2003

Comparison of classification methods for perspiration-based liveness algorithm

Sujan T. V. Parthasaradhi
West Virginia University

Comparison of Classification methods for perspiration-based liveness algorithm

Sujan T.V. Parthasaradhi

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

Committee:
Stephanie Schuckers, Ph.D., Chair
Lawrence Hornak, Ph.D.
Harshinder Singh, Ph.D.
Department of Computer Science and Electrical Engineering
Morgantown, West Virginia, 2003

Keywords: Biometrics, Fingerprints, Liveness, Spoofing
Fingerprint scanners, Classification

ABSTRACT

Comparison of classification methods for perspiration-based liveness algorithm

Sujan T.V. Parthasaradhi

In the modern world there is a need for security. Biometric technologies provide a means for providing this security. Of the many different available biometric technologies, fingerprint recognition is the most popular. As with all security measures, biometric devices may be subject to attacks on the system. Fingerprint scanners may be susceptible to spoofing using artificial materials, or in the worst case, dismembered fingers. Liveness, i.e. to determine whether the introduced biometric is coming from a live source, has been suggested as a means to circumvent attacks that use spoof fingers. It has been shown that water based casting materials and cadaver fingers were able to be scanned and verified for most fingerprint scanner technologies. In our laboratory an anti-spoofing method based on liveness detection has been developed for use in fingerprint scanners. This method quantifies a specific temporal perspiration pattern present in fingerprints acquired from live claimants. For this thesis, perspiration detection algorithm is optimized for different fingerprint scanner technologies, using a larger, more diverse data set, and a shorter time window. Several classification methods are tested in order to separate live and spoof fingerprint images. Each method had a different performance with respect to each scanner and time window. All the classifiers achieved approximately 90% classification rate for all scanners, using the reduced time window and the more comprehensive training and test sets. Based on the classification results, it is believed that this perspiration-based method has a potential to reduce the susceptibility of the fingerprint scanners to spoof attacks.

I dedicate this thesis to my entire family, especially to my parents for providing unlimited love, guidance, support and enthusiasm throughout my life.

Also, I dedicate this to Vijay uncle, Vahini aunty, my brother Suman, sister in law Meghna, and my fiancé Shilpa who have been great source of motivation and inspiration.

Acknowledgement

I am very grateful to my advisor, Prof. Stephanie Schuckers, who devoted immense time and effort in this research. She provided lot of motivation, knowledge and enthusiasm that helped me in successfully finishing my Masters. I also acknowledge Prof. Lawrence Hornak for his insightful and constructive comments. I am indebted to Prof. Harshinder Singh for helping me in discriminant analysis and for coming all the way to Virginia for my defense. I also thank Reza for the valuable comments and his research, which was the base of my thesis. Many thanks to Pisut, Simona, Rohin and Chris for their co-operation and necessary feedback. I am also thankful to Nina Clovis and all the people who participated in data collection, without whom my research would be incomplete.

Table of Contents:

Table of Figures:

1 Introduction and Background

1.1 Introduction

Biometrics can play a vital role in enhancing security systems and is under consideration for dramatically increased use in order to minimize security threats in military organizations, government centers, and public places like airports. Biometrics systems use physiological or behavioral characteristics to automatically determine or verify the identity of a person. Biometrics is the only unit, which evolves extensively around several processes like programming, integrating technologies, digital identity management, data mining, etc. Examples of biometric technologies include fingerprint, face, iris, hand geometry, voice, and keystroke recognition. Biometrics has several applications like

- Controlling access in hospitals, hotels, and private sectors.
- Network security
- In telecommunications for call centers, telephone banking.
- For secure use of handheld devices like PDA'S and cell phones.
- Time and attendance
- ATM and credit cards
- Internet banking and shopping
- Electoral polling method
- Protecting automobiles from illegal access

1.2 Background

No security system is infallible. As with all security measures, a biometric system is subject to various threats like attacks at the sensor level, replay attacks on the data communication stream and attacks on the database [1]. This research will focus on countermeasures to attacks at the sensor level of fingerprint biometric systems or spoofing, the process of defeating a biometric system through an introduction of a fake biometric sample or, worst case, a dismembered finger. The potential solution is liveness detection. Liveness detection, i.e. to determine whether the introduced biometric is coming from a live source, has been suggested as a means to circumvent attacks that use spoof fingers.

Liveness detection plays a vital role in the security of the input mechanism of biometric devices. Liveness detection in the biometric devices depends upon two things that are: (1) determining one or more qualities of a biometric sample and (2) checking their consistency with the qualities associated with samples during enrollment. The term “liveness” refers to distinguishing between a living person and an artificial representation of person in a biometric system. The lack of liveness detection in a biometric system makes it susceptible to spoofing. “Spoofing” is the process of defeating a biometric system through fake biometric samples. Therefore a biometric system may need “liveness” test for detection of spoof attacks. Any biometric system should be designed by keeping the liveness detection in perspective. In order to avoid the processing of non-live data, liveness detection may be performed at acquisition stage or identification/verification stage.

Our laboratory has demonstrated vulnerability to spoofing using dental materials for casts and Play-Doh for molds [2], [3]. Furthermore, we have tested fingerprint scanners with cadaver fingers. In our testing, ten attempts were performed for all available security levels for optical, capacitive AC, capacitive DC, and electro-optical technologies [2]. Results showed that the spoofing rate for cadaver fingers was typically 90% when verified against an enrolled cadaver finger, whereas for Play-Doh and water-based clay, results varied from 45-90% and 10-90%, respectively, when verified against an enrolled live finger. This research demonstrated that water-based casting materials and cadaver fingers are able to be scanned and verified for most fingerprint scanner technologies. Example images from live, cadaver and spoof fingers, obtained using commercially available fingerprint sensor technologies, are shown in Fig. 1.

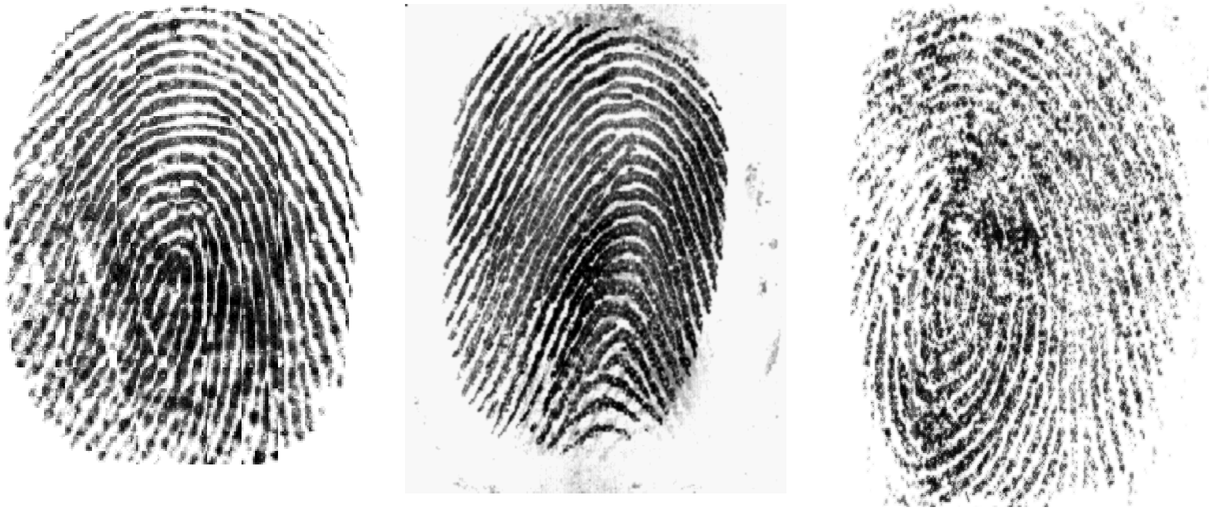


Figure 1.1: Images captured with commercial fingerprint sensors from live, cadaver and spoof fingers.

Initially, an anti-spoofing method developed in our lab was based on a time-series of fingerprint images captured from a DC capacitance-based Si CMOS fingerprint scanner [3]. The method uses the physiological process of perspiration to determine the vitality of a fingerprint. The initial algorithm extracted the grey levels along the ridges to form signals, calculated a set of features, and used a neural network to perform classification. The training and test sets were formed from 18 live, 18 spoof, and 18 cadaver fingerprints. Results gave 100% precision for distinguishing between fingerprints collected from live and spoof/cadaver fingers. While these initial results were encouraging, they also raised a number of issues, which, if adequately addressed would aid in the assessment of the viability of the approach. These include the performance of the techniques across a more diverse population, the contraction of the time series data to achieve user transparency of the technique, and the applicability of the approach to other fingerprint sensor technologies.

As per definition, biometric technologies can be categorized into two types: One is physiological biometrics and another is behavioral biometrics. Examples of physiological biometrics are fingerprint, face, iris, retina, hand geometry, etc. Examples of behavioral biometrics are speech, handwritten signature and keystroke analysis. This chapter will describe spoof attacks in various biometric technologies and discuss how “liveness detection” in biometric devices provides a possible solution to spoof attacks.

1.3 Liveness Detection for Physiological Biometric Techniques

Fingerprint Recognition:

In fingerprint scanning different types of fingerprint sensors like optical, capacitive and ultrasound are used. Capacitive scanners are most popularly used. Previous work has shown that it is possible to spoof a variety of fingerprint technologies through relatively simple techniques. These include utilization of latent fingerprints on the scanner with pressure and/or background materials (e.g., a bag of water), molds created from casts of live fingers, and molds from casts made from latent fingerprints lifted from a surface and reproduced with photographing etching techniques [2] - [7]. Casts have been made from wax, silicon and plastic, and molds from silicon or gelatin (gummy finger) [4], [5].

In order to avoid spoof attacks of fingerprint biometric systems, various liveness countermeasures have been considered including thermal sensing of finger temperature [8], laser detection of the 3-D finger surface and pulse [9], pulse oximetry [8], [10], ECG [8], and impedance and electrical conductivity of the skin (dielectric response) [11]. Other techniques that can make spoofing more difficult include challenge response, use of passwords, tokens, smart cards, and multiple biometrics. Summaries of liveness and anti-spoofing methods are given in [2], [12], [13]. Most methods require additional hardware, which is costly and, unless integrated properly, may be spoofed with an unauthorized live person. In addition, most previously developed methods are not available commercially and/or have not been tested rigorously in order to determine their effectiveness.

In our research, we have developed a method for detecting the perspiration pattern in the finger that identifies the liveness of a fingerprint by looking at a series of fingerprints captured at different time instants. The perspiration pattern is an efficient and important countermeasure as it is absent in spoof and cadaver fingers. Perspiration is a main characteristic of live skin, which regulates human body temperature. Sweating is defined as "active secretion of a watery fluid onto the body surface from either ecrine or apocrine sweat glands". Our method maps two-dimensional images into one-dimensional signals, which represent the gray level values along the ridge. Variations in gray levels correspond to variation in moisture. This method calculates a static measure, which quantifies the static variability in gray level along the ridges, and several dynamic measures, which measure the difference in the local maximums and minimums in the ridge signal. Details about the perspiration algorithm and its features are explained at the end of this chapter.

Iris Recognition:

There are many companies, which are developing various iris scan cameras based on the algorithms developed by John Daugman [14]. Iris consists of trabecular meshwork of connective tissues, colageneous stromal fibres, ciliary processes, contraction furrows, and rings colorations. 256 features of such type are used to form a 512 byte template. It is very difficult to spoof an iris scan camera because of the unique feature of iris, i.e., the structure of human iris is unchanged from the eighth month of gestation until a few minutes after death [15]. Also, a detached eyeball cannot be used as it changes very quickly to the state where it would not match. Some iris scan cameras that do not include a liveness countermeasure. Such cameras can be spoofed with the help of an 'artificial' eye. The artificial eye is made by printing digital iris images on a paper that had a small hole in the middle and behind where the hidden pupils of actual human beings were placed [16]. In order to prevent this some cameras are provided with a liveness counter measure that looks for the "hippus movement" i.e. the constant shifting and pulse that takes place in the eye. This liveness test ensures that the reading is fresh. Also drooping lid of eye has been considered as one of the counter measures. Occurrence of these natural activities in the eye makes iris recognition as one of the better biometrics to ensure liveness.

Facial Scanning:

Different facial recognition cameras use various technologies like local feature analysis, Eigenface evaluation and "learning" systems using neural networks. Some facial recognition cameras were easily spoofed with the help of high quality video clip of a registered person. To avoid such attacks, facial recognition cameras are provided with visual processing techniques that check "liveness". These techniques detect liveness in the following ways:

- It looks for reliable cues in input that indicate whether the source is two rather than three-dimensional.

- A “challenge response” mechanism is incorporated into software for physical access control. It asks the user to present a particular expression. If the requested change is detected then access is allowed otherwise not.

- It tries to determine whether the head is moving against the background or not. [15]

- It also observes for a degree of three-dimensionality. [15]

- It also looks for the edge boundaries of a picture. [17]

Hand Geometry:

This method measures distinct characteristics of the hands, which include external contour, internal lines, and geometry of hand, length and size of fingers, palms and fingerprints. This technology can be spoofed by making a good cast of the hand.

In order to avoid this, it may be provided with a temperature sensor and also a sensor that could measure the flow of blood in the blood vessel pattern. These have not been implemented in any commercial system, to date.

1.4 Liveness Detection in Behavioral Biometric Techniques

Speech Recognition: This method uses vocal characteristics such as mouth, nasal cavities, vocal tract that make the production of speech. High quality recordings may also pose a threat to any voice authentication system. Liveness tests can eliminate the threats to all these attacks. Liveness tests are performed in the following ways:

- Some applications are installed, which verify callers by asking them to repeat randomly generated digits or phrases, or rotating challenge questions, ensuring that there is a live person on line. [17]

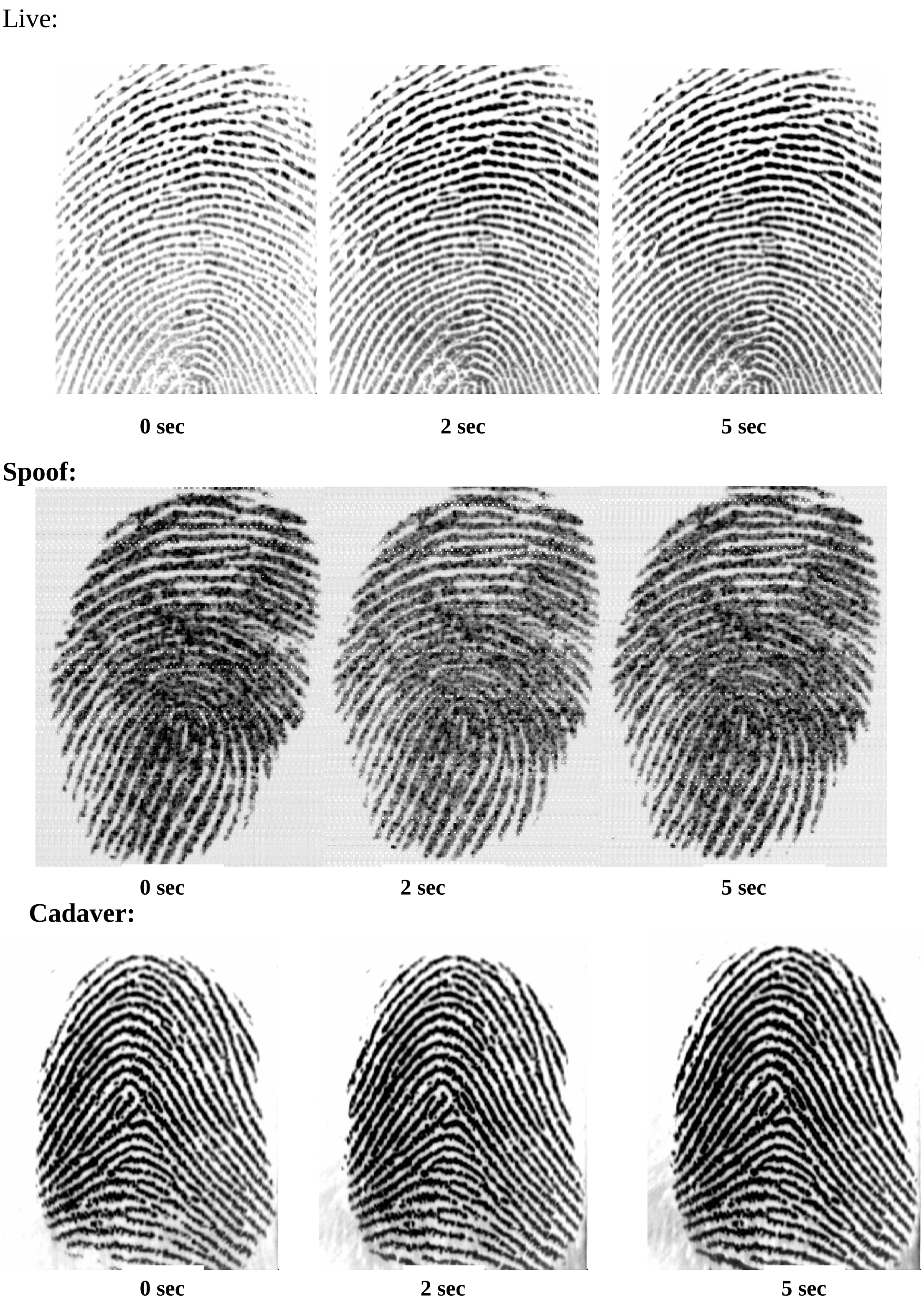
- A lip tracking system is provided, which locates the lips in the video sequence and then perform feature extraction, such that lip dynamics helps speech recognition in addition to providing liveness testing. [18]

DNA pattern, sweat gland identification [19], odor detection and ear recognition are other new biometric techniques. Among these, sweat gland recognition is believed to the best as it identifies the location of the sweat glands [19] on the ridge of the fingerprint and automatically checks for liveness as a part of the process.

The objective of our research is adding the vitality detection to fingerprint scanners. In this thesis fingerprint scanners of different technologies were studied including optical, capacitive AC, capacitive DC, electro-optical etc. The following section details previous work in the development of this perspiration detection.

1.5 Perspiration Detection Algorithm

The basis for our original method and details of the algorithm are discussed in detail in [4]. In brief, when in contact with the fingerprint sensor surface, live fingers, as opposed to cadaver or spoof, demonstrate a distinctive spatial moisture pattern, which evolves in time due to the physiological perspiration process. Optical, electro-optical, and solid-state fingerprint sensors are sensitive to the skin's moisture changes on the contacting ridges of the fingertip skin. These sensors can capture the time dependent, spatial pattern (Fig. 2).



Live:

0 sec **2 sec** **5 sec**

Spoof:

0 sec **2 sec** **5 sec**

Cadaver:

0 sec **2 sec** **5 sec**

Fig 1.2 Example fingerprint images from live (top), spoof (middle), and cadaver (bottom) fingers captured at 0, 2 and 5 seconds (left to right) after placement on the scanner.

To quantify the perspiration phenomenon, the algorithm maps a 2-dimensional fingerprint image to a "signal" which represents the gray level values along the ridges (Fig. 3). Variations in gray levels in the signal correspond to variations in moisture both statically (on one image) and dynamically (difference between consecutive images). The static feature measures variability in gray level along the ridges due to the presence of perspiration around the pores. The dynamic features quantify the temporal change of the ridge signal due to propagation of this moisture between pores in the initial image relative to image captures two (or five) seconds later.

The basic steps performed in the algorithm are described as follows. More information about the initial algorithm and its calculation of seven measures is available in [4]. First, two fingerprint images are captured within a 2 (or 5) second interval (referred to as first and last capture). The results are enhanced by having the subjects wipe their fingers immediately before capture. The captured images are binarized and thinned to locate the ridges. Ridges that are not long enough to cover at least 2 pores are discarded. Using the thinned ridge locations as a mask, the gray levels of the original image underneath these ridge paths are recorded. The resulting signals for the first and the last capture are representative of the moisture level along the ridges for a given image in the time series. Fig. 3 illustrates these steps by showing a portion of the ridge signals derived from the first and last captures from a live source along the mentioned mask.

