Multimodal Biometric Models for Improving the Productivity and Security of the Terminal Gates

Final Report

METRANS Project 11-19

July 2012

Principal Investigator: Xiaolong Wu

Associate Professor

Co-Principal Investigator: Burkhard Englert

Professor

California State University Long Beach

Department of Computer Engineering and Computer Science

1250 Bellflower Boulevard

Long Beach, CA 90840

Tel: (562) 985-5291

Fax: (562) 985-7823

Email: Xiaolong.Wu@csulb.edu

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, and California Department of Transportation in the interest of information exchange. The U.S. Government and California Department of Transportation assume no liability for the contents or use thereof. The contents do not necessarily reflect the official views or policies of the State of California or the Department of Transportation. This report does not constitute a standard, specification, or regulation.

Abstract

The purpose of this project is to study and analyze the existing biometric technology, and propose a multi-layer biometric security system for one of the largest ports on the west coast of the United States, the port of Los Angeles in California. The multi-layer biometric security system contains a new mechanism against impersonation attack based on voice recognition, which will be protecting the port from any outside, unauthorized breach mainly that could be caused by a breach from the transportation medium personals. The multi-layer biometric security system will also create redundancy path in case of one technology is down or misused. The proposed system will mainly work on verification mode; however in case of a breach, it will automatically switch mode to identification mode to try to find a match of identity in the wanted or terrorist databases collected by the different government agencies.

Contents

Disclosure

Project was funded in entirety under this contract to California Department of Transportation.

1 Introduction

The port of Los Angles is considered to be one of the largest and busiest ports on the west coast. This port is not only considered to be the premier gateway for international commerce, but also known for its ground breaking environmental initiative and educational facilities.

The port of Los Angeles covers about 7500 acres of land and water. It features 25 passengers and cargo terminals and facilities that handle sensitive shipments and cargo worth billions of dollars each year [1]. Its throughput was ranked the highest on the nation in 2010. Also, it is the third busiest port in the world, which handles 14.2 million 20-foot unit equivalent containers annually with a total value of about $295 billion [1]. In addition, 44% of U.S. imports enter into the country through the port.

Because of these reasons, the port of Los Angeles could be considered one of the initial terroristic targets that can greatly affect the United States economy. Indeed, a research work shows that with a dirty bomb explosion that causes a one-year shutdown of the port (because of possible radiation activity) could result in the loss of $252 billion, 25% reduction in the property values in the plume area, and 10% reduction in business activity[19, 20].

Given the high sensitivity to the safety, Los Angeles port is putting huge amount of efforts into the security guarantee mechanism. Every day the port of Los Angeles encounters thousands of trucks that are transporting cargo and shipping containers into and out of the port. Each truck is forced to stop at the entrance gate and to take the routine examination of unauthorized personal as well as dangerous or illegal cargo.

However, the current approach to this fine-grained and seemingly sufficient checking process has two major limits. First, very surprisingly, this critical security checking process until today is done by simply checking the truck driver's Identification card. This is extremely dangerous as anyone could easily forge a fake driver license. And even without having to produce a fake driver license, one can find someone look more or less similar to himself and use his driver license instead. On the other hand, if the police suspects a difference between the photo on the ID and the driver, one can easily explain and come up with relatively reasonable arguments because the photo on the ID could indeed be very different from the driver's current appearance, as that photo might be taken up to 8 years ago[18]. Thus the simple check by letting the police to compare the photo and the real person could be very difficult and error-prone. Given the simple checking process, it is very possible that the potential threats are overlooked and thus the port is exposed to dangers. In 2004, an explosion took place in Los Angeles Port just because of the carelessness of security inspection [21]. Although no personal was injured in the accident, it is enough to call for the attention to a stronger inspection mechanism in the port's security assurance.

Another obvious drawback of the inspection process is that it creates a bottle neck for the port drastically affecting the movement of cargo into and out of the port, thus in turn affecting its throughput. In a port as busy as the one in Los Angeles, even a stop sign could create dramatically huge traffic jam, not mentioning that the drivers need to interact with the police. Reports show that a negative correlation exists between the port's throughput and security level, that is, the higher the security level is, the more severe the throughput is negatively affected [22, 23].

Productivity at the port of Los Angeles and Long Beach (POLA/POLB) is of interest to numerous governmental agencies and communities throughout the Southern California Region, the state, and the national as whole. Relative to other port operations in North America, POLA/POLB demonstrate a higher level of productivity (~5000 TEUs/acre in 2006); however, when compared to the productivity of other leading ports around the world (Asian counterparts with more than 25,000 TEUs/acre in 2006), POLA/POLB generally perform at a significantly lower level of productivity. Meanwhile, to accommodate future projected growth in demand at POLA/POLB, POLA/POLB terminals will need to at least double their current productivity in terms of the efficient use of available space. Pure physical expansion is constrained by a limited supply of available land and escalating environmental concerns, especially for urban center ports such as POLA/POLB. For local and regional authorities, the expansion of port capacity on already developed urban land, or through the creation of newly reclaimed space, represents a costly and procedurally difficult choice. This leaves expanding port cargo handling capacity by improving the productivity of existing terminal facilities the only choice and the most immediately viable solution for terminal operators. Meeting these environmental and social expectations while improving productivity sufficiently to accommodate both existing and anticipated demand in container volume, however, presents a daunting challenge for terminal operators and port authorities, particularly within the port operating regimen as currently found in the US.

Generally, the container productivity measures are directly related to the movement rate of ship-to-shore operations or berth productivity, the turn-time for truck, and the movement rate of gate transactions or gate productivity. Berth productivity is determined by the crane productivity and the productivity of workers employed. The Turn-time for truck is largely controlled by the dwell time. Gate productivity, on the other hand, measures the movement rate of gate operations which is often determined by the number of gate lanes/booths; by an efficient arrangement of gate operations; by the type of gate transaction; and most importantly, by the technology or type of data processing system used in processing gate transactions. Considered the expensive and unpractical physical expansions and strict labor rules at both POLA/POLB Ports, it is virtually impossible to increase the usages of berths and cranes, to increase the moves per man-hour, to adapt the high-density stacking option instead of "on-wheel" storage configuration to further increase the productivity in ship-to-apron transfer, apron-to-storage, storage, and intermodal transfer areas for a container terminal. This brings the need to expand the terminal gate productivity within current physical facilities by introducing advanced information and processing technology to the forefront.

POLA/POLB implemented the appointment system in 2002 in response to California Assembly Bill (AB) 2650, which seeks to reduce truck queuing at the ports' terminal gates and associated vehicle emissions. However, Giuliano and O'Brien in pointed out that there is no evidence that the appointment system affect queuing at marine terminal gates; while a majority of the terminals did implement an appointment system in response to the legislation, most did so in order to avoid paying the high labor costs associated with extending operations to off-peak hours. Meanwhile, the new labor agreement that followed the 2002 shutdown allowed for use of certain technologies, which enhanced the efficiency of terminal operations just inside the gate. As pointed out by Booz Allen, biometrics-enabled intelligence has quickly become an accepted tool for solving immediate identity problems. They argue that "Biometric information exhibits an inherent reliability and can use it as the central criteria to establish identity, whether it is collected overtly or covertly". In particular, biometric data is used as a form of identity access management and access control using one or more intrinsic human physical traits, such as fingerprint, facial recognition, iris/retina, voice, etc.

