A FRAMEWORK FOR ANALYZING BIOMETRIC TEMPLATE AGING AND RENEWAL PREDICTION

DISSERTATION

John W. Carls, Lieutenant Commander, USN

AFIT/DCS/ENG/09-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/DCS/ENG/09-07

A FRAMEWORK FOR ANALYZING BIOMETRIC TEMPLATE AGING AND RENEWAL PREDICTION

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

John W. Carls, BS CS, MS CS

Lieutenant Commander, USN

March 2009

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/DCS/ENG/09-07

A FRAMEWORK FOR ANALYZING BIOMETRIC TEMPLATE AGING AND RENEWAL PREDICTION

John W. Carls, BS CS, MS CS

Lieutenant Commander, USN

Approved:

_____//signed//________________________ __________

Richard A. Raines, PhD Date
Committee Chairman

_____//signed//________________________ _________

Michael R. Grimaila, PhD Date
Committee Member

_____//signed//________________________ _________

Steven K. Rogers, PhD Date
Committee Member

Accepted:

_____//signed//________________________ ___19 Mar 09___

M. U. Thomas, PhD Date
Dean, Graduate School of
Engineering and Management

AFIT/DCS/ENG/09-07

Abstract

Biometric technology and systems are modernizing identity capabilities. With maturing biometrics in full, rapid development, a higher accuracy of identity verification is required. An improvement to the security of biometric-based verification systems is provided through higher accuracy; ultimately reducing fraud, theft, and loss of resources from unauthorized personnel. With trivial biometric systems, a higher acceptance threshold to obtain higher accuracy rates increase false rejection rates and user unacceptability. However, maintaining the higher accuracy rate enhances the security of the system. An area of biometrics with a paucity of research is template aging and renewal prediction, specifically in regards to facial aging. Through the methods presented in this research, higher accuracy rates are obtained without lowering the acceptance threshold, therefore improving the security level, false rejection rates, and user acceptability. As a proof of concept, this research develops a biometric template aging and renewal prediction framework currently absent in the biometric literature. The innovative framework is called the Carls Template Aging and Renewal Prediction Framework (CTARP Framework). The research integrates a diversity of disparate developments to provide a critical fundamental framework of significant advancement in the biometrics body of knowledge. This research presents the CTARP Framework, a novel foundational framework for methods of modeling and predicting template aging and renewal prediction based on matching score analysis. The groundwork discusses new techniques used in the template aging and renewal prediction framework, to include "perfect match score matrix", "error score matrix", and "decay error estimate" concepts. The matching scores are calculated using commercially available facial matching algorithms/SDKs against publicly available facial databases. Improving performance error rates over biometric authentication systems without a template aging and renewal prediction process is accomplished with the new CTARP framework while maintaining or improving upon the overall matching and/or rejection levels. Using such scores, timeframe predictions of when an individual needs to be renewed with a new template is feasible.

Acknowledgments

First, I would like to thank God for blessing me with everything He has given to me in life. Although I do not always understand why He has put me on certain paths in my journey through life, I know it is all part of His greater plan for me.

I can never express enough gratitude for my wife. I want to thank my loving, beautiful, and patient wife for helping me through this journey with all she has done for me. My job was easy because of everything she did for our family at home. I also want to thank my children for being accepting of my frequent absences from home during the pursuit of this degree. Thanks to my family for enduring the many nights and weekends that we shared together, yet apart. I may have been home physically for most of the time, but my time and thoughts were spent advancing my research and career. I also thank my parents, for giving me the best opportunities for success as they could. They showed me the virtues worth striving for in life and the value of hard work.

I thank Dr. Richard Raines, my advisor, for allowing me to spread my wings, to test uncharted waters, and yet keeping me on course to graduation. I also thank my committee (Drs. Raines, Grimaila, and Rogers) for the numerous document reviews, feedback, and support of my research, publications, and dissertation.

Academics aside, I thank Ms. Stacey Johnston, the unsung hero of the Center for Cyber Research for always selflessly taking care of the CCR students (and staff!), making our lives at AFIT that much less stressful.

I would like to express gratitude to Samuel Dewolfe and the Biometric Fusion Center for utilization of resources; to Dr. Kevin Bowyer and Dr. Patrick Flynn of the

University of Notre Dame for support of the Collection B database; to Dr. Karl Ricanek, Jr. of UNC-Wilmington for support of the MORPH database; and Cognitec Systems for an evaluation copy of the FaceVACS SDK.

It takes the support of many people to achieve success. I thank all those people, named and unnamed, now and in the past, for their help in getting me this far in life. I am fortunate to have such a caring assemblage of people touch my life. I hope I am able to return the favor.

Table of Contents

List of Figures

Page

List of Tables

Page

List of Acronyms

ABIS	DoD Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AFIT	Air Force Institute of Technology
ANSI	American National Standards Institute
API	Application Programming Interface
AUTH	Authentication
BEE	Biometric Experimentation Environment
BioAPI	Biometric Application Programming Interface
BTF	U.S. Army Biometrics Task Force
BSWG	Biometrics Standards Working Group
CBEFF	Common Biometric Exchange Formats Framework
CER	Crossover Error Rate
CI	Confidence Interval
CIO	Chief Information Officer
CMC	Cumulative Match Characteristic
DE	Decay Error estimate
DET	Detection Error Trade-off
DoD	Department of Defense
DV	Distance Vector
EBTS	Electronic Biometric Transmission Specification
EER	Equal Error Rate
EFTS	Electronic Fingerprint Transmission Specification
FAR	False Acceptance Rate
FERET	Face Recognition Technology
FRGC	Face Recognition Grand Challange
FRR	False Rejection Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FpVTE	Fingerprint Vendor Technology Evaluation
FRVT	Face Recognition Vendor Test
FTA	Failure to Acquire
FTE	Failure to Enroll
GWOT	Global War on Terrorism
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Iris Challenge Evaluation
IDS	Identity Dominance System
IEC	International Electro-technical Commission
IEEE	The Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ESM	Error Score Matrix
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
MPA	Match Prediction Accuracy

ND	University of Notre Dame
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
PMSM	Perfect Match Score Matrix
REP	Re-Enrollment Point
RF	Radio Frequency
RFID	Radio Frequency Identification
RFC	Request For Comments
ROC	Receiver Operation Characteristics
SDK	Software Development Kit
StdDev	Standard Deviation
TRPA	Template Renewal Prediction Algorithm
UNC-W	University of North Carolina at Wilmington
USNA	United States Naval Academy

List of Definitions

Accuracy: A catch-all phrase for describing how well a biometric systems performs. The actual statistic will vary by task (verification, open-set identification (watchlist), and closed-set identification).

Algorithm: A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc.

Arch: A fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point.

Attempt: The submission of a single set of biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual.

Authentication: 1. The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: “This individual’s name is ‘Joseph K.’ ” or “This child is more than 5 feet tall.” 2. In biometrics, “authentication” is sometimes used as a generic synonym for verification. 3. The verification of the identity of a person, object or process.

Automatic Identification and Data Capture: A broad term that covers methods of identifiying objects, collecting information about them,, and entering it directly into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.

Automatic identification: A broad term that covers methods of identifying objects, capturing information about them and entering it directly into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.

Behavioral Biometric Characteristic: A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics.

Bifurcation: The point in a fingerprint where a friction ridge divides or splits to form two ridges.

Biological Biometric Characteristic: A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavioral trait. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry. Also known as: physical/physiological biometric.

Biometric Sample: Information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.

Biometric System: Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of: 1. Capturing a biometric sample from an end user; 2. Extracting and processing the biometric data from that sample; 3. Storing the extracted information in a database; 4. Comparing the biometric data with data contained in one or more reference references; 5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved. A biometric system may be a component of a larger system.

Capture: The process of collecting a biometric sample from an individual via a sensor.

Comparison: Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision.

Database: A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related end user information, etc

Decision: The resultant action taken (either automated or manual) based on a comparison of a similarity score (or similar measure) and the system's threshold.

Enrollment: The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Eigenface: A set of eigenvectors used in the computer vision problem of human face recognition.

Feature(s): Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference.

Failure to Enroll (FTE): Failure of a biometric system to form a proper enrollment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

False Acceptance Rate (FAR): A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim.

False Match Rate (FMR): A statistic used to measure biometric performance. Similar to the False Acceptance Rate (FAR).

False Non-Match Rate (FNMR): A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not.

False Rejection Rate (FRR): A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.

Identification: A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity.

Impostor: A person who submits a biometric sample in either an intentional or inadvertent attempt to claim the identity of another person to a biometric system.

Live Capture: Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface).

Liveness Detection: A technique used to ensure that the biometric sample submitted is from an end user. A liveness detection method can help protect the system against some types of spoofing attacks.

Match: A decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (difference or hamming distance).

Matching: The process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold.

Modality: A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

Multimodal Biometric System: A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

Neural Network: A type of algorithm that learns from past experience to make decisions.

ROC - Receiver Operating Characteristics: A method of showing measured accuracy performance of a biometric system. A verification ROC compares false accept rate vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

Sensor: Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.

Sensor Aging: The gradual degradation in performance of a sensor over time.

Similarity Score: A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference.

Template: A digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.

Template Aging: The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.

Template Size: The amount of computer memory taken up by the biometric data.

Threshold (η): A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

True Accept Rate (TAR): A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

True Reject Rate (TRR): A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

Type I Error: An error that occurs in a statistical test when a true claim is (incorrectly) rejected. For example, John claims to be John, but the system incorrectly denies the claim.

Type II Error: An error that occurs in a statistical test when a false claim is (incorrectly) not rejected. For example: Frank claims to be John and the system verifies the claim.

Verification: A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template.

Whorl: A fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain two or more deltas.

A FRAMEWORK FOR ANALYZING BIOMETRIC TEMPLATE AGING AND RENEWAL PREDICTION

I. Introduction

1.1 Background

Biometric-based systems are becoming more popular, replacing knowledge-based systems such as password or token-based systems. A biometric is used to associate an individual's identity to their unique physical characteristics. Biometrics cannot be as easily compromised as their knowledge-based counterparts. They are used in a variety of security applications, with one or more biometric devices operating either sequentially or simultaneously. The biometric-systems are classified into one of two categories: identification-based or authentication-based. Identification-based systems are used to identify the owner of the biometric by comparing the template to the entire database. This process is known as 1:N matching. Authentication-based systems are used to compare identities to a corresponding stored claimed identity, known as 1:1 matching, and determine if the individual is authentic or an imposter. A matching score is compared to a threshold to determine the validity of the individual's authentication [Ano07, MaG05].

The biometric-based systems and devices that provide authentication of an individual are used to provide the rights or ability to have access to resources. These resources can be physical, such as a facility, building, or lab; or electronic, such as a computer, network, stored data, or information. Resource authentication requires an initial registration and enrollment process. This initial process creates a template that is saved and utilized by the system for future comparisons. An open-ended research question with biometrics and templates is associated with the dynamics of biometric data and the rate in which stored data must be updated to minimize the rates of false-rejection (FRR) (Type I errors) and false-acceptance (FAR) (Type II errors) into/from the system. Biometric template aging is a concept wherein individual biometric data deviates from enrollment and therefore must be updated periodically. The template update rate can vary from a relatively short period of time to once every few years. Research is needed to ascertain the rate of update versus the accuracy of these updates over an extended period of time.

One way of addressing the template aging problem is to renew the template with a certain periodicity. This can be unnecessary, especially if the biometrics have not changed or are costly, time consuming, and resource intensive for large organizations such as a government or defense department. On the other hand, if the template is not updated the individual may not be able to gain access. Even harsher consequences, an imposter may be able to gain access due to changes in their own physical traits over time. The periodicity of change is not easily determined. The frequency of renewal needs to be determined based on historical changes and variances over time. Renewal determination needs to be based on a figure of merit that is maintained over time, although the changes and periodicity are unknown. Through the method presented in this dissertation, improved accuracy rates up to 20% are obtained without lowering the acceptance threshold, therefore improving the security level, False Rejection and Acceptance Rates, and improving user acceptability.

This research develops a foundational framework for biometric template aging and renewal process. This new framework further advances the body of knowledge and provides improvement to receiver operation characteristic (ROC) curves of the False Acceptance Rate (FAR) and False Reject Rate (FRR) for biometric-based authentication systems.

1.2 Problem Statement

Identity capabilities are being revolutionized by biometrics (more specifically for this research - biometric-based authentication systems). However, there is a multitude of problem areas involved with template aging. Problems range from image quality to biometric, sensor, and environmental variance as well as malicious intent [DaY06, JaR05]. These problems could allow for higher false accept and false rejection rates into the system. A higher accuracy of identity verification is becoming a requirement. This higher accuracy will provide improvements to the security of biometric verification systems; ultimately reducing fraud, theft, and loss of resources from unauthorized personnel. With previous systems, a higher acceptance threshold to obtain higher accuracy rates increased FRRs and user unacceptability. However, maintaining the higher accuracy rate enhances the security of the system. Expecting a system to perform with 100% accuracy over time is unobtainable. Machines and humans that use them are subject to errors. These error rates need to be reduced to prevent fraud, theft, and resource loss from unauthorized personnel. Verification error rates need to provide near-perfect accuracy with every attempt. This allows for only the correct individual to access resources and eliminates imposter access. Unfortunately, verification falls short of that capability. Current accuracy rates range from 80% to 99.9% depending on the modality [Ulu06]. Additionally, no template renewal process currently exists as the template ages, only that the template is aged and may have to be renewed. Finally, there are components that provide details on how to handle biometrics and biometric templates during certain events; but there is no identified process or framework for the entire lifecycle of biometrics, biometric templates or the template aging process, including renewal.

One area of biometrics that has a paucity of research is template aging and the adult age-progression, particularly facial aging. This dissertation presents a method of modeling and predicting facial template aging based on matching score analysis, not through algorithm improvements. The groundwork discusses the techniques used in the template-aging framework. Matching scores are calculated using commercially available facial matching algorithms/SDKs against publicly available facial databases. This new framework improves performance error rates while maintaining or improving upon the overall matching and/or rejection levels. Using such scores, the prediction of a timeframe is deterministic for when an individual needs to be re-enrolled. This framework ultimately enhances the security of the biometric system.

1.3 Research Goal

This research develops a novel biometric facial template aging framework architecture, dubbed the “Carls Template Aging and Renewal Prediction Framework” (CTARP Framework for short), to biometric systems (namely, verification). To achieve this goal, the CTARP Framework combines key biometric functionalities in a way that improves performance error rates while maintaining or improving upon the overall matching and/or rejection accuracy levels and security of that implementing biometric verification system. Implementing the CTARP Framework tightly couples the biometric template to the user's identity, significantly reduce the acceptance of imposters trying to steal or fraud biometrics systems to gain access to benefits and resources; and will reduce costs while improving user acceptability. Reduced cost equates to more resources available for the implementing organization. This translates to more capital for the organization where additional resources may be necessary.

1.4 Research Contributions

1.4.1 Template Aging and Renewal Prediction Framework for Biometrics

The primary objective of this research is to develop a coherent biometric template aging and renewal prediction framework that improves upon current false acceptance and rejection rates. The methods used in this research are based on a matching score output from a face recognition system against publicly available facial databases.

1.4.2 Extension of CTARP Framework to Other Biometric Modalities

Once the CTARP Framework is established using the facial modality (aging), the methodologies are expandable to include other biometric modalities. It also applies to any future biometric system framework and metrics. This matrix and fusion of time, aging, and renewal factors are combined to make biometric applications more readily reliable, improving biometric system performance, and more widely deployed, thus meeting the needs of not only homeland defense and security needs, but the security needs of the deployed forces.

1.5 Assumptions/Limitations

The CTARP Framework assumes the biometric verification system and associated databases has sufficient data to support template aging over an extended period of time. Another assumption is that there is significant variance to the template due to aging over an extended period of time. The advantage of the CTARP Framework is to provide a mechanism for developing biometric template aging predictions using the innovative methodology to reduce costs.

1.6 Dissertation Organization

This document is divided into five chapters. This chapter provided a brief motivation for the necessity of the research and identifies problems and inefficiencies that are currently faced within biometric verification systems. Chapter II reviews relevant literature for biometrics, biometric-based authentication, biometric templates, and biometric template aging. Chapter III discusses the development and the details of the CTARP Framework, along with the motivation for pursuing this architecture. This chapter also discusses the modeling setup, biometric template aging simulations and models that support the framework. Chapter IV presents the results and analysis of the numerous simulations performed during the course of this research. Chapter V concludes the document with a brief summary of the research, highlights of the contributions this research provides to the biometrics community along with recommendations for future research.

II. Literature Review

2.1 Chapter Overview

This chapter summarizes the current state of biometrics and represents the results of an extensive literature research review covering the broad related areas of: 1) biometrics, the different modalities, and biometric-based authentication systems; 2) biometric functions of capture, enrollment, verification, templates, storage, and security; 3) biometric standards; and 4) biometric template aging and prediction. The first area of review includes biometrics and the various biometric modalities utilized by biometric-based authentication systems. The second areas covers the various functionalities implemented and encompass a biometric-based authentication system. The third area of research review pertains to the biometric standards that are currently in use with the various components, technologies, and systems. Finally, the last area reviews the latest prediction models and template aging research.