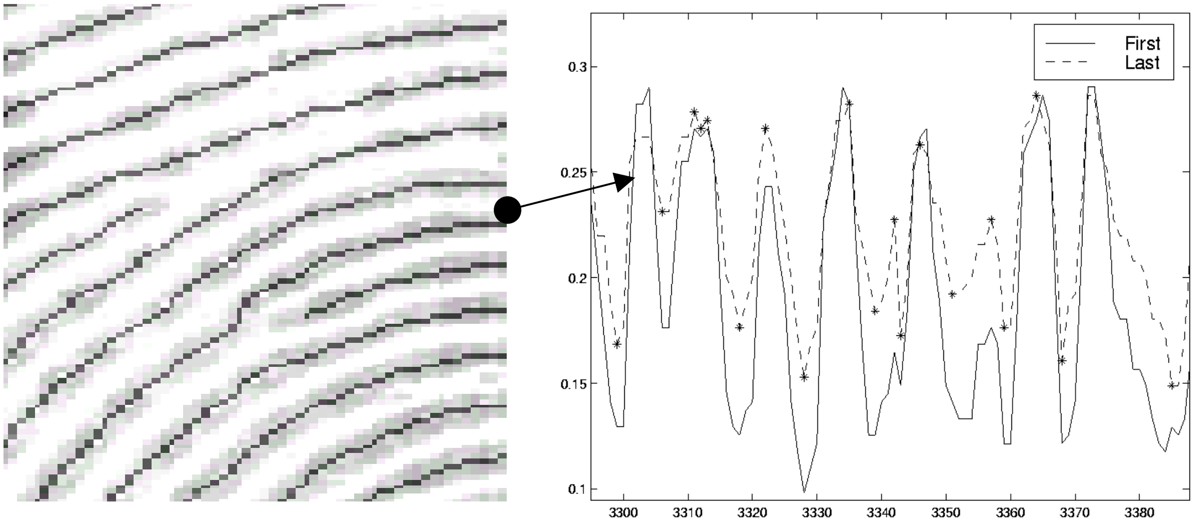


Fig 1. 3 Ridge mask superimposed over the original grayscale fingerprint image (left) and resulting ridge signal for two image captures, 0 (solid) and 5 (dashed) seconds (right)

Prior work established and obtained test results from one static and four dynamic measures [4]. The static measure (SM) uses the Fourier transform of the ridge signal from the first image capture and quantifies the existence of active pores through the corresponding spatial frequencies. The four dynamic measures quantify the specific ongoing temporal changes of the ridge signal intensity due to active perspiration. The first dynamic measure (DM1) is the total swing ratio of the first to last fingerprint signal. The second dynamic measure (DM2) is the growth ratio of the minimum to maximum of the first and last fingerprint signal. The third dynamic measure (DM3) is the mean of the differences of the first and last fingerprint signals, and the fourth dynamic measure (DM4) describes the percentage change between the standard deviations of the first and last fingerprint signals.

To increase the robustness of the classification, two additional measures were introduced later and are explained here. In the case that the fingerprint signal swings beyond a device's dynamic range (i.e. the device enters cut-off or saturation due to extreme dryness/moisture), the information about the minimums and maximums and their rate of change, utilized in the second dynamic measure, will be lost. These two measures address this by taking advantage of the upper and lower cut off region lengths of the fingerprint signals and converting them into perspiration rates. The fifth dynamic measure (DM5) indicates how fast the low cut-off region of the ridge signal is disappearing, thus extracting further perspiration rate information from the low-cutoff region. The sixth dynamic measure (DM6) indicates how fast the high cut-off region of the ridge signal is appearing, thus extracting further perspiration rate information from the wet-saturation region.

1.6 Thesis Overview:

This research presented in the thesis has two phases; (i) spoofing fingerprint scanners and (ii) evaluation of a newly developed liveness method. This dissertation discusses the research in three parts.

- **Chapter 2: Scanners and Spoofing** describes the scanners technology and their results of spoofing for different security levels.
- **Chapter 3: Data Collection** details the methods used for collection of a larger, more diverse dataset which includes 33 live, 33 spoof (based on the 33 live individuals), and 14 cadaver fingers for each scanner.

- **Chapter 4-5: Classification** describes the classification techniques tested in order to separate live and spoof fingerprints and presents their performance with respect to each scanner and time window.

2 Scanners and Spoofing

2.1 Scanners

Many technologies including capacitive AC, capacitive DC, optical prism based, and optical non-prism based, thermal, pressure and ultrasonic, etc have been used to develop reliable fingerprint scanners.

Scanners of interest were classified according to their basic capturing technology:

1. Optical
   - i. With prism
   - ii. Without prism
2. Capacitive
   - i. DC
   - ii. AC
3. Other, Proprietary
   - i. Tactile sense

Other technologies like ultrasound were not considered relevant for this study. Since they are not likely to be sensitive to perspiration.

Capacitive and optical fingerprint scanners are the most popular. Four types of fingerprint scanner technologies in this study: capacitive DC (Precise Biometrics, 100sc), electro-optical (Ethentica, Ethenticator USB 2500), optical (Secugen, EyeD hamster model no HFDUO1A) and capacitive AC (Authentec, AES 4000). These systems were selected based on considerations of technology diversity, availability and flexibility of the software developer kit (SDK), availability of raw image through

SDK, reasonability of price and ability to readily access and construct a time series of sensor raw images.

2.2 Basic Principle of Optical Scanner

Optical scanners consists of charge coupled device (CCD) and an array of light emitting diodes. LED’s are used to illuminate the finger. When a finger is placed on the scanner, the CCD takes picture of the finger like camera and generates an electrical signal with the help of reflected light. This signal consists of light and dark pixels representing ridges and valleys in the finger respectively. This electrical signal is converted into a digital template with the help of analogue to digital converter. The image generated from optical scanner is inverted. [20]

2.2 Basic Principle of Capacitive Scanner

Capacitive scanners consist of 2 dimensional array of capacitors with a thin dielectric layer using the CMOS process. This dielectric layer protects the surface of sensor from moisture, chemicals, dirt, etc. Capacitors present in sensor act as a bottom plate and the finger acts as an upper capacitor plate. As the distance between the finger and sensor changes, the measured capacitance also changes with the ridges and valleys in fingerprint. This variation in capacitance generated through the change in voltage creates an analogue signal. This signal is converted into digital form with the help of analogue to digital Converter [20]. The dielectric constant plays very important role in capacitive sensor and is of great importance for the developed vitality detection algorithm. In brief, if moist skin is in touch with sensor then it will measure higher capacitance because of high dielectric constant of perspiration and if the skin is dry then it will have lower capacitance.

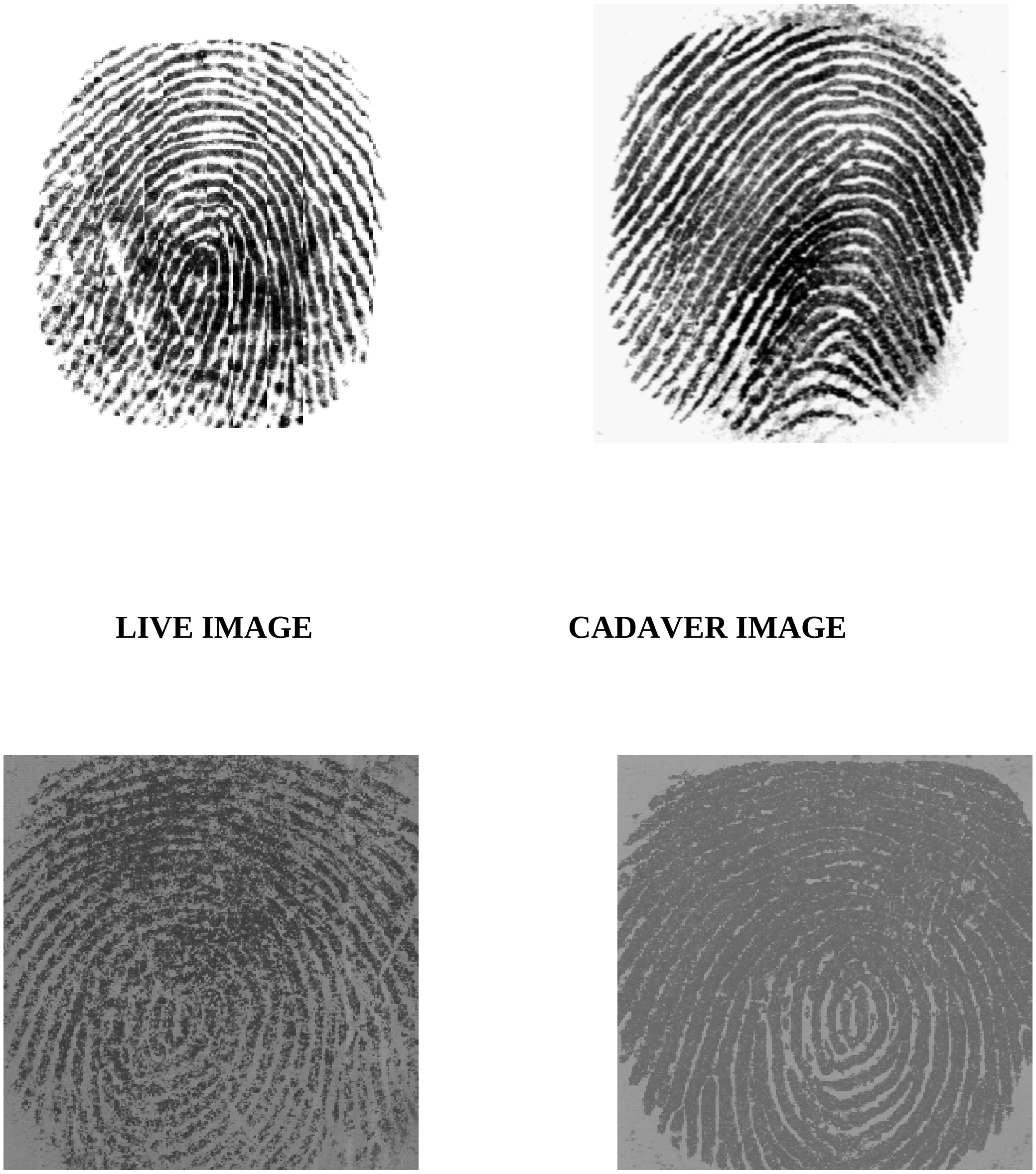
2.4 Scanner Details

Precise Biometrics 100SC:

This device is a DC capacitive based and it has a resolution of 500 dpi. A fingerprint data is captured with the help of a solid state capacitive sensing. The finger acts one plate of capacitor and surface of sensor acts as another plate, which consists of a silicon chip having an array of capacitors. These sensing plates form an 8-bit raster scanned image of a finger. This scanned image is converted into a template using “Precise Biomatch” minutia based algorithm [21]. It also has a provision of smart card. So it is possible to store the template at smart card to be used for verification purpose. The acquiring time is about 1 sec. This technology scans live and cadaver finger, and water based materials such as clay, play- doh, and wet rubber. It does not scan Polymer clay, dry rubber. Lastly, DC capacitive verifies live, cadaver fingers, clay, and play-doh made molds.

The following are the observations made for Precise Biometrics 100SC device:

- Perspiration is distinctly detectable.
- First capture is patchy.
- Perspiration progresses from pores



LIVE IMAGE

CADAVER IMAGE

CLAY IMAGE

PLAYDOH IMAGE

Figure 2.1 Images from different materials for Precise

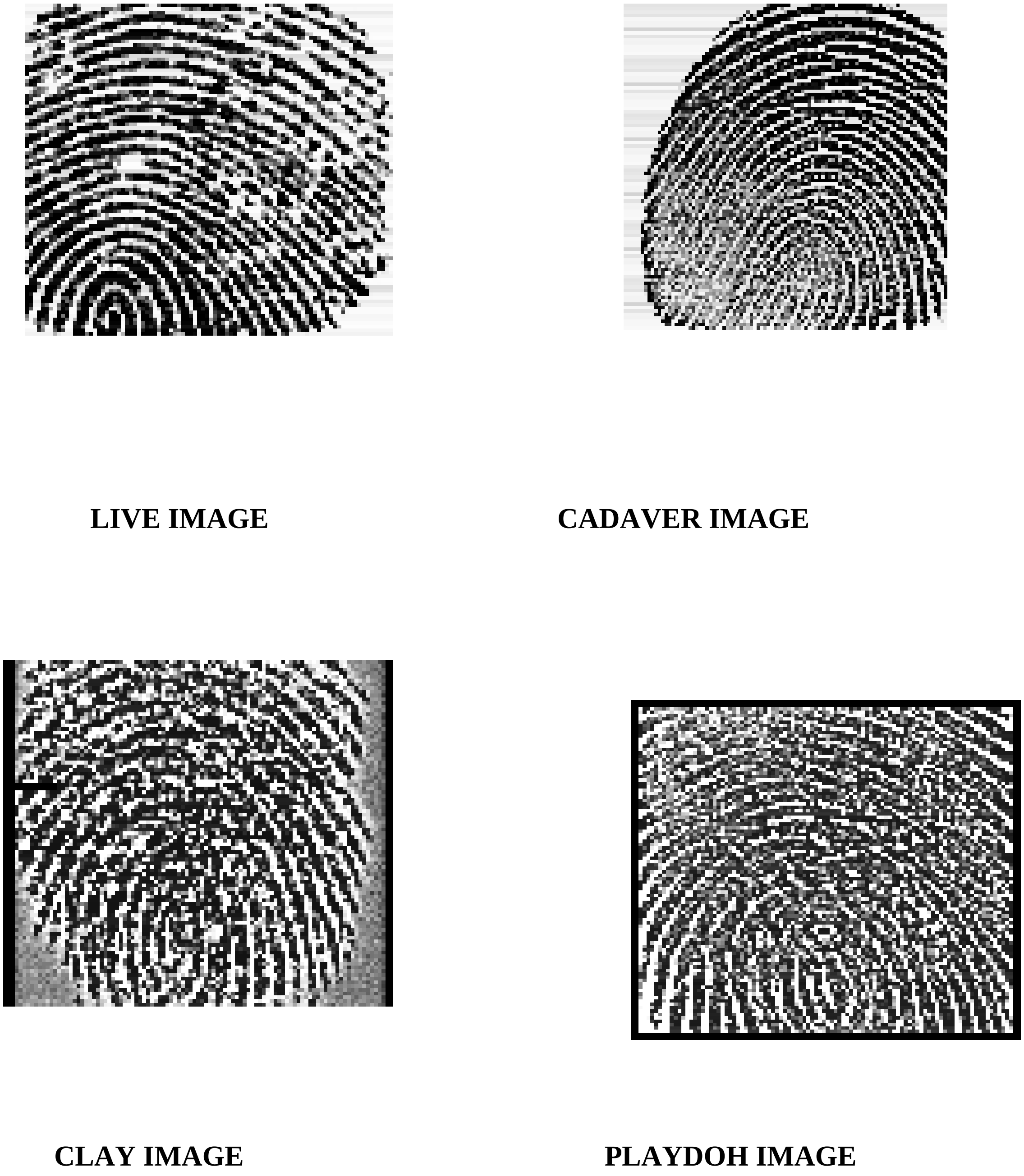
Device: Authentec AES-4000.

This device is AC capacitive based, and it has a resolution of 250-1000 dpi. It uses CMOS AC based technology called TruePrint, which scans the inner layer of the skin. It has a RF signal generator on a chip. The sensor is surrounded by a conductive surface, which sends a RF signal into the inner layer of skin. There are some variations in the signal as it follows through ridges and valleys. The sensor consists of array of antennas that receive this signal and uses it to generate a digital template. The software performs dynamic optimization by changing parameters of signal till an acceptable image is obtained. It uses cores, deltas, scars, ridge pattern and sweat glands of finger for creating templates [22]. The image obtained from the scanner is not raw; in other words it has been processed and hence, the images were not useful for processing by perspiration detection algorithm that requires a constant gray level over time. For this reason, the scanner was not used for data collection from cadavers but it was used for live data collection where it may be used in the future. In addition, the perspiration algorithm was not optimized for this device since the small perspiration changes in the grey level were masked by changes performed by the scanner. The acquiring time is 0.075 sec. AC capacitive device scans live and cadaver fingers, and water based materials such as clay, play-doh and does not scan wet rubber, dry rubber, and polymer clay. This technology verifies live, cadaver fingers, clay, and play-doh made molds.

Following are the observations made for the Authentec AES4000 device:

- Perspiration is not detectable
- Output images are processed

- Changes contrast, brightness, etc



LIVE IMAGE

CADAVER IMAGE

CLAY IMAGE

PLAYDOH IMAGE

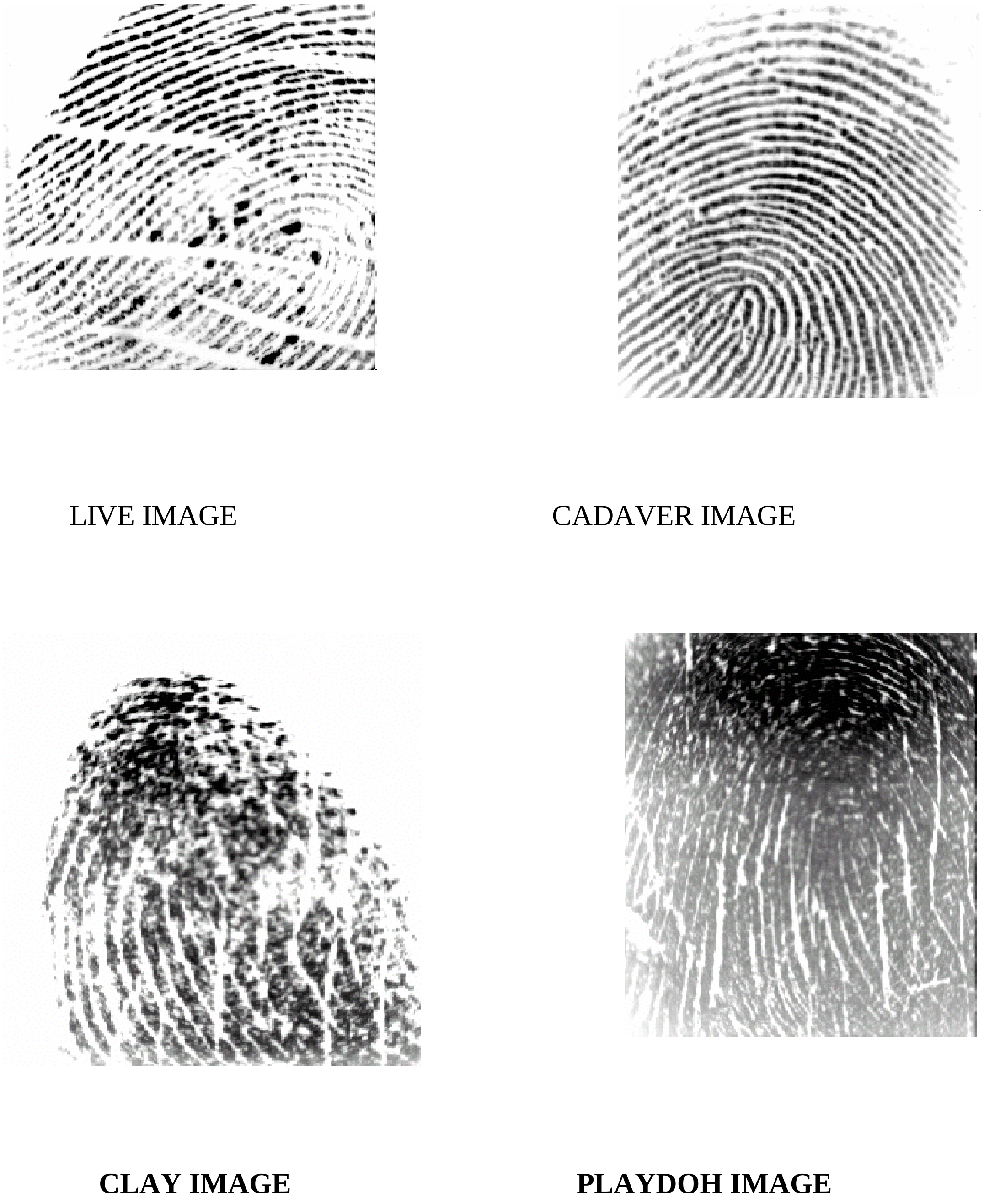
Figure 2.2 Images from different materials for Authentec

Device: Secugen EyeD Hamster

This device is optical based with a prism and has a resolution of 500 dpi. It uses Surface Enhanced Irregular reflection (SEIR) technology [23] along with the CMOS sensor to capture fingerprint images. A minutia based algorithm processes the fingerprint image and converts that into a digital template. The image acquisition time is about 1 sec. This optical device scans all i.e. live, cadaver, play-doh, clay, wet rubber, dry rubber, polymer, and clay and verifies live, cadaver fingers, clay and play-doh made molds.