In order to attack the above disadvantages of the current approach, this paper is proposing an intelligent multi-layer biometric security protocol with a new mechanism against impersonation attack based on voice recognition. By utilizing automatic approach and advanced biometric characteristic identification and analysis, a significant increase in the accuracy is expected because the captured characteristics are immutable and do not depend on the time passing by, or simple change in the appearance of the testees. At the same time, an automatic approach could significantly boost the inspection speed. With high performance image capturing utilities and analysis platforms, a non-stop approach could be finally deployed, and the movement in the port would not be blocked at all. Therefore the throughput of the port could be increased to its maximum.

2 History and Overview

After September 11, 2001, the US government authorities invested substantial amount of money on the port security, and the Los Angeles Port has spent $400 million on security upgrades, including a new command center with 300 high-tech cameras [23].

At the same time, research efforts to develop an extreme database that contains almost unlimited data from biometrics are also invested. These researches discovered new methods to identify individuals more accurately. These technologies are described one at the time in each subsection of section 3 indicating the advantages and disadvantages of each technology, leading the writer to choose the most suitable technology for the field of application. Section 4 will discuss the evaluation methodology for a given biometrics system and the different types of the performance measurements. Section 5 will discuss the proposed architecture, redundancy paths and the chosen technologies, working together to eliminate forgery and misuse. Finally section 6 will discuss four of the most important performance measurement, explaining how to yield exceptional performance measurements.

3 Available Biometric Technologies

3.1 Available Biometric Technologies

The fingerprint identification is mainly based on recognizing the location and the direction of the friction ridge print which for has proved for decades its uniqueness. The fingerprint is normally taken by a variety of sensors, such as capacitive, thermal, optical, and ultrasonic collecting a digital imagery of the fingerprint. The darker lines on the taken sample are the highs and the lighter lines indicate the valleys on the fingerprint. From the collected information a series of pattern recognition are performed to locate the friction ridge as figure1 shows below. Please note that there are two types of ridges: ridge ending and ridge bifurcation. The ridge ending is a split in the valleys and ridge bifurcation is a split in the highs.

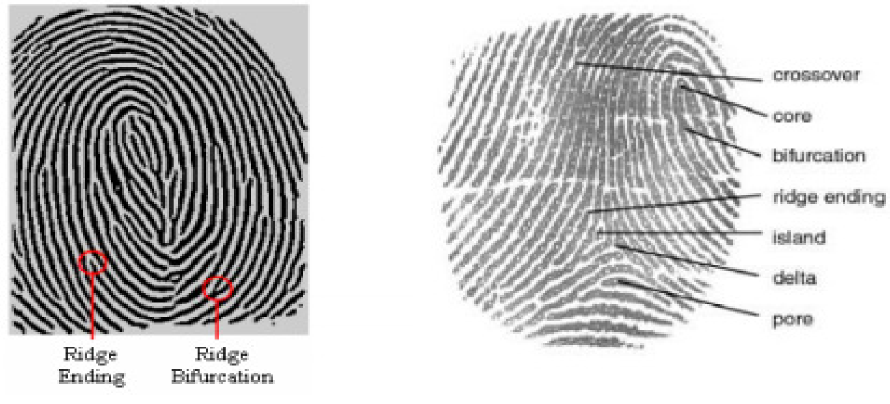

Figure1. Fingerprint Characteristics [2]

The major advantage of the finger print technology is: This technology has been proven for decades to be reliable, assuring uniqueness and most importantly there are enormous amount of data available from the different inter-governmental agencies. The only disadvantage to this technology is the hygienic practice, since the scanner is touched by thousands of people daily.

3.2 Palm Print Recognition

The palm print recognition uses the same theory behind the fingerprint identification and recognition. It is mainly based on recognizing the location and the direction of the friction ridge print, along with the recognition of the raised portion of the epidermis. In other words, it recognizes the skin textures (lows (valleys) and highs); refer to figure1 for better understanding and further reference, then searches and recognizes the friction ridges. The friction ridges have been proved for decades for their uniqueness. Just like the fingerprint technology, the palm print hardware and software requirements are the same. The palm imprint is normally taken by a variety of sensors, such as capacitive, thermal, optical, and ultrasonic, all collecting a digital imagery of the characteristics of the palm print as figure2 shows below.

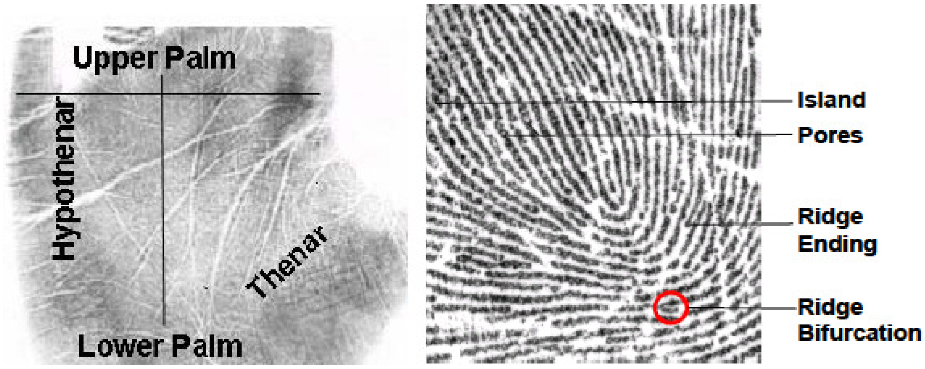

Figure2. Palm print Characteristics [3]

The major advantages of the palm print technology are: firstly, the fingerprint recognition could be a subset of the palm print recognition since no additional sensing devices are required. In other words, if the hardware of the palm prints sensing area is expanded large enough to capture the characteristics of the fingers it will work with the existing sensing technology. The software will be slightly changed to captures, identify and finally classify the fingers not just the characteristics of the highs and lows of the imprint. Doing so, we will increase the security ten folds. Secondly, the palm print, imprints has been proven for decades for its uniqueness and reliability. Finally, just as the fingerprint recognition, the U.S. government has collected an enormous database shared by all the inter-governmental agencies holding the palm and the finger prints, which can be easily shared with and imported to the port of Los Angeles security office. The main disadvantage of the palm print technology is same as the fingerprint technology discussed in the previous section; it is considered non hygienic procedure.

3.3 Palm Geometry Recognition

The palm geometry recognition is one of the oldest ways implemented for biometrics; it was widely used since 1980. The theory behind this approach is done by measuring different hand measurements such as, fingers and palm length, fingers and palm width. It also measures fingers, thenar and hypothenar thickness and several combinations thereof. Finally it also computes the palm’s surface area. This is all done by simply placing the hand under a charge couple device camera, guided by five pegs. Then the camera captures the hand’s digital picture and computes the distances mentioned above from different angles as figure3 below indicates.

