common way security is breached."[28] The ultimate goal of keystroke recognition system is to provide increased computer security and the protection of resources against computer fraud.

Keystroke recognition system is simple to implement due to the fact that it does not require any specific hardware and it is relatively easy to learn. Although, there are a number of products available we will focus on two. They are the KeyGhost Keylogger and Net Nanny. The purpose of KeyGhost is to "Record and retrieve everything typed, including emails, chat room activity, instant messages, website addresses, search engine searches and more."[29]

KeyGhost is a very simple concept and extremely easy to get started. The only thing required is the connection of a USB cable to the back of the computer and one to KeyGhost. Figure 3.13 illustrates the ease of connecting a computer to KeyGhost.

[27] Ibid.

[28] Soto, Monica, Inside Eastside Business, Seattle Times, Keystrokes tell Net Nanny Who's Typing, Wednesday, March 22, 2000, Available Online, [http://www.seattletimes.com].

[29] KEYGHOST, The Hardware Keylogger, Interface Security, Available Online, [http://www.keyghost.com.], November 5, 2002.

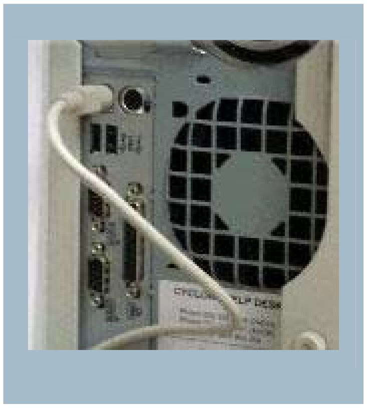
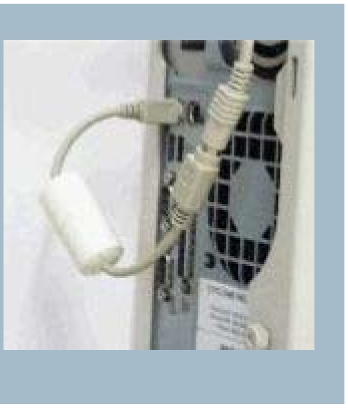
BEFORE	**AFTER**
	
For security reasons, the photo (above right) is only a representation of what the KeyGhost looks like. The actual KeyGhost II is injection molded to look exactly like an EMC Balun.	

Figure 3.13. Before and After Connection to KeyGhost. (From: Protective Security Management, We Understand Security, KeyGhost Logger, Available Online, [http://www.prosecman.com.au./keyghost/logger.htm], November 5, 2002).

KeyGhost Keylogger offers a great deal of advantages that should be considered in the pursuit of a robust system. KeyGhost Keylogger offers some distinct advantages:

- “It records every keystroke, even those typed in the critical period between computer switch on and the operating system being loaded
- It works with any PC operating system, and stores a continuous log even across multiple operating systems on one computer
- No software installation is necessary to record or retrieve keystrokes
- It has a capacity of up to 2,000,000 keystrokes stored with STRONG 128-bit encryption. (This is approximately 300,000 words, or 1 years worth of typing).
- Impossible to detect and/or disable by using software
- It is very user-friendly, you do not need to know how to program to use it. Simply plug the device into the keyboard cable

- The log in the **KeyGhost** cannot be tampered with"[30]

Net Nanny is a new software product that performs the same primary function as KeyGhost. "The new product, Biopassword LogOn for Windows NT, uses algorithms to measure the keystrokes of its user and create a "thumbprint," so to speak. The method is supposed to prevent someone from using another person's password."[31]

A survey of 240 random users, conducted last fall by IBG demonstrated that if users had a choice of biometrics used they would prefer something other than keystrokes. In all actuality keystrokes and handwriting came in last. Figure 3.14 depicts the results of the IBG random survey.

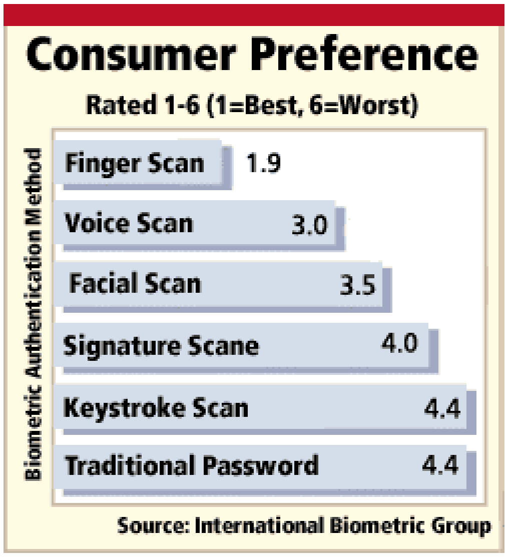


Figure 3.14. IBG Random Survey Results. (From: Bruno, Mark, Technology, That's My Finger, "The Results Are In. And The Winner Is the Finger," Available Online [http://www.us-banker.com/usb/articles/usbfeb01-9.shtml], October 27, 2002).

C. CHOOSING THE RIGHT BIOMETRICS

Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening our national borders, in travel documents, visas and in preventing ID theft. Congressional offices and different Government agencies are addressing the important role that biometrics will play in

[30] Ibid.

[31] Soto, Monica, Inside Eastside business, Seattle Times, Keystrokes Tell Net Nanny Who's Typing, Wednesday, March 22, 2000, Available Online, [http://www.seattletimes.com].

> identifying and verifying the identity of individuals and protecting national assets.[32]

The implementation of a robust biometric based UbiSurv requires a great deal of consideration. The considerations that must be made are very challenging to the respective owners of such a system. Some of the more important factors that must be considered are listed below:

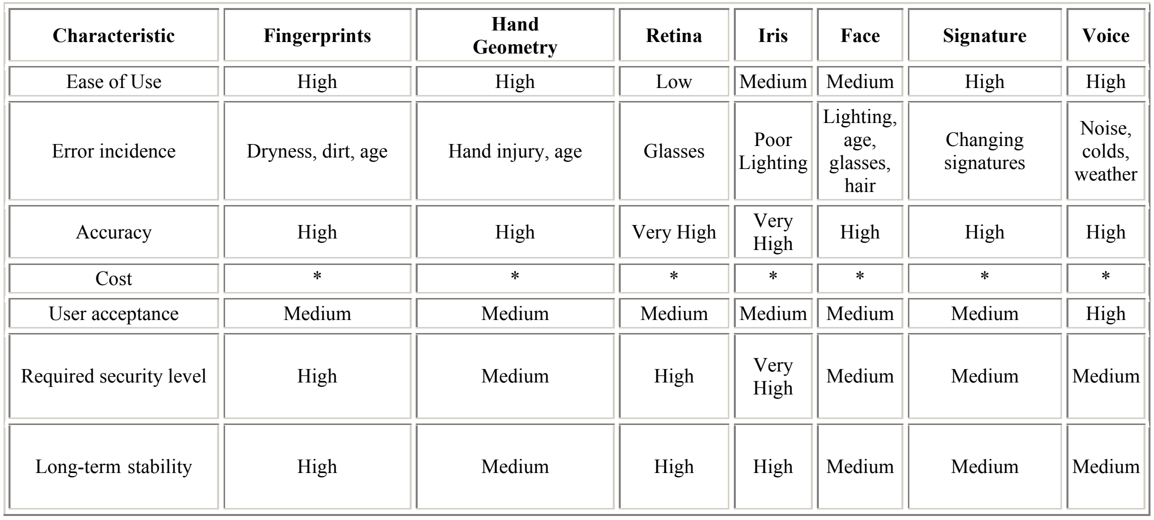
- **"Comfort:** duration of verification and the ease of use
- **Exactness:** minimal error rates (clarity, consistency, measurability)
- **Availability:** the portion of a potential user group who can use biometrics for technical identification purposes (universal, measurable)
- **Costs:** essentially due to the sensors."[33]

As demonstrated in Figure 3.15, a table of Biometrics Considerations, March 2000, building the robust UbiSurv with the appropriate biometric trait is extremely difficult. The norm is to choose the biometric trait that is widely available at the least expensive costs. However, with the continual rise in security concerns of our homeland, citizens of the United States, and the huge monetary increase in biometric technology – the focus has shifted from cost to comfort and exactness. "The biometric industry represents a $500M market with an anticipated revenue growth to 1.1B by the year 2003. The market for personal authentication through biometrics is much larger. For example, it is expected that 230M people will be conducting wireless transactions representing $100B/year with more than 1B transaction."[34]

[32] The Biometric Resource Center Website, Legislation, Available Online, [http://www.itl.nist.gov/div895/biometrics/legislation.html], January 8, 2003.

[33] Page, Douglas, High Technology Careers Magazine, Feature Presentation, Biometrics: Facing Down the Identity Crisis, p. 4, Available Online, [http://www.hightechcareers.com/doc198/biometrics198.html], October 9, 2002.

[34] Podio, Fernando L., National Institute of Standards and Technology, " Biometrics – Technologies for Highly Secure Personal Authentication," Available Online, [http://www.itl.nist.gov/lab/bulletns/bltnmay01.htm], March 16, 2003.



Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

Figure 3.15. (From: find BIOMETRICS – "A Practical Guide to Biometric Security Technology," Selecting a Biometric Technology, Available Online, [http://www.findbiometrics.com/Pages/lead3.html], August 23, 2002).

3. Consumer Considerations

The primary consumer considerations in the implementation of a biometric based security system should be that of overall comfort to the user, the enrollment process and the method of extracting data. The enrollment process and user direct involvement of biometric based systems vary based upon trait selected. User enrollment in fingerprint biometric based systems requires the user to have his or her fingers rolled on an inkpad then onto a form. The original form becomes the template. The template is versatile, it can remain in paper format or stored digitally on a computer for easy retrieval or match. "Current fingerprint-based systems offer fully mature technologies for capturing, encoding, storing, matching, and verifying searches against large databases. In addition, they are one of only two biometrics – the other is facial feature recognition – that can support enrollment (e.g., via paper forms such as photographs or, in the case of fingerprints, by means of inked or livescan-printed fingerprint cards)."[35] The enrollment process during gait recognition technology requires actual videotaping of the user walking and running. Gait recognition technology does not require physical user interaction. Extracting data is also a consideration of consumers because certain

[35] Biometric Technical Assessment (updated August 19, 2002), Available Online, [http://www.bioconsulting.com/Bio TechAssessment.html], p. 34.

biometric features requires a large data set in order to determine accuracy or a match with that of the data stored on the templates.

"Nancy Jamison of Jamison Consulting, a BioMarket Project consultant, noted that a variety of approaches to biometrics are receiving public support. 'Of the five biometric technologies that we examined, finger recognition and voice verification had the highest acceptance rates in part due to higher existing levels of public awareness', she stated."[36] One of the least accepted biometric traits in terms of user interests is the retinal scan. Based upon a Scandinavian report, "The 'users have... concerns about retina identification, which involves shining an infrared beam through the pupil of the eye...' Also, Retinal Scan requires 'a precise alignment and a pause while the scan is done, while (other biometric techniques) such as voice and fingerprint can be done in a more natural and casual manner.[37]

The enrollment process and the rejection rate are of major concern to the user. The user is curious to know the amount of times they will have to submit before a template is actually made and before a match is determined. Although, all biometric features have a different False Enrollment Rate and False Rejection Rate, they vary slightly.

4. Secrecy or Privacy Concerns

As the general public is more educated in terms of biometric features, it may embrace the need for a better security or surveillance system with certain assurances. The assurances at the top of the list are that their privacy will not be violated and that the data retrieved during the enrollment process will be used only for the intended purpose. There were numerous questions concerning the legality of the surveillance cameras installed in the stadium in Tampa, Florida, during Superbowl XXXV. As a result, the Supreme Court ruled that privacy issues do not exist concerning the surveillance of parts of the human body that are continuously exposed to the public, i.e., your face.

[36] Breaking News on Biometrics, Introduction to Speech Solutions for Financial Services, Available Online, [http://speechtek.com.], October 15, 2002.

[37] Ruggles, Thomas, Comparison of Biometric Techniques, Copyright 1996, August 28, 2002, Available Online, [http://www.bioconsulting.com/bio.htm].

Although biometrics is extremely accurate in the identification and verification of a user, compromise and misuse are still possible. “Such applications could include those in which an authorized user cannot control the processing of his or her biometric traits and is not aware of the processing.”[38] “Another problem is that not every biometric authentication technique may be completely spoof proof. If biometric data are stolen or sold, it may be possible to use them to execute a successful masquerade.”[39]

The incorporation of biometric data in the UbiSurv raises other concerns. The primary concern of utilizing UbiSurv is the associated security vulnerabilities. “Experiments have been made where the average person equipped with a wireless laptop computer and an antenna can drive around looking for hot spots.”[40] Hot spots are areas where the operator of the laptop can access data operating on wireless networks. An individual possessing the ability to access a wireless network from his car with minimal equipment indicates that he or she could access critical data.

C. SUMMARY

The thought processes that went into the implementation of this specific UbiSurv were made based upon the actual use and the anticipated users. The intended use of the UbiSurv is to provide a method of access control in a designated laboratory and specific computers in the laboratory. Once admission to the laboratory is granted, the UbiSurv will provide a measure of surveillance of users while in the laboratory.

The initial enrollment in the UbiSurv is strictly voluntary and restricted to Information Systems and Operations, Information Management Technicians and Computer Science curriculum staff and students. Given careful consideration to all biometric features – the conscious decision was made to have multi-modal system. A multi-modal biometric system offers added sense of security and accurateness due to the fact that it requires more than one feature in order to obtain a positive match. The multi-modal features selected for this UbiSurv are facial recognition and fingerprint, to be

[38] BIOIDENTIFICATION, Frequently Asked Questions, September 30, 2002, [http://www.home.t-online.de/home/manfred.bromba/biofaqe.htm].

[39] Biometric Technical Assessment, Updated 19 August 2002, Available Online, [http//bioconsulting.com/Bio Tech Assessment.html].

[40] Dinolt, George, Associate Professor, Naval Postgraduate School, August 2002.

incorporated by follow-on thesis students. Although, the initial UbiSurv will focus only on facial recognition, it does allow for expansion of other biometric features.

The enrollment process of the volunteer users will consist of fingerprinting with an inkpad and paper template. The intent is to digitally scan the fingerprint template for incorporation into the database. Facial images will be captured with a digital camera and stored in the database.

The volunteer users of the UbiSurv are required to read, understand and sign a privacy statement and a memorandum of agreement. The primary purpose of the UbiSurv is not to infringe upon individual privacy rights but to promote the advancement of homeland security in the protection of our nation, border crossings, immigration and naturalization, customs, law enforcement agencies and airports. Additionally, it is designed to provide development of the concept and thorough data collection to Naval Postgraduate School and Department of Defense students.

The anticipated difficulties of the UbiSurv are the development, implementation and the management of database for facial recognition and fingerprint recognition that are interoperable. Some distinct disadvantages of facial recognition systems are:

- "Can be fooled by identical twins
- A recent test performed by the editors of PC Magazine found that at least one popular facial feature recognition system can be fooled by imposters holding in front of their faces a full-size, color picture of the person they are trying to impersonate, cutting a hole for their nose to add an artificial depth quality to the imaged face.
- The EER (Equal Error Rate) for facial recognition algorithms can be very high when compared to other types of biometrics. This is especially true for potential matches against a database consisting of facial records that are 12 or more months older than the search data."[41]

[41] Biometric Technical Assessment, August 19, 2002, Available Online, [http://bioconsulting.com/Bio_Tech_Assessment.html].

IV. WIRELESS NETWORK

This chapter will discuss the basic components the UbiSurv and 802.11b standard wireless local area network. The UbiSurv Testbed consists of biometric and embedded technologies supported by a wireless local area network (WLAN). This chapter will discuss the basic components the UbiSurv and 802.11b standard wireless local area network. This chapter will also discuss the inherent security problems of the IEEE 802.11b WLANs and the applications we plan on implementing to solve some of the problems.

Wireless networks operate by broadcasting information via radio-frequency signals. "Wireless networks are categorized in three groups based on their coverage range: Wireless Wide Area Network (WWAN), Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN)."[42] The WWAN consists of technologies that cover a large area like cellular technologies, or the Global System for Mobile communications. The WLAN includes 802.11, Hyperlan, H.323. Bluetooth, Infrared Data Association (IrDA), Shared Wireless Access Protocol (SWAP) and HomeRF are all examples of WPAN. The UbiSurv testbed consists of a WLAN with limited Bluetooth capability.

A wireless local network can consist of a fixed and/or mobile network infrastructure. The wireless portion of the network infrastructure consists of an access point (AP), and stations or nodes with a wireless adapter also know as a network interface card (NIC). A NIC is a radio modem that has the logic to interact with the client machine, software, and communicate with an access point. An Access Point (AP) consists of a radio modem on one side and a bridge to the Ethernet backbone on the other side. Access points receive and transmit data to components that are equipped with a wireless adapter. The Linksys WAP 11 is the access point used in UbiSurv because it has the capability to roam, act as a bridge, perform load balancing, and network traffic filtering which is vital for time critical information. Other notable features of the Linksys

[42] The NIST Handbook, Special Publication 800-12, "An Introduction to Computer Security".

WAP 11 are MAC address filtering, IP filtering, DCHP client and password protection. The operating ranges of the Linksys are listed in the Table 3.1.

Indoor	**Operating Range in feet**	**Mpbs**
	0 – 164	11
	0 – 262	5.5
	0 – 393	2
	0 – 492	1
Outdoor	0 – 820	11
	0 – 1148	5.5
	0 – 1312	2
	0 – 1640	1

Table 3.1. Linksys Operating Ranges vs. Mpbs.

A. 802.11B STANDARD AND GENERAL ARCHITECTURE

The Wireless Local Area Network standard is IEEE 802.11 which is designed to support medium-range, higher data rate application, allow mobile stations or nodes to access the LAN while in motion or stationary. Wireless networks that utilize the 802.11b standard can establish a peer to peer (point to point) network or a based on stationary access points (AP) that mobile nodes communicate through. A cell is the area covered by the AP and is referred to as a Basic Service Set (BSS). The collection of a network is known as a Extended Service Set (ESS) 26. This topology is useful for providing wireless coverage in and between buildings or around a campus. As the UbiSurv testbed extends beyond the confines of the Giga-Lab, this property of the 802.11b standard will enable the UbiSurv to be implemented campus wide. In most WLANS a station or client consist of a laptop or PC with a wireless NIC. A client can consist of a Personal Digital Assistant (PDA), desktop, laptop or handheld device. In the UbiSurv testbed the stations will consist of a Dell Desktop and laptop. The clients consist of a Compaq PDA, and laptop.

Wireless connected computers using a Hardware Access Point.