2.2 Biometrics, Modalities, and Authentication

This section provides an overview discussion of biometrics. Several typical questions asked are: What is biometrics? What does biometrics do? How does biometrics work? With some understanding of biometrics, further questions surface, such as: What are biometric templates? What is biometric template aging? How are templates created or selected? These questions and more will be answered to provide the background for the research.

The definitions of biometrics are various and can be summed up to be: “automated method of identifying or authenticating a person from a physiological or behavioral characteristic that makes that person different from others” [WaJ05]. Biometrics are used for identification and/or verification of an individual using characteristics or traits associated with the person. Ideally, biometric systems use characteristics that are unique to each individual and do not have duplicates. For example, no two fingerprints are the same, similar to no two snowflakes being identical. Biometrics are both physiological (hand, eye, etc) and behavioral (walk, talk, signature). The biometric-based systems are used to perform two different roles: 1) verification – you say who you are and the sample is verified against the template on file, and 2) identification – your template is matched in a database against other templates identifying you as a certain individual. A physiological biometric is derived from the physical body – iris, retina, facial features, fingerprint, hand geometry. This is opposed to a behavioral biometric – some action unique to you; such as: your signature; keystroke traits - how long it takes you to type a pattern; or your voice traits - such as pitch and pronunciation. A biometric is a measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an enrolled user. Physical features typically used for biometric identification are fingerprint, retinal, iris, facial, or hand geometry. By determining an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, identification for a specific user can be determined and authentication for access be granted [WaJ05].

There are qualifying characteristics of biometrics that are used as an identifier:

- Universal/Universality - Each person should have the specific biometric trait
- Distinctiveness/Uniqueness - Any two people should be sufficiently different in terms of the characteristic or identifiers
- Collectible - Biometric traits must be obtainable/collected and quantitatively measured
- Permanent/Permanence - Traits remain sufficiently invariable over time, allowing for repeatable measures [MaM03].

A good overview statement about biometrics as proclaimed by PassUK.com's website:

> "Biometrics is becoming the 'norm' for not only large applications and projects, but for protecting access to individual computers, cell phones, pocket sized personal computers, networks, web servers and database applications, as well as during transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with keyless entry and keyless ignition. Current stringent Data Protection Regulations with regard to access control to sensitive or personal data held within Corporate network is adding to the demand for much tighter access control. Markets such as Healthcare, Banking/Finance, and Government are specifically sensitive to the problem" [Ano05a].

2.2.1 Biometric Systems

Biometrics are benefiting from research that is leading to an increased number of biometric systems. Almost a decade ago, the biometrics industry was almost non-existent and is now developing into a key producer of profits in the fields of access control and security. Regulations within the government are requiring an elevated level of security to maintain authenticity, integrity and confidentiality (AIC security triad) of information systems and technology. The guidelines have been established by the government with the Sarbanes-Oxley Act of 2002, which mandates companies to ensure that physical and logical access of company resources are complied with. The U.S. Food and Drug

Administration's (FDA) Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11) requires companies to have controls in place to identify access regulations, create and maintain audit trails, and implement and uphold security of the system. The government has highly encouraged and recommended biometrics as a security choice as part of the compliance for the guidelines [Shi05].

A biometric system is both a data capture system and a pattern recognition system with the ability to recognize an individual based on specific physiological or behavioral characteristics that an individual possess. A biometric system is an automated system capable of capturing a biometric sample from an individual and extracting biometric data from that sample. The digital representations of the raw biometric characteristics are processed by a feature extractor to produce a small expressive representation called a template used for matching purposes (Represented as X_I in Figure 1). The system then captures a new biometric data sample and compares the biometric data with the data contained in one or more reference templates. The classifier within the biometric system decides how well the comparison matches between the template and the new sample provided and generates a figure of merit indicating the magnitude of the match, and possibly a measure of the quality of the match. If the match figure of merit crosses a predetermined threshold, then a match is deemed to have occurred and authentication has succeeded. Notification is given whether or not an authentication of identity has been achieved (See Figure 1). Additionally, the biometric system is responsible for storing and managing the information dedicated to the biometric application. The biometric system has one of two modes of operation for authentication: 1) Uni-modal: which uses a single biometric; or 2) Multi-modal: which uses multiple biometrics. A multi-modal biometric system performs the verification process either sequentially or simultaneously [Ano06b, Hon98, WoO03].

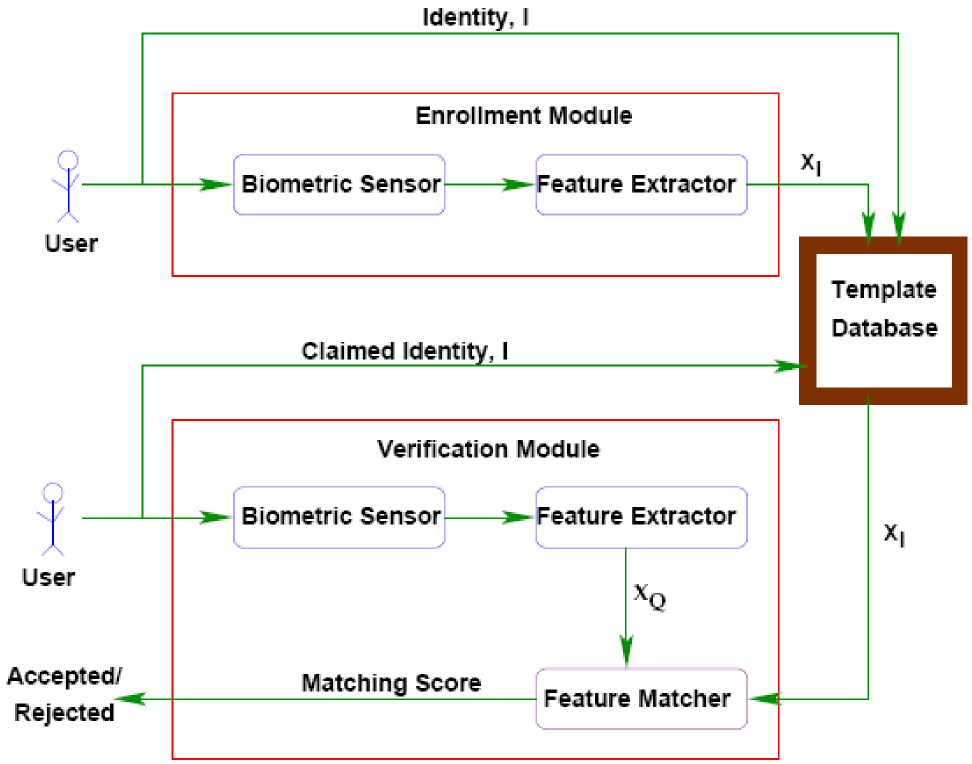


Figure 1 - Basic Enrollment and Verification Process [Ros03]

A biometric system, in simplicity and at a minimum, is composed of four important modules: 1) Sensor Module – which captures an individual's biometric data. For example: a fingerprint sensor that captures fingerprint impressions of a user; 2) Feature Extraction Module – where the acquired data has feature values processed and extracted. For example: a fingerprint's position and orientation of minutiae points would be computed; 3) Matching Module – verification feature values are compared against those in the template by generating a matching score. For example: the verification query minutiae and template minutiae number of matches can be computed and treated as a matching score; and 4) Decision-making Module – where the proposed individual's claimed identity is either accepted or rejected based on the matching score generated in the matching module (authentication) [Ros03]. Additional modules that may be incorporated into a biometric system are: storage and communications. The storage module is a database that maintains the collection of the templates. The communications module is used for transferring biometric data from one biometric system to another biometric system. Figure 2 below is an example of a general biometric system incorporating the models.

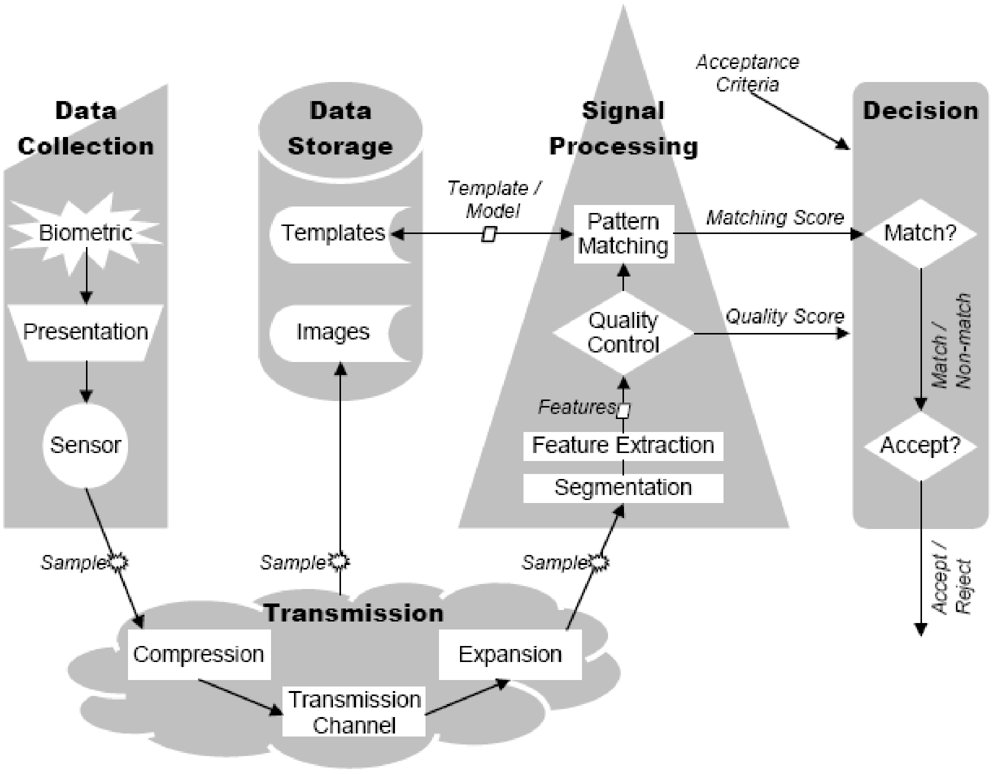


Figure 2 – General Biometric Systems [MaW02]

Pattern classification and algorithms used to process recognition have been used in the field of data mining for a long time. The premise in achieving pattern classification to various fields is the underlying consistency following the observable fact. With this, pattern classification algorithms are exceptional candidates for biometric systems. The biometric features are unique and universal allowing the application of pattern classification. Biometric systems use these algorithms as the backbone. A typical biometric system consists of the following four stages: 1) Measurements; 2) Feature Extraction; 3) Classifier; and 4) Class Label.

Subject interaction with the sensor occurs during the measurement phase, where appropriate measurements are taken. The feature extraction phase is where the suitable biometric features are selected using the biometric input from the measurement phase. This phase also includes relevant features selection. Feature selection is a process that combines related features to make the data manageable and removes poor features. The process fulfills the four criteria of discrimination among data, reliability, independence, and small numbers to increase efficiency.

The major goal of the feature extraction and selection phase is to create the best separation capability between individuals by raw data transformation. For instance, decreasing the number of variables without losing any quality of data. The most significant phase is classification. This is the foundation of the biometric system. The classifier creates categories and rules using training data. Once completed, the classifier is ‘trained’. The goal of the classifier is to categorize new data by the rules created during enrollment. The individual enrolls in the system and provides training data to create their own class. During authentication, the new data provided to the biometric system will be classified into the appropriate class of that individual. The false acceptance rate (FAR) and false reject rate (FRR) rely on the accuracy of the classifier. A distinctive class label is created for each class as the output of the classification phase. Of the different methods to classification, the most proficient ones for biometric data are fuzzy logic, neural network, and statistical [Shi05]. Fuzzy logic's foundation is impreciseness based on humans not requiring accurate data to make decisions. The intent of fuzzy logic is to automate the process of arriving at an answer given inaccurate and/or lost data. Artificial neural networks mimic the nervous system of humans. The nervous system is comprised of levels of organized neurons working together to solve problems. Artificial neural networks use this technique to learn about the individual from the system provided enrollment data using that knowledge to authenticate individuals. Statistical classification uses data distribution, normality, maximum likelihood, and assumption probability. Prior data distribution is necessary for statistical classification methods to perform correctly. Classifiers have varying results based on the data and its nature that is to be categorized. The following criteria are used when comparing classifier performance: Error Probability; Tradeoff of Error/Rejection; Computational Complexity; and Flexibility. "The criticality of the data and protection level requirement will determine the importance of the above stated criteria. Example: for a company designing a biometric system to regulate access to their private financial records, computational complexity and flexibility will not be a concern, whereas probability of error that an unauthorized individual gains access to the data will be a major concern" [Shi05].

2.2.2 Biometric Modalities

There are different types of biometric modalities. These modalities are categorized into two groups: 1) The biological biometric – modality traits of a physical nature, and 2) The behavioral biometric – modality traits repeated through a trained action.

2.2.2.1 The Biological Biometric

The biological biometric utilizes the physiological traits or composition of the human body. These elements include the finger, hand, palm, face, eye – to include the iris and retina, and DNA. Other biological biometrics that are far less known or developed include the ear, veins, and body odor. The following is a summary of the popular biological biometrics in use today.

2.2.2.1.1 Fingerprint Systems

Fingerprinting is one of the oldest forms of personal identification and the most prevalent in use. Using fingerprint biometrics is gaining greater societal acceptance as a biometric. Examples of the acceptance are the IBM Commercials aired on public television. Although in high use today, the DoD Biometrics Management Office states that fingerprints will not be the only biometric of choice and there will be more biometrics in use in the future [MaM03].

The fingerprint biometric system uses a captured image of the fingerprint and looks for a unique pattern in the lines of the tips of the fingers. These unique patterns have been defined as a loop, whorl, or arch. The patterns are broken down into what is called the “minutiae point” (ridges and valleys that come together, begin, or end), which makes up the fingerprint. This is the uniqueness of the fingerprint on an individual and contains the various characteristics: 1) Bifurcation – which is where multiple ridges split out from a single point; 2) Divergence – where parallel ridges join together or spread apart; 3) Enclosure – where a ridge briefly splits and then joins together very closely to the original split; 4) Ending – where the ridge stops; and 5) Dot – single point [JaB02, MaM03]. Due to the age of this biometric, it is the most mature biometric system available in the industry for identification, especially in terms of numbers in database systems (i.e. – Law Enforcement) and variety of economical capturing devices, and is considered highly reliable.

2.2.2.1.2 Facial Recognition Systesm

Facial recognition is a widely accepted form of biometric because it is fairly non-invasive or non-intrusive. The recognition of faces is very commonly used with ID cards, but requires an added level of complexity when the face is used in a biometric recognition system. First, the face must be detected by the biometric system for identification, and then the face must be recognized. However, facial recognition has significantly advanced to incorporate both two dimensions (2D) and three dimensions (3D), as is evident of the Face Recognition Vender Test (FRVT) and Face Recognition Grand Challenge (FRGC) over the last several years [PhS07]. For detection, the capturing camera must isolate the face and facial features of the eyes, nose, and mouth to determine measurements. This measurement process creates a facial frame often called a binary mask. This mask can now be used for identification in the biometric system by performing a one-to-many comparison to find a match. One of the difficulties of using facial recognition is the aging of the face over time. The database needs to be updated periodically to keep the templates current [Col06, MaM03].

> "Facial images are probably the most common biometric characteristic used by humans to make a personal identification. Face recognition is one of the most active areas of research with applications ranging from static, controlled mug shot verification to dynamic, uncontrolled face identification in a cluttered background. In the context of automatic personal identification, face recognition usually refers to static, controlled full frontal portrait recognition. Face recognition is non-intrusive technique. People generally do not have any problem in accepting face as a biometric characteristic" [Hon98].

For facial recognition algorithms, the key objective is to analyze two facial images and determine if they are the same individual. There are two major processes in facial recognition: 1) detect the face within the image; and 2) process the facial image for a particular application. With the advances of facial recognition in 2D and 3D, they both have three main methodologies for face recognition: 1) Analytic methods – rely on data about the face to measure important features on the face. An example is the extended accounts of facial recognition research in which the basis is on the separation involving sets of known fixed points on the face; 2) Holistic methods – manages the input vector as an anonymous identity and in spite of any investigative data of the items being established and applies the learning algorithms to the entire vector. An example of this is an eigenface, which uses a complete method to generate the primary components of a set of facial images for training and mapping new face images onto these vectors to identify individuals. The algorithm used for eigenface is repeatedly referenced due to its ease and speed. Nonetheless, in order to achieve good performance this algorithm needs a high correlation between the faces in the database and changes from the conditions used during training (position, lighting, and expression) hinders performance; and 3) a hybrid of both analytic and holistic methods [Col06].

To fully utilize the increased benefits of 3D facial recognition, there are four tasks that research has generally focused on: 1) Collection methods for 3D data – focusing on collection using commercially available 3D scanners with structured lighting and/or stereo imaging; 2) Facial normalization and correction of the input – is to use 3D information to normalize the face data; this normalization includes pose, lighting/color and expression correction; 3) 3D facial recognition feature development – is to rely on the 3D channel and recognize the face without using color because it avoids problems with changes in lighting and color; and 4) Exploration of schemes for combining 2D and 3D face recognition algorithms – is to combine 2D and 3D recognition channels into a single classifier achieving better performance than each individually [Col06].

