2005

Fingerprint testing protocols for optical sensors

Travis W. Rosiek
West Virginia University

Fingerprint Testing Protocols for Optical Sensors

Travis W. Rosiek

Thesis Submitted to the
College of Engineering and Mineral Resources
at West Virginia University
in partial fulfillment of the requirements
for the degree of

Master of Science
in

Electrical Engineering

Bojan Cukic Ph.D., Chair
Arun A. Ross Ph.D.
Lawrence A. Hornak Ph.D.

Lane Department of Computer Science and Electrical Engineering

Morgantown, WV
2005

Keywords: Biometrics, Fingerprint, Testing, Protocol

ABSTRACT

Fingerprint Testing Protocols for Optical Sensors

Travis W. Rosiek

Currently there is a variety of conflicting and contradictory testing protocols for biometric technologies. There is currently no biometrics testing standard, which allows vendors to skew their test results in their favor. The research discussed in this thesis aims to address these issues by developing and validating testing protocols for optical fingerprint sensors. Angle of rotation, translation, lighting, and device placement have been identified in this work as variables potentially affecting system performance and protocols were developed to evaluate their effects on optical fingerprint sensor performance. Testing was done by capturing raw images under different scenarios, then offline analysis of data was performed to see how these variables impact performance. Based on the results of this research, it can be shown that these variables have an effect on system performance in optical fingerprint sensors and these protocols have some relevance in the evaluation of optical fingerprint sensors.

Sponsoring Agency: National Biometric Security Project, Morgantown, WV

Acknowledgments

I would like to thank my parents for supporting me over the years and giving me all of the opportunities that they have. I would also like to thank Dr. Cukic for all of his tutelage and guidance over the past several years. Dr. Cukic has always been very supportive and helpful in all of my endeavors. I would also like to thank Dr. Ross for always taking time to answer questions concerning biometrics and protocols. Next, I would like to thank Dr. Hornak for offering advice and expertise over the years. As a whole, all three of these professors are excellent teachers and I would like to thank them for everything they have taught me. They also have always made time to talk with me and answer questions. I would also like to thank all of the folks at the West Virginia office of National Biometric Security Project (NBSP) for all of their help and support in developing and testing these protocols. I would like to thank West Virginia University students, Gaurav Gupta and Nick Bartlow for all of their support in this work. Finally, I would like to thank all of those who volunteered their time and fingerprints for testing purposes. Most importantly, I would like to thank them all for being great people.

Table of Contents

List of Figures

Chapter 1. Introduction

1.1 Biometrics

Biometrics is the automated identification or verification based on physiological or behavioral traits. Two main functions of a biometric system are verification and identification. Both identification and verification involve enrollment of users into a database.   Enrollment is the process of acquiring users' biometric traits, converting them into a template and then storing them in a database. Verification/Authentication is a one to one matching in which the user claims an identity to the biometric system, and the system tries to validate the claimed identity. Positive identification is determining the identity of an unknown user in which the user's biometric data compared to users in the database, which is a one to many matching. Negative identification is determining if the user is not enrolled in the system. Authentication/Verification is a one to one matching, meaning it is the validation of whether a person is who they claim to be. See Figure 1 for a graphical representation of these functions.

Biometric systems can identify or verify a person by fingerprint, face, iris, retina, voice, gait, etc. to name a few. Multimodal biometrics is becoming a popular way to improve the performance of biometric devices by combining the strengths of two or more biometric modalities.

Characterics of a biometric trait are universality, distinctiveness, permanence, and collectability. Universality is to what extent people possess this trait. Distinctiveness can also be called uniqueness and is how different the trait is from person to person. Permanence describes how much or how little the trait changes over a period of time. Collectability is how easily the trait can be acquired from the user [13].

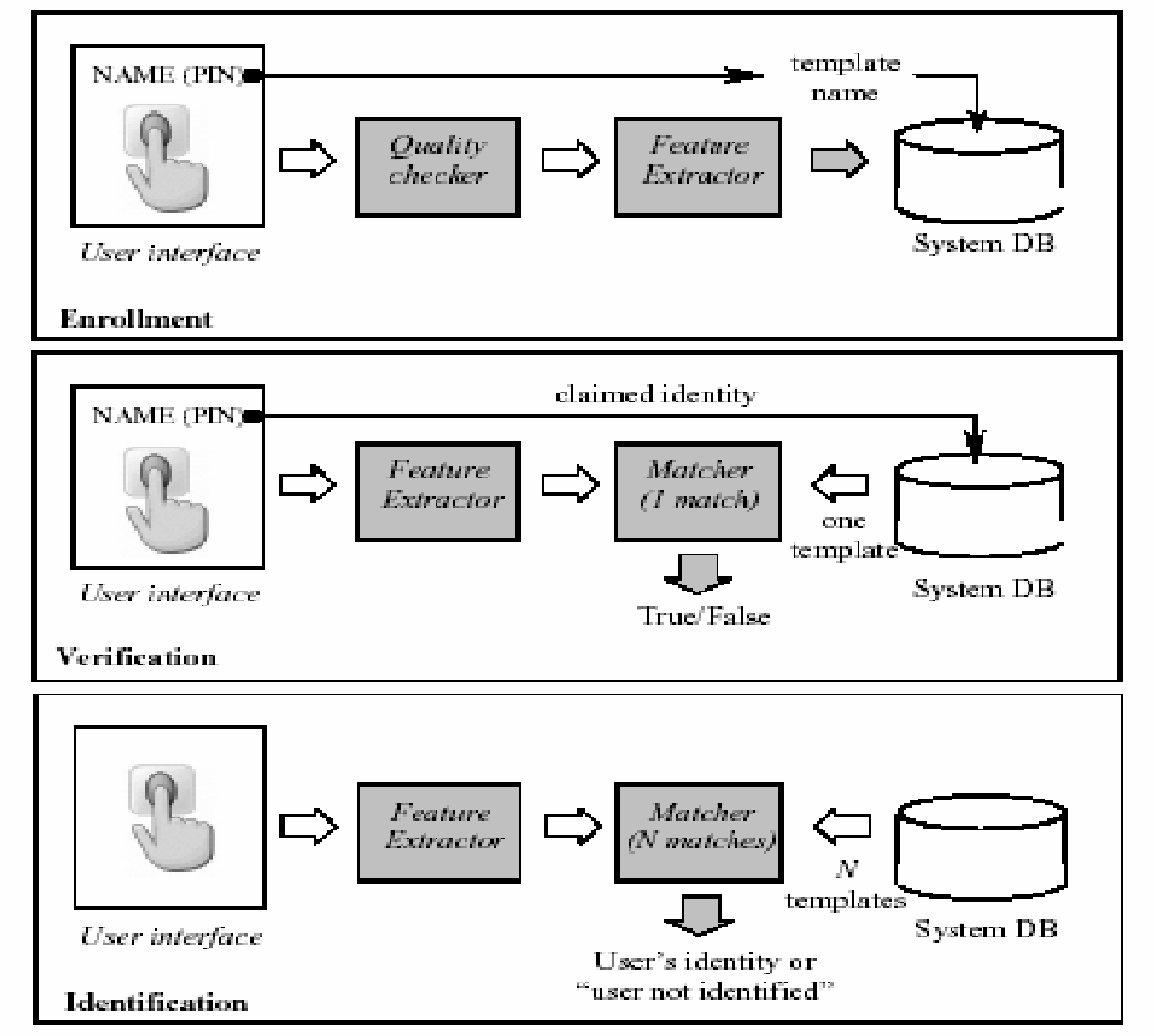


Figure 1. Functions of a Biometric System

From [13].

1.2 The Need for Biometric Systems

There are three main ways to be identified by a computer system:

1. What you know: Personal Identification Numbers, passwords, etc.
2. What you have: Identification cards, keys, etc.
3. Who you are: Biometrics

A motivation for using biometrics for identification is the fact that passwords and PIN's can easily be forgotten, lost, or stolen. The use of biometrics would dramatically reduce these inconveniences.

1.3 Biometric System

A biometric system is made up of the following modules: sensor module, feature extraction module, matching module, decision module, and a system database. Some issues to consider when deploying a biometric system are performance, acceptability, and circumvention. Performance can be broken down into speed and accuracy. Acceptability is a social issue that reflects to what degree users are willing to use their biometric trait(s) in biometric systems. Circumvention depicts how easily a biometric system can be spoofed/fooled by a fraudulent user [13]. See Figure 2 for a diagram of a biometric system and its modules.

- Sensor Module

  This module acquires the raw image of the biometric trait for the user [18].

- Feature Extraction Module

  This module processes the raw image data and extracts certain features to represent the biometric trait into what is known as a feature set [18].

- Matching Module

  The matching module compares an extracted feature set against templates stored in a biometric database by generating a match score [18].

- Decision Module

  The decision module uses matching scores to determine a user's claimed identity or to identify a person. In some papers, this module is included as part of the matching module [11].

- System Database

The system database is responsible for storing user templates to match against.

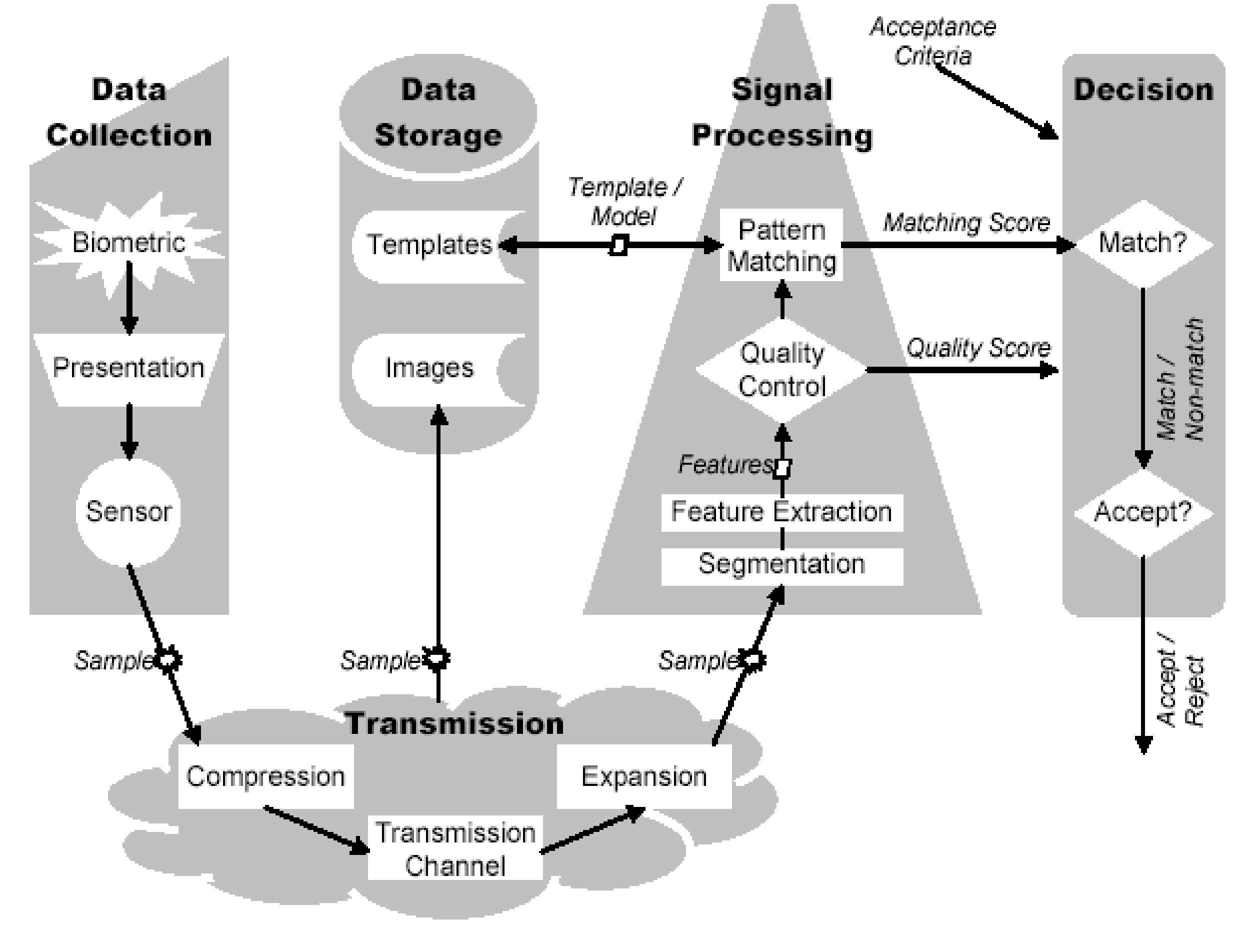


Figure 2. Biometric System Modules

From [15].

1.4 Biometric Applications

The number of applications of biometrics is continually increasing. Applications are generally divided into three main categories: forensic applications, civilian applications, and commercial applications. Some examples for forensic applications are using biometric systems for corpse identification, criminal investigation, and parenthood determination. Civilian applications of biometric systems can include a national identification system, drivers' licenses, welfare disbursement, and border crossings to name a few. Commercial biometric applications include some of the following: ATM's, access control, cellular phones, and credit cards.

1.5 Fingerprint as a Biometric Modality

Fingerprint systems are the oldest and most commonly used form of biometric identification today [13]. Fingerprints have not been scientifically proven to be unique for every individual, but through observations appear unique [14].

Features of a fingerprint can be extracted into what is known as a feature set. This feature set is later used in matching. Some common features on a fingerprint that can be used in creating a feature set are minutiae points, ridge maps, singular points, orientation field, and texture analysis. Minutiae points can either be ridge endings(terminations), ridge bifurcations cross-overs, lake, island, spur, or an independent ridge. See Figure 3 for some common minutiae points. Texture analysis examines the texture of the fingerprint. The singular points method examines the location of singular points, which consist of core and delta points. See Figure 4 for some common singular points.

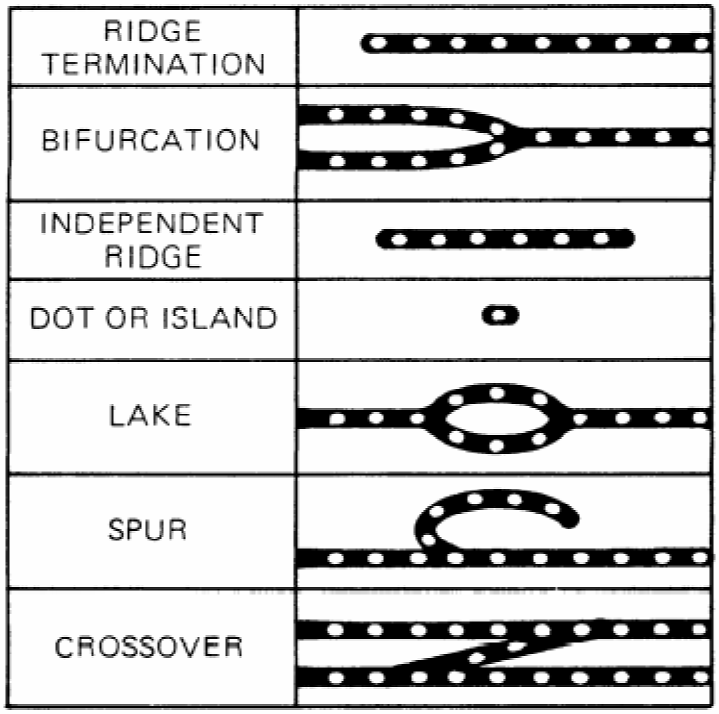


Figure 3. Fingerprint Minutiae Points:

From [22].

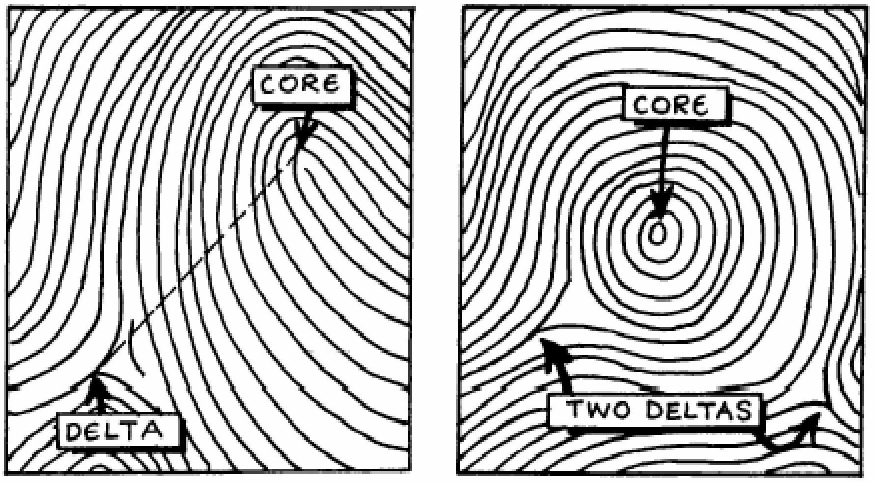


Figure 4. Fingerprint Single Points:

From [22].

1.6 Fingerprint Sensors

There are several types of sensors that are used today to image fingerprints. Some of the most common types of sensors are optical, capacitive, ultrasound, pizeo-electric, and temperature differential, etc.

- **Optical**: Optical sensors use what is called FTIR (Frustrated Total Internal Reflection) to image fingerprints. The ridges of a fingerprint will be in contact with the sensing prism, while the valleys will be at a distance. Light is generated from a light source and is reflected off of the fingerprint through a sensing prism to a FTIR sensor chip. Light is absorbed by the ridges and reflected by the valleys, allowing the ability to image the fingerprint [22]. See Figure 5 for a schematic of an optical fingerprint sensor.
    - Pros: Low cost, good resolution, good image quality.
    - Cons: Large size/bulkiness, latent fingerprints.

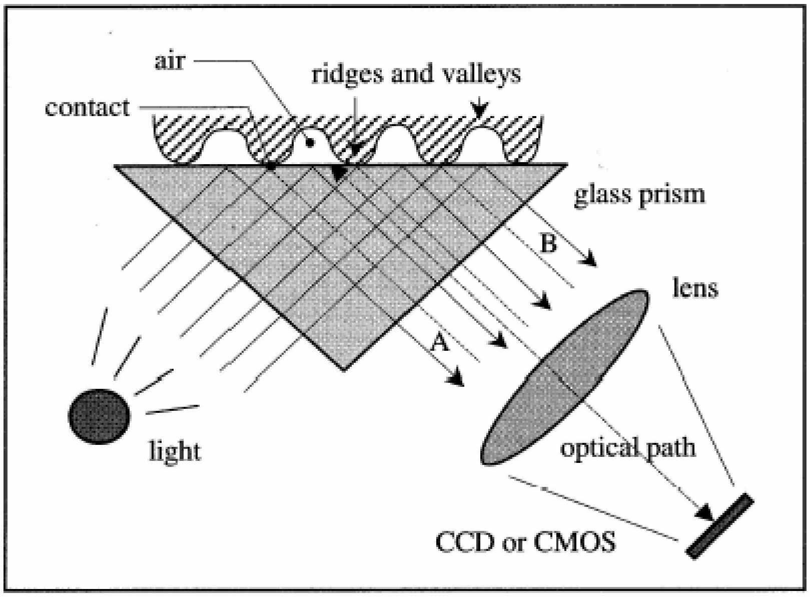


Figure 5. Optical Fingerprint Sensor

From [22].

- **Capacitive**: Capacitive sensors consist of an array of micro-capacitors, each capacitor when it comes in contact with a ridge of a fingerprint creates variations in electric charge. Theses variations result in the image capture of the fingerprint [22]. See Figure 6 for a diagram of a capacitive fingerprint sensor.
    - Pros: small, compact.
    - Cons: contact based, ESD effects, latent fingerprints, dust, and corrosion.

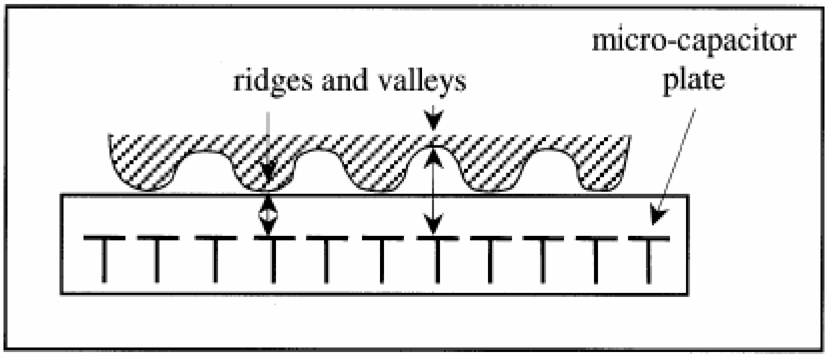


Figure 6. Capacitive Fingerprint Sensor

From [22].

- **Ultrasound**: Acoustic signals are sent from the device and are then reflected by the fingerprint. Variations in this reflection depict valleys from ridges, thus allowing the fingerprint to be imaged [22]. See Figure 7 for a diagram of an ultrasound fingerprint sensor.
    - Pros: contactless, images below the skin, very accurate.
    - Cons: Large size/bulkiness, expensive.

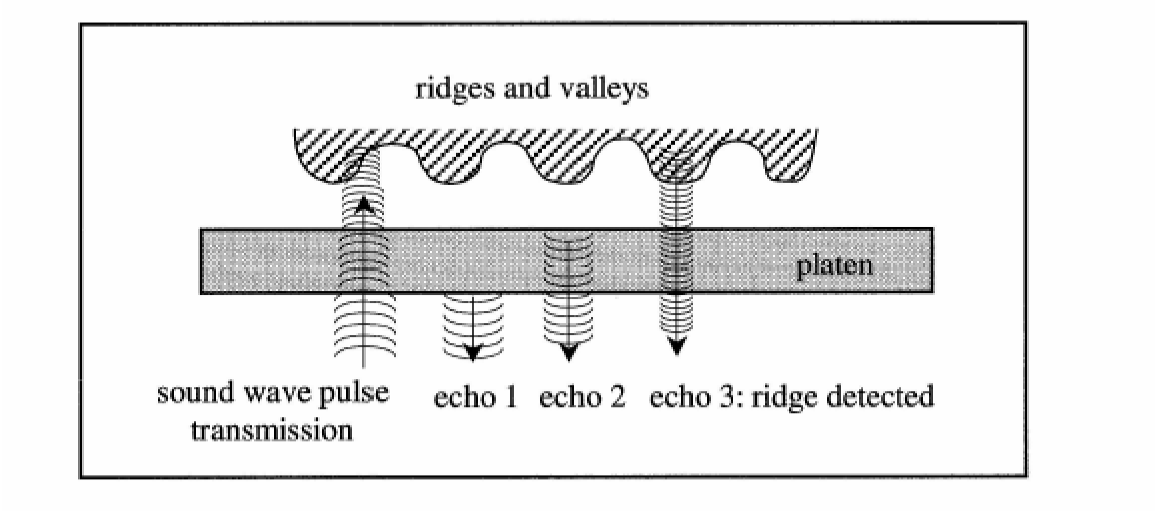


Figure 7. Ultrasound Fingerprint Sensor

From [22].

- **Pizeo-electric**: This type of sensor has a surface made of a non-conductive dielectric material. By applying pressure from a finger, a current is generated based on the amount of pressure. Different pressure generated from the ridges and valleys allows the fingerprint to be imaged [22].
    - Pros: can detect between a fake finger and a real finger.
    - Cons: blurred images, not always good resolution.

- **Temperature Differential**: These sensors are made of pyro-electric material that detects variations in temperature. Temperature differences in the ridges (warmer) compared to that of valleys (cooler), allow the fingerprint to be imaged. They can be implemented by a swipe sensor [22].
    - Pros: Not affected by ESD, no thick protective coating, can do a form of liveness Detection.
    - Cons: Deformation by placing finger on sensor.

1.7 Deformation of Fingerprints

A fingerprint is a three dimensional object and when placed on a fingerprint sensor, a two dimensional image is created. The process of placing the fingerprint on the sensor, causes non-linear distortions in the ridge structure of the fingerprint. These distortions can lead to alterations in the spatial location of minutiae points, which can lead to errors in the matching process [20]. Several factors can cause these distortions, some of which are the amount of pressure applied by the subject, whether the subject is standing or sitting, orientation of the sensor with respect to the subject, elasticity of skin, and the moisture content of the skin. These distortions in a fingerprint can vary from one acquisition to the next [21]. See Figure 8 for an example of fingerprint deformation.

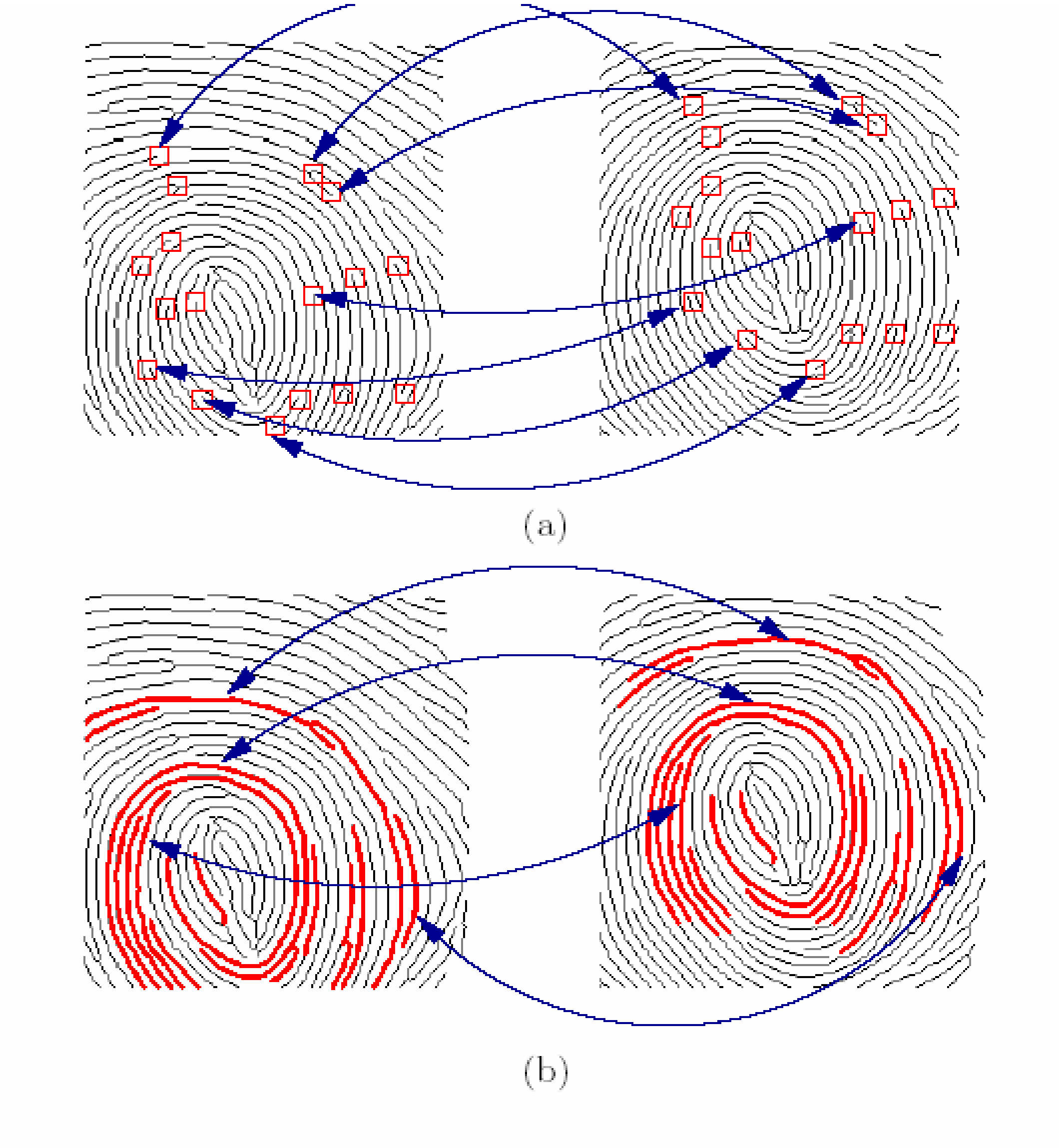
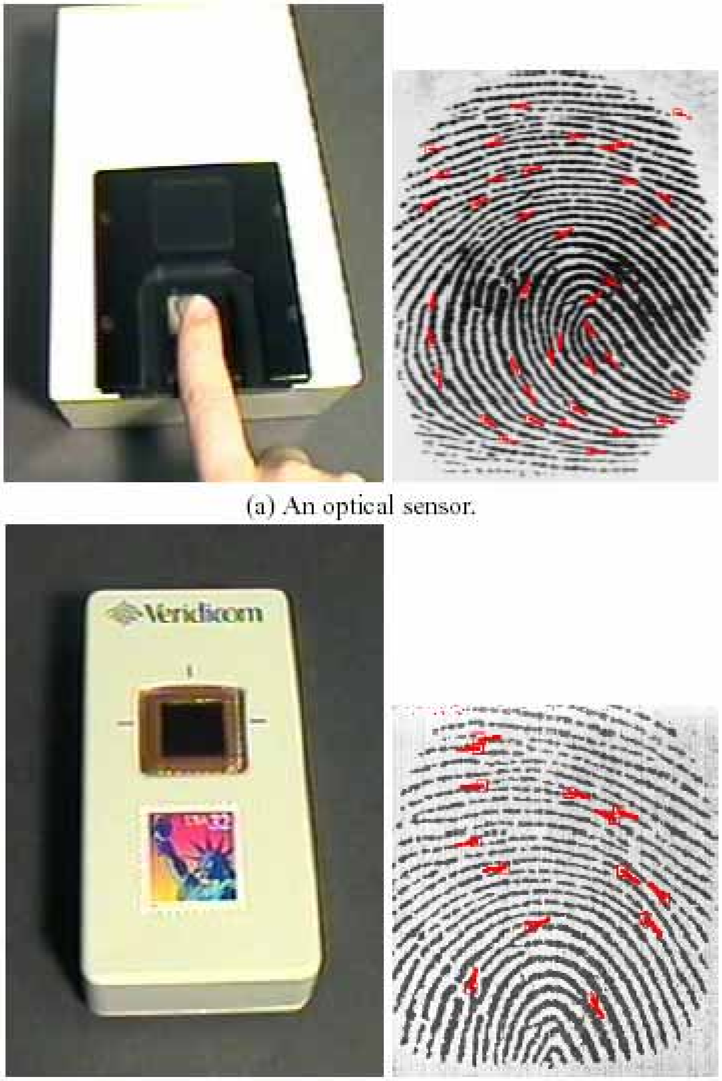


Figure 8. Fingerprint Deformation Example

(a) Minutiae point correspondences, (b) Ridge curve correspondences between two impressions of the same finger. From [20].