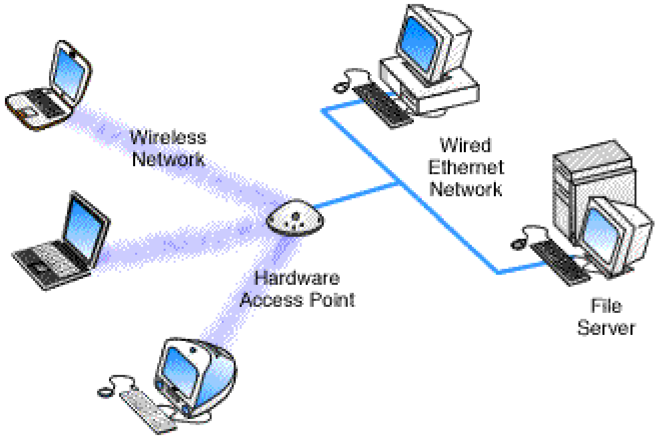


Figure 4.1. Hardware Access Point. (From: [www.computer.howstuffworks.com\wireless-network.htm], August 15, 2002)

Wireless connected computers using a Software Access Point.

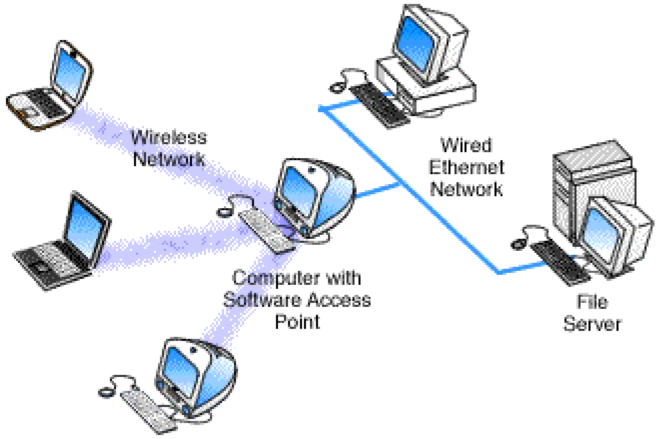


Figure 4.2. Software Access Point. (From: [www.computer.howstuffworks.com\wireless-network.htm], August, 15, 2002)

B. WHY WIRELESS?

The four primary benefits a WLAN offers to the UbiSurv are User/Operator Mobility, Rapid Installation, Flexibility, and Scalability.

- "User/Operator Mobility allows users to access files, and network resources without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the LAN.

This benefit gives the UbiSurv administrator the ability to roam the campus and still monitor the network.

- Rapid Installation is comparison to an instillation of a wired network. No addition, removal, or traversing through walls or ceilings of wires are required for new additions to the UbiSurv. Once the node is activated it is on the network.
- Flexibility means user/operators can install and uninstall UbiSurv nodes whenever and wherever necessary. Flexibility allows UbiSurv operators to temporarily setup wireless, biometric, or surveillance nodes for a particular application then take it down after its intended use.
- Scalability allows WLAN network topologies to be easily configured to meet specific application and installation needs and to scale from small P2P networks to very large enterprise networks that enable roaming over a broad area. Scalability is crucial to the success of the UbiSurv because without the interoperability of the various brands of equipment the testbed cannot function."[43]

C. IEEE 802.11B OPERATING MODES

IEEE 802.11 has two operating modes: ad hoc mode, also known as peer-to-peer mode, and Infrastructure mode. Ad hoc mode allows to clients communicate directly with each other without an access point. Ad hoc would allow nodes to communicate with each other if they traveled out of the range of an access point or if an access point experiences failure. Infrastructure mode has at least one wireless AP and one wireless client. The wireless client acquires resources of the wired portion of the network through the wireless AP. The wired network can consist of an Ethernet, Intranet or the Internet or a combination depending on the placement of the Access Point. The preferred mode of the UbiSurv is Infrastructure mode with ad hoc network capability for back up purposes.

D. 802.11B OPERATION BASICS

Once the Linksys WAP 11 is operational it establishes an association. An association is the process where a wireless adapter chooses a wireless AP to connect to. If the wireless client is configured to operate in infrastructure mode, an association is made when the adapter scans across the wireless frequencies for wireless APs and other wireless clients in ad hoc mode. The Linksys WAP 11 automatically selects a wireless AP to connect with by using an SSID, signal strength and frame error rate information.

[43] IEC 7498-2, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, February 1989.

Afterwards, the wireless adapter changes to the assigned channel of the selected wireless AP and agrees on the use of a port. A port is a channel of a device that can support a single point-to-point connection. For IEEE 802.11b, a port is an association, a logical entity over which a single wireless connection is made. Most wireless client with a single wireless network adapter has one port and can support only one wireless connection. The Linksys WAP 11 has multiple ports and can simultaneously support multiple wireless connections therefore increasing the number of nodes operating with one access point. The logical connection between a port on the wireless client and the port on a wireless AP is a point-to-point bridged LAN segment—similar to an Ethernet-based network client that is connected to an Ethernet switch.[44]

The wireless adapter can also establish a re-association if the wireless access point signal strength is too low, the error rate too high, or if instructed by the operating system (in the case of Windows XP). If one of these conditions exists, the wireless adapter searches for other wireless APs to verify if another wireless AP can provide a stronger signal or lower error rate. If a wireless AP is located, the wireless adapter changes to the channel of that wireless AP and negotiates the use of a port. Re-association usually occurs with a wireless AP when the signal weakens due to the wireless adapter moving away from the wireless AP or the wireless AP experiences congestion with excessive traffic or interference. The wireless adapter evenly distributes the load to other wireless APs by re-association thus increasing the performance for other wireless clients. Contiguous coverage over large areas can be achieved by strategically inserting wireless APs so that their signal areas overlap. Overlapping signals allow a wireless client to roam across different signal areas, thus enabling the adapter to associate and re-associate from one wireless AP to another, maintaining a continuous logical connection to the wired network. The campus wide versions of the UbiSurv will need this feature in order to insure that all the nodes are connected and communicating with the network.

E. AD HOC NETWORKS

Ad Hoc networks like Bluetooth dynamically connect remote devices such as cell phones, laptops, and Personal Digital Assistant (PDA). Bluetooth is low cost, low power, and low profile technology that allows users to create small UbiSurv networks.

[44] [www.microsoft.com/technet/treeview/].

Bluetooth features include fast and reliable transmission of voice and data. The topology can be established on a temporary and random basis. Ad Hoc networks constantly shift their topology by depending on a system of mobile routers connected by wireless links to allow components to correspond with each other. In a Bluetooth network, mobile routers control the flow of data between devices that are capable of supporting direct links to each other. As devices travel in unpredictable fashion, the network reconfigures itself on the fly to handle the dynamic topology. This ensures that a remote mobile device remains connected to the network. The router also controls the stream of communication and the routing protocol allows the UbiSurv to constantly reconfigure itself as devices randomly move in and out of the network. Once the UbiSurv is implemented outside the campus of the Naval Postgraduate School, ad-hoc mode will play a more vital role. Bluetooth will allow UbiSurv system nodes to be set up with mobile platforms. Bluetooth will also ensure that the nodes are constantly connected to the network

F. WIRELESS SECURITY

The UbiSurv will contain a hybrid infrastructure based on fixed, mobile and ad hoc topologies and technologies. The biggest concern of the UbiSurv use of a WLAN is information assurance. Information assurance is defined as information security and information availability. The UbiSurv's architecture must " (a) provide sufficient security measures, (b) be survivable under node or link attack or failure and (c) be designed such that sufficient capacity remains for all critical services (and preferably most other services) in the event of attack or component failure."[45]

For the UbiSurv, reliable information exchange and secure communications during component failure or security breach is vital. The UbiSurv's survivability and security issues are harder than a wired network because of the broadcast nature of wireless components like access points. The UbiSurv is also extremely vulnerable to malicious attacks and susceptible to inadvertent damage to nodes. Additionally, the rate mobile nodes enter and leave the network directly impact the degree of survivability, security and communications reliability. If the network is constantly associating nodes the throughput of the network is slowed. Wireless cards associate with the access point

[45] Kabara, Joseph, Krishnamurthy, Prashant, Tipper, David, "Information Assurance in Wireless Networks", [www.cert.org/research/isw/isw2001/papers/kabara.pdf].

that provides the most power. If an access point is beaconing with more power than other access points all the nodes will associate with the beaconing access point thus reducing the efficiency of the network The unique features of the UbiSurv results in “limited applicability of standard survivability and security techniques developed for wired networks.”[46]

UbiSurv needs information availability devices that can compensate for failures caused by malicious attacks or unintentional breakdown. Special network mechanisms are needed in critical sections and protocols to automatically maintain communication and information flow. UbiSurv must be able to automatically reconfigure to provide critical services at the minimum and other services, to the extent possible in the event of component failure or attack. UbiSurv must have features like location management, mobility management and radio resource management. The primary objective of resource management is to maximize the available capacity at a radio-level and to allocate this capacity in a way to obtain an efficient Quality of Service. Resource management is defined terms of standards, benchmarks, network architectures and protocol. Very few wireless vendors address performance during failures, survivability and information assurance in the network design/architecture. The neglect of the management features can cause catastrophic network failure and resource misallocation. Network survivability of the UbiSurv involves network failure prevention; minimizing the impact of failures on testbed nodes and providing the means for the network to automatically overcome failures. If the UbiSurv has restoration protocols that allow service during and after a failure many of the inherent wireless security problems will not gravely affect the UbiSurv operation.

The National Institute of Standards and Technology (NIST) handbook “*An Introduction to Computer Security* classifies security threats into one of nine categories:

1) Errors and omissions, 2) fraud and theft committed by authorized or unauthorized users of the system, 3) employee sabotage, 4) loss of physical and infrastructure support, 5) malicious hackers, 6) industrial espionage, 7) malicious code,

[46] Ibid.

8)foreign government espionage, and 9) threats to personal privacy."[47] The most threatening to the UbiSurv is theft, fraud committed by authorized and unauthorized users of the system, malicious hackers, malicious code, and espionage. Theft is considered a high threat because some the surveillance nodes are dual use, such as a teddy bear or radio with a hidden camera. Malicious hacking of the UbiSurv is easier compared to wired networks because hackers can bypass firewalls, and intrusion detection systems by entering the network through wireless connections. Malicious entities can also perform Denial of Service attacks, steal the identity of legitimate users which enables them to monitor their movements and transactions, disrupt normal network operations, or launch an attack with their true identity concealed. Espionage stems from the relative ease in which eavesdropping can occur on radio transmissions.

The UbiSurv employs the Wired Equivalent Protocol (WEP) to provide security services in the wireless operating environment. WEP is designed to provide the same level of security as that of a wired LAN. WEP offers link level data protection during transmission between clients and access points. WEP only protects the wireless portion of the connection. End to end security does not exist with WEP.

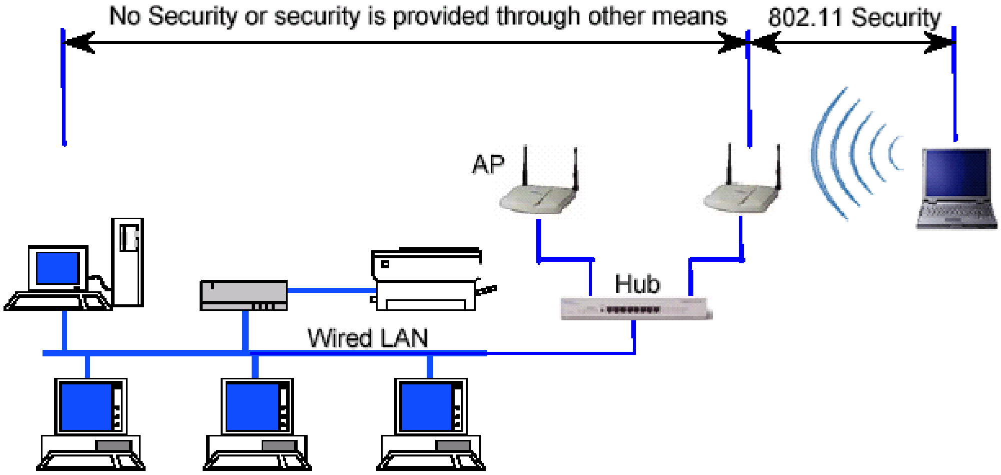


Figure 4.3. Wireless Security of 802.11b in Typical Network From (From: The NIST Handbook, Special Publication 800-12, An Introduction to Computer Security).

[47] The NIST Handbook, Special Publication 800-12, An Introduction to Computer Security.

The fundamental security standards for IEEE WLAN are Authentication, Confidentiality, and Integrity. Authentication allows only authorized users to access the network. The identity verification of wireless clients is WEP's primary goal. WEP's secondary design goal is confidentiality. Confidentiality is "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."[48] Confidentiality prevents information compromise from casual eavesdropping (passive attack). It only authorizes allowed personnel to view data. Integrity is "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."[49] Integrity assures that data is trustworthy and has not been tampered with in transit between the wireless clients and the access point in an active attack.

An attacker can break into a wireless network by associating to an access point with its wireless NIC running in promiscuous mode, and 'sniffer' software (e.g., ethereal) to capture the Service Set Identifier (SSID). If an AP is running in open authentication mode then an intruder may access the wireless network by simply changing their SSID to that which she just discovered. Also, given that all (authenticated) clients know or have access to the SSID, then a bit of social engineering is all that is needed to acquire the SSID from a client. To prevent these kinds of attacks , in the UbiSurv, all access points will deactivate the SSID broadcast.

Media Access Control (MAC) address filtering amounts to allowing predetermined clients with specific MAC addresses to authenticate and associate. "The addition of MAC address filtering increases security, however it is not a perfect solution given that MAC addresses can be spoofed"[50]. Also, the process of manually maintaining a list of all MAC addresses can be time consuming and error prone. Nevertheless, UbiSurv will utilize MAC address filtering because it will be a small and fairly static testbed.

MAC address filtering alone cannot provide adequate security, authentication, and identification. In order to provide proper security one must monitor the airwaves. MAC address spoofing is when someone places a valid MAC address on to a rogue AP. The

[48] ISO/International Electrotechnical Commission (IEC) 7498-2, July 25, 2000.

[49] Network Working Group Request For Comment (RFC) 2828, May 2000.

[50] Cole, E., "Hackers Beware", Boston, MA: New Riders, April 2002, p. 1.

attacker starts off by finding a MAC, updating the registry, and making the association. The attacker then unplugs a workstation, copies a valid network internal MAC to an AP, then inserts that AP into the network.

There are several software tools, extensively and freely available over the Internet that allows attackers to listen and capture wireless transmissions on the UbiSurv. Some of these have the ability to break Wired Equivalent Privacy (WEP) if provided a sufficient number of encrypted packets. Some of those tools are Airsnort, WEPcrack, and ethereal. These sniffing tools have WEP decrypting capabilities. Some of the more popular scanning tools are NetStumbler, Kismet, AirMagnet, and AeroPeek. NetStumbler is a freeware Wireless AP Detector that listens to broadcast beacons that identify AP's. It actively sends out probes on all channels searching for AP's. It listens for all types of traffic but if the AP is not broadcasting its SSID it will not detect them. Kismet is better than NetStumbler because it operates at Layer (3) and higher of the Open Systems Interconnection Reference model. Kismet submissively observes all traffic, sorting and organizing of wireless packets.

AirSnort works by setting the wireless NIC into capture (promiscuous) mode. Airsnort has the ability to capture SSIDs, which is sanitized for confidentiality, whether WEP is enabled, the last IV transmitted, the number of packets sent, encrypted packets, and so on.

"Session hijacking is when an attacker takes over an existing session, meaning the attacker is relying on an existing authenticated connection to acquire access to network resources"[51].

[51] Craiger, Philip J., "802.11,802.1x & Wireless Security", June 23, 2002, [www.sans.org/rr/wireless/80211.php].

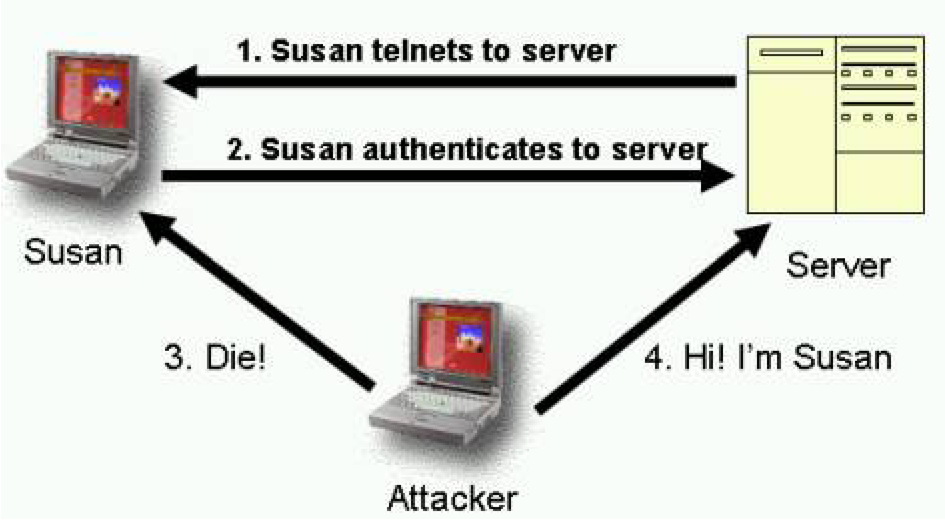


Figure 4.4. Hijacking Session. (From: Craiger, Philip J., “802.11,802.1x & Wireless Security”, June 23, 2002).

Figure 4.5 shows an attacker waiting until Susan (a valid user) authenticates, then kills or blocks Susan’s connection and subsequently pretends to be Susan. This requires that the attacker spoof the authenticated user’s IP address in order to maintain the connection.

Current Encryption and authentication standards do not provide fail-safe security. Intruders can perform identity theft by stealing the SSID and Media Access Control (MAC) addresses to steal the identity of a user. Changing the default SSID of each access point usually prevents Identity theft. The default SSID for Linksys access points is linksys. Default SSIDs immediately alerts hackers that the wireless system is vulnerable. Hackers perform Man in the Middle attacks by placing a rogue station between an authorized station and access point where all traffic between the authorized station and access point is routed through the rogue station.