The following are the observations made for Secugen EyeD Hamster device:

- Perspiration is distinctly detectable
- First capture is patchy
- Progression from pores alongside ridges



LIVE IMAGE

CADAVER IMAGE

CLAY IMAGE

PLAYDOH IMAGE

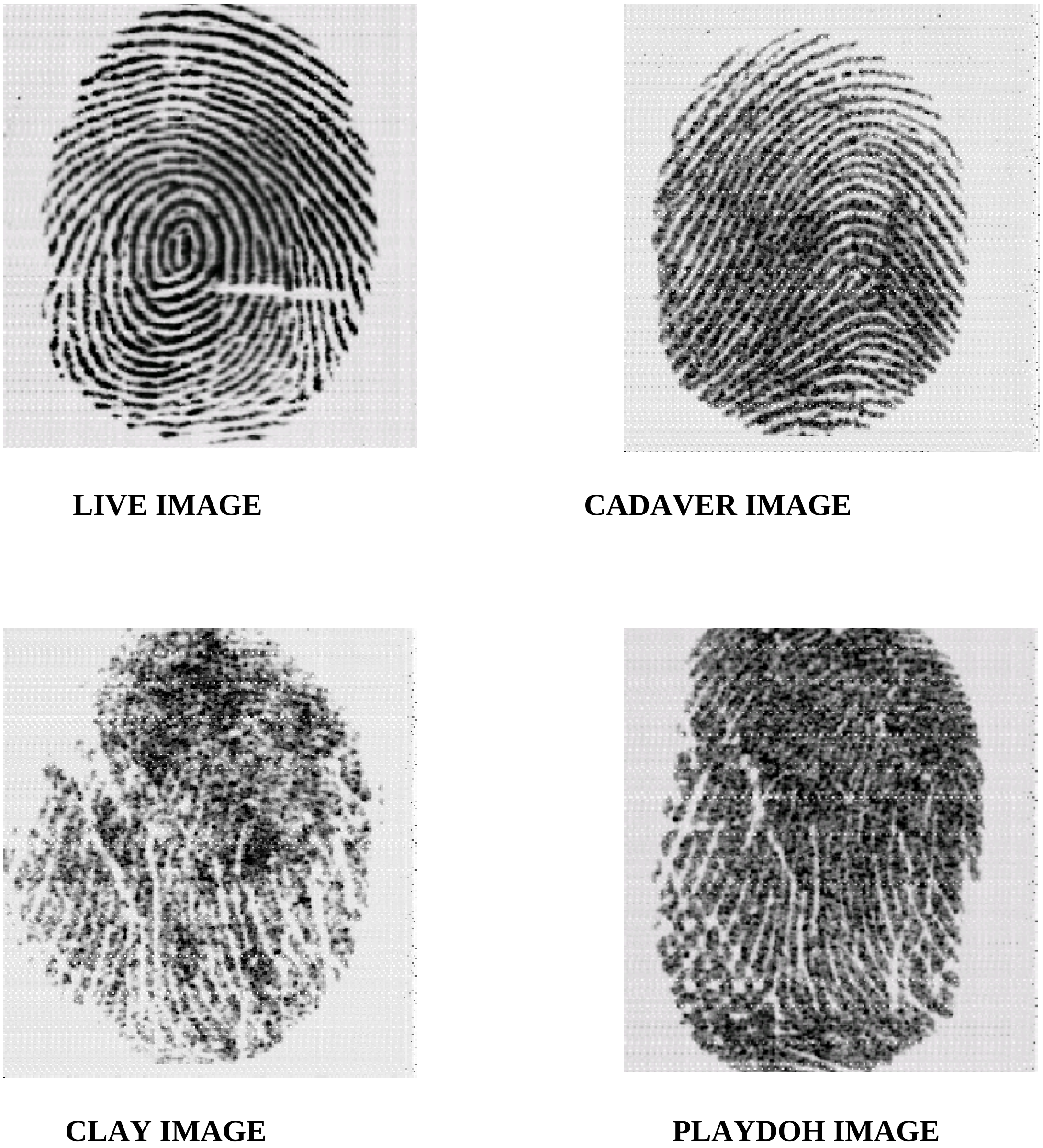
Figure 2.3 Images from different materials for Secugen

Device: Ethentica Ethenticator 2500.

This device is tactile sense based and has a resolution of 403 dpi. It is an electro optical (combination of glass camera and tactile sense polymer) fingerprint scanner. The Tactile sense polymer consists of several layers including a black coat layer for protecting the sensor from sunlight, a conductive layer for supplying current, and a light emitting layer for illuminating fingerprint image. After the image is illuminated, the glass camera detects the illumination and image is translated into digital template with the help of ASIC [24]. The image acquisition time is 0.6 sec. The electro-optical device scans live and cadaver fingers, water-based materials such as clay, play-doh, and wet rubber and does not scan non water-based materials such as polymer clay and dry rubber. The device verifies live, cadaver fingers, clay and play-doh made molds.

The following are the observations made for Ethentica Ethenticator 2500 device:

- Perspiration is not distinctly detectable.
- First capture is partially patchy.
- Some progression from pores alongside ridges.



LIVE IMAGE

CADAVER IMAGE

CLAY IMAGE

PLAYDOH IMAGE

Figure 2.4 Images from different materials for Ethentica

2.5 Spoofing

The process of defeating a biometric system through fake biometric sample is called spoofing.

As we know there are various fingerprint spoofing techniques like gummy fingers, breathing on the fingerprint scanner to reactivate the latent fingerprint, using a bag of water on top of the latent fingerprint, dusting the latent fingerprint using graphite powder, stretching adhesive film over it and applying pressure, using halogen light along with latent fingerprint and graphite powder for intense backlighting for optical spoofing, and using wax casts and silicon molds.

Our laboratory has developed a spoofing technique for testing the liveness detection algorithms. This method uses a mold made from dental impression materials and using playdoh and paper clay for function of casts. A detailed procedure is explained as follows.

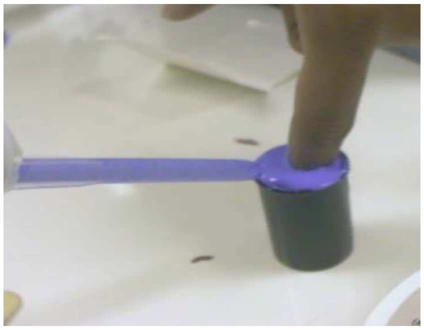
2.6 Procedure for Creating Spoof Fingers

The apparatus required is as follows: polyvinylsiloxane dental impression materials of type 3, polyvinylsiloxane dental impression materials of type 0, film-can, spiral nozzles, Extrude gun.

The procedure is as follows:

1. Take polyvinylsiloxane dental impression materials of type 3 (precision- 20 micron) and 0 (lower precision, higher consistency and strength).

2. Type 0 mix is put in a film-can to make outer supportive shell.
3. Push finger in paste and hold it that position for 5-6 minutes.



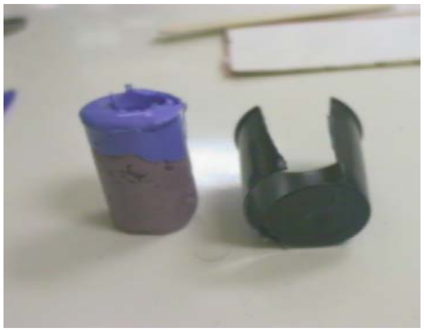
3. Take finger out of the paste and put type 3 rubber on subject’s hand.

4. Put back finger in can and fill it up with more type 3 rubber to complete the mold.

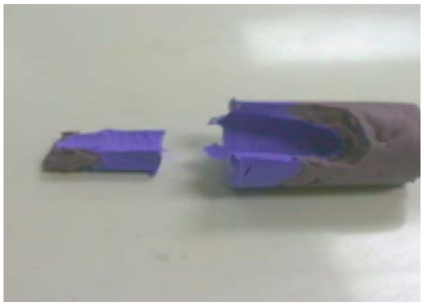
5. Hold the finger in still position.

6. Remove the finger after 5-7 minutes.

7. Take out the mold.



8. Cast is made ready by cutting the back and sides of the mold properly.



9. Then use any water-based material to make the spoof of finger.

10. Press material firmly into the mold and remove it gently.

11. Spoof finger is prepared.

Table 2.1 **Device Summary Table**

Device/ Material	Pers- -piration Seen?	Cadaver		Clay		Play-doh		Wet rubber		Polymer clay		Dry rubber	
Capture (C) /Verify (V)		C	V	C	V	C	V	C	V	C	V	C	V
Ethenticator (tactile sense)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N
Secugen (prism optical)	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N
Authentec (CMOS AC)	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Precise (Capacitive DC)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N

C- capture V-verify Blue- water based Grey- Non water based

Table 2.1 summarizes the types of materials that can be scanned by various fingerprint scanners. Playdoh and paper clay were chosen as the best for spoofing because these materials are moisture based and easily scanned by all scanners. As mentioned earlier in this chapter each scanner has different security levels and can be adjusted according to the application, we attempted to spoof the fingerprint scanner at all possible security levels. Using a single cast, preliminary spoofing tests were done at all security levels both with playdoh and paper based clay. Then, using 10 different casts each scanner was spoofed at the default security level. Spoofing in our laboratory included playdoh fingers, paper based clay and cadaver fingers.

Play-doh spoofing included kneading of play-doh, pressing it firmly into the mold and removing it gently. After the spoof finger is prepared it is used to verify against an enrolled finger. Ten live subjects were enrolled, casts were created from each of the ten subjects, and verification with a spoof finger was attempted six times per person. For cadaver spoofing a cadaver finger is enrolled and then verified against the same enrolled finger. Fourteen cadaver fingers (from 4 subjects, of male age 41, female ages 55, 65, and 66) collected in collaboration with the Musculoskeletal Research Center (MSRC) at the West Virginia University Health Science Center were used for spoofing research. A detailed description of data collection of spoof fingers is given in Data Collection chapter. Protocols for these data collection are shown in the appendix section.

Each scanner was tested with cadaver fingers with 10 attempts each finger. The results section in this chapter consists of following three graphs for each scanner.

(i) Comparison of verification rate of live vs. playdoh vs. water based clay. Each experiment included 10 attempts per security level using a cast from the individual.

(ii) Spoofing results of 10 different casts at default security level. Each cast was attempted for six times. Each bar in the graph denotes how many times out of six, what percentage of casts was verified.

(iii) Cadaver Results

2.7 Spoofing Results of Different Scanners

Figure 2.71: Spoofing Results for Capacitive AC Fingerprint Scanner

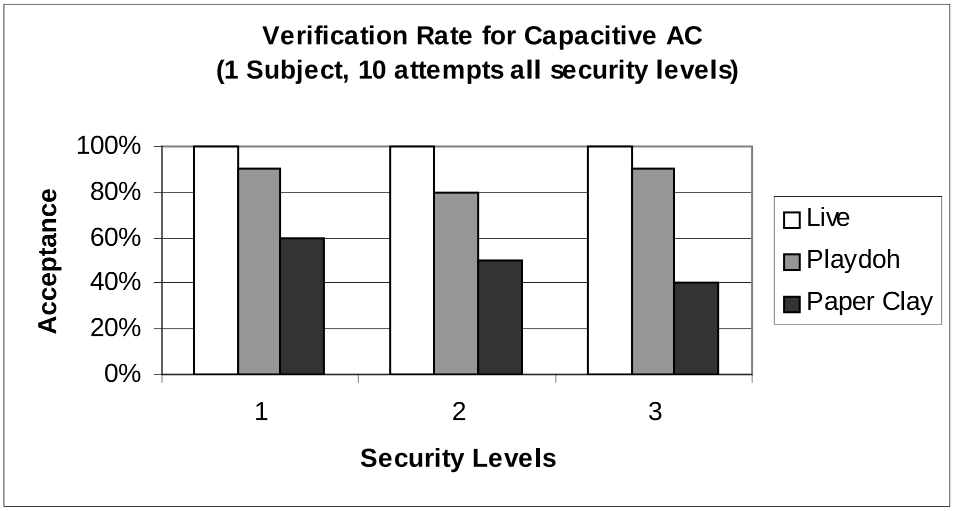


Figure 2.71(i)

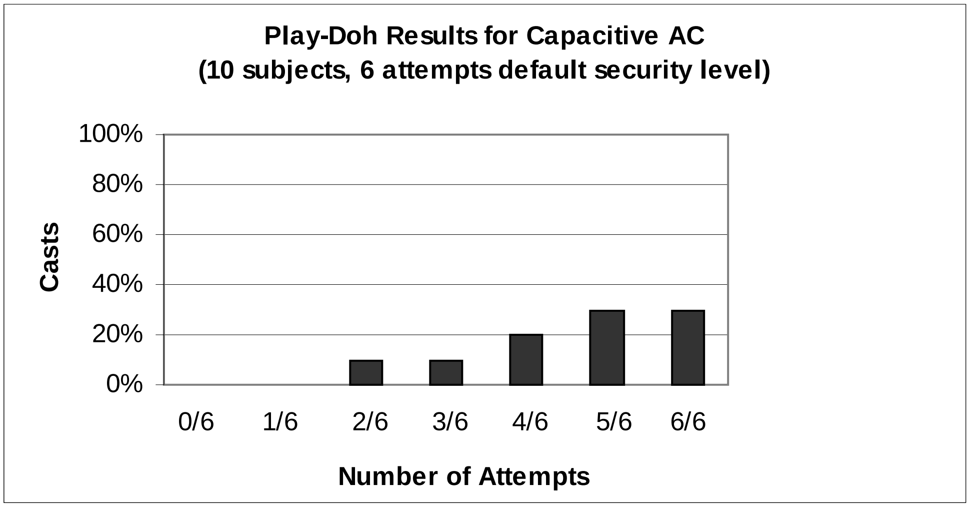


Figure 2.71(ii)

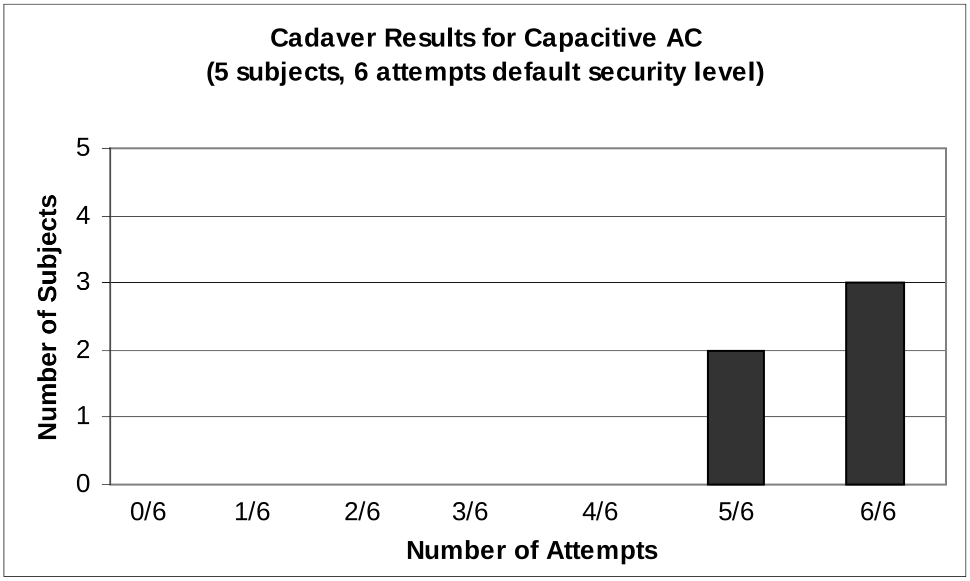


Figure 2.71(iii)

Figure 2.72: Spoofing Results for Capacitive DC Fingerprint Scanner:

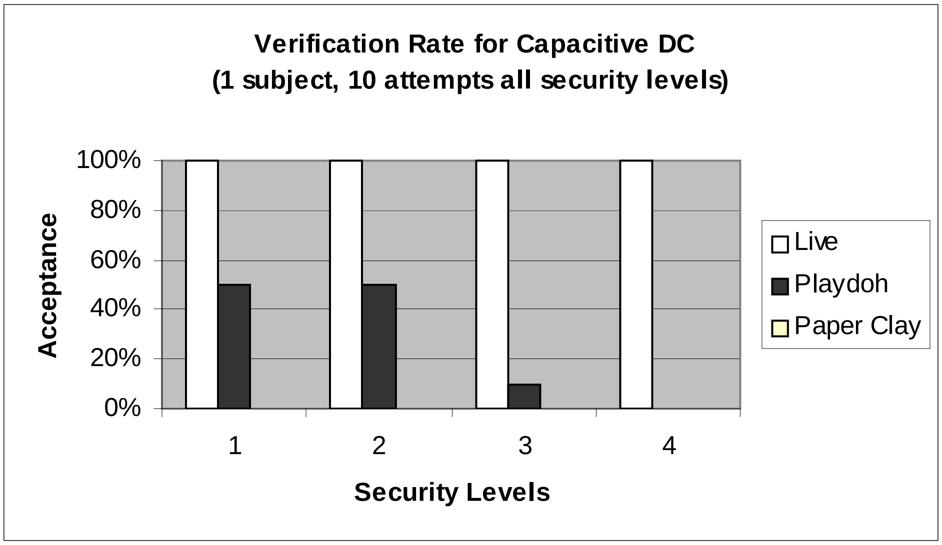


Figure 2.72(i)

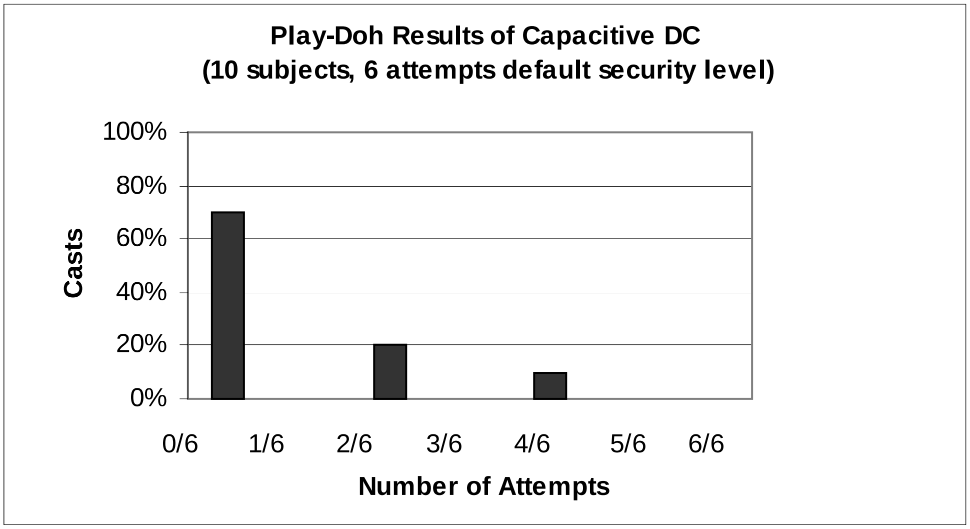


Figure 2.72(ii)

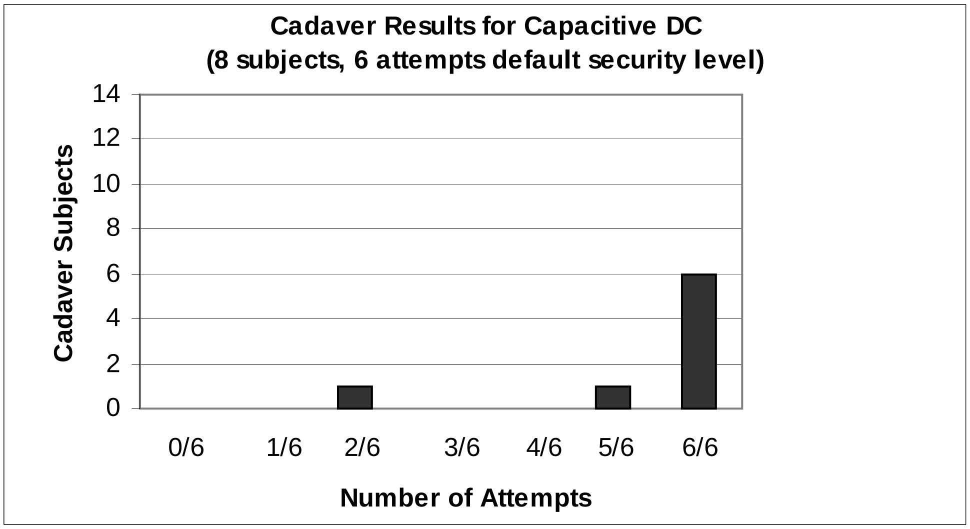


Figure 2.72(iii)

Figure 2.73: Spoofing Results of Electro-Optical Fingerprint Scanner:

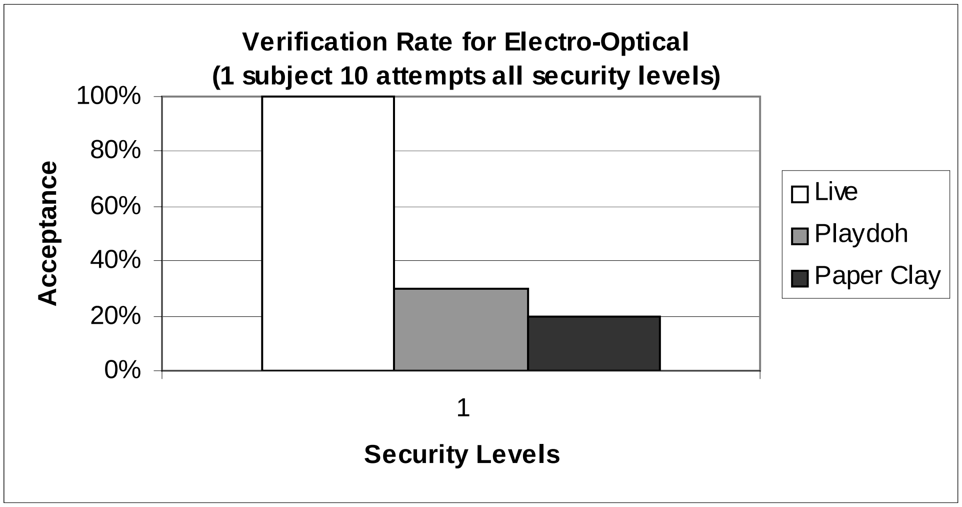


Figure 2.73(i)

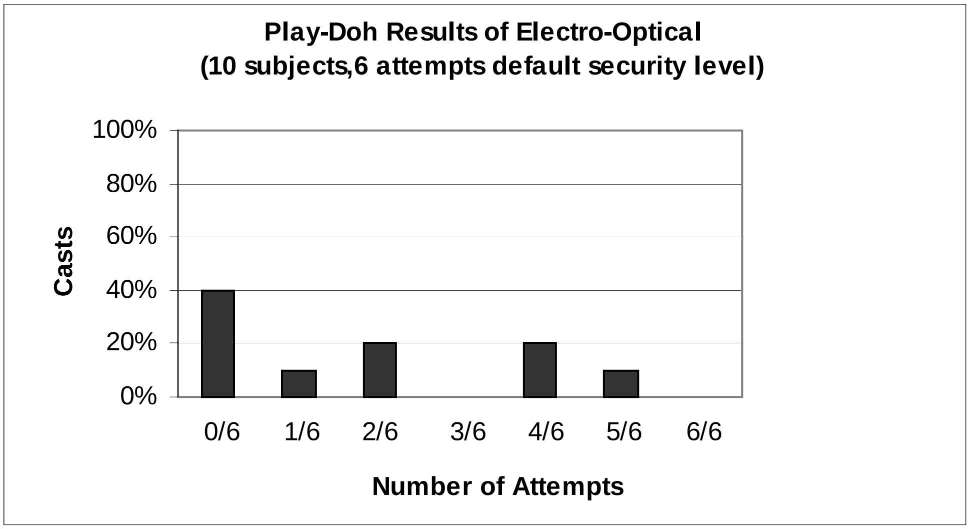


Figure 2.73(ii)

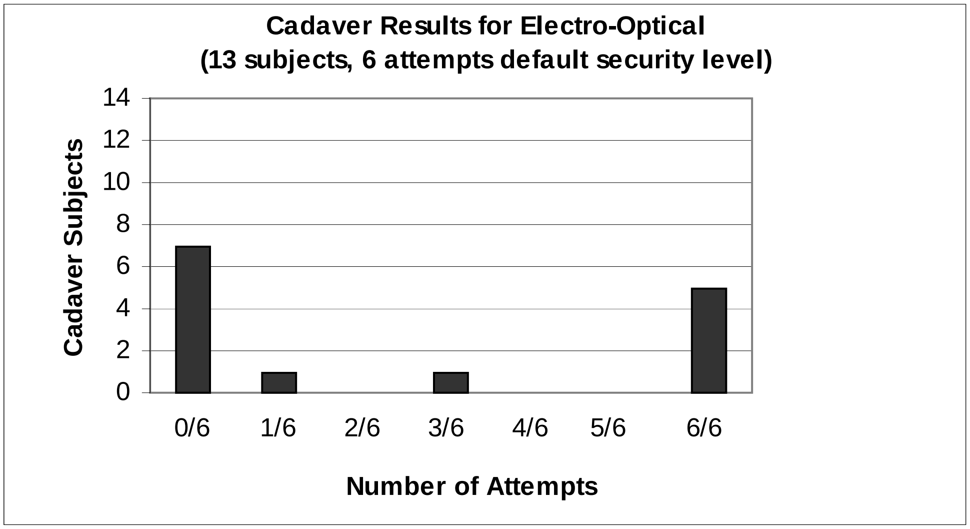


Figure 2.73(iii)

Figure 2.74: Spoofing Results for Optical Fingerprint Scanner:

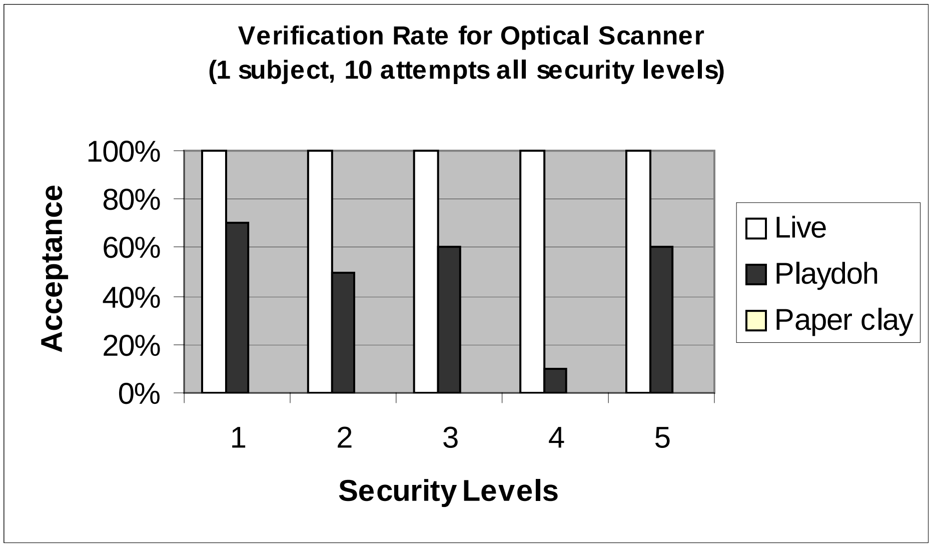


Figure 2.74(i)

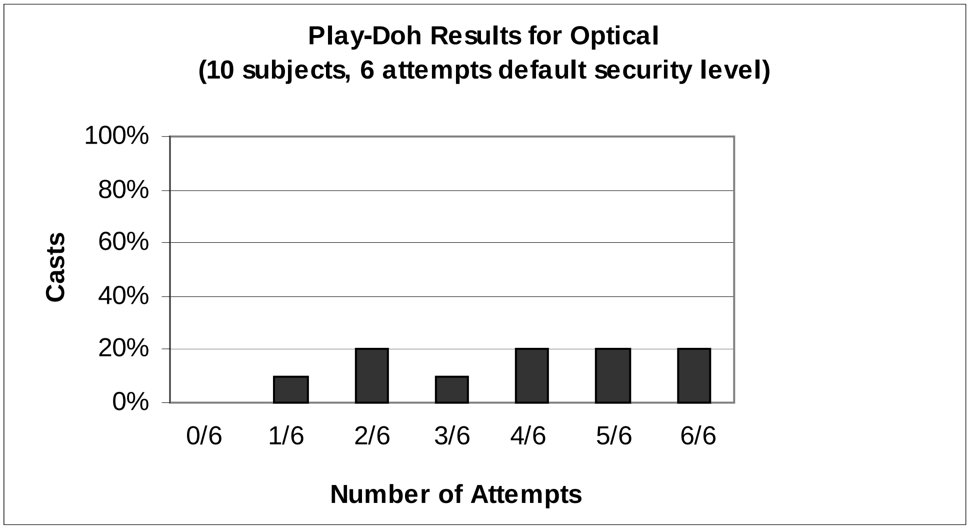


Figure 2.74(ii)

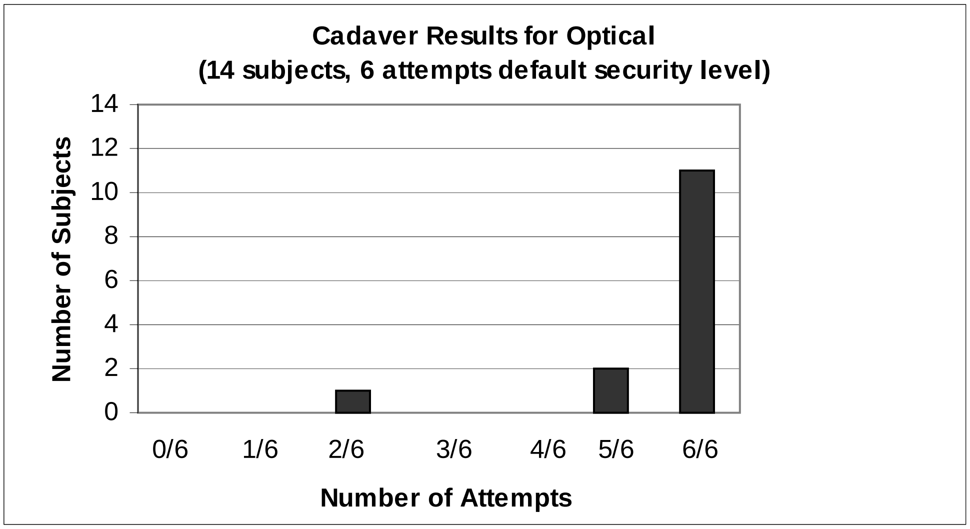


Figure 2.74(iii)

2.8 Spoofing Results Summary

The results present the success rate of verification for live and spoof fingerprints for each device. Figures 2-71(i), 2.72(i), 2.73(i), 2.74(i) shows spoofing success of Playdoh and paper based clay fingers of a single cast at different security levels for different scanners. For capacitive AC spoofing success ranges from 80-90% for playdoh fingers and from 40-60% for paper based clay, respectively for security levels from 1-3. For capacitive DC spoofing success ranges from 10-50% for playdoh fingers and 0% for paper based clay, respectively for security levels from 1-4. Since the spoofing success was 0% at 4th security level for playdoh, it was not done for remaining 5,6,and 7th security levels. For optical spoofing success ranges from 10-70% for playdoh fingers for security levels from 1-5. Spoofing the capacitive DC and optical scanners was very difficult using paper based clay. Spoofing success of paper based clay ranged from 10-20% and 30-40% for capacitive DC and optical device respectively. For electro-optical spoofing success is 30% for playdoh fingers and 20% for paper-based clay, for the only one security level available.

Figures 2-71(ii), 2.72(ii), 2.73(ii), 2.74(ii) shows the spoofing rate of playdoh at default security levels for different scanners. Spoofing included 10 different casts with six attempts per cast. Spoofing success was determined by the ratio of the sum of the number of successful attempts for all casts to the sum of total number of attempts made for all casts. Denominator was constant as 60 (10 x 6) for all scanners. For capacitive AC spoofing success is 0.77 (46/60), for capacitive DC spoofing success is 0.13 (8/60), for Optical spoofing success is 0.63 (38/60) and for electro-optical spoofing success is 0.3 (18/60). Over all, at least 3 of 10 subject casts were successful in spoofing all fingerprint scanners at least once. The spoofing success may vary as it is highly related to the quality of the cast and material used.

Initially five fingers of one cadaver subject were tested on different fingerprint scanners at all security levels. Approximately 90-100% success was achieved for all scanners. Figures 2-71(iii), 2.72(iii), 2.73(iii), 2.74(iii) show spoofing rate of cadaver at default security levels for different scanners. Cadaver spoofing included fourteen cadaver fingers (from 4 subjects, of male age 41, female ages 55, 65, and 66) collected in collaboration with the Musculoskeletal Research Center (MSRC) at the West Virginia University Health Science Center. Only the fingers that were able to enroll were considered for study. Six cadaver fingers were excluded from capacitive DC because of failure to enrollment. One cadaver finger was excluded from the electro-optical device because of technical difficulties with the scanner. Spoofing success was determined by the ratio of the sum of the number of successful attempts for all cadaver fingers to the sum of total number of attempts made for all cadaver fingers. For capacitive AC, cadaver study was discontinued because the images obtained from the device were not raw, so the images were not useful for processing by perspiration detection algorithm. Also, during the cadaver study of optical scanner only five attempts were made for one of the cadaver subjects. Hence the total number of attempts for optical is 83. The spoofing success is 0.86 (71/83) for optical, spoofing success is 0.90 (43/48) for capacitive DC and the spoofing success is 0.40 (34/84) for electro-optical.

Conclusion:

For all technologies at default security level, at least 3 of 10 subject's casts were of sufficient quality to spoof fingerprint devices at least once. Results showed that the successful spoofing rate for playdoh varied from 13-77% when verified against an enrolled live finger, depending on the device technology (optical, electro-optical, capacitive AC, and capacitive DC). Whereas for a single cast at all security levels of scanners play-doh and water-based clay results varied from 45-90% and 10-90%, respectively, when verified against an enrolled live finger. Spoofing success rate for cadaver fingers varied from 40-90% when verified against an enrolled cadaver finger. Therefore, water-based casting materials and cadaver fingers are able to be scanned and verified successfully for most fingerprint scanner technologies

3. Data Collection Procedure

3.1 Data Collection

In order to check the robustness of the perspiration detection algorithm, a large, more diverse dataset was collected. In collection of the dataset, several age groups (11 people between ages 20-30 years, 9 people between 30-40, 7 people between 40-50, and 6 people greater than 50), ethnicities (Asian-Indian, Caucasian, Middle Eastern), and approximately equal numbers of men and women were chosen. The dataset presents a diverse set of fingers and hence there may be some potential problems (dry finger, saturated finger, ridge variations, etc.). For each device, fingerprint images were collected from live, spoof, and cadaver fingers. Protocols for data collection from the subjects were followed that were approved by the West Virginia University Institutional Review Board (IRB) (HS#14517 and HS#15322). Our data set consists of 73-75 fingerprints from live, cadaver and spoof. As shown in the following chart, the data collection procedure is divided into three steps: live collection, spoof collection and cadaver collection. For each subject and device, fingerprint images for 20 seconds were collected using customized programs developed using manufacturer-provided SDK functions. The images utilized are the first image and images from approximately two seconds and five seconds after the start of the time-series collection. Spoof fingerprint images were generated using finger casts created from thirty subjects who participated in the fingerprint study.

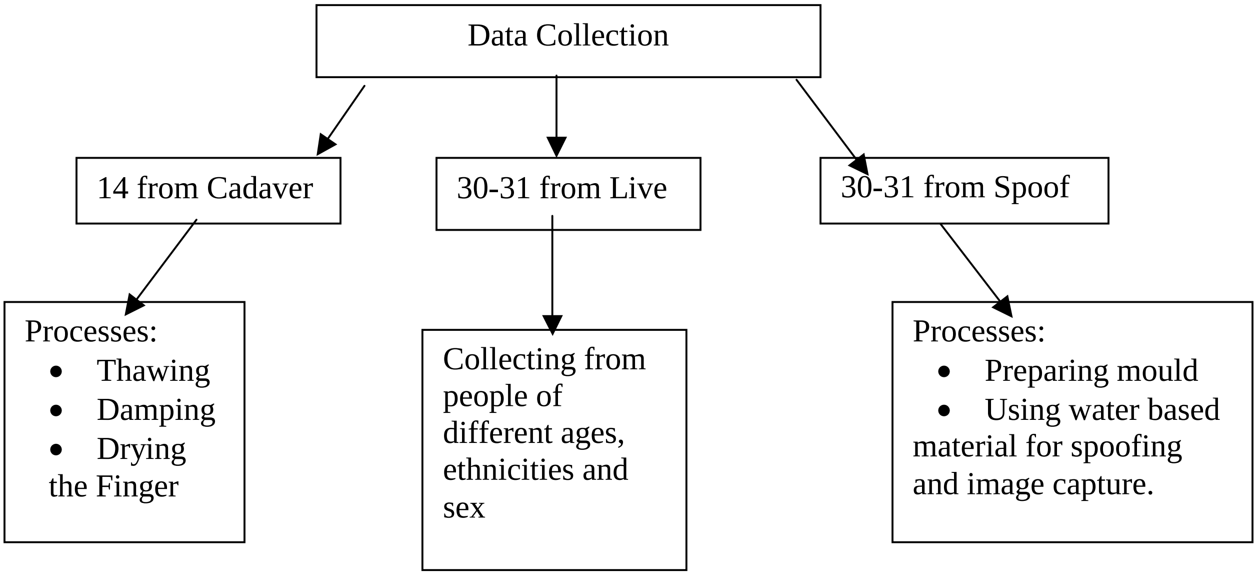


Figure 3.1 Data Collection chart

3.11 Live Collection

In this particular step fingerprints are collected from different groups of people of different age, sex and ethnicity. A protocol was developed to follow this procedure. The procedure is as follows:

1. Take the fingerprint scanner and wipe it.

2. Ask the subject to clean and dry the finger.

3. Enroll subject's finger.

4. If its enrolled in first attempt go to the verification stage; else attempt to enroll for 5 times. It is still not enrolled, go to the next fingerprint scanner.

5. During the enrollment save the enrolled image and template. (performed by the developed software)

6. After enrollment, ask the subject to verify his finger for six times. During verification, the default match score is used and the verified image and template are saved.

7. Wipe the fingerprint scanner with a tissue paper or cloth.

8. Ask the subject to clean and wipe his/her finger before taking a 20 sec capture.

9. During the capture make sure that capture and placement of finger both take place simultaneously.

10. Repeat the above procedure for three different scanners.

11. After that go to the next subject.

3.12 Spoof Collection

A protocol was developed to collect spoof data. Creation of the cast was described in section 2.6

1. Take the fingerprint scanner and wipe it.

2. Take the playdoh and finger cast.

3. Squeeze the playdoh in the finger cast and remove it properly

4.Playdoh finger is gently placed on the fingerprint scanner.

5. Scan the playdoh finger and take 20 sec capture of it.

6. If the capture is not good, knead the playdoh and repeat steps 3,4 and 5.

7. If capture is good, follow the above procedure for another scanner.

8. After capture for all scanners are complete, go to next playdoh finger and repeat the same procedure.

9. Verification was only done for a small set of spoof fingers.

3.13 Cadaver Collection

Protocol for cadaver collection is similar to live collection except that instead of a live finger, a cadaver finger was used. Flow charts for protocols of live, spoof and cadaver data collection are present in the appendix section.

3.2 Data Collection Summary

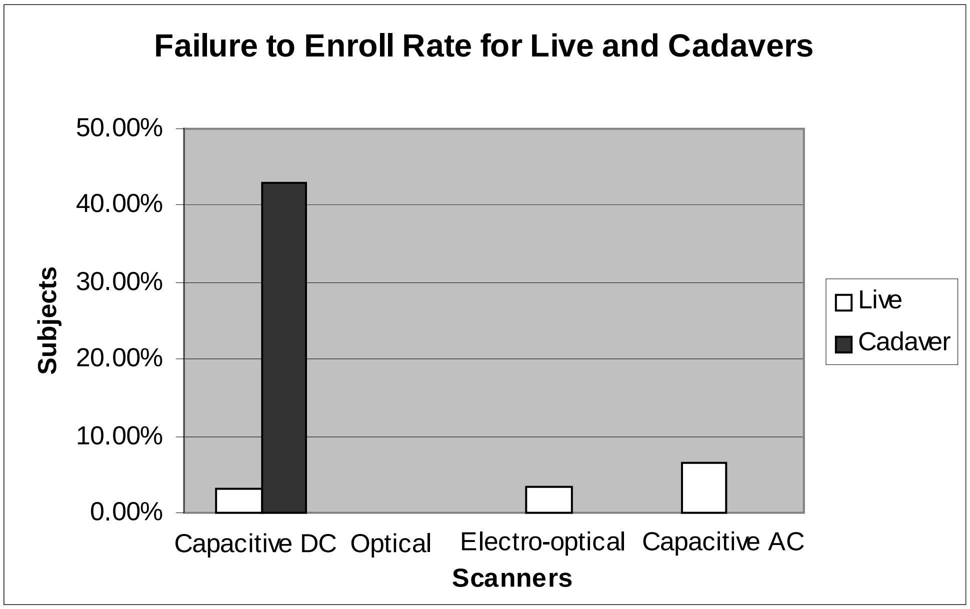


Figure 3.2 Failure to Enroll Rate

Figure 3.2 presents failure to enrollment rate for live and cadaver subjects. One live subject and 6 cadaver subjects were unable to enroll for capacitive DC device. Only one live subject was unable to enroll for electro-optical device. Cadaver study was discontinued for capacitive AC, as it was not producing raw images, therefore only 5 cadaver subjects were performed. Live collection was continued with a view to utilize the collected information in future. Two live subjects were unable to enroll for capacitive AC. For optical device all live and cadaver subjects were able to enroll. Thirty-three volunteers were solicited and represented a wide range of ages (20-60 years), ethnicities, and both sexes (17 men and 16 women). Two live subjects were excluded in two devices and three in another device due to following reasons: (i) inability to enroll and (ii) a technical error. Three subjects in the spoof category were excluded because a spoof cast was not created due to subject time constraints or quality of spoof cast.