1.8 Interoperability of Fingerprint System Components

Interoperability in fingerprint sensors is an increasing concern as fingerprint systems are deployed in more locations and in many cases proprietary algorithms are used for specific sensors. For instance, a user enrolls into a system by using a capacitive fingerprint sensor, but in the future must use an optical sensor to verify themselves. This is due to the fact that the result of the quality and nature of raw data is greatly affected by using different sensors from enrollment to verification. This can cause variances in minutiae points extracted and generation of match scores. This is a challenge for most matching modules because few matching algorithms are able to handle the variations in different sensors [20]. See Figure 9 for sample fingerprint images taken from different sensor technologies.



(a) An optical sensor.

(b) A solid-state sensor.

Figure 9. Multiple Fingerprint Sensor Technologies

Fingerprint images of the same finger acquired using (a) Digital Biometrics' optical sensor and (b) Veridicom's solid state sensor. The number of detected minutiae points in the corresponding images are 39 and 14, respectively. From [20].

1.9 Biometrics Performance

With the ever increasing market for biometric devices, there is a growing need for a consistent way to evaluate biometric systems. There have been many documents written to address the issue of biometric device testing, but few have developed generic testing protocols for biometric systems. The development of generic test protocols that are designed to produce repeatable results will help standardize testing efforts.

Today, most biometrics systems are evaluated by many parameters. Some include false match rate, false non-match rate, false accept rate, false reject rate, Receiver Operator Characteristic (ROC) curve, Failure To Enroll (FTE) rate, Failure To Acquire (FTA) rate, etc. When it comes to comparing biometrics products with any of these parameters, they can be divided into matching error rates, decision error rates, image acquisition error rates, and performance measures among others [15]. See Figure 10 for an example of imposter and genuine user distributions, along with an example of FAR, FRR, and EER.

- **Decision Error Rates:**
    - **False Rejection Rate (FRR):** It is the number of times genuine users are falsely rejected divided by the number of trials.
    - **False Acceptance Rate (FAR):** It is the number of times an imposter user is falsely granted access to the system divided by the total number of trials.
    - **Equal Error Rate (EER):** It is the value is the rate when FAR equals the FRR of the biometric system.

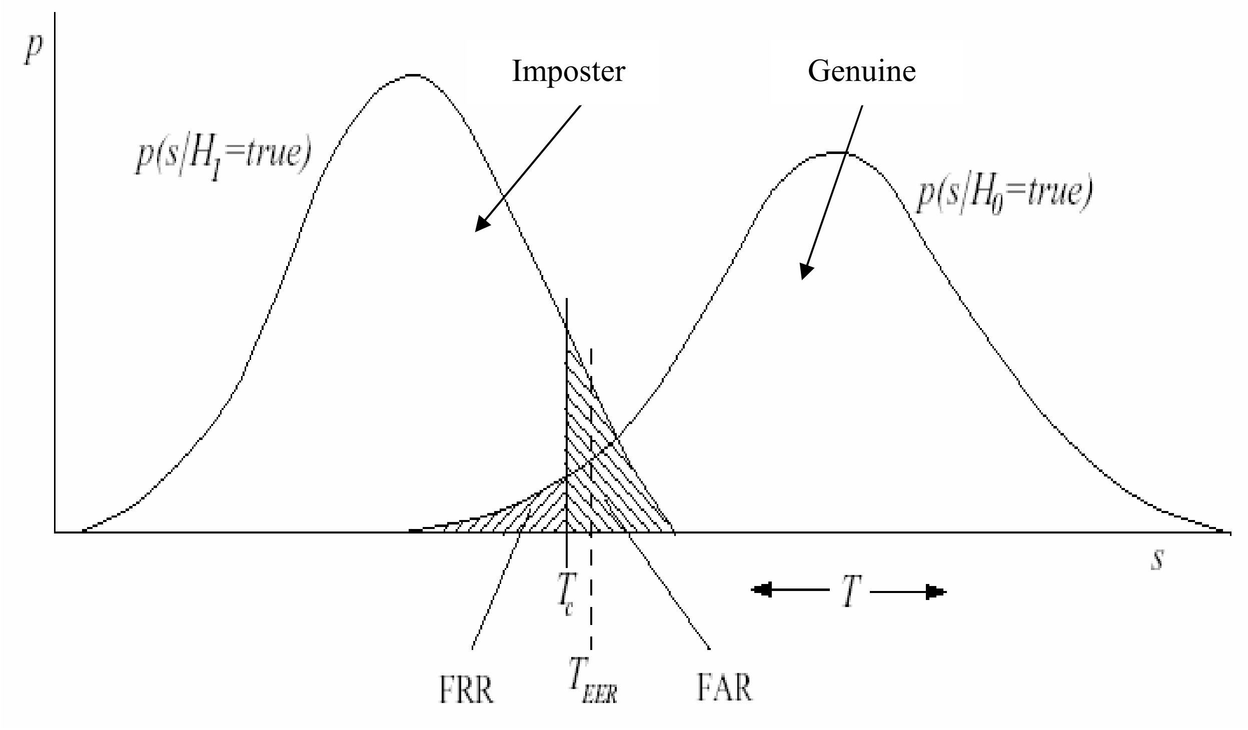


Figure 10. Probability Distribution for Genuine and Imposter Users

Probability distribution of genuine and imposter users. T is the decision threshold. From [16].

- **Matching Errors:**
  - **False Match Rate (FMR):** FMR is the rate at which a template is falsely matched to a template in a database [29].
  - **False Non-Match Rate (FMNR):** FNMR is the rate at which a template is falsely not-matched to a truly matching template in the database [29].
- **Image Acquisition Errors:**
  - **Failure to Enroll (FTE):** FTE is the percentage of time users are unable to enroll in the biometric system [11].
  - **Failure to Acquire (FTA):** FTA is the percentage of time the biometric system is unable to capture a biometric sample when one is presented [11].

- **Performance measures:**
    - **Receiver Operating Characteristics (ROC):** ROC curve is the curve relating FAR to FRR across various thresholds. ROC curves are one way biometric system performance can be evaluated.
    - **Detection Error Trade-off (DET):** DET curve is a modified ROC curve.
    - **D Prime:** D prime is a common scalar means of evaluating biometric system performance. It is the normalized difference between the means of genuine and impostor match scores. D prime is also known as a "measure of goodness", and assumes distributions to be normal [3].

$$d' = \frac{|\mu_1 - \mu_2|}{\left((\sigma_1^2 + \sigma_2^2)/2\right)^{1/2}}$$

The accuracy of a biometric system is only as good as its sensor and the degrees of freedom of the biometric trait being measured [2]. The accuracy of a biometric system is represented by its FAR- False Accept Rate and its FRR- False Reject Rate. These two scores can be plotted against each other through out all possible threshold values to show performance. This is called the ROC- Receiver Operating Characteristic curve [13]. See Figure 11 for an example of an ROC curve.

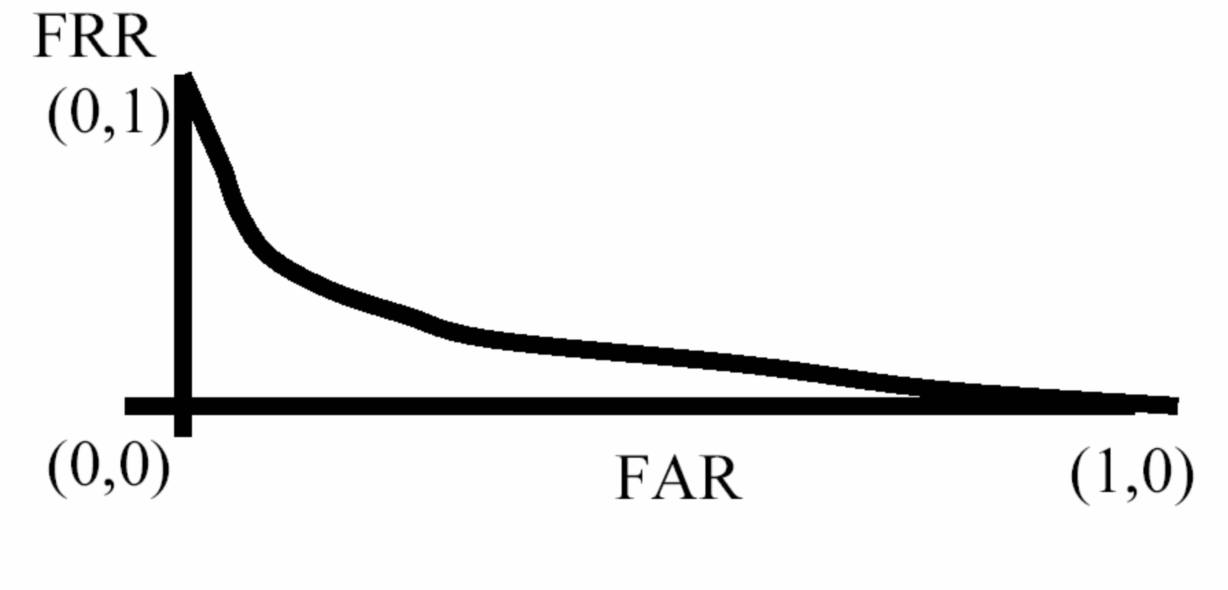


Figure 11. ROC Curve

- **Decision errors vs. matching errors**

FMR and FNMR are calculated over the number of comparisons while FAR and FRR are calculated over the number of transactions. Another difference is that FAR and FRR also account for FTA rates [15].

- **Type I and Type II Errors**

Type I errors occur when the positive hypothesis otherwise known as the true condition is rejected when it should have been accepted.

Type II errors occur when the negative hypothesis otherwise known as a false condition is accepted when it should have been rejected [30].

- **Systematic and Random Errors**

Performance estimates of biometric systems will be affected by systematic errors and random errors. Random errors result from the natural variation in biometric samples or users, for example. Systematic errors are errors that are caused by the bias in testing procedures [15].

1.10 Biometric Users

Doddington has classified types of users in a biometric system as sheep, goats, wolves, and lambs. This is commonly called Doddington's Zoo. Wolves are imposters who try to gain access while pretending to be a genuine user. Wolves are successful at impersonating other users, which cause false accepts. Goats as a class are very different from other classes, however determining a user from this group is difficult. Goats have high FRR. Lambs as a class are not very unique from other classes and can be easily imitated; many imposters can successfully pretend to be lambs. Lambs have high FAR. Sheep as a class are unique among other classes, and each sheep is well separated from other members of the sheep class [6]. It is necessary to characterize biometric users in this fashion because it helps to identify the types of users in a system and how they interact with the system. Little work has been done in the area of identifying users and generalizing user groups. However work has been done in multibiometrics to account for variability in users by assigning user specific weights [10].

1.11 Thesis Objective and Contribution

Currently there is a variety of conflicting and contradictory testing protocols for biometric technologies [15]. It is important to note that in an ideal case a user's feature set is supposed to be the same for every use. However, this is not the case due to several factors. These factors can be the result of using different sensors, variations in the environment, improper user interaction (ex. the biometric trait not properly presented to the sensor), and alterations in the biometric trait [18]. Also there is currently no biometrics testing standard; this allows vendors to skew their test results in their favor [1]. The research discussed in this paper aims to address these issues by developing and validating testing protocols for optical fingerprint sensors. This research consists of five main areas:

1 Identification of variables that can affect the performance of an optical fingerprint system. It is extremely important to control and account for as many variables as possible to improve the accuracy of test results.

2 Development of repeatable testing protocols for the some of the aforementioned variables. Repeatability is a major focus of this research.

3 Selection of an optical fingerprint sensor to test. In this research it is important to choose a sensor that allows for the capture of raw images to allow for offline testing.

4 Fine tuning the developed protocols to the chosen optical fingerprint sensor. Even though the testing protocols developed in this research are for optical fingerprint sensors, they must be altered to accommodate the sensor being tested. For example, the development of a mask for the sensor will have to be altered for various shaped sensors (oval, square, etc.) and some alterations might be necessary in testing other variables. Thus, in some degree the protocols developed in this paper are somewhat generic in nature.

5 Test the above protocols in hopes to validate these newly created protocols. The work in this paper concludes with the analysis of the results in testing the above protocols.

Chapter 2. Related Work

2.1 Testing Methodologies

The "Best Practices" document focuses on technical performance testing and was written because there are no guidelines for protocol creation for biometric systems [15]. There are several forms of biometrics testing:

1. Reliability, availability, and maintainability
2. Technical Performance
3. Vulnerability
4. Security
5. User Acceptance
6. Human Factors
7. Cost/Benefit
8. Privacy regulation compliance

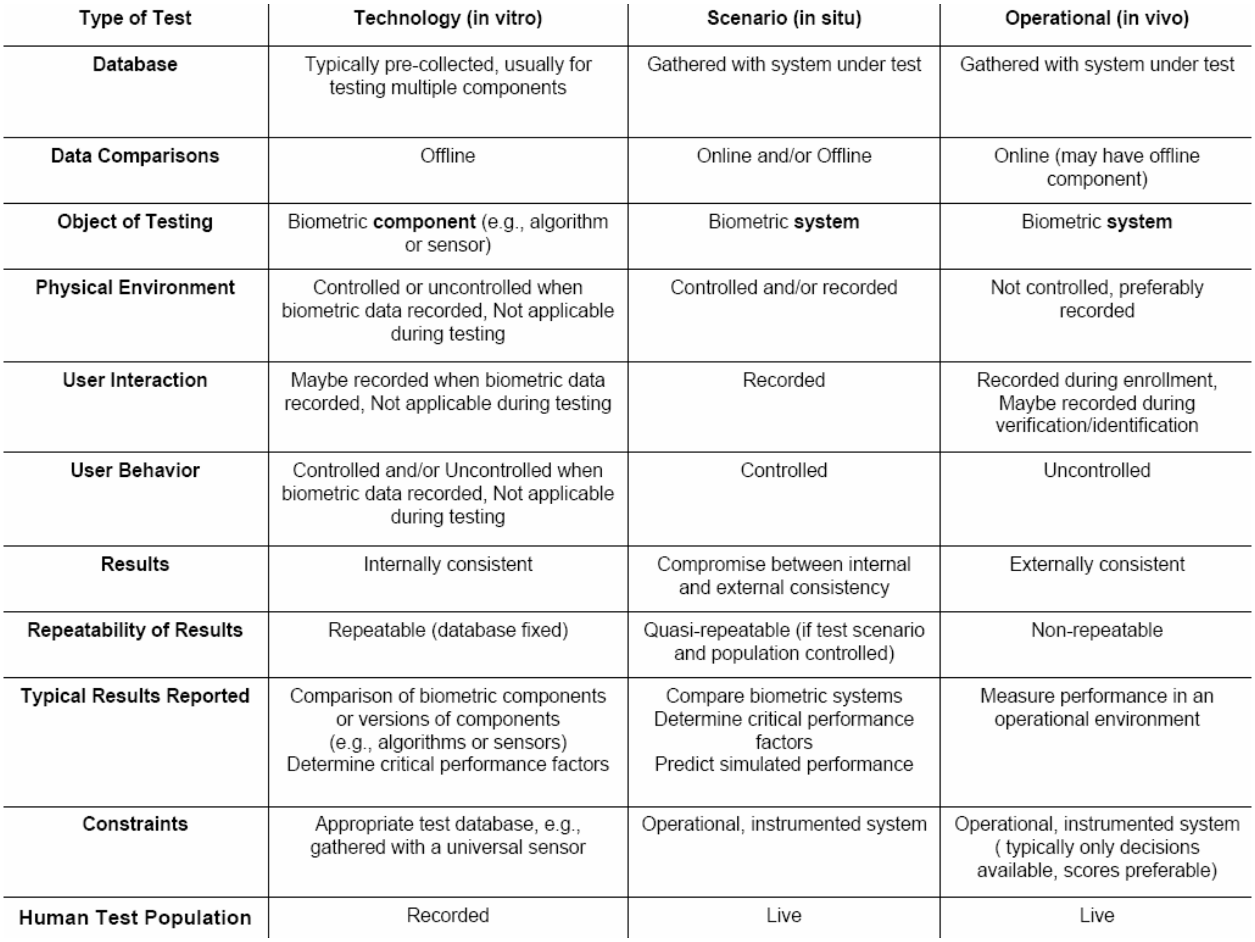
There are three main types of evaluation of biometric systems [15]:

1. Technology evaluation
2. Scenario evaluation
3. Operational evaluation

Technology evaluations compare competing technologies from a single technology by testing all algorithms on a standardized database by a "universal" sensor. This approach tests novel data, and is done offline. Since the database is fixed, these technology test results are repeatable [15]. Two common technology evaluations are the FpVTE and the FVC.

FVC is the Fingerprint Verification Competition and its aim is to track recent advances in fingerprint verification, for both academia and industry, and to benchmark the state-of-the-art in fingerprint technology. This competition should not be viewed as an “official” performance certification of biometric systems, since: the databases used in this contest have not been necessarily acquired in a real-world application environment and are not collected according to a formal protocol. only parts of the system software will be evaluated by using images from sensors not native to each system [7]. FpVTE is the Fingerprint Vendor Technology Evaluation (FpVTE) and is independently administered technology evaluation of fingerprint matching, identification, and verification systems [8].

Scenario evaluations determine the performance of a complete biometric system in an environment that models a real-world target application. These test results can only be repeatable if the modeled scenario is controlled. In operational evaluations biometric system performance is determined by testing in a specific environment and with a specific population. These tests offer limited repeatability because of many unknown variables in the operational environment [15]. See Figure 12 for a table of the various evaluation methods.



Type of Test	Technology (in vitro)	Scenario (in situ)	Operational (in vivo)
Database	Typically pre-collected, usually for testing multiple components	Gathered with system under test	Gathered with system under test
Data Comparisons	Offline	Online and/or Offline	Online (may have offline component)
Object of Testing	Biometric **component** (e.g., algorithm or sensor)	Biometric **system**	Biometric **system**
Physical Environment	Controlled or uncontrolled when biometric data recorded, Not applicable during testing	Controlled and/or recorded	Not controlled, preferably recorded
User Interaction	Maybe recorded when biometric data recorded, Not applicable during testing	Recorded	Recorded during enrollment, Maybe recorded during verification/identification
User Behavior	Controlled and/or Uncontrolled when biometric data recorded, Not applicable during testing	Controlled	Uncontrolled
Results	Internally consistent	Compromise between internal and external consistency	Externally consistent
Repeatability of Results	Repeatable (database fixed)	Quasi-repeatable (if test scenario and population controlled)	Non-repeatable
Typical Results Reported	Comparison of biometric components or versions of components (e.g., algorithms or sensors) Determine critical performance factors	Compare biometric systems Determine critical performance factors Predict simulated performance	Measure performance in an operational environment
Constraints	Appropriate test database, e.g., gathered with a universal sensor	Operational, instrumented system	Operational, instrumented system (typically only decisions available, scores preferable)
Human Test Population	Recorded	Live	Live

Figure 12. Various Testing Modes

From [26].

- **Avoidance of Data Collection Errors**

It is extremely important to reduce the number of data collection errors because error rates in the collection process can exceed the error rates of the fingerprint system. These collection errors can be classified as either mis-acquired image or mislabeled image errors [15].

- **Factors Affecting Performance**

Mansfield and Wayman have defined factors that affect biometric system performance. These factors can be divided into four main classes:

1. Factors incorporated as independent variables in the experiment and then observe the

effect of these factors.

2. Factors controlled to become part of the experimental conditions

3. Factors “randomized out” by the experiment.

4. Factors of negligible effect

Performance of a biometric system can vary greatly on the application, environment, and population, and thus should be considered when developing a testing protocol [15]. Dr. Hale Kim has done research on some environmental impacts on optical fingerprint sensors. Figure 13 shows the impact of temperature on image quality. Figure 14 shows the effects of humidity on image quality. Figure 15 shows the impact of finger pressure on the sensor. Figure 16 shows the impact of fingerprint moisture on image quality [12].

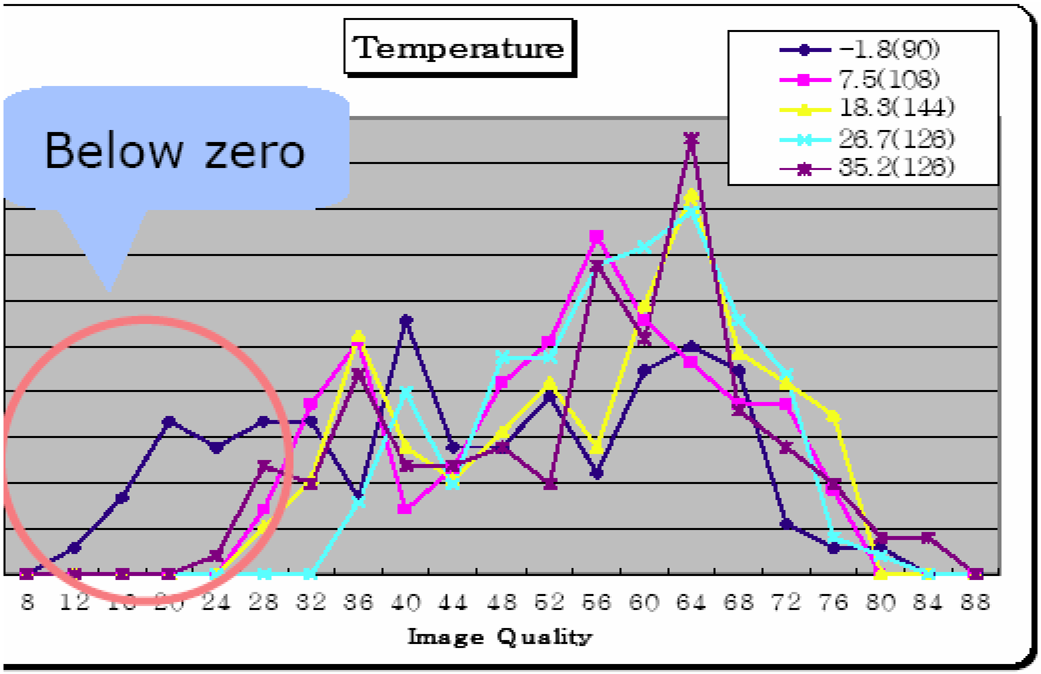


Figure 13. Effects of Temperature on Optical Fingerprint Sensor

From [12]

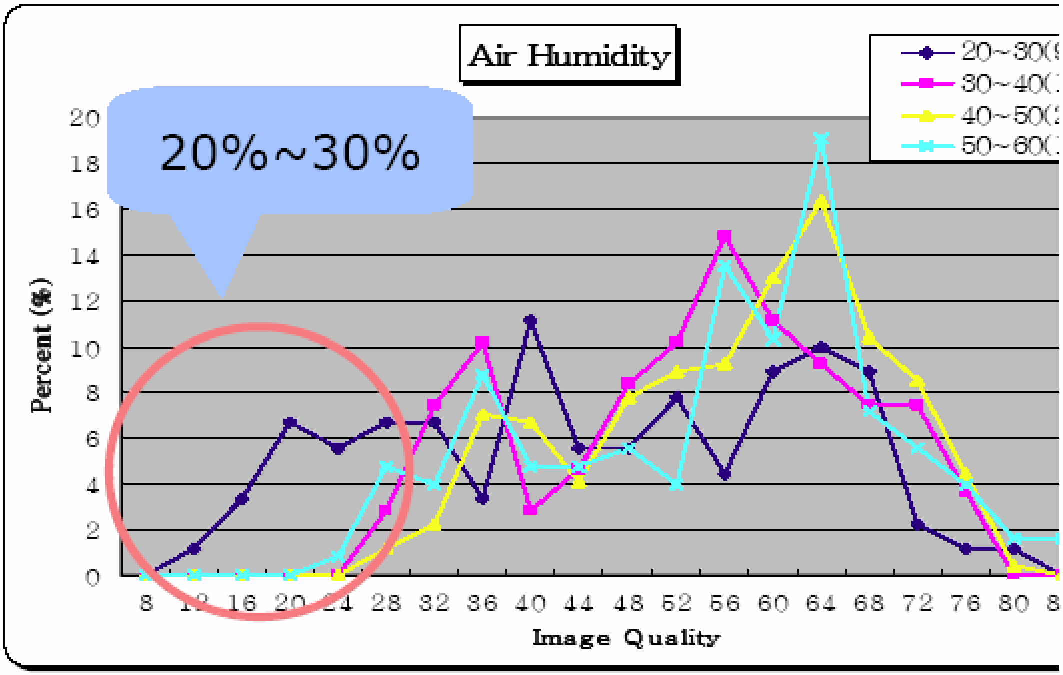


Figure 14. Effects of Humidity on Optical Fingerprint Sensor

From [12]

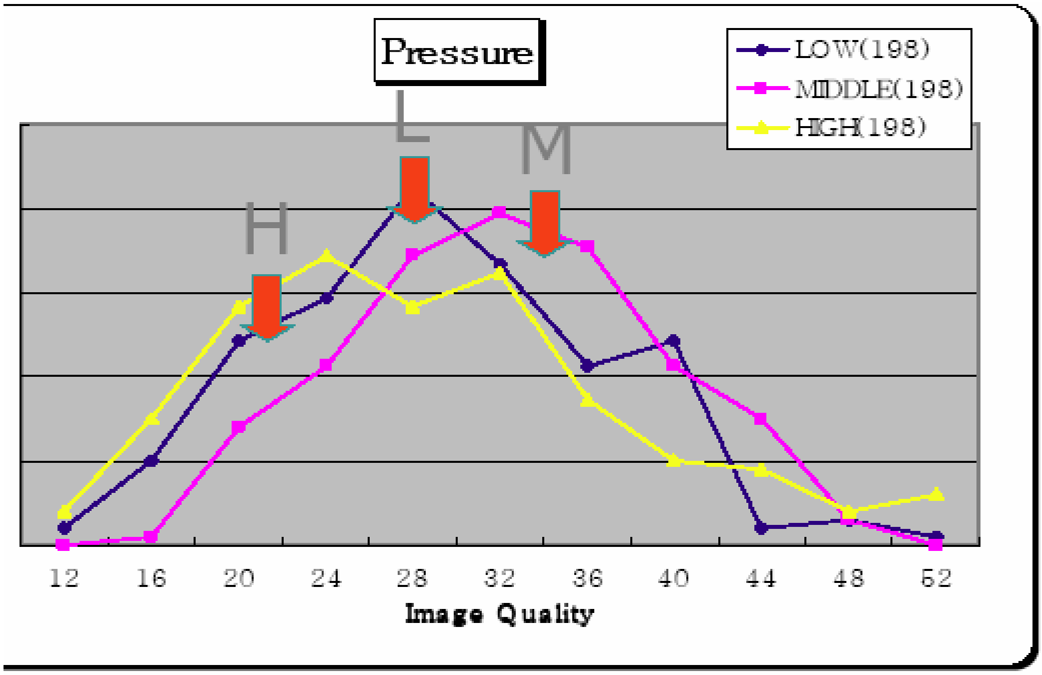


Figure 15. Effects of Pressure on Optical Fingerprint Sensor

From [12]

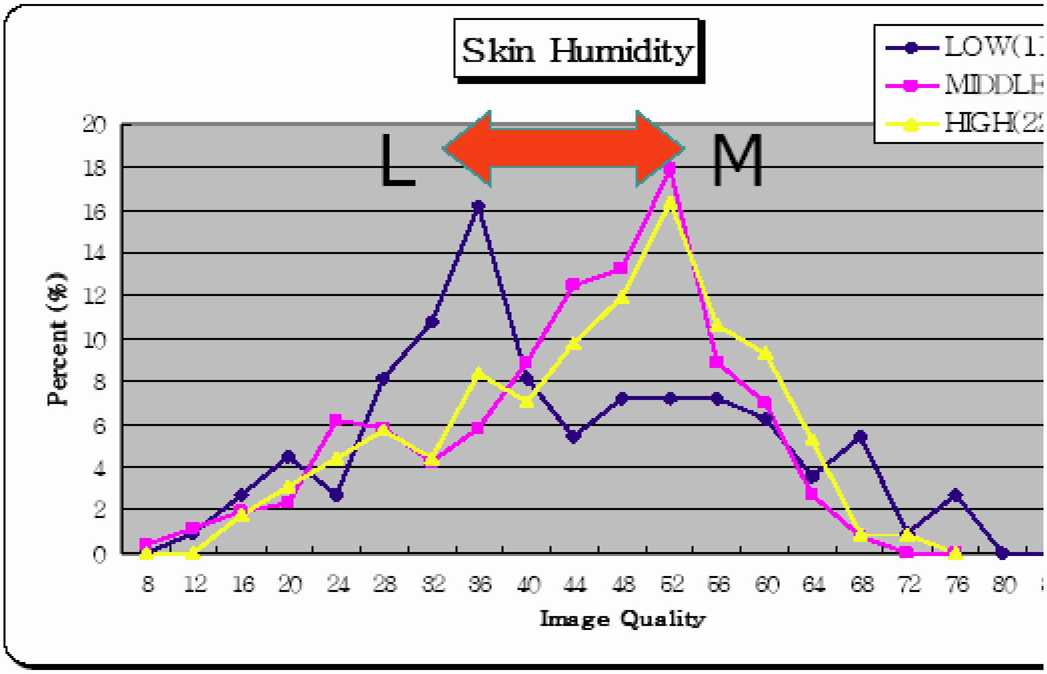


Figure 16. Effects of Skin Humidity on Optical Fingerprint Sensor From [12]

- **Volunteer selection**

The volunteer group in scenario testing should be demographically similar to target population of the desired application. Recruiting members for the group may bias the tests, therefore it may be necessary to select unevenly from volunteers so that the group is as well representative as possible [15].