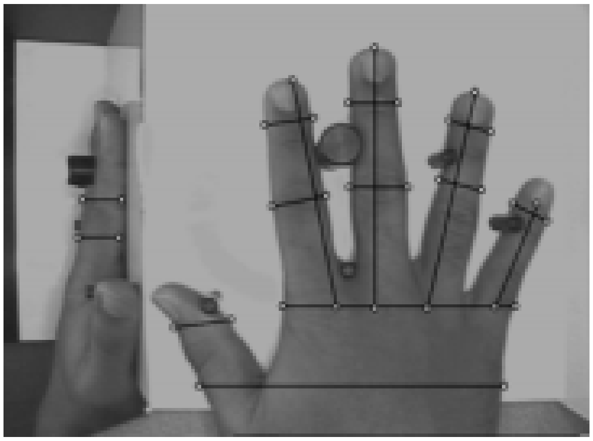

Figure3. Hand Geometry Characteristics [4]

The advantage in using such technology is: this technology is cost effective, and it is extremely easy to program or configure. However, the major disadvantage of this method is that it doesn’t assure uniqueness between individuals as one can imagine. Since the correlation factor between each component as well as the number of factors are low. For this reason this method is ultimate only for verification tasks that don’t require extensive security measures.

3.4 Dynamic Signature Recognition

The dynamic signature recognition is a modality that is used to recognize the person from his/her handwriting characterization. This method should not be confused with the digital signature that is used with most of the ATM machines and grocery stores. The digital signature recognition only matches the signature to a pixilated image. On the other hand, the dynamic signature uses various personalized factors that each human uses when he/she writes, such as, the velocity, acceleration, timing, pressure, and signature direction, then analyze them in the 3-dimentional space on the x,y,z coordinates, as figure4 shows below. Then the picture is digitized then quantized using digital signal processing techniques to measure the correlation factors between the original and one that is taken.

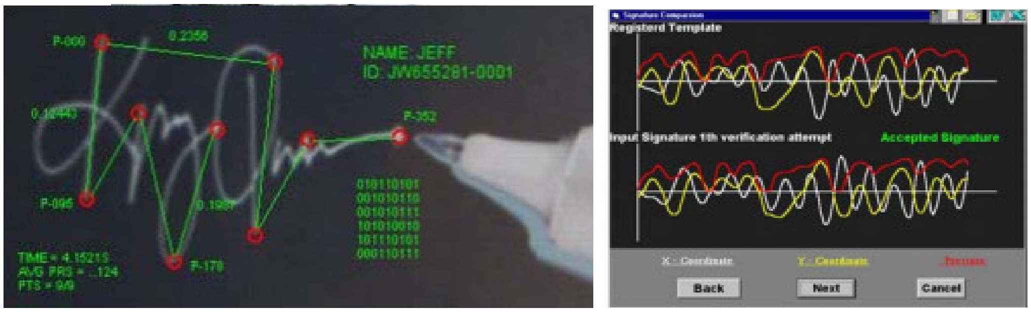

Figure4. Left-Dynamic Picture Characteristics, Right-DSP- outcome [5]

The software used for the recognition process has learning ability to change and adapt to human changes. This method has been proven to be very accurate and extremely secure. In fact, the features that this method is looking for is almost impossible to replicate, unlike the normal graphical image recognition which can be easily forged.

3.5 Vascular Pattern Recognition

The vascular pattern recognition is a newly developed modality that detects the human feature by simply tracing the location of the blood vessels. This is done by emitting near infra-red light through the hand and absorbing the outcome by a Charge Coupled Device Camera (CCD) constructing a digital imagery on the other side. Later, digital signal processing techniques will be used to identify the blood vessels. The Blood Vessels will be clearly identified by its darker colors among the normal tissues and muscles since the near infra red rays are absorbed by the hemoglobin in the blood, as picture5 shows below. Where later a recognition algorithm is run to find a match is the stored database.

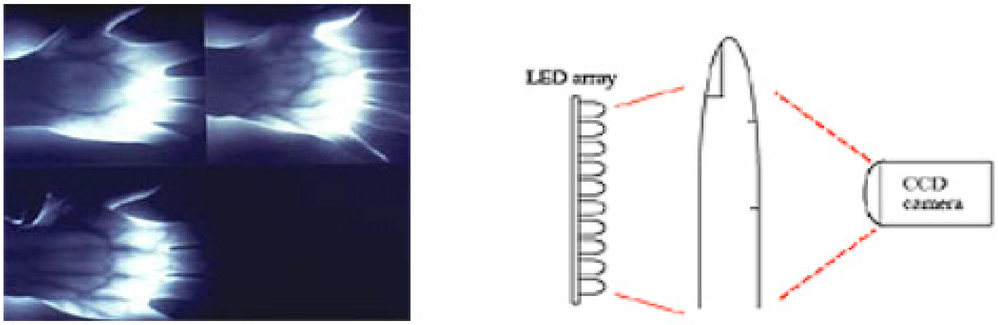

Figure5. Left - Vascular Patterns, Right- Tools needed [6]

The main advantages for using the vascular pattern recognition is that: Firstly it is impossible to forge. Secondly, it is hygienic since it doesn’t require any equipment touching. Thirdly, it is practical; it has been already in use for ATM and hospitals in Japan. The main disadvantages of using the vascular pattern recognition method are mainly because it is a new technology. Also, the U.S government agencies didn't completely adapt this method. Therefore, constructing the database for such technology will be costly.

3.6 Iris Recognition

The iris is the muscle within the eye that regulates the size of the pupil as figure6 shows below on the left hand side; it controls the amount of light that enters the eye [7]. It is the colored portion of the eye. It was discovered in 1936 that each iris contains a unique pattern associated to each person. This finding has imposed the importance of using the iris as one of the methods for recognition. As shown by the picture below on the right hand side, each iris contains a unique pattern to it which can be captured and analyzed.

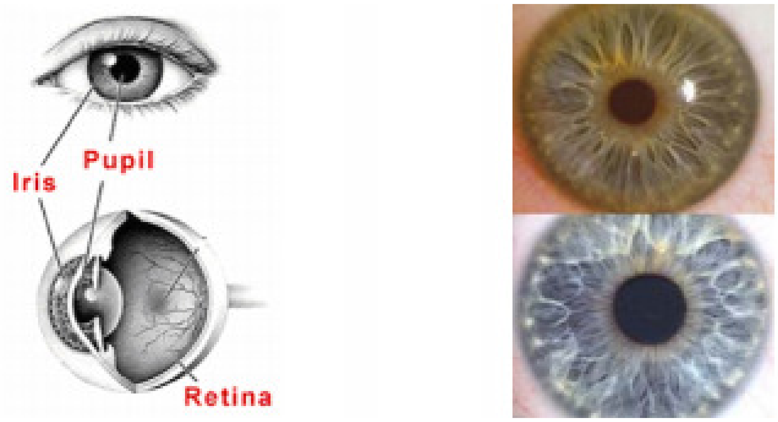

Figure6. Left – Eye structure, Right- Iris Patterns [7]

The iris scan is done by a high resolution digital camera, normally illuminated by an infrared light. The first step for the iris recognition is the feature isolation and extraction. At this step the localization of the iris is done removing all the noise in the system, such as the eye lids, the reflection, the eyelashes, and the pupils. Removing this noise will enhance and speeds up the recognition process drastically. The process isolation is normally done by several digital signal processing techniques for picture feature extraction. Then the iris is then outlined and the picture is encoded to the iris code format as the figure7 shows below.