The UbiSurv has two security priorities. The first is strong authentication to prevent unauthorized persons from accessing testbed and strong encryption to protect data in transit. Although WEP uses authentication techniques, it is not strong enough for the UbiSurv. Along with WEP, the UbiSurv needs something that can operate with WEP and provide strong encryption and filtering of packets between wireless clients. Virtual Privacy Network (VPN) is needed for the UbiSurv because it can employ strong authentication and encryption mechanisms and end-to-end security. VPN creates a tunnel between end points, which protects the packets from intrusion. VPN also employs a Internet Key Exchange (IKE) protocol that provides three techniques for protecting data and communications. IKE also supports digital signatures, which provides an additional level of confidentiality. In the UbiSurv, a VPN would be placed behind every access point thereby establishing one to one secure connection wireless nodes that does not involve WEP. The biggest disadvantage of using a VPN is that most VPN products are proprietary and do not interoperate well.

V. OPERATIONAL ANALYSIS OF THE UBISURV

A. INTRODUCTION

This chapter discusses the setup and operations of the UbiSurv testbed. Equipment used, expected results, actual results and modifications and upgrades. Applicable Hardware and Software. As previously mentioned, the UbiSurv is set up the GIGA LAB in Root Hall. The setup is shown here in Figure 5.1

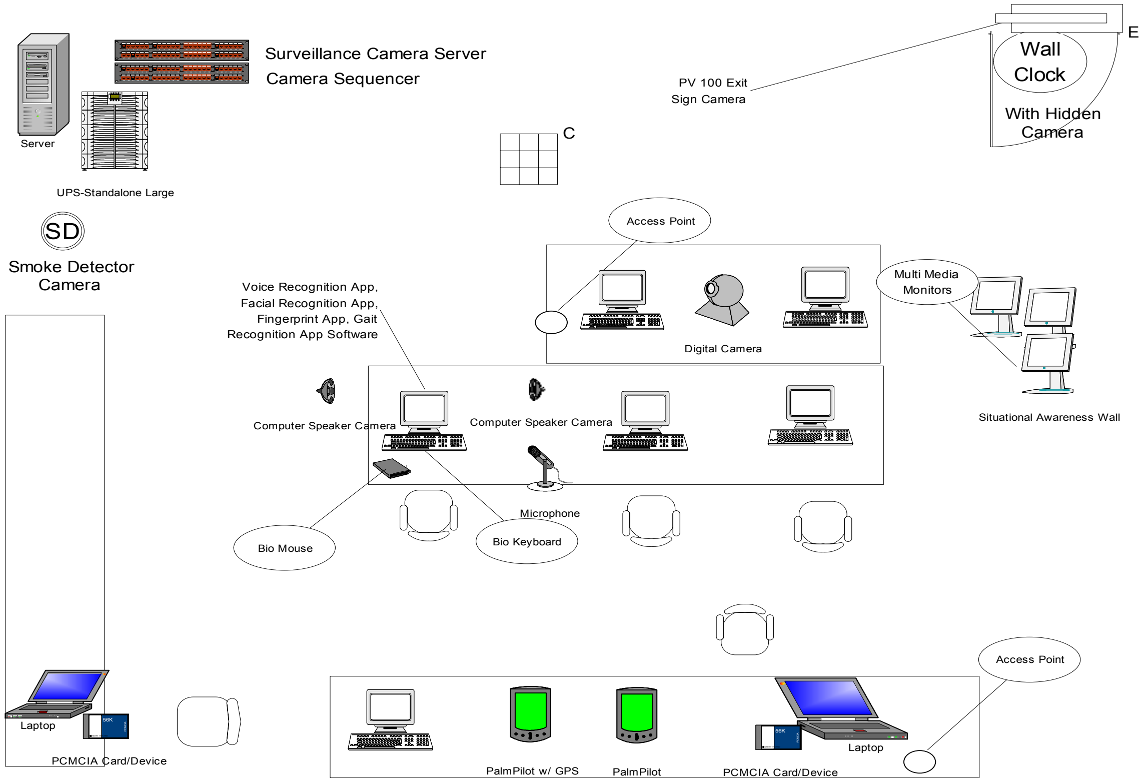


Figure 5.1. UbiSurv Setup.

B. SENSORS

1. Canon GL1 Digital Video Camera

The digital video camera served as the main input tool into for our facial recognition database. The Canon GL1's versatility allowed us the ability to capture motion and still images and save them as templates used for facial recognition. The digital video camera also served as a surveillance tool in the UbiSurv testbed.

2. PalmVID Camera

The three hidden cameras used in the UbiSurv testbed are the PVCOMPSPEAKERS700, PVWALLCLOCK700 and PVBOOK700. All hidden cameras were manufactured by PalmVID. The hidden cameras were selected because of their wireless capabilities; particularly a monitoring range up to 700ft. Tables 5.1 – 5.3 lists the specifications of the PV700 respective hidden cameras and Peripheral Equipment. "The stated wireless ranges are based on LOS (line of sight) distances. The signal will penetrate walls, floors, furniture, and other items. The actual range will depend on the density of the material, distance between the transmitter and receiver, and other factors. The 700' LOS system will typically yield ranges of 400'-500' through more than 2-3 interior walls."[52]

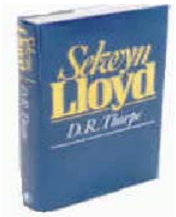
[52] Palmvid.com/pdf/pvcompspeakers700.pdf, February 20, 2003.

PVCLOCK 700

PVREC700LCDMON	Wireless 4 Channel 2.4Ghz Receiver with built-in Color Video Monitor
PVREC700	Wireless, 4 Channel, 2.4Ghz Receiver
Transmitter Specifications:	
Transmitting frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Transmitted power:	10mw (max)
Video format:	NTSC or PAL
Receiver Specifications:	
Video output:	RCA/SCART—jack 1 Vp-p
Stereo audio output:	left/right RCA/SCART– jack 1 Vp-p
Operation frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Receiver sensitivity:	80 dBm
Dimensions:	155mm x 80mm x 41mm
Video format:	NTSC or PAL
Power Requirements:	+12VDC 500mA (max)
Operating Conditions:	Indoor use only
Resolution:	380 TV Lines (Color) - 420 TV Lines (B/W)
Lens:	90° f3.8mm pinhole lens
Low light compensation:	1 lux, F2.0 (Color) - 0.1 lux, F2.0 (B/W)
Power requirements:	12VDC 300Mah
Enclosure Dimensions:	1” (D) x 9” (R)
Camera iris:	ELC light compensation
Imaging device:	1/3” CCD Grade 1st
Wall Clock Camera Specifications:	
Warranty	1 Year parts and labor warranty (standard)
Scanning System:	2:1 Interlace
Electronic Shutter:	1/60~1/10,000,000 Sec. Automatic
Operating Temperature:	-10ºC~50ºC
S/N Ratio:	More than 50dB
Signal System:	E:EIA 60Hz
USBVIDEO RCA CABLE	RCA Video Cable for Connecting Receiver
PS12V	Camera and Receiver Power Supplies

Table 5.1. PVWALLCLOCK700. From (Yamaha YST-M101) Specifications.

PVBOOK700



PVREC700LCDMON	Wireless 4 Channel 2.4Ghz Receiver with built-in Color Video Monitor
PVREC700	Wireless, 4 Channel, 2.4Ghz Receiver
Transmitter Specifications:	
Transmitting frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Transmitted power:	10mw (max)
Video format:	NTSC or PAL
Receiver Specifications:	
Video output:	RCA/SCART—jack 1 Vp-p
Stereo audio output:	left/right RCA/SCART– jack 1 Vp-p
Operation frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Receiver sensitivity:	80 dBm
Dimensions:	155mm x 80mm x 41mm
Video format:	NTSC or PAL
Power Requirements:	+12VDC 500mA (max)
Operating Conditions:	Indoor use only
Resolution:	380 TV Lines (Color) - 420 TV Lines (B/W)
Lens:	90° f3.8mm pinhole lens
Low light compensation:	1 lux, F2.0 (Color) - 0.1 lux, F2.0 (B/W)
Power requirements:	12VDC 300MAh
Enclosure Dimensions:	9.5” (H) x 1.5” (D) x 6.5” (H)
Camera iris:	ELC light compensation
Imaging device:	1/3” CCD Grade 1st
Book Camera Specifications:	
Warranty	1 Year parts and labor warranty (standard)
Scanning System:	2:1 Interlace
Electronic Shutter:	1/60~1/10,000,000 Sec. Automatic
Operating Temperature:	-10ºC~50ºC
S/N Ratio:	More than 50dB
Signal System:	E:EIA 60Hz
USBVIDEO RCA CABLE	RCA Video Cable for Connecting Receiver
PS12V	Camera and Receiver Power Supplies
PVBATT/CHRG/KIT	

Table 5.2. PVBOOK700 Specifications. From ID 2000

PVCOMPSPEAKERS700

PVREC700LCDMON	Wireless 4 Channel 2.4Ghz Receiver With built-in Color Video Monitor
PVREC700	Wireless, 4 Channel, 2.4Ghz Receiver
Transmitter Specifications:	
Transmitting frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Transmitted power:	10mw (max)
Video format:	NTSC or PAL
Receiver Specifications:	
Video output:	RCA/SCART—jack 1 Vp-p
Stereo audio output:	left/right RCA/SCART– jack 1 Vp-p
Operation frequency:	2.4—2.483 GHz (4 channel)
Modulation:	FM
Receiver sensitivity:	80 dBm
Dimensions:	155mm x 80mm x 41mm
Video format:	NTSC or PAL
Power Requirements:	+12VDC 500mA (max)
Operating Conditions:	Indoor use only
Resolution:	380 TV Lines (Color) - 420 TV Lines (B/W)
Lens:	90° f3.8mm pinhole lens
Low light compensation:	1 lux, F2.0 (Color) - 0.1 lux, F2.0 (B/W)
Power requirements:	115 VAC
Enclosure Dimensions:	8.5” (H) x 3” (W) x 5.5” (D)
Camera iris:	ELC light compensation
Imaging device:	1/3” CCD Grade 1st
Amplifier Output	3W + 3W
Frequency Response	80Hz – 20 kHz
Input Sensitivity	200mV
Speaker Unit	21/2” Cone (6.5cm), Full Range with magnetic shielding
Computer Speakers Camera Specifications:	
Warranty	1 Year parts and labor warranty (standard)
Scanning System:	2:1 Interlace
Electronic Shutter:	1/60~1/10,000,000 Sec. Automatic
Operating Temperature:	-10ºC~50ºC
S/N Ratio:	More than 50dB
Signal System:	E:EIA 60Hz
USBVIDEO RCA CABLE	RCA Video Cable for Connecting Receiver
PS12V	Camera and Receiver Power Supplies

Table 5.3. PVBOOK 700 Camera.

3. Dazzle Digital Video Creator 80 Hardware (DVC 80)

The Dazzle Digital Video Creator Hardware provides interoperability between the camera and computer. It transfers the images from the camera to the facial recognition software application. The DVC 80 consists of an USB to RCA Video Capture Device with a RCA, video, and USB inputs. The Digital Video Creator hardware also has a software application that serves as a video editing tool. The primary goal of the DVC 80 is to provide interoperability of surveillance cameras and send imaging info to the database. With the cameras strategically placed, they would provide optimum coverage of the GIGA LAB with limited blind spots.

In addition to interoperability, the DVC 80 provides three different operation formats for cameras. The PVCOMPSPEAKER, PVCLOCK, and PVBOOK 700 cameras all operated on the composite format. The Composite format transmits all video information using a single wire. The Cannon GL 1 camera operates on the S-Video format. The S-Video format transmits luminance and color information on two separate wires, producing a higher quality image than Composite. The RGB format transmits video information on three separate wires, producing a higher quality image than Composite or S-Video but there is no camera in the UbiSurv testbed that utilizes the RGB format.

C. NETWORK COMPONENTS

1. Desktop Workstation/Server

The main monitoring station is a Dell Dimension 4500 desktop workstation. The desktop also serves as the server for the ID-2000 database and cameras. The wireless network service is supplied by the Naval Postgraduate School network. Inside the GIGA LAB there is a Linksys wireless router and three access points. The desktop connects through the wireless network via the access point. In a larger scenario, the desktop represents the Network Operating Center.

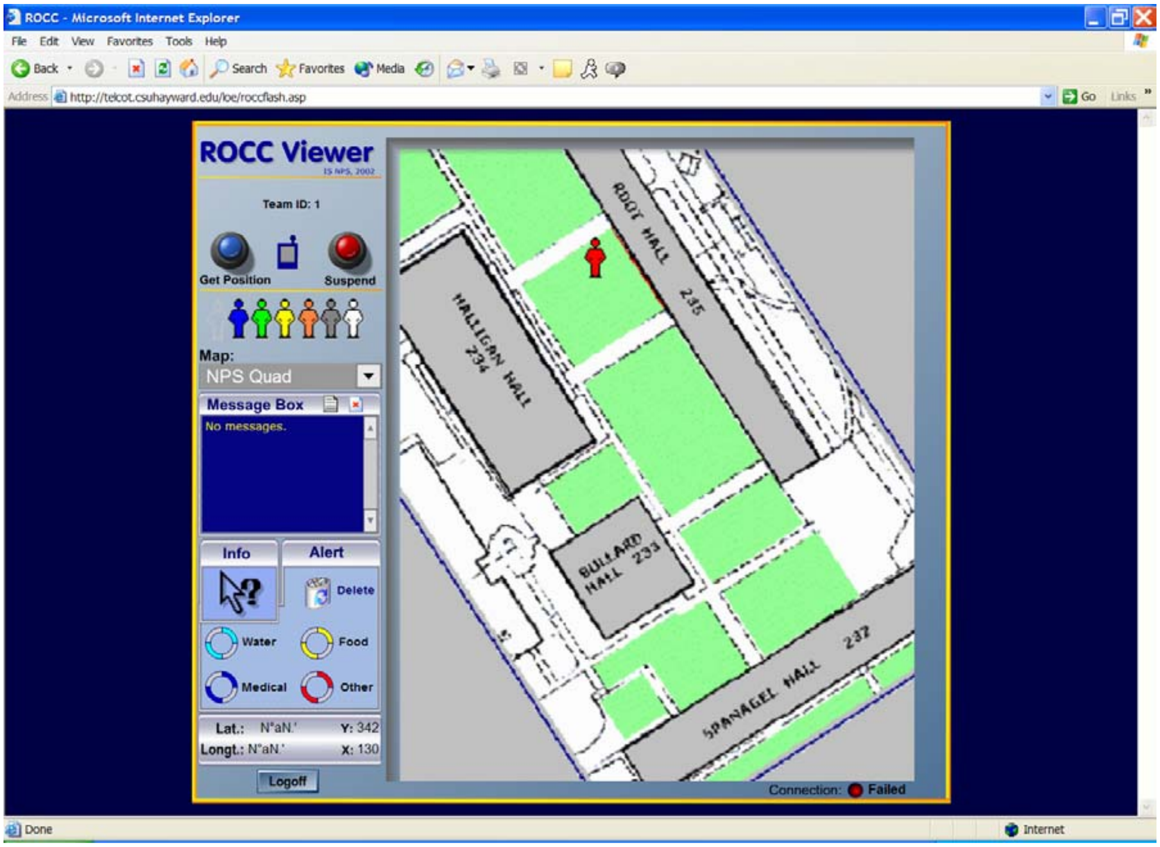
2. Mobile Nodes

One of the testbed mobile nodes is a Dell Inspiron 8200 laptop. The laptop serves as a client for the ID -2000 software. The biggest difference between the client and the server is the server holds the database image. The operator can add, probe, delete, and edit images utilizing the software depending on the privileges. As long as the laptop has an Internet connection it can monitor the network. This allows the operator to monitor the testbed from anywhere.

Another mobile node of the testbed is the Compaq iPaq(pocketpc). The iPaq is also equipped with the Pocket PC 5800 camera, GPS receiver, network access card, and expansion pack. These accessories allow the iPaq to remain connected to the network, serve as a monitoring node, and serve as a node for the ROCC software. The iPaq can also communicate with other iPaqs using instant messaging software. Software installed on the iPaq is the Teletype GPS. This allows the iPaq to be tracked when by the ROCC viewer software when it is outside the GIGA LAB.

D. SITUATIONAL AWARENESS SOFTWARE

The Relief Operations Coordinating Center (ROCC) Situation Awareness tool designed by Eugene Buorgkov is software that monitors areas outside the GIGA LAB. In the case of the UbiSurv testbed it monitors the NPS quad. The tools needed to run the software are a GPS receiver and an Internet capable device. The ROCC viewer allows mobile nodes to communicate with each other and the NOC in the GIGA LAB. GPS allows every node within the network to know the physical location of the other. The instant messaging aspect allows operators to communicate with other and send alerts. Any map can be downloaded on the ROCC viewer which allows any area in the world to be viewed by the software.



Address http://telcot.csuhayward.edu/loe/roccflash.asp

Team ID: 1

Map: NPS Quad

No messages.

Lat.: N°aN.' Y: 342

Longt.: N°aN.' X: 130

Connection: Failed

Figure 5.2. ROCC View Situational Awareness Software.

E. NETWORK MANAGEMENT SOFTWARE

The UbiSurv uses the Solar Winds Orion Network Performance Monitor Software. Solar Winds monitors percent of bandwidth utilized, memory utilized, CPU utilized, disk space utilized. It can also be configured to alert and report parameter violations and send email to any compatible device, including cell phones. The event monitor allows you to view events sorted by device name, type, and date period. Solar Winds is designed to monitor the state of the UbiSurv testbed at all times.

F. IMAGIS ID 2000 SDK SOFTWARE APPLICATION

ID-2000 uses a 3-dimensional deformable surface model to first locate the face within the image. The surface model is built from a series of deformations that ID-2000 can dynamically apply to the model while the face finding and fitting execute.

Starting from a default surface, the encoding process applies deformations within the spatial orientations of pitch, roll, and yaw of the head. At the same time, the surface model is re-rendered to different light source positions to achieve a best fit to the face.

Once the encoding procedure finds the best fit for the entire surface, selected smaller sub-regions are used to perform a more localized and finely tuned fit to the features of interest – the eyes and nose. ID-2000 uses these features of interest to establish the coordinate system for the final encoding. There are two types of images enrolled and probe images. Enrolled images are those images that ID-2000 has encoded and stored in the database. Probe images are those images ID-2000 queries the database with. The image requirements for enrolled and probe images are similar. ID-2000 recognizes photographs, live or recorded video, and digital video files. The software can also encode and conduct searches on artist rendered images.