- **Suggested Test Methodology**

A suggested overall test methodology as stated by [24] is presented below:

1. Determine the overall goal(s) of the test, including the device(s) to be evaluated and the test location(s).
2. Identify the operational environment and measurable parameters that need to be

evaluated in order to define the success or failure of the device.

3. Draft a test plan that provides sufficient detail to allow for project planning with regard to the required resources and subsequent costs and schedules.
4. Collect relevant baseline data on the existing test location(s) prior to the installation of the biometric device(s).
5. Install the biometric device(s) and verify that operation is per the manufacturer's specifications.
6. Evaluate the biometric device(s) per the test plan.
7. Analyze the results, particularly with respect to the baseline data, in order to evaluate the overall operational effectiveness of the biometric system.

- **Multiple Attempts or Tests**

In some tests, it may be necessary to collect multiple attempts or test multiple scenarios per person. In these instances, user behavior may vary with each successive attempt [15]. This variation will make it difficult to control the user familiarity/habituation factor. Averaging error rates over multiple attempts/tests can help to reduce the effects on accuracy [15].

- **Test Size**

There are two commonly used methods for determining test sizes. It is well known that the larger the test size the better the results. Also, the more representative of the target population the test set is the better the results [15]. Rule of 3 and Rule of 30 provide a lower bounds for test size [26].

- **Rule of 3**

The Rule of 3 addresses the question “What is the lowest error rate that can be statistically established with a given number N of independent comparisons?”. This error rate, p, is the probability of no errors in N trials [15].

- **Rule of 30**

The Rule of 30 states that for there to be 90% confidence that the true error rate is within ± 30% of the observed error rate there must be at least 30 errors. The Rule of 30 assumes independent trials and a binomial distribution [15].

2.2 Statistics in Biometrics

Estimation of confidence intervals has been a main focus in developing means of determining how well a biometric system performs. False Accept Rate (FAR) and False Reject Rate (FRR) are the two most commonly used error rates when describing a biometric system's matching performance. Some of the common confidence interval methodologies have been proposed by Doddington, Mansfield and Wayman, Bolle et al., Schuckers, and Michaels and Boult [23]. They are briefly described below.

- **Doddington's Rule**

Doddington's Rule assumes a binomial distribution and gives a 90% confidence interval for the mean error rate. Doddington's Rule is intended to be used when the following is true [5]:

$$S = \sum_{i=1}^{n} X_i \geq 30$$

Where S is the number of errors, X_i is, and n is the number of users. The confidence interval is then created by taking +/- 30% of this estimated mean error rate, π. This interval is as follows [5]:

$$\pi \pm 0.30\pi$$

- **Best Practices Approach**

The Best Practices approach assumes a normal distribution and gives a 95% confidence interval for the mean error rate. This approach also uses a method of moments approach. A drawback to this approach is that the distribution isn't always normal and thus can lead to negative values for the observed error rates [15].

- **Subset Bootstrap**

The Subset Bootstrap approach is non-parametric and achieves a 95% confidence interval for the mean error rate. In Subset Bootstrap, replicate datasets are generated and resampling is used estimate the distribution of estimated error rates [23].

- **Beta-Binomial**

The Beta-Binomial approach can use either maximum likelihood approach or an analysis of variance approach to estimate confidence intervals. In both parametric approaches, an extra-variation model is given for the mean and variance to aid in the estimation of these parameters [23].

- **Logit Beta-binomial**

The Logit Beta-Binomial approach is derived from using Beta-Binomial approach and a logit function. The logit (log odds) function is as follows:

$$\mathbf{logit\ (y) = log\ (y/\ (1\text{-}y))}$$

This approach allows more coverage of the confidence interval and this interval is guaranteed to fall within a 0 to 1 range [23].

Chapter 3. Scenario Testing Procedures

3.1 Generic Modes of Operation

In the following sections protocols were developed to perform scenario testing while keeping in mind generic modes of biometric system operation. The first step is to decompose a biometric system into various generic components and applications. A biometric system can be viewed as being either a stand-alone system or a networked system. Next, the system can either control physical access or logical access. These are all important factors to consider when developing testing procedures. The next crucial component is to evaluate which operational modes are possible in the fingerprint system. Below is an excerpt from Rosiek & Gupta's paper *Generic Biometric System* describing some common modes of operation for a biometric system.

> **Modes of Operation**
>
> **Acquisition** is the process of acquiring the biometric data from the user is known as acquisition. The output parameter (performance parameter) that will be affected by this is FTA (Failure to acquire). As shown in Figure 17, the acquisition mode's input is the biometric trait(s) and its output is the raw image(s) of the trait. The biometric trait(s) may need to be re-imaged if the initial image(s) do not pass the quality control parameter. The quality of raw images will greatly affect other related modes. Poor image quality will create a snowball effect throughout the system [17] .

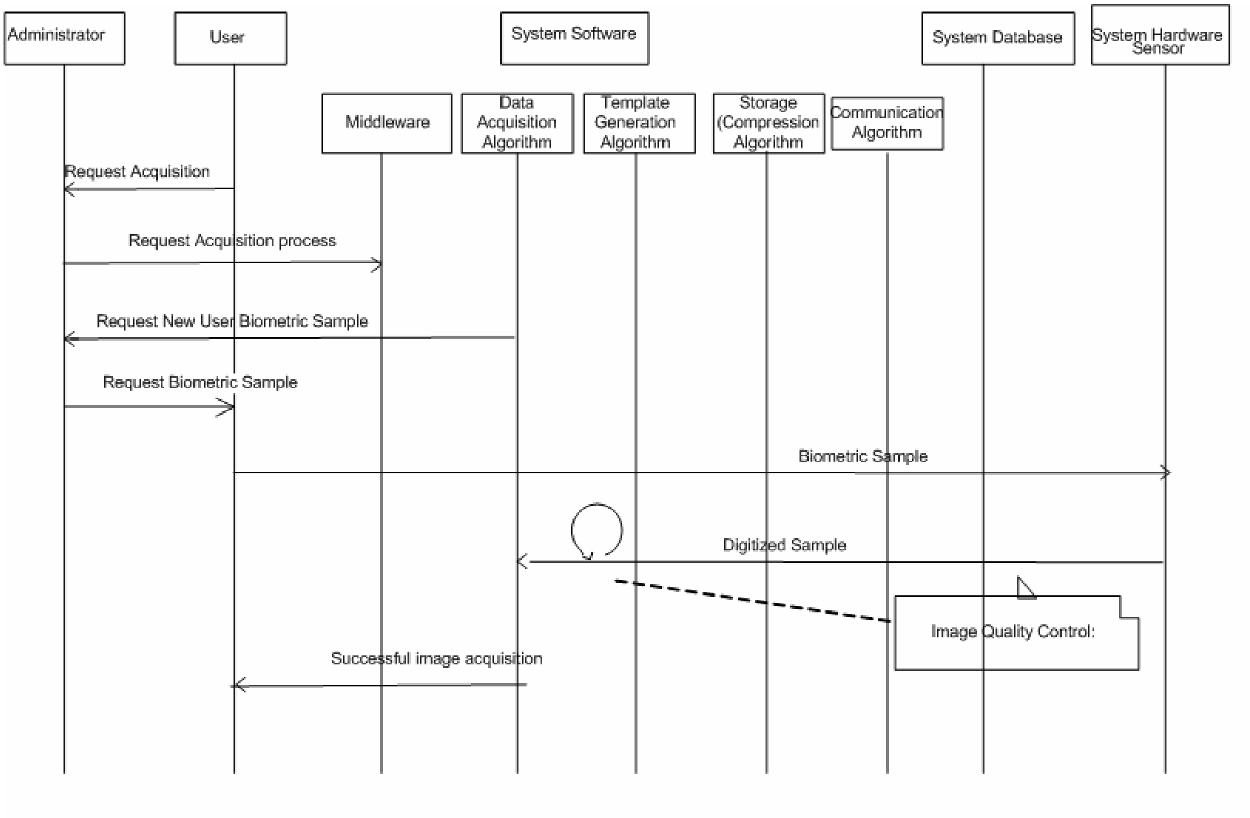


Figure 17. Acquisition Mode

Enrollment is the process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. FTE (Failure to enroll) is the performance parameter that will be affected by this mode. Inputs to the enrollment mode are results from the acquisition mode, the algorithm to use to generate templates, and user specific parameters. Next, a query is done to determine if the user already exists in the user database. Then the user template is generated and quality score is computed. The quality of templates will greatly affect other related operational modes. Poor template quality will propagate throughout the system, diminishing performance. See Figure 18 for a representation [17] .

Verification is 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. This mode will affect V_FRR (Verification False Reject Rate) and V_FAR (Verification False Accept Rate). Inputs to the verification mode are user login information, results from image acquisition, template generation and matching algorithm, and user specific parameters. As shown in Figure 19, the intermediate steps are to generate the user template for matching and then perform a one to one matching on the user database. The result of the verification mode will be a matching score upon which a decision is made [17].

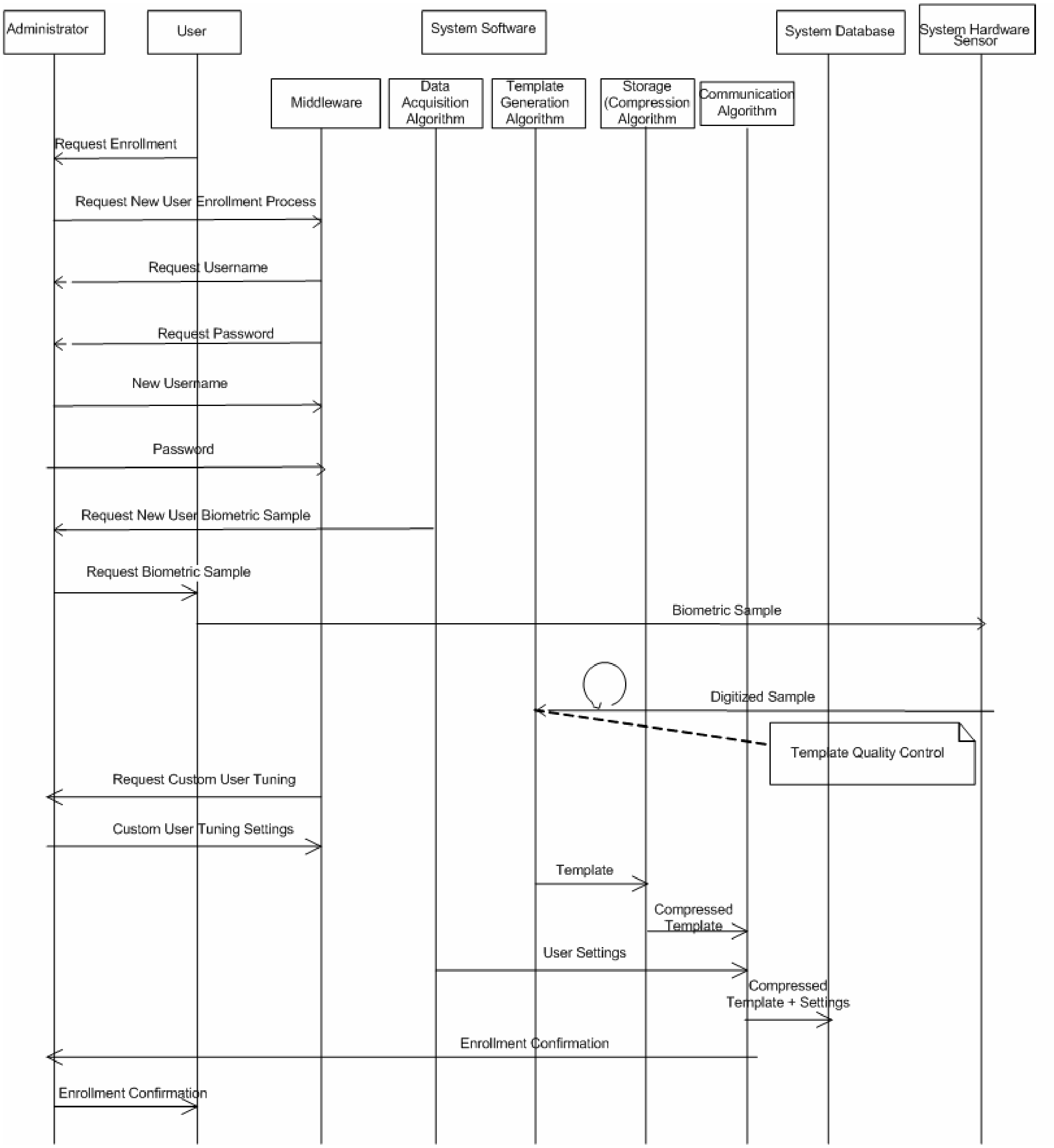


Figure 18. Enrollment Mode

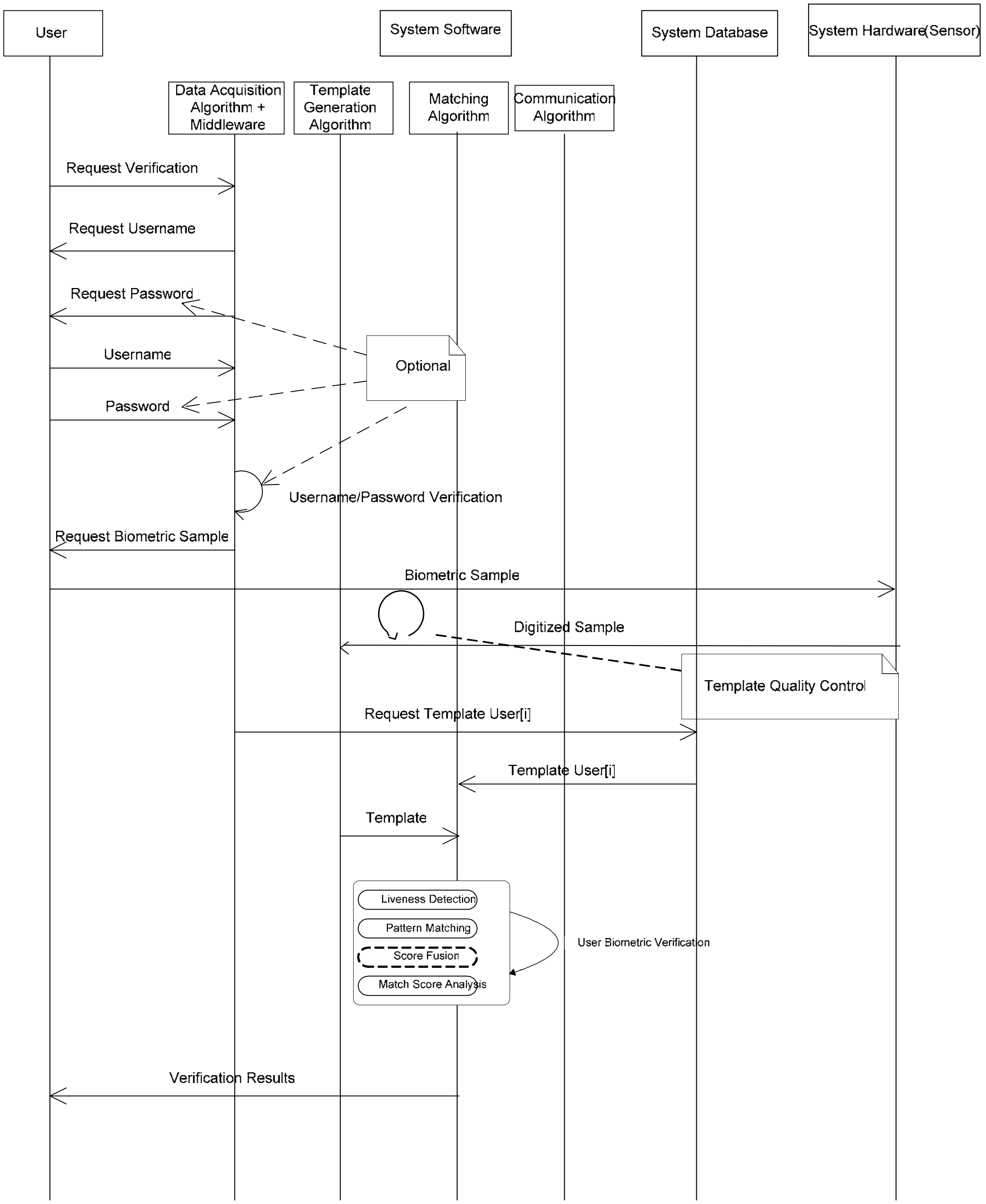


Figure 19. Verification Mode

Identification is 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). This mode will affect I_FRR (Identification False Reject Rate) and I_FAR (Identification False Accept Rate). Inputs to the identification mode are matching algorithm, results from image acquisition, and template generation algorithm. As shown in Figure 20, the intermediate steps are to generate the user template for matching and then perform a one to one matching on the user database. The results of the identification mode will be a matching score upon which a decision is made [17].

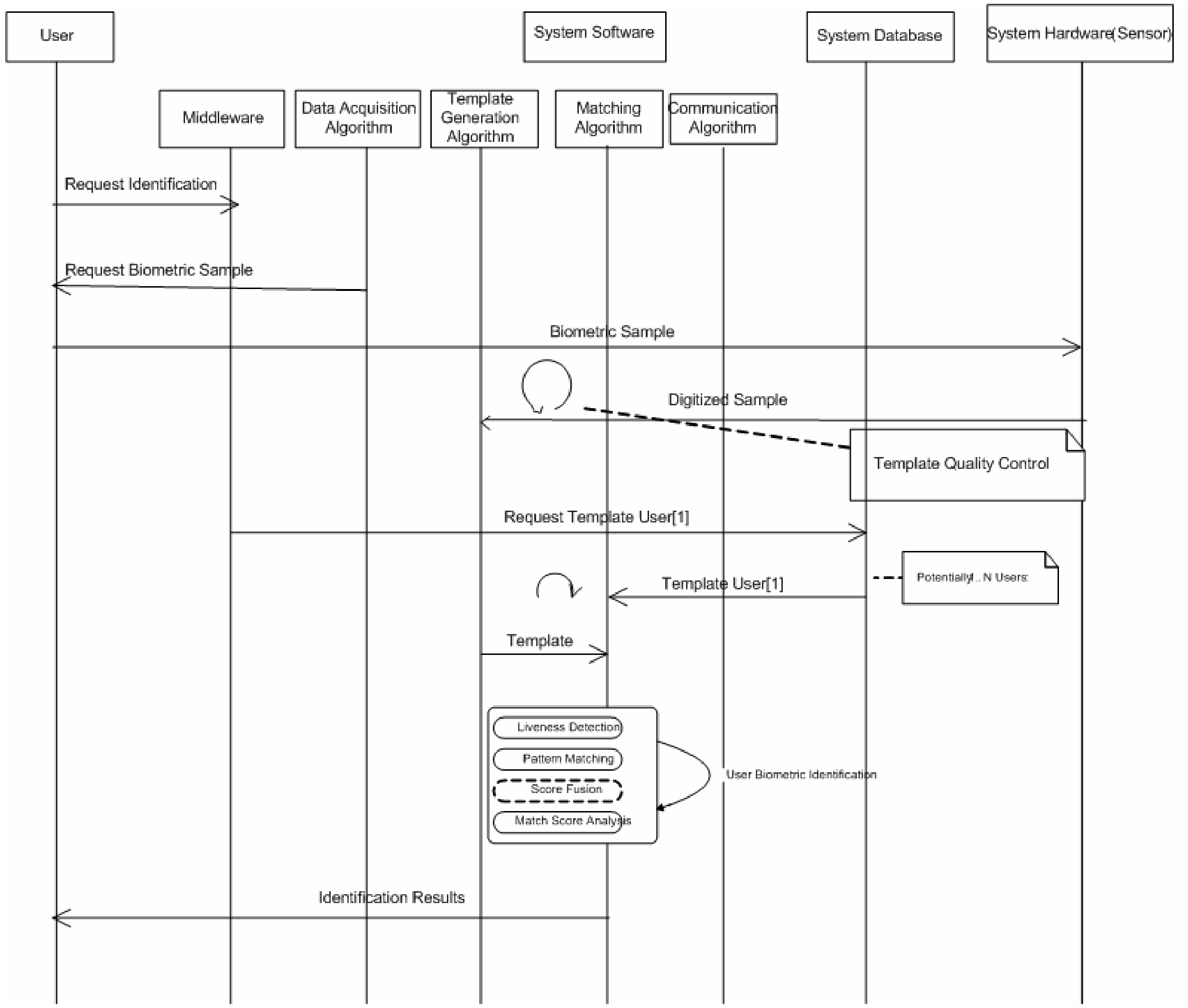


Figure 20. Identification Mode

Template Update is the process of refreshing (re-enrolling) a user's templates stored in the system to counteract template aging. FTE will be affected by this mode. Inputs to the user template update mode are results from the acquisition mode, the algorithm to use to generate templates, and user specific parameters. Next, a query is done to retrieve the user record from the user database. Then the user template is generated and quality score is computed. User templates can vary over time and it is necessary to periodically update user templates to combat template aging. The performance of the biometric system will be greatly affected by how current the templates are in the user database. See Figure 21 for a representation [17].

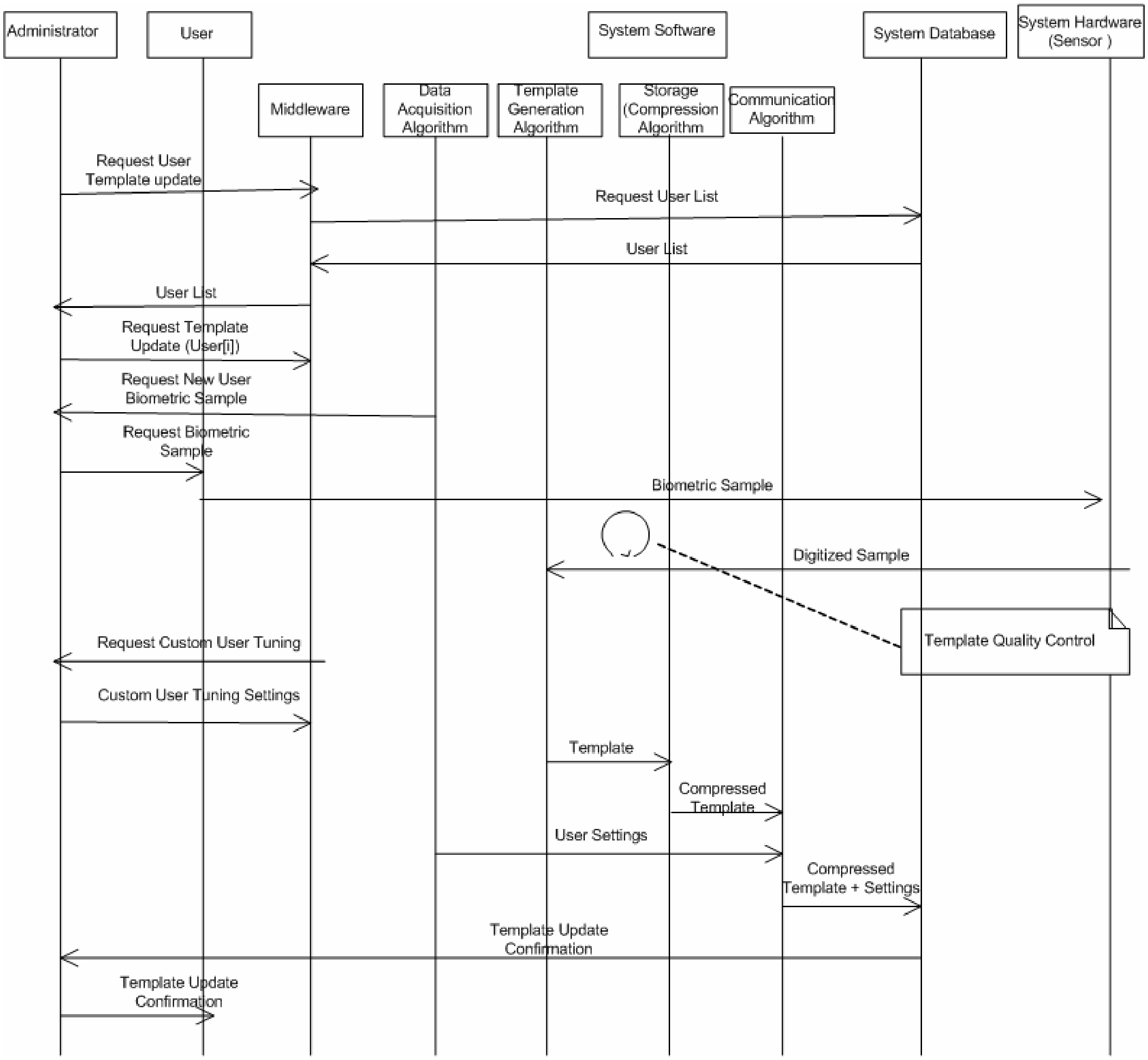

Administrator
User
System Software
System Database
System Hardware (Sensor)
Middleware
Data Acquisition Algorithm
Template Generation Algorithm
Storage (Compression Algorithm
Communication Algorithm
Request User Template update
Request User List
User List
User List
Request Template Update (User[i])
Request New User Biometric Sample
Request Biometric Sample
Biometric Sample
Digitized Sample
Template Quality Control
Request Custom User Tuning
Custom User Tuning Settings
Template
Compressed Template
User Settings
Compressed Template + Settings
Template Update Confirmation
Template Update Confirmation

Figure 21. Template Update Mode

Administrative functionality: This functionality can be divided into the following**:**

- **System Setting Configuration** is the process of setting system configurations like match score threshold, contrast, allowed login attempts etc. The administrator enters the updated system settings and awaits confirmation that the update has been made [17]. See Figure 22.
- **User Removal** is the process of removing users from the system. This requires administrator's involvement. The administrator inputs the identification information of the user to be removed. A query to the user database is performed to verify that the user exists, and then is removed from the database. A confirmation of user removal is outputted from this mode, as shown in Figure 23 [17].
- **User Setting Configuration** is the process of setting configurations like threshold, allowed login attempts of the user. The administrator inputs the identification information of the user to be updated. A query to the user database is performed to verify that the user exists, and to retrieve the user's record. The administrator then enters the updated user specific parameters and awaits confirmation that the update has been made [17]. See Figure 24.