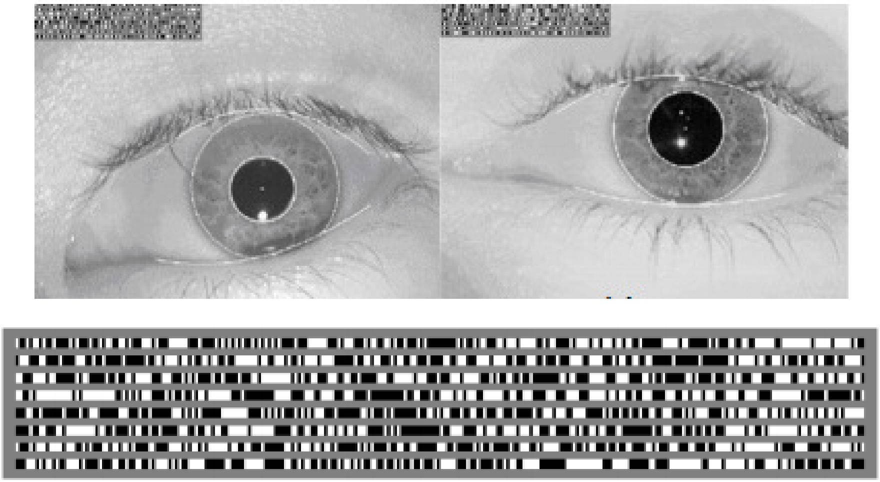

Figure7. Above – Retina Extraction, Below- Iris Code [7]

The iris code contains all the iris information about its pattern using 256 bytes of data in polar coordination format. The iris code then is compared against the templates using the Hamming Distance (HD) to measure the statistical distance, which in return resembles the dependence between the two codes.

The main advantages in using the iris recognition: First, it guarantees uniqueness between individuals as the fingerprint does. Secondly, it guarantees hygiene manners since it doesn't require any physical contact. Many may think that the iris scanners may harm the eye since the infrared light is shined on it; on the contrary, the infrared source doesn't have enough energy to destroy the photo cells in the eye. The only source of risk is the thermal side effect. However, this is unlikely due to the fact that it using only one diode for this operation. The main disadvantage in using the iris scan is that it has been in use only since 1994, which means that the government agencies haven't adapted this method as primary method for recognition. In other words, there will not be enough data to be shared between agencies and imported into the security office of the Port of Los Angeles.

3.7 Retina Recognition

The retina is a light-sensitive tissue lining the inner surface of the eye. The retina is composed of multiple layers of sensory tissues and millions of photoreceptors whose function to transform light rays into electrical impulse [9.] In other words, this is where the human eye creates the visual picture. At the back of the retina, there are retinal blood vessels, which supply blood to the eye as figure8 shows below.

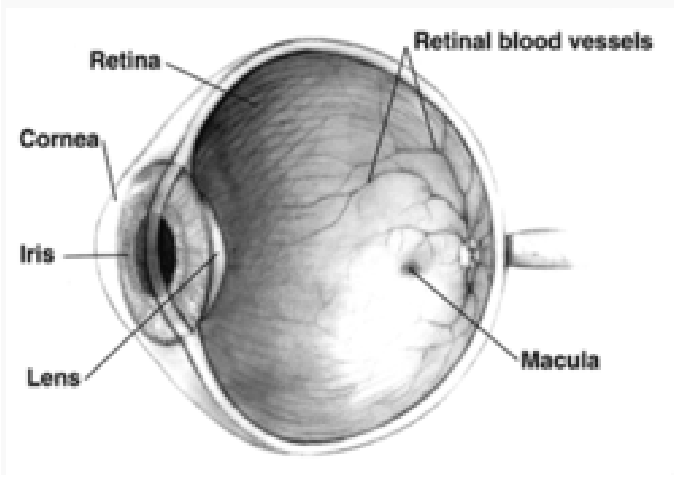

Figure8. Eye Anatomy [8]

The retina recognition technique is similar to the one of the vascular pattern recognition discussed in section 3.5 above; where an image of the eye is taken by a Charge Coupled Device camera lighten by a near infrared LED. Then the image is processed using Digital Signal Processing Techniques to extract the blood vessels from the picture and process it using recognition algorithms to find matches in the stored database.

The main advantages in using the retinal pattern recognition are: Firstly, that it guarantees uniqueness. There are several studies that confirmed the uniqueness of the blood vessel patterns found in the retina. The first research was published by Dr. Simon and Dr. Goldstein in 1935 and the second research was conducted by Dr Tower in 1950. Secondly, it is very difficult, in reality near impossible to forge. Therefore, it is considered to be one of the most secure biometric methods. The main disadvantage in using this technology that is it is fairly new, which means that there is not much data provided by the inter-governmental agencies. Many would argue that this method is not safe to use since it shines a near infrared light onto the eye. However, just as discussed in the iris scan technology, the infrared light doesn't have enough energy to cause any photochemical damage.

3.8 Face Recognition

The face recognition is one of the most commonly used methods by our brains for recognizing individuals. As a matter of fact, we know how a certain person looks by simply looking at his/her facial features, without any further subdues. Therefore, researches about the automatic face recognition were and still are highly encouraged by many field applications. The face recognition is one of the most complicated methods in the field of intelligence recognition due to the fact of its complicated structure and dependencies. The face recognition requires profound understanding of linear algebra, as well as thorough knowledge about the classification and clustering techniques. Every facial recognition technique is built based on two predominant approaches: geometric and photometric. The Geometric approach simply means it is based on the several distance calculations from the facial features. On the other hand, photometric approach simply means it is based on the view of the individual. Furthermore, these techniques are implemented using mainly three different algorithms: Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Elastic Bunch Graph Matching (EBGM) [10.]

3.8.1 Principal Component Analysis (PCA)

This method is known as Eigenfaces. It pioneers the use of the linear algebra and the matrix manipulation algorithms from the linear algebra for the facial classification. This is done by firstly normalizing the captured image to match the size and the location of certain features such as the eyes, nose, and mouth with the template picture. Then it compresses the image, revealing the most effective low dimension data and removing the unused features; then it decomposes the face structure into uncorrelated and orthogonal components known as Eigenfaces. Each produced face is represented as a weighted sum and stored into an array structure, as figure9 shows below. In the recognition stage, each element of array will be compared with the pictures that were previously stored in the database.