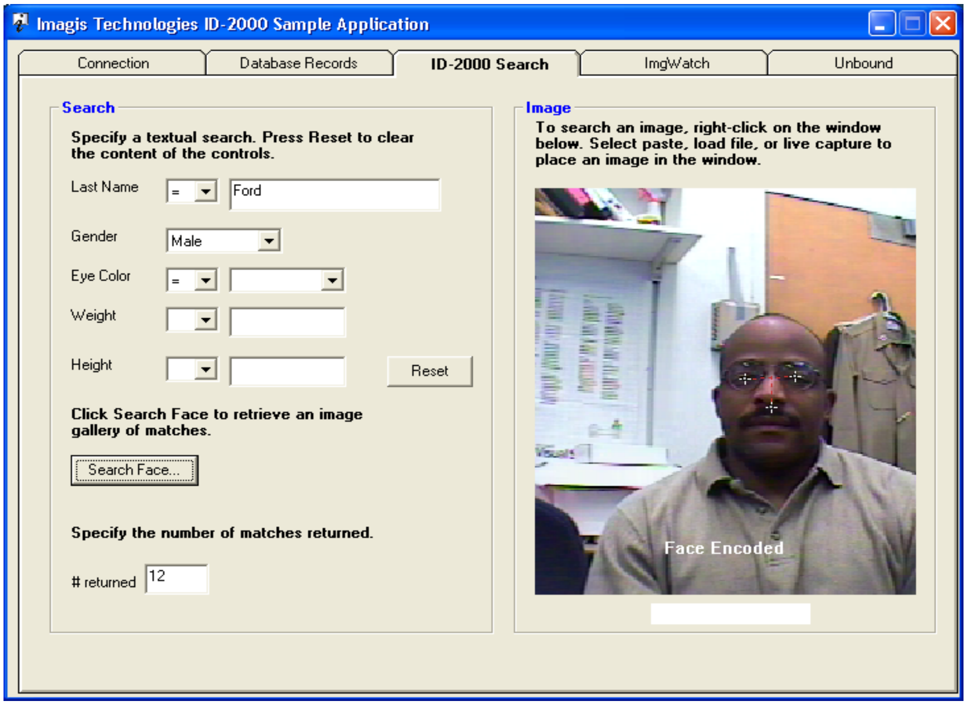
The final encoding utilizes spectral filters at various sizes, frequencies, and orientations to produce an array of coefficients. ID-2000 applies these filters to the captured face using a coordinate system configured from the eyes and nose locations. The coefficients generated from the final encoding are collectively described as the encode array. When ID-2000 first enrolls a subject in the system, the system stores the subject's encode array along with their record identifier in the database. Later, during recognition, ID-2000 again generates the subject's encode array and matches the array against the previously enrolled subjects to produce a sorted list of top matches.[53]

We obtained a temporary license from Imagis Technologies to use in the UbiSurv testbed. The software has the ability to connect to a Microsoft Access, Oracle and SQL database servers. ID 2000 has a client/server capability and can scale and accommodate tens of millions of user records. The software is an easy to use and understand database. It enables captured images from all sensors to be implemented into the system, stored and retrieved when a match has been determined. The software has great potential, although, not a three-dimensional (3-D) system, we can still have the 3-D affect by taking three images of an individual. The images taken must be head on, approximately twenty degrees to the right and twenty degrees to the left.

1. Search Tab

The ID-2000 Search tab is designed to search for an image already in a database. The subject is input into the image block as shown in Figure 5.3.

[53] ID-2000 Technical Resource Guide, p. 6.



Search

Specify a textual search. Press Reset to clear the content of the controls.

Last Name = Ford

Gender Male

Eye Color =

Weight

Height

Click Search Face to retrieve an image gallery of matches.

Specify the number of matches returned.

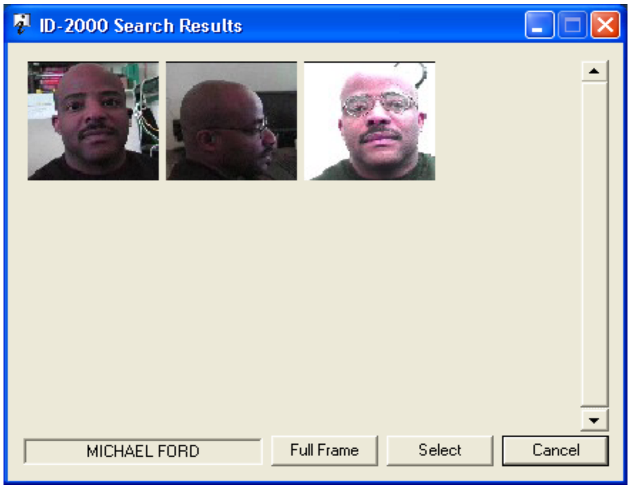
returned 12

Image

To search an image, right-click on the window below. Select paste, load file, or live capture to place an image in the window.

Figure 5.3. ID 2000 Search Tab Template.

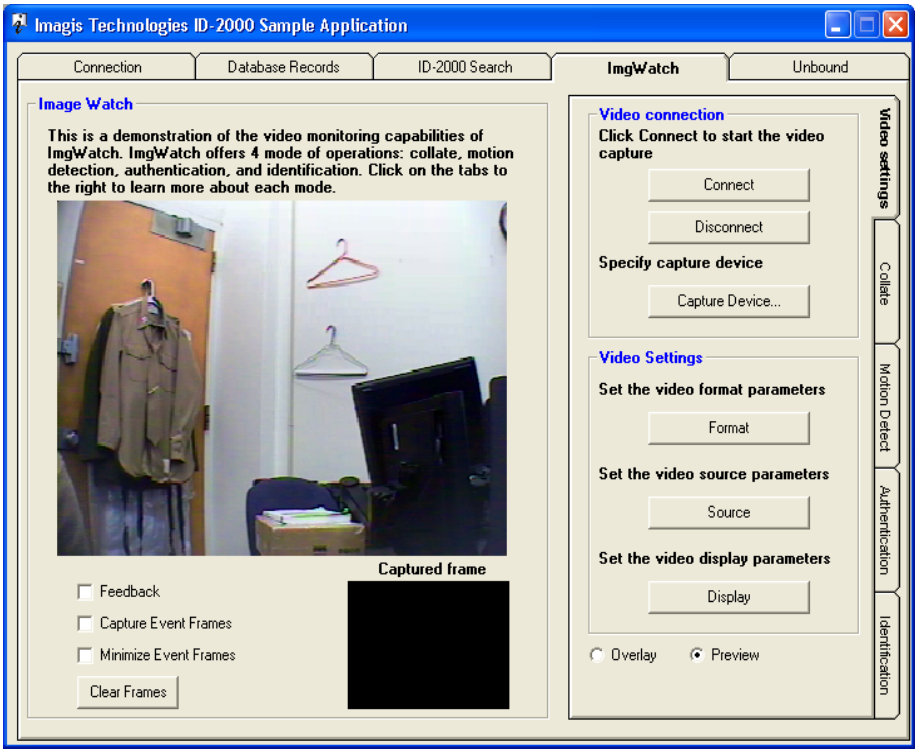
The image block is capable of holding a live video image, still photo, or an image from a database. The expected successful result should look like Figure 5.4.



MICHAEL FORD

Figure 5.4. Successful Search Result on Subject.

The ImgWatch tab has four video monitoring capabilities: Collate, Motion Detect, Authentication, and Identification. The ImgWatch template also has a video settings tab that allows the user to connect to the designated camera, specify which camera to use for event capturing, and format the video imagery.



This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

□ Feedback
□ Capture Event Frames
□ Minimize Event Frames

Click Connect to start the video capture

Specify capture device

Set the video format parameters

Set the video source parameters

Set the video display parameters

○ Overlay ● Preview

Figure 5.5 Video Settings Tab.

The Video Stream Control is the picture box on the upper left side of the tab. It shows the video input. The check boxes below the Video Stream Control apply to all four modes of operation. “Feedback allows you to easily see the motion causing the events to trigger. Capture Event Frames allows you to view the frame that triggered an event. The Captured frame window displays the frame in question. Minimize Event Frames Allows you to save each captured frame in a separate window. The application will create a new minimized window for each captured frame.”[54]

2. Collate

The collate mode compares live video with a reference frame or series of reference frame. The Video Stream Control will alarm if it sense a difference between the live video and the reference frames.

[54] ID 2000 Technical Resource Guide.

> The Threshold field controls the frequency of an event from the Video Stream Control. When the correlation between the reference frame(s) and the live capture falls below the specified threshold, the control will fire an event. The box at the bottom of the tab displays the correlation between the two frames.[55]

When the correlation drops below the threshold, the OnNoCollation event is fired, indicating the scene has been disturbed. When the correlation rises above the threshold the OnCollation event is fired indicating that the scene has returned to normal.

When in Collate mode, the Video Stream Control displays a red and blue bar at the bottom of the control. The bar designates the present correlation between the reference frames and the live capture. If the current correlation is above the threshold value, the portion between the threshold and the current correlation is blue. The portion below the threshold is red.

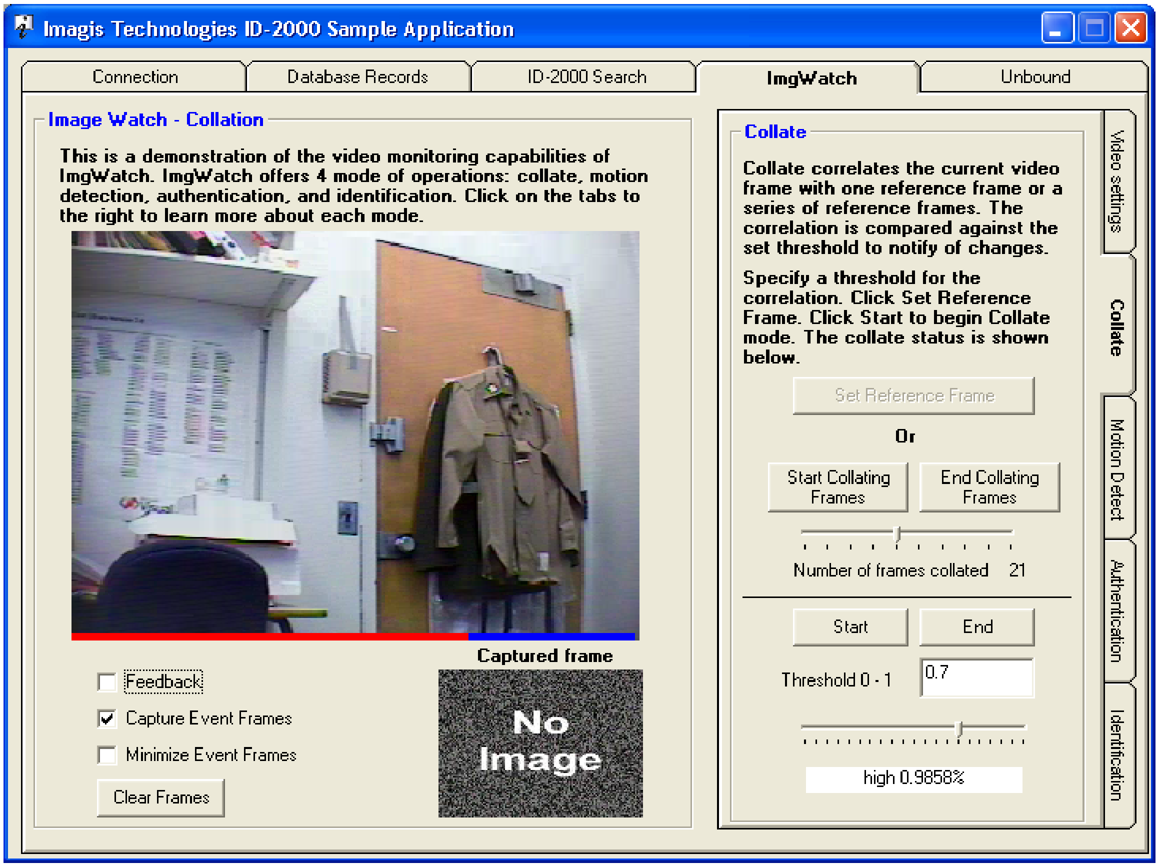


Image Watch - Collation

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

☐ Feedback

☑ Capture Event Frames

☐ Minimize Event Frames

Collate

Collate correlates the current video frame with one reference frame or a series of reference frames. The correlation is compared against the set threshold to notify of changes.

Specify a threshold for the correlation. Click Set Reference Frame. Click Start to begin Collate mode. The collate status is shown below.

Number of frames collated 21

Threshold 0 - 1 0.7

high 0.9858%

Figure 5.6. The Collate Tab.

[55] ID 2000 Technical Resource Guide, p. 40.

The bottom line indicates the current correlation level. The red area indicates the current threshold setting. The blue area indicates the difference between the current correlation and the threshold. The collate option gives the UbiSurv testbed the capability to serve as an intrusion detection system into the GIGA LAB, or observe extraordinary events. If an event occurs that does not correlate to the reference frame a feedback alarm goes off and indicates the difference in the captured frame box. The Alarm can be sent via email or trigger other safety features in the testbed.

3. Motion Detect

Motion Detection mode evaluates succeeding video frames, allowing motion tracking for a scene. When the Video Stream Control detects motion, the control will trigger an event. The Sensitivity field allows the user to denote the sensitivity of the detection. The higher the sensitivity, the less motion required to generate an alarm. Also, the Video Stream Control displays a red dot in the center of the area where it has detected motion.

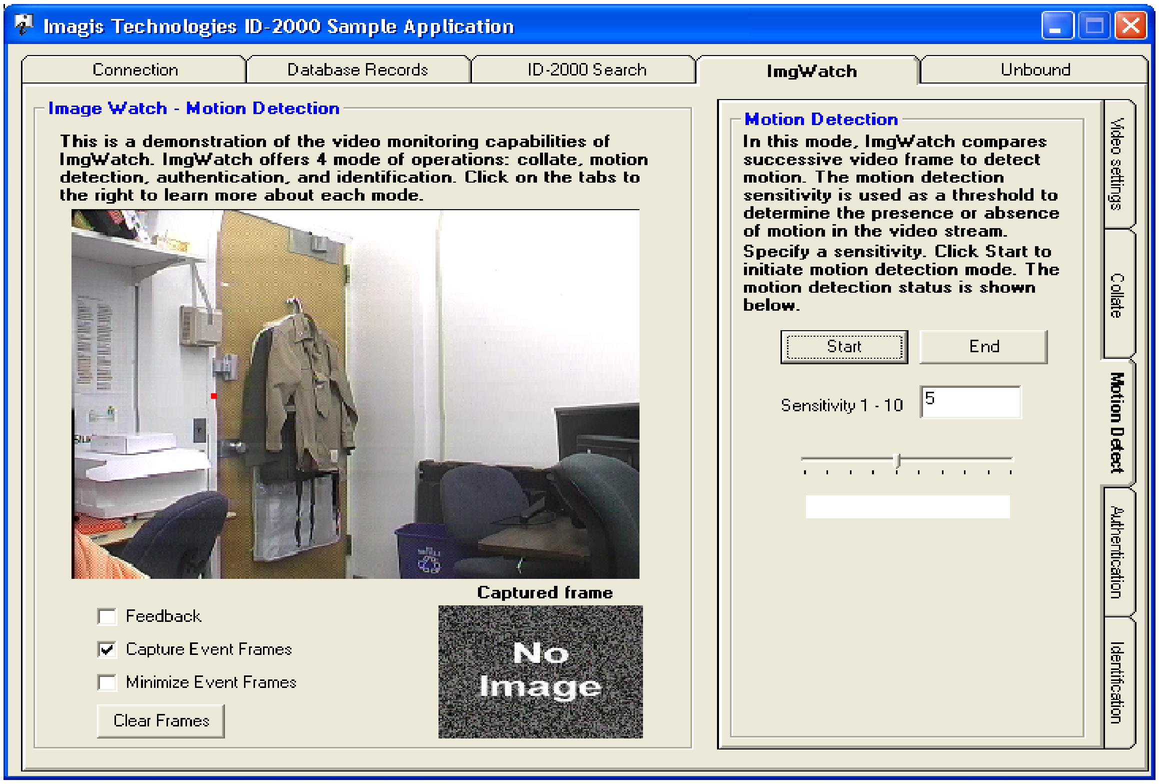


Image Watch - Motion Detection

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

☐ Feedback

☑ Capture Event Frames

☐ Minimize Event Frames

Motion Detection

In this mode, ImgWatch compares successive video frame to detect motion. The motion detection sensitivity is used as a threshold to determine the presence or absence of motion in the video stream. Specify a sensitivity. Click Start to initiate motion detection mode. The motion detection status is shown below.

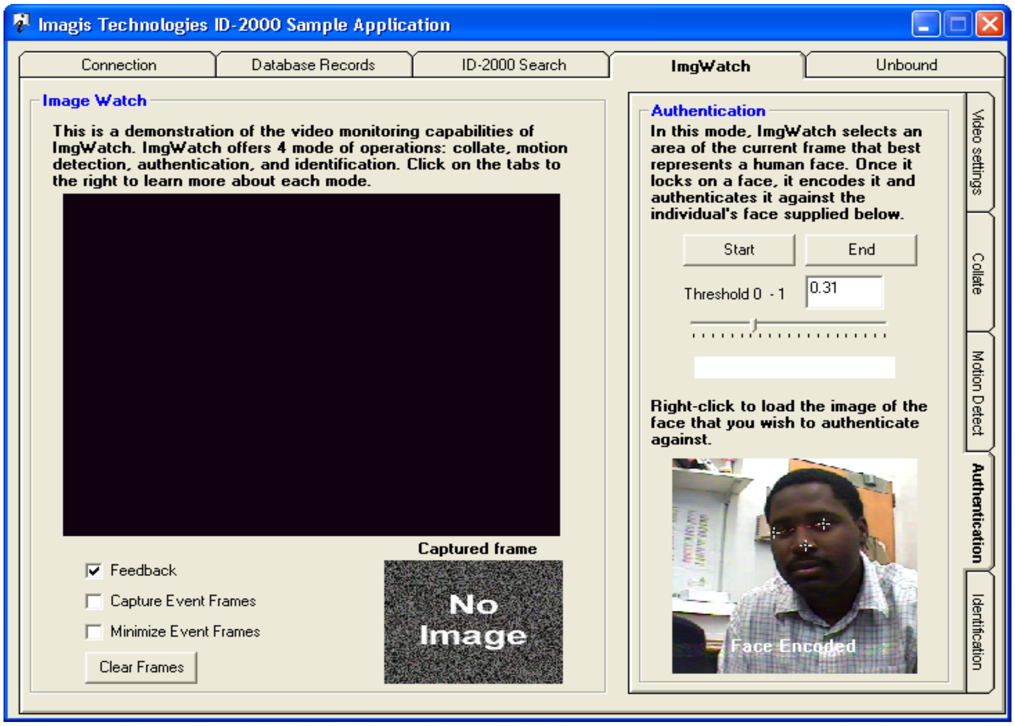
Sensitivity 1 - 10: 5

Figure 5.7. Motion Detection Tab.