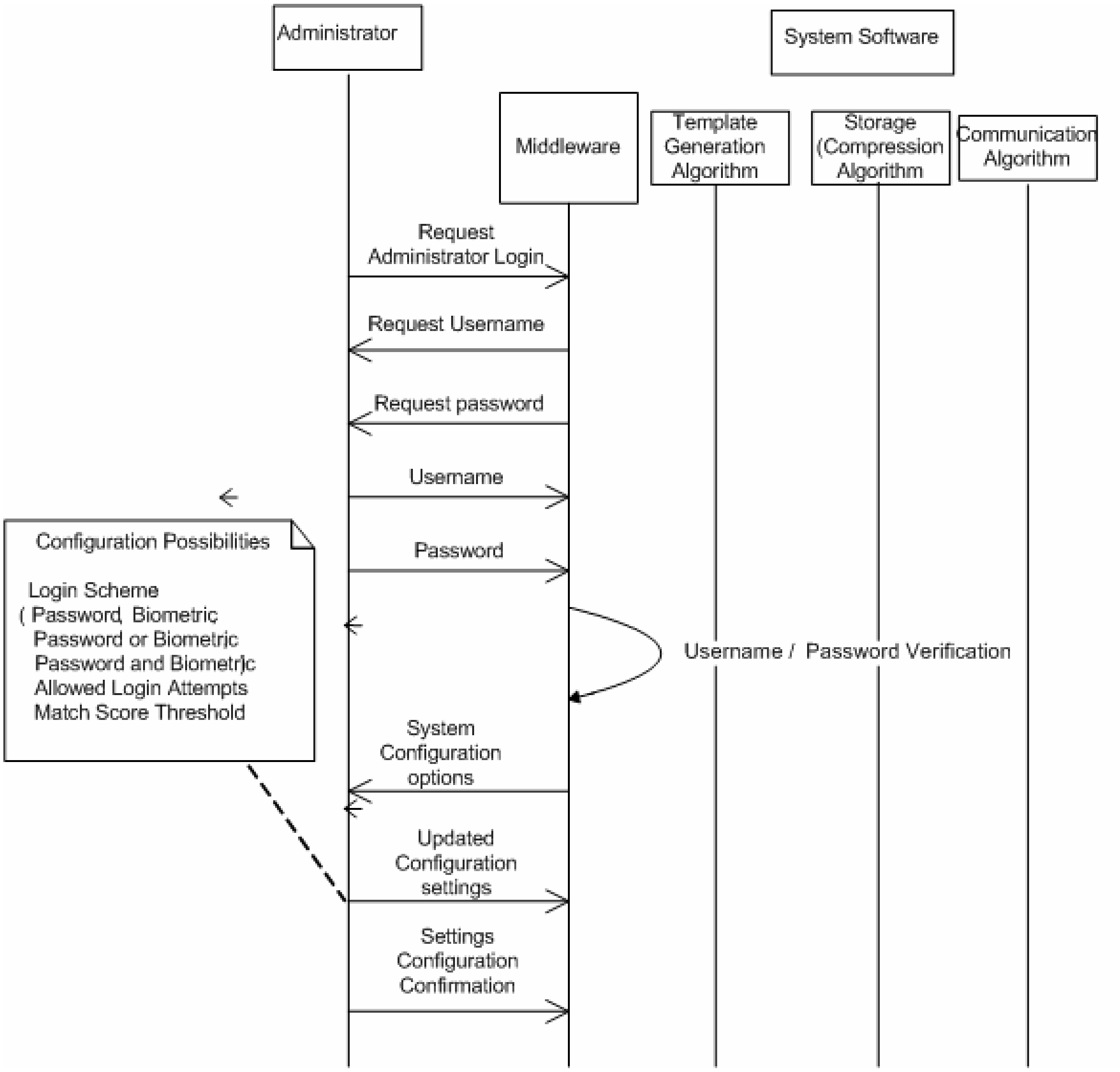

Administrator
System Software
Middleware
Template Generation Algorithm
Storage (Compression Algorithm
Communication Algorithm
Request Administrator Login
Request Username
Request password
Username
Password
Configuration Possibilities
Login Scheme
(Password, Biometric
Password or Biometric
Password and Biometr)c
Allowed Login Attempts
Match Score Threshold
Username / Password Verification
System Configuration options
Updated Configuration settings
Settings Configuration Confirmation

Figure 22. System Setting Configuration Mode

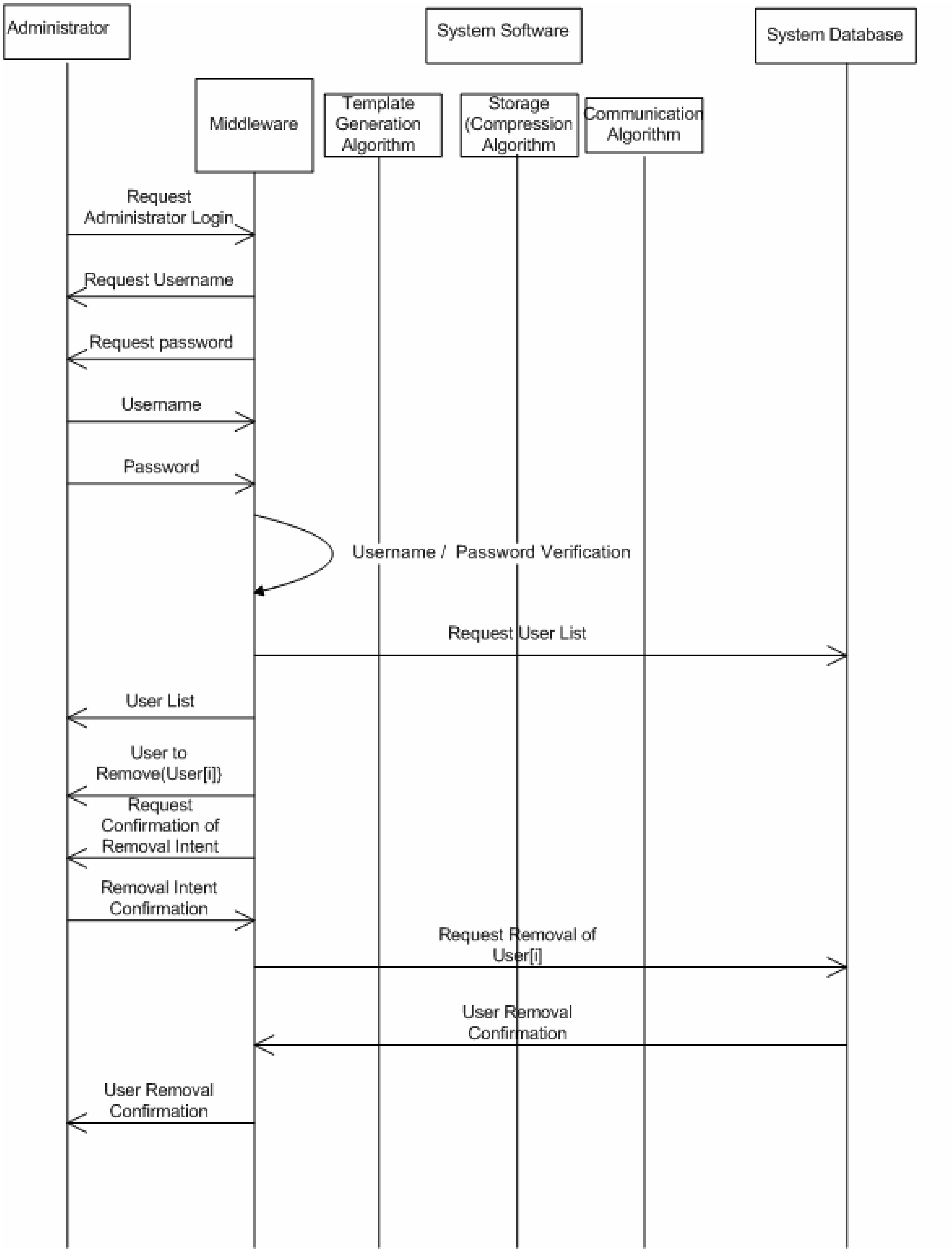

Administrator
System Software
System Database
Middleware
Template Generation Algorithm
Storage (Compression Algorithm
Communication Algorithm
Request Administrator Login
Request Username
Request password
Username
Password
Username / Password Verification
Request User List
User List
User to Remove(User[i])
Request Confirmation of Removal Intent
Removal Intent Confirmation
Request Removal of User[i]
User Removal Confirmation
User Removal Confirmation

Figure 23. User Removal Mode

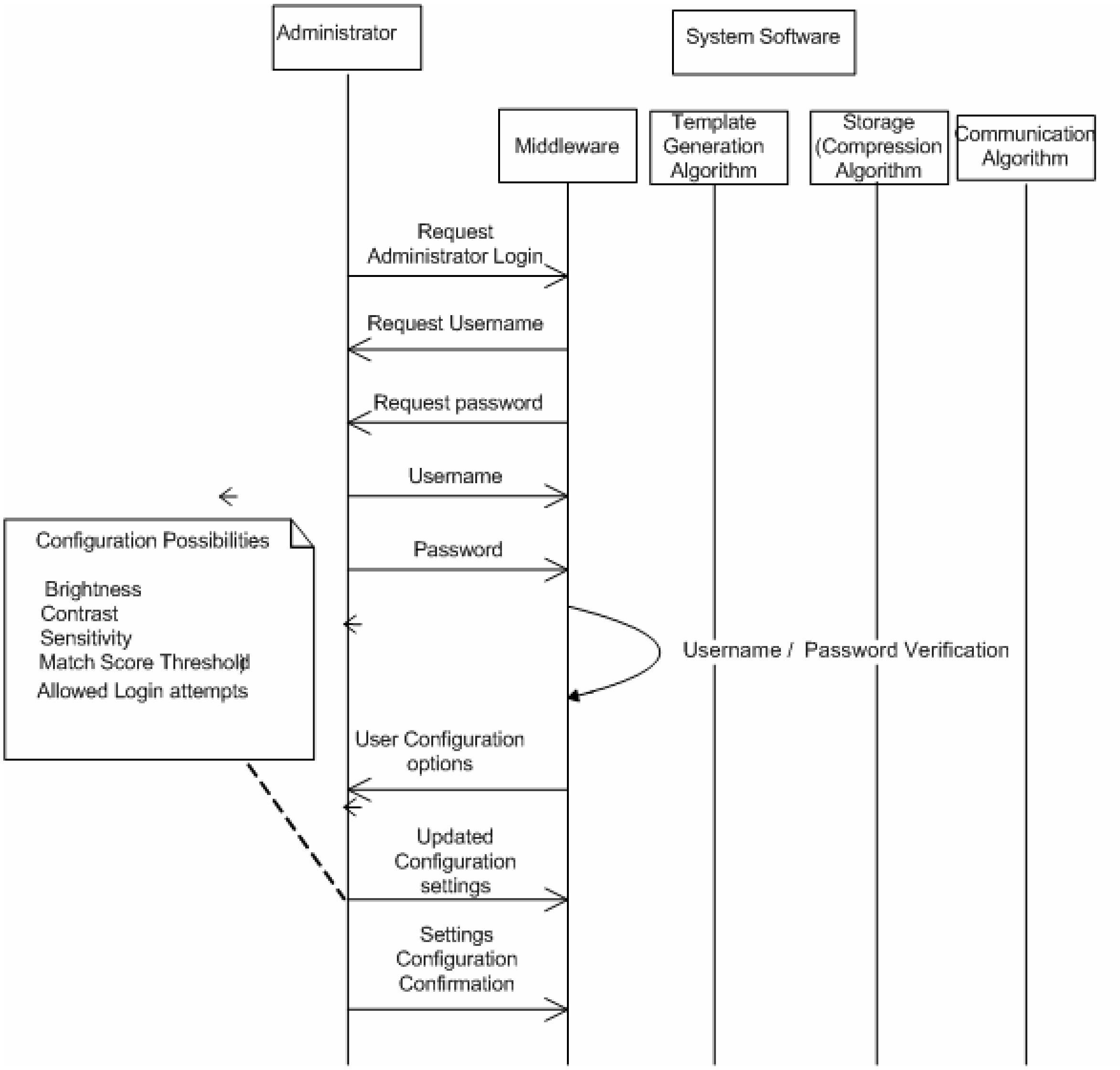

Administrator
System Software
Middleware
Template Generation Algorithm
Storage (Compression Algorithm
Communication Algorithm
Request Administrator Login
Request Username
Request password
Username
Password
Configuration Possibilities
Brightness
Contrast
Sensitivity
Match Score Threshold
Allowed Login attempts
Username / Password Verification
User Configuration options
Updated Configuration settings
Settings Configuration Confirmation

Figure 24. Update User Setting Configuration Mode

3.2 Variables Affecting Biometric System Performance

The key to achieving repeatable testing is to develop testing protocols that identify and adapt to the variables that can affect biometric system performance. However, this task is extremely difficult. Some variables that have been considered for an optical fingerprint system in this document are divided into the following categories: subject, biometric presentation, system maintenance, environmental factors, and device placement. Subject variables are also referred to as human factors and can consist of user training, biometric presentation: angle of rotation and translation, presentation of biometric trait, covert/overt, attended/non-attended, cooperative/non-cooperative, gender, age, demographics, population size, template aging, user health conditions, and user profession. Some environmental factors that can affect performance are temperature, humidity, and lighting. Some biometric placement variables than can affect performance are angle of rotation, translation, and quality of image. Some variables than can affect device placement are angles of pan and tilt of the sensor.

3.3 Hardware Used

In this research, certain equipment was needed to aid in the testing of the fingerprint sensor. Below is a listing of equipment used in this research.

- Temperature/Humidity Meter

  A temperature and humidity meter was used to measure the test environment's temperature and relative humidity. The meter used in this testing was: Amprobe Digital Sling Psychrometer: THWD-2i. It is able to measure temperature in the range of -20 to 60° Celsius and relative humidity in the range of 1 to 99%.

- Light Meter

  A light meter was used to measure luminance of the test environment in lux, which is lumens per square meter [27].

- Robotic Tripod

  The robotic tripod is used to control the device placement variables, angles of pan and tilt. The device used it called "Tracker Pod" and is offered at www.trackercam.com. The angles can be controlled through a USB port on a pc using the software included.

- Secugen Sensor

  The optical fingerprint sensor used throughout this research is Secugen EyeD Hamster, model: HFDFU01A. See Appendix B for more information.

- Lamp w/ 60 watt bulb

  This single bulb desk lamp was used in the lighting protocol and was used to in conjunction with a lamp dimmer to regulate light intensity on the fingerprint sensor.

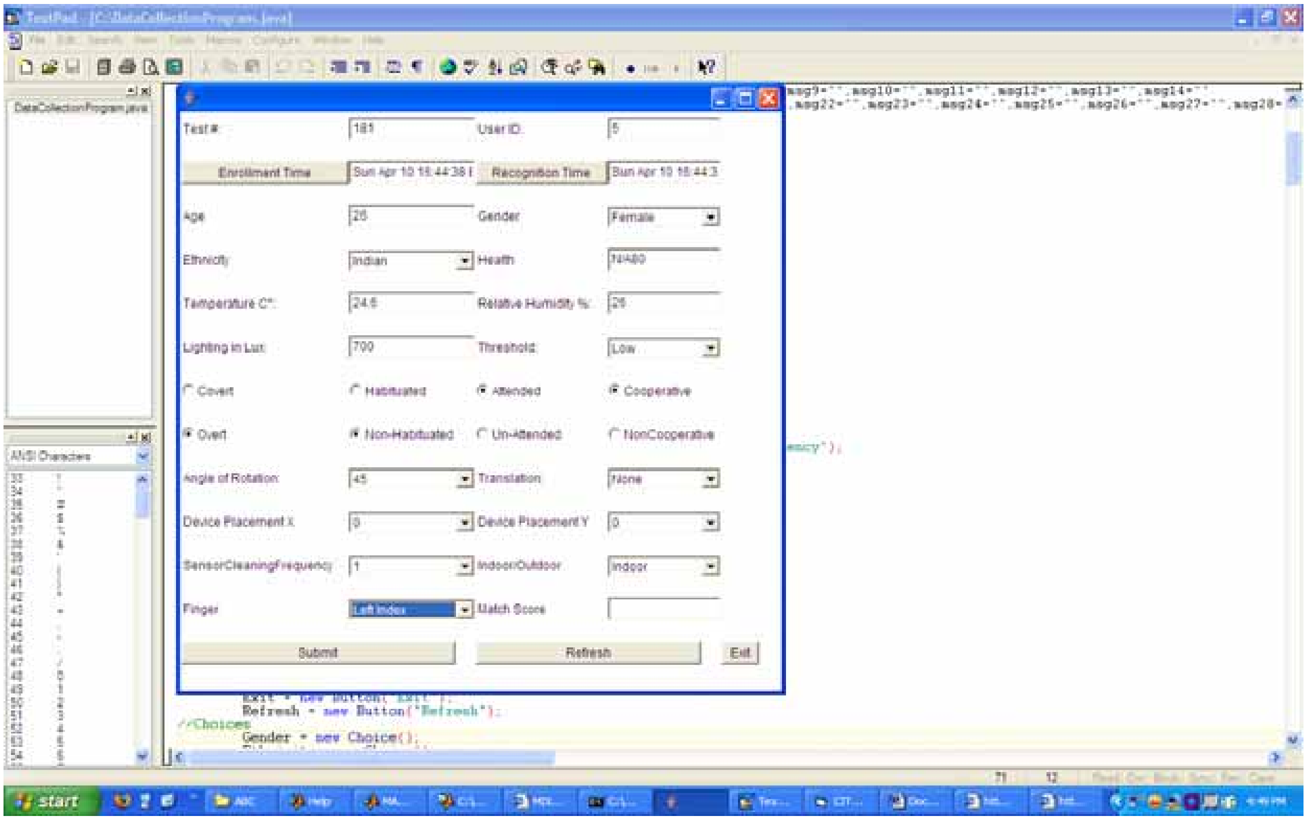
- Lamp Dimmer

  The lamp dimmer used in this research was made a Lutron 300 Watt White Credenza® Lamp Dimmer. Model Number: TT300NLH-WH

3.4 Software Used

- Data Collection Software

  Data collection software was used in this research to aid in the documentation of user and environmental information important to testing. The goal of this software is to help reduce data collection errors which will hopefully result in more accurate test results. The Data Collection Software used in this research was written by West Virginia University student Gaurav Gupta. See Figure 25 for a screen shot.


TextPad - [C:\DataCollectionProgram.java]
DataCollectionProgram.java
ANSI Characters
start

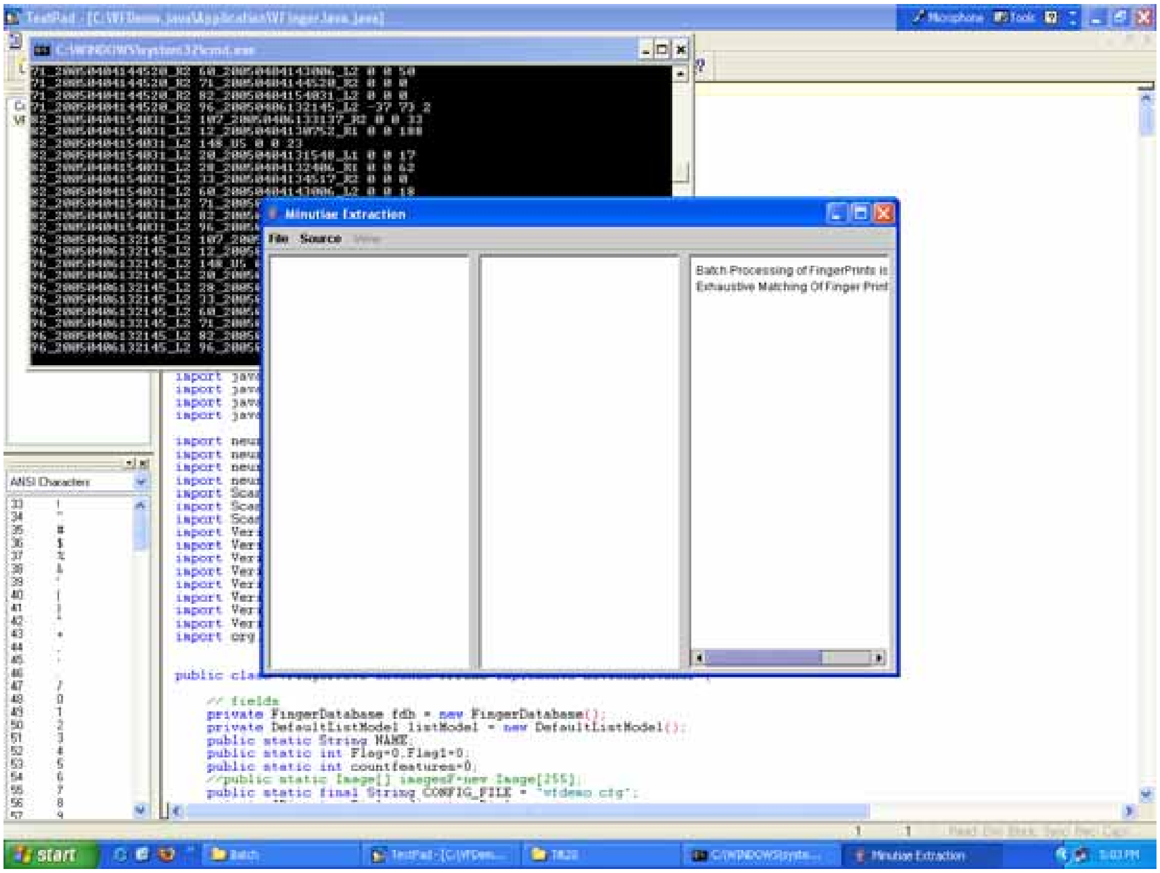
Test #	181	User ID	5
Enrollment Time	Sun Apr 10 15:44:38 I	Recognition Time	Sun Apr 10 15:44:3
Age	26	Gender	Female
Ethnicity	Indian	Health	N/A80
Temperature C°:	24.6	Relative Humidity %:	26
Lighting in Lux:	700	Threshold:	Low
○ Covert	○ Habituated	● Attended	● Cooperative
● Overt	● Non-Habituated	○ Un-Attended	○ NonCooperative
Angle of Rotation:	45	Translation	None
Device Placement X	0	Device Placement Y	0
SensorCleaningFrequency	1	Indoor/Outdoor	Indoor
Finger	Left Index	Match Score	

```
        Refresh = new Button("Refresh");
//Choices
        Gender = new Choice();
```

Figure 25. Data Collection Software Screenshot

- Verifinger: Modified Version

Once the raw image was captured, a modified version of Neurotechnologija's Verfinger version 4.1 software was used to generate match scores and to determine the number of minutiae points matched between two fingerprints. See Figure 26 for a screen shot.



```
71_20050404144520_R2 60_20050404143006_L2 0 0 50
71_20050404144520_R2 71_20050404144520_R2 0 0 0
71_20050404144520_R2 82_20050404154031_L2 0 0 0
71_20050404144520_R2 96_20050406132145_L2 -37 73 2
82_20050404154031_L2 107_20050406133137_R2 0 0 33
82_20050404154031_L2 12_20050404130752_R1 0 0 100
82_20050404154031_L2 148_US 0 0 23
82_20050404154031_L2 20_20050404131540_L1 0 0 17
82_20050404154031_L2 28_20050404132406_R1 0 0 62
82_20050404154031_L2 33_20050404134517_R2 0 0 0
82_20050404154031_L2 60_20050404143006_L2 0 0 18
82_20050404154031_L2 71_2005
82_20050404154031_L2 82_2005
82_20050404154031_L2 96_2005
96_20050406132145_L2 107_2005
96_20050406132145_L2 12_2005
96_20050406132145_L2 148_US
96_20050406132145_L2 20_2005
96_20050406132145_L2 28_2005
96_20050406132145_L2 33_2005
96_20050406132145_L2 60_2005
96_20050406132145_L2 71_2005
96_20050406132145_L2 82_2005
96_20050406132145_L2 96_2005
```

Batch Processing of FingerPrints is
Exhaustive Matching Of Finger Print

```
import jav
import jav
import jav
import jav

import neu
import neu
import neu
import neu
import Sca
import Sca
import Sca
import Ver
import Ver
import Ver
import Ver
import Ver
import Ver
import Ver
import Ver
import org

public cla

    // fields
    private FingerDatabase fdb = new FingerDatabase();
    private DefaultListModel listModel = new DefaultListModel();
    public static String NAME;
    public static int Flag=0,Flag1=0;
    public static int countfeatures=0;
    //public static Image[] imagesF=new Image[255];
    public static final String CONFIG_FILE = "vfdemo.cfg";
```

Figure 26. Verifinger Software Screenshot

- SecuGen SDK

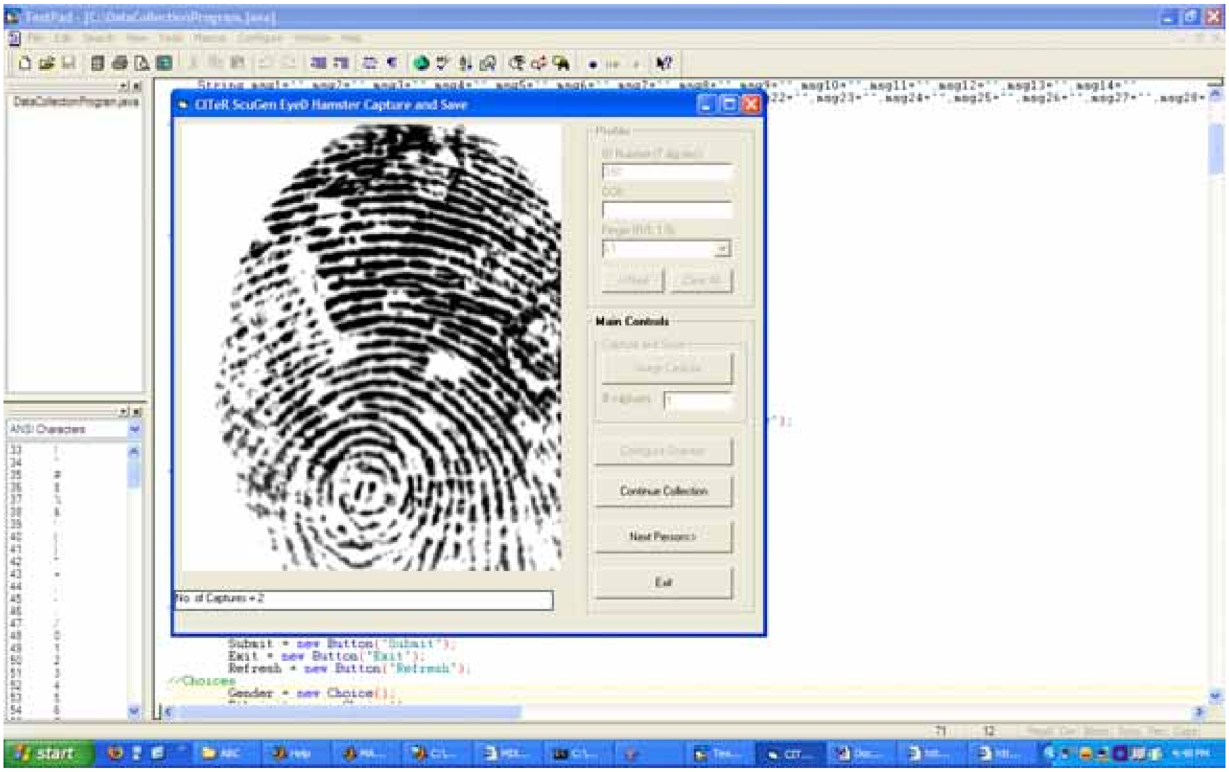
The Software Development Kit used in this research was for the SecuGen Hamster optical fingerprint sensor. The software is named: FDx Development Kit by SecuGen.