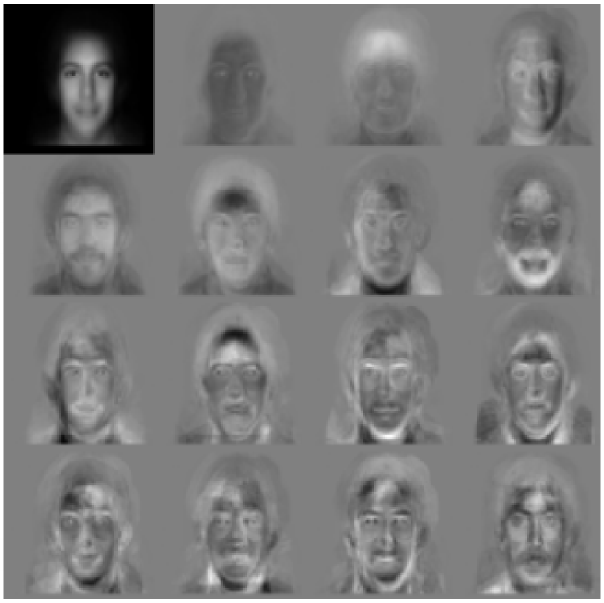

Figure9. Principle Component Analysis [10]

This main advantage in using this approach is that it substantially reduces that data needed to the order of the 1/1000th. However, the main disadvantage of this method is that it requires pictures to be taken only by full frontal faces.

3.8.2 Linear Discriminant Analysis (LDA)

This method is based on pre-classification prior recognition, following a classification of an unknown class sample based upon the training samples of the known classes. This method maximizes the factors between the class variance and minimizes the features difference within a class variance. Figure10 shows each class separated in a block of picture. As we can see, that the variance between classes resembles a much larger change than within a block.

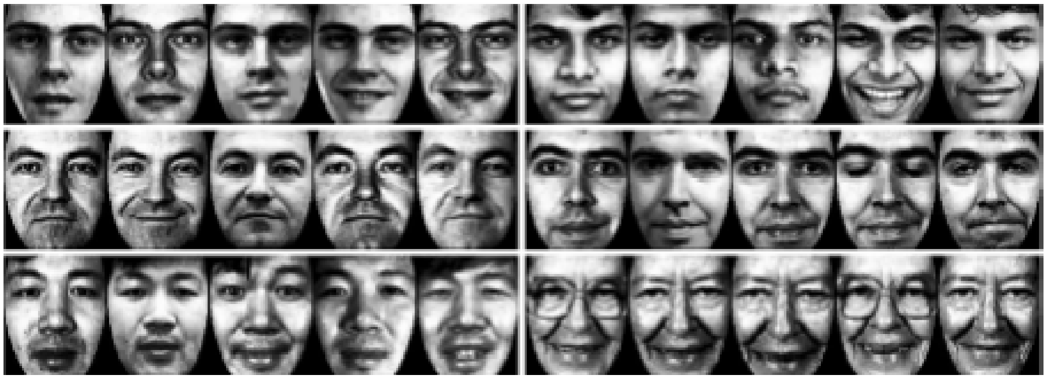

Figure10. Linear Discriminant Analysis [10]

The main advantage of this method that it is simpler to implement; as well as, it recognizes human in different modes and scenarios such as when a person is happy, sad, smiling, scared, frowning, etc. The main disadvantage of this scenario is the training required to acquire all the above information about the person; moreover, to be able to recognize a person in such variety, the recognition threshold much be lowered to accommodate this requirement, which might lead to higher false reject. This accept, and reject criterion will be discussed in the next sections.

3.8.3 Elastic Bunch Graph Matching (EBGM)

This is one of the recognition methods that classify real face images that have many non-linear characteristics. We can safely say that this is one of the smarter algorithms that can recognize human faces in different forms or scenarios. These may include: the illumination, pose, expression, rotation, and tilt. This method creates an elastic grid that gets overlaid on the top of the human head marking all his/her features oh this grid using a Gabor wavelet transform as figure11 shows below. Then a Gabor filter is used to detect shapes and extract the facial and head features using the convolution function from the digital signal processing functions. The convolution expresses the amount of overlap between the collected samples. Finally the results of the recognition are based on the Gabor filter response's outcome.

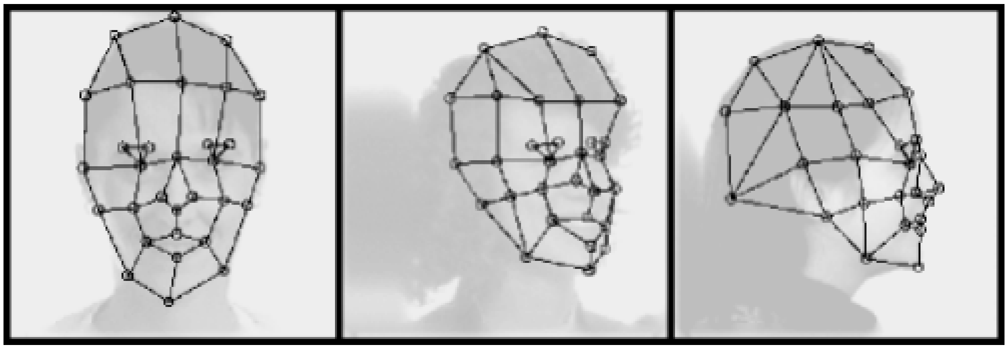

Figure11. Elastic Bunch Graph Matching [10]

The main advantage of this technique that it is realistic and non linear, which means it will recognize the individual in any form; it can even recognize the driver in his/her car without the need to step outside and stand directly in front of the camera. These can speedup the verification process at the gates. The main disadvantage of this method is that it requires feature localization technique to identify the facial features. This can easily be done by combining one of the techniques discussed in 3.8.1 and 3.8.2 with this one.

3.9 Voice Recognition

This type of recognition identifies the human based on his/her voice. It shall not be confused with the speech recognition that is normally used to recognize the words as they are articulated. The voice recognition looks for vocal features that are produced by the vocal cords, airways, soft tissue cavities, jaw, tongue, larynx and resonance in the nasal passages. There are two types of voice recognition. The first is text dependent; it is also known as constraint mode, where the user is supplied by special numbers and characters; then, he/she is asked to repeat. The second approach is text independent; it is known as non-constraint mode, where the voice sample is taken without any restrictions. We can see that this method can be more beneficial in case if the sample has to be taken without the person's prior consent or knowledge.

In either voice recognition modes, the analog voice sample is taken using then digitized using Fourier transformation, and other digital signal processing techniques, then the frequency, intensity, quality, duration, dynamics and the pitch of the signal are analyzed to determine the person's identity. In text dependent voice recognition model, the statistical analysis is taken by the Hidden Markov Model (HMM). HMM normally takes into consideration the temporal variation that occurs to the person's voice. On the other hand, text independent voice recognition model usually uses the Gaussian Mixture Model to perform the statistical analysis. In this method, the system creates numerous vector or states to characterize the person based on his/her physiological limitations and behavior, which then will be compared against the sample taken.