The control has detected the motion by comparing successive frames that occurred between the right and left image. A red square is drawn at the center of the area where the motion occurred. As long as motion occurs, the red square remains visible. When motion stops occurring, the red square disappears and the OnNoMotion event is fired. When the red square becomes visible again, the OnMotion event is fired.

4. Authentication

Authentication mode allows the user to investigate a scene for a particular individual, also known as a one-to-one search. Once the Video Stream Control discovers the individual of interest, the control will activate an alarm. The Threshold field allows for sensitivity adjustment. The Threshold field allows you to specify the sensitivity. The higher the threshold value, the closer the match has to be. The Still Image Control at the bottom of the tab allows the user to specify the face to search for in the scene. When the image is properly authenticated the result is shown in the captured frame image box.



This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

In this mode, ImgWatch selects an area of the current frame that best represents a human face. Once it locks on a face, it encodes it and authenticates it against the individual's face supplied below.

Threshold 0 - 1: 0.31

Right-click to load the image of the face that you wish to authenticate against.

☑ Feedback
□ Capture Event Frames
□ Minimize Event Frames

Figure 5.8. The Authentication Tab.

5. Identification

Identification mode searches a scene for a face, and compares it to faces in a database. This is also known as a one-to-many search. Once the Video Stream Control identifies a face in the scene, it searches the database for a match using the identified face as the probe image. The Threshold field specifies the sensitivity of facial recognition. The higher the threshold value, the closer the match has to be. The default is .71. The Top matches windows will display the top four matches returned from the search as shown in Figure 5.9.

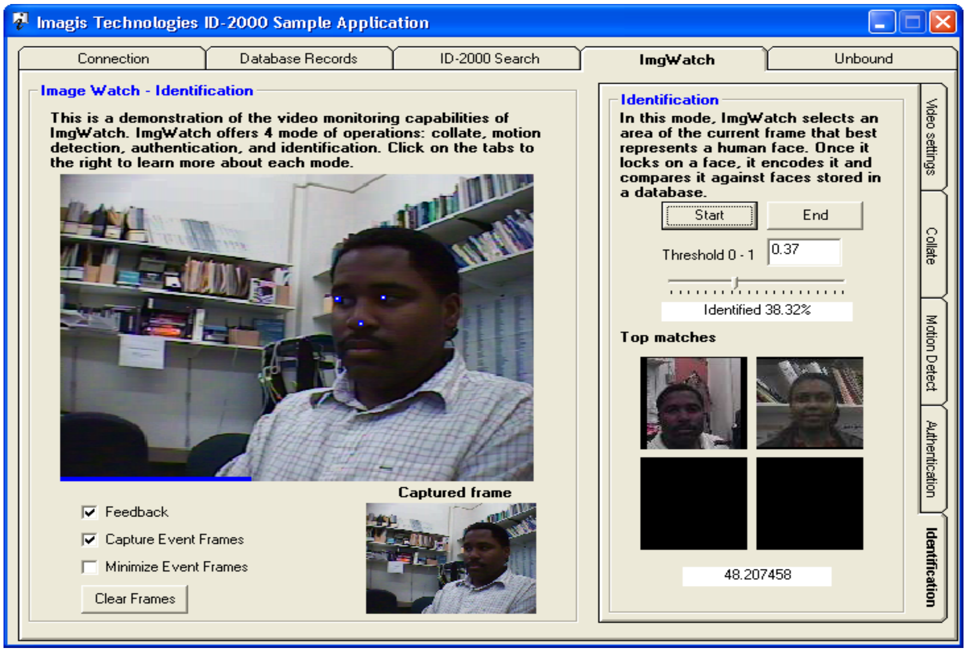


Image Watch - Identification

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

Captured frame

☑ Feedback

☑ Capture Event Frames

☐ Minimize Event Frames

Identification

In this mode, ImgWatch selects an area of the current frame that best represents a human face. Once it locks on a face, it encodes it and compares it against faces stored in a database.

Threshold 0 - 1: 0.37

Identified 38.32%

Top matches

48.207458

Figure 5.9. Identification Tab.

G. EXPECTED RESULTS

The UbiSurv was designed with the intent of conducting actual and constant surveillance of subjects in the Giga Lab. Depending on the criticality of the situation, search time is vital. The formula used to determine search time is: Length of time (in seconds) = 5 X n / 1,000,000. Where n is the number of images in the database. Since the UbiSurv has 100 images in its database, the expected search time for each application is .0005 seconds. In order for the testbed qualify as a ubiquitous habitat, it must be pervasive, embedded, nomadic, adaptable, powerful, intentional and eternal. As far as facial recognition is concerned it, the software application needs to be able to identify subjects at a distance of 10 feet at any angle. Facial hair, glasses, cold sores, swelling and change of hair styles should not hamper the identification process. The software should function equally with races and gender. An expert should not be needed to operate the software. The UbiSurv must also be scalable. Whenever additions, Substitutions, or removal are needed, the UbiSurv should still be able to operate without error. The immediate overall expectation of the UbiSurv testbed is to yield at least a 90% accuracy rate on facial recognition. All cameras in the testbed should yield this accuracy rate when utilized by the facial recognition software.

H. ACTUAL RESULTS

This section focuses on the actual results derived from testing the UbiSurv testbed. Although the setup and implementation was relatively simple it required finesse, exactness and often advice via telephone conversation with the Technical Representative from Imagis Technologies and PalmVID. The primary emphasis in this section will be the methods of capturing images, surveillance, identification, default threshold level and collation.

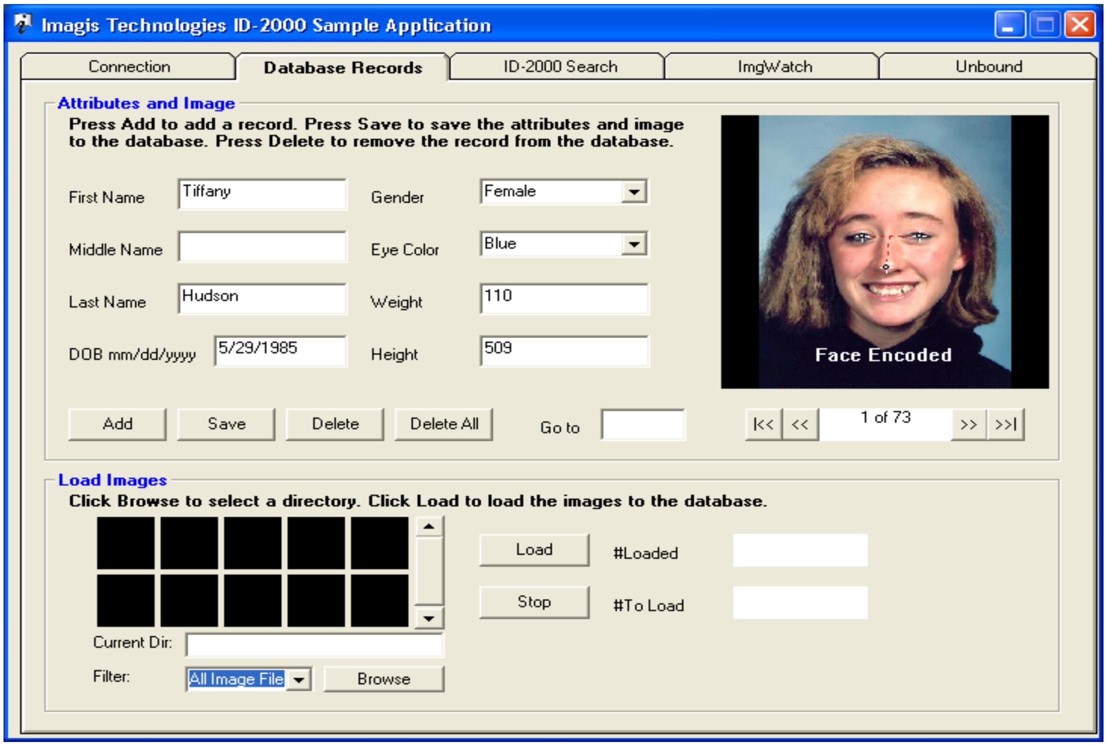
1. Methodology

The primary method of capturing images was conducted using the Canon GL1 Digital video camera. There were several people already working on other projects in the Giga Lab familiar with our project and willing to assist us with the UbiSurv testbed. To improve the accuracy of identification, a head-on shot, a 20 degree angle shot from the left and right were taken of each person enrolled in the database. In order to get good results, we attempted to enroll images as similar as possible to probe image environment. All of the subject's pictures were taken in the UbiSurv testbed room to ensure the scenery, subject resolution, background and lighting are similar. All the images have over 150 pixels in height because the software does not encode images less than 100 pixels in height. All images taken are in JPEG format.

Once the images are taken they are transferred to the computer via the ID-2000 SDK software database records. The process required is as follows:

- Left click Add feature

- Place mouse on photo image on the right and right click
- Scroll down and right click on left click on Capture Live Image
- Once the desired image appears on the computer left click Freeze
- Right Click Paste
- Input the necessary data that will be stored in the database; i.e., name, birthdate, height, weight.
- Save data
- Encode the image



Attributes and Image

Press Add to add a record. Press Save to save the attributes and image to the database. Press Delete to remove the record from the database.

First Name: Tiffany
Gender: Female
Middle Name:
Eye Color: Blue
Last Name: Hudson
Weight: 110
DOB mm/dd/yyyy: 5/29/1985
Height: 509

1 of 73

Load Images

Click Browse to select a directory. Click Load to load the images to the database.

Current Dir:
Filter: All Image File

Figure 5.10. Database Record Template.

2. Identification Tab Performance Evaluation

We took our first observation on the Identification tab. Our initial results showed that a slow and inaccurate return on matches from the database. ID-2000 SDK software has a default threshold level of .71. Webster defines threshold as "a level, point or value above which something is true or will take place and below which it is not or will not."[56] The highest recommended threshold level from Imagis is .90. Initial testing revealed that

[56] Webster's Ninth New Collegiate Dictionary, MERRIAM-WEBSTER INC., Publishers, Springfield, Massachusetts, 1986, p. 1229.

the system did not provide a positive match when the threshold level was set on default. Once we lowered the threshold to .55 we started to receive accurate matches. The .55 threshold level is well below the expected results set for the UbiSurv testbed and for facial recognition systems.

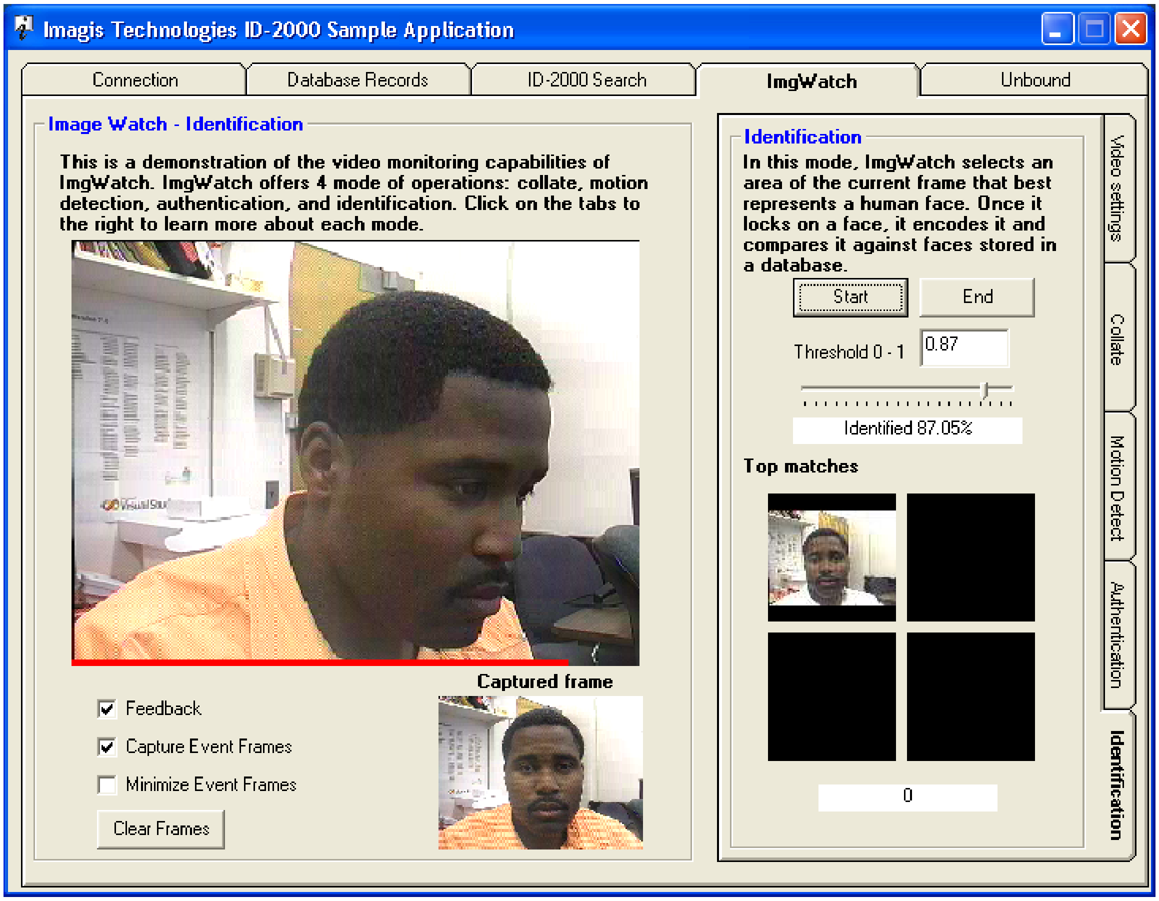
After talking to Jason Close, who is Imagis Technologies' head Technical expert, we learned that the size of the face in the frame is also a major in factor proper facial recognition. If the face is small in the frame, chances of the ID-2000 properly recognizing the subject is minimal. If the face occupies the majority of the image, the chances of the software identify the subject is greater. Jason Close gave us the following guidelines for subject size and location:

- Ensure enrolled image and your probe image have the same number of pixels between the eyes
- The optimum number of pixels between the subject's eyes is 100, however the software can produce satisfactory results with lesser values. The minimum acceptable number is 30. Anything less produces too much chunkiness in the sampling. As the number of pixels between the eyes decrease, it becomes even more important that the enrolled image has the same number of pixels as the probe image.
- The image subject should occupy the majority of the frame area even though ID-2000 will accept faces that occupy between 30-75% of the image area
- Images must have at least an 8-bit image depth
- Do not resize the image in such a way as to change the aspect ratio. This will adversely affect image encoding.
- No part of the subject's head, hair or face should be outside the borders of the image.
- Hair should not cover any part of the eyes or area around the eyes
- The camera height and the height of the subject's eyes should be essentially the same; the subject should be neither looking up or down at severe angles into the camera
- The iris position in the subject's eye sockets is important. The subject should be looking straight ahead.
- ID-2000 finds faces where both eyes are visible. Ideally, the subject should be centered in the image looking generally towards the camera. ID-2000 will find a face with ± 20 degrees of yaw, ± 10 degrees of pitch and ± 20 degrees

a. Problems, Re-Evaluation and Results

Our problem was the faces in our images were either too small or too large. Some of our images have distortion in it which blurred some of the pixels. We adjusted the pixel setting to 320 and captured three images of an individual as previously stated, head-on, twenty degrees left and twenty degrees right. We ensured the subjects face covered 75% of the images. We also edited some of the images by normalizing, equalizing, sharpening, and smoothing to produce a more accurate match at a higher threshold level.

After re-enrolling and editing the images, we perform several evaluations of the Identification tab with the Cannon GL1 camera. The accuracy of the image match improved the highest threshold level we achieve was .89. Glasses, facial hair, hair styles did not hinder proper identification. The software properly identified subjects regardless of race and gender. The software accurately identified subjects at a distance up to seventeen feet at a .88 threshold. It could properly identify subject over twenty feet at lower threshold frequencies. The identification process was also executed in a timely fashion.



This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

In this mode, ImgWatch selects an area of the current frame that best represents a human face. Once it locks on a face, it encodes it and compares it against faces stored in a database.

Threshold 0 - 1: 0.87

Identified 87.05%

0

☑ Feedback

☑ Capture Event Frames

□ Minimize Event Frames

Figure 5.11. Successful Identification of ID Tab.

b. PalmVID Camera Evaluations

We also evaluated the identification tab with the PVCOMPSPEAKERS 700 camera. We got accurate matches at a threshold level of .78. The furthest distance the software would accurately identify subjects was nine feet. Any distance more than that cause the software to take up to forty five seconds to properly identify at lover threshold levels. The PVCOMPSPEAKERS 700 camera could not detect subjects when they wore glasses. If the subject removed his glasses the software immediately identified them.

The PVCLOCK700 produce less accurate results at a threshold level of .75. The accurate recognition did not take place until the subject was a distance of seven feet. The PVCLOCK700 detected subject’s profile shots better than any other angle. The side shot at seven feet produced accurate results with the identification tab. The other two cameras had problems identifying subjects once their face angle exceeded twenty five degrees.

3. Collate Tab Performance Evaluation

Our evaluation scenario for the collate tab was the monitoring of the Giga Lab Door. The reference consisted of 21 collated frames of the door as shown in Figure 5.9. If someone walked through the door we expected the system to alarm. Once the event was in the captured frame we attempted to authenticate the person walking through the door. Also, if the person did not close the door the system would alarm. All alarms were expected to show in the captured frame box. Our evaluation with the Cannon GL1 camera produced marginal results.

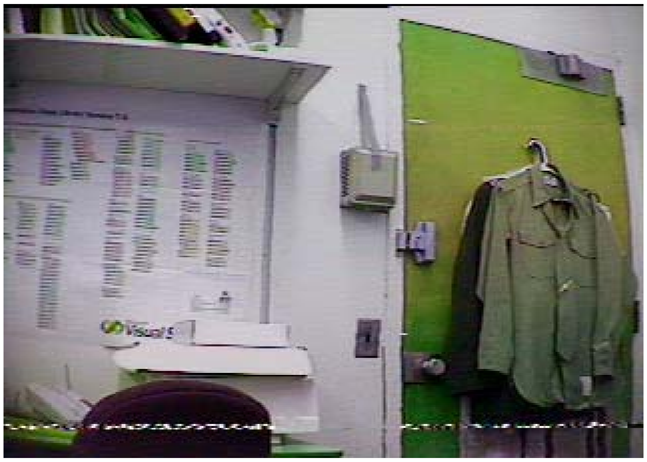


Figure 5.12. Reference Frame.