2.2.2.1.3 Iris/Retinal Systems

The iris biometric has a relatively short history compared to the fingerprint, but "is claimed to be one of the best biometrics" [Liu06]. The iris has many unique characteristics that can be used for identification and verification. The iris experiences little change after the childhood years and is purported as unique for an individual. This biometric process requires the cooperation of the individual at template creation as well as for the verification or identification process. The iris has six times more features than the fingerprint. This allows the iris to be a more robust identification method. The distinct characteristics include: arching ligaments; corona; contraction furrows; striations; pits; collagenous fibers (connective tissue); zigzag collarette; filaments; dark areas of the iris known as crypts; serpentine vasculature; rings; ridges; and freckles. The iris biometric is fast and accurate in conducting the recognition. Most iris systems use either the Daugman's algorithm or Wildes' system for detection and recognition of the iris [Liu06]. There have been other research projects in recent years related to iris recognition with the majority of the work focused on optimizing or proposing new methods to Daugman's algorithm and Wildes' system [Dau04, JaB02, Liu06, MaM03].

The retina biometric is one of the most invasive of all the biometrics in use. The collecting of the biometric requires full cooperation of the individual in both enrollment and collection to create the template and for verification or identification. This biometric examines the retinal veins in the back of the human eye. The process is accomplished by looking into an eye-piece at a predetermined location and using light of low-intensity reflected off the back of the retina to illuminate the retinal veins. Although very intrusive, the retina biometric is considered one of the most secure forms of identification due the difficulty in replicating the retina of an individual. The process involves an infrared LED that projects onto the back of the retina to reflect back the pattern of the blood vessels [Hon98, JaB02, MaM03].

2.2.2.1.4 Hand Geometry Systems

This biometric uses shape and geometrical features of the hand. Hand geometry is considered an acceptable biometric for low and medium-level security applications. There are two main classifications of hand geometry systems: 1) Pegged systems – where the placement of the hand is guided by pegs; and 2) Pegless systems – where the hand is placed in an arbitrary position with the fingers separated as the only restriction.

The hand geometry systems employ various feature selection techniques such as: 1) Gaussian Mixture Model (GMM) (best performance); 2) Implicit Polynomials; and 3) Geometrical and Shape using GMM features first followed by a metric of distance [MaO05].

The hand geometric characteristics are measured to form the template, which is then compared against future requests. The measurements used are: 1) Widths – of each finger and palm; 2) Heights – of each finger; 3) Distances – between valleys and to center of hand; and 4) Angles – between valley points. These measurements provide 34 possible features for extraction with 28 utilized. The human hand has certain features that are relatively different and do not change over time, and these characteristics are captured by an imaging system. Hand geometry is usually used for verification and not used for identification due to its lack of scalability and average reliability [MaM03, MaO05].

2.2.2.2 The Behaviorial Biometric

Behavioral traits reflect an individual's psychological makeup through characteristic behaviors that are well-established over a period of time but may change through training or influences. Several behavioral characteristic examples include Voice, Speech, Handwriting, Keystroke Signature, and Gait.

2.2.2.2.1 Voice / Speech

The voice biometric is not the same thing as speech recognition. Speech recognition is used to convert what is said to something typed on the computer. An example application is Dragon NaturallySpeaking by Nuance Communications, Inc

[Nua06]. With the voice biometric system, a reference template must be established for comparison, just as in other identification systems. Several characteristics of the voice are pitch, dynamics, and waveform that are influenced by the throat, mouth, vocal tract, nasal cavities, and speech processing mechanisms. There are two main methods of voice/speech biometrics: 1) Text-dependent – which is based on predetermined phrase or text; and 2) Text-independent – which is not constrained by the text or phrase and is more challenging for verification. Difficulties associated with voice biometrics include background noise and changes in voice due to illness or aging. The voice biometric is considered an acceptable biometric, is unobtrusive, and can be accepted as recognition over the phone for identification [Hon98, JaB02, MaM03].

2.2.2.2.2 Handwriting / Signature

The handwriting biometric is also known as the signature biometric because the identification process uses characteristics of the stroking of the pen to produce the signature as well as the direction, pressure, and points where the pen is lifted and placed back on the paper. The handwriting biometric has two different variations of either the behavioral writing or the habitual writing. Different variations can occur in the usage as well. The signature can be used for verification whereby an individually signed document matches the one being presented, but can be fooled by professional forgers. Additionally, handwriting biometric is considered a behavioral biometric because it can change over time or be influenced by physical or emotional conditions [ElH06, JaB02, MaM03].

2.2.2.2.3 Keystroke Pattern

The keystroke pattern biometric is also called typing rhythms or keystroke dynamics. The keystroke biometric uses dynamic characteristics resulting from the striking of keys on the keyboard. The process of authentication is based on an individual's typing patterns. The keystroke biometric uses the rhythm of latencies between keystrokes or the duration to type in certain word patterns, measuring the amount of time between keys (flight time or keystroke latency); and how long the key is held down (dwell time or keystroke press). These patterns provide a unique digital signature template that can be used to identify individuals. This signature can be relatively constant for well-known, regularly typed strings. Like the handwriting biometric, keystroke is a behavioral biometric because it can change over time or be influenced by physical or emotional conditions [JaB02, MaM03, Shi05].

Verification of keystroke dynamics has two modes of classification: Static Verification and Dynamic Verification. Static verification results in a smaller template size and a short time for enrollment because the template can consist of only the particular word being checked and is usually performed during specific times such as login. A disadvantage is the ability for the session to be hijacked through duplicating the static keystroke timing to create a template match. Dynamic verification is performed periodically preventing the session from being compromised. Disadvantages of dynamic verification are the computational complexity, enrollment time, and the large template size that is created from the larger pattern of words typed during enrollment to authenticate the individual [Shi05].

2.2.2.2.4 Gait Recognition

The gait biometric is based on the way an individual walks or runs. It can be difficult or challenging in capturing on video or computer vision and has a high computing and input intensity. The human gait has behavioral influences of physical conditions, injury, and psychophysical; with extensive studies for medical uses such as the treatment of pathologically abnormal patients and none of concern for biometrics. Gait recognition has the advantages of being non-invasive, difficult to conceal, capturing capability unbeknownst to the walker and it is unlikely obscured. There are two methods to gait recognition categorization: model-based and model-free. Model-based methods use the human body structure as models and extract image features to map them into structural components of models or to derive motion trajectories of body parts. Additionally, model-based "statistical approaches have been deployed to recognize people by their walk, such as using spatio-temporal pattern, velocity moments, combining Canonical Analysis and eigenspace, static body parameters and image self-similarity. Nevertheless, model-based approach is relatively rare" [YaN02]. Model-free methods use the entire movement sequence of individuals to summarize the gait. These methods are independent of the underlying fundamental configurations. The gait biometric is an acceptable and successful biometric for identification, but has minimal acceptance [Hua01, MaM03, VeN05, YaN02].

2.2.3 Authentication Systems

Authentication accuracy and user convenience are measured by False Accept Rate (FAR) and False Reject Rate (FRR) metrics, respectively. FAR is the probability of how likely an imposter access attempt will be accepted. FRR is the probability of a likely failure by a genuine access attempt. Equal Error Rate (EER) is the point where FAR = FRR. The Genuine Accept Rate (GAR) is another commonly used metric that is the probability of a successful genuine access attempt. Therefore, $GAR = 1 - FRR$. The metrics rely on a threshold for the decision T and are labeled for a specific threshold T_1 as FAR_{T1} and GAR_{T1}. The decision threshold T can be varied, e.g., $T = T_{1,}\ T_{2,\ \ldots,}\ T_K$, and obtain multiple (K) system *operating points*. The plot of GAR versus FAR yields the Receiver Operating Characteristics (ROC) curve, which is commonly used to evaluate the performance of biometric systems. Figure 3 shows the ROC curve of a fingerprint verification system [Ulu06].

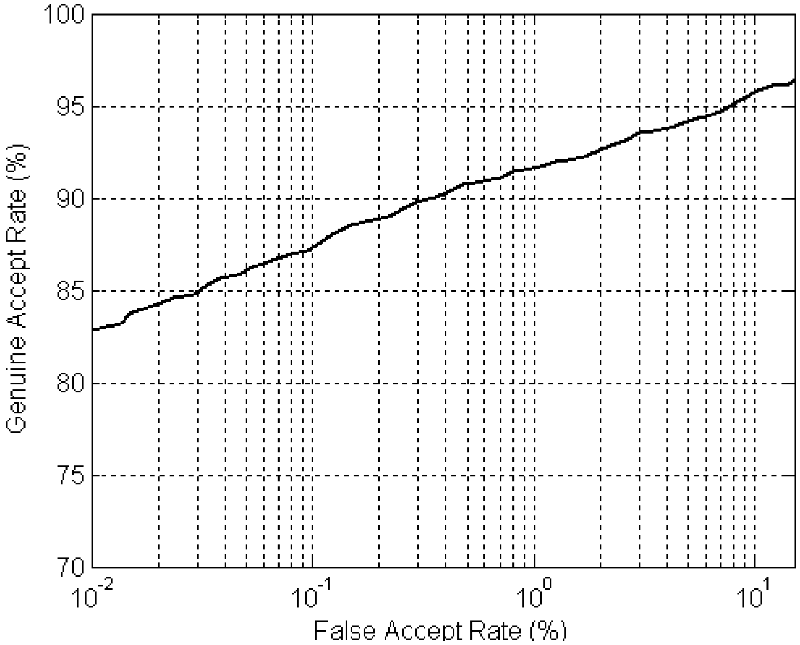


Figure 3 – Typical ROC curve of a Fingerprint Verification System [Ulu06, Woo04]

2.3 Biometric System Functions

This section covers the various functionalities that are integrated and implemented to make a biometric-based authentication system. The biometric system functions are: capture, enrollment, verification, templates, storage, and security.

2.3.1 Capture Devices

The biometric capture device for a biometric system varies depending on the modality used. Most of the capture devices use an optical system to “capture” an image of the biometric. Fingerprint biometrics use either optical, capacitance, or radio frequency scanning to capture the fingerprint features in the image. Iris/Retina biometrics use optical scanning techniques. Facial / Hand Geometry biometrics use an optical camera to capture the image. These biometrics are either physical or biological biometrics. The biometrics involving a trait or behavior use different capturing devices. These capturing devices are behavior specific. As an example, voice uses an audio recording device to “capture” the sound or key stroking dynamics uses timing patterns between selected typed letters or words [ElK04, WaJ05].

2.3.2 Enrollment

The enrollment process is used to enter an individual into the biometric system. This process may be used for authentication or identification. The biometric enrollment process requires several steps: collecting a biometric sample from an end user; converting it into a biometric reference; and storing it in the biometric system’s database for later comparison. These steps must be completed sequentially. The first step consists of using the biometric device to capture the biometric sample, such as the image of a fingerprint or iris. The next step is to process the image, extract the features, and convert the sample into a template that will be used for future comparisons. There are many different ways to create the template (see below). The last step is storing the template. There are three different ways to store the template for future retrieval. The two major template storage approaches are: 1) locally to the biometric device or local processing system; or 2) across a network in a central database server. A third option of storage is becoming popular. This option stores the template on portable storage devices such a smart card [WoO03]. There are pros and cons to each of the different storage methods due to security implications that are involved with the different storage capabilities. The enrollment steps discussed are shown in the diagram below (see Figure 4 below).

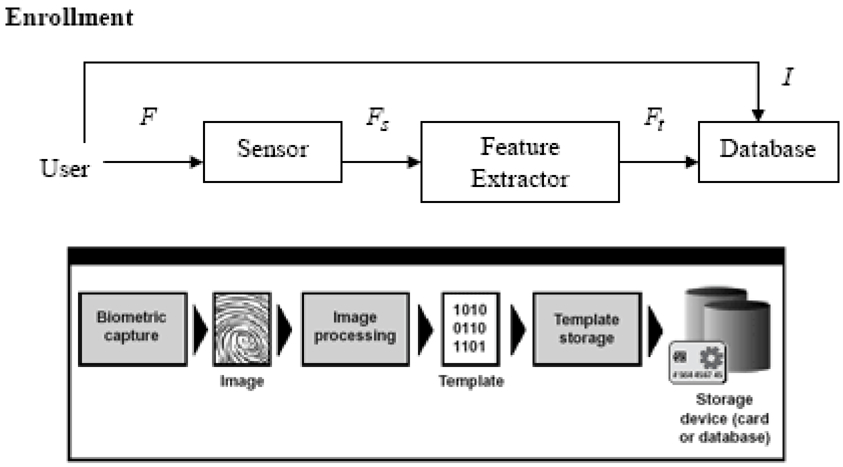


Figure 4 - Basic Enrollment Process [Ano05b, Ulu06]

The BioAPI specification (see Section 2.4.2) describes the enrollment process as a function [Ano06c]. This function captures the biometric data for the purpose of creating a biometric record for enrollment, verification, or identification (i.e., a reference template). The reference template is provided for use in creating the new template, if template updating is supported by the system. The enrollment function initializes (serializes) the sensor device, and if multimodal, then it will enroll using the first device to respond, with the other sensors waiting until the first is complete.

An example fingerprint-based enrollment: during enrollment the user presents finger *F* to the sensor with output F_s (e.g., fingerprint image) passed to a feature extractor to arrive at template F_t. With the identity *I* of the individual, it is saved in a database for future comparisons (note: see template storage below) [Ulu06].

2.3.3 Verification

The verification function captures biometric data from the attached sensor, extracts the features to create a verification template, and compares it against a reference template. The application requests a maximum false match rate (FMR) criterion (threshold) for a successful match. If using the BioAPI, the function call returns a Boolean result indicating whether verification was successful or not, as well as the FMR achieved indicating how closely the biometric records actually matched [Ano06c].

Verification is the process in which an individual claims to be an identity and that identity is then proven against necessary credentials to gain access. The verification and template comparison process is used to read in a new biometric sample. The process then compares the current sample (comparison template or temporary template) to the master template, and makes a decision to accept or reject the individual trying to gain access to resources protected by the biometrics. The current biometric sample taken typically goes through the same template creation process as the enrollment. However, it is only stored temporarily and used for comparison to the master template created during the enrollment process. After the comparison process, the current (comparison or temporary) template is discarded. The system must make a decision on the comparison to accept the current biometric sample template being offered and allow access, or to reject it and deny access. The system has a predefined threshold that determines acceptance or rejection. This threshold can be lowered, allowing for a higher acceptance and increasing the number of false accepts. Or the threshold can be raised, allowing for higher accuracy and increasing the number of false rejects. The verification process is shown below (see Figure 5) [JaB02, WaJ05, WoO03].

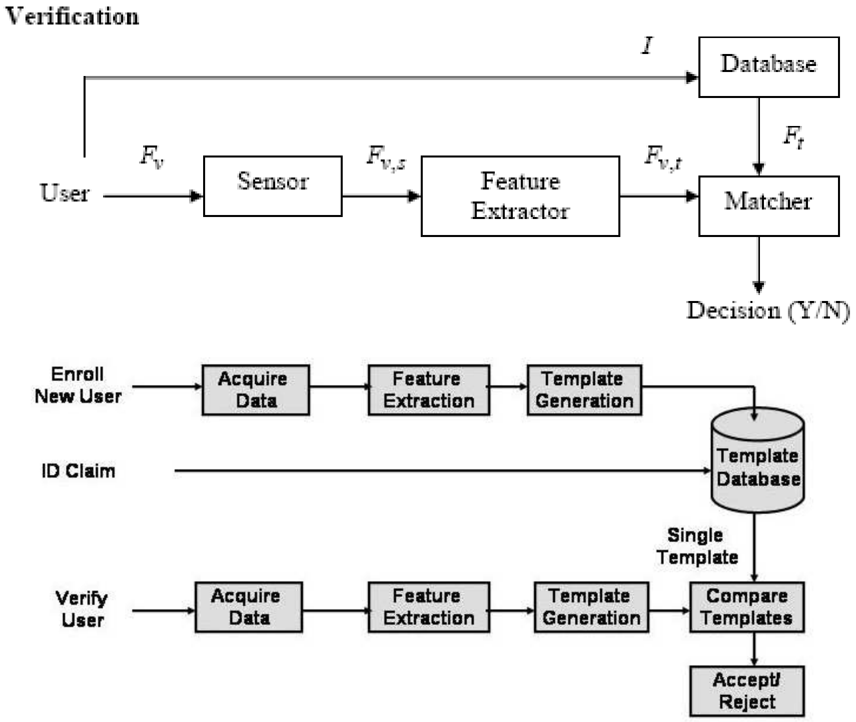


Figure 5 - Basic Verification Process [Ulu06, Woo04]

The verification problem is posed as the following equation:

$$(I, X_Q) \in \begin{cases} \omega_1 \, if \;\; S(X_Q, X_I) \geq \eta, \\ \omega_2 \, otherwise, \end{cases} \qquad (1)$$

such that claimed identity I and X_Q (the input feature vector) determine if (I, X_{Q}) belongs to ω_1 or ω_2, where ω_1 indicates that the claim is a genuine user (true) and ω_2 indicates that the claim is an impostor (false). Normally, X_Q and X_I are matched against each other, with the biometric template associated to user I to determine its category. The $\boldsymbol{S}$ function measures the similarity between X_Q and X_I, and η is a predefined threshold. Therefore, every claimed identity is classified as ω_1 or ω_2 based on the variables X_Q, I, X_I and η, and the function $\boldsymbol{S}$ [Ros03].