- Robotic Tripod Software

This software came with the "Trackerpod" robotic tripod as noted above. The software is titled: TrackerCam, version 5.12. This software controls the "Trackerpod" via a USB port.

- CITER Raw Image Capture Software

In this research, raw image capture software developed by CITER (Center for Identification Technology Research) was used to capture raw images in conjunction with the SDK (Software Development Kit) for the Secugen Hamster optical fingerprint sensor. This software has also been used in the data collection for work described in: [4]. See Figure 27 for a screen shot.



No. of Captures = 2

```
        Submit = new Button("Submit");
        Exit = new Button("Exit");
        Refresh = new Button("Refresh");
//Choices
        Gender = new Choice();
```

Figure 27. Raw Data Collection Software Screenshot

3.5 Protocols

In this research, scenario based testing protocols have been developed for unhabituated and cooperative users in testing that is attended and overt. Rosiek and Gupta's paper have identified some 50 variables that can possibly affect biometric system performance. In this scenario testing, the image acquisition mode has been selected as the basis for all testing protocols. It has been chosen to test protocols in the image acquisition mode because poor quality fingerprint images are difficult to match and offer worse accuracy than on good quality fingerprint images [28]. Another reason for this choice is that the image acquisition mode's output is used by enrollment, identification, and verification modes of operation, thus broadening the scope of testing. Therefore it is important to identify which variables can affect the image acquisition mode, i.e. affect the fingerprint sensor during acquisition, when developing testing protocols.

The protocols in Appendix A have been written to reduce systematic errors and accommodate for the variables that can affect the fingerprint sensor during image acquisition. The protocols in Appendix A have been written to test following variables:

1. Biometric Presentation: Angle of Rotation and Translation
2. Lighting
3. Device Placement

The protocols in Appendix A were implemented as follows:

- Environmental Chambers

  Ideally, environmentally controlled chambers should be used to help control environmental factors and to help improve the repeatability of testing. In this research, such chambers were not available.

- Repeatability of Testing

  Many steps were taken to help improve the repeatability of testing. Various masks were created to aid in the repeatability of testing protocols. A software tool was used to document environmental conditions, user characteristics (not name), and other variables to keep track of each biometric sample and to reduce the chances of error in reporting testing data. This software was developed by Gaurav Gupta.

- Data Collection

  Raw image capture software which was developed for CITER which allowed for the capture of raw fingerprint images for the SecuGen fingerprint sensor was used in this testing. Raw data was collected for 10 users for all protocols mentioned in Appendix A. Due to time constraints and limited user availability, 10 users were all that was possible for this work. Steps were followed for the following protocols with some minor changes as noted in this section: Lighting, Biometric Presentation: angle of rotation and translation, and Device Placement. Refer to Appendix A for a detailed explanation of these protocols.

- Match Score Generation

  Once all of the biometric samples were collected, analysis of these samples was done offline. Offline testing allows for multiple tests without the reacquisition of data and more in depth analysis. Using a modified version of Verifinger software, mentioned above, genuine and imposter match scores were computed from the test data. The result of each comparison gave a match score, translation along x and y axis , angle, and number of minutiae points matched. For genuine match scores, each image taken per user per protocol is matched to the genuine user’s fingerprint image taken at an angle of rotation of

90 degrees and no translation, please refer to Appendix A for these parameter definitions. In this research, I computed imposter match scores by matching the genuine user's fingerprints under each protocol compare to other users whose fingerprints were placed with an angle of rotation of 90 degrees and no translation.

- Ceiling Lighting

Ceiling lighting is important to consider in optical fingerprint sensors. This is mainly due to the creation of shadows that are imaged by the sensor. See Figure 28 for a diagram of the overhead lighting used during testing.

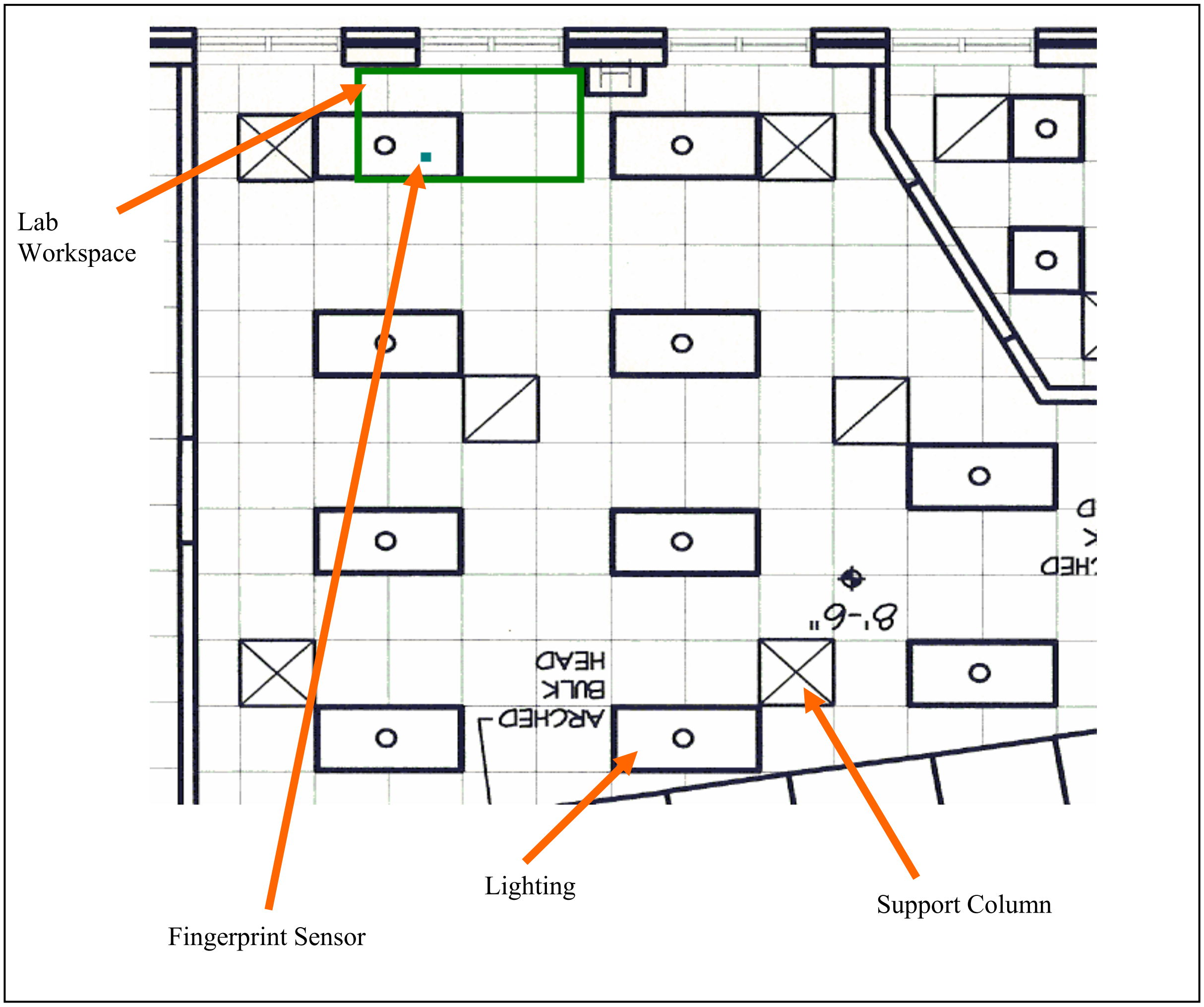


Figure 28. Overhead Lighting Setup

3.5.1 Biometric Presentation

Testing was performed in two steps, one for angle of rotation and the second was translation. See Figure 29 for setup of devices for testing both protocols. This figure shows the environmental meters as well as the SecuGen optical fingerprint sensor with the angle of rotation mask applied.

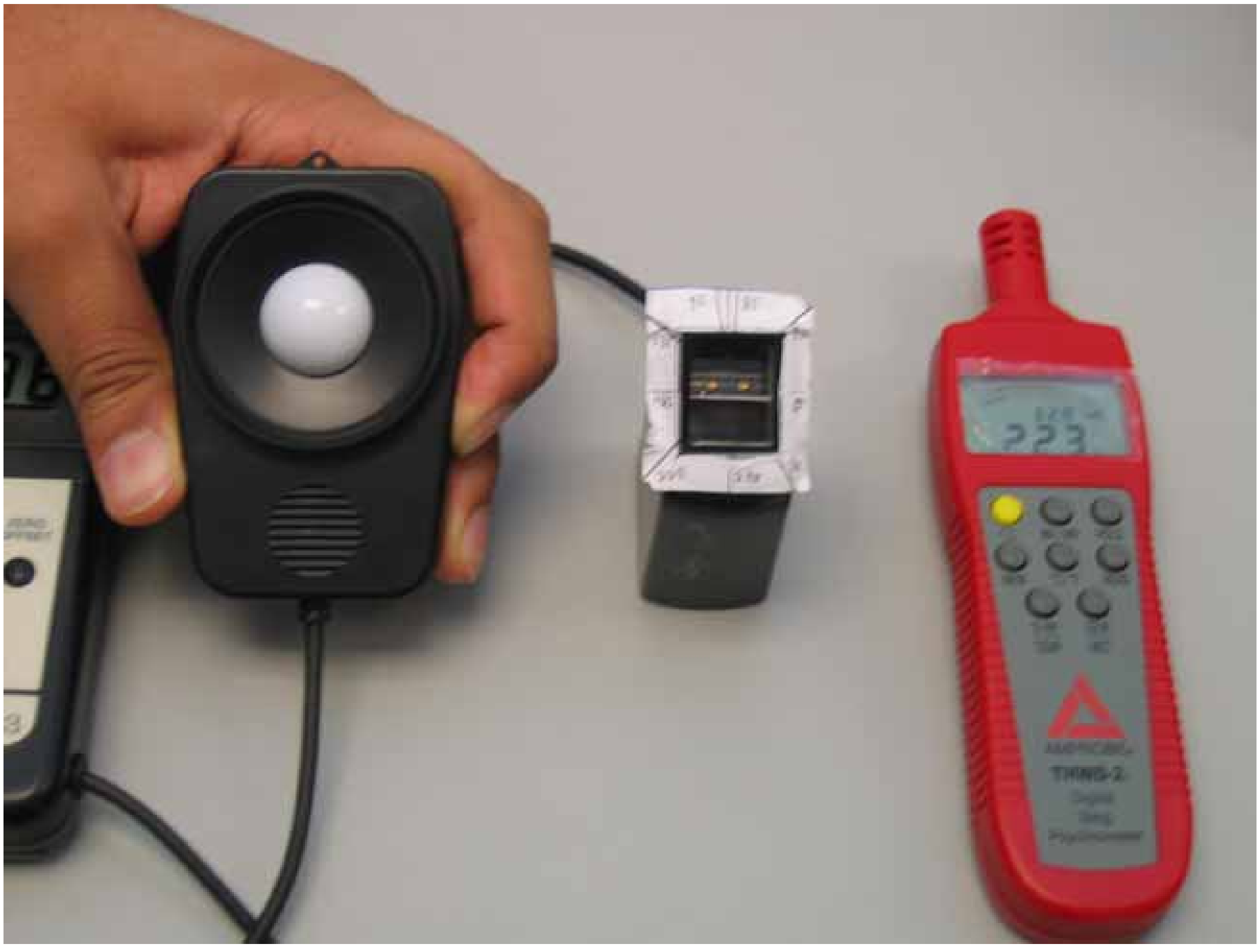


Figure 29. Test Setup Image

Angle of Rotation:

Testing was performed for the following angles of rotation for all users: 0, 45, 85, 90, 95, 135, 180, and 270 degrees. See Appendix A for more details.

Translation:

With the SecuGen optical fingerprint sensor, it was determined that using the four quadrant cut-outs would cause the sensor to be unable to image fingerprints, every attempt would result in a Failure to Acquire. Thus, two cutouts were used, A and B. They were created as shown in Figure 30.

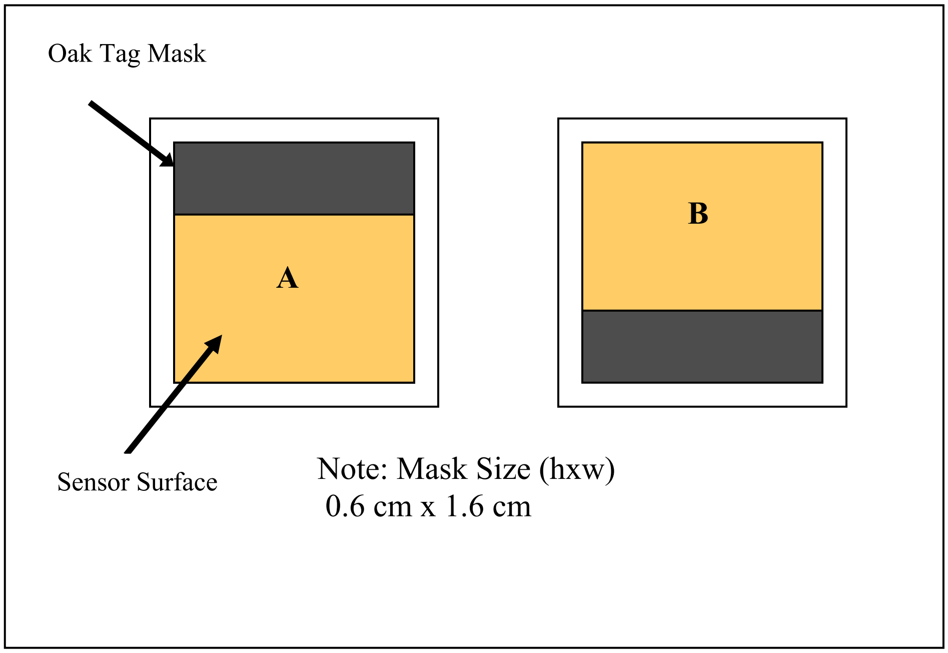


Figure 30. Oak Tag Masks for Optical Fingerprint Sensor

3.5.2 Lighting

For the lighting protocol, a desk lamp with lamp dimmer was used to alter lighting conditions. In this case it is important to keep the test subject's body out of the experiment. This will help to isolate the effect of lighting on the optical fingerprint sensor performance. To accomplish this, the equipment was setup as shown in Figure 31 in a dark room. The center of the sensor was 20 cm from the base of the lamp's neck and the center of the light bulb was 16 cm away from the center of the surface at an angle of 60 degrees. The SecuGen Hamster sensor states that it will work up to 4000 lux, however our lighting system was only able to produce up to 1100 lux. See Figures 31 and 32 for images of the lighting protocol setup.

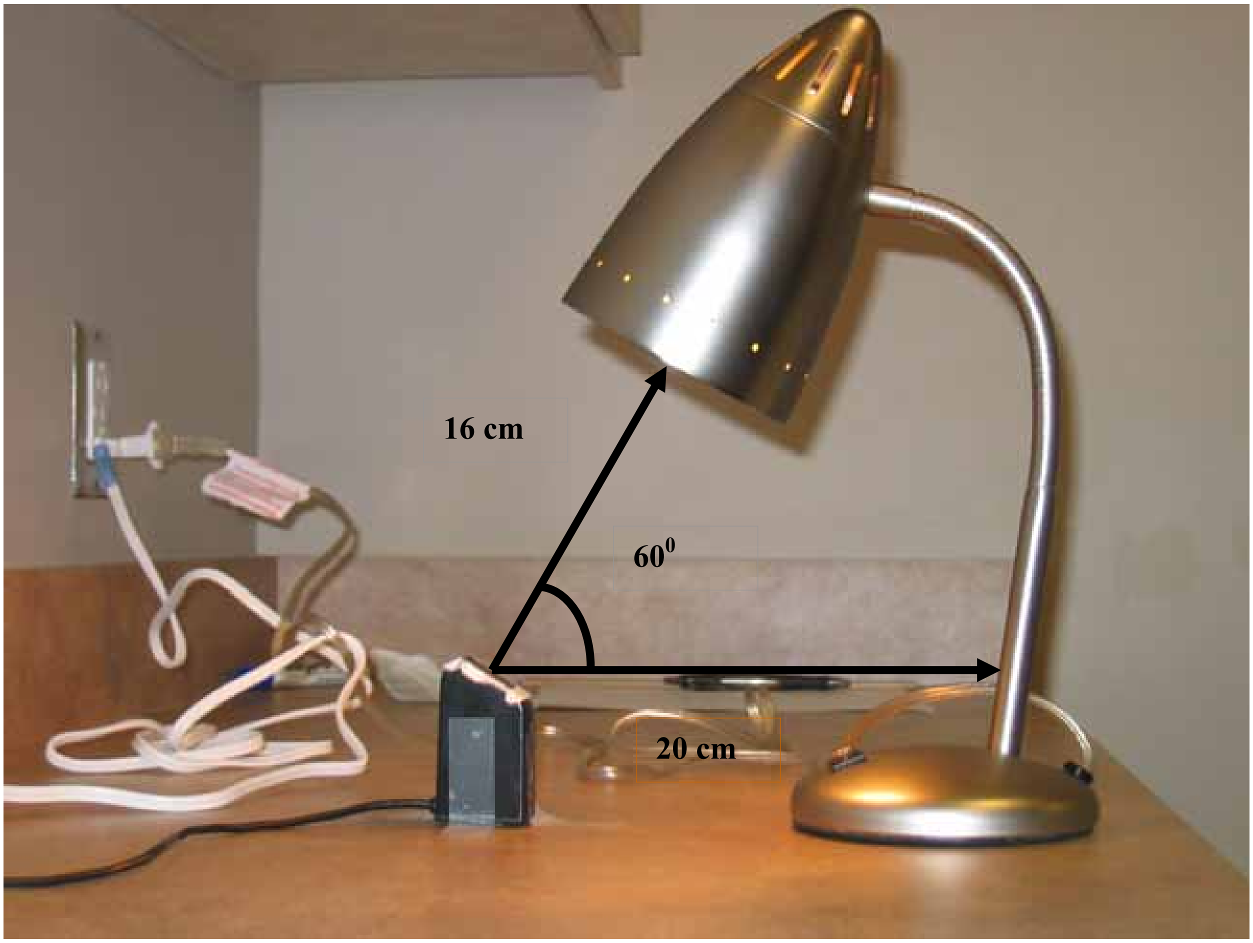


Figure 31. Lighting Protocol Test Setup (side view)

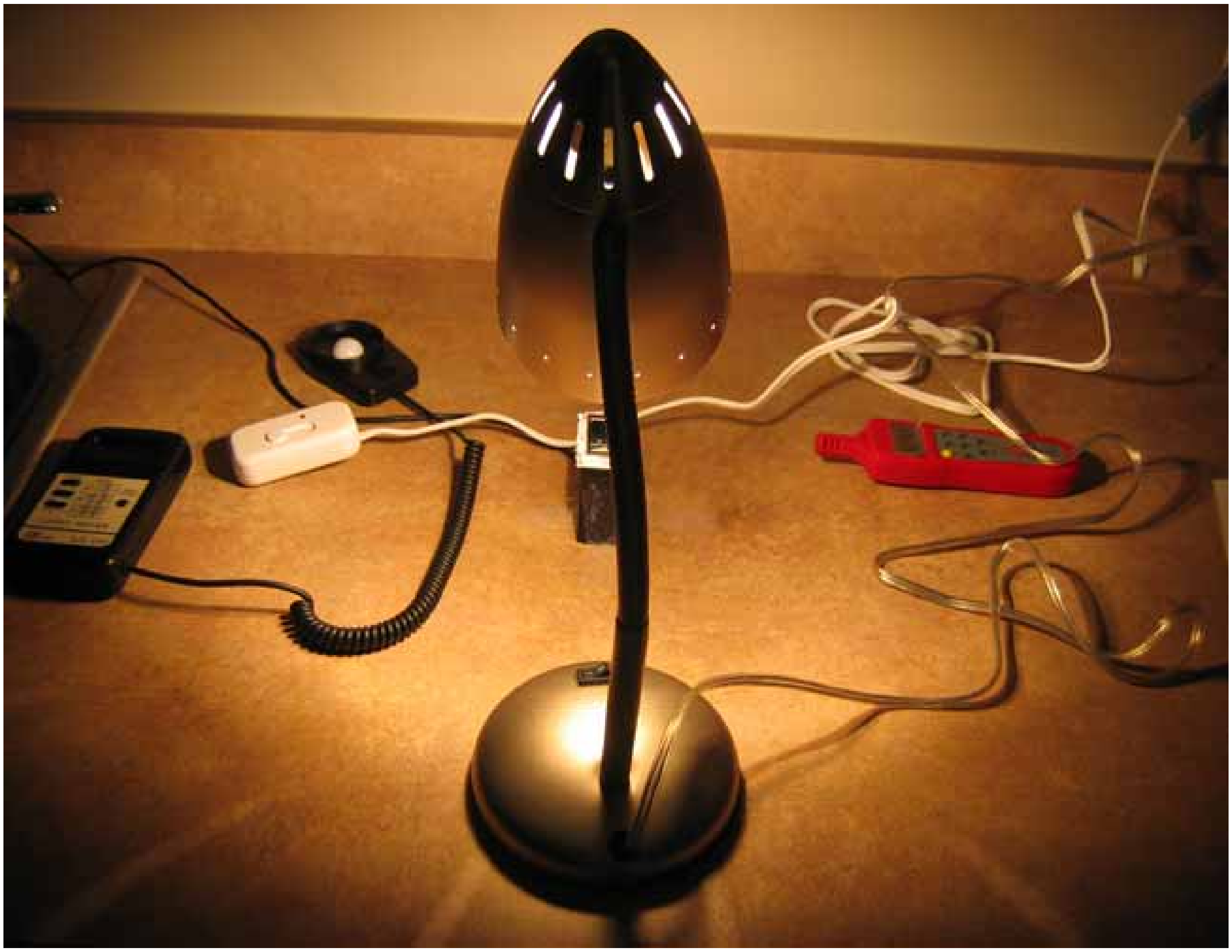


Figure 32. Lighting Protocol Test Setup

3.5.3 Device Placement

Device Placement protocol was tested per the instructions stated above and in Appendix A. See Figure 33 for a photograph of the device setup for testing. Pan angles of 20 and -20 degrees, as well as tilt angles of 20 and -20 degrees were tested and compared to pan and tilt angles of 0 degrees.

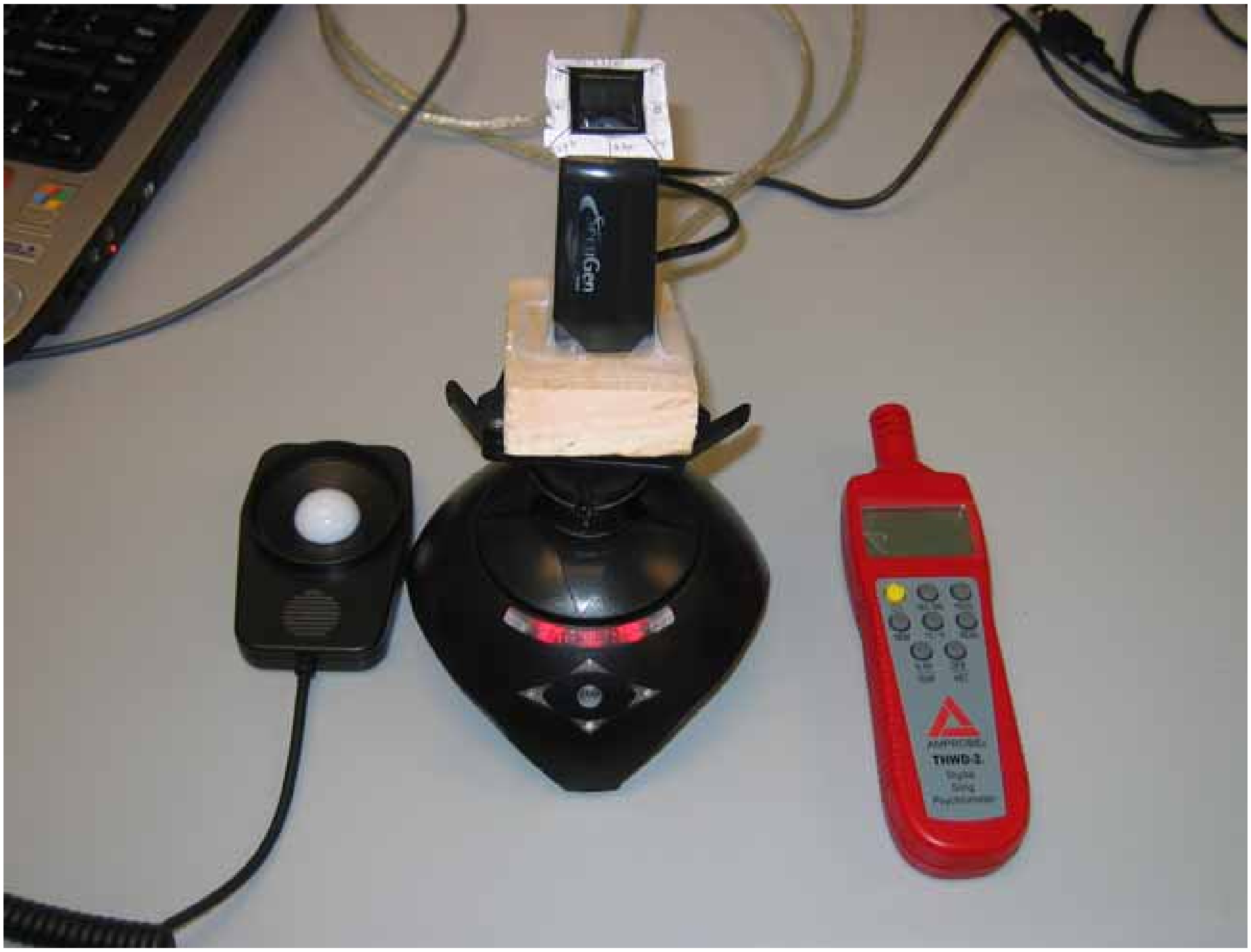


Figure 33. Device Placement Setup

Chapter 4. Results and Analysis

4.1 Results

Due to a lack of time, I was limited to the number of volunteers used in testing these protocols. Ten users volunteered, and offered fingerprints to test the protocols discussed above. Once fingerprint images were captured, match scores were generated as described in Section 3.5. To better depict the results of the testing, various methods were used to display the test results. In Figures 34 to 41, graphs were created that show the average number of minutiae points matched for all ten genuine users and the average genuine match scores for all ten users. No user had noted any major health conditions and had an average age of 33 years old. It was assumed that users were not habituated to the system, since each sample taken was at different positions. Figure 34 shows the average match score for all ten users at various angles of rotation when compared to the genuine user's fingerprint at 90 degrees angle of rotation. It should be noted that angles of rotation 85, 90, and 95 produced the highest average match scores, and that an angle of rotation of 95 produced the highest average match score.