When the evaluation was conducted with the Cannon GL1 camera, it failed to notice the abnormality of someone walking through the door at the default threshold. Once the threshold was lowered to .43, it observed the abnormality.

a. PVCOMPSPEAKERS 700 Evaluation

When the evaluation was conducted with the PVCOMPSPEAKERS700, the application observed the abnormality immediately at the default threshold as shown in Figure 5.13.

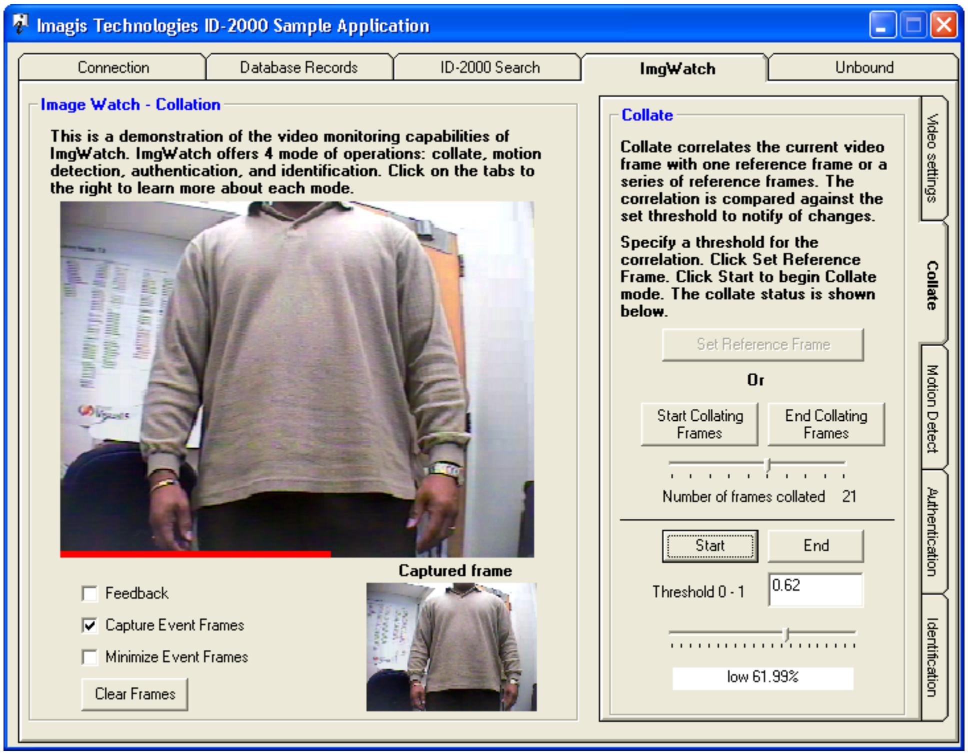

Imagis Technologies ID-2000 Sample Application

Image Watch - Collation

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

Captured frame

☐ Feedback
☑ Capture Event Frames
☐ Minimize Event Frames

Collate

Collate correlates the current video frame with one reference frame or a series of reference frames. The correlation is compared against the set threshold to notify of changes.

Specify a threshold for the correlation. Click Set Reference Frame. Click Start to begin Collate mode. The collate status is shown below.

Number of frames collated 21

Threshold 0 - 1: 0.62

low 61.99%

Figure 5.13. Collate Evaluation with PVCOMPSPEAKERS 700.

b. PVCLOCK and PVBOOK 700 Evaluations

The PVCLOCK700 and PVBOOK700 also determined an abnormality in events. The ID-2000 software could not authenticate anyone coming through the door because the captured event frame rarely showed the subject's face only their body as shown in Figure 5.13.

4. Motion Detection Evaluation

The Cannon GL 1 camera, the software could detect motion easily with a sensitivity level of 10; but, it did not capture frames for review until it was set at threshold level 4.

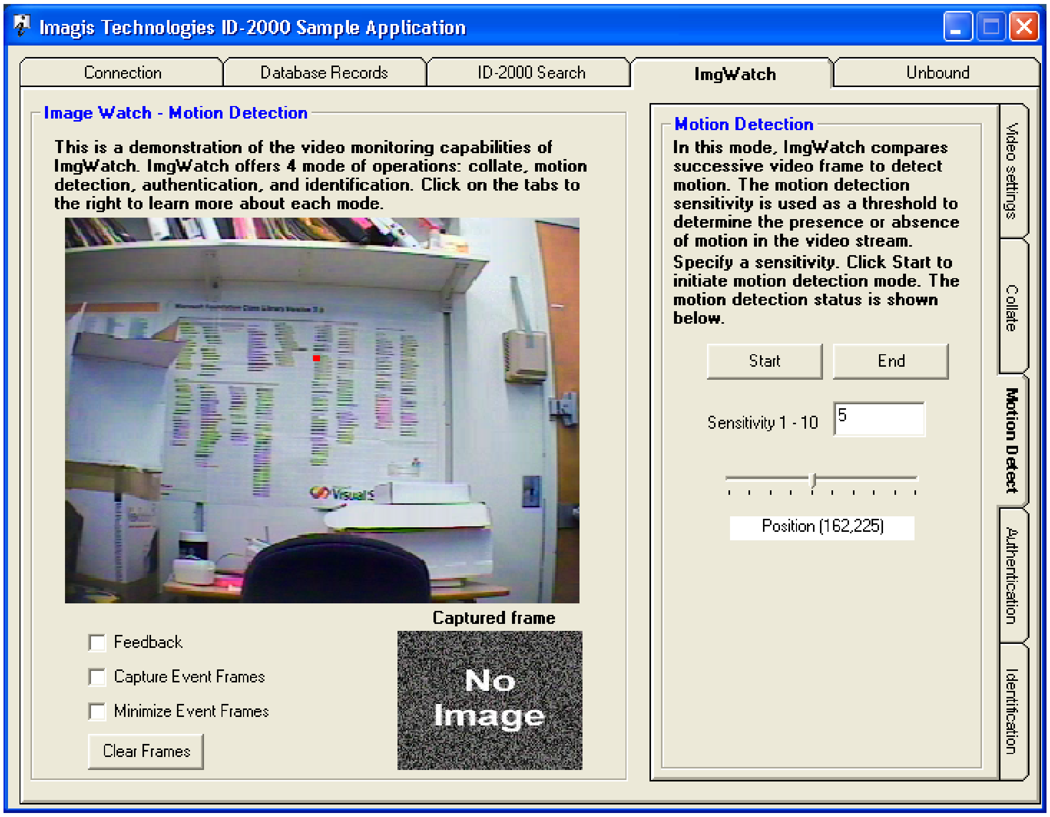


Image Watch - Motion Detection

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

Captured frame

□ Feedback

□ Capture Event Frames

□ Minimize Event Frames

Motion Detection

In this mode, ImgWatch compares successive video frame to detect motion. The motion detection sensitivity is used as a threshold to determine the presence or absence of motion in the video stream.

Specify a sensitivity. Click Start to initiate motion detection mode. The motion detection status is shown below.

Sensitivity 1 - 10 5

Position (162,225)

Figure 5.14. Motion Detection Event.

a. PalmVID Camera Evaluations

The PVCOMPSPEAKERS and PVCLOCK 700 motion detect capability was better than the digital camera. Due to the distortion of the camera, the ID-2000 software would detect false movement and report it as such.

The PVBOOK700 also worked well with the Motion Detect feature. We decided to place the book camera in Dr. Alex Bordetsky's office to test the range of the transmitter. The ID-2000 software worked well and detected motions that were outside of the office like the trees blowing in the wind.

5. Authentication Tab Performance Evaluation

All four cameras worked excellent in Authentication mode. It properly authenticated subjects to the stored images in the database at all thresholds. Glasses, race, gender, facial hair nor hairstyles prevented the software from successfully authenticating subjects. All cameras were able to authenticate subjects at a distance of 10 feet.

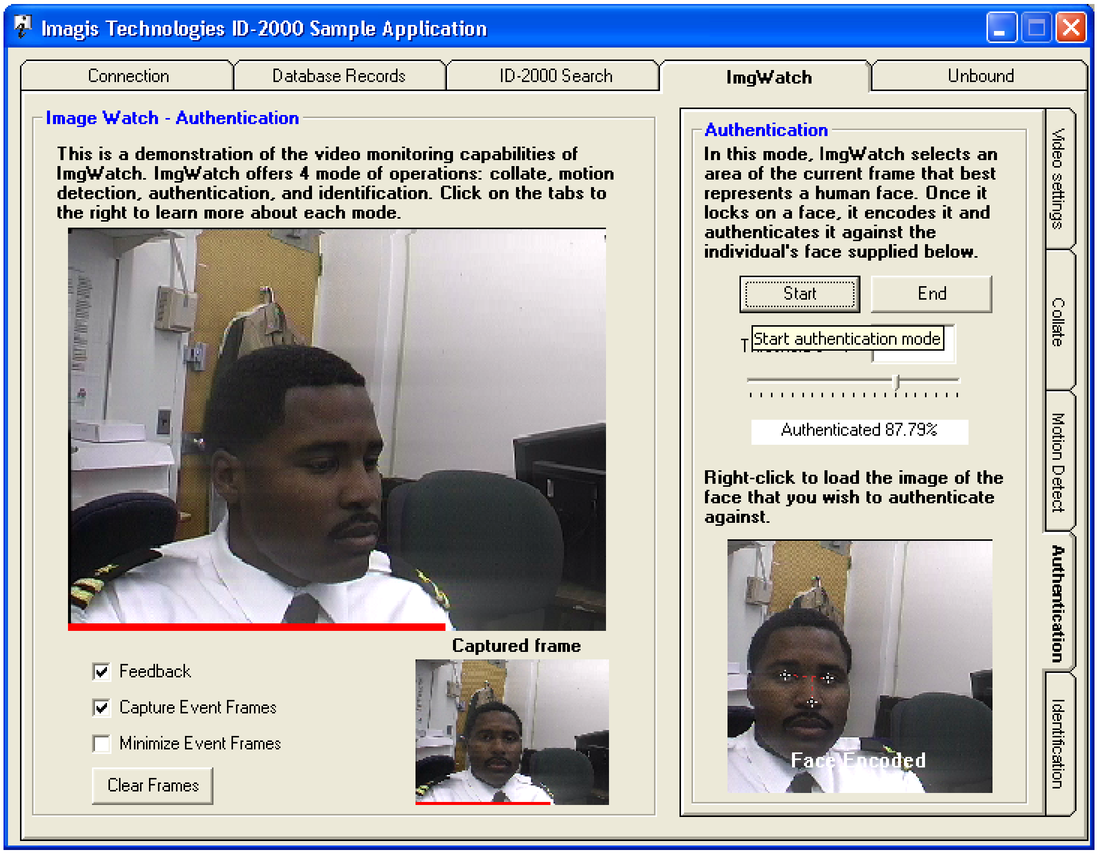


Image Watch - Authentication

This is a demonstration of the video monitoring capabilities of ImgWatch. ImgWatch offers 4 mode of operations: collate, motion detection, authentication, and identification. Click on the tabs to the right to learn more about each mode.

☑ Feedback

☑ Capture Event Frames

□ Minimize Event Frames

Authentication

In this mode, ImgWatch selects an area of the current frame that best represents a human face. Once it locks on a face, it encodes it and authenticates it against the individual's face supplied below.

Authenticated 87.79%

Right-click to load the image of the face that you wish to authenticate against.

Figure 5.15. Successful Authentication of ID-2000.

I. SUMMARY OF EVALUATION

Overall the camera that produced the best results was the Cannon GL 1. For an image to hold meaningful data, the camera must provide a clear, undistorted image and high quality signal source. Lens quality was crucial to providing clear, unvarnished imagery. The Palm VID camera lenses sometimes distorted the image giving it a “fish eye” effect which reduced matching accuracy. Cannon GL1 camera has a lighting compensation mechanism, and a manual iris override option to accommodate intensity. These features greatly enhance the accuracy of the ID-2000 software. Higher quality images produce better results. The main factor behind image quality is: Image format and color, subject resolution and position, lighting, and setting

Lighting was vital when encoding and searching. The Giga Lab presents a control environment where we can ensure pure white light, and subject positioning. Lighting in the Giga Lab prevents shadows and eliminates hot spots on the facial image. In the uncontrolled environment like the office, it was harder for the software to recognize subjects because of the changing effects of lighting and non compliance of subject positioning.

At extreme angles, the software experienced great trouble identifying subjects. Extreme angles include directly overhead, from below or from behind. The height of subjects produces different results. Taller subjects overall produced less accurate matches than shorter subjects. Camera positioning also played a role in this phenomenon. Color balance did not play a critical role like light intensity, because images are reduced to grayscale for encoding. Eyeglasses and sunglasses hid key features and reduced recognition quality. When the probe image had eyeglasses and the enrolled image does not or vice versa the software had a very hard time finding matches. The ID-2000 can produce matches with glasses provided the eyes are visible and not occluded by dark tints or glare. Thick frames also affected search results. High resolution scanned images and digital camera captures of photographs do not produce matches of any kind when probed

The ID-2000 software worked well with all races and genders. Facial hair growth had a small effect on accuracy but hair styles did not results. The more enrolled images of a subject, the better the results. Subjects who had one image enrolled in the database produced less accurate matches than those who had multiple images enrolled in the database.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY

This thesis has provided a thorough evaluation for the early development of the UbiSurv. There are a conglomeration of issues surrounding the evolving efforts on the path to homeland security and the potential uses of various surveillance and biometric technologies. In the post-analysis, the research reveals that the technological advances in surveillance are a natural and predictable evolution for managing the threats to security. The UbiSurv testbed has the potential to be a useful sensor-rich pervasive computing habitat that performs many useful functions for the Department of Homeland Security and Department of Defense. There is a need to continue to improve on the current specialized technologies for the testbed. The Office of Homeland Security's overarching strategy, non-technical human factors and policy also will have a big effect on the UbiSurv testbed.

This chapter will discuss the results of the facial recognition aspect of the UbiSurv, current capabilities and limitations, possible applications of the UbiSurv with other projects, future upgrades, and follow on thesis possibilities.

A. ID 2000 RESULTS

Although the ID 2000 has most of the attributes were looking for, it still leaves a lot to be desired. The software can be fooled if someone has an 8 x 10 size picture of an image that is enrolled in the database. This defeats all other security aspects if a malicious individual ever got a hold of a picture. The ID 2000 does not work well in uncontrolled environments. The Giga Lab provides a nice controlled setting where the environment does not change and subjects are compliant. If the subjects were outside in bright sunlight, overcast skies, in a different environment than the enrolled image, ID 2000 experienced problems detecting the subject. In order to achieve matches at accuracy over .9, the subject had to look directly into the camera. Subjects in an uncontrolled UbiSurv environment will most likely not know where the camera is. Therefore they may not ever look directly into the camera. The UbiSurv needs facial recognition software that is three-dimensional and accurately detect subjects at mostly all angles in a controlled or uncontrolled environment. Also, the facial recognition software should be able to accurately detect subjects at a minimum distance of ten feet.

The ID 2000 can operate on Windows 98, NT, ME, 2000, and XP platforms. The UbiSurv testbed maybe better suited for facial recognition software that can operate on a Windows CE platform. This would allow the software to operate on mobile platforms like PDAs. The ID-2000 also comes with a programmer's resource guide which allows you to write your own program and implement it into the software. This is an important feature because it allows us to tailor the software application to perform our standards.

B. UBIQUITOUS HABITAT COMPARISON

1. Pervasive

The current setup of the UbiSurv is pervasive within the range of the 802.11b standard. Many of the nodes are portable and use the same information base. The ROCC viewer extends the range of the testbed to anywhere a GPS receiver can be detected.

2. Embedded and Nomadic

The UbiSurv is entrenched and nomadic in and out the Giga Lab. There are sensors embedded in a wall clock, book, computer speaker, and PDA. Subjects were not aware of sensor and locations until informed. The Identification and Authentication process causes no inconvenience the subject because facial recognition is non obtrusive. Testbed managers also access to the testbed at remote locations using a desktop, laptop, or PDA.

3. Adaptable

The UbiSurv has great flexibility and spontaneity. The testbed is currently set up for multi-modal operations. The integration of fingerprinting, iris and retina recognition, gait recognition, and voice recognition components will greatly reduce the false rejection rate and false accuracy rate. UbiSurv can provide access control, intrusion detection, and identification. The UbiSurv is also capable of integrating with the Relief Operations Coordination Center (ROCC) situational awareness application. The UbiSurv will also become a part of a Special Operation student's thesis which involves a model Unmanned Vehicle utilizing the collate function of the ID-2000 to monitor a geographic area. The components of the UbiSurv can easily be placed in another environment and work just as well as if it was in the Giga Lab.

4. Powerful

The UbiSurv is currently not powerful enough because of camera resolution limitations. Evaluations revealed the ID-2000 experienced a hard time probing images from the PalmVID camera video control stream when the subject was at a distance greater than five feet. Embedded cameras need to have stronger resolution, which would enable the facial recognition software to make accurate matches.

5. Eternal

The UbiSurv is far from meeting the demands of eternal. Currently there is no back up power supply to the testbed. If power is lost, all UbiSurv components will be temporarily interrupted until power is restored. If a denial of service occurred on the wireless network side of the UbiSurv, there are no contingencies in place to counter. The UbiSurv cannot provide constant 24/7 surveillance due to lack of a sufficient camera server, the battery operated PVBOOK700, and the embedded power save function of the Cannon GL1. The current camera server, DVC 80, is capable of displaying one camera view simultaneously. Although components of the UbiSurv are mobile and adaptable, it lacks redundancy needed for continuous surveillance.

C. RECOMMENDATIONS FOR SUCCESS

Future components of the UbiSurv must endure more than testing in a controlled environment. The sensors and components must perform flawlessly under various environmental conditions, lighting, distances, and other factors that cannot be replicated in a lab. The testbed must also overcome the challenges of multiple and uncooperative subject identification. In real world situations, biometric devices cannot be dependent on a subject always being in the perfect position for probing.