As an example of a fingerprint-based verification, consider the following: the user's fingerprint is captured again, and the generated template $F_{v,t}$ is matched against the retrieved database template F_t corresponding to I, the claimed identity. If these two representations are within close proximity of each other, the decision matcher outputs a “Yes" result. This decision is typically based on a (dissimilarity) similarity score or measure: if the (dis)similarity score between two representations is (lower) higher than the specified threshold T, a “Yes" decision is output, otherwise, a “No" decision is output. On the other hand, for identification, the individual's template generated $F_{i,t}$ is matched against *all* templates in the database. If matched, the provided output is the associated identity I of the individual [Ulu06].

2.3.4 Templates

Templates are small representatives of the original raw image or sample. The extracted information taken from the sample is used to build a reference known as a master template. The sample is the raw data or image that represents the applicant characteristic as captured by a system device. The image is enhanced and processed through various methods and filters (e.g. Eigenface, Gabor) based on modality. After the image has been processed, extracted features create the template. The master template is modality dependent. Features usually consist of distinct characteristics that are repeatable yet unique to each individual. It is very unlikely that any two samples from individuals are identical. For example, fingerprint features consist of bifurcations, loops, and ridge endings. Given digital compression techniques inaccuracies, results of template matching comparisons can only be expressed in terms of probability [Ano06a, JaB02, WaJ05, WoO03]. A template is created during both the enrollment and verification process. Once the master template is created, it goes through an aging process. Template aging is "the increase in error rates caused by time-related changes in the biometric pattern, its presentation, and the sensor" [Sch06]; and in which the template becomes distanced over time from enrollment [Ano06a]. Although defined, no known research investigates what happens to the comparisons between the original enrollment template and the future comparison of verification templates as individuals age over time. There have been studies to show the effects of aging on the human face, fingers, body, voice, and gait [CaM06, LaD04, LaT02, MuA04, RaC06a, RaC06b, RiB05, RiT06, VeN05]. These studies only show the effects against algorithms, they do not incorporate how the effects result in the authentication of applications or show matching scores over time.

Templates are small representatives of the original raw biometric image or sample. The biometric reference data is the extracted information taken from the biometric sample and is used to build a reference known as a master template. The stored biometric reference data is known as features. The biometric sample is the raw data or image that represents the biometric characteristic of an applicant as captured by a biometric system device. The image is enhanced and processed through various methods and filters (e.g. Eigenface, Gabor) depending on the modality being used. After the image has been processed, the features are extracted to create the template. The master template is modality dependent. The features usually consist of distinct characteristics that are repeatable yet unique to each individual. It is very unlikely that any two samples from an individual are identical. For example, fingerprint features consist of bifurcations, loops, and ridge endings. Given the inaccuracies of digital compression techniques the results of template matching comparisons can only be expressed in terms of probability. The two possible resulting criteria are: False Match Rate (FMR) and False Non-Match Rate (FMNR) [Ano06c, JaB02, WaJ05, WoO03].

Templates are "a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample" [Ano06b]. The extracted information taken from the sample is used to build a reference known as a master template. The sample is the raw data or image that represents the applicant characteristic as captured by a system device. The image is enhanced and processed through various methods and filters (e.g. Eigenface, Gabor) based on modality. After the image has been processed, extracted features create the template. The master template is modality dependent. Features usually consist of distinct characteristics that are repeatable yet unique to each individual. It is very unlikely that any two samples from individuals are identical. For example, fingerprint features consist of bifurcations, loops, and ridge endings. Given digital compression technique inaccuracies, results of template matching comparisons can only be expressed in terms of probability [Ano06c, JaB02, WaJ05, WoO03]. A template is created during both the enrollment and verification process. Once the master template is created, it goes through an aging process. Template aging is "the increase in error rates caused by time-related changes in the biometric pattern, its presentation, and the sensor" [Sch06]; and where the template becomes separated by time from enrollment [Ano06b]. Although defined, no known research has investigated the time-based validity of an enrollment template as a subject ages. There have been studies to show the effects of aging on the human face, fingers, body, voice, and gait [CaM06, LaD04, LaT02, MuA04, RaC06a, RaC06b, RiB05, RiT06, VeN05]. These studies only show the effects against algorithms, they do not incorporate how the effects result in the authentication of applications or show matching scores over time.

2.3.4.1 Template Creation

Features are used to create a biometric template. These features have different criteria which are based on the biometric modality. The following is a list of the modalities and the feature criteria used in template creation.

1. Fingerprint - Features for fingerprints include arches, bifurcations, and ridges. The fingerprint features produce complex pattern combinations of lines, arches, loops, and whorls; which is how the fingerprint is formed.
2. Facial – Features for facial biometrics use the eyes, nose, and mouth and the distances associated with each feature.

3. Hand Geometry – Features for hand geometry are the length of fingers, width of fingers, thickness of hand, size of hand, and total area.
4. Iris / Retina – The iris features include furrows, striations, pits, collagenous fibers, filaments, crypts, serpentine vasculature, rings, and freckles. The features of the retina use the patterns of the blood vessels in back of eye, which is the choroidal vasculature.

The BioAPI has a function for creating templates called BioAPI_CreateTemplate [Ano06c]. This function is used for creating templates in both the enrollment phase and verification phases. The function is described as taking a biometric record data in intermediate form for the purpose of creating a new enrollment template. A new record is constructed from a new capture, and may perform an update (if supported) based on the existing reference template, with the old template remaining unchanged [Ano06c].

2.3.4.2 Template Selection

As discussed earlier, templates are the stored feature set of the biometrics. Most systems will store multiple templates for the variations that occur in an individual's biometric template. During verification, the stored templates are compared to the presented template. In conjunction with verification, several templates are created, but only one is selected and used for this process. From the various stored templates, the biometric system needs to automatically select the template. The selection process is accomplished in one of two different methods. The two methods are called DEND, which performs clustering, and MDIST, which uses averages. The systematic template selection method resulted with improved Equal Error Rates (EER) as opposed to the templates chosen at random and template selection not used [JaU03].

The DEND method uses clustering, computes similarities of the templates, compute the average distance from the template samples, and then the minimum distance template is selected. Clustering places the images in groups that are similar to each other. From this clustering, distances between each pair can be computed. The distance scores are compared to find the minimum distance score. The minimum distance score is selected and the resulting image is used for the template.

The MDIST method uses an average distance score, computes a pair-wise distance between all images. It computes the average distance with the other images, and the smallest average distance template is selected.

One thing to keep in mind is the storage feasibility of the biometric system. Large numbers of samples per template to compute the DEND and MDIST may be computationally demanding.

2.3.4.3 Template Updating

The process by which existing templates are either replaced or modified is defined as template updating [Ano06b]. There are different ways to update templates [JaU03, KeS05, Sch06, UlR03, VeK06, YiZ05]. Additionally, the BioAPI addresses template updating by including a function call [Ano06c]. The BioAPI function defines the template update function. It provides the application with a previously enrolled or reference template for updating and instructs where a new template may be returned, if this feature is supported. This may be accomplished through newly captured biometric data to update the referenced biometric record. The update is performed to keep the enrolled record fresh and at the highest possible quality. The update is determined or defined by the biometric service provider criteria such as quality, elapsed time, and significant differences, if supported [Ano06c].

The three forms of template updating approaches are: Template Aging, Template Improvement, or Template Replacement [FrM08, UlR03]. The current research methods for template updating are: Statistical Inference, Batch Update, Augmentation Update, and Automatic Replacement [FrM08, Sch06, ScM07, UlR03]. Statistical inference is used for evaluating the significant changes in the template error rate (template aging). Two statistical inference approaches used to determine the error rate changes are: Generalized Linear Model and Likelihood Ratio Approach.

Generalized Linear Model: Evaluates whether error rates have changed linearly as measured between enrollment and return presentation of the image. The generalized linear model approach is used for assessing the covariates error rates impact. The model is: $g(\mu Y_i \,|\, t_i) = g(\pi) = \beta_0 + \beta_1 t_i$.

This allows for the question of whether or not β_1 is different from zero with a great significance which concludes “that there is a change in the log-odds of a decision error over time” [Sch06].

Likelihood Ratio Approach: Tests require the specification of a density function for data using the Beta-binomial distribution. The test “considers whether or not the error rate, π, is constant or changes over the *T* time periods” [Sch06].

Batch updating is accomplished through replacing all the current templates with the newly acquired templates from the current authentication process. During the authentication phase, there is a new set of templates that are created for comparison to the stored template. These templates are then used for the replacement of the stored templates. This process will account for changes over time that the individual's biometric traits may take place [FrM08, UlR03].

Augmentation updating is accomplished through replacing the current templates with the better of the two templates used in the current authentication phase. Both templates are considered during the authentication phase. The newly acquired template is augmented to the current listing of stored databases. Then all templates, including both the new one and the old one, are processed for template selection. The template selection process keeps the better of the two, which may be the current template or the enrollment template [FrM08, UlR03].

Automatic replacement is accomplished through replacing the templates with several well-known computer science caching fundamental concepts. The caching computer science fundamental concepts are: First-In First-Out (FIFO) – replacing the oldest template sample with the current one; Least frequently used (LFU) – replacing the template with the fewest number of authentications; and Least recently used (LRU) – replacing the template with the longest time since access. This newly acquired template replaces one of the templates maintained in the current storage listing. The old template processed for replacement is removed from the system [FrM08, ScM07].

2.3.4.4 Template Aging

Biometric template aging is the process in which the template becomes distanced over time from enrollment [Ano06b]. As discussed above, the biometric template is created during both the enrollment process and verification process. Once the master template is created, it goes through an aging process. Template aging is "the increase in error rates caused by time-related changes in the biometric pattern, its presentation, and the sensor" [Sch06]. The National Science and Technology Counsel (NSTC) Subcommittee on Biometrics define template aging as "the degree to which biometric data evolves and changes over time, and the process by which templates account for this change" [Ano06b]. Another term associated with template aging is template dormant time which is "the elapsed time between the creation, or last update, of a template and its current use" [Ano06b]. The age of the template or template maturity is also associated with "the number of biometric samples, including the original sample, contributing to the template currently on file" [Ano06b]. There is no final step or phase defined in template aging, however, the last step associated with templates is to place the biometric template into some form of storage for later access or retrieval. As defined previously, template aging is associated with changing biometric traits that vary with time or interactions with the sensor. Some examples of the biometrics traits that change or vary with time are: 1) hand – changes with growth from childhood through adulthood, as well as weight gain or loss; 2) face – changes with growth and aging; and 3) fingerprints – changes from cuts, scratching, and scaring. The effect of template aging is not consistent with all the modalities and their various thresholds. Template aging for biometric identification devices is one of importance but is lacking studies to provide large amounts of data [HaW05].

2.3.4.4.1 Template Aging Environment

Biometric template aging is the process in which the template becomes distanced over time from enrollment [Ano06b]. Although this process has been defined, no known research investigates what happens to the comparisons between the original enrollment template and the future comparison of verification templates as the individual ages over time. There have been studies to show the effects of aging on the human face, fingers, body, voice, and gait [CaM06, LaD04, LaT02, MuA04, RaC06a, RaC06b, RiB05, RiT06, VeN05]. These studies only show the effects against algorithms, they do not incorporate how the effects result in the authentication of applications or show matching scores over time. As noted previously, one of the previous facial grand challenges showed that matching algorithms had difficulty with faces that had several years of separation, again, not showing a progression of scores over time [Dau02].

There is a multitude of problem areas that are involved with the template aging environment. The first area is during the template enrollment process. If the quality of the image captured is of poor quality, this will generate a poor enrollment template [DaY06]. This could allow for a possible higher false acceptance rate into the system. One way to ensure the enrollment template is of high quality is to ensure the enrollment image capture is of the highest quality. The second problem area is due to variance in the biometric system. There is variance with regards to the sensor and the different types of sensors that are available (whether the sensor is optical, capacitive (CCD), or Infrared).

Associated with sensors is the variance in the placement of the biometric in relation to the sensor. The finger or eye may not always line up in the exact same way or orientation. The third problem area is due to variance of the environmental factors. There is variance of lighting, positioning, moisture, and cleanliness (dirt/dust/residual residues). Some sensors provide artificial lighting to minimize exposure; others provide placement guidelines to control positioning; where the skin moisture can affect image quality. Another area is related to the verification process. The problems mentioned above for enrollment also apply to verification. When combining enrollment and verification, there is a significant amount of variance that can occur that affects template aging. One way to help combat the variance is to decrease that variance over time with the correction for aging with template renewals. Finally, there are the biological aging issues. The issues associated with biological aging are facial features that change over time such as wrinkles, lines, freckles, weight, ethnicity, and gender that have an effect on the recognition algorithms. Therefore, the multitude of problem areas has an adverse effect on the enrollment and verification templates.

2.3.5 Biometric Storage Methods

Biometric template database storage takes place through different location methods, such as database (central or local law enforcement database) or a smart-card issued to an individual [Ulu06]. The four major locations are: Portable Token, Central Database, Individual Workstation, and a Sensing Device. Each storage method has privacy concerns along with associated advantages and disadvantages. The following is a summary of each associated template storage method:

1. Portable Token or SmartCard – is a credit-card like device that has a microchip with some basic functionality and memory. This is also known as a Personal Identity Verification (PIV) Card throughout the U.S. Government and described in-depth in NIST Special Publication 800-76 [WiG07]. The advantages are: the template is not centrally stored in a database, the template does not traverse the network (where it could possibly be captured), and the users have the feeling of being in control of when and where the biometric template and their personal identification is accessed. The disadvantages are the cost of implementation is higher due to additional hardware requirements and the smartcard must be read to compare to a fresh biometric scan that must be accomplished before the user is authenticated [HaH06, Pod02, Rug02].
2. Central Database/Network Appliance – is storing the biometric template in a networking environment where every user's biometric template data are stored. The advantages are: the templates are stored in one central location; allow for multiple sign-on locations without having to transport the biometric template; and allows for ease of backup. A disadvantage is the potential for a replay attack due to network traffic "sniffing" [Pod02, Rug02].
3. Individual Workstation – is where the biometric template is stored locally on the workstation that requires biometric identification and/or authentication. The advantages are: more privacy for the biometric storage preventing a single source for an attack. The disadvantages are: multiple locations are required for sign-on; multiple templates are created and may vary from workstation to workstation; and duplicates of hardware/software [Rug02].

4. Sensing Device – is the device that is used to obtain the biometric, such as a fingerprint scanner. The advantages are: provides a quicker response for authentication and/or identification; the template does not traverse the network; and the portability ease of the device to switch between networks or systems. The disadvantages are: the limited storage capacity of the sensing device; only one sign-on location; and the device could be easily stolen allowing for theft of the biometric templates that are used for authentication and verification [Rug02].

2.3.6 Security of Biometrics Systems

Biometric systems have vulnerabilities to attacks [JaR05, UmA04]. While a biometric system can enhance user convenience and bolster security, it is also susceptible to various types of threats.

2.3.6.1 Circumvention

An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can also modify sensitive data.

2.3.6.2 Repudiation

A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the system. A bank clerk, for example, may modify the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen his/her biometric data.

2.3.6.3 Covert Acquisition

An intruder may surreptitiously obtain the raw biometric data of a user to access the system. For example, the latent fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artifact of that user's finger.

2.3.6.4 Collusion

An individual with super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.

2.3.6.5 Coercion

An impostor may force a legitimate user (e.g., at gunpoint) to grant him/her access to the system.

2.3.6.6 Denial of Service (DoS)

An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. For example, a server that processes access requests can be flooded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed.

Research has identified several different levels of attacks that can be launched against a biometric system (Figure 6): 1) a fake biometric trait such as an artificial finger may be presented at the sensor; 2) illegally intercepted data may be resubmitted to the system; 3) the feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets; 4) legitimate feature sets may be replaced with synthetic feature sets; 5) the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security; 6) the templates stored in the database may be modified or removed, or new templates may be introduced in the database; 7) the data in the communication channel between various modules of the system may be altered; and 8) the final decision output by the biometric system may be overridden.

The UK BiometricWorking Group (UK-BWG) lists several factors that can affect the integrity of the template: 1) accidental template corruption due to a system malfunction such as a hardware failure; 2) deliberate alteration of an enrolled template by an attacker; and 3) substitution of a valid template with a bogus template for the purpose of deterring system functionality [JaR05].