The main advantage of using the text dependent method is that it is easier to predict the outcome of the individual, and also it is more spoof secure; in other words, the system can generate a random sequence of letters that the tested individual will not be able to predict. On the other hand, it is less flexible than the text independent. The main advantage of the text independent is that the samples can be taken from the individual without his/her knowledge. On the other hand, it is much more susceptible to spoofing and forging since the tested person has the complete freedom to manipulate the system.

3.10 Checking Chain for Voice Recognition

In a voice recognition system, when the number of drivers recorded in the system database is large, the voice recognition rage will not be one hundred percent accurate. This shortcoming has a potential vulnerability, which could enable an attacker impersonate a legitimate driver to pass the voice recognition, as the attacker is able to take the advantage of the fact that his voice could be very similar to one of drivers' voice in the system database. Hence, when the attacker is under the recognition, the voice recognition system suffers from failing to recognize his/her real identity and wrongly treats the attacker as one of legitimate drivers in our system.

The probability of this attack occurrence is getting higher when the attacker keeps challenging the voice testing questions. Supposed the accuracy rate of our voice recognition is p, the probability for the attacker to pass the voice recognition is 1-p. The accuracy rate will be down to p^n after the attacker tries n times to pass the voice recognition. Therefore, the probability that the attacker can successfully impersonate is up to 1-p^n. For example, if P is equal to 90%, n is equal to 15, and the probability that the attack succeeds is up to 53.67% (=1- 0.95^15) when he keeps trying 15 times to pass the voice recognition. Furthermore, when n is equal to 30, the probability for the attacker to pass the recognition is up to 80%, which cannot be tolerated by any system, since this number shows that the attack can obsoletely launch this impersonate attack if he/she keeps trying and challenging the recognition system.

To resolve the above issue, we propose a new mechanism for voice recognition named checking chain. In checking chain, firstly, we record more information for each driver, i.e., license plate numbers, to our voice identifier database. Each driver's identity is bound with his/her license plate. Secondly, when the driver is under the voice testing, in addition to saying the words shown on the screen of the voice identifier, the driver is also required to say their license plate numbers. The voice recognition checks both his/her voice and the license plate number that the driver provided. If both of these two pieces of information are identical, the system will give the truck access. Otherwise, the system will refuse to give the driver permission to entrance. As attackers do not know who the exact person is that they are impersonating, they cannot provide the corresponding right license plate numbers. Therefore, it becomes more difficult for them to launch the impersonation attack.

Nevertheless, a sophisticated attacker is still able to launch the attack by collecting all trucks' license plate numbers and launching a brute-force attack. For instance, an attack could spend a week waiting at the dock and collecting all the truck license plate numbers he saw. Based on their collections, attackers are able to launch a brute-force attack by trying all license plate numbers they collected when they are under the voice recognition. In particular, in Figure 12, driver B is an attacker, the license plate number on his/her truck is B. His/her voice is very similar to driver Q's, and drive Q is a legal driver recorded in the system. The voice recognition system will wrongly recognize driver B as driver Q. Even through the attacker does not know driver Q's license plate number, he can try all license plate numbers he collected. If one of the numbers the attacker collected is driver Q's license plate number, the attack can successfully impersonate driver Q and obtain the permission to entrance.

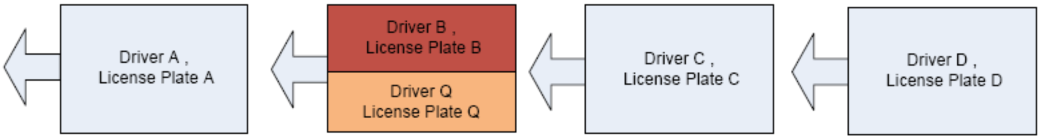

Figure12. Impersonation in Voice Recognition

In order to address this security issue, we propose a scheme, called checking chain. In checking chain, when a driver is passing a voice identifier, in addition to saying himself/herself license plate number, he/she also needs to say the license plate number of the truck in front of him/her. For example, in Figure 12, when the driver D is under the voice checking, he/she not only need to say his/her own license plate number, but also the license plate of the truck C which in front of him. In this way, if there is a brute force attacking happening as we mentioned before, the next driver is able to report the attack to the system. An example is shown in Figure 12, driver B is an attacker, his/her license plate number is B. Driver B impersonates driver Q (whose license plate number is Q) and enters the dock. Driver C is driver behind of the attacker driver B, and driver C is a legitimate user. When driver C is under the voice testing, he/she will report the real number of driver B's license plate, which is not recorded in the system. Therefore, the system will recognize that driver B is doing a brute force attacking, since if there is no attack happening, the sequence of entering the gate should be A->Q->C->D, but the sequence is A->B->C->D, which implies a a impersonation attack. Obviously, as long as this case happens, the system alarms and reports the attack to an authority (e.g., police office).

4 Evaluation Types

Prior architecting the multi-layer biometric system, we must understand the evaluation methodologies and the difference between the different recognition scopes.

There are mainly two different recognition types classified based on their scope: Recognition for verification, and recognition for identification. The recognition for verification, it acts to confirm that a person is really who he/she says. This is simply done by asking the person to enter his/her name, or to scan his/her badge. Then the recognition protocol will determine if the sampled features of this person match his/her file. Using artificial intelligence methodologies for recognition, it is clearly obvious that the match will never be 100% match. Therefore, a threshold is introduced to separate the classification. In other words, if the match percentage is above a chosen threshold value, it is a match; otherwise it is not a match. Choosing the threshold value has to be determined by a detailed research on site, this topic will be discussed more in details in section 6 below.

On the other hand, the recognition for identification is the act of searching for a person in a given database, for example, searching for a match in the terrorist or wanted database. As one can see, this method is time consuming and exhaustive process.

In reality there are many methods for measuring the recognition performance. These methods are: cross-over error rate, hamming distance, detection error trade-off, equal error rate, failure to enroll, false match rate, false non match rate, true accept rate, and true reject rate. Some of these methods will be discussed in details in section 6 below. If one technology is chosen as the absolute verification or identification methodology, then many of these methods will not be satisfied. For that reason, this paper is proposing a multi-layer recognition system that can enhance the throughput and increase the detection accuracy, which promises satisfaction of the above performance measures.

5 Proposed Multi-layer System and Architecture

The purpose of this paper is to propose a multi-layer recognition system that fulfills the shortcomings of each standalone biometric technology. The proposed multi-layer system is composed of 3 layers. At the first layer, the driver will be scanning his/her badge, which means that the proposed recognition system will mainly have verification scope. At the second layer, the driver will be asked to scan his/her retinal. The reason this paper proposes the retinal scan is that it is one of the only few technologies that is near impossible to forge. The third layer will be divided into two technologies performing a secondary verification, and identification in case of miss-match from layer 2/ layer 3 occurs. The third layer adopts the fingerprint scan and the facial recognition using the Elastic Bunch Graph Matching (EBGM) assisted by the Linear Discriminant Analysis (LDA) to locate and identify the facial features. Figure13 below shows the basic layering system proposed by this paper.