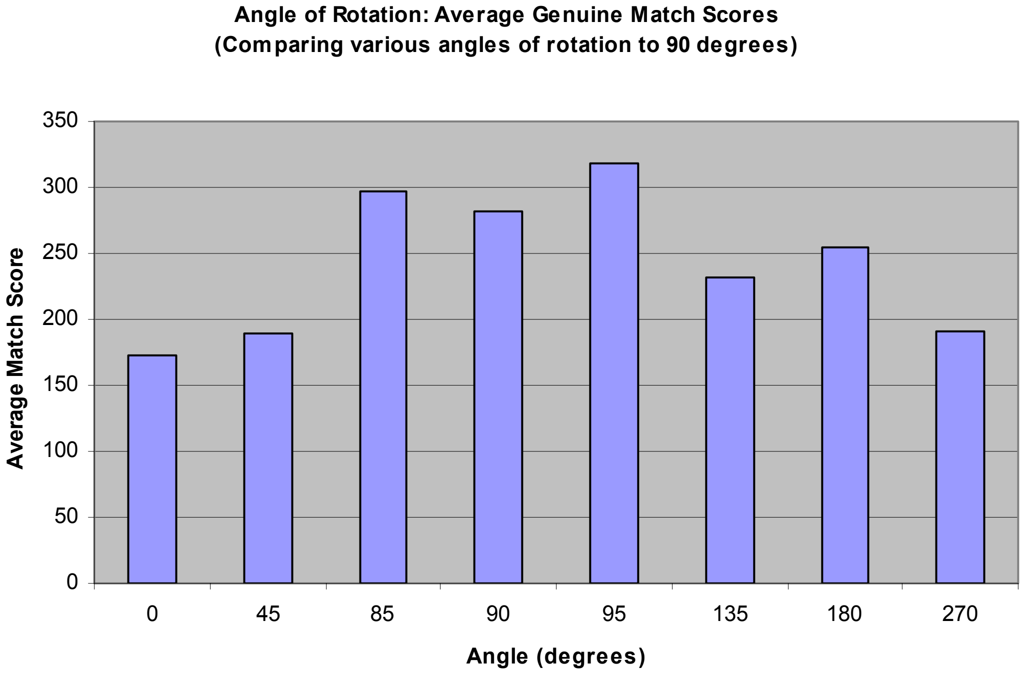


Figure 34. Average Genuine Match Score for Angle of Rotation

Figure 35 shows the average number of minutiae points matched for all ten users at various angles of rotation when compared to the genuine user's fingerprint at 90 degrees angle of rotation. It should be noted that angles of rotation 85, 90, 135, and 95 produced the highest average number of minutiae points matches, and that an angle of rotation of 95 produced the highest average number of minutiae points matched.

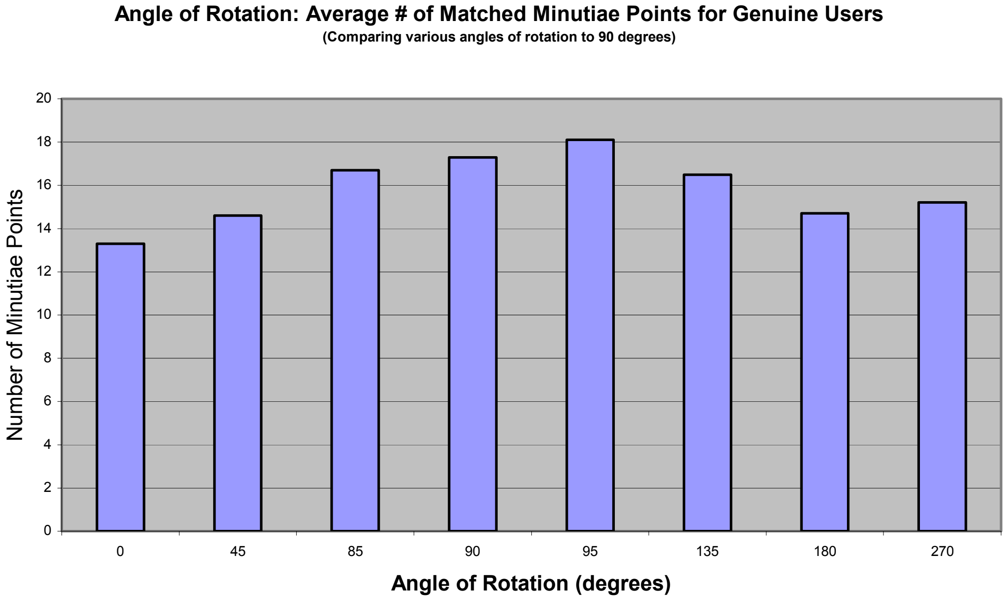


Figure 35. Average # Minutiae Points Matched for Angle of Rotation

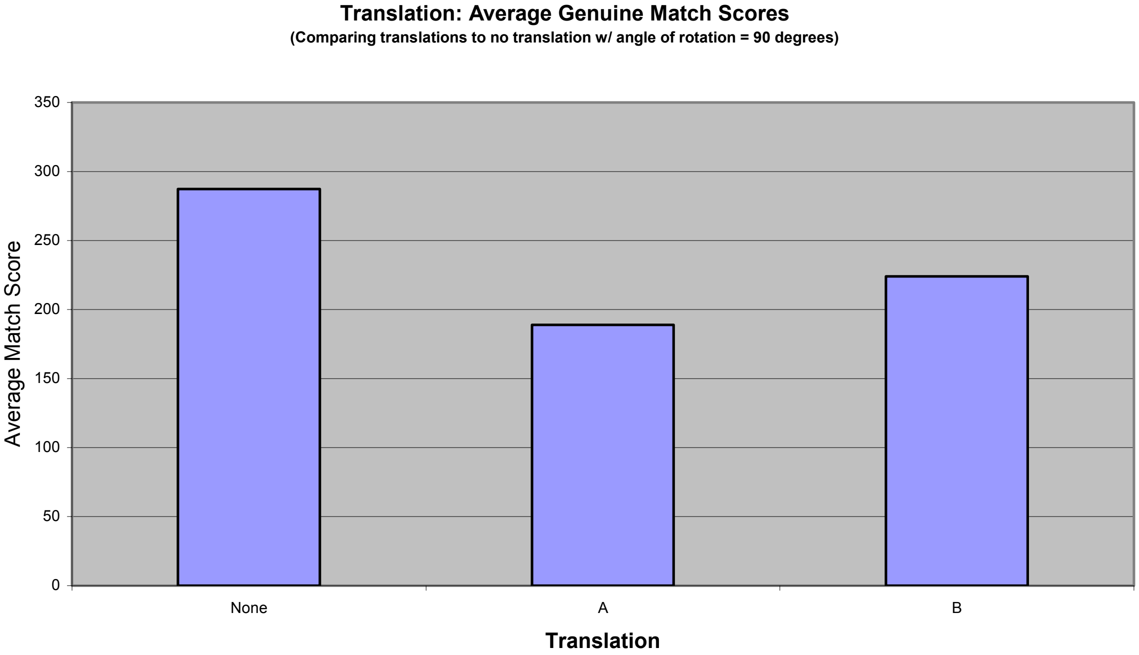


Figure 36. Average Genuine Match Score for Translation

Figure 36 shows the average match score for all ten users at translation schemes when compared to the genuine user's fingerprint at 90 degrees angle of rotation and no translation.

When the translation masks were used as noted in Appendix A, the sensor was unable to detect a finger, resulting in a FTA of 100. It should be noted that when translation is introduced, the average match score is reduced.

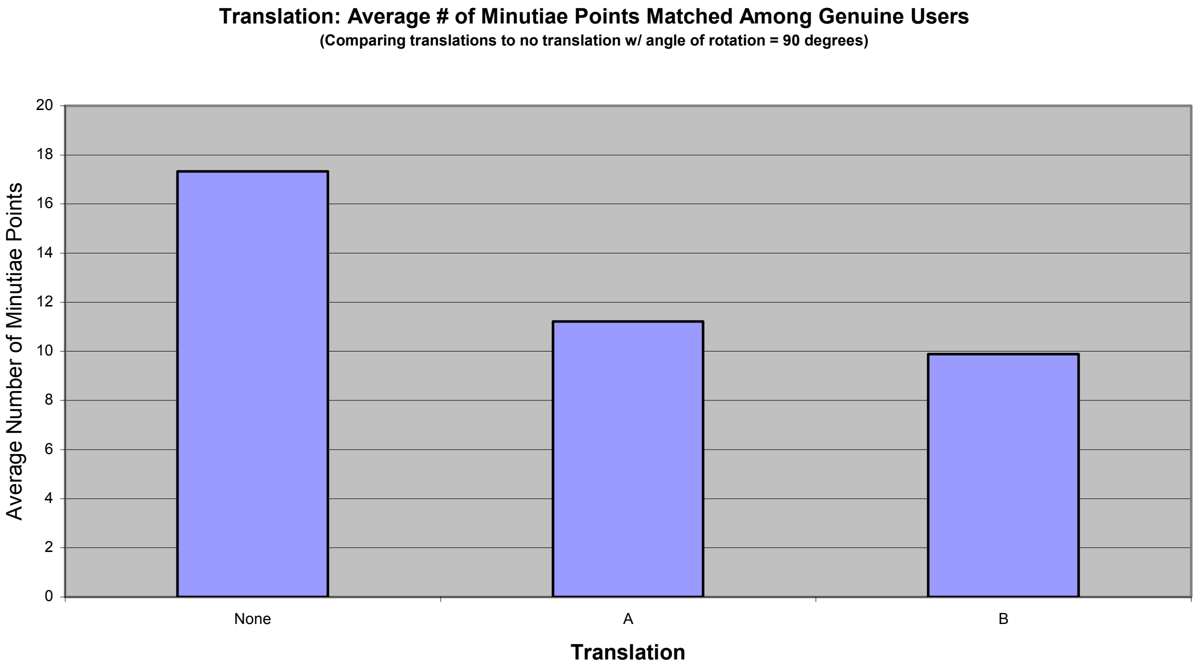


Figure 37. Average # of Minutiae Points Matched for Translation

Figure 37 shows the average number of minutiae points for all ten users at translation schemes when compared to the genuine user's fingerprint at 90 degrees angle of rotation and no translation. When the translation masks were used as noted in Appendix A, the sensor was unable to detect a finger resulting in a FTA of 100. It should be noted that when translation is introduced, the average number of minutiae points matched is reduced.

Figure 38 shows the average match score for all ten users at device placement angles of pan and tilt +/- 20 degrees when compared to the genuine user's fingerprint at 90 degrees angle of rotation and pan and tilt degrees of zero. When the fingerprint sensor was placed at pan and tilt angles of -20 degrees, this resulted in better higher average match scores.

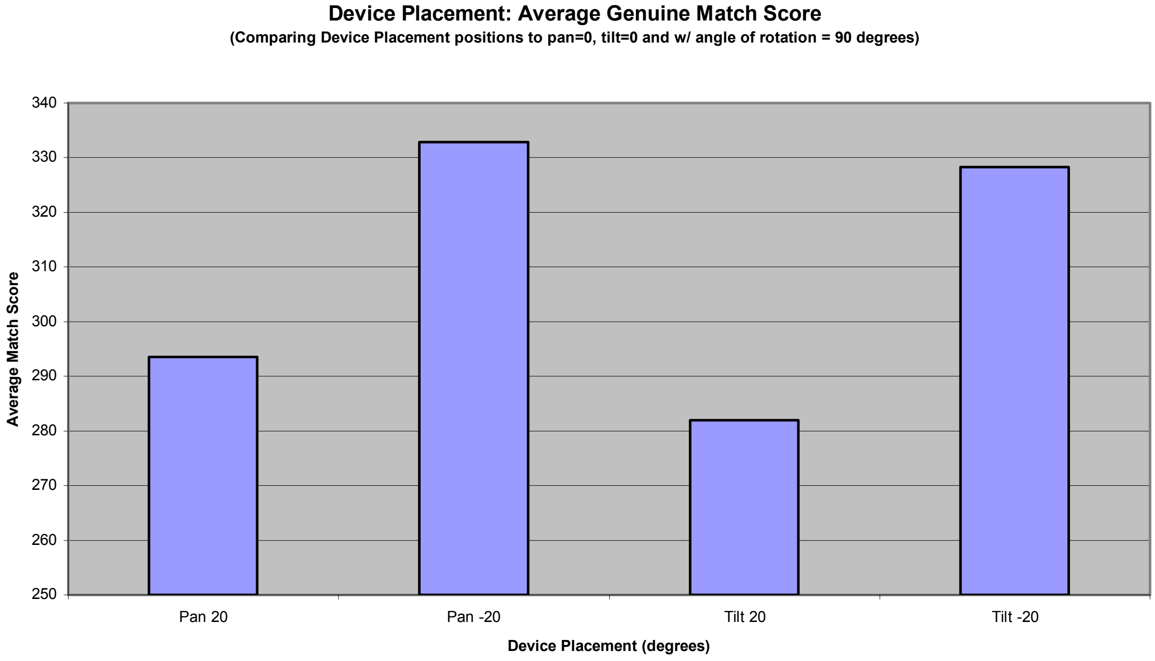


Figure 38. Average Genuine Match Score for Device Placement

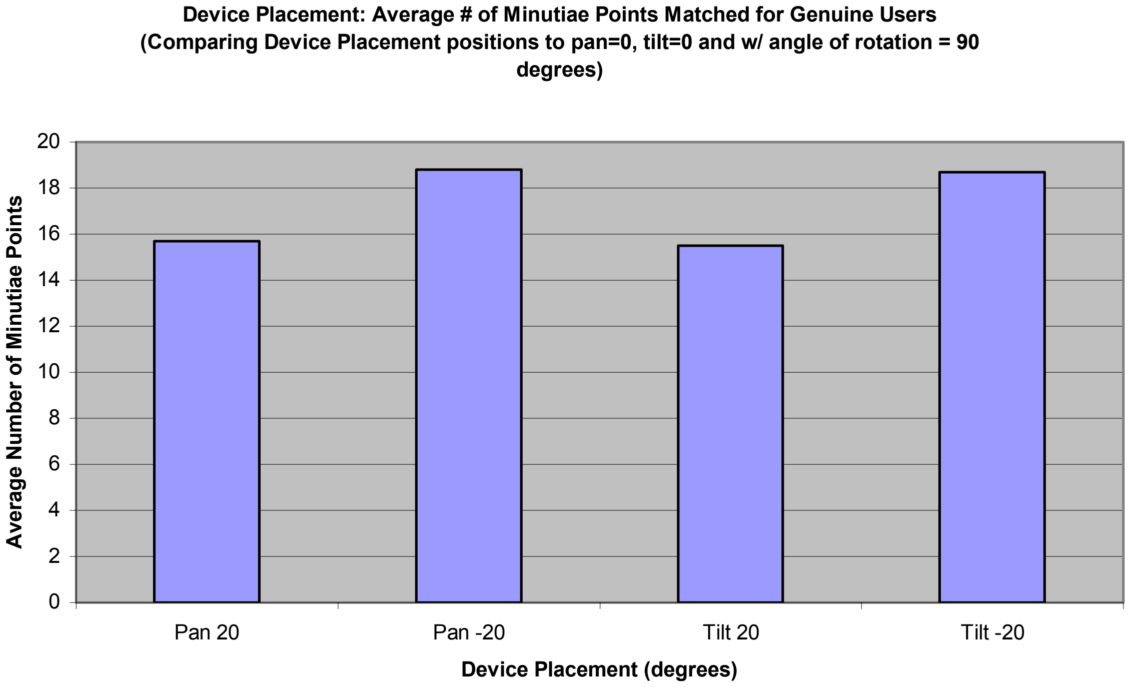


Figure 39. Average # of Minutiae Points Matched for Device Placement

Figure 39 shows the average number of minutiae points for all ten users at device placement angles of pan and tilt +/- 20 degrees when compared to the genuine user's fingerprint at 90 degrees angle of rotation and pan and tilt degrees of zero. When the fingerprint sensor was placed at pan and tilt angles of -20 degrees, this produced a higher average number of minutiae points matched.

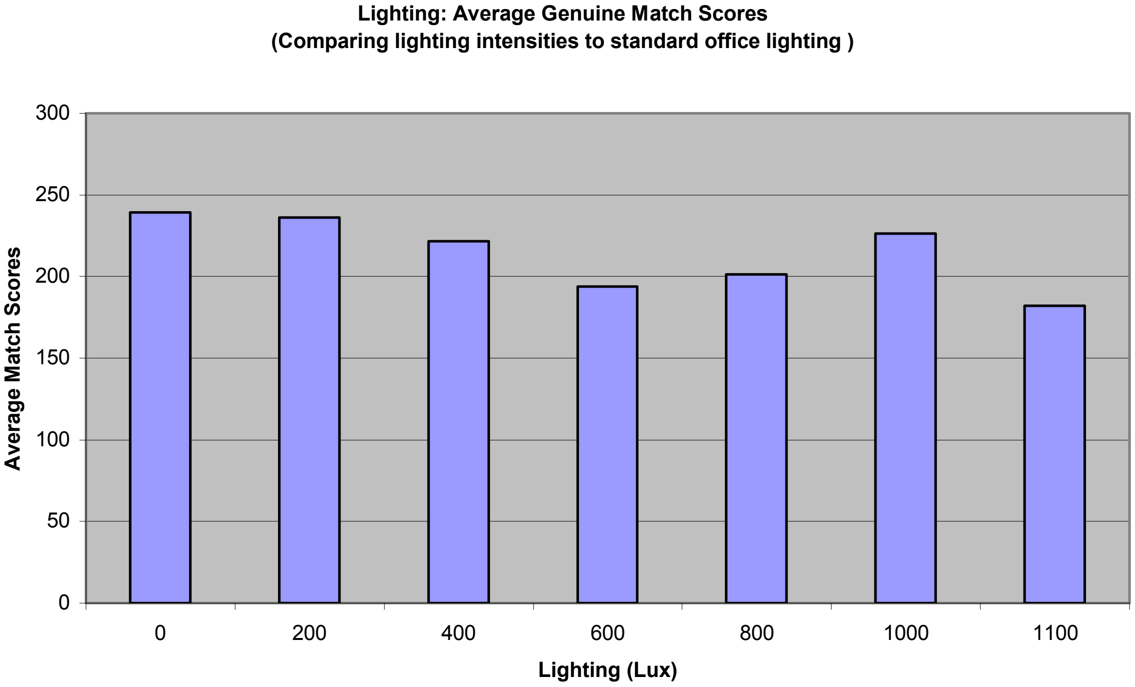


Figure 40. Average Genuine Match Score for Lighting

Figure 40 shows the average match score for all ten users at various lighting conditions compared to the genuine user's fingerprint at 90 degrees angle of rotation and at normal office lighting. When the fingerprint sensor was introduced to various lighting conditions variability was noticed in the average match scores.

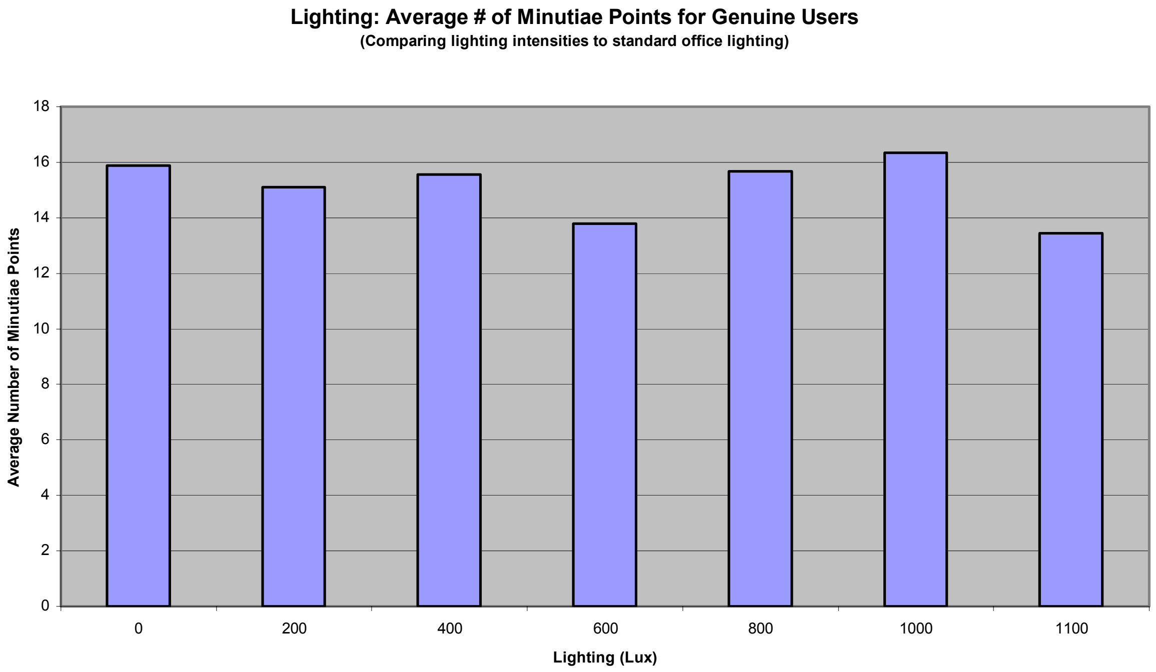


Figure 41. Average # of Minutiae Points Matched for Lighting

Figure 41 shows the average number of minutiae points for all ten users at various lighting conditions compared to the genuine user's fingerprint at a 90 degree angle of rotation and at normal office lighting. When the fingerprint sensor was introduced to various lighting conditions variability was noticed in the average number of minutiae points matched.

To show the percent change in average match score when compared to genuine images with angle of rotation of 90 degrees, no translation and no device placement for all four protocols see Figures 42 to 45. Figure 42 shows the percent change in average match score for the various angles of rotation when compared to the genuine user's match score at a 90 degree angle of rotation. Angles of rotation 85, 90, and 95 show a slight percentage change in average match score, while the other angles of rotation produce more than a 10% decrease in average match scores.

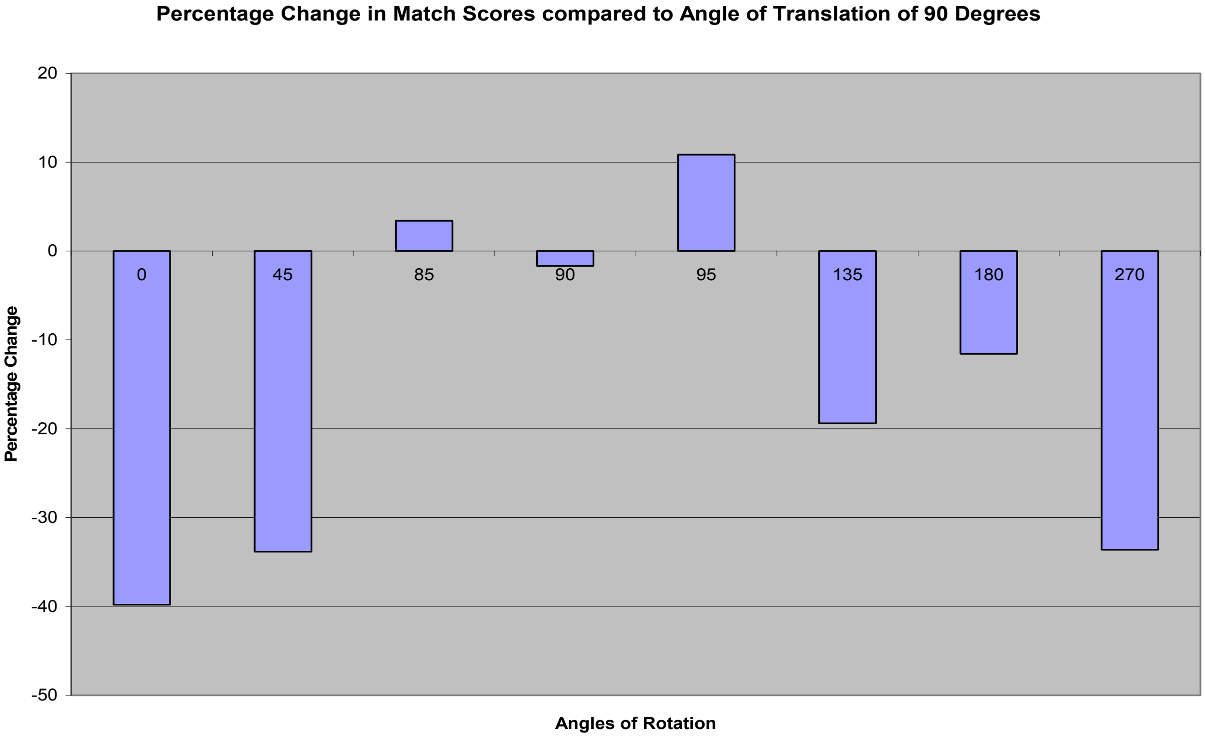


Figure 42. Percent Change in Average Genuine Match Score for Angle of Rotation

Figure 43 shows the percent change in average match score for the various translation masks when compared to the genuine user's match score at a 90 degree angle of rotation and no translation. Translation with A and B masks resulted in more than 20 percent decrease in average match score.

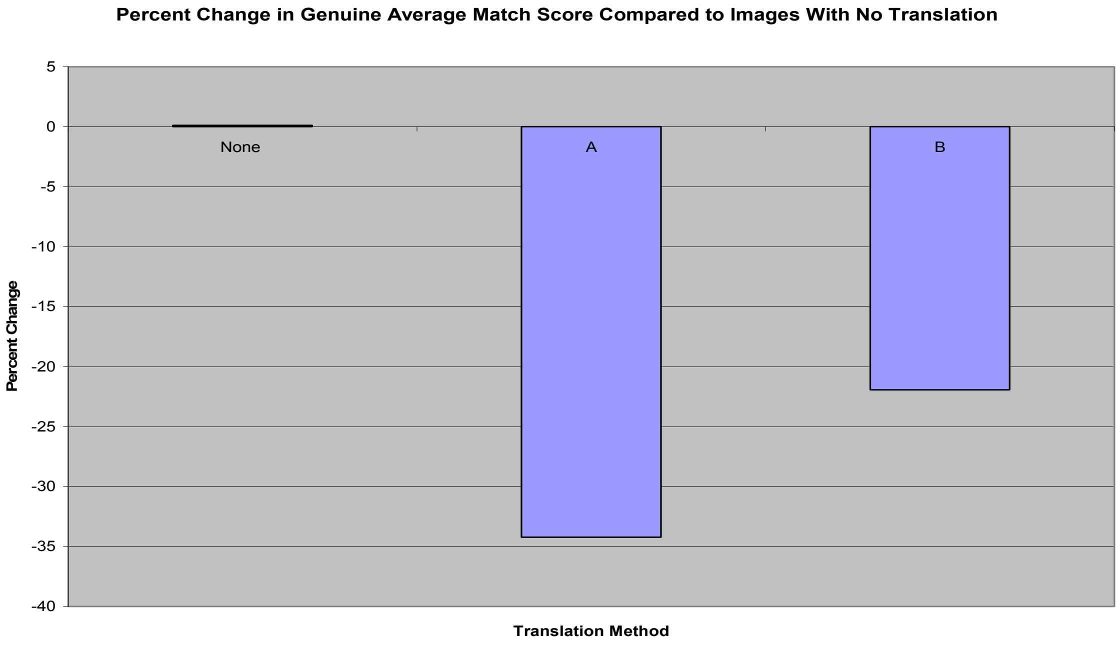


Figure 43. Percent Change in Genuine Match Score Compared with No Translation.