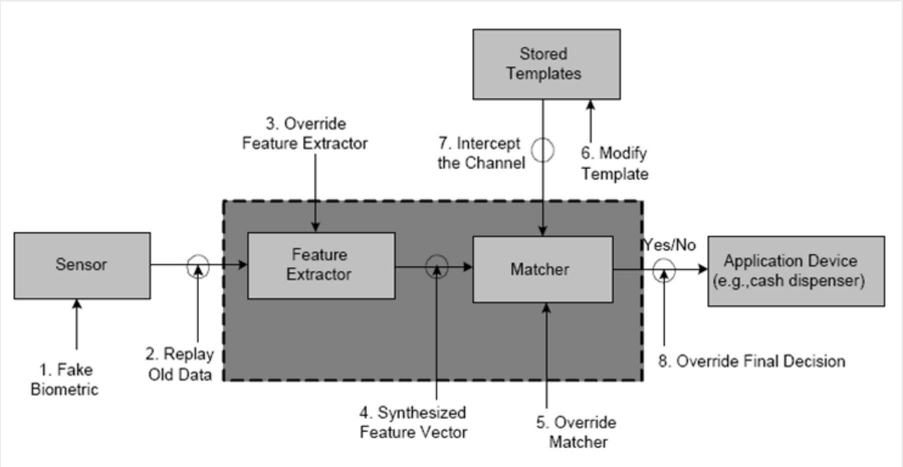


Figure 6 – Biometric Vulnerabilities[JaR05]

2.4 Biometric Standards

The biometric standards and interoperability framework models provide the ability for the collection, sharing (transmission), and storage of biometric data, as annotated in Figure 7. The biometric standards are not specific to any platform, application, or system. Standards allow for the development, interoperability, interchange, and functionality of open systems and avoid vender-specific, proprietary solutions. Examples of these specifications or standards are: Common Biometric Exchange File Format (CBEFF) [PoD01], Biometric Application Programming Interface (BioAPI) [Ano06c], and Electronic Biometric Transmission Specification (EBTS) [Ano06d, Ano06e].

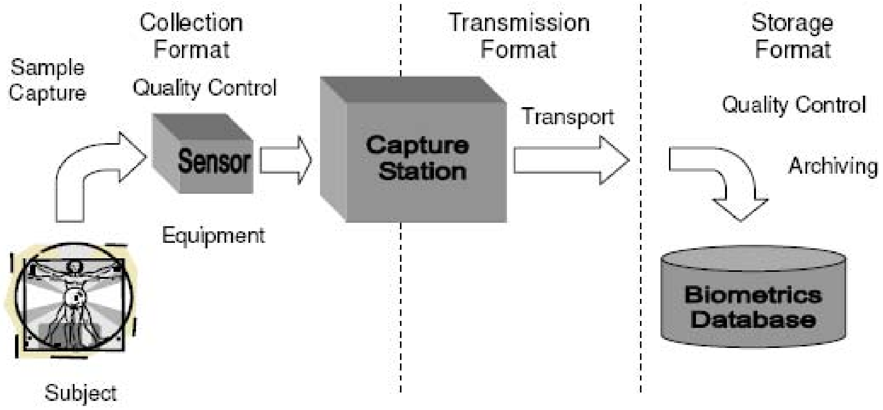


Figure 7 – Biometric Collection, Transmission, and Storage Process [HaH06]

2.4.1 Common Biometric Exchange File Format (CBEFF)

The Common Biometric Exchange File Format (CBEFF) represents a list of data elements required to universally support biometric technologies [PoD01]. The data can be placed in a single biometric file to exchange information between different biometric components or biometric systems. This promotes interoperability between biometric-based applications and systems that are developed by different vendors therefore allowing for data exchange. The CBEFF initial design was accomplished through several workshops sponsored by the National Institute of Standards and Technology (NIST) and the Biometric Consortium. The CBEFF offers future compatibility for new improvements in technology to allow for the creation of new data formats. The implementation by CBEFF allows for easier integration of hardware and software offered by different vendors. Biometric-based systems and applications will be supporting multiple biometric devices and data. The CBEFF explains a common set of data elements to assist the biometric technologies. The data is placed in a single file and is exchanged between various components and systems. The benefits of CBEFF are the ability to: 1) identify different biometric data structures supporting multiple biometrics within an application or system; 2) reduce the need for supplementary software development; and 3) support cost savings throughout development. The adoption and compliance of the CBEFF allows for interoperability of biometric systems and applications produced by a mix of vendors. Current progress in the industry is seen through specifications such as the BioAPI [Ano06c] and the X9.84 ANSI standard on Biometric Information Management and Security [Ano3]. The CBEFF uniqueness advances interoperability between different biometric systems, allocates for the sharing of biometric data between various systems, and tolerates systems with different requirements to decipher various formats [PoD01].

2.4.2 Biometric Application Programming Interface (BioAPI) Framework

The Biometric Application Programming Interface (BioAPI) has two versions currently in use [Ano01b, Ano06c]. Version 1.1 is in use in the United States and was the proposed standard from the American National Standards Institute (ANSI). Version 2.0 has been published jointly by the International Standards Organization (ISO) and International Electromechanical Commission (IEC) as ISO/IEC 19784-1. Version 2.0 has improvements and allows for multiple biometrics. The ISO/IEC 19784 BioAPI specification is suited for most forms of biometric technology and provides a high-level generic biometric authentication model.

The BioAPI is the interface between the biometric technology and its applications. The BioAPI specification supports interoperability by allowing applications to communicate in a universal way to a wide variety of biometric technologies. The BioAPI is an “open systems’’ specification. This allows for: 1) easy integration and exchange among multiple biometric technologies using the same interface; 2) numerous application usage across biometric technologies; and 3) development of applications are quick increasing competition and reducing expenses. The BioAPI is designed for handling a wide variety of applications from a full-scale national ID system to an embedded cell phone device, on top of authentication for user applications related to computer and network access [Ano06c, Pod02].

As mentioned earlier, the BioAPI is appropriate for most forms of biometric technology offering a high-level general biometric authentication model without specific support for multimodal biometrics. The BioAPI is an architectural model enabling biometric system components provided by various vendors to work together through the Application Programming Interface (API). One key feature of the framework is the BioAPI Framework, which supports calls by application components using the BioAPI specification. The framework of the BioAPI provides support through a called Service Provider Interface (SPI) to the different vendors’ Biometric Service Provider (BSP) components, as required by an application. The hardware and software performs capture, matching, and archiving of biometric functions at the lowest levels. The BioAPI Units of the architecture are integral to a BSP or supplied as a separate BioAPI Function Provider (BFP) component. As long as data structures conform to International Standards, interactions between various vendors' BSPs can take place through the BioAPI Framework. The last part of the BioAPI architecture is that the BSP can provide biometric services in two ways. First is through Units of the BioAPI that are integral or managed by the BSP; and secondly by calling components integral to the BFP through the BFPI (BioAPI Function Provider Interface). The BioAPI Units contain biometric sensor, algorithms, or archives that may consist of software, hardware and/or a combination. The Units can be dynamically added or deleted from the system for each type of supported BSP or BFP, generating signaled events to an application through the BSP and BioAPI Framework. An overview of the BioAPI can be seen in Figure 8.

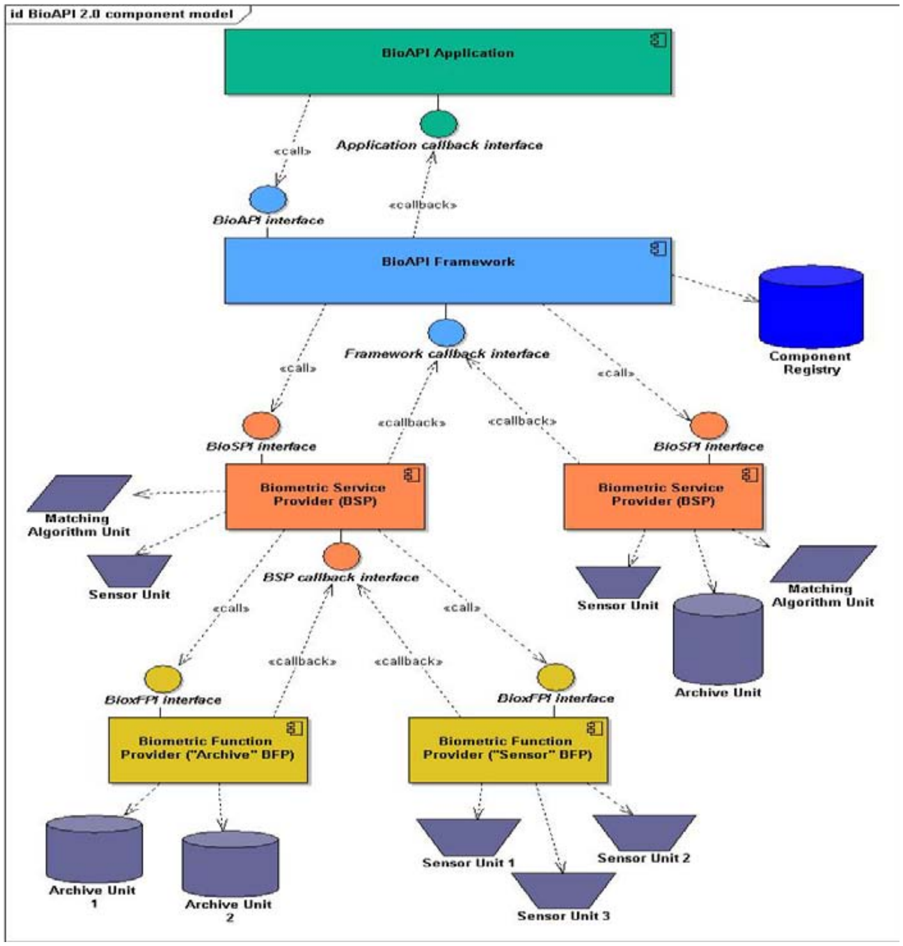


Figure 8 – BioAPI 2.0 Standard [Ano06c]

The BioAPI specification covers the simple biometric functions of Enrollment, Verification, and Identification. This includes a database interface that allows applications to manage biometric records storage through an archive BioAPI Unit that is controlled by a BSP or BFP. This allows for the biometric system performance to be optimized for archiving and searching processes. The application interface provides primitives that allow managing the capture of biometric samples by accessing the corresponding BioAPI Unit sensors and using Enrollment samples and subsequent Verification or Identification against those stored records.

Several function calls included are:

- **BioAPI_CreateTemplate**: This function takes a BIR containing biometric data in intermediate form for the purpose of creating a new enrollment template.
- **BioAPI_VerifyMatch**: This function performs a verification (1-to-1) match between two BIRs: the ***ProcessedBIR*** and the ***ReferenceTemplate***.
- **BioAPI_Enroll**: This function captures biometric data from the attached device (sensor unit) for the purpose of creating a ***ProcessedBIR*** for the purpose of ***BioAPI_PURPOSE_ENROLL***, ***BioAPI_PURPOSE_ENROLL_FOR_VERIFICATION_ONLY***, or ***BioAPI_PURPOSE_ENROLL_FOR_IDENTIFICATION_ONLY*** (i.e., a reference template).
- **BioAPI_Verify**: This function captures biometric data from the attached device (sensor unit) and compares it against the ***ReferenceTemplate***.

The BioAPI also returns a quality score of images used for templates. The quality scores range from 0 to 100 and are divided into categories. The first category is UNACCEPTABLE with a range of 0 to 25. If the images fall in this range, then it can not be used for the purpose specified by the application and needs to be replaced using additional biometric samples. The second category is MARGINAL with a range of 26 to 50. For this category, the image will have poor application performance and possibly compromise the application's intent. The third category is ADEQUATE with a range of 51 to 75. This category provides a good application performance but may require a higher quality if the application requires significant use. The final category is EXCELLENT and is in the range of 76 to 100. The biometric data in this category will provide good performance for the specified application [Ano06c].

2.4.3 Electronic Biometric Transmission Specification (EBTS)

There are two versions of the Electronic Biometric Transmission Specification (EBTS) [Ano06d, Ano06e]. The first specification is developed by the Federal Bureau of Investigation (FBI). The second specification is a variant of the one developed by the FBI to be used for DoD developers.

2.4.3.1 FBI Electronic Biometric Transmission Specification (EBTS)

The FBI has developed a standard for transmitting and encoding electronically the arrest data, identification, and fingerprint image in support of the development of the Integrated Automated Fingerprint Identification System (IAFIS) and recommendations from the National Crime Information Center Advisory Policy Board Identification Services Subcommittee. This standard was originally directed to define the content, format, measurement units, and a common interface for exchanging information. It is used in subject fingerprint identification between worldwide criminal justice organizations and administrations using AFIS. The Electronic Fingerprint Transmission Standard (EFTS) was developed from the ANSI/NIST-ITL-2000. This led to the development of the FBI's EBTS, derived from the ANSI/NIST-ITL-2007 and replaced the FBI EFTS. Revisions have included additional biometric modalities of palm, facial, and iris. Future revisions will incorporate requirements for Logical Records within the

ANSI/NIST-ITL-2007 standard and a capability to facilitate multi-modal biometrics and a complete biometric and biographic profile of the subject records [Ano06d].

2.4.3.2 DoD Electronic Biometric Transmission Specification (EBTS)

The DoD customized the Electronic Fingerprint Transmission Specification (EFTS) from the FBI. The customizations are necessary to utilize the Automated Biometric Identification System (ABIS) specified by the DoD. The DoD ABIS combines applications and databases to support storage, retrieval, and searching of fingerprints. The ABIS also includes additional biometric modalities of face, iris, and voice. It also maintains compatibility and compliance with the FBI EFTS and EBTS. The DoD's version includes additional transaction types and code requirements beyond those defined in the EFTS to handle different encounters and detainment circumstances. This specification is primarily for developers and support systems that interface with the DoD ABIS. Knowledge of the EFTS and ANSI/NIST-ITL 1-2000 is expected. The specification addresses the transactional functionality necessary for interfacing with the DoD ABIS. Future versions will be compatible with ANSI/NIST-ITL 1-2000 and ANSI/NIST-ITL-2007 revisions and may include additional functionality areas of iris, face image, voice samples; support for submittal, storage, and searching of CBEFF information. Support for ANSI/INCITS standards-based biometric formats and for Web services / XML encoding will be needed [Ano06e].

2.4.4 Defense Biometric Identification System (DBIDS)

The Defense Biometric Identification System (DBIDS) is a security and identification system that is configurable to enhance security and safety through accurate identification and access with a centralized biometric information database. The DBIDS system is a rules-based access verification system that produces identification cards. The DBIDS has provided security at access control points by assigning rules governing installation access and by registering users into a database with personal information, photographs, and 2-print fingerprints.

2.5 Biometric Aging and Prediction

This section reviews the latest prediction models and template aging research in the facial modality. Currently there is no known research in the other modalities in regards to prediction models nor template aging.

2.5.1 Facial Aging Models

Although facial recognition and biometric algorithms have improved, template aging and aging prediction is still an open research area [RiB05]. As mentioned above, the biometric template is created during the enrollment, identification, and verification processes. Once the master template is created, it begins an aging process. Currently there is no final step in the template aging process. The biometric template is usually placed in some form of storage for future retrieval. The template aging is associated with the changing biometric traits that vary with time or interactions with the sensor. Some examples of the biometrics traits that change or vary with time are: 1) hand – changes with growth from childhood through adulthood, as well as weight gain or loss; 2) face – changes with growth, weight gain or loss, and aging; and 3) fingerprints – changes from cuts, scratching, and scaring. The effect of template aging is not consistent across all modalities and their various thresholds. Template aging for biometric identification devices currently lacks extensive research to provide large amounts of data [HaW05].

Human aging is beginning to be addressed in biometrics and its effects on facial recognition. Research is addressing the facial changes and how it the facial recognition algorithms are affected. Research is addressing how the face ages to aid Agencies in finding missing people or assist in the capture of criminals [RiB05].

2.5.2 Facial Aging Prediction

Facial aging is a growing research area [LaT02, MuA04, RaC06a, RaC06b, RiB05]. Research is being conducted on automating facial aging. The aging of the face is being used to assist forensics in Missing Children Agencies, Law Enforcement Agencies, Department of Defense, and Homeland Defense. This is accomplished by taking an image of the individual and adding features such as wrinkles, freckles, sagging skin, or removing of hair and color (graying) [MuA04]. This was initially accomplished by a “forensic artist” using computer-aided software (i.e. Adobe Photoshop) and pictures from family members, if available [LaT02]. Research is progressing to make the “forensic artist” interpretations performed automatically through aging algorithms by the software [LaT02, RaC06a].

2.5.2.1 Facial Aging Research

Automatic facial aging techniques are currently being research at the University of Kent, United Kingdom, and University of North Carolina, Wilmington [HiS05, RiB05]. At the University of Kent, research focuses on automatically progressing the appeared age of the face through the use of software by statistical calculations of faces over time [HiS05]. At the University of North Carolina Wilmington, Dr. Eric Patterson and Dr. Karl Ricanek, Jr. are conducting research on automatically progressing the age of the face. Dr. Patterson is researching 2-D images and 3-D facial models to include facial expressions. Dr. Karl Ricanek, Jr. is researching facial age progression and building a database of facial images over a time span of years. The database is called MORPH and maintains images of individuals spanning several years of age progression. The database contains a minimum distance of 46 days, a maximum of 29 years, and an average of eight years on successive images. The research is still ongoing with no definitive application produced [RiB05, RiT06]. Another area of research is on the synthesis of facial aging by the isolation of the wrinkles, freckles, and spots associated with the face and aging [MuA04]. Other areas of concern that need to be addressed in the facial aging are if the individual is a smoker, amount of sunlight, region, and lifestyle since all these factors influence on how a person ages [TaS00].