Table 3.1 summarizes the number of subjects used for each device and category.

	Live	**Spoof**	**Cadaver**
Capacitive DC	31	30	8
Electro-Optical	30	30	13
Optical	30	30	14

4. Classification-I

4.1 Classification

Classification is an integral part in the various research areas like biometrics, medicine and computer science. Different methods of data collection create large and complicated data sets such that it is difficult to extract valuable information using simple calculations. Hence the aim of the classification is to interpret the data, predict the data and then classify it [25]. Basically classification comes into picture, when there is a scenario of more or less scattered objects over a large range of variation, falling into several groups. There are many classification procedures like artificial neural networks, cluster analysis, classification trees, discriminant analysis, etc. Three classification methods were used in this research: neural networks, discriminant analysis, and One R.

Classification was performed separately for each time window (2 and 5 seconds). Classification of images is divided into live and spoofs where spoof fingerprint images include images from Play-Doh spoofs and cadavers. With approximately 75 images for each scanner, 50% of the data was used as a training set and the remaining 50% as the test set for classification.

4.2 Introduction of Discriminant Analysis

This chapter deals with discriminant analysis and stepwise discriminant analysis in detail and describes briefly statistical analysis. Discriminant analysis is a classification technique used for classifying observations in any of the two groups on the basis of measurements on independent variables. It is also used for interpreting the relation between variables, predicting the important variables, and solving critical research problems. Discriminant analysis has several applications in various areas like pattern recognition, psychology, meteorology, remote sensing, etc.

A linear discriminant function is presented in the following way:

L1 = **Constant + $X_1w_1 + X_2w_2 + X_3w_3 + X_4w_4 + X_5w_5$................$X_nw_n$.**

Where $X_1, X_2, X_3, X_4, X_5, ...X_n$ are the variables and $w_1, w_2, w_3, w_4, w_5, ... w_n$

are their coefficients respectively.

Depending on the number of groups, discriminant analysis is used to generate multiple functions. Number of functions generated is one less than the number of groups. There is no limitation on the number of discriminating variables as long as the overall number of cases in a group exceeds the number of discriminating variables by two. Another condition for discriminant analysis is that the number of cases in a group should exceed the number of discriminating variables by greater than two [26].

As mentioned in the previous chapter that seven measures are generated from the perspiration-based algorithm. More information about the perspiration based algorithm and the seven measures generated from the algorithm can be found in ref [4]. One static and six dynamic measures are used as features for classification of images. These measures were obtained from two different time windows of two and five seconds.

Discriminant functions are used for the classification of two or multiple groups. Since fingerprint images are to be classified into two groups live and spoof, this case is a two-group problem. Discriminant analysis was performed with R [27] and SAS [28]. There are certain assumptions required for better performance of discriminant analysis.

Assumptions are as follows:

- Variables must have a joint multivariate normal distribution.
- In the two groups, variance-covariance matrixes of variables are equal.
- Two perfectly correlated variables should not be used at the same time.

Discriminant analysis uses pooled sample variance-covariance matrix of variables for generating a linear combination of variables called discriminant function [29]. Mathematical part of deriving discriminant function for each scanner for each time window is explained later in chapter. In our case as seven measures (1 static measure, 6 dynamic measures) are present, so first stepwise discriminant analysis was performed using stepwise selection to determine the variables that have meaningful contribution. The Normal quantile plots using R, a statistics software tool, verified normality of the individual variables.

4.3 Stepwise Discriminant Analysis

Stepwise discrimination process is a variable selection method that repeats the process of adding and removing the variable at each step. Stepwise discrimination can perform analysis using backward elimination, forward selection, or stepwise selection of the variables. In this research all methods of stepwise selection were performed and same subset of variables was obtained for each scanner and time window except for Ethentica 5 sec. For Ethentica 5 sec window an extra variable was selected by forward selection when compared to stepwise selection, but there was not a major change in its classification rate. In stepwise selection there is a chance of excluding some important variables in the process, as it does not consider the relationship between the variables that are not selected. Hence, stepwise selection may not build the best model. A procedure for performing discriminant analysis of data having several variables includes stepwise discrimination. It consists of the following two steps:

1) Perform stepwise discrimination process for the entire data to determine the important variables or the best subset of variables.
2) Perform the discriminant analysis and generate linear discriminant function using those important variables.

Forward selection starts with zero variables in the process. At each step, based on the value of F test a variable having significant contribution is entered. The forward selection process stops if the unselected variables do not meet the entry criterion.

Backward elimination starts with all the independent variables in the model. At each step, based on the value of F test a variable having least contribution to the discrimination model is dropped. The backward elimination process stops if all the remaining variables satisfy the criteria to stay in the model.

Stepwise selection procedure is the combination of forward selection and backward elimination. It starts similar to forward selection with none of the variables in the model. The model is examined at each step. The variable having the least contribution as measured by F test is removed and the variable, which is not present in the model but having significant contribution, as measured by F test is entered. Basically it uses ‘F to enter and F to remove’ process. The stepwise selection process stops, if all the variables in the model satisfy the criterion to stay and none of the other meets the criterion to enter.

For any selection process, only one variable can be entered into the model at each step. This selection process does not take into consideration the relationship between the variables that were not chosen. Stepwise selection process picks up a subset of powerful variables from the total set of variables to construct a good discrimination model for the best classification rate. There are many selection criteria for stepwise selection like

- Using significant F values from covariance analysis in which selected variables act as covariates and the variables taken under consideration act as dependent variable. It is also called F test.

- Using the squared partial correlation of variables for selecting the variable.

Both criteria may choose different number of variables but they make decision in the same order. The tolerance test is also required in selection process [28].

Initially univariate F values are computed for each variable assuming each variable as the only predictor. At step 1 the variable with the largest F value is entered. After a variable is entered, the wilks’ lamda, partial F values and tolerance levels for all variables are computed. From this step partial F values are used for selecting important predictors. Partial F values are covariance –controlled and are derived from an analysis of covariance. The selected variables in model act as covariates and the variable under consideration acts as a dependent variable. Univariate F values neglect the correlation among the variables. Hence partial F values are used for selecting important predictors.

At the second step, F value of the already selected variable is computed and tested for removal before the entry of new variable. If it satisfies the criteria to stay then it is used as a covariate in the covariance analysis for selecting the variable.

Then among the variables not in the model, the variable with the largest partial F value is selected.

In the next step, each of the two variables in the model is tested for the removal and then the next variable with largest F value is selected and so on. Similarly, consecutive steps add variables based on their partial F values. This process continues until all variables in the model satisfy the criteria to stay and the variables not in the model fail to satisfy the entry criteria. Normally liberal significance levels (α-values) in the range of 0.10 to 0.25 are used for higher chance of retaining important variables in the discrimination model. In this case default value of α equal to 0.15 was used [28].

For this particular criterion, if the sample size is larger, a larger number of variables is selected. This particular F value condition is applied only to the variables that are in the discriminant function at a given step not for all the variables. At the end of stepwise procedure a summary is computed which consists of the variables entered or removed and their respective F ratios.

The table summarizes the list of variables selected by stepwise procedure for each scanner for each time window.

Scanners	2 Sec Time Window	5 Sec Time Window
Electro-Optical	SM, DM2, DM6	SM, DM2, DM4, DM5
Capacitive DC	SM, DM2, DM4	SM, DM2, DM6
Optical	SM, DM2	SM, DM3, DM6

Using the above stepwise selected variables, discriminant analysis was also performed.

4.4 Mathematical Description of Discriminant Analysis

Discriminant analysis uses sample pooled variance covariance matrix of both the groups to generate coefficients for the discriminant function. A pooled sample variance covariance matrix is calculated using matrices of two groups in its deviation form [29].

$$\mathbf{Xld= X_1- \bar{X}_1,}$$

$$\mathbf{Xsd= X_2- \bar{X}_2}$$

Where Xld and Xsd are the live and spoof vectors in its deviation form,

X_1 is the vector containing seven variables of all live subjects.

X_2 is the vector containing seven variables of all spoof (spoof + cadaver) subjects.

Matrix in deviation form is calculated by subtracting the mean vector of all the variables from the vector containing the original values of variables. A covariance matrix for each group is obtained by multiplying the transpose of the vector in deviation form with the matrix in the deviation form i.e. x1′ *x1. Similarly a covariance matrix for another group is calculated i.e. x2′ *x2. Then a pooled variance covariance matrix is calculated using the following formula:

$$\mathbf{S= (1/ (n_1+n_2-2)) (X_{Ld}'{*}\, X_{Ld} + X_{sd}'{*}\, X_{sd})}$$

Matrix containing the coefficients of the discriminant function is calculated by multiplying pooled sample variance covariance matrix with the difference of the mean matrices of the two groups. The formula [29] used for generating coefficient matrix is

$$\hat{\mathbf{b}}' = \mathbf{S}^{-1} (\bar{\mathbf{X}}_1 - \bar{\mathbf{X}}_2)$$

where

$\hat{\mathbf{b}}'$ is a co-efficient matrix

$\bar{\mathbf{X}}_1$ is a mean vector of seven variables of live group

$\bar{\mathbf{X}}_2$ is a mean vector of seven variables of spoof group

4.5 Discriminant Functions

Following are the discriminant functions obtained for each scanner for each time window using all seven variables.

Ethentica 2sec

$$\mathbf{DF_{Es2s} = -3.6952 + 0.87092SM - 0.1049DM1 - 0.01444DM2 - 2.37793DM3 + 7.8126DM4 + 0.02042\,DM5 - 0.2475DM6}$$

Ethentica 5sec

$$\mathbf{DF_{Es5s} = -6.3216 + 1.12536SM + 0.48089DM1 - 0.0468DM2 - 2.43311DM3 + 9.9654DM4 + 1.02976\,DM5 - 0.03711DM6}$$

Precise 2sec

$$\mathbf{DF_{p2s} = -3.94646 + 0.34497SM + 0.04036DM1 - 0.03188DM2 + 2.21613DM3 - 10.02131DM4 + 0.00482\,DM5 - 0.10794DM6}$$

Precise 5sec

DF_{p5s} = 0.56809 + 0.34208SM + 0.27985DM1 – 0.02082DM2 – 2.6852DM3 +5.28757DM4 – 0.00357 DM5 – 0.50822DM6

Secugen 2sec

DF_{s2s} = -10.30355 + 0.52716SM + 2.12812DM1 – 0.03003DM2 + 1.36177DM3 +2.57626DM4 – 0.01733 DM5 + 0.26927DM6

Secugen 5sec

DF_{s5s} = -13.72569 + 0.61328SM + 2.54566DM1 – 0.0823DM2 + 2.48303DM3 +0.79854DM4 – 0.02073 DM5 + 0.67942DM6

Following are the discriminant functions obtained for each scanner for each time window using important variables obtained from stepwise selection process.

Ethentica 2sec

DF_{Es2s} = -5.01574 + 0.73007SM – 0.05042DM2 – 0.12587DM6

Ethentica 5sec

DF_{Es5s} = -7.99049 + 0.84978SM – 0.07184DM2 + 5.17942DM4 + 0.77126 DM5

Precise 2sec

DF_{ps2s} = -2.12902 + 0.35855SM – 0.01646DM2 – 9.23935DM4

Precise 5sec

DF_{ps5s} = -1.75715 + 0.34309SM – 0.02616DM2 – 0.36642DM6

Secugen 2sec

DF_{ss2s} = -5.9192 + 0.49833SM – 0.0171574DM2

Secugen 5sec

DF_{ss5s} = -7.17108 + 0.58774SM – 1.04406DM3 + 0.49991DM6

4.6 Classification Rule

Discriminant function obeys a classification rule for assigning observations or individuals (measures in our case) in one of the two groups (live or spoof).

If ‘x’ is any vector consisting of seven measures obtained from a pair of fingerprint images. If $\overline{x}_1$ is a mean matrix of seven variables of live group and $\overline{x}_2$ is a mean matrix of seven variables of spoof group, then the classification rule [29] is as follows:

x will be classified into live if

$$|\hat{b}`\ (x - \overline{x}_1)| \leq |\hat{b}`\ (x - \overline{x}_2)|$$

and it will be classified into spoof if

$$|\hat{b}`\ (x - \overline{x}_2)| < |\hat{b}`\ (x - \overline{x}_1)|$$

Where $\hat{b}'$ is a co-efficient matrix

Discriminant analysis was performed for all seven variables and also for the variables obtained from stepwise selection process.

4.7 Discriminant Analysis Results

Figs 4.11 and 4.12 present the classification rate for live and spoof fingerprints for each device and time window using discriminant analysis. The figures compare discriminant analysis using all variables and variables selected by stepwise analysis. The following table summarizes the classification results achieved from two sets of variables.

Labels:

P2S-precise 2 sec   P5S-precise 5 sec

E2S-Ethentica 2 sec   E5S- Ethentica 5 sec

S2S-Secugen 5 sec   S5S- Secugen 5 sec

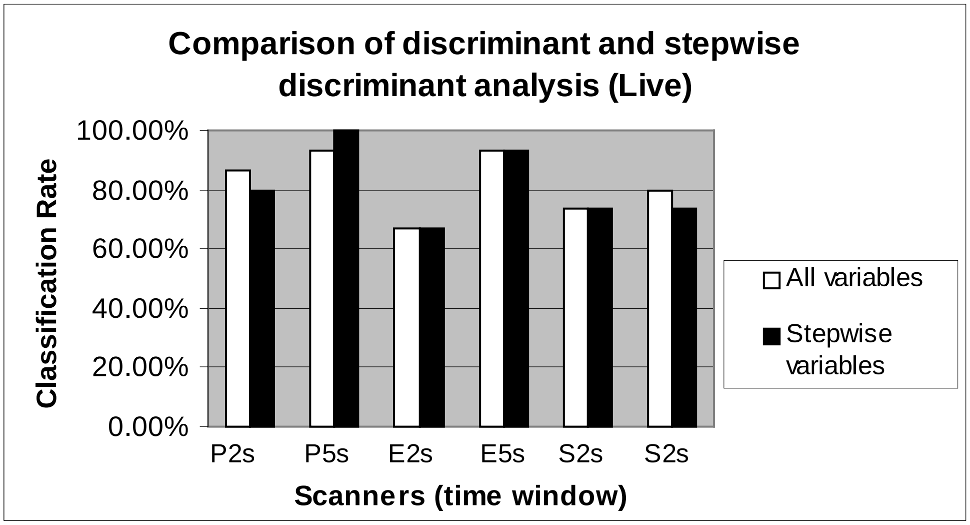


Figure 4.11

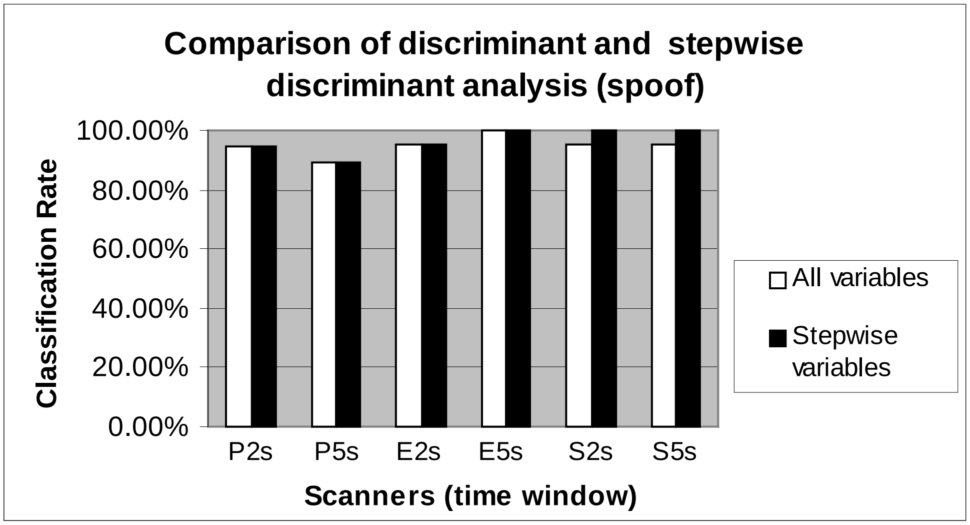


Figure 4.12

Figures 4.11 and 4.12 Comparison of discriminant and stepwise discriminant results for live and spoof

Table 4.1 Live Classification Table

Scanners	Discriminant analysis results using all variables	Discriminant analysis results using important variables
P2S	86.6%	80%
P5S	93.3%	100%
E2S	66.6%	66.6%
E5S	93.3%	93.3%
S2S	73.3%	73.3%
S5S	80%	73.3%

Table 4.12 Spoof Classification Rate

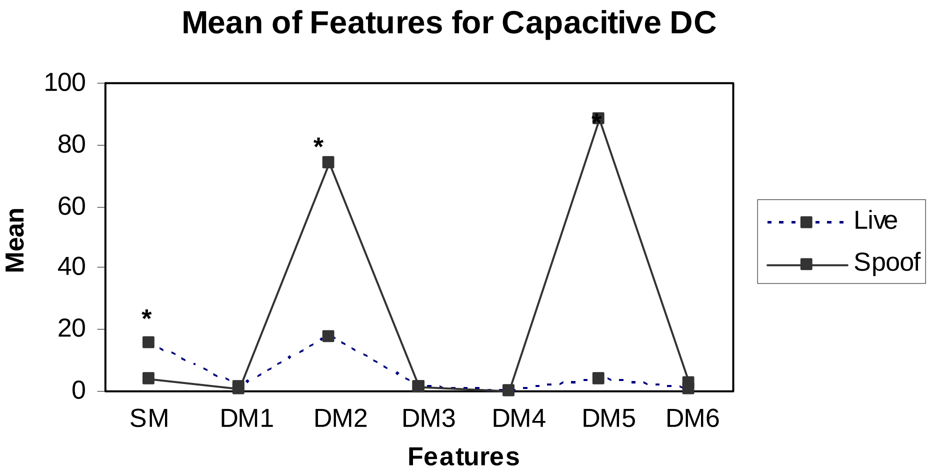
Scanners	Discriminant analysis results using all variables	Discriminant analysis results using important variables
P2S	94.7%	94.7%
P5S	89.4%	89.4%
E2S	95.2%	95.2%
E5S	100%	100%
S2S	95.4%	100%
S5S	95.4%	100%

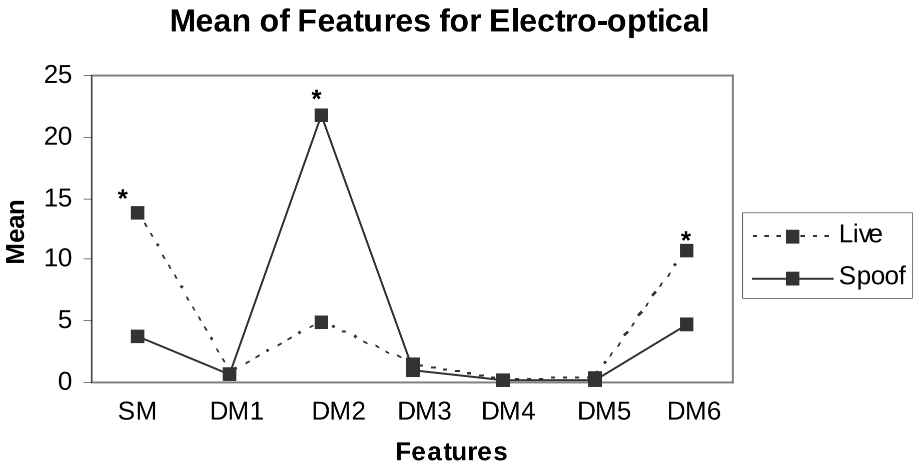
For capacitive DC device when variables chosen by stepwise were used for discriminant analysis, the classification rate for live fingers decreased slightly from 86.667% to 80% for 2 sec window and increased from 93.33% to 100% for 5 sec window. For the electro-optical device, classification rate for live fingers remained same for 2 sec and 5 sec window for both sets of variables. For optical device when variables selected by stepwise were used for discriminant analysis, classification rate for live fingers remained same for 2 sec window but for 5 sec window decreased slightly from 80% to 73.33%.

During the application of stepwise variables the classification rate for spoof fingerprints remained same for each device and time window except for optical device. For the optical device, classification rate for spoof fingers increased from 95.45% to 100% for both 2 sec and 5 sec time windows. Over all about 90% accuracy was achieved. It is expected that with more images, improved classification results can be accomplished

4.8 Statistical Analysis

Additionally, statistical analysis was also performed for understanding the importance of existing measures. Following figures (4.3) show the mean of each feature for live and spoof (which includes both cadaver and Play-doh fingerprint images) for each device.