Figure 44 shows the percent change in average match score for the various angles of device placement when compared to the genuine user's match score at a 90 degree angle of rotation and pan and tilt angles of 0 degrees. Pan and tilt angles of -20 degrees produced more than a 14 percent increase of average match scores across all users. While pan and tilt angles of +20 degrees produced moderate change in match score.

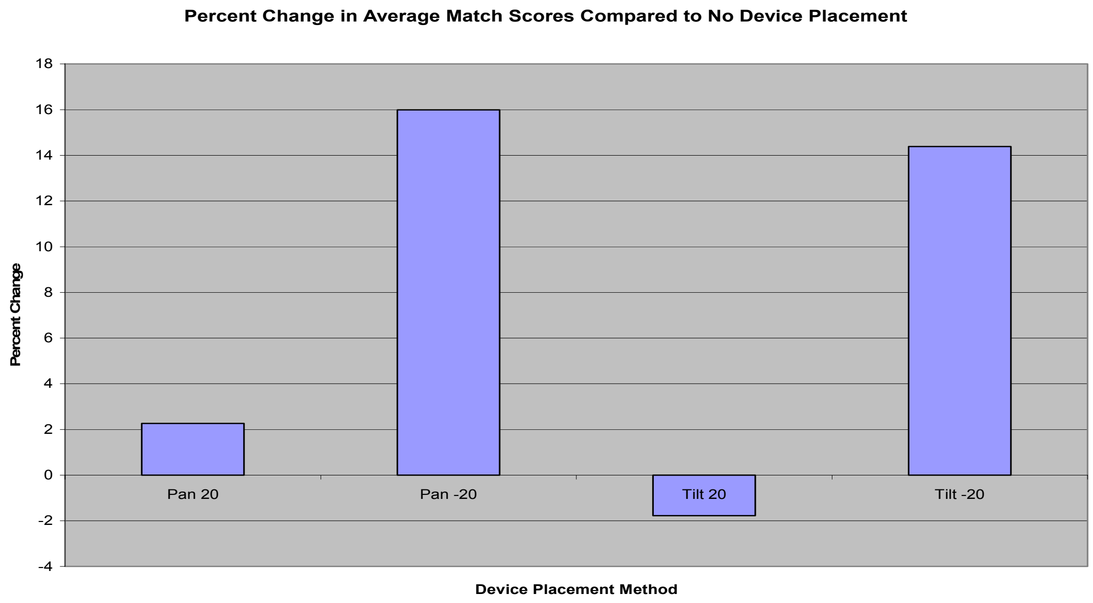


Figure 44. Percent Change in Average Match Score with Changes in Device Placement

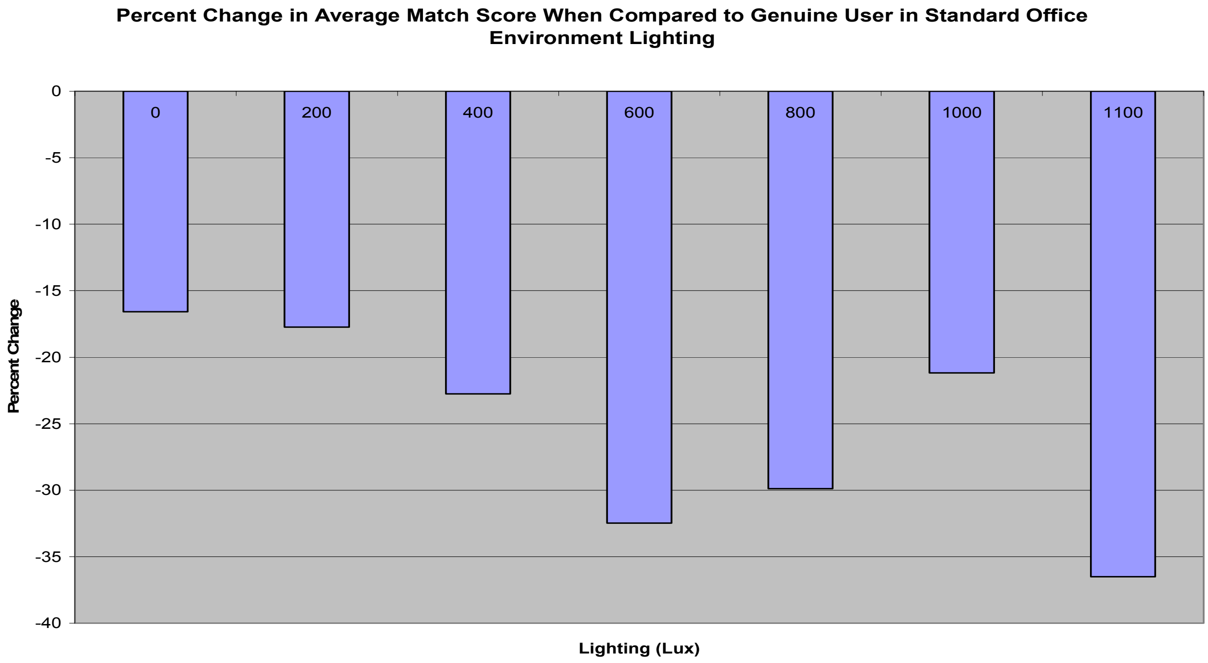


Figure 45. Percent Change in Average Match Score with Changes in Light Intensity

Figure 45 shows the percent change in average match score for the various lighting conditions when compared to the genuine user's match score at a 90 degree angle of rotation at normal office lighting. These results show that when a light source is introduced in this case results in reduced average match scores. When lux was set at 1100, more than a 35% decrease in match score was measured.

Next, to get a more detailed view of the match scores, boxplots were generated for each protocol. Boxplots produce a box and whisker plot. The box has lines at the upper and lower quartiles as well as at the median. The whiskers are lines extending from the box to show the rest of the data. See Figures 46 to 49 for these boxplots. Figure 46 shows the boxplot of the average genuine match scores at various angles of rotation for all ten users when compared to a fingerprint placed at a 90 degree angle of rotation. As mentioned earlier, angles of rotation 85, 90, and 95 produced much high match scores than angles of rotation farther away.

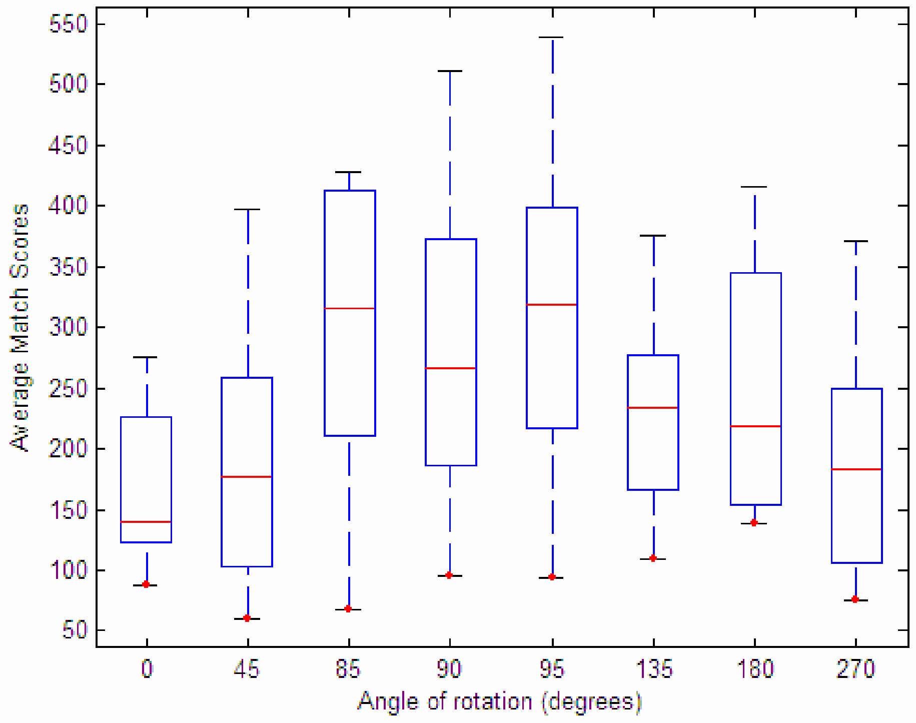


Figure 46. Genuine User Box Plot for Angle of Rotation

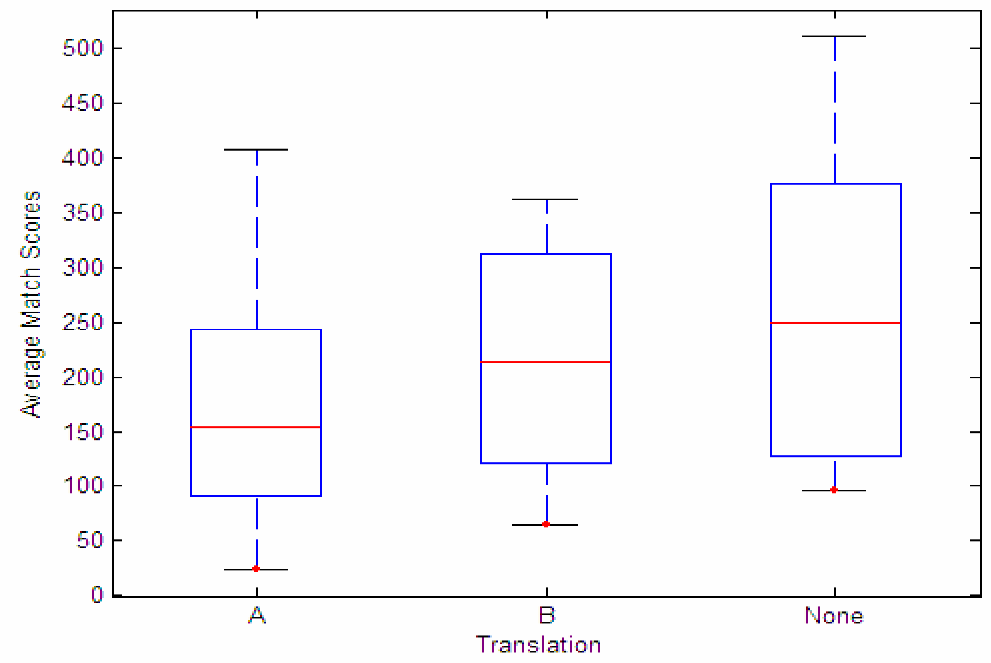


Figure 47. Genuine User Box Plot for Translation

Figure 47 shows the boxplot of the average genuine match scores at various translations for all ten users when compared to a fingerprint placed at a 90 degree angle of rotation and no translation. As mentioned earlier, translation at A and B produced much lower match scores than no translation.

Figure 48 shows the boxplot of the average genuine match scores at various angles of device placement for all ten users when compared to a fingerprint placed at a 90 degree angle of rotation and pan and tilt angles of zero degrees. There is some noticeable variability in average match score when pan and tilt angles were altered.

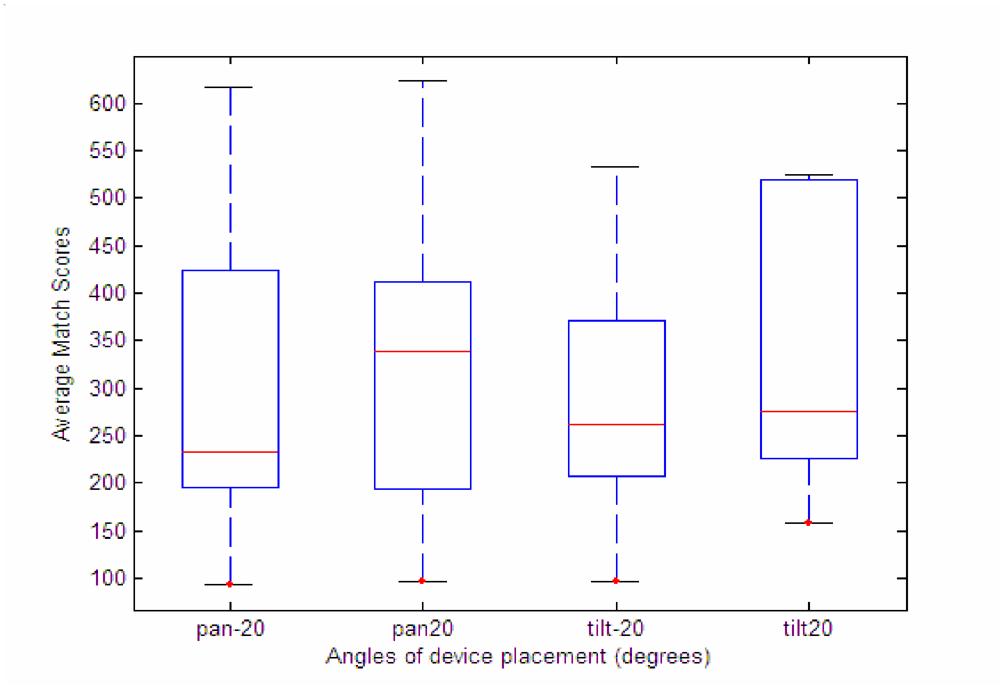


Figure 48. Genuine User Box Plot for Device Placement

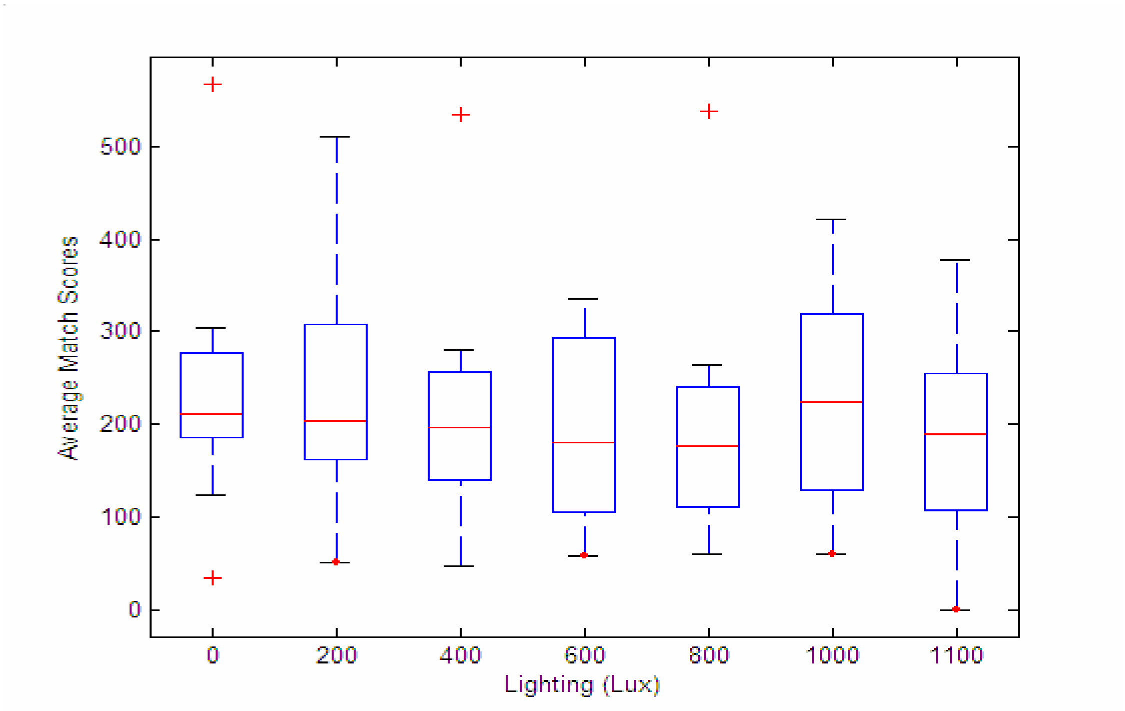


Figure 49. Genuine User Box Plot for Lighting

Figure 49 shows the boxplot of the average genuine match scores at various lighting conditions for all ten users when compared to a fingerprint placed at a 90 degree angle of rotation and at normal office lighting.

4.2 Analysis

As a result of this testing, it is determined that not all variables were accounted for in testing. Fingerprint placement is still a factor despite many efforts to control this. In some cases, with fingers covering most of the sensor surface, lighting had no affect, since very little could reach the sensor. On the contrary when fingers didn't cover most of the sensor surface, the results were either an FTA or poorer quality images. Also, many fingerprint images were of poor quality due to dry fingers, too moist fingers, pressing too hard or too soft for example. These variations, despite many efforts to control other variables, made it difficult to ensure quality image capture.

In some instances, fingerprints were noticed to develop some form of a shadowing effect when placed at certain angles. This is due to the relation of overhead light to the fingerprint sensor. See Figure 50 and Figure 51 for test images containing this shadowing effect.

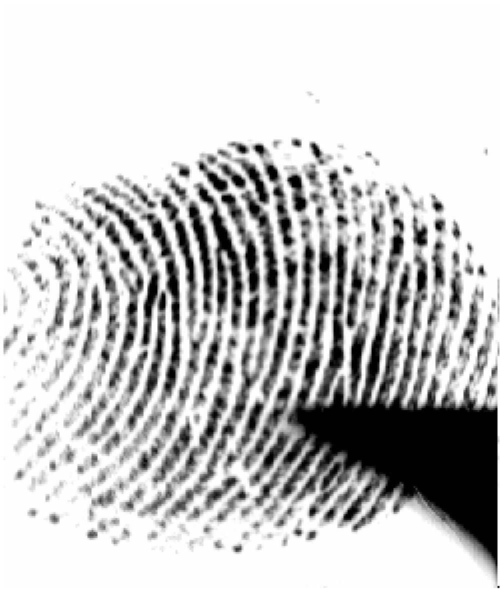


Figure 50. Shadowing Effect on Fingerprint Sample

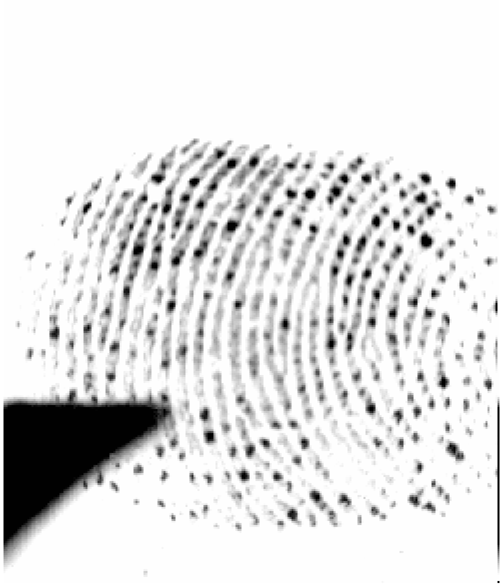


Figure 51. Shadowing Effect on Fingerprint Sample

Chapter 5. Summary and Future Work

Despite being able to account for all variables these protocols proved to show the effects of the four variables: Angle of Rotation, Translation, Device Placement, and Lighting for optical fingerprint sensors. In conclusion, based on the results it appears that many issues can be addressed in future work. Most importantly, testing the above protocols with more test subjects is necessary to get a more accurate representation of imposter and genuine distributions, and will hopefully lead to attempts at modeling these variables. Some other possibilities have been listed below.

1. Image Quality Score vs. Environment: Work can be done to determine which affects performance more, the quality of images or the effects of the environment on the sensor.
2. Image Quality Score: One such work is using an image quality score/parameter ensure images are "Good enough for testing" are used. Such a process can be implemented by establishing a threshold and using only fingerprint images that have a minimum number of minutiae points identified by the system. If this threshold is not met, then the image should not be used in testing. Or a more complex method that takes into account illumination of the image and number of minutiae points and outputs an image quality score. An example of research involving image quality score can be found in [25].
3. Repeatability: Determination of how repeatable these protocols are will go a long way in trying to isolate which variables are most important in the development of repeatable protocols.
4. Fingerprint Placement: Another area that needs improvement is a better means to control how a user places their fingerprint on the sensor. However, by using an image quality method users can place their fingerprints several times until one is imaged above the threshold for testing.

5. Solid-State Sensor: These protocols should be performed on a solid state fingerprint sensor to determine if or how it is affected by these variables.

6. Deformation Modeling: Another area that can be explored is modeling deformation of fingerprints to see how that improves system performance.

7. Environmental controlled Chambers: Use of environmentally controlled chambers and more precise/effective lighting controls for the lighting protocol.

8. Angle of Rotation: Another, but more challenging test method would be to rotate the sensor instead of the user to test the angle of rotation method and determine if there is a change in the results mentioned in this work.

References

1. (2001). *Interpreting Fingerprint Authentication Performance Technical White Paper*. Fidelica Microsystems Inc.
2. Ashbourn, J. (2000). Biometrics: Advanced Identity Verification. Springer, London.
3. Bolle, R. M., Pankanti, S., & Ratha, N. K. (2000). *Evalution Techniques for Biometrics-Based Authentication systems (FRR)*. Yorktown Heights, NY: IBM.
4. Crihalmeanu, S., Ross, A., Govindarajan, R., Hornak, L., & Schuckers, S. A. C. (2004). *A Centralized Web-Enabled Multimodal Biometric Database*. Retrieved April 16, 2005 from http://www.wvu.edu/~bknc/2004%20Abstracts/A%20Centralized%20Web-Enabled%20Multimodal%20Biometric%20Database.pdf
5. Doddington, G. R., Pryzbocki, M. A., Martin, A. F., & Reynolds, D. A. (2000). *The NIST Speaker Recognition Evaluation: Overview Methodology, Systems, Results, Perspective* (31). Speech Communications.
6. Doddington, G., Liggett, W., Martin, A., Przybocki, M., & Reynolds, D. (1998). Sheep, Goats, Lambs, and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation. *International Conference on Spoken Language Processing*.
7. Fingerprint Verification Competition. Retrieved on 04/12/2005 from: http://bias.csr.unibo.it/fvc2004/default.asp
8. The Fingerprint Vendor Technology Evaluation (FpVTE). Retrieved on 04/12/2005 from: http://fpvte.nist.gov
9. Haas, N., Ratha, N. K., & Bolle, R. M. (2002). *Pre-enhancing Non-uniformly Illuminated Fingerprint Images*. Retrieved April 2, 2005 from http://www.research.ibm.com/ecvg/pubs/norm-enhance.pdf

10. Jain, A. K., & Ross, A. (September 2002). Learning User-specific Parameters in a Multibiometric System, *Proc. of IEEE International Conference on Image Processing (ICIP)*, (Rochester, NY), pp. 57-60.

11. Jain, A. K., Ross, A., & Prabhakar, S. (Eds.) (2004). An Introducation to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14 (4).*

12. Kim, H. (2003). Evaluation of Fingerprint Readers: Environmental factors, Human Factors, & Liveness Detecting Capability. Retrieved April 2, 2005 from: http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint20-%20Presentation%20of%20HaleKim%20-%20v2.1.ppt%20[.pdf

13. Lawrence, O. (1999). Fingerprint Verification. In Jain, A., Bolle, R., & Pankanti, S. (Eds.), *Biometrics: Personal Identification in Networked Society* (p. 43). Boston: Kluwer.

14. Maltoni, D., Dario, M., Jain, A., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* London: Springer.

15. Mansfield, A. J., & Wayman, J. L. (August 2002). *Best Practices in Testing and Reporting Performances of Biometric Devices, Version 2.01* (NPL Report CMSC 14/02). UK: National Physical Laboratory.

16. Ratha, N. K., Connell, J. H., & Bolle, R. M. (Oct. 2001). *Secure Fingerprint-Based User Authentication for Lotus Notes* (). : ACM Multimedia and Security Workshop.

17. Rosiek, T., & Gupta, G. (2005). Generic Biometric System. *West Virginia University Internal Technical Report*.

18. Ross, A., & Jain, A. (2004). *Biometric Sensor Interoperability: A Case Study In Fingerprints*. Paper presented at the meeting of the International ECCV Workshop on Biometric Authentication (BioAW). Prague, Czech Republic.

19. Ross, A., Jain, A. & Qian, J. (June 2001). Information Fusion in Biometrics, *Proc. of 3rd International Conference on Audio- and Video-Based Person Authentication (AVBPA)*, (Halmstad, Sweden), LNCS vol. 2091, pp. 354-359, Springer Publishers.

20. Ross, A., Dass, S., & Jain, A. (2004). *Estimating Fingerprint Deformation*. Paper presented at the meeting of the International Conference on Biometric Authentication. Hong Kong.

21. Ross, A., Dass, S., & Jain, A. (2005). A Deformable Model for Fingerprint Matching. *Pattern Recognition, 38,* 95-103.

22. SandstrÄom, M. *Liveness Detection in Fingerprint Recognition Systems.* Retrieved on 04/14/2005 from http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf

23. Schuckers, M. E., Hawley, A., & Livingstone, K. (2004). *A Comparison of Statistical Methods for Evaluating Matching Performance of a Biometric Identification Device- a Preliminary Report* .

24. Speaks, D., Anderson, L., & Hutson, J. (2004). *Biometric Performanc Operational Testing and Reporting* (M1/04-0216).

25. Tabassi, E., Wilson, C., & Watson, C. (2004). *Fingerprint Image Quality* (NIST 7151). Retrieved April 15, 2005 from http://fingerprint.nist.gov/NFIS/ir_7151.pdf

26. Valencia, V. (2004). Biometric Testing: It's Not as Easy as You Think. http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/bc076_ValenciaBrief.pdf

27. Whois.com. (2001, April 18). Retrieved April 16, 2005, from http://whatis.techtarget.com/definition/0,,sid9_gci542011,00.html

28. Wilson, C., Hicklin, K., Bone, M., Korves, H., Grother, P., Ulery, B., et al. (2004). *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report* (NISTIR 7123).

29. Woodward, J. D., Webb, K. W., Newton, E. M., Bradley, M., & Rubenseon, D. (2001). *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns.* : RAND Corporation.

30. Woodward, J. D., Orlans, N. M., Higgins, P. T., (2003). *Biometrics: Identity Assurance in the Information Age.* (p. 187). Osborne: Mcgraw Hill.

Appendix A. Testing Protocols for Optical Fingerprint Sensors

1. Introduction

This document defines and lists several testing protocols for optical fingerprint systems. To date, this document can not encompass all possible testing protocols and is meant to lay the ground work for the testing and the evaluation processes.

2. Setup

It is important for all testing to be repeatable and that all variables involved in each test are documented. We assume that all hardware and software for the fingerprint system has been properly installed based on the instructions supplied by the vendor.

2.1. Environmental Factors

The environment can alter the quality of the image acquired by the fingerprint system, thus affecting its matching performance. The environment is very difficult to control and presents a great challenge in producing repeatable results. As a baseline, it is always important to measure and document, at a minimum, temperature, humidity, and light intensity before each experiment. If the environmental factors vary greatly, then the test results may become less accurate. For normal operating conditions testing, these measured values should always be compliant with vendor recommended values.

To help improve the repeatability of testing, we suggest the use of environmentally controlled chambers when relevant. These chambers can accurately set and maintain various environmental variables and improve the accuracy of the testing.

If the vendor does not state “normal operating environment”, then we suggest using:

- Standard room temperature (67-72°F)
- Standard humidity (35-40%)
- Standard level of lighting

2.2. Device Placement

Device Placement is the position a biometric device is placed. The key factor to consider is whether the device during the enrollment mode is at the same location relative to the user as the device during the image acquisition process for other operational modes. One component of device placement is location, which can be broken down into height, altitude, angle, and surface.

Location can be tested by comparing the performance of the device when location is varied to when it is held constant. Variations in location can result from changes in height, altitude, angle, and surface of the device placement. Location is an important factor because if it varies throughout the system's deployment then results can greatly be altered because of its effects on biometric presentation which greatly affects image acquisition quality.

Height, altitude and surface all can affect the performance of the system, but can be easily controlled throughout most test protocols. Angle is a little more difficult to control and is defined as two angles to consider: pan, σ and tilt, Φ. See Figure 1 for a graphical representation.

We shall define normal device placement as (0, 0), meaning $\sigma = 0$ degrees and $\Phi = 0$ degrees. For example see Figure 1, a device placement of (80, 65) means $\sigma = 80$ and $\Phi = 65$.