2.5.2.1.1 Facial Aging Approaches

There are a couple of approaches to automatic face aging. The first method uses statistics. This method of facial aging uses a statistical approach of modeling faces from childhood into adulthood. This is accomplished through statistically modeling the changes and applying that differential rate of change to the regions that grow. The shape is modeled by placing landmarks onto the face using a coordinated system for each face, and includes adding wrinkles, changing the coloring of the hair, and adding lines in strategic locations such as the forehead, eyes, or chin [HiS05, MuA04].

The second method uses linear transformations. This approach uses a transformation formula and applies it to features of the face to show aging and growth. The transformation formula models a growth pattern and ratios of expansion on the craniofacial regions from adolescence to adult [RaC06a].

2.5.2.1.2 Facial Aging Software

The software used to predict facial aging varies both in usage and the application. The software is used by a "forensic artist" to create a facial image and then apply aging techniques. Adobe Photoshop is a popular application used by "forensic artists" to show aging and used by the National Center for Missing and Exploited Children and the Federal Bureau of Investigation (FBI) to aid in finding missing people [Lof07, Tai07]. The aging is accomplished by gathering photographs from family members to evaluate the family's aging and apply that to the missing person's photograph. Table 1 below gives a list of applications, a brief summary of the software, and location on the web.

Table 1 – Facial Aging Software

SOFTWARE APPLICATION	DESCRIPTION	WEBSITE
Adobe Photoshop	Software used to manually perform aging using artist techniques and photos from family members to identify the aging process	http://www.adobe.com
April Age	Statistically based age progression software using wrinkling/aging algorithms are based upon ages, ethnicities, and lifestyle habits. Images can be adjusted to compare aging (smoker vs non-smoker; added excessive weight sun exposure)	http://www.aprilage.com
FACETTE	German software program used for creating facial sketches from scratch for identifying criminals and crime solving purposes	http://www.facette.de/eng/
Faces	Program used to create facial sketches or images to aide in the identifying of criminals	http://www.iqbiometrix.com/
EFIT	Computer-aided composite system for assisting detectives in creating faces	http://www.efitforwindows.com

2.5.3 Facial Recognition Algorithms

The algorithms used for facial recognition varies significantly. Many of the facial recognition algorithms are proprietary to the company that owns them. One algorithm is Verilook by Neurotechnologija [Neu07]. The Verilook face recognition algorithm implements advance face localization, enrollment, and matching using digital image processing algorithms. The features generalization mode produces the collection of the generalized face features from several images of the same subject. Each face image is processed, features extracted, and the collections of features are analyzed and combined into a single generalized features collection. The enrolled feature template is more reliable and the face recognition quality increases considerably. Another algorithm is FaceVACS by Cognitec [Cog07]. The FaceVACS face recognition implements a face tracker interface to find the human face and eyes in images, and supports enrollment, verification, and identification using the latest algorithms for performance. The features include characteristics of portrait images such as red eye, reflection on face, and uniform lighting, or suitability for photo-id card documents.

Three algorithms that have high levels of performance and were tested during the FRGC are: 1) Semi-Naïve Bayesian Classifier; 2) a type of neural network called SNoW; and 3) a cascade of classifiers [BeA07]. The Semi-Naïve Bayesian Classifier is based upon the research by Schneiderman at Carnegie Mellon University [ScK04]. The essential idea is to find modest sized clusters of low-level image features that have highly correlated class dependent statistics. The SNoW classifier is based upon an algorithm highlighted in a survey of face detection algorithms presented by Yang et al [YaD02]. It is based upon a Sparse Network of Winnows (SNoW) learning architectures with single layer neural network with binary input units. SNoW develops a decision rule from a weighted rule from a weighted sum of observed binary features. The cascade classifier is based upon the work of Viola and Jones [ViJ04]. It is based off weak classifiers and will outperform single, stronger classifiers. The cascade is a serial arrangement of weak classifiers.

2.5.4 Best Practices Summary

In determining performance of biometric devices, a framework performance report provides guidelines for conducting technical performance testing of a system to field a performance estimation [MaW02]. This performance estimation can be used and applied to aid in determining or solving template aging.

Template aging prediction can be conducted using estimates of variance in performance measures monitored over a time period. The variance is a statistical measure of uncertainty, and can be used in estimating confidence intervals. The performance estimates are affected by systematic (test bias) and random errors (natural variation). The uncertainty arising from random effects are reduced as the test size increases and estimated from collected data. There are some assumptions in the distribution of matching the formula estimating the variance of performance measures. These assumptions are: volunteer is a representative of the target population; different subject collection attempts are independent; attempts are threshold independent; error rates vary with population; and observed errors are not too small [MaW02].

2.6 Summary

This chapter provides an in-depth look at the current state of biometrics, biometric systems and their components, standards, and biometric template aging. The first area discussed utilization of biometrics followed by the different modalities used by biometric-based systems. This was followed by the biometric standards in use today followed by facial prediction models. Finally, facial aging research, facial recognition algorithms, and best practices germane to the focus of this research were addressed.

III. Methodology

3.1 Chapter Overview

This chapter presents the methodology for the development of the Carls Template Aging and Renewal Prediction Framework (CTARP Framework), a novel template aging and renewal framework for a biometric-based verification system. The CTARP Framework addresses the paucity of template aging research, namely the lack of prediction of template renewal. This chapter begins with the motivation for developing the CTARP Framework. The validity to utilize template renewal preditions is presented, along with its practicality. Next, the development of the Carls Template Aging and Renewal Prediction Framework is presented followed by a detailed discussion of the modeling and simulation environment, along with the descriptions and specific parameters for each of the developed prediction algorithms. The metrics collected and analyzed are defined in this chapter as well. The chapter concludes with model verification and validation.

3.2 CTARP Framework Motivation

There are still a number of intrinsic drawbacks in biometric systems. One is that there is a need for solving the aging issue in today’s biometric systems. There is not a known and developed strategy for aging and renewal. Current approaches are incomplete and simplified towards a means of measuring biometric template aging and renewal prediction. The research performed to date surveys the historic and state of the art in biometric systems, aging, recognition algorithms, and modalities, which suggests a real potential to model and measure template aging and renewal prediction through statistical methods. Among the developed techniques for biometric recognition, the facial recognition is the most promising and interesting modality in regards to aging. Out of the evolution of a time domain, a framework can be developed and applied to all biometric modalities. This research is not about devising a new algorithm or determining potentials and limitations of existing techniques, but of improving error rates and the exploitation of the time dimension.

There are two extreme approaches to template renewal due to aging: 1) Continuous and 2) Static. The first approach is costly and does not guarantee improved error rates. The second approach is conservative and can lead to unacceptable error rates over an extended period of time. The continuous method is to renew the template with every opportunity therefore preventing template aging from occurring. This becomes costly due to the resources required for continuous enrollment demanded of the system. This method provides the most current template available to the system for verification. However, the new template is not guaranteed to provide the best scores because the image used to generate the new template could have less quality resulting in poor future matches. The static approach is not costly but will eventually result in unacceptable or higher error rates through increased FRRs. This method creates a template during enrollment and never updates the template. Over time the system may be unable to verify the identity thus preventing access to resources, therefore forcing a re-enrollment. These methods of template renewal do not deal with trying to provide the optimal time to change the template. In fact, “the face status at a particular age will affect all older faces, but will not affect those younger ones” [GeZ07]. The goal is a deterministic prediction that it is now time to change the template due to aging, not because the individual is being falsely rejected.

Although facial recognition and algorithms have improved, template aging and aging prediction is still an open research area. Human aging is beginning to be addressed in biometrics and its effects on facial recognition. Research is addressing the facial changes, how the facial recoginition algorithms are affected, and how the face ages to aid in finding missing people or assist in the capture of criminals. Three unique features that are in contrast to other variations of the face are: the uncontrollable aging progress; aging patterns are personalized; and the temporal data of aging patterns must obey the order of time [GeZ07, RiB05].

3.3 Template Aging and Renewal Prediction Validation

The biometric template aging and renewal process is a difficult problem. Further research is still needed in the area of the exploitation of the time dimension. "It has been noted that for images taken at least 1 year apart, even the best face recognition algorithms have error rates from 43% to 50%" [Dau02]. The improvements made over the last several years have improved the success rate of recognition algorithms, increasing from 80% to 98% [PhS07]. However, this improvement is for controlled image settings and does not include time factors. Gait biometric recognition algorithms suffer similarly as their performance has been shown to drop significantly from 82% to 6% over an interval of 6 months [VeN05]. To improve facial recognition algorithms, the U.S. Government has established research challenges [PhG03a, PhG03b, PhS07]. These challenges are designed to have various academia and venders test their algorithms against one another to see which performs the best. The face recognition challenge started with the FERET database in 1993 with six competitions over the last 13 years. The latest two being the Facial Recognition Vendor Test (FRVT) 2006 and the Facial Recognition Grand Challenge (FRGC) 2006 [PhS07]. Other biometric challenges sponsored by the U.S. Government include the Iris Challenge Evaluation (ICE) 2006, the Fingerprint Verification Competition (FVC) 2006, and the Fingerprint Vendor Technology Evaluation (FpVTE). These competitions are aimed at improving algorithms, performance, and matching. However, there is still a research gap that needs to be filled. The competitions do not cover the entire aspect of biometrics, and one of primary importance - time. This gap is a fundamental component to biometric template aging and the foundational framework for a template aging and renewal process. This research is not intended to improve upon or develop a better algorithm for any biometric modality or multi-modality, but to develop a new framework that will define the biometric template aging and renewal process, whether it is single or multi-modality. This template aging and renewal framework will aid in improving the overall biometric system's false acceptance and false rejection rates.

Biometric modalities are continuously being researched and developed to improve their algorithms, sensors, and systems. But there is a need for statistically reliable estimates to determine template aging and renewal prediction. The one area that is missing from the improvements is an aspect of time and aging. With the fusion of time into the biometric system, this will impact and enhance the overall system performance providing a greater robustness for that biometric modality. This time relation is one intrinsic drawback in the biometric techniques that have not been pursued to date. Part of the reason is the lack of data sets to support a longitudinal study over any great length of time.

3.4 CTARP Framework Development

This section presents the strategy for developing the framework and for modeling the effects of template aging and renewal prediction. This effort is comprised of three stages: adopt an architecture to provide as the baseline model; enhance this generic baseline framework by adapting improved relevant portions of the frameworks; and finally, demonstrate the expected increase in efficiency and overall system performance through simulation and analysis.

3.4.1 Framework Architecture

This section documents the methodology for determining template aging and template renewal prediction. Accomplished first is the function of matching, specifically facial matching. The matching provides a basis for establishing the element of template aging. Template renewal prediction is implemented through the element of template aging. These elements and functions molded together provide a novel framework of template aging and renewal prediction christened as the Carls Template Aging and Renewal Prediction (CTARP) Framework.

3.4.1.1 Facial Matching

The facial matching framework used to demonstrate template aging is one specific modality. Exploited are the commercial facial algorithms in the testing conducted on the publicly available ND ‘B’ and MORPH facial datasets [FlB07, Ric07].

3.4.1.2 Template Aging Framework

The elemental template-aging framework demonstrates facial aging over time. This is only in one specific modality; however, it provides the foundation for all modalities. The publicly available ND 'B' and MORPH facial datasets provide statistically sufficient data to emulate the aging process. These databases aid in establishing trends related to facial aging and in addition, a relation to biometric template aging. The template-aging framework gives an initial baseline framework to base future metrics and tests to be conducted on other modalities.

3.4.1.3 Renewal Prediction Framework

The template renewal prediction framework provides predictions to future template scores which are utilized to determine if or when templates should be renewed on the next verification. This aids in establishing trends for renewals related to biometric template aging. The renewal prediction framework gives an initial baseline architecture to base future metrics and tests to be conducted on other modalities.

3.4.2 Establishing the Framework Architecture for Authentication

The final element of the CTARP Framework is composing the overall structure and then to demonstrate performance and its improvements. This is demonstrated through simulation of the CTARP Framework utilizing software. Specifically, the framework methods are used to build the architecture from face recognition database matching score outputs to predicting when it is time to renew the template to improve error rates.

3.5 Modeling Template Aging

This section discusses the developed and evaluated strategy for modeling the effects of template aging, as it pertains to given match scores. The template aging process is a difficult problem to address specifically since the effects of template aging spans across all modalities to various degrees. Since faces tend to change rapidly compared to other modalities [Dro06], face was chosen as an initial focal point of this research. Modeling template aging is performed through utilizing publicly available facial data sets that extend over a period of time, usually greater than eighteen months of time from first picture to last picture. Every capture attempts to maintain pose, lighting, and facial expressions as similar as possible.

3.5.1 Public Data Sets

For testing, two publicly available databases are used. The Notre Dame Collection ‘B’ database (ND ‘B’) [Fly07] and the MORPH database [RiT06] are used in the experiments. The two data sets were chosen due to the ability to represent individual subject aging over an extended time span. Not all database subjects had images spanning an extended period of time. Therefore, only subjects that have 14 or more time-separated images are used to simulate changes over time. The initial reasoning behind using 14 images as a minimum is this provided the maximum number of subjects available for testing based on the modes of the databases. The mode of images for ND ‘B’ is 17 and MORPH is 14. This initial number proved to be insightful and accurate, as most subjects tested showed match scores falling below the system default threshold after 14 images on average, as discussed in Chapter IV. The ages and separation of time between images in the databases are unevenly distributed in wide ranges. The distribution statistics, number of subjects, and images used are tabulated in Table 2. Besides the aging, most sequences display other variations in pose, illumination, expression, and occlusion. Although these variations may be detrimental, all images are used in the experiment because deficiency of data is a more serious problem. There are over 27 publicly available facial databases for testing [Gro05]. Only the databases in Table 2 had a sufficient minimum time span between the first image and last image of more than one year to show aging. Subjects selected from ND 'B' averaged approximately 25 images with a maximum of 42. Subjects selected from MORPH only averaged approximately 19 images with a maximum of 53 for one individual.

Table 2 - Database Statistics

Database	ND 'B'	MORPH	FG-NET
Minimum Age (Years)	Not Available	15	0
Maximum Age (Years)	Not Available	68	69
Average Age (Years)	Not Available	27	16
Minimum Span Between Images	7 Days	46 Days	365 Days
Maximum Span Between Images	386 Days	29 Yrs	18 Yrs
Average Span Between Images	14 Days	8.6 Yrs	2.5 Yrs
Subjects	334	515	82
Subjects Used	77	70	0
Minimum Images per Subject	14	14	6
Maximum Images per Subject	42	53	18
Average Images per Subject	25	19	12
Mode of Images per Subject	19	14	13

3.5.1.1 Notre Dame Collection 'B' Public Dataset

The Notre Dame Collection B (ND 'B') is a subcomponent of the University of Notre Dame Biometrics Database Distribution (ND BDD) available through the Computer Vision Research Laboratory (CVRL) [Fly07]. The ND BDD consists of 23 different biometric modality data sets of face, hand, and ear captured with different sensors, angles, lighting and dimensions. The modality data set is called a component. There are various modal components grouped together as collections. ND ‘B’ dataset consists of frontal images comprised of components 1, 4, and 8 from the University of Notre Dame Biometrics Database Distribution. ND ‘B’ contains 32,247 face images from 334 subjects. Subjects were photographed with a high-resolution digital camera under different lighting and expression conditions. Many subjects were photographed every week for 10 weeks in Spring 2002, 13 weeks in Fall 2002, and 15 weeks in Spring 2003. Hence, this database provides a significant amount of 'repeat data' to assess performance of systems with respect to time elapsed since enrollment [FlB07, Fly07]. Table 3 below displays each of the components details.

Table 3 – ND ‘B’ Dataset

CompID	Period	Modality	Sensor	Angle	# Subjects	# Images	Size
1	Spring 2002	Face	Visible	frontal	82	3387	3.2 GB
4	Fall 2002	Face	Visible	frontal	333	12004	13.8 GB
8	Spring 2003	Face	Visible	frontal	334	17856	34.9 GB

3.5.1.2 MORPH Dataset

The Craniofacial Morphology Database, referred to as MORPH, is maintained by the University of North Carolina at Wilmington [RiT06]. In the MORPH database, there are 1,724 face images from 515 subjects. The database maintains images of individuals spanning several years of age progression. The database contains a minimum distance of 46 days, a maximum of 29 years, and an average of eight years on successive images.

These images represent a diverse population with respect to age, gender, and ethnicity. There are 1,278 images of individuals of African-American decent, 433 images of individuals of Caucasian decent and 3 images classified as other. There are 294 images of females and 1,430 images of males. For the male images, 76 percent have some form of facial hair. The average age of the individual at the time of acquisition is 27.3 years, with a standard deviation of 8.6 years. Maximum age is 68 years. The average maximum age span of the images is 8.6 years, based on the age difference of the first enrolled image and subsequent images. The minimum span between images is 46 days with a maximum of 29 years. Each subject's images were cropped about the face and have different lighting and expression conditions [Ric07, RiT06]. Hence, this database provides a significant amount of 'repeat data' to assess performance of FR systems with respect to time elapsed since enrollment.