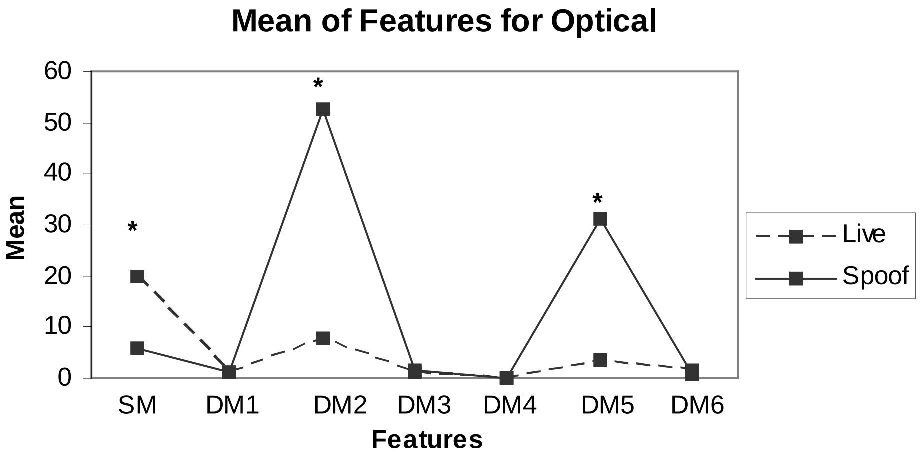


Figure 4.3 Plot of mean of features for capacitive DC, electro-optical and optical.

For some features the mean appears graphically different between groups. Further exploratory statistical analysis was performed which showed that the means were statistically different (p<0.01) for DM2 and DM5 for capacitive DC, SM, DM2, and DM6 for electro-optical, and SM, DM2 and DM5 for optical (as indicated by a *). The statistical analysis showed different features having relevance for difference devices.

5. Classification-II

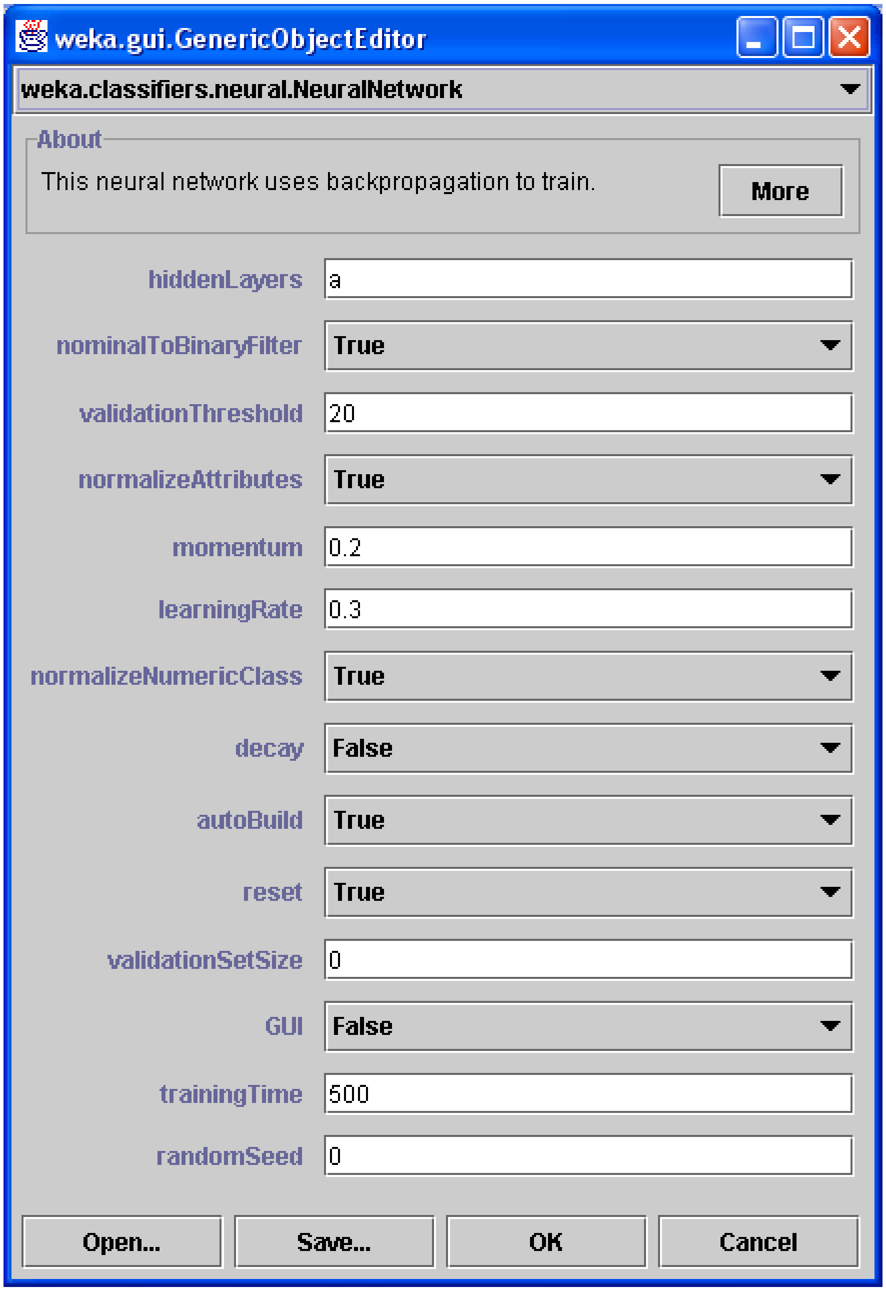
As mentioned earlier, classification of the images performed using different classification methods. Three classification methods were used: neural networks, discriminant analysis, and One R. Discriminant analysis and its results are explained in the previous chapter. This chapter briefly explains other two classification methods, its results and presents the comparison of the classification results of all the three methods. One R and neural network classification was performed using a software tool called WEKA (Waikato Environment for Knowledge Analysis)

5.1 WEKA

WEKA (Waikato Environment for Knowledge Analysis) is a freely available software tool on the internet developed at the University of Waikato in New Zealand. This system is java based and can be used on different computer platforms [30]. It can be used for various purposes like classification, regression, pre-processing, visualization, clustering etc. It provides different classification techniques for large data sets. WEKA concentrates mainly on classifiers and filter algorithms. An input data should be in ARFF format or CSV format and saved in data folder of Weka. The data must have a proper declaration of variables and class. Once the file is in required format, it can be fed to Weka for processing. Weka can also be used for implementing our own programs.

5.2 Neural Network

Neural Networks are used for regression, pattern recognition and classification. They have many applications like image recognition, industrial robotics, aeronautics, data mining and medical imaging. Neural networks consist of interconnected processing elements called neurons. These neurons respond in parallel to the given set of inputs. It is an adaptable system in which, given the set of inputs and related desired outputs, then the network determines the input-output relationship and builds a model with minimum error. Output is determined by the organizations and weights of these connections. Training algorithms use the gradient of the performance function for arrangement of weights. This gradient is determined by back propagation, a technique to perform backward calculations through the network. For neural network classification, a back propagation algorithm (with momentum 0.2) was used to train the data set with the hidden layer of 4 nodes derived from (attributes + groups)/2) (where there are seven attributes and two groups). Other default specifications include momentum of 0.2, a learning rate of 0.3, nominal to binary filter, and validation threshold of 20 and are shown in the following figure.

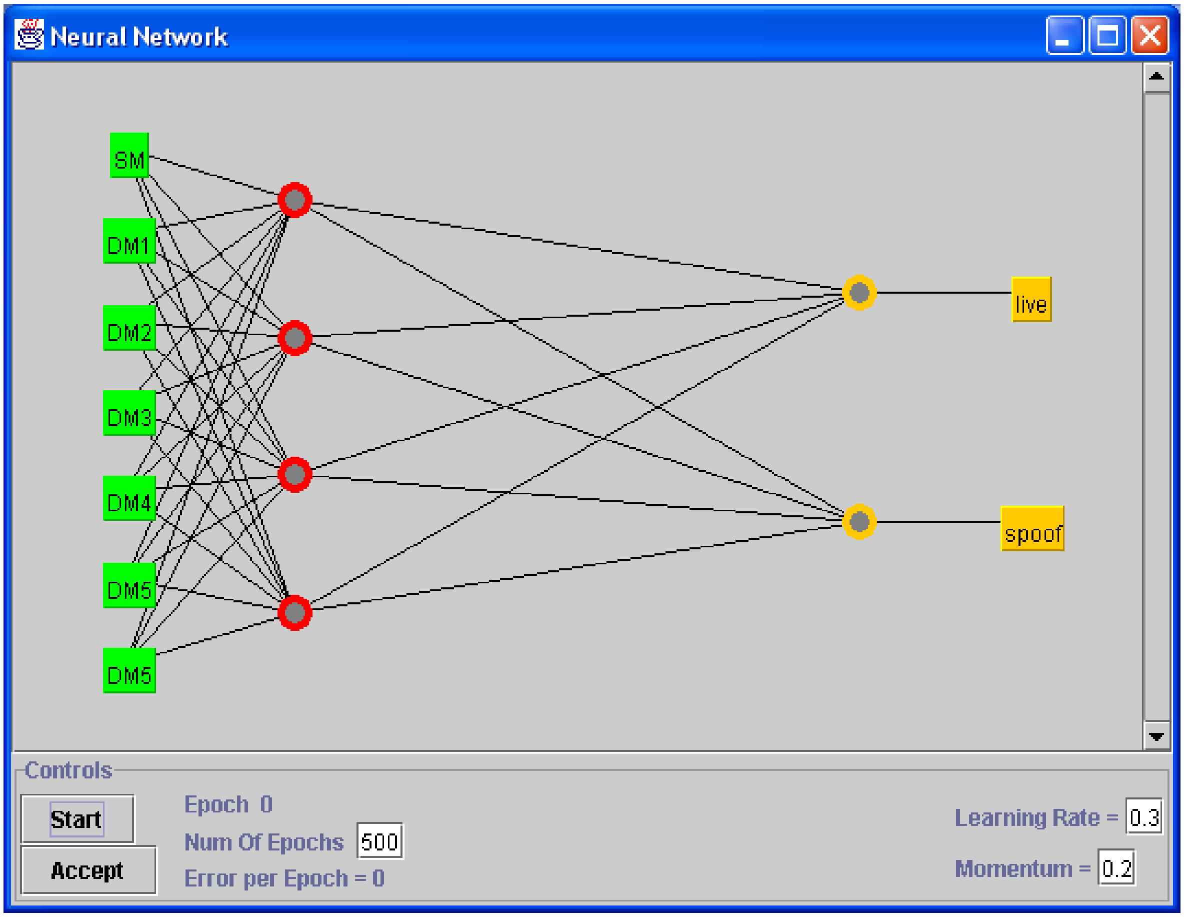


weka.classifiers.neural.NeuralNetwork

About

This neural network uses backpropagation to train.

hiddenLayers	a
nominalToBinaryFilter	True
validationThreshold	20
normalizeAttributes	True
momentum	0.2
learningRate	0.3
normalizeNumericClass	True
decay	False
autoBuild	True
reset	True
validationSetSize	0
GUI	False
trainingTime	500
randomSeed	0



Epoch 0

Num Of Epochs 500

Error per Epoch = 0

Learning Rate = 0.3

Momentum = 0.2

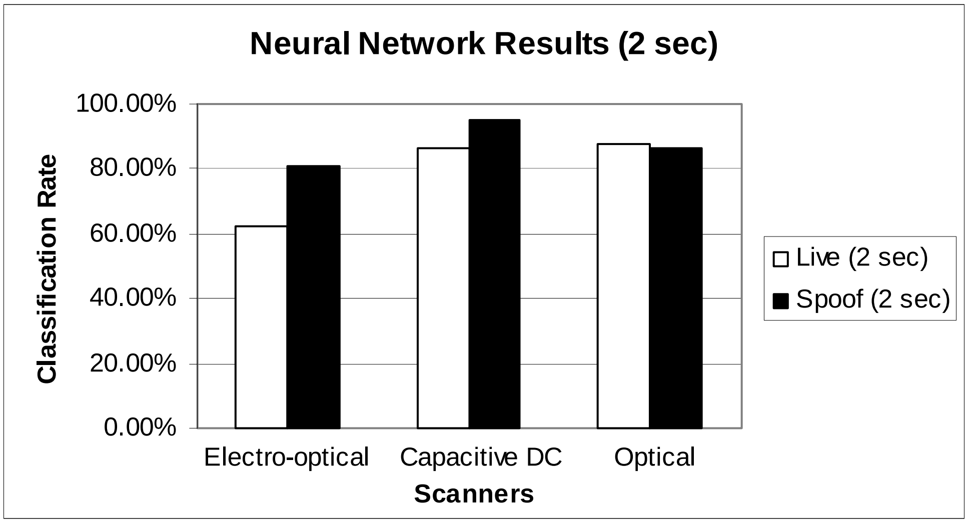


Fig 5.1: Neural Network results for all scanners for 2 sec time window

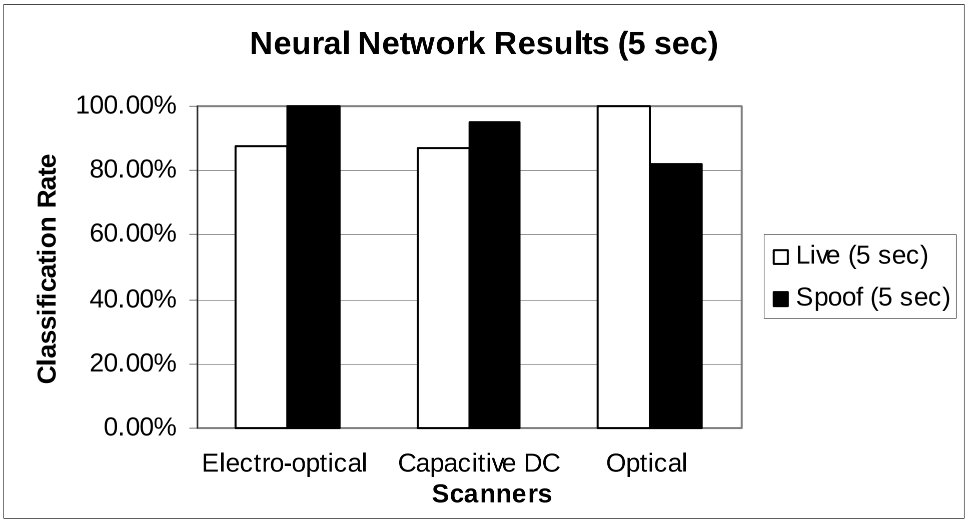
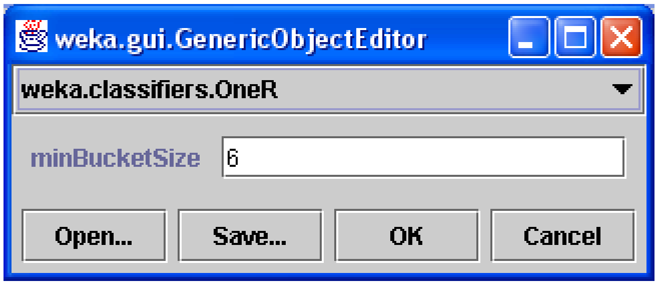


Fig 5.2: Neural Network results for all scanners for 5 sec time window

Figs. 5.1 and 5.2 present the neural network classification rate for live and spoof fingerprints for each device and time window. For the electro-optical device from 2 sec to 5 sec window, classification rate of live increased from 62.5% to 87.5%, classification rate of spoof increased from 81% to 100%. For the capacitive DC device, there is no change in classification rates of live and spoof with respect to both time windows. The classification rate of live and spoof remained 86.7% and 95% for both time windows respectively. For optical device, from 2sec to 5 sec window, classification rate of live increased from 87.5%-100% and classification rate of spoof decreased little bit from 86.40% to 81.80%.

5.3 One R

One R is the most simple classification tree method. It uses 'one-rule' to form a single level decision tree [31]. The rule tests each variable and different threshold. It enumerates how frequently each class appears for each value of the variable. Then it determines the most frequent class, creates the rule, and assigns a class for that particular value of variable. Likewise, it forms different rules for different variable values and computes the error rate for each rule on the training data. Finally it selects the rule with the smallest error rate to classify the groups. For One R, a minimum bucket size has to be specified. A bucket is 'a minimum number of instances in an interval'. In order to avoid the trouble of overfitting the minimal size of bucket, One R classifier with minimum bucket size of 6 (default) was used in our case. One R chose the static measure to form a rule for all scanners.



weka.classifiers.OneR

minBucketSize 6

The following table shows the threshold values of static measure used for live and spoof classification of different scanners and different time windows.

Scanners	2 sec	5 sec
Ethentica	SM < 7.27 spoof SM ≥ 7.27 live	SM < 7.72 spoof SM ≥ 7.72 live
Precise	SM < 6.28 spoof SM ≥ 6.28 live	SM < 7.75 spoof SM ≥ 7.75 live
Secugen	SM < 11.98 spoof SM ≥ 11.98 live	SM < 9.35 spoof SM ≥ 9.35 live

Table 5.1

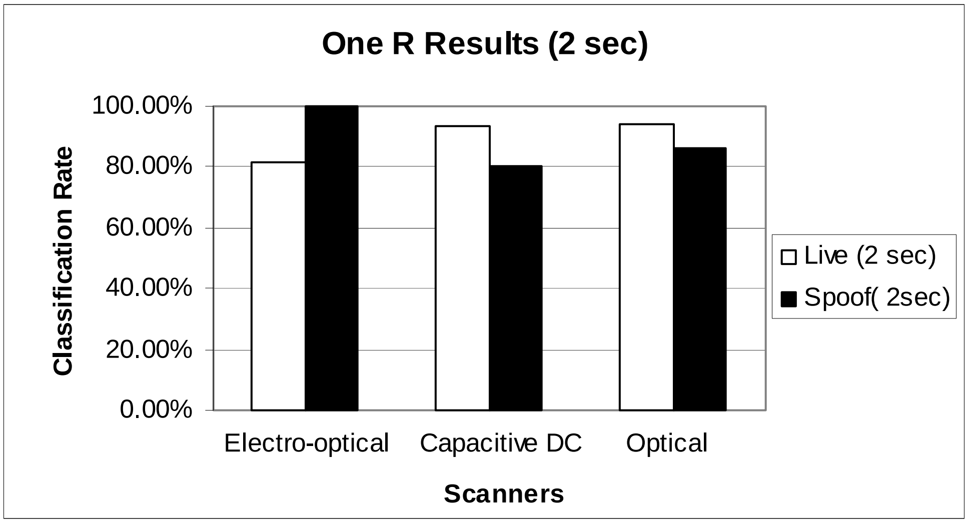


Fig 5.3: One R results for all scanners for 2 sec time window

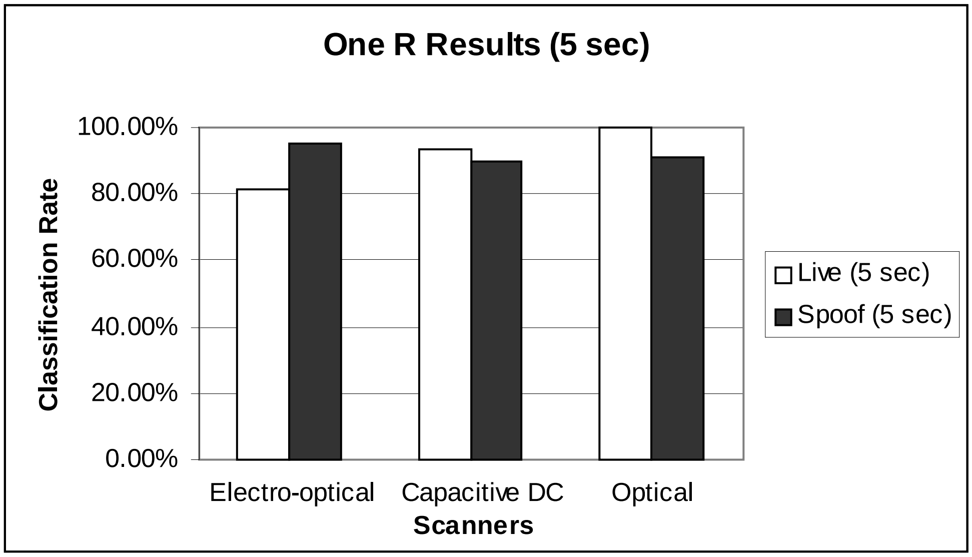


Fig 5.4: One R results for all scanners for 5 sec time window

Figs. 5.3 and 5.4 present One R classification rate for live and spoof fingerprints for each device and time window. For the electro-optical device, from 2 sec to 5 sec window, the classification rate of live remained the same 81.3%, and the classification rate of spoof decreased from 100% to 95.20%. For the capacitive DC device, classification rate of live remained same 93.30% for both time windows but classification rate of spoof increased from 80% to 90%. For the optical device from 2 sec to 5 sec window, the classification rate of live increased from 93.80% to 100%, and the classification rate of spoof increased from 86.40 to 90.90%.