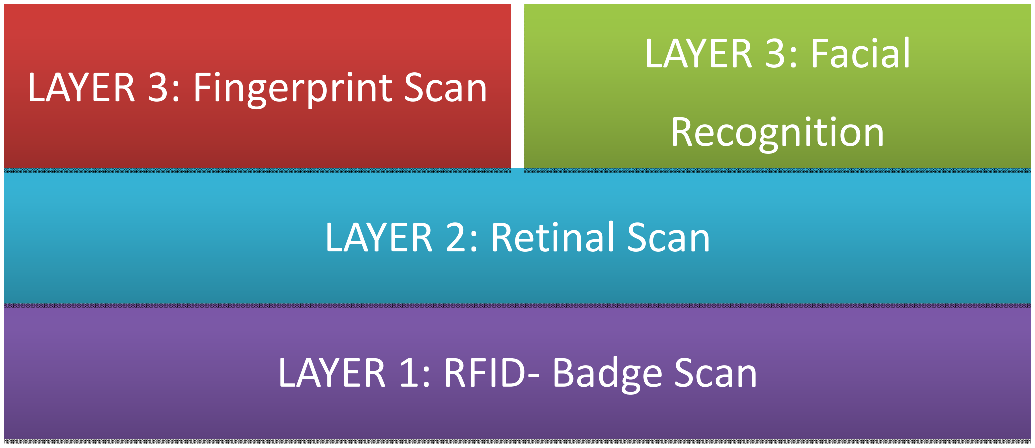
LAYER 3: Fingerprint Scan
LAYER 3: Facial Recognition
LAYER 2: Retinal Scan
LAYER 1: RFID- Badge Scan

Figure13. Multi-layer basic architecture.

In case of a miss match from layer 2 or layer 3, layer 3 will start performing the identification recognition protocol, looking mainly for a match in the wanted or watch list. The identification will still be performed by the two technologies, and confirmed deterministically by the correlation factor between them. Figure14 below shows the basic logic flow chart for the operation of the proposed multi-layer system. Please note that if a miss match occurs at layer one (RFID badge is not in database) layer 3 will be performing the identification protocol directly without giving access to the second layer.

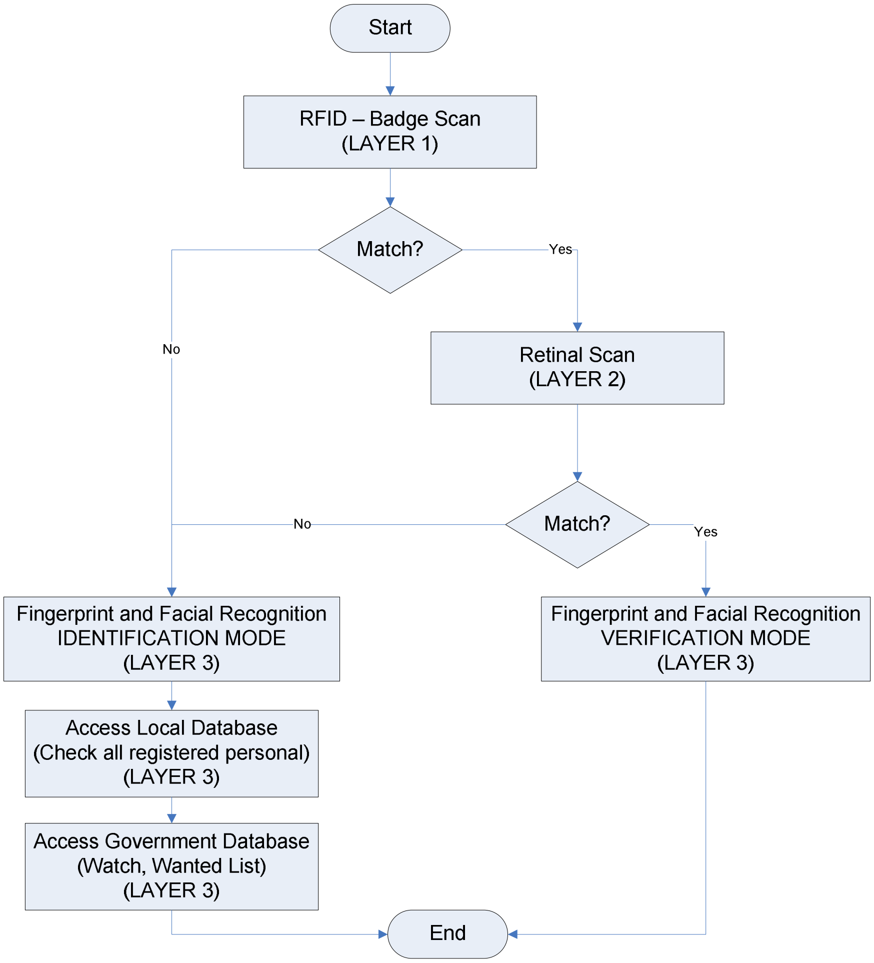

Figure14. Multi-layer Basic Logical Flow Chart.

Thus, the proposed system will be near impossible to forge due to the fact that not only the retinal scan is near impossible to forge, but also it is quite impossible to forge all three technologies all together. Secondly, it performs multiple redundant checks to confirm the person’s identity more accurately.

6. Recognition Performance Measurements

As discussed at the end of section 4 there are several performance measurements that are performed upon the system to guarantee accuracy and conformity. This section will focus on mainly four performance measurements: True Accept Rate, True Reject Rate, False Match Rate, and False Non-Match Rate. All these four issues can be easily enhanced by simply choosing the correct threshold value. The True Accept Rate is simply measured by counting the amount the system has correctly identified the person as accept over the number of accept. Likewise the True Reject Rate, it is simply measured by counting the amount the system has correctly identified the person as reject over the total number of reject. They are expressed by the following formulas.

$$True\ Accept\ Rate = \frac{\#\ Correct\ Accept}{Total\ Accept},$$

$$True\ Reject\ Rate = \frac{\#\ Correct\ Reject}{Total\ Reject}.$$

The False Match Rate is the same as the False Accept Rate, where the person was identified as accepted falsely. This means that we granted access to an authorized person. On the other hand the False Non-Match Rate is the same as the False Reject Rate. This means the system didn’t grant access to an authorized person. These values can be calculated by the following formulas:

$$\text{False Accept Rate} = 1 - \text{True Accept Rate},$$

$$\text{False Reject Rate} = 1 - \text{True Reject Rate}.$$

Ideally, the system should have 100% True Accept and True Reject Rate and 0% False Accept Rate and False Reject Rate. Unfortunately, this is not achievable in real system due to the error factor. Achieving better results can be done in two ways. The first approach is choosing an optimum threshold value. This exclusively can be difficult to achieve due to the fact that the verification rate, the true reject rate and the false reject rates are independent variables. In many cases when the threshold value is increased the verification rate increases as well as the false reject rate combined with the false accept rate. Also when we decrease the threshold, the verification rate increases, as well as the false reject rate combined with the false accept rate. This is best described by figure15 below [13]