3.5.1.3 FG-NET Dataset

Although discussed, the FG-NET Aging Database [LaC07] was not utilized in the experiments due to its lack of sufficient subject samples. The subject ages in the database are unevenly distributed in wide ranges from 0 – 69. The maximum number of images from an individual is 16. On average, there are 13 images per individual. Not utilizing images of an individual under age 18, there was an average of 7 images per individual left for testing. This is below the set limit required for CTARP Framework simulation of facial aging. The defined number of images required for CTARP is 14, which is the baseline number of images where the average match score falls below the default match threshold. Although this database provides a significant amount of 'repeat data' to assess performance of face recognition systems with respect to time elapsed since enrollment, it is limited by the age of the individual in the images.

3.5.2 Algorithms / SDKs

Two commercially available algorithms and associated software development kits (SDK) are used for testing. The vendors' algorithm software packages/SDKs are PC-based facial recognition technologies. Both algorithms/SDKs are camera independent, webcam capable and offer a set of programming samples and tutorials written in major programming languages, such as C++ or .Net [Cog07, Neu07]. The first software package used for this experiment is the VeriLook 3.0.1.0 Standard SDK by Neurotechnologija, Inc [Neu07]. The second software package used for this experiment is the FaceVACS 6.3.0.0 Standard SDK by Congnitec Systems, GmbH [Cog07].

3.5.3 Score Matrix

There are two matrices of scores used. The first is called the "Perfect Match Scores Matrix" (PMSM). The second is called the "Error Scores Matrix" (ESM). The PMSM and ESM are published in [CaR08] and described below. The PMSM has 1's on the diagonal, where the ESM has 0's on the diagonal, as explained below. The matrices are an integral part of the CTARP Framework and used in the predictions of match scores and renewals.

3.5.3.1 Perfect Match Score Matrix

A matching function maps a query image to one that represents its identity and then returns a probabilistic score of likeness. In the facial matching system, the gallery set is denoted as $G = \{g_1, g_2, ..., g_n\}$, consisting of n gallery images whose identity is known to the algorithm. The query set is denoted as $Q = \{x_1, x_2, ..., x_m\}$, consisting of m query images whose identity is unknown to the algorithm. A face matching algorithm measures the relationship between the query image and each gallery image. For rank k matching, the system outputs a file of gallery images corresponding to the k top matches [WaJ07]. In this study, k is defined as $k = m = n$, which is the number of images in the gallery, therefore matching all images.

The "perfect match" (PM) is similar to the "perfect recognition" described by [WaJ07], although no sorting is performed on the results. The matching score is symbolized as $M(x_i, g_j)$ or $M(i, j)$, for the comparison between the query x_i and the gallery g_i, where higher matching scores represent better matches, or, less aging. In the testing and analysis, all the gallery and query images used are of the same individual over an extended timeframe. The matching scores of a query image x_i are ordered historically from oldest to newest by the image date, building the matrix row by row. The returned matching scores are in the range $[0,1]$; thus the matching scores in the gallery and query images can be compared. With PM, the gallery set G is the query set Q such that $Q = G = \{g_1, ..., g_n\}$. The PM uses the identical set for matching, and obtains scores of each query image $PM : M_i = \{M(g_i, g_1), M(g_i, g_2), ..., M(g_i, g_n)\}, i = 1, ..., n$. The result of the query matches is a matrix with 1's on the diagonal. This is called the "Perfect Match Scores Matrix" (PMSM).

The PMSM is derived by matching the images of the same person over the aged images. The oldest image is enrolled into the system to create the master template. The master template is then compared against all other images. This creates the first entry row in the matrix. Then that image is un-enrolled and the second oldest image is enrolled into the system to create the master template. That template is then compared to all the images. This is repeated for all images in G. This results in PM, a square matching score matrix with a PM score of 1's on the diagonal. Table 4 is a partial PMSM. Note of interest: the matrix is not symmetrical for one of the algorithms. An example from Table 4: Row 1, Column 3 (Image 118 vs. Image 128) match score (0.949) is not equal to Row 3, Column 1 (Image 128 vs. Image 118) match score (0.964) although they are the same images. This is opposed to a symmetrical matrix generated by the other algorithm. The asymmetric nature is believed to be due to how the images are processed by the different algorithms by methods such as principle component analysis (PCA), independent component analysis (ICA), or linear discriminant analysis (LDA), although the underlying facial recognition algorithm is not revealed by the commercial vendors. The first algorithm uses the real-time raw image for enrollment and verification. The second algorithm uses a static converted raw image; a digital representation of extracted sample features for enrollment and verification. The PMSM is utilized in the prediction of future match scores for both linear and neural-networks.

Table 4 – Perfect Match Score Matrix (PMSM) Example

Image	118	122	128	134	140	146	152	158	164	170
118	1	1	0.949	0.875	0.933	1	0.881	0.964	0.941	0.952
122	1	1	1	1	1	0.907	0.847	1	1	0.903
128	0.964	1	1	1	1	0.927	0.825	1	0.904	0.824
134	0.876	1	1	1	1	0.842	0.792	0.949	1	0.82
140	0.933	1	1	1	1	0.886	0.772	1	0.882	0.842
146	0.994	0.906	0.934	0.84	0.892	1	0.967	0.977	0.943	0.932
152	0.865	0.836	0.826	0.814	0.769	0.965	1	0.856	0.993	0.739
158	0.956	1	1	0.961	1	0.98	0.862	1	1	0.86
164	0.934	1	0.908	1	0.879	0.941	0.983	1	1	0.779
170	0.932	0.895	0.819	0.825	0.845	0.915	0.728	0.855	0.773	1

3.5.3.2 Error Score Matrix

Using the PMSM, a matrix of error scores is then created. This is accomplished by subtracting the match score from 1, such that $error = 1 - match\ score$. The error is symbolized as $E(x_i, g_j)$ or $E(i, j)$. This represents the comparison error between the query x_i and the gallery g_j, where a higher error (larger value) represents a greater aging effect. The "error matrix" obtains error scores of each query image such that $EM : E_i = \{E(g_i, g_1), E(g_i, g_2), ..., E(g_i, g_n)\}, i = 1, ..., n$. The result is a matrix with 0's on the diagonal. The "Error Score Matrix" (ESM) is a result of comparisons across images. Table 5 is a partial ESM example generated from the PMSM example in Table 5.

Table 5 – Error Score Matrix (ESM) Example

Image	118	122	128	134	140	146	152
118	0	0	0.06	0.13	0.07	0	0.12
122	0	0	0	0	0	0.10	0.16
128	0.04	0	0	0	0	0.08	0.18
134	0.13	0	0	0	0	0.16	0.21
140	0.07	0	0	0	0	0.12	0.23
146	0.01	0.10	0.07	0.16	0.11	0	0.04
152	0.14	0.17	0.18	0.19	0.24	0.04	0

3.6 Modeling Template Aging and Renewal Prediction Strategy

This section presents the developed and evaluation strategy for modeling the prediction of template-aging match scores and associated Prediction Algorithms (PA), the Decay Error estimation (DE), and Template Renewal Prediction Algorithm (TRPA), as it pertains to the history of match scores of a given PMSM. The template aging match score predictions and renewal is a difficult problem to address specifically due to the many effects discussed (aging, biometric capture, and/or sensor variance). One of the key aspects to the research is the exploitation of the time dimension and its effects on the probability of matching any given biometric template to its original sample.

3.6.1 Approaches

Using the PMSM, the match scores are used in the prediction algorithm for predicting the ‘next match score’. To establish a baseline for performance comparison, a linear model is used first. From this, a set of neural-networks are used to gage predictive performance improvements. Neural-networks are implemented in the prediction approaches for their ability to problem-solve, adaptability to learning, and being well-suited for prediction [Bis95, HaD02]. To determine accuracy and a metric for comparison, the predicted score P is compared to the actual score. The number of correct predictions, to be defined below, is used as a basis for comparisons to the various linear and neural-network predictors to determine the highest accuracy. This is defined as the Match Prediction Accuracy (MPA) percentage rate, where $MPA = \frac{\#correct}{\#predictions} * 100$.

3.6.1.1 Linear Prediction Algorithm Approach

The linear baseline template-aging match score prediction model uses simple linear techniques for baselining the prediction performance. This baseline is established to compare to future evaluations. The template-aging match score linear prediction algorithm model is such that $P = \frac{\Delta y}{\Delta x} + y$, where *y* is the newer score compared to the other scores utilized in the algorithm. The linear predictions are described in Chapter IV, where the results are analyzed and discussed.

3.6.1.1.1 Baseline Simple Linear Approach

The simple linear baseline template-aging match score prediction model is a straight-forward linear approach. The baseline linear prediction algorithm is a simple linear calculation using two points to create a slope. The slope calculation is $m = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$, where y_2 is the newer score and $x_2 - x_1 = 1$. As an example from the above PMSM: $P = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1} + y_2 = \frac{0.949 - 1}{2 - 1} + 0.949 = -0.051 + 0.949 = 0.898$. The next predicted match score is $P = 0.898$. This predicted match score is compared to the actual score, in this example, 0.875. The final results are analyzed and discussed in Chapter IV.

3.6.1.1.2 Three-Node Linear Approach

The next linear template match score prediction model uses three points in the linear approach. The three-point linear approach is used to provide evaluation comparisons to the three-node neural-network. The template match score uses a linear-regression prediction model such that $P = \frac{\Delta y}{\Delta x} + y_3$, where y_3 is the newer score. This linear prediction algorithm is a linear calculation using three points to create a slope. The slope calculation is $m = \frac{\Delta y}{\Delta x} = \frac{n\sum(xy) - \sum x \sum y}{n\sum(x^2) - (\sum x)^2}$, where $n = 3$. The linear-regression prediction algorithm is $P = \frac{\Delta y}{\Delta x} + y_3 = \frac{n\sum(xy) - \sum x \sum y}{n\sum(x^2) - (\sum x)^2} + y_3$. An example from the above PMSM (Table 4): $P = \frac{\Delta y}{\Delta x} + y_3 = (m = y_1, y_2, y_3) + y_3$ $= (m = 1, 0.949, 0.875) + 0.875 = -0.0625 + 0.875 = 0.8125$. The next predicted score match score is $P = 0.8125$. This predicted match score is compared to the actual score, in this example, 0.933. The final results are analyzed and discussed in Chapter IV.

3.6.1.1.3 Four-Node Linear Approach

The next linear template match score prediction model uses four points in the linear approach. The four-point linear approach provides an evaluation comparison to the four-node neural-network. The template match score uses a linear-regression prediction model such that $P = \frac{\Delta y}{\Delta x} + y_4$, where y_4 is the newer score. This linear prediction algorithm is a linear calculation using four points to create a slope. The slope calculation is $m = \frac{\Delta y}{\Delta x} = \frac{n\sum(xy) - \sum x \sum y}{n\sum(x^2) - (\sum x)^2}$, where $n = 4$. The linear-regression prediction algorithm is $P = \frac{\Delta y}{\Delta x} + y_4 = \frac{n\sum(xy) - \sum x \sum y}{n\sum(x^2) - (\sum x)^2} + y_4$. This predicted match score is compared to actual scores. The final results are analyzed and discussed in Chapter IV.

3.6.1.2 Neural Network Prediction Algorithm Approach

The neural-network template-aging match score prediction model uses multi-layer perceptron modeling to analyze the predictive performance. The template-aging match score neural-network prediction algorithm model is such that $P = Neural\ Network\ Score$.

Using the PMSM, the match scores are used for training and validating the neural-network. Once trained, the neural-network is used to predict the next match score. The type of neural-network used in the approach is feed-forward. Feed-forward neural-networks (FFNN) have one-way connections from input to output layers and most commonly used for prediction and pattern recognition [HaD02].

A neural-network has inputs connected to neurons, which learn based on the input values. The outputs are derived from a transfer function. The transfer function chosen is based on the function the neural-network is attempting to solve. The neural network algorithms use either a single or multiple-layer network. The first layer consists of the inputs and matching neurons. The next layer is the hidden layer. There may be several hidden layers used in calculating weighted values. The last layer is the output layer, yielding the results [Bis95, HaD02]. For this research, the results are the match score predictions. Figure 9 is an example of a multiple-layer network.

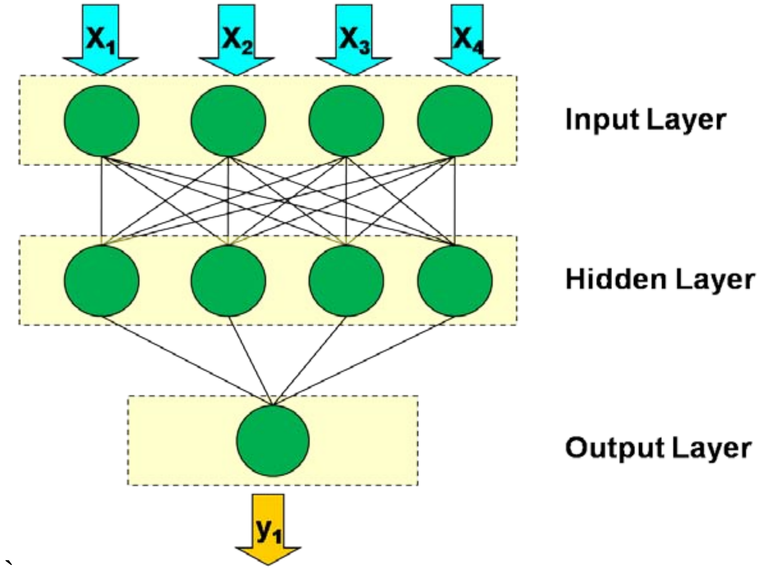


Figure 9 – Neural Network Example

The neural-network has various function capabilities to process the input and determine the output which is called activation threshold or transfer functions [Bis95, HaD02]. There are three basic categories of transfer functions: 1) Linear – where the output is proportional to the input; 2) Threshold – where the output has two levels depending on whether the total input is greater than or less than a threshold value; and 3)

Sigmoid – where the output varies continuously, not linearly, as the input changes. The transfer functions utilized in the research are linear and sigmoid, specifically: 1) Linear, 2) Log-Sigmoid, and 3) Hyperbolic Tangent Sigmoid. A transfer function transforms the input(s) of the neural-network to simulate the output of a specific task, such as predicting matching scores. Figure 10 is an example of Log-Sigmoid transfer function.

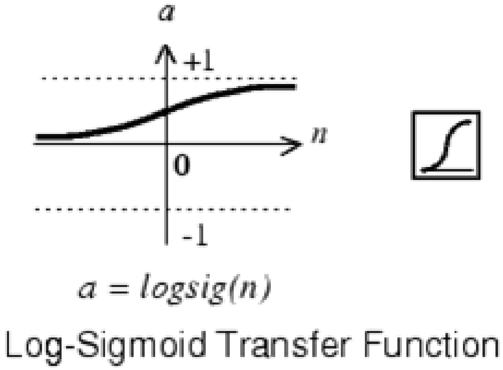


Figure 10 – Transfer Function Example

3.6.1.2.1 Three-Node Neural Network Approach

The first neural-network template match score prediction model uses three inputs of scores in the neural-network approach. The template match score uses a three-node feed-forward neural-network prediction model such that $P = (y_1, y_2, y_3)$, where y_3 is the newer score. This neural-network prediction algorithm uses three points to create a predicted score. This predicted match score is compared to actual scores. The final results are analyzed and discussed in Chapter IV.

3.6.1.2.2 Four-Node Neural Network Approach

The second neural-network template match score prediction model uses four inputs of scores in the neural-network approach. The template match score uses a four-node feed-forward neural-network prediction model such that $P = (y_1, y_2, y_3, y_4)$, where y_4 is the newer score. This neural-network prediction algorithm uses four points to create a predicted score. This predicted match score is compared to actual scores. The final results are analyzed and discussed in Chapter IV.

3.6.2 Decay Error Estimates

The Decay Error (DE) estimate is used to determine if the amount of error change from the original enrollment to the current match comparison is significant enough for template renewal. The decay error estimation, as determined by the template renewal prediction algorithm (TRPA), is such that $DE = TRPA = \frac{\Delta Score}{Average\ \Delta\ Scores}$, where $\Delta Score$ is the slope of the error from the previous error score to the current error score and $Average\ \Delta\ Scores$ is the averages of all the slopes up to and including the current comparison. The template renewal prediction algorithm is a linear calculation using two points to create a slope. The slope calculation is $m = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$, where y_2 is the newer error score, and x_i are the image indexes. The template renewal prediction algorithm is

$$TRPA_n = \frac{\Delta Score}{Average\ \Delta\ Scores} = \frac{\frac{\Delta y}{\Delta x}}{\frac{\sum \frac{\Delta y}{\Delta x}}{n}} = \frac{\frac{y_n - y_{(n-1)}}{x_n - x_{(n-1)}}}{\frac{\sum_{i=2}^{n} \left| \frac{y_i - y_{(i-1)}}{x_i - x_{(i-1)}} \right|}{n}}$$

, where y_i is the newer error score, x_i are the image indexes, and n is the total number of decay error slopes. Although $x_2 - x_1$ is representative of the image indexes to simulate the time variant in this research, other modalities might not be as consistent with the delta between images. The Decay Error estimate is the numerical result of the Template Renewal Prediction

Algorithm function as depicted in Figure 11. There is no defined range for the Decay Error estimate; however DE scores had a range of (-1989, 9375) during the testing.