5.4 Classification Summary

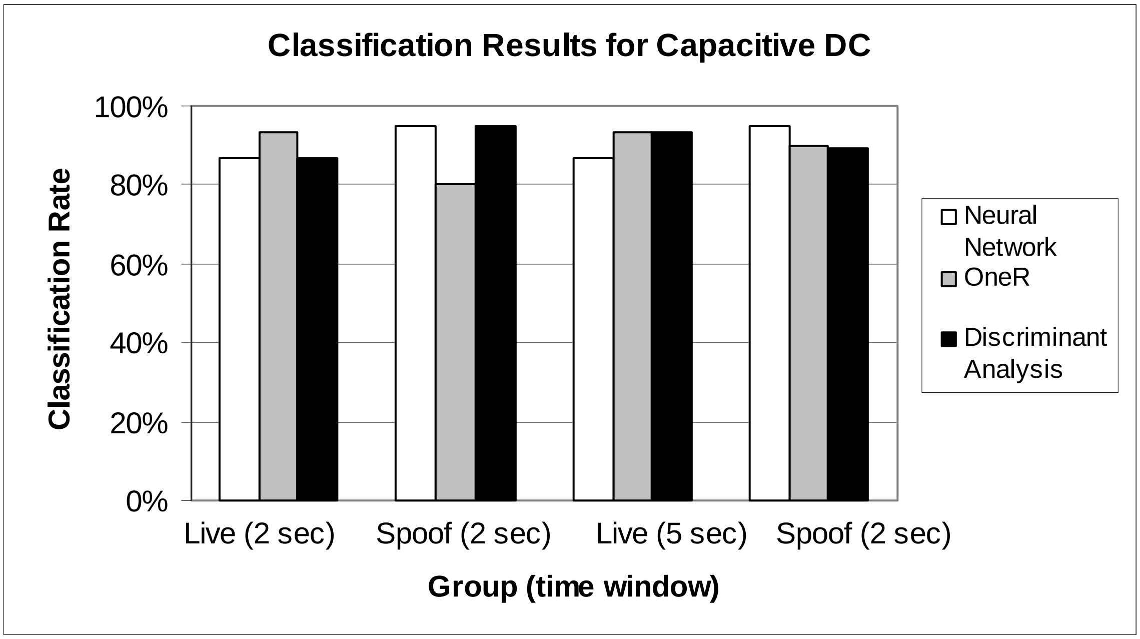


Figure 5.5: Classification results for capacitive DC using all three classification methods

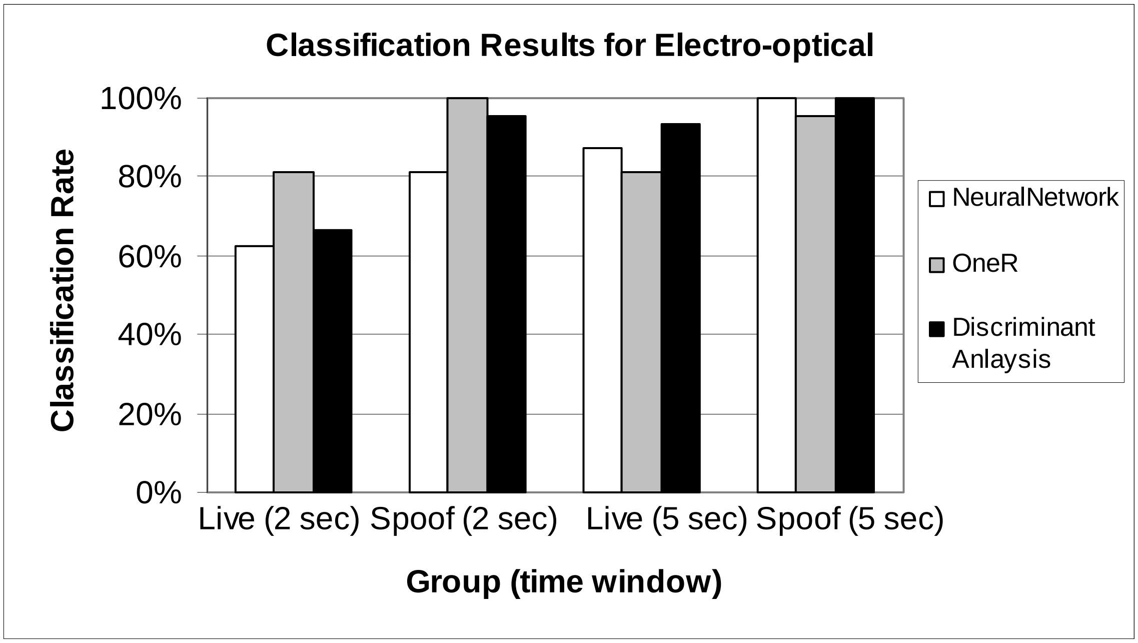


Figure 5.6 Classification results for electro-optical using all three classification methods

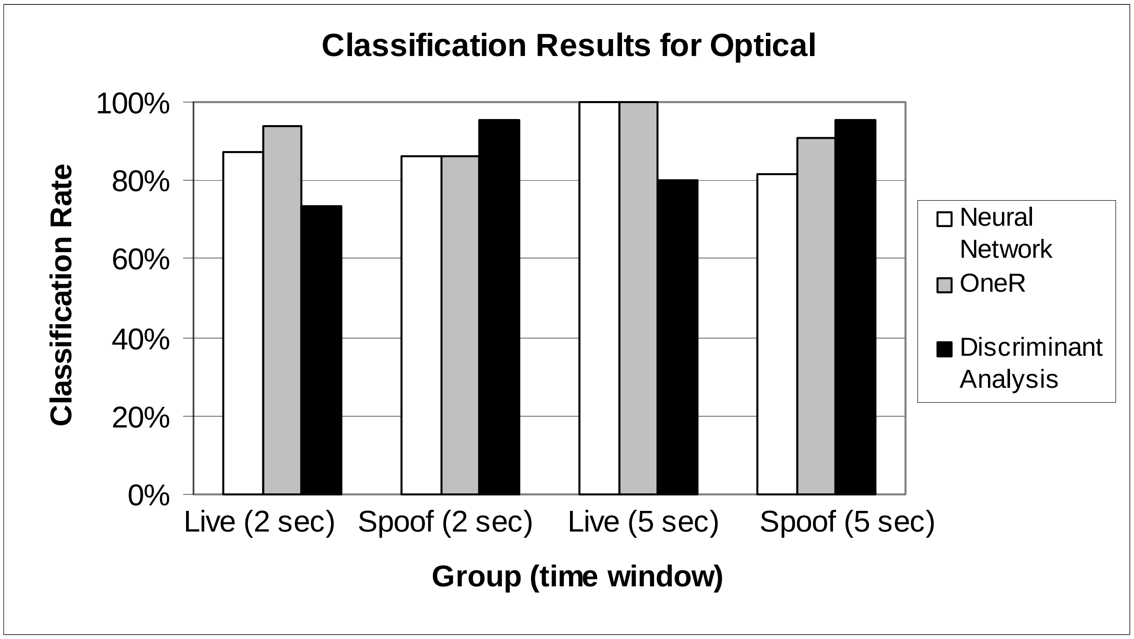


Figure 5.7 Classification results for optical using all three classification methods

Figures 5.5, 5.6 and 5.7 present the comparison of the classification results of the three methods for each device and time window. The capacitive DC device demonstrates between 86.67% to 93.3% classification for live fingers and 80 to 95% for spoof fingers, depending on the method and time window. There is little difference in the results for two seconds as compared to five seconds. For the electro-optical device, 62.5 to 93.3% classification is achieved for live and 81 to 100% for spoof. There is a modest improvement in live classification from two to five seconds (62.5-81.3% to 81.3-93.3%), with a smaller increase in spoof classification (81-100% to 95.2-100%). For optical, classification ranged from 73.3-100% for live and 85.7-95.4% for spoof with a small change for live classification from two to five seconds (73.3. -93.8. % to 80. -100%).

6. Conclusion

6.1 Discussion and Future Work

Increasing security at the sensor would definitely force hackers to find another weak point. Any material or data used to spoof biometric device may have non-live characteristics, but so long as it can replace the feature set which is responsible for liveness, the system is vulnerable. Although liveness detection in biometric devices is not entirely foolproof but it will make devices more secure, reliable and effective. For fingerprint recognition, several liveness methods including temperature, pulse, pulse oximetry, and electrocardiogram have been suggested [2], [7]-[12]. The difficulty with these measurements is that they require hardware in addition to the fingerprint scanner to capture these liveness features. This is expensive, bulky, and the liveness technique may be spoofed with a live finger presented in combination with a spoof. Furthermore, proposed liveness methods have not been rigorously tested and evaluated with relation to impact on statistical measurements like false reject and false accept ratios, user acceptance, universality, and collectability.

The research presented here suggests a new method, which detects the perspiration process through a time-series of fingerprint images measured directly from the scanner itself. The classifiers achieved approximately 90% classification rate for all scanners, with reduced time window and more comprehensive training and test sets. Using image processing and pattern recognition, fingerprint images captured from live fingers can be separated from those captured from spoof or dismembered fingers. This method relies solely on the underlying fingerprint scanner with the addition of software-based image processing and pattern recognition to make the liveness decision. This method is more difficult to spoof, since the spoof would have to replicate perspiration emanating from the pores and spreading across the ridges. Through this thesis and other published work, this method is being evaluated in terms of statistical performance and other biometric characteristics for its appropriateness to be used widely in combination with fingerprint authentication.

The initial version of the algorithm was performed for a DC capacitance scanner with a five second window for eighteen subjects (ages 20-45) [4]. This study expands this research to consider (1) a variety of technologies, (2) a large, more diverse dataset, and (3) a shorter time window. First, results demonstrate that using standard classification tools, algorithms can be created to separate live and spoof/cadaver fingerprint images for optical and electro-optical technologies, in addition to DC capacitance. Second, in collection of the dataset, a variety of age groups (11 people between ages 20-30 years, 9 people between 30-40, 7 people between 40-50, and 6 people greater than 50), ethnicities (Asian-Indian, Caucasian), and approximately equal numbers of men and women were chosen. While in this small dataset, it is impossible to consider these groups separately, the dataset presents a diverse set of fingers and therefore begins to consider potential problems (dry finger, saturated finger, ridge variations, etc.). Even with this diversity, we were able to achieve approximately 90% classification considering standard pattern recognition algorithms and a common set of features. Third, the original algorithm utilized a five-second-time window to show feasibility of the concept. The latest results demonstrate that a shorter time window of two seconds achieves similar classification results. It is also noted that the emergence from the data of device dependent feature sets are potential avenue for further improvement in this vitality based countermeasure to fingerprint system spoofing.

The classification performed here used a standard set of seven features and standard classification routines: neural networks, One R (selection of the best single measure and threshold), and discriminant analysis. Training was performed with images from 15 live subjects and 23 spoof samples. Training was separate for each device and time window. A device-independent algorithm was not developed due to the large differences in the measurements across devices, which is shown by the statistical analysis of different features having relevance for difference devices. Between the statistical analysis and classification results, a device-specific approach would most likely be the most successful for classification. That is, different measures have varying effectiveness for different technologies.

The future direction of this research will be (i) to further explore the features and determine the correlation between existing features (ii) to attempt to develop new additional features using multi resolution analysis, image processing and wavelet based methods for improving the classification rate (iii) to develop new spoof techniques using base materials like wax, moldable silica, wheat floor and to apply them for verifying the robustness of algorithm to variety of spoof cases (iv) to apply different classification techniques like decision trees, regression analysis for analyzing the importance of existing and newly extracted features and determining the best subset of features for classification.

While this study begins to address some of the limitations of the original work, more data is needed for further verify that this phenomenon is applicable across the population. Potentially, subjects having dry and overly moist fingers may receive a false rejection. Environmental testing will be necessary to demonstrate applicability to a wide variety of settings. While reasonable classification is achieved for a variety of devices using a common set of features, it is necessary to consider each device separately to expand and fine-tune the features and algorithms for each device. This could potentially improve classification performance. Also, features are averaged across the entire fingerprint image. Targeting areas of the image that are changing due to perspiration may improve the separation of live and spoof measurement. Lastly, in this method the fingerprint image is converted to a ridge signal. While effective in pinpointing the parts of the image which are most effected by perspiration, image processing techniques may provide enhanced features, particularly considering the entire area around the pores, and therefore improving classification.

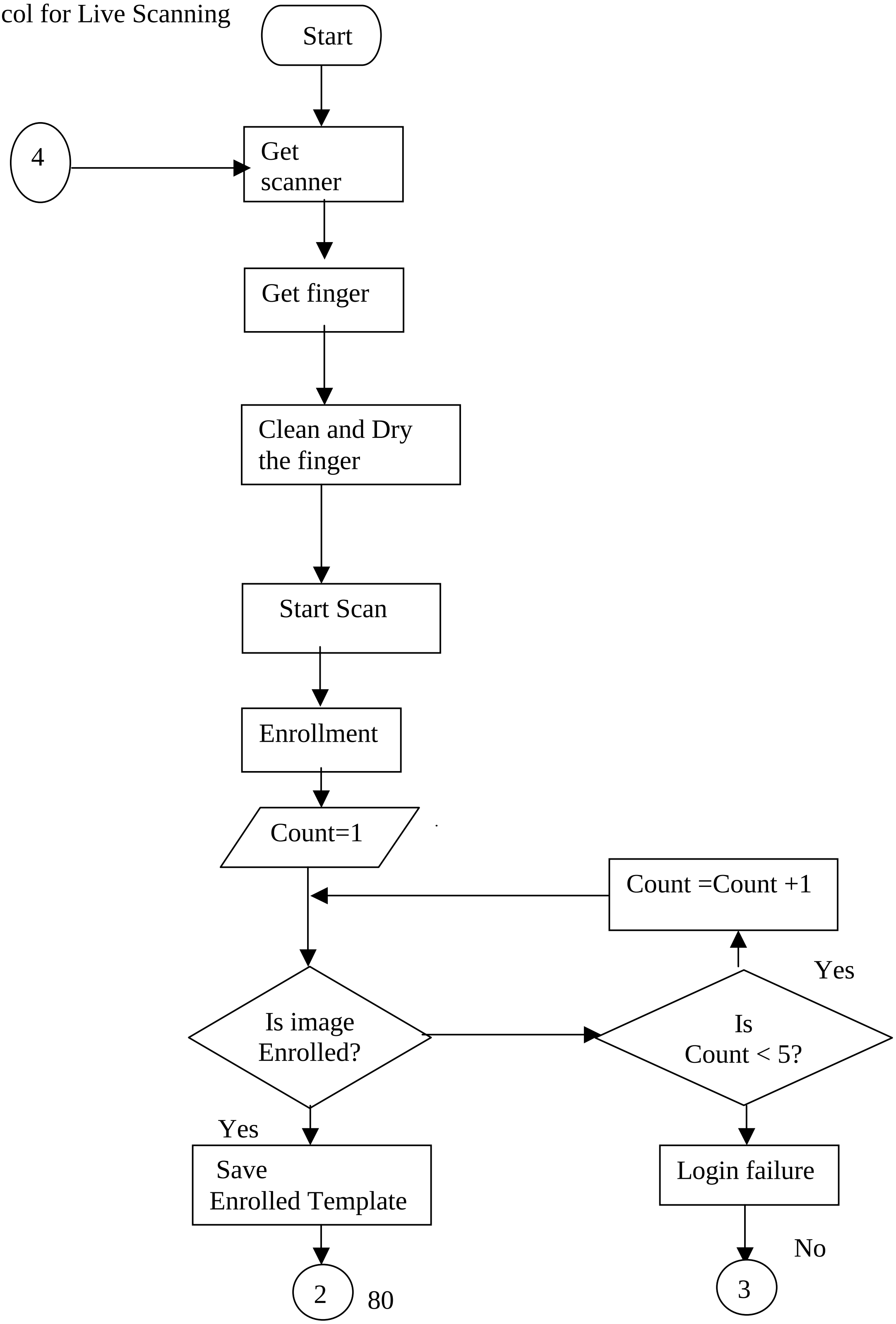
6.2 Conclusion

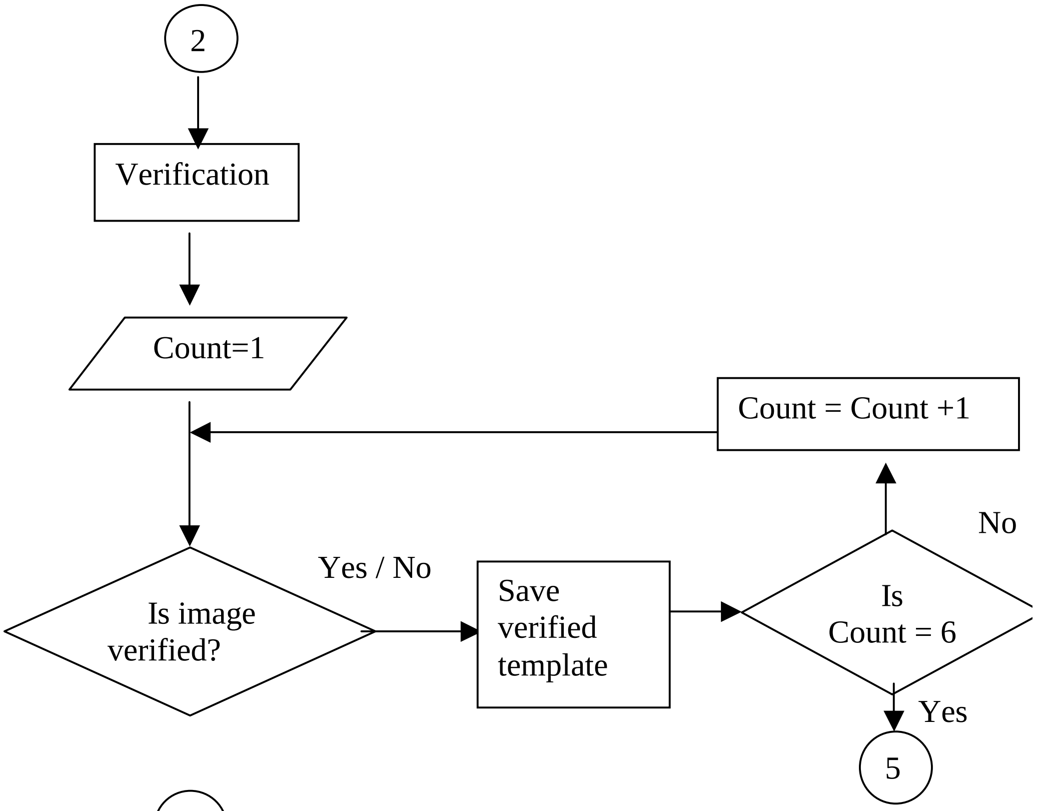
This research describes spoofing results of different scanners, data collection procedure, design and implementation of data collection protocols, a unique method to determine liveness through measurement of perspiration process in the finger and application of different classification techniques and their results. The perspiration based liveness method is totally software based and no additional hardware is required. Results are presented which improve upon past reports by decreasing the time needed to make the decision and demonstrating its applicability to a variety of fingerprint sensor technologies. A diverse subject population was tested and ~90% classification rate for all scanners was achieved. Application of this liveness method can increase the difficulty of spoof attacks for fingerprint scanners.