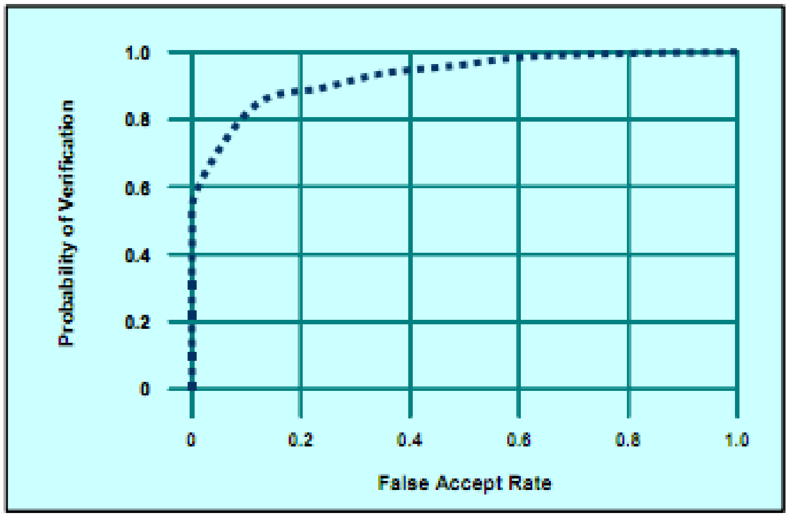

Figure15. Probability of Verification vs. False Accept Rate

The second approach is to use the proposed multi-layer system. Multi-layer Biometric system will reduce both the global False Reject Rate and False Accept Rate because these values will be determined by the outcome of the three layer system all combined and not by only one miss predicted value.

7. Conclusion and Discussion

In this project, we present the proposed multi-layer biometric system for the port of Los Angeles. This multi-layer system consists of three layers: the first layer is composed of RFID badge scanning; the second layer is composed of retinal scan; finally at the last layer, it is composed of fingerprint scan and facial recognition scan. The top layer mainly works in verification mode as a secondary authentication method. It also works in identification mode when either the second or third layer fails to verify the person. Using multi-layer biometric system decreases the False Reject Rate and the False Accept Rate, which in return it drastically increases the performance. Using the multi-layer biometric system in combination with the optimum tested threshold value, will create a secure, optimal, artificially intelligent system.

In the future, a computer simulations model will be developed expecting to provide preliminary data to compare with the existing adopted gate appointment system. Thus, our initial goal of computer simulation is targeted at the queue time outside the gate using the proposed multimodal biometric model. Different case scenarios such terminals, gates, weather, will be taken into account.

To obtain information on queue times and transaction times as well as to compare total turn time for transaction, we will conduct truck counts and measured queue times at different terminals (field observations). We will collect observations over a period of several consecutive days in order to keep the data as representative of normal condition as possible. Data on wait times from the on-site data collection will be used to compare with the computer simulation results. Once complete above-mentioned computer simulation and filed observations, detailed crossover comparison between the computer simulation results and filed-collected data will give us feedbacks so that we can continue to improve the proposed model.

References

[1] The Port of Los Angeles in California "About the Port", http://www.portoflosangeles.org/idx_about.asp.

[2] Biometrics Fingerprint recognition "Fingerprint recognition", http://www.biometrics.gov/Documents/FingerprintRec.pdf.

[3] Biometrics Palm print recognition "Palm print recognition", http://www.biometrics.gov/Documents/PalmPrintRec.pdf.

[4] Biometrics hand geometry recognition "Hand geometry recognition", http://www.biometrics.gov/Documents/HandGeometry.pdf.

[5] Biometrics Dynamic Signature recognition “Dynamic Sign. Recognition”, http://www.biometrics.gov/Documents/DynamicSig.pdf.

[6] Biometrics Vascular Pattern recognition “Vascular Pattern Recognition”, http://www.biometrics.gov/Documents/VascularPatternRec.pdf.

[7] Biometrics Iris recognition “Iris Recognition”, http://www.biometrics.gov/Documents/IrisRec.pdf.

[8] Retina “Retina”, http://en.wikipedia.org/wiki/Retina

[9] Biometrics Retina Recognition “Retina Recognition”, http://www.biometricnews.net/Publications/Biometrics_Article_Retinal_Recognition.pdf.

[10] Biometrics Face recognition “Face Recognition”, http://www.biometrics.gov/Documents/FaceRec.pdf.

[11] Dissertation submitted in partial fulfillment for the masters degree in computer science. Roger Woodman, University of West England, Bristol “A Photometric Stereo Approach to Face Recognition”, http://www.brl.ac.uk/~rwoodman/files/A_Photometric_Stereo_Approach_to_Face_Recognition.pdf.

[12] Biometrics Voice recognition “Voice Recognition”, http://www.biometrics.gov/Documents/SpeakerRec.pdf.

[13] Artificial Intelligence Biometrics Acceptance Criterion “Biometrics Recognition Acceptance. Criterion”, http://www.biometrics.gov/Documents/BioTestingAndStats.pdf

[14] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition System (Springer: New York, 2004).

[15] Maltoni, Davide, et al. Handbook of Fingerprint Recognition (Springer: New York, 2005).

[16] A.J. Goldstein, L.D. Harmon, and A. B. Lesk, "Identification of Human Faces," Proc IEEE, May 1971, Vol 59, No. 5, 748- 760

[17] P.J. Phillips, H.Moon, S. A. Rizvi, Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Transactions on PAMI, 2000, Vol. 22, No. 10: 1090-1104.

[18] Virginia Department of Motor Vehicles, http://www.dmv.state.va.us

[19] H Rosoff and D Winterfeldt, "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach", Risk Analysis, Vol. 27, No. 3, 2007.

[20] Peter Gordon, James Moore, Harry Richardson and Qisheng Pan, "The economic impact of a terrorist attack on the twin ports of Los Angeles-Long Beach", http://www.usc.edu/dept/ise/.

[21] Los Angeles Port Explosion a "Wake Up Call" for Strong Measures to Close Gaps in Port Security, http://www.ttd.org/index.asp?Type=B_PR&SEC={CDD58357-6DE6-4062-9C3B -84944448BF89}&DE={73C940A3-09F7-4542-BE21-F8A8AAEC4563}

[22] Port of Miami Cargo Gate: Using Technology to Improve Throughput and Enhance Security.

http://www.porttechnology.org/technical_papers/port_of_miami_cargo_gate_using_technology_to_improve_throughput_and_enhance

[23] US Port Security. http://bpa.odu.edu/port/research/US%20Port%20Security%20A%20v11.doc.

[24] LA More Secure From Terrorism But Still Vulnerable, http://www.nbclosangeles.com/news/local/LA-More-Secure-From-Terrorism-But-Still-Vulnerable-129487573.html.