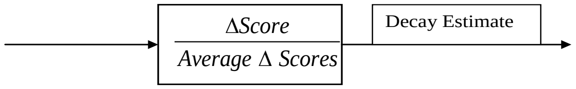


Figure 11 – Decay Error Estimates

3.7 Testing Strategy

A testing strategy is developed and evaluated for this research. The testing approach uses a step-by-step block process of examining the overall template renewal prediction strategy. The first step starts with the renewal strategy and creation of the individual PMSMs. Once the PMSM is established, the ESM is created, followed by the predictions of the next match score and DE estimate. The testing strategy continues with establishing the linear baseline. Then the additional linear approaches are completed for comparison. This is followed by the neural-network approach to provide evidence of improved performance to the linear baseline approaches. Once the linear and neural-network approaches are completed, the Match Prediction Accuracy (MPA) rates are evaluated in determining an overall conclusion.

3.7.1 Template Aging and Renewal Prediction Testing Strategy

The template aging strategy uses a building block process of multiple steps in determining the template renewal prediction estimation. These steps are repeated throughout the process. The first step starts with the creation of the PMSM. Once the PMSM is established, the creation of the Error Score Matrix is next accomplished. This is followed by the Decay Error estimate, which is utilized in the template renewal decision. Figure 12 below is the block diagram for the renewal strategy.

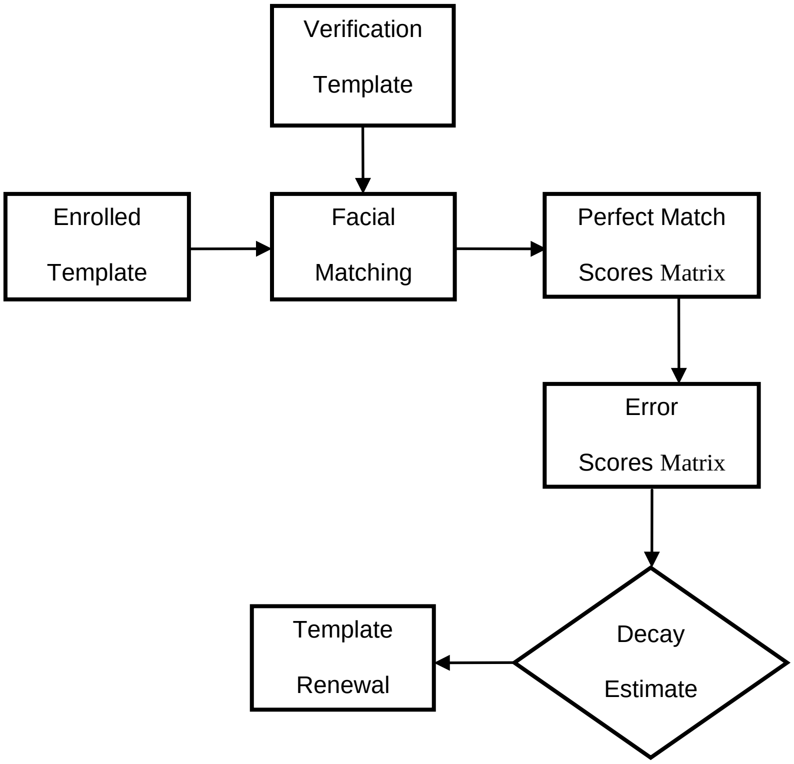


Figure 12 – Renewal Strategy Block Diagram

The renewal prediction strategy modifies the template aging strategy with an extra building block. As in the template aging, it creates a PMSM from the individual's images through iterations. The PMSM is converted to the ESM. However, using the historical score, a prediction is made on the next match score, being added to the PMSM and subsequently, the ESM. The DE estimate is calculated using the new prediction score. If the calculated decay error estimate increases beyond the set system threshold level, then the template should be renewed on the next iteration if the actual match score is approximate to the predicted match score. A large change in the decay error estimate signifies a re-enrollment opportunity. This is called a "Re-Enrollment Point" (REP).

Figure 13 below is the block diagram for the combined template aging and renewal prediction strategy.

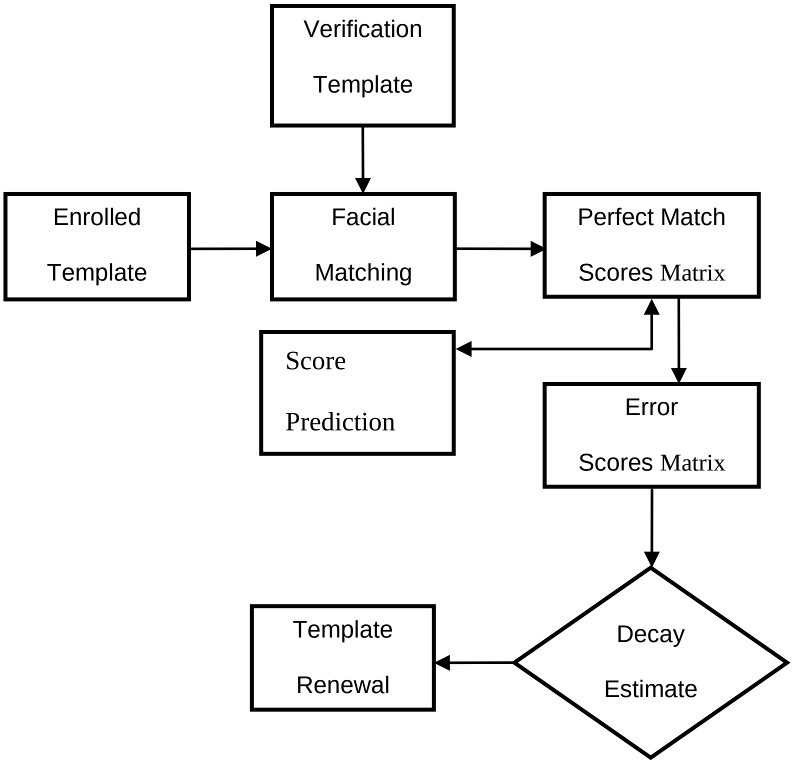


Figure 13 – Updated Renewal Strategy Block Diagram

3.7.1.1 Match Prediction Accuracy Testing Strategy

To determine accuracy of the next match score, the next match score is calculated and compared to the actual match score. If the predicted score is within a predefined percentage of the actual match score, then it is considered a valid predicted match score. The total number of matches is used in the MPA rate. The MPA rate is used to provide insights into the best performing predictive architecture. The final results are analyzed and discussed in Chapter IV.

3.7.1.2 Neural Network Testing Strategy

The neural-network testing strategy uses the PMSM created from the individual's images. The match scores from odd-numbered rows are used for training the neural-network, starting with the third row. The even-numbered rows are used for validation of the neural-network, starting with the fourth row. The third and fourth rows are arbitrarily chosen for starting points as inputs for training and validation data, but also allows for the maximum amount of training data. The importance is to ensure the training data comes from the same PMSM of the individual tested so the scores are accurately predicted for that same individual. As a general rule of thumb, there should be more than three times the number of inputs to the neural-network relative to the size of training data [RoK91], such that the ratio is greater than or equal to 9:1 for the three-node where $\frac{training\ samples}{(\#inputs = 3)*3} \geq 9$, and such that the ratio is greater than or equal to 12:1 for the four-node where $\frac{training\ samples}{(\#inputs = 4)*3} \geq 12$.

There are multiple neural-network configurations used to predict the next matching score. The multiple configurations implemented determine which neural-network provides the highest prediction capability as set forth in the criteria described below. The best neural-network configuration meeting the criteria will be utilized in the CTARP Framework. The configurations are divided into two sections, one with three inputs for the three-node neural-network and the other with four inputs for the four-node neural-network. The two sections are categorized into different transfer functions. The first section of three-input, three-node neural-networks utilizes a four-vector matrix of the

PMSM for training and prediction, where a sample matrix row is the input vector, for example: [1, 0.94, 0.87; 0.93]. The first three numbers are the inputs to the three-node neural-network and the fourth is the actual match score. The second section of the four-input, four-node neural-network configurations utilizes a five-vector matrix of the PMSM for training and prediction, where a sample matrix row is the input vector, for example: [1, 0.94, 0.87, 0.93; 1]. The first four numbers are the inputs to the four-node neural-network and the fifth is the actual match score. Next is the number of hidden layers in the network, either one or two layers. Finally, the different types of transfer functions are: 1) Tansig (T), which is a tangent-sigmoid; 2) Logsig (L), which is a logarithm-sigmoid; and 3) Purelin (P), which is linear. These transfer functions are selected for several reasons. The transfer functions are the default recommendations for prediction with neural-networks in MatLab®, best suited for predictions, and best suited for non-linear functions – as in match scores changing over time [Bis95, HaD02, Mat07, RoK91]. An example of a multiple-node neural-network/transfer combination is: TTL441 represents a neural-network with four inputs, two hidden layers each with four-nodes, and one output with transfer functions between the layers in the order of Tansig, Tansig, Logsig. The multiple-node neural-network/transfer configurations are tested to determine which neural-network performed best. The final results are analyzed and discussed in Chapter IV.

3.8 Simulation Environment and Framework Models

In general, experiments and simulations are used to study the performance of processes and systems. Experiments consist of several inputs, of which some variables are controllable, and others are not. These inputs are processed by the system, and a response is observed. To increase the reliability of the system analysis, multiple reproductions of the same experiment are processed, and the observations recorded and analyzed. One method of analyzing the data is through simulations. This allows the complexities of the numerous stages to be divided and controlled into manageable steps with available observations throughout the system process. The controlled observations throughout the simulations are the multiple prediction frameworks.

The neural-network simulations were created using MatLab® version R2007b [MAT07] to compare the MPAs and demonstrate improved performance over the representative linear frameworks. *Match Prediction Accuracy* (MPA) is defined as a measurement of accurately predicting the correct number of match scores as compared to the actual match score. The MPA forms the basis for determining the best accuracy among the different match score prediction approaches, both linear and neural-network. *Improved Performance* is defined as a higher MPA rate than the baseline MPA rate. The higher the MPA rate the better the improved performance.

3.8.1 Simulation Environment

In this model, all prediction approaches are managed through the CTARP Framework. As a new identity is initiated, the request is processed step-by-step through the framework. At the completion of all the identities, the statistics are tabulated and summarized for analysis in Chapter IV.

Throughout the rest of this document, the following terms are defined as follows. A *Simulation* refers to a specific MatLab® script file to code each of the neural-networks.

A *Scenario* is a given simulation configuration, with certain parameters that remain constant throughout the entire simulation (e.g., the prediction architecture), and certain parameters (e.g., identity inputs) that vary throughout the given simulation. A *Template-Aged Time Step* is where the next verification event occurs. An *Iteration* is when the complete execution of a single template-aged time step instance occurs, completing all steps of the CTARP Framework. After each iteration, the PMSM and ESM are increased by one row and one column of scores. This is true because there has been a new verification image added, before the simulation loops through the steps of the given iteration. As the simulation executes through the time steps, the appropriate actions are taken for each prediction architecture before proceeding to the next time step. This ensures each prediction architecture is operating on the same template-aged time.

3.9 Simulation Equipment

There were multiple research, development, and simulation computers used throughout the development. The initial tests to bulk process and collect facial image matching scores was run on the 80-processor, 21 blade hardware cluster at the DoD Biometric Fusion Center (BFC), which is also used for large scale algorithm testing. The research and development computer to perform error scores, linear predictions, neural-network predictions and template renewal predictions was a XEON workstation with two three-gigahertz “Dual-Core” Hyper-Threaded XEON CPUs, along with 4 gigabytes of random access memory, dual 75 gigabyte hard drives, and dedicated video card with 128 megabytes of random access memory. This computer is typically capable of running upwards of eight simultaneous MatLab® simulations, due to its eight virtual CPUs, with no apparent slowdown. Additional tests were performed using a generic “white-box” “Dual-Core” Hyper-Threaded Intel CPU along with 4 gigabytes of random access memory, 80-gigabyte hard drives, and dedicated video card with 128 megabytes of random access memory. With the exception of the BFC hardware cluster, the computers were Microsoft Windows®-based computers with Matlab® and Microsoft Windows® Visual Studio.

3.10 Model Verification

Model verification was accomplished using a systematic approach. Modified vendor SDK C++ and MatLab code was used for the modeling and simulation of the CTARP Framework. A spiral testing and verification method was employed on the architecture. Problems with syntax and illegal statements were identified and corrected after each section of code was written. Further, each section of code was checked for proper, expected execution to ensure each progressive feature was correct before the next section was developed.

During development, most of the errors involved logical problems building the PMSM and implementing neural-networks, such as enrolling/dis-enrolling, matching subject images, and training the neural-networks for prediction of match scores. These errors were identified by stepping through the code, using the results of the PMSM structure and comparing the output of functions with the expected output. Perfect match score matrices and match score prediction plots, error score matrices and re-enrollment point plots, and thresholds were used throughout the development and testing to ensure the expected outcome occurred and to verify that the code was executing properly given certain subdirectories and subjects. These areas indicate what template-aged time step and iteration stage of the framework the subjects were in, and how many were remaining, thus allowing a verification of each subject’s progress.

The neural-network match score prediction verification was accomplished through using the PMSM match scores. The data is separated into training data and verification data. This is accomplished by using odd-numbered rows for training, starting with the third row. Then even-numbered rows are used for validation of the neural-network, starting with the fourth row.

3.11 Model Validation

Model validation was difficult since there are no known implementations of similar template aging and renewal prediction frameworks. Therefore, the CTARP Framework model was validated against other publicly available algorithms/SDKs willing to offer the license temporarily for research. Full replication of the simulation experiments to validate the CTARP model was possible; however, only with a second vendor’s algorithm/SDK.

The results found using the first vendor algorithm/SDK demonstrate a trend similar to the results found in the second vendor algorithm/SDK when the CTARP Framework incorporated the scenarios. Figure 14 and Figure 18 shows a subject’s aging sequence of images from ND ’B’ where there are changes over time that affect matching scores. Although not as discernable in the second image sequence below (although noticeable in the actual detailed image), the images with asterisks below signify aging changes that reflects in the match score (i.e. facial hair growth) and predicted as re-enrollment points, depending on the threshold level set (as described in Chapter IV) by either one or both algorithms/SDKs. The CTARP Framework applied with Vendor 1 provided reflective re-enrollment points where the subject has aged, seen in the decay error estimation values plotted in Figure 15 and Figure 19. The results are favorably validated when Vendor 2 is applied to the CTARP Framework with similar reflective re-enrollment points where the subject has aged, as shown in the decay error estimation values plotted in Figure 16 and Figure 20. The CTARP Framework decay error estimate values of Vendor 1 and Vendor 2 are plotted together, as shown in Figure 17 and Figure 21. The trend of the results shown in Figure 17, compared to the results shown in Figure 21, lends credibility to the CTARP Framework model.

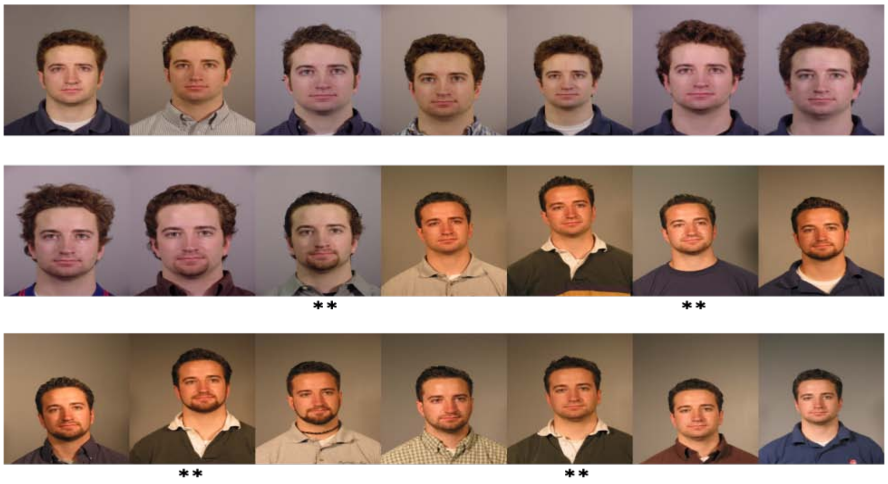
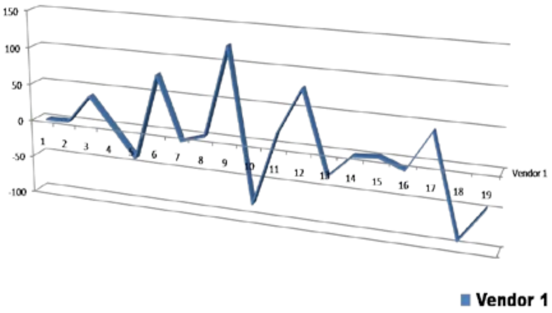


Figure 14 – Subject’s Image Facial Aging Sequence [FlB07]



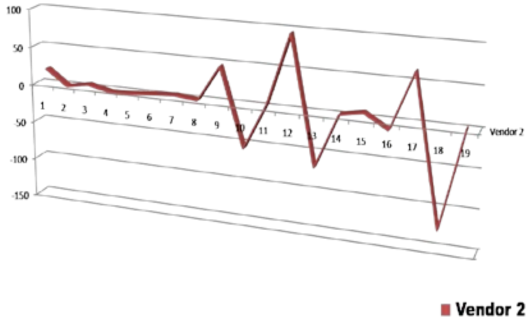