1. Surveillance and Biometric Application Standards

In order for the testbed to be successfully integrated into an enterprise model, standards must be set for biometric applications. Integrity and interoperability of information are key issues regarding ubiquitous surveillance. Biometric standards must be clear and sanctioned formats. They must also address physical and logical security concerns, including digital encryption.

a. The Bio Application Programming Interface (BioAPI) Standard

The biometric industry has over "150 different vendors which most of them use different interfaces, algorithms and data structure. The BioAPI standard is an open-systems standard developed by a consortium of more than 60 vendors and government agencies."[57] The standard requires each biometric application perform the same functions like enrollment of subjects, identifications and authentication. There are other standards that are critical to the success of biometrics. Microsoft who originated the BioAPI standard dropped it and formed another standard called BAPI. The Common Biometric Exchange File Format "defines a common means of exchanging and storing templates collected from a variety of biometric devices."[58] Biometric Assurance is the confidence that a biometric device can achieve the intended level of security. Currently there is no standard testbed that can measure the different technologies. What may work in one scenario may miserably fail in another.

b. Multi-Modal Functions

The UbiSurv must become a multi-modal biometric system that is convenient and flexible enough to identify and authenticate subjects combining several biometric applications. "To date, there have been systems performing authentication by combining multiple biometrics methods. However, biometric methods and combined judgment operations have been fixed for these systems, and there have not been systems capable of flexibly changing between/among biometrics methods and combined judgment operations."[59] The UbiSurv must operate with these characteristics in order to ensure its success when placed in an uncontrolled environment. If the UbiSurv has the ability to choose the two most optimal biometric applications for a scenario, the chances of accurate identification and authentication are increased.

[57] FindBIOMETRICS.com Complete Identification Verification Resource, "A Practical Guide to Biometric Security Technology, 'Uses for Biometrics'," findBIOMETRICS.com, Available Online, [www.findbiometrics.com/Pages/lead2.html], August 23, 2002.

[58] Ibid.

[59] FindBIOMETRICS.com Complete Identification Verification Resource, "Multi-Modal Biometrics Authentication System," findBIOMETRICS.com, Available Online, [www.findbiometrics.com/Pages/multimodal%20articles/multi_2.html], August 2002.

c. *Biometric Technology Selection*

Different scenarios will call for different biometric technologies and applications. Choosing the right biometric application is vital to the UbiSurv's success. Error incidence, accuracy, cost, user acceptance, security level, and stability are all factors that need to be considered when choosing products. Failure to do so may degrade the maturation of the testbed.

D. FUTURE UPGRADES AND ENHANCEMENTS

The planned upgrades and enhancements for the UbiSurv includes a camera server capable of providing multiple inputs and monitoring capabilities. More robust three-dimensional facial recognition software is highly recommended. Geometrics, Tridenity, and HNeT are the leading vendors in three-dimensional facial recognition software. Also future plans involve fingerprinting, iris and retina recognition, gait recognition, and voice recognition applications and components. Stronger WEP encryption application for the wireless LAN portion of the UbiSurv is also planned. The wireless security application Air Defense provides the best security suitable for the UbiSurv. A UPS is also planned for future installation into the UbiSurv. This will provide a backup power supply in the event of power failure. The Canon DL1 camera also shuts off when it is not actually recording after five minutes.

1. Sensor Enhancements

a. *Cameras*

Cameras are the first layer of the UbiSurv. The UbiSurv needs video forensic tools, "smart" cameras, to improve its facial recognition capability. New advances in digital video and video forensic tools (like Sarnoff Corporation's Video Detective) and various products from companies (such as Avid Technology and Ocean Systems) provide agents with new methods to extract clear pictures of surveillance scenes and suspects from poor-quality images. By digitizing analog video images and processing them through PCs, video tapes can be stabilized so that it is easier to follow a suspect in a video clip, extract license plate numbers hidden in shadows, or filter out rain and snow in a background to have a better view of an image scene

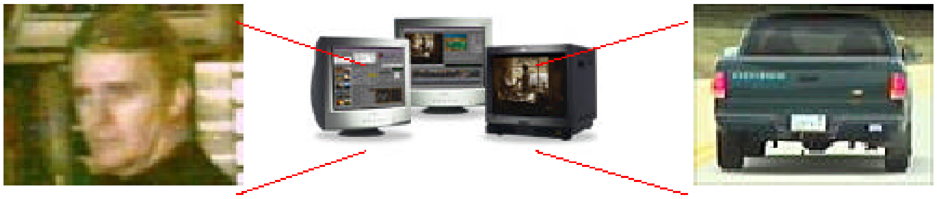


Figure 6.2. Video Forensic Tools. (From: Sarnoff, 1 Apr 2002 & Avid, 19 Jun 2002).

The use of “smart” cameras can aid in monitoring large areas such as the Naval Postgraduate School campus. The Sarnoff Corporation, located in Princeton, N.J., has “developed advanced video microprocessors that along with developed computer algorithms could allow security cameras to monitor an area, recognize suspicious behavior, focus on it, and send an alert if any action is deemed dangerous”[60]

b. Smart Dust

The integration of Smart Dust in the UbiSurv would vastly increase its range and autonomy. Smart Dust is defined as “tiny devices containing sensor and communication capabilities.”[61] These tiny sensors are solar, and barometrically powered thus enabling an eternal aspect of the UbiSurv. The sensors can also monitor movement, large geographic areas, and chemical agents. The best aspect of Smart Dust is that it is relatively inexpensive to buy and operate.

c. Project Oxygen

The integration of certain project oxygen entities like the object recognition and tracking and person tracking components would also enhance the efficiency of the UbiSurv. Object tracking “automatically learns to detect limited-domain objects (e.g., people or different kinds of vehicles), etc. in unconstrained scenes using a supervised learning technology.”[62] Object tracking is the perfect solution for scenarios where facial recognition is not practical. Object tracker does not have to have an image of the object in its database to track it. Once it sees it, it inserts the image in its database automatically and begins to track for there. The person tracking system is the equivalent to having GPS indoors. It uses three stereo cameras that create an all encompassing,

[60] Sarnoff, “Video Detective Workstation from PVT Enhances Images for Law Enforcement Use,” April 1, 2002.

[61] McFedries, Paul, “Smart Dust”, October 26, 1999, [http://www.wordspy.com/words/smartdust.asp].

[62] Darrell, Trevor, About Project Oxygen, [http://oxygen.lcs.mit.edu/Vision.html], Jan 13, 2003.

three-dimensional view of a room. Once a person enters the room, the system begins to track the person and compiles biometric information on the subject such as gait, posture, and facial. The person tracking system can receive all this information independent of the person's position. A system like this embedded in an inconspicuous object like a clock, smoke detector, or exit sign would be desirable.

2. Software Improvements

Three-dimensional facial recognition software is important to the maturation of the UbiSurv. Software like Holographic Neural Technology (HNet) looks at the entire face thus producing more accurate probes on subjects. This allows the subject to be accurately probed in various environments, lighting conditions, and positions. HNet can also simultaneously probe four subjects, which would allow subjects to be picked out of crowd.

3. Situational Awareness Improvements

Software that could integrate and the various systems, sensors, and components of the UbiSurv are vital to the success of the UbiSurv. All the future components are capable of providing a copious amount of information. The decision maker has to know what information is vital and what is not. With all the information coming into the UbiSurv NOC, it would be easy for the decision maker to get confused. Situational Awareness and analysis tools crucial in helping the decision maker make the right decision.

E. FOLLOW ON THESIS OPTIONS

Follow on thesis include improvements on the current facial recognition to possibly include access control and extended surveillance ranges. Other opportunities include:

database programming for the UbiSurv
interoperability testing with other Homeland Security programs
integrating other biometric applications into the UbiSurv
integrating web based applications for the UbiSurv
evaluation of UbiSurv in uncontrolled environments
aircraft onboard cabin video surveillance
artificial intelligence
cargo screening technologies
chemical, biological, and nuclear detection technologies
collaborative information sharing technologies
computer forensics
computer modeling and simulation
critical infrastructure protection
decision support systems
enterprise architecture
enterprise storage
foreign policy
fuzzy logic
globalization impact on world conflict
grid computing
human factors in IT implementation
impact of technology on privacy
inference and analytical engines
information warfare
infrastructure protection
international cooperation
knowledge management
managing change in complex organizations
management information bases
medical surveillance technologies
mobile robotic surveillance technology
multi-agent systems
network security for surveillance
neural networks
predictive analysis
project management
smart card technology
terrorist networks
ubiquitous computing
wireless surveillance and mobile
biometric devices

Table 6.1. Recommended Areas for Further Thesis Study. From Makarski, Richard E. and Marrero, Jose A., “A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security”, Master’s Thesis, Naval Postgraduate School, September 2002.

F. CONCLUSION

This chapter provides an overview of facial recognition in the UbiSurv testbed. Facial recognition is all but one aspect of the UbiSurv. There are numerous other technologies that can be implemented into the testbed enhance it. Our research shows that there are major flaws in facial recognition technology that can be supplemented with other biometric applications. Furthermore, emerging biometric, sensor, and network management technologies are conducive to the success of the UbiSurv testbed. The recommendations made in this chapter would transform the testbed into a premier ubiquitous habitat. All of these recommendations may not be feasible for reasons of economic availability and interoperability problems. Nevertheless constant upgrades to the current testbed will greatly benefit the students and faculty at the Naval Postgraduate School and the Department of Homeland Security.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. BIOMETRICS GLOSSARY

Source: I/O Software, Inc., 2002.

Algorithm

A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template is a match.

American National Standards Institute (ANSI)

Established in 1918, ANSI is a voluntary organization that creates standards for the computer industry. The FBI commissioned ANSI to create an image standard for the exchange of fingerprint data between AFIS systems.

Application Programming Interface (API)

A set of services or instructions used to standardize an application.

Attempt

The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Authentication

The action of verifying information such as identity, ownership, or authorization. The preferred biometric term is verification.

Authentication Routine

A cryptographic process used to validate a user, card, terminal, or message contents. Also known as a handshake, the routine uses important data to create a code that can be verified in real time or batch mode. (See verification)

Automated Fingerprint Identification System (AFIS)

A specialized biometric system that compares a single finger image with a database of finger images. In law enforcement, AFIS is used to collect fingerprints from 1920 criminal suspects and crime scenes. In civilian life, fingerprint scanners are used to identify employees, protect sensitive data, etc.

Automatic ID/Auto ID

An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one to-many identification.

Behavioral Biometric

A biometric that is characterized by a behavioral trait that is learned and acquired over time, rather than a physical or physiological characteristic. (contrast with physical biometric)

Bifurcation

A branch made by more than one finger image ridge.

Binning

Taking advantage of different fingerprint pattern classifications to reduce the number of comparisons that must be performed to find a match in an identification system. Enrolled fingerprints that can be classified with a high degree of confidence are assigned to "bins" corresponding to each classification. A submitted print that cannot be classified with high confidence must be matched against all the bins (the entire database), but prints that can be classified need only be matched against the corresponding bin or bins

Biometric

A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric Application Programming Interface (BAPI)

This is an API that allows the programmer to develop applications for a broad range of virtual biometric devices (VBDs) without knowing the specific capabilities of the device. The API is comprised of three distinct levels of functionality from high device abstraction to low (device specific) abstraction.

Biometric System

An automated system capable of capturing a biometric sample from an end user; extracting biometric data from that sample; comparing the biometric data with that contained in one or more reference templates; deciding how well they match; and indicating whether or not an identification or verification of identity has been achieved.

Biometrics

The automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic to a comprehensive database for purposes of identification.

Block Cipher

A symmetric cipher, which encrypts a message by breaking it down into blocks and encrypting each block.

BPI

Bits per inch, as on a magnetic stripe card.

CAPI

Cryptographic Application Programming Interface.

CSP

Cryptographic Service Provider.

Capture

The method of taking a biometric sample from the end user.

Cipher

An encryption/decryption algorithm.

194

Ciphertext

Encrypted data.

Classification

A scheme for categorizing fingerprints according to their overall patterns. Some fingers do not fit into any of the classes, and some may have attributes of more than one class. (see binning)

Coding

Image processing software for extracting minutiae features from the image.

Comparison

The process of comparing a biometric sample with a previously stored reference template or templates. (see one-to-many and one-to-one)

Cryptography

The art and science of us ing mathematics to secure information and create a high degree of trust in the electronic realm. (see public key and private key)

Cryptographic Key

(see key and public key)

Cryptosystem

An encryption/decryption algorithm (cipher), together with all possible plaintexts, ciphertexts and keys.

Data Encryption Standard (DES)

Data Encryption Standard, a block cipher developed by IBM and the U.S. Government in the 1970s as an official standard.

Decryption

The inverse (reverse) of encryption.
195

Demographic Data

Census information about an individual, such as name, address, gender, race, and year of birth.

Digital Signature

The encryption of a message digest with a private key.

Direct Fingerprint Reader (DFR)

A device capable of scanning finger images directly from an individual's fingers.

Electronic Benefits Transfer (EBT)

Electronic Benefits Transfer enables automatic benefits distribution. It is currently implemented in WIC and Food Stamps programs.

Encryption

The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption of) the ciphertext.

End User

A person who interacts with a biometric system to enroll or have his /her identity checked.

Enrollee

A person who has a biometric reference template on file.

Enrollment

The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollment Time

The time a person must spend to have his/her biometric reference template successfully created.
196

Enrollment Station

A workstation at which an individual's biometrics (fingerprint, voiceprint, etc.) and personal information (name, address, etc.) can be entered into a bio-identification system.

Extraction

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

False Acceptance Rate (FAR)

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. Also known as the Type II error rate.

False Rejection Rate (FRR)

The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. Also known as the Type I error rate.

Fingerprint Identification Unit (FIU)

A biometric system capable of capturing, storing, and comparing fingerprint data for the purposes of verifying an individual's identity.

Fingerprint Template

A description of all the detected minutiae in a fingerprint pattern. The template contains each minutia's x/y coordinate, slope, and type, thus summarizing the characteristics of the fingerprint for purposes of matching the fingerprint against candidates.

Identification

A one-to-many comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity within a database, rather than verify a claimed identity. (contrast with verification)

Image Database

The database that contains all fingerprint templates in the system. The image database can contain images of the fingerprints, as well as photograph and signature images.

International Standards Organization (ISO)

The major international standards-setting organization for cards of all types.

Key

A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. (see private key and public key)

Key Management

The various processes that deal with the creation, distribution, authentication, and storage of keys.

Live Capture

The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Match/Matching

The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Minutiae

Points corresponding to the ridge endings, deltas, and bifurcations of a finger pattern. Minutiae are described in a fingerprint template.

Minutiae Database

The database that contains all fingerprint templates in the system. The minutiae database is contained within the image database.

Non-repudiation

A property of a cryptosystem. Non-repudiation cryptosystems are those in which the users cannot deny actions they performed.

One-to-Many

Fingerprint search that compares the minutiae from a candidate fingerprint image against the fingerprint minutiae database to determine whether the candidate exists in the database. (synonym for identification.)

One-to-One

Fingerprint search that compares the minutiae from an individual's live fingerprint image against fingerprint minutiae stored on a card or in a specific database record to determine whether or not the individual is who he or she claims to be. (synonym for verification.)

Original Equipment Manufacturer (OEM)

A biometric organization (manufacturer) that assembles a complete biometric system from parts, or assembles a biometric module for integration into a complete biometric system.

Password Bank

A database for storing username, password, and other personal information, to be released upon verification of an individual's identity.

Personal Identification Number (PIN)

A security method whereby a (usually) four-digit number is entered by an individual to gain access to a particular system or area.

199

Physical/Physiological Biometric

A biometric that is characterized by a physical characteristic rather than a behavioral trait. (contrast with behavioral biometric)

Plaintext

The data to be encrypted.

Private Key

In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used for encryption with digital signatures.

Public Key

In public-key cryptography, this key is made public to all. It is primarily used for encryption but can be used for verifying signatures.

Public Key Cryptography

Cryptography based on methods involving a public key and a private key.

Public Key Infrastructure (PKI)

PKIs are designed to solve the key management problem. (see key management)

Password List (PWL)

A database for storing username, password, and other personal information, to be released upon verification of an individual's identity.

Recognition

The preferred term is identification.

Reference Template

Data that represents the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Registration

Process of registering biometric data with a Fingerprint Identification Unit (FIU) or other biometric system.

Rejection/False Rejection

When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee. Also known as a Type I error.

Response Time/Processing Time

The time period required by a biometric system to return a decision on identification or verification of a biometric sample.

Smart Card

A card-shaped portable data carrier that contains one or more integrated circuits for data storage and processing. A typical smart card chip includes a microprocessor or CPU, ROM (for storing operating instructions), RAM (for storing data during processing), and EPROM (or EEPROM) memory for nonvolatile storage of information.

Software Developer's Kit (SDK)

A programming package that enables a programmer to develop applications for a specific platform. Typically, an SDK includes one or more APIs, programming tools, and documentation.

Threshold

The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Type I Error

The failure of a fingerprint identification system when it does not match a candidate fingerprint pattern with its mating fingerprint pattern (in other words, a failure to make a match that should have been made).

Type II Error

The failure of a fingerprint identification system when it matches a candidate fingerprint pattern with a non- mating fingerprint pattern (in other words, making a match that should not have been made)

Validation

The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification

A comparison of two sets of biometrics to determine if they are from the same individual; or, in fraud prevention applications, a one-to-one comparison of a live finger and a previously enrolled record to ensure that the applicant is who he/she claims to be.

APPENDIX B. BIOMETRIC PRODUCTS AND APPLICATIONS

Company	Products
IrisScan Inc., U.S.A.	• InrisScan 2020 • System 2000 EAC • System 2100
Sensar, U.S.A.	• IrisIdent System
Panasonic, U.S.A.	• Authentication

Table B.1. Iris Scanning Products. (From: Polemi, p. 24).

Company Products

Company	Products
PrintScan International, U.S.A.	• WinFing 3.1
Startek, Taiwan	• FingerCheck
Identix, U.S.A.	• TouchPrint 600 • TouchPrint 2000 Live Scan System
Sony, Japan	• FIU-710 “Puppy” Fingerprint ID unit Precise Biometrics, U.S.A. • SC-100, MC-100, A-100 • BioKeyboard 100, • BioAccess MC, BioAccess Mifare
FingerScan, Australia	• FingerScan
FingerMatrix, U.S.A.	• FingerScanner
Bioscrypt, Canada	• V-Pass, V-Flex, V-Prox, V-Smart • MV 1200, Core
AuthenTec, Inc., U.S.A.	• EntrePad AES3500
Biocentric Solutions, Inc., U.S.A.	• BioSentry
BioEnable Technologies, India	• BioEnable FRT
BioPay, LLC, U.S.A.	• BioPay Check Cashing System
Bioscrypt, Inc., U.S.A.	• V-Smart
Cansec Systems Ltd., U.S.A.	• Zodiac Fingerprint Reader
DitigalPersona, Inc., U.S.A.	• U.are.U Pro
U.are.U Pro Fujitsu Microelectronics America, Inc., U.S.A.	• MBF300 Sweep Sensor
Global Biometric Corporation	• ID Plus Token
IDynta Systems, Inc., U.S.A.	• BioLink Products
NEC Technologies, Inc., U.S.A.	• TouchPass
Printrak (Motorola), U.S.A.	• Omnitrak 8.0 AFIS/Palmprint
Identification Technology Raytheon, U.S.A.	• IDENT
Visionics, U.S.A.	• FingerPrinter CMS
SENSE Holdings, Inc., U.S.A.	• BioClock

Table B.2. Fingerprint Recognition Products. (From: Polemi, p. 23 and BiometriTech, March 26, 2002).

Company	Products
Computer Data Systems, U.S.A	• Hand Geometry Readers
Recognition Systems, U.S.A.	• HandPunch • ID3D HandKey • Hand Geometry Readers
BioMet Partners, U.S.A.	• Digi-2
Biometric Security Systems, U.K	• BioDentity System
Biometrics, Inc, U.S.A.	• FastPass II
Talos Technology Inc, U.S.A.	• PG-2001
IDentiCard, U.S.A.	• Hand Geometry Reader

Table B.3. Hand Geometry Products. (From: Polemi, p. 27).

Company	Products
Dectel Security Systems, U.K.	• Facial Data Base Systems
Forensic Security Services, U.K.	• Thermace • VIAS
Technology Recognition Systems	• FR1000
Facial Reco Associates	• Sherlock Face Recognition
Identicator, U.S.A.	• Facial Search System
Lawrence Livermore National Laboratory, U.S.A.	• KEN
National University of Singapore	• FACEit
George Mason University	• ARGUS
MIT Artificial Intelligence Lab	• Face Pass
UMIST	• FACE-SOM
University of Essex	• Facial Recognition Software
Dextel Security Systems, UK	• Dextel Crime Net
Identification Technologies International Inc., U.S.A.	• One on One Facial Recognition Systems
ZN Security, Germany, Germany	• ZN-Face
NeuroMetric Vision Systems	• MuflMaster
AcSys Biometrics Corporation, Canada	• AcSys FRS Entry • Acsys FRS Logon IT
	• AcSys FRS CoLo
BioDentity Systems Corporation, Canada	• SecureIDent
BioID America, Inc., U.S.A.	• Single Sign-on
Cognitec AG, U.S.A.	• Cognitec AG, U.S.A.
GraphCo Technologies, Inc., U.S.A.	• Facetrac
Identico Systems, U.S.A.	• True ID
ImageWare Systems, Inc., U.S.A.	• Face ID
Imagis Technologies, Inc., Canada	• ID-2000
Neuridynamics Limited, U.K.	• Tridentity 3 Dimensional Face Recognition
Photo Vision, Inc., U.S.A.	• QuadHDTV Video Image Sensor
Visionics, U.S.A.	• FaceIt (Figure 5.15.)
Viisage Technology, Inc., U.S.A.	• FaceFINDER (Figure 5.16.)

Company	Products
	• Face EXPLORER
	• FacePASS, FacePIN, FaceTOOLS
Symtron Technology, U.S.A.	• FaceOn Logon System
	• FaceOn Surveillance System

Table B.4. Facial Recognition Products. (From: Polemi, p. 25 and BiometriTech, 15 May 2002).

Company	Products
ABS, Germany	• VOCAL • VOCAL SCW1 • VOCAL ZKE
T-NETIX, U.S.A.	• PIN-LOCK, voice verification system
Bell Security, U.K.	• Caller Verification System
Speakez, U.S.A.	• Tele-MAtic
Domain Dynamic Limite, UK	• Domain Dynamic Limite, UK
Anovea Authentication Technology, Inc., U.S.A.	• Anovea Speaker Authentication System
BioID America, Inc., U.S.A.	• BioID 3.0
Buytel (VoiceVault), Ireland	• Voice Vault Services
InterVoice-Brite, Inc., U.S.A.	• Speech Access
Keyware, U.S.A.	• Centralized Authentication Software (CAS)
Nuance Communications, U.S.A.	• Nuance Verifier 3.0
OTG, Canada	• HELP YOURSELF/SecurPBX
Persay Ltd., U.S.A.	• Orpheus
Sonic Foundry, Inc., U.S.A.	• Unified Security View
SpeechWorks International, Inc., U.S.A.	• SpeechSecure
SpeakEZ, U.S.A.	• Voice Print Speaker Verification SDK
Veritel Corporation	• VoiceCheck
VeriVoice, Inc., U.S.A.	• VeriVoice Security Lock (SL)
Vocent Solutions, Inc., U.S.A.	• Voice Secure Suite

Table B.5. Voice Recognition Products. (From: Polemi, p. 29 and BiometriTech, 1 March 2002).

Company	**Products**
Communication Intelligence Corp., U.S.A.	- Signature Verification Software
Gadix, U.S.A.	- Cyber-SIGN
Quintet, U.S.A.	- Electronic Signature Verification System
British Technology Group, U.K.	- Rolls Royce Signature Verification
PenOp Inc., U.S.A.	- Signature Analyzer
AEA Technology, U.K.	- Countermatch
cadix International, Japan	- ID-007
IBM. U.S.A.	- IBM Transaction Security System
Checkmate Electronice, U.S.A.	- Sign/On

Table B.6. Handwriting/Signature Recognition Products. (From: Polemi, p. 30).

Company	**Products**
BioPassword Security Systems, U.K.	- BioPassword
Electronic Signature Lock Corporation, U.S.A.	- Electronic Signature Lock
M&T Technologies, U.S.A.	- Keystroke Analyzer
TNO-FEL, Netherlands	- Keystroke Analyzer

Table B.7. Keystroke Analysis and Recognition Products. (From: Polemi, p. 30).

LIST OF REFERENCES

A Hand Geometry – Based Verification System, “Capturing Hand Images and Extracting Features,” Available Online, [http://biometrics.cse.msu.edu/hand_proto.html], August 30, 2002.

Abreu, Elinor Mills, “Computerized ‘Mr. Potato Head’ System Aids Police,” San Francisco, InageWare Sytems, Inc., June 27, 2002, Available Online, [http://www.iwsinc.com/reuters.cfm], August 6, 2002.

AcSys Biometrics Inc., “AcSys Face Recognition System. Nothing Compares,” Available Online, [http://www.acsysbiometricscorp.com/hml/face.html], August 25, 2002.

Alanko, Timo; Kojo, Markku; Liljeberg, Mika; Raatikainen, Kimmo, ProQuest, “Mobile Access to the Internet: A Mediator-Based Solution”, Available Online, [http://proquest.umi.com/pdweb?Did=000000117541721], August 4, 2002.

Anonymous, “Wireless LAN Standards and Applications,” Microwaves & RF, May 2002, Available Online, [http://proquest.umi.com/pqdweb?Did=000000120608015&Fmt=3&Deli=1&Mtd=1&Idx=9..], August 8, 2002.

Automatic Gait Recognition and Extraction, Model-Based Gait Recognition – Variation in Hip Inclination, Downloaded August 25, 2002, Available Online, [http://www.isis.ecs.soton.ac.uk/image/gait/david_cunado/index.php3].

Bacon, Jean, University of Cambridge, “Toward Pervasive Computing”, DS Online Update, Available Online, [http://ieee/pervasivecomputing.com], Sept 25, 2002.

Bellavista, Paolo, Corradi, Antonio and Stefanelli, Cesare, Integrated Environments, “The Ubiquitous Provisioning of Internet Services to Portable Devices”, Available Online, [http://ieee/pervasivecomputing.com], September 25, 2002.

BenAbdelkader, Chiraz, Cutler, Ross and Davis, Larry, “Stride and Cadence as a Biometric in Automatic Person Identification and Verification,” Proceeding of the Fifth IEEE International Conference on Automatic Face and Gesture Recognition (FGR’02), IEEE Computer Society.

Benditt, John, “Creepy Functions, ‘Leading Edge’,” An MIT Enterprise Technology Review, February 25, 2002, Available Online, [http://www.technologyreviewcom/articles/benditt0901.asp], August 6, 2002.

Biometrics Institute, The Biometric Resource Center, Available Online, [http://www.biomet.org/voiceproducts.html], August 19, 2002.

Biometric Technical Assessment, August 19, 2002, Available Online, [http://bioconsulting.com/Bio_Tech_Assessment.html].

Bordetsky, Alex, Dennis, LeRoy and Ford, Michael, Proposal for Homeland Security Research and Academic Support, "Emergency and Surveillance Network-Centric Habitats for Homeland Defense," November 2002.

Brown, Eric, "Persuasive, Pervasive Computing," An MIT Enterprise Technology Review, February 25, 2002, Available Online, [http://www.technologyreviewcom/articles/wo_brown022502.asp], August 6, 2002.

Brown, Eric S., "Project Oxygen's New Wind, 'Q&A with Rodney Brooks and Victor Zue'," An MIT Enterprise Technology Review, December 20, 2001, Available Online, [http://www.technologyreview.com/articles/wo_brown12001.asp], August 6, 2002.

Bruno, Mark, Technology, That's My Finger, "The Results Are In. And The Winner Is the Finger," Available Online [http://www.us-banker.com/usb/articles/usbfeb01-9.shtml], October 27, 2002.

Buderi, Robert, "Computing Goes Everywhere," An MIT Enterprise Technology Review, January/February 25, 2002, Available Online, [http://www.technologyreviewcom/articles/buderi0101.asp], August 6, 2002.

Cameron, David, "Walk This Way," An MIT Enterprise Technology Review, April 23, 2002, Available Online, [http://www.technologyreviewcom/articles/wo_brown022502.asp], August 6, 2002.

Canterinicchia, Dan, "Army MPs Go Biometric," March 18, 2002, Available Online, [http://www.fcw.com/fcw/articles/2002/0318/news-bio-03-18-02.asp], August 6, 2002.

Canterinicchia, Dan, "Army Tests Base Security App," March 21, 2002, Available Online, [http://www.fcw.com/fcw/articles/2002/0318/news-army-03-21-02.asp], August 6, 2002.

Cunado, David, Dr., Automatic Gait Recognition and Extraction, "Model-Based Gait Recognition-Variation in Hip Inclination," Available Online, [http://www.isis.ecs.soton.ac.uk/image/gait/david_cunado/index.php3], August 25, 2002.

Darrell, Trevor, About Project Oxygen, Available Online, [http://oxygen.lcs.mit.edu/Vision.html], January 19, 2003.

Davies, Nigel and Gellersen, Hans-Werner, Reaching for Weiser's Vision, "Beyond Prototypes: Challenges in Deploying Ubiquitous Systems," Pervasive Computing, January-March 2002, Available Online, [http://computer.org/pervasive].

Estrin, Deborah, Culler, David, Pister, Kris and Sukhatme, Gaurav, "Connecting the Physical World with Pervasive Networks," Reaching for Weiser's Vision, Pervasive Computing, January-March 2002.

FaceIt Image Product, Identix, Empowering Identification, "Facial Surveillance," [Available Online, [http://www.identix.com/products/pro_faceit.html], October 26, 2002

FindBIOMETRICS.com Complete Identification Verification Resource, “A Practical Guide to Biometric Security Technology, ‘Selecting a Biometric Technology’,” findBIOMETRICS.com, Available Online, [www.findbiometrics.com/Pages/lead3.html], August 23, 2002.

FindBIOMETRICS.com Complete Identification Verification Resource, “A Practical Guide to Biometric Security Technology, ‘Uses for Biometrics’,” findBIOMETRICS.com, Available Online, [www.findbiometrics.com/Pages/lead2.html], August 23, 2002.

FindBIOMETRICS.com Complete Identification Verification Resource, “Multi-Modal Biometrics Authentication System,” findBIOMETRICS.com, Available Online, [www.findbiometrics.com/Pages/multimodal%20articles/multi_2.html], August 23, 2002.

Fingerprint Identification, Available Online, [http://biometrics.csu.edu/fingerprint.html], March 16, 2003.

Gaetano, Borriello and Roy Want, “Embedded Computation Meets the World Wide Web,” Association for Computing Machinery, Communications of the ACM; New York; May 2000, Available Online, [http://proquest.umi.com/pqdweb?Did=000000053769908&Fmt=4&Deli=1&Mtd=1&Idx=1..], August 8, 2002.

Imagis Technology, Inc., “ID-2000 SDK – Face & Image Recognition Software Development Kit,” Available Online, [http://www.imagistechnologies.com/Product/ID2000SDK.htm], August 6, 2002.

ImageWare Systems, Inc., “ImageWare Brings Facial Recognition to the Web,” ImageWare Systems, Inc., Available Online, [http://www.iwsinc.com/identix.cfm], August 6, 2002.

I/O Software, Inc. – Securing Your Digital World, “The Power of SecureSuite”, Available Online, [http://www.iosoftware.com/pages/Products/SecureSuite/index.asp], February 2, 2003.

Johanson, Brad, Fox, Armando and Winograd, Terry, Integrated Environments, “The Interactive Workspaces Project: Experiences with Ubiquitous Computing Rooms,” Pervasive Computing, April-June 2002, Available Online, [http://computer.org/pervasive].

Johnson, R. Collin, Advanced Technology, “Companies Test Prototype Wireless-Sensor Nets”, January 29, 2003, Available Online, [http://www.eet.com/at/news/OEG20030128S0028].

Karygiannis, Tom and Owens, Les, “Draft Wireless Network Security 802.11, Bluetooth and Handheld Devices”, National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce, July 2002.

Kodak, Rajiv Mehrotra, Editor, In The News, "More than Face Value: Airports and Multimedia Security," Proceedings of the Fifth IEEE International Conference on Automatic Face and Gesture Recognition (FGR'02), IEEE Computer Society.

Leo, Alan, "Show Your High-Tech ID," An MIT Enterprise Technology Review, October 25, 2001, Available Online, [http://www.technologyreview.com/articles/wo_leo102501.asp], August 6, 2002.

Liu, Simon and Silverman, Mark, "A Practical Guide to Biometric Security Technology," Security, IT Pro, January/February 2001.

Makarski, Richard E. and Marrero, Jose A., "A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security", Master's Thesis, Naval Postgraduate School, September 2002.

McCabe, Alan, Ph.D. Student, "Markov Modeling of Simple Directional Features for Effective and Efficient Handwriting Verification," Available Online, [http://www.cs.jcu.edu.au/~alan/handwriting/], November 1, 2002.

McFedries, Paul, "Smart Dust", October 26, 1999, Available Online, http://www.wordspy.com/words/smartdust.asp.

MISC Program Brings 3D Modeling and Mathematical Information to Handwriting Identification and Document Examination, Available Online, [http://qdewill.com/mics.htm], October 28, 2002.

Nanavati, Samir, Thieme, Michael, "Biometrics: Identity Verification in a Networked World," Jon Wiley and Sons, Inc., U.S.A., 2002.

Neurodynamics, "Tridentity – Adding a New Dimension to Facial Recognition" Available Online, [http://www.newrodynamics.com], August 25, 2002.

Podio, Fernando L., "Personal Authentication Through Biometric Technologies," National Institute of Standards and Technology, Gaithersburg, Maryland.

Retina Scan Technology, Available Online, [http://www.retina-scan.com/retina_scan_technology.htm], October 28, 2002.

Ruggles, Thomas, "Comparison of Biometric Techniques", Copyright 1996, August 28, 2002, Available Online, [http://www.bioconsulting.com/bio.htm].

Satyanarayanan, M., Carnegie Mellon University and Intel Research Pittsburgh, "A Catalyst for Mobile and Ubiquitous Computing," Available Online, [http://www.computer.org/pervasive], September 25, 2003.

Satyanarayanan, M., Carnegie Mellon University and Intel Research Pittsburgh, "Integrated Pervasive Computing Environments," Available Online, [http://www.computer.org/pervasive], September 25, 2002.

Sarnoff, “Video Detective Workstation from PVT Enhances Images for Law Enforcement Use,” April 1, 2002.

Speech Production System, Speaker Verification, Available Online, [http://biometrics.cse.msu.edu/speaker.html], November 5, 2002.

Speir, Michelle, “The New Face of Security ‘Understanding the Promises and Pitfalls of Facial-Recognition Technology’,” March 4, 2002, Federal Computer Week, Available Online, [http://ww.fcw/articles/2002/0304/tec-face-03-04-02.asp], August 6, 2002.

Stikeman, Alexandra, “Recognizing the Enemy,” An MIT Enterprise Technology Review, December 2001, Available Online, [http://www.technologyreview.com/articles/stikeman1201.asp], August 6, 2002.

Tristram, Claire, “Battle for the Unseen Computer,” An MIT Enterprise Technology Review, May 2001, Available Online, [http://www.technologyreview.com/articles/tristram0501.asp], August 6, 2002.

Timo Alanko, Markku Kojo, Mika Liljeberg and Kimmo Raatikainen, “Mobile Access to the Internet: A Mediator-Based Solution,” Internet Research, Bradford, 1999, Available Online, [http://proquest.umi.com/pqdweb?Did=000000117541721&Fmt=3&Deli=1&Mtd=1&Idx=4..], August 8, 2002.

UK Biometrics Working Group, “Use of Biometrics for Identification and Authentication Advice on Product Selection”, Issue 1.0, November 23, 2001.

Voice Analysis, Speaker Verification, Available Online, [http:biometrics.sce.mdu.edu/speaker.html], November 5, 2002.

Walton, Marsha, “Wireless ‘Cloud’ May Offer Silver Lining Or Is It Just ‘Pie-in-the-Sky’ Technology,” CNN Sci-Tech, Available Online, [http://www.cnn.com/2002/TECH/science/07/31/coolsc.wireless.cloud/index.html], July 31, 2002.

Woodward, Jr., John D., “Biometrics ‘Facing Up to Terrorism’,” RAND, October 2001.

Wrolstad, Jay, “Wireless ID System Passes Police Trial,” January 14, 2002, Available Online, [http://www.WirelessNewsFactor.com], Part of the NewsFactor Network.

Yam, Chew Yean, Nixon, Mark S. and Carter, John N., “Performance Analysis on New Biometric Gait Motion Model,” Fifth IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI’02), IEEE Computer Society.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Department of the Navy
Office of the Chief of Naval Operations (N6109)
Washington, DC

4. Dr. Dan Boger
Naval Postgraduate School
Code 06/IS
Monterey, California

5. LCDR Steven J. Iatrou
Naval Postgraduate School
Code IW/Is
Monterey, California

6. Alex Bordetsky
Naval Postgraduate School
Code 06 IS
Monterey, California

7. Capt (Ret) Randy J. Hess
Naval Postgraduate School
Monterey, California

8. Lieutenant LeRoy P. Dennis III
Naval Postgraduate School
Code 32 ISO
Monterey, California

9. Lieutenant Michael K. Ford
Naval Postgraduate School
Code 32 ISO
Monterey, California