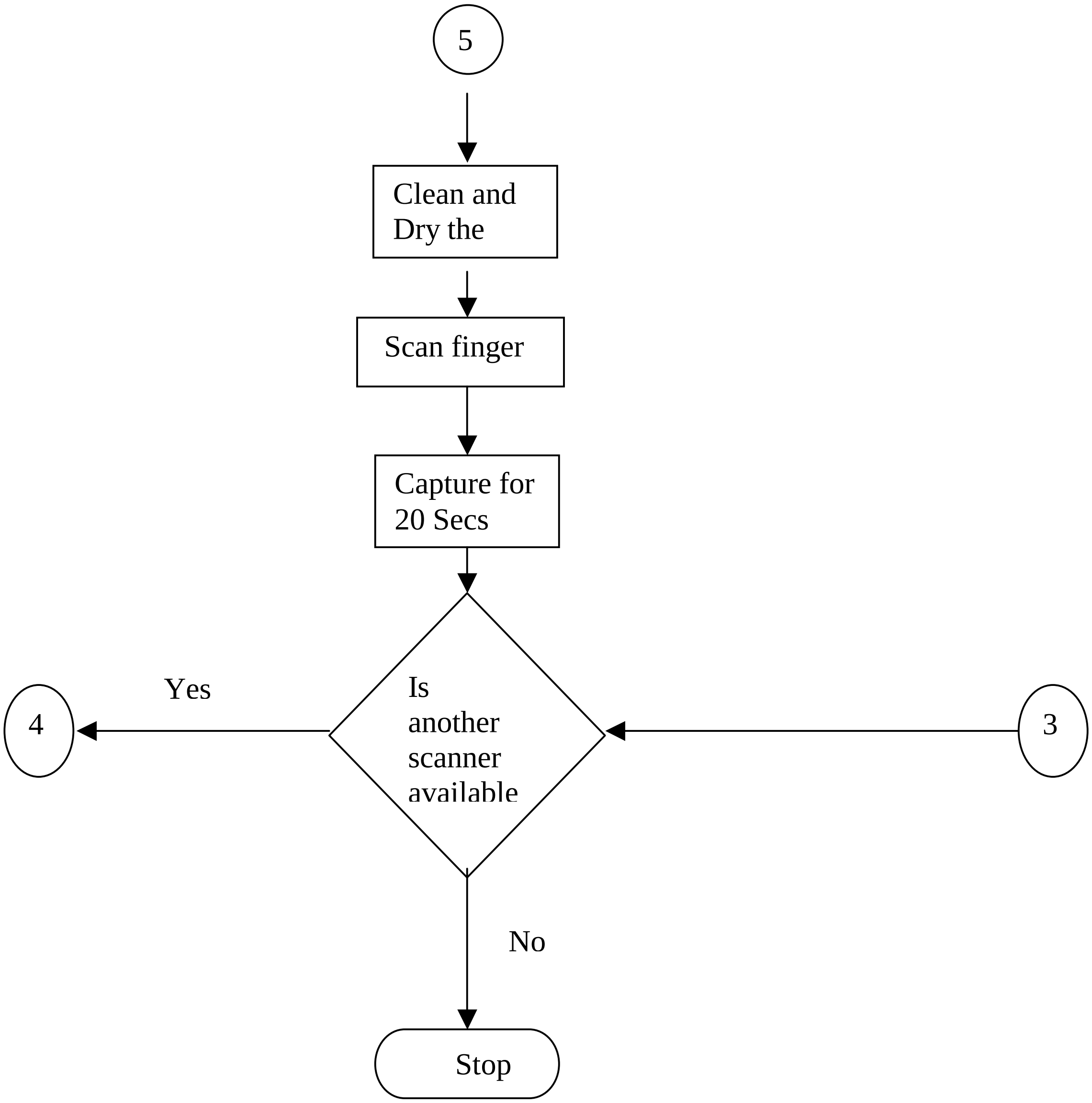
Appendix

Protocols: Following are the protocols designed for live collection, Spoof Collection and Cadaver Collection respectively.

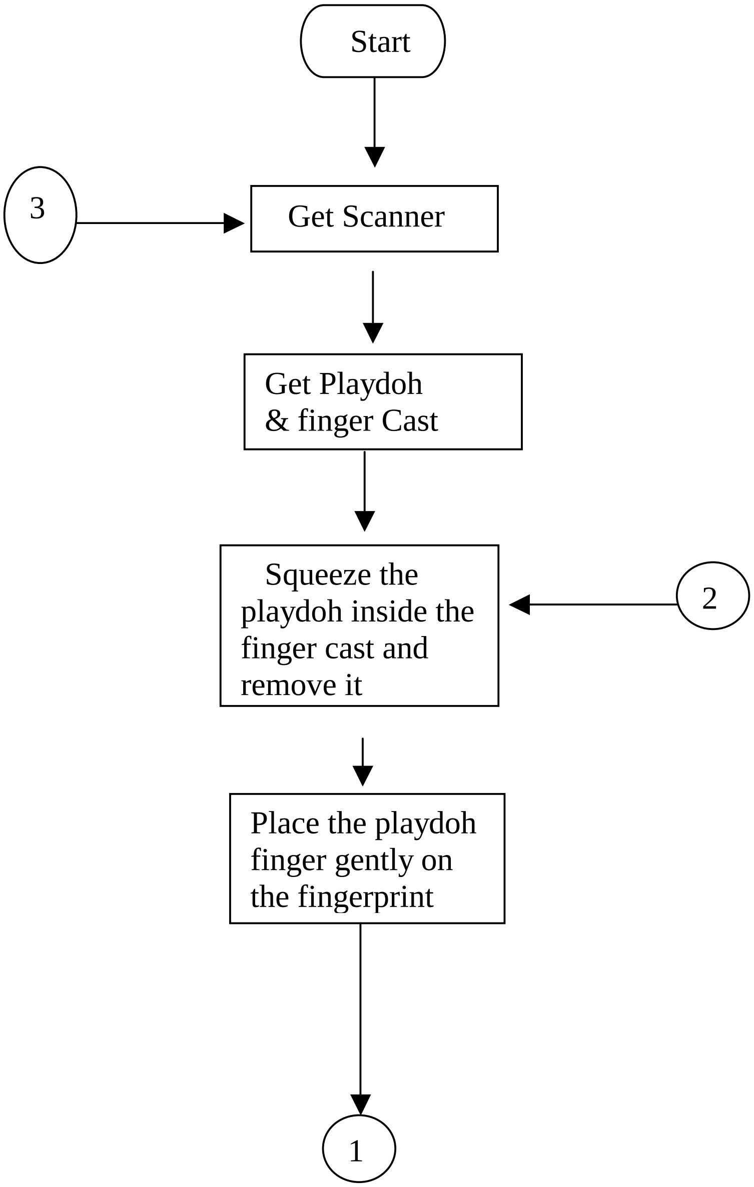
1.1 Protocol for Live Scanning

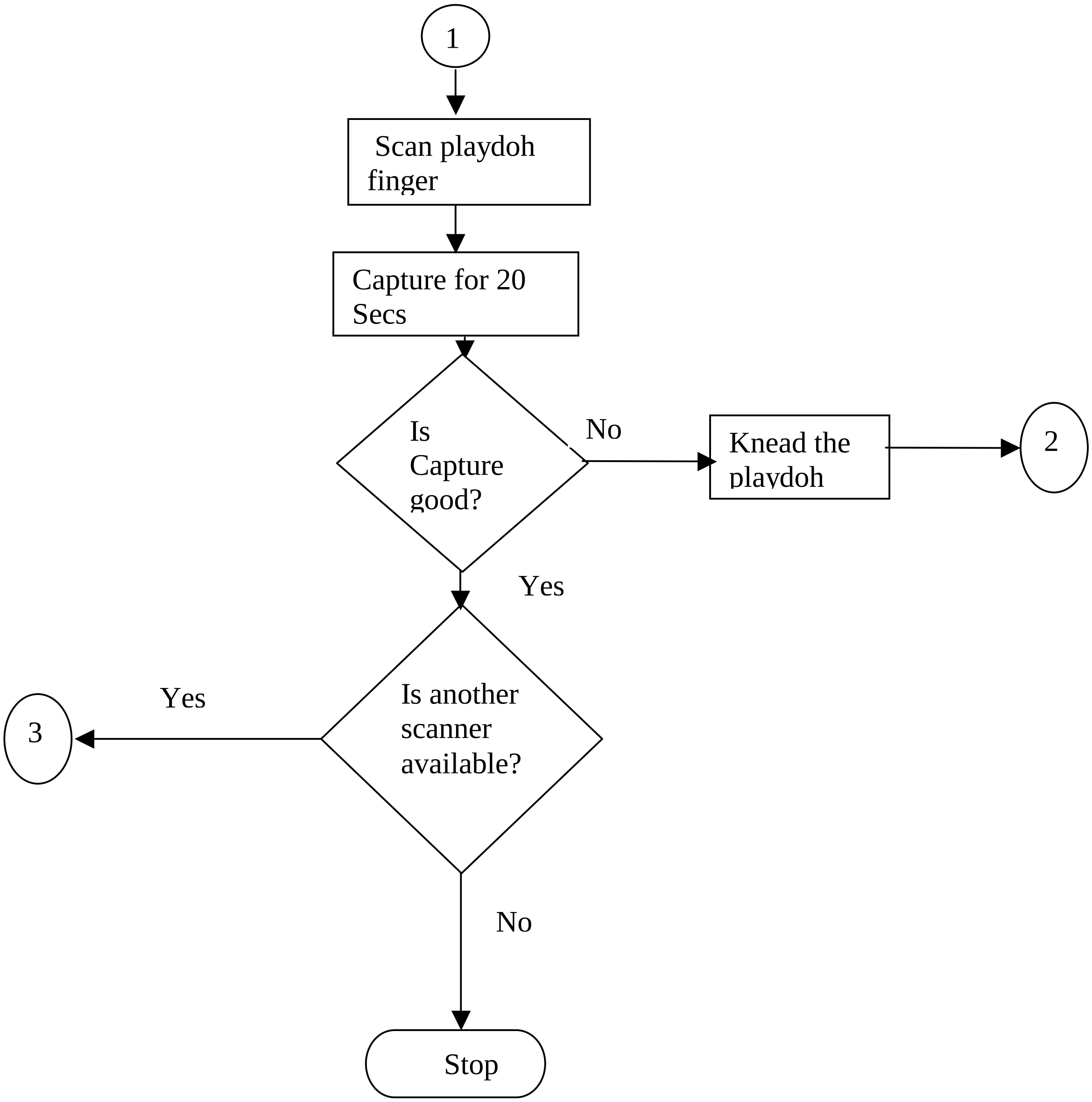



2
Verification
Count=1
Count = Count +1
No
Yes / No
Is image verified?
Save verified template
Is Count = 6
Yes
5

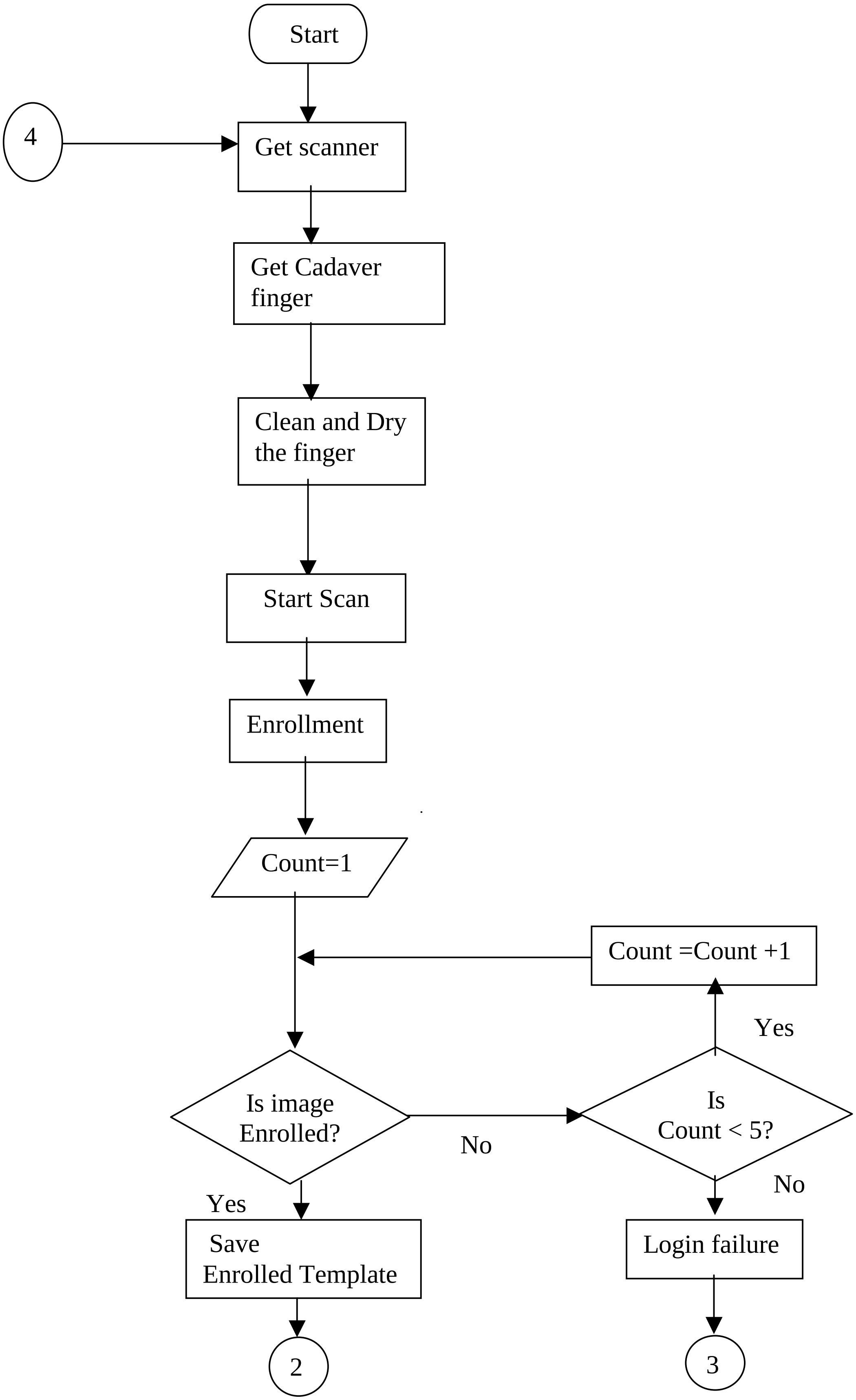

5
Clean and Dry the
Scan finger
Capture for 20 Secs
Yes
4
Is another scanner available
3
No
Stop

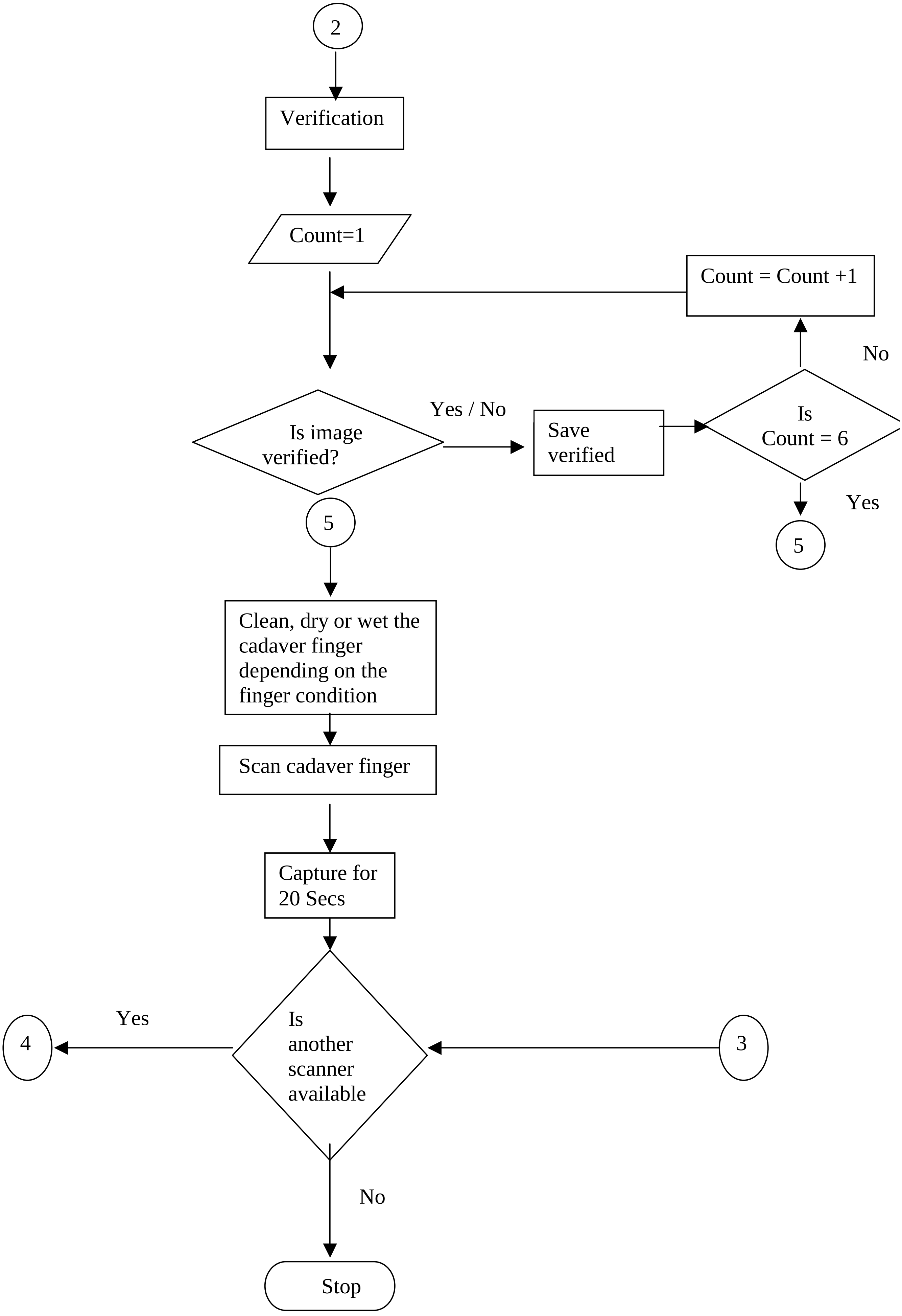
1.2 Protocol for Spoof Capture


Start
3
Get Scanner
Get Playdoh & finger Cast
Squeeze the playdoh inside the finger cast and remove it
2
Place the playdoh finger gently on the fingerprint
1


1
Scan playdoh finger
Capture for 20 Secs
Is Capture good?
No
Knead the playdoh
2
Yes
Is another scanner available?
Yes
3
No
Stop

1.3 Protocol for Cadaver Capture




2
Verification
Count=1
Count = Count +1
No
Yes / No
Is image verified?
Save verified
Is Count = 6
Yes
5
5
Clean, dry or wet the cadaver finger depending on the finger condition
Scan cadaver finger
Capture for 20 Secs
Yes
4
Is another scanner available
3
No
Stop

References:

1. N. K. Ratha, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol.40, no. 3, pp. 614-634, 2001.

2. S. A. C. Schuckers, "Spoofing and anti-spoofing measures," *Information Security Technical Report*, Vol. 7, No. 4, pages 56 – 62, 2002.

3. R. Derakhshani, S. A. C. Schuckers, L. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners." *Pattern Recognition Journal*, Vol. 36, No.2, 2003.

4. T. van der Putte, and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, pp. 289-303, 2000.

5. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems", *Proceedings of SPIE*, vol. 4677, January, 2002.

6. L. Thalheim, and J. Krissler, "Body check: biometric access protection devices and their programs put to the test", *c't magazine*, November 2002.

7. D. Willis, and M. Lee, "Biometrics under our thumb", *Network Computing*, June 1, 1998.

8. D. Osten, H. M. Carim, M. R. Arneson, B. L. Blan, "Biometric, personal authentication system", Minnesota Mining and Manufacturing Company, U.S. Patent #5,719,950, February 17, 1998.

9. Kurt Seifried, "Biometrics - What You Need to Know," Security Portal 10 January 2001 (http://www.securityportal.com/closet/closet20010110.html).

10. P. D. Lapsley, J. A. Less, D. F. Pare, Jr., N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow", SmartTouch, LLC, U.S. Patent #5,737,439, April 7, 1998.

11. P. Kallo, I. Kiss, A. Podmaniczky, and J. Talosi, "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus", Dermo Corporation, Ltd. U.S. Patent #6,175,64, January 16,2001.

12. V. Valencia and C. Horn, "Biometric Liveness Testing," in *Biometrics*, J. D. Woodward, Jr., N. M. Orlans, R. T. Higgins, Ed., Osborne McGraw Hill, New York, to be published.

13. Liveness Detection in Biometric Systems, International Biometric Group white paper, Available at http://www.ibgweb.com/reports/public/reports/liveness.html.

14. http://www.cl.cam.ac.uk/~jgd1000/

15. http://developer.novell.com/research/appnotes/2001/july/01/a010701.pdf

16. http://www.heise.de/ct/english/02/11/114/

17. http://www.rofin.com.au/pr_bssfaq.html#voice

18. http://users.ece.gatech.edu/~xzhang/Publications/spie01_mmsv.pdf

19. http://www.biometritech.com/enews/112202a.htm

20. http://computer.howstuffworks.com/fingerprint-scanner.htm

21.http://www.precisebiometrics.com/data/content/DOCUMENTS/26082002_165017_6061769WhitePaper%20-BioMatch.pdf

22. www.authentec.com

23. www.secugen.com

24. http://www.securityfirstcorp.com/tactwhtpr.pdf

25. “Classification” by A.D. Gordon

26. “Discriminant Analysis” by William R. Klecka

27. R software, http://cran.r-project.org/mirrors.html

28. SAS Insititue Inc., SAS Campus Drive, North Carolina 27513.

29. W. R. Dhillon and M. Goldstein, *Multivariate Analysis Methods and Applications*, Wiley-Interscience, 1984.

30. WEKA software, The University of Waikato, http://www.cs.waikato.ac.nz/ml/weka

31. I. H. Witten and E. Frank, *Data Mining Practical Machine Learning Tools and Techniques with Java Implementations,* Morgan Kaufmann, 1999.