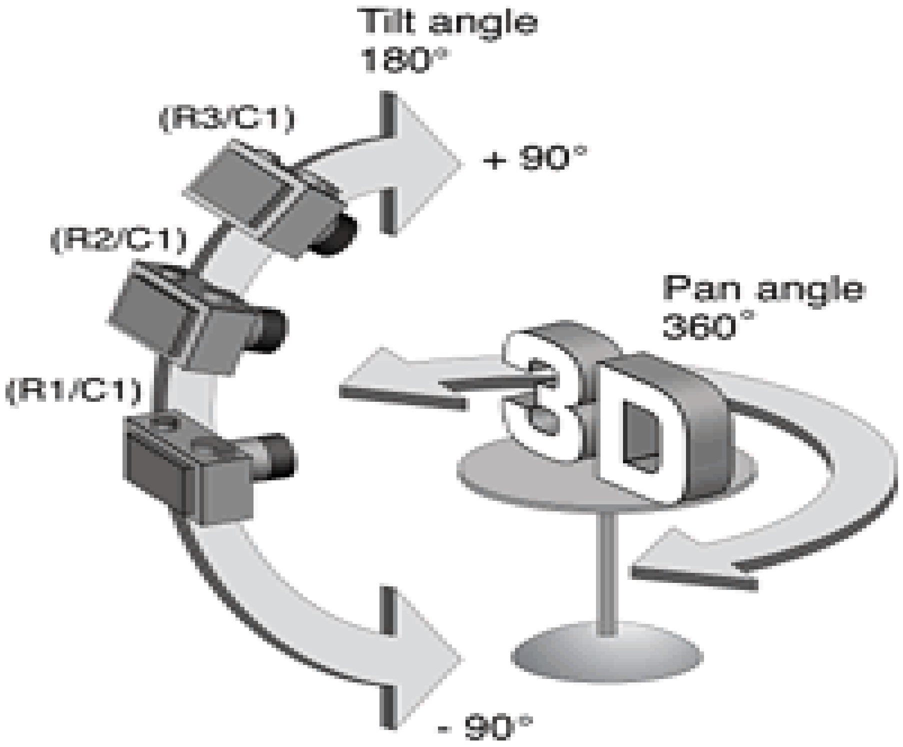


Figure 1 Device Placement Angles

From http://developer.apple.com/documentation/QuickTime/InsideQT_QTVR/art/iqtvr_pantilt.gif

2.3. Biometric Presentation

Biometric presentation considers the effects of the way a user presents their biometric trait(s) to the system. The presentation of a user's biometric trait(s) greatly affects the system's ability to correctly match/identify genuine users. This can be subdivided into:

- Pose and/or Orientation of the biometric: This can be further divided into two a) the angle of rotation and b) distance from the device (translation for fingerprint). One approach to evaluating a system's susceptibility to variations in pose and/or orientation would be to compare the system's results for various poses and orientations. Image quality will be affected which will eventually affect the biometric system's performance in matching templates.
- Presentation: The quality and clearness of a biometric trait as it is presented to the biometric system. This will greatly affect the quality of templates the biometric system creates and thus will affect its matching performance.
- Covert/Overt: Covert biometric systems are used without the subject's knowledge of their existence, while the subject knows the existence of overt biometric systems.
- Attended/Non-Attended: Having the biometric attended can help system performance by offering guidance to novice/beginner users while also helping to identify/deter impostors.
- Cooperative/Non-Cooperative User: Whether the subject is physically willing to allow their biometric(s) to be scanned can greatly affect the performance of the biometric system.

We will further define the angle of rotation and distance from device (for fingerprint systems this is translation). To improve the repeatability of angle of rotation, we suggest applying a mask (calibrated label) to the finger sensor. See Figure 2. For the case with zero (no) translation (central fingerprint placement), see Figure 3. For further repeatability, the user should physically mark the central axis of their finger on their fingernail to help align the finger with the mask, as shown in Figure 4. Figure 4 also shows the application of the mask on a fingerprint sensor and the placement of a fingerprint with an angle of rotation of 90 degrees with no translation.

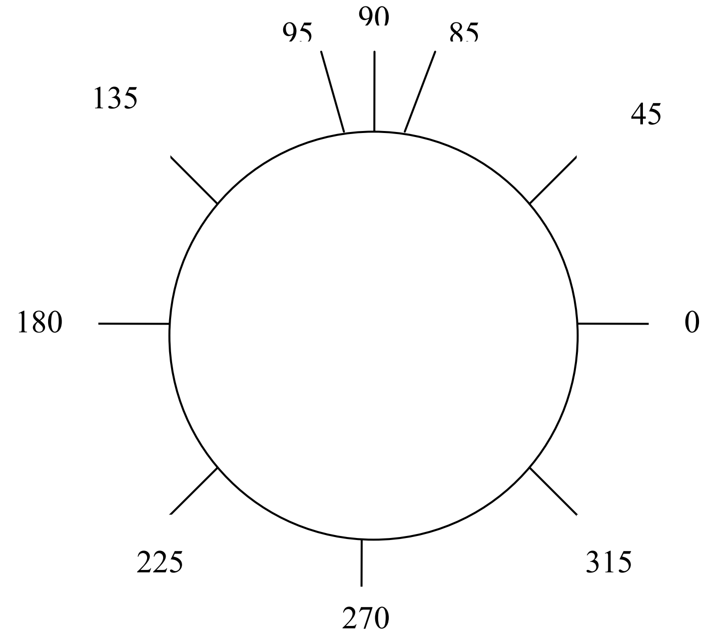


FIGURE 2- Angle of Rotation Calibrated Mask

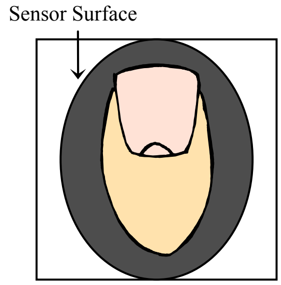


FIGURE 3- Center Fingerprint Placement (No Translation)

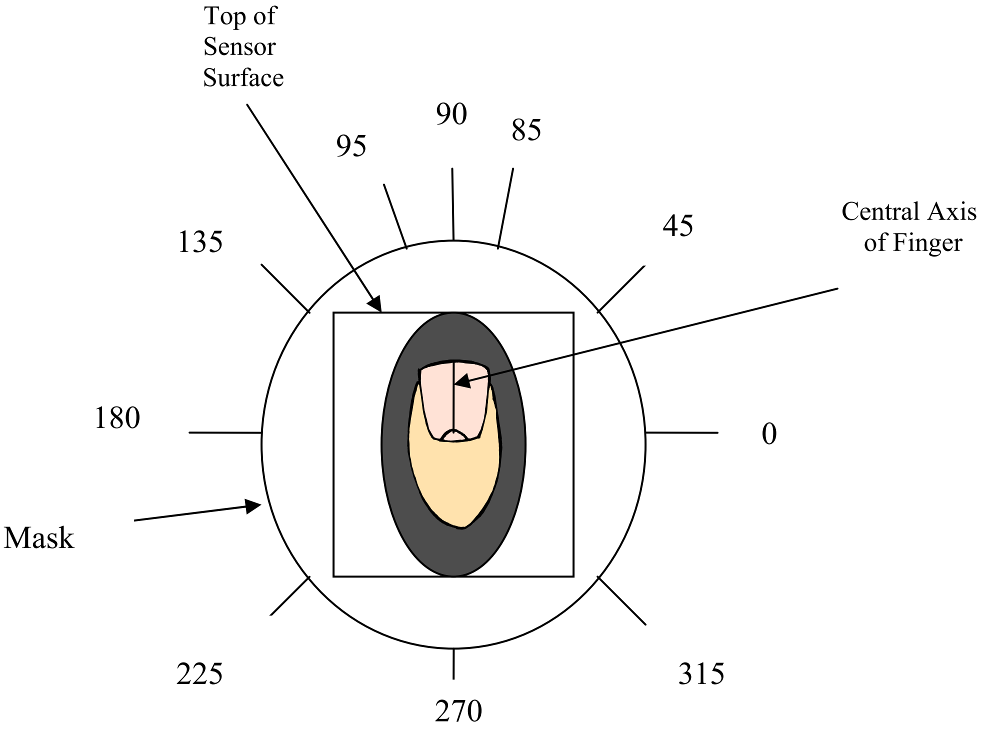


FIGURE 4- Fingerprint Sensor with mask and No Fingerprint Translation

2.4. Sensor Cleaning/Replacement

Sensor cleaning/replacement is how often the fingerprint sensor should be cleaned. Cleansing of the device will improve the system performance as it will lead to quality image capture. In some cases, the vendor will specify the maximum number of touches a fingerprint sensor can withstand before it needs to be replaced. One should follow the cleaning instructions for the sensor as stated by the vendor. If no instructions are provided, the vendor should be contacted to ensure the proper cleaning solution is used.

2.5. Threshold Settings

In biometric systems, the threshold setting greatly affects performance rates. It is important throughout all testing to maintain a constant threshold setting unless otherwise specified. The threshold value should be set to that specified by the vendor. If no threshold value is specified, we suggest using the default (out of box) threshold settings for most tests. It is important that the threshold value used during the testing is documented.

2.6. Subject

The subject, whose fingerprint is being imaged, can greatly affect the accuracy of testing results. That is why it is very important that each human factor be held as constant as possible so that it does not affect the test protocols for variables other than subject.

2.8. Software

Software can greatly affect the performance of a fingerprint system. To obtain the most accurate test results, it is important that once testing has begun, no software is updated on the system, unless otherwise specified.

2.9 Session

We define a session as the time frame between when a user enters the temperature controlled chamber and when the user exits the chamber. This will help reduce any effects of template aging, any changes in user habituation, user health, biometric health, and other human factors during the testing process that could affect the accuracy of the results.

3 Testing Protocols

Assumptions: In testing these protocols it is assumed that the system is overt, only cooperative users are being tested, and the system is attended during all testing. Also, we assume that the test population is well representative of the user population. Some factors are biometric health, user health, demographics, gender, age, etc. We also assume that the same finger is used during enrollment and the testing process unless otherwise stated. It is assumed that the user testing and the user's enrollment occur in the same session, as defined in section 2.9.

3.1. Lighting

This test is designed to evaluate the effects of lighting on an optical fingerprint sensor during operation. For the optical fingerprint system, this test can be performed during the acquisition operational mode, and should be the same for the remaining operational modes. Please refer to **Generic Biometric Testing Protocols** for more information on the operational modes. In this evaluation, we assume that the enrollment and tests are performed in the same session. In this case, we define a session as the time frame between when a user enters the temperature controlled chamber and when the user exits the chamber. For best results, once the chamber has returned to the normal operating environment as stated by the vendor, the test subject should re-enroll into the system database for each test. This will help reduce any effects of template aging, any changes in user habituation, user health, biometric health, and other human factors during the testing process that could affect the accuracy of the results.

In this evaluation we assume that the same finger is used during the enrollment and testing process. It is also assumed that during the enrollment process, the fingerprint was imaged and the template was generated under normal conditions as stated by the vendor. The next step is to compare the newly acquired fingerprint image to the fingerprint image obtained during enrollment. This difference (if any) could be attributed to the adverse effect of lighting on the fingerprint system.

INPUTS:

Humidity, temperature, lighting, threshold values, sensor cleaning frequency, date, time

METHOD:

Setup:

With the temperature controlled chamber used in section 3.1 and an appropriate variable light source, the fingerprint sensor should be placed in the chamber such that there are no obstructions between the variable light source and the fingerprint sensor. Threshold values should be set to the appropriate values and held constant throughout the testing process. See section 2.5 for more information on threshold values. The fingerprint sensor should be stationary and placed at normal biometric device placement, (0, 0). See section 2.2 for further information about device placement. Throughout this entire test protocol, the fingerprint sensor should remain at normal biometric device placement, (0, 0).

Once the fingerprint system is properly setup and the user is in the test chamber, the chamber can now be sealed.

Environment:

Inside the chamber, the lighting condition should be measured, temperature should be measured, humidity should be measured, the date and time of the testing should be documented, threshold value should be recorded, and the sensor cleaning frequency should also be recorded. These measured input values should simulate “normal operating conditions” as stated by the vendor and should be held as constant as possible throughout the testing, with the exception of lighting. Please refer to section 2.1 for more information regarding environmental factors. The use of the temperature controlled chamber will help to eliminate fluctuations in the environmental variables and will aid in making this test repeatable. Before enrolling the user, the sensor surface should be properly cleaned. Please refer to section 2.4 for more information.

Testing:

Now that the sensor surface is clean, the user should enroll into the fingerprint system per the instructions provided by the vendor. During enrollment, the user should properly present their fingerprint to the fingerprint sensor for imaging. In this test, the biometric presentation variable, angle of rotation should be at 90 degrees and translation should be 0 (none). For more information, please see section 2.3.

Once enrolled, sensor cleaning should be consistent throughout the entire testing process. For best results, we recommend cleaning the fingerprint sensor surface after each touch. Once cleaned, the variable light source should be set to the light intensity that is in question. Once the light intensity has been measured and recorded, the other environmental variables measured above should also be measured again and documented. These values should be consistent with the previously measured values. Once complete, the user can now present their fingerprint, used during enrollment, to the sensor.

Once the fingerprint has been properly imaged, the variable light source can be returned to its initial setting and further testing can be pursued.

Results:

The template generated during enrollment should be compared to the templates acquired during the testing process. A percent match should be assigned to this comparison and recorded. The (FTE) Failure To Enroll rate and (FTA) Failure To Acquire rate should also be documented. These performance measurements will help to determine the effects of lighting on the fingerprint device.

OUTPUTS:

FTA

FTE

Percent match

Time between enrollment and testing

Sensor surface cleansing frequency

3.2. Biometric Presentation

This test is designed to evaluate the effects of biometric presentation on an optical fingerprint sensor during operation. For an optical fingerprint system, this test can be performed during the acquisition operational mode, and should be the same for the remaining operational modes. Please refer to **Generic Biometric Testing Protocols** for more information on the operational modes. Biometric presentation is comprised of angle of rotation and translation (for fingerprint sensors). In this evaluation, each of these components will be tested separately.

3.2.1. Angle of Rotation:

In this evaluation, we assume that the enrollment and tests are performed in the same session. In this case, we define a session as the time frame between when a user enters the temperature controlled chamber and when the user exits the chamber. For best results, once the chamber has returned to the normal operating environment as stated by the vendor, the test subject should re-enroll into the system database for each test. This will help reduce any effects of template aging, any changes in user habituation, and other human factors during the testing process that could affect the accuracy of the results.

In this evaluation we assume that the same finger is used during the enrollment and testing process. It is also assumed that during the enrollment process, the fingerprint was imaged and the template was generated under normal conditions as stated by the vendor. The next step is to compare the newly acquired fingerprint image to the fingerprint image obtained during enrollment. This difference (if any) could be attributed to the adverse effect biometric presentation, in particular angle of rotation, has on the fingerprint system.

INPUTS:

Humidity, temperature, lighting, threshold values, sensor cleaning frequency, date, time

METHOD:

Setup:

With the temperature controlled chamber used in section 3.1, the fingerprint sensor should be placed inside the chamber and the test subject must be able to properly present their fingerprint(s) to the device in the chamber while maintaining isolation from the outside environment. Threshold values should be set to the appropriate values and held constant throughout the testing process. See section 2.5 for more information on threshold values. The fingerprint sensor should be placed at normal biometric device placement, (0, 0). See section 2.2 for further information about device placement. Throughout this entire test protocol, the fingerprint sensor should remain at normal biometric device placement, (0, 0).

Once the fingerprint system is properly setup and the user is in the test chamber, the chamber can now be sealed.

Environment:

Inside the chamber, the lighting condition should be measured, temperature should be measured, humidity should be measured, the date and time of the testing should be documented, threshold value should be recorded, and the sensor cleaning frequency should also be recorded. These measured input values should simulate "normal operating conditions" as stated by the vendor and should be held as constant as possible throughout the testing. Please refer to section 2.1 for more information regarding environmental factors. Before enrolling the user, the sensor surface should be properly cleaned. Please refer to section 2.4 for more information on sensor cleaning.

Testing:

Now that the sensor surface is clean, the user should enroll into the fingerprint system per the instructions provided by the vendor. During enrollment, the user should properly present their fingerprint to the fingerprint sensor for imaging. For enrollment, the biometric presentation variable, angle of rotation should be at 90 degrees and translation should be 0 (none). For more information, please see section 2.3.

Once enrolled, sensor cleaning should be consistent throughout the entire testing process. For best results, we recommend cleaning the fingerprint sensor surface after each touch. Before each test, the environmental variables previously measured above should also be measured again and documented. These values should be consistent with the previously measured values and comply with the vendor's recommended "normal operating environment." Once complete, the user can now present their fingerprint, used during enrollment, to the sensor at an angle of rotation at 90 degrees. ***NOTE:*** *The biometric presentation variable, translation should be kept constant.*

We suggest performing tests at the following angles of rotation: 0, 45, 85, 90, 95, 135, 180, and 270. 270 degrees is a good angle to test because it represents the case when the sensor is inverted. Angles of 85 and 95 degrees are significant because they represent cases in which the fingerprint is presented slightly off center.

Results:

The template generated during enrollment should be compared to the templates acquired during the testing process. A percent match should be assigned to this comparison and recorded. The (FTE) Failure To Enroll rate and (FTA) Failure To Acquire rate should also be documented. These performance measurements will help to determine the effects of angle of rotation on the fingerprint device.

OUTPUTS:

FTA

FTE

Percent match

Time between enrollment and testing

Sensor surface cleansing frequency

3.2.2. Distance from Device (Translation for Fingerprint Systems)

In this evaluation, we assume that the enrollment and tests are performed in the same session. In this case, we define a session as the time frame between when a user enters the temperature controlled chamber and when the user exits the chamber. For best results, once the chamber has returned to the normal operating environment as stated by the vendor, the test subject should re-enroll into the system database for each test. This will help reduce any effects of template aging, any changes in user habituation, and other human factors during the testing process that could affect the accuracy of the results.

In this evaluation we assume that the same finger is used during the enrollment and testing process. It is also assumed that during the enrollment process, the fingerprint was imaged and the template was generated under normal conditions as stated by the vendor. The next step is to compare the newly acquired fingerprint template to the template created during enrollment. This difference (if any) could be attributed to the adverse effect biometric presentation, in particular translation, has on the fingerprint system.

INPUTS:

Humidity, temperature, lighting, threshold values, sensor cleaning frequency, date, time

METHOD:

Setup:

With the temperature controlled chamber used in section 3.1, the fingerprint sensor should be placed inside the chamber and the test subject must be able to properly present their fingerprint(s) to the device in the chamber while maintaining isolation from the outside environment. Threshold values should be set to the appropriate values and held constant throughout the testing process. See section 2.5 for more information on threshold values. The fingerprint sensor should be placed at normal biometric device placement, (0, 0). See section 2.2 for further information about device placement. Throughout this entire test protocol, the fingerprint sensor should remain at normal biometric device placement, (0, 0).

Obtain a piece of oak tag board or manila folder. Cut out 4 pieces of board such that they are the exact shape and size of the sensor surface area. Referring to Figure 5, cut out one quadrant in each of the four pieces to create four different fingerprint placement masks and label them as pictured below. Label each mask A, B, C, and D according to Figure 5.

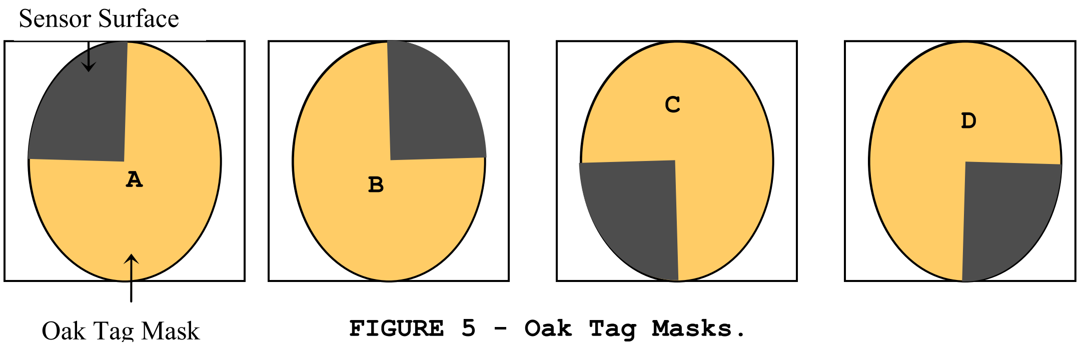


FIGURE 5 - Oak Tag Masks.
From: WVU Student: Nick Bartlow

Environment:

The lighting condition should be measured, humidity should be measured, the date and time of the testing should be documented, threshold value should be recorded, and the sensor cleaning frequency should also be recorded. These measured input values should simulate "normal operating conditions" as stated by the vendor and should be held as constant as possible throughout the testing. Please refer to section 2.1 for more information regarding environmental factors. Before enrolling the user, the sensor surface should be properly cleaned. Please refer to section 2.4 for more information on sensor cleaning.

Testing:

Now that the sensor surface is clean, the user should enroll into the fingerprint system per the instructions provided by the vendor. During enrollment, the user should properly present their fingerprint to the fingerprint sensor for imaging. For enrollment, the biometric presentation variable, angle of rotation should be at 90 degrees and translation should be 0 (none). For more information, please see section 2.3.

Once enrolled, sensor cleaning should be consistent throughout the entire testing process. For best results, we recommend cleaning the fingerprint sensor surface after each touch. Before each test, the environmental variables previously measured above should also be measured again and documented. These values should be consistent with the previously measured values and comply with the vendor's recommended "normal operating environment."

Now place template A on the sensor surface. Next the user should place the center of their fingerprint on the open (top-left) quadrant at an angle of rotation at 90 degrees. Once imaged and the match score documented, repeat this process for the remaining quadrants (B thru D). Figure 6 provides a visual representation of the appropriate placements.

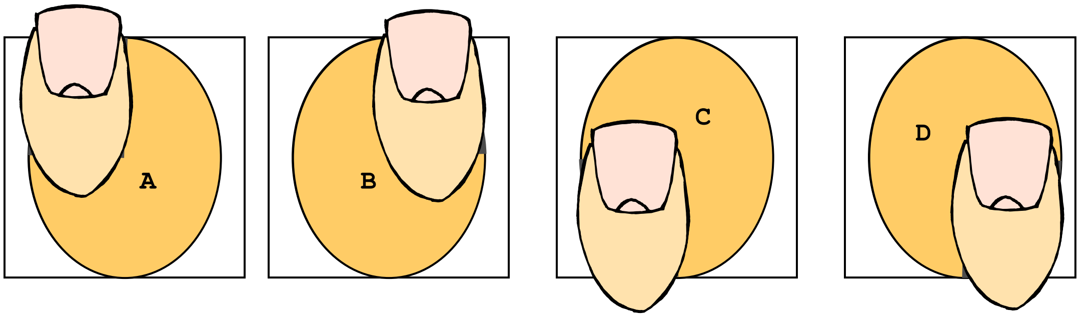


FIGURE 6 - Fingerprint scanning positions.
From: WVU Student: Nick Bartlow

Results:

The template generated during enrollment should be compared to the templates acquired during the testing process. A percent match should be assigned to this comparison and recorded. The (FTE) Failure To Enroll rate and (FTA) Failure To Acquire rate should also be documented. These performance measurements will help to determine the effects of biometric presentation, in particular translation, on the fingerprint system.

OUTPUTS:

FTA

FTE

Percent match

Time between enrollment and testing

Sensor surface cleansing frequency

3.3. Device Placement

In this evaluation, we assume that the enrollment and tests are performed in the same session. In this case, we define a session as the time frame between when a user enters the temperature controlled chamber and when the user exits the chamber. For best results, once the chamber has returned to the normal operating environment as stated by the vendor, the test subject should re-enroll into the system database for each test. This will help reduce any effects of template aging, any changes in user habituation, and other human factors during the testing process that could affect the accuracy of the results.

In this evaluation we assume that the same finger is used during the enrollment and testing process. It is also assumed that during the enrollment process, the fingerprint was imaged and the template was generated under normal conditions as stated by the vendor. The next step is to compare the newly generated fingerprint template to the fingerprint template generated during enrollment. This difference (if any) could be attributed to the adverse effect device placement, in particular σ and Φ, has on the fingerprint system.

INPUTS:

Humidity, temperature, lighting, threshold values, sensor cleaning frequency, date, time

METHOD:

Setup:

In order to produce repeatable tests for device placement, in particular σ and Φ, it is important to precisely tilt the fingerprint sensor at these angles. We recommend placing the fingerprint sensor on top of a robotic tripod. The robotic tripod will allow angle measures to be inputted and will improve repeatability. With the temperature controlled chamber used in section 3.1, the fingerprint sensor should be placed inside the chamber and the test subject must be able to properly present their fingerprint(s) to the device in the chamber while maintaining isolation from the outside environment. Threshold values should be set to the appropriate values and held constant throughout the testing process. See section 2.5 for more information on threshold values. The fingerprint sensor should be placed at normal biometric device placement, (0, 0). See section 2.2 for further information about device placement. Throughout this entire test protocol, the fingerprint sensor should remain at the same device placement variables except for the angles σ and Φ.

Once the fingerprint system is properly setup and the user is in the test chamber, the chamber can now be sealed.

Environment:

Inside the chamber, the lighting condition should be measured, temperature should be measured, humidity should be measured, the date and time of the testing should be documented, threshold value should be recorded, and the sensor cleaning frequency should also be recorded. These measured input values should simulate "normal operating conditions" as stated by the vendor and should be held as constant as possible throughout the testing. Please refer to section 2.1 for more information regarding environmental factors. Before enrolling the user, the sensor surface should be properly cleaned. Please refer to section 2.4 for more information on sensor cleaning.

Testing:

Now that the sensor surface is clean, the user should enroll into the fingerprint system per the instructions provided by the vendor. During enrollment, the user should properly present their fingerprint to the fingerprint sensor for imaging. For enrollment and all testing, the biometric presentation variable, angle of rotation should be at 90 degrees and translation should be 0 (none). For more information, please see section 2.3.

Once enrolled, sensor cleaning should be consistent throughout the entire testing process. For best results, we recommend cleaning the fingerprint sensor surface after each touch. Before each test, the environmental variables previously measured above should also be measured again and documented. These values should be consistent with the previously measured values and comply with the vendor's recommended "normal operating environment." Once complete, with the aid of the robotic tripod, set the angles σ and Φ to 0 and 0 respectively. The user can now present their fingerprint, used during enrollment, to the sensor at an angle of rotation at 90 degrees with no translation. ***NOTE:*** *The biometric presentation variables should be kept constant.*

At all times keep either σ =0 and Φ =0, and repeat this process for the following σ and Φ angle values:

σ	Φ
20	20
0	0
-20	-20

Results:

The template generated during enrollment should be compared to the templates acquired during the testing process. A percent match should be assigned to this comparison and recorded. The (FTE) Failure To Enroll rate and (FTA) Failure To Acquire rate should also be documented. These performance measurements will help to determine the effects of device placement, in particular σ and Φ, on the fingerprint device.

OUTPUTS:

FTA

FTE

Percent match

Time between enrollment and testing

Sensor surface cleansing frequency

Appendix B. SecuGen Hamster Optical Fingerprint Sensor Specifications

I used an infrared remote control to determine whether or not the sensor has an infrared filter. Based on this test, the SecuGen Hamster appears to have an infrared filter. Technical specification for SecuGen Hamster could not be found, but some of the specifications for the SecuGen Hamster III are displayed below.

Technical Specifications

Fingerprint Sensor	SecuGen FDU02™
Dimensions (w/o stand)	1.1" x 1.6" x 2.9" (27 x 40 x 73 mm)
Weight (w/o stand)	3.5 oz. (100 g)
Resolution	500 dpi ± 0.2%
Verification Time	Less than 1 second
Operating Temperature	32° to 104°F (0° to 40°C)
Operating Humidity	< 90% relative, non-condensing
Supply voltage	5 V ± 5%
Interface	USB 1.1
Supported Operating Systems	Windows 2003 / XP / 2000 / Me / 98 SE - Download driver Windows CE, CE .NET, Linux - Available with SDK
Certifications	FCC

From: http://www.secugen.com/products/ph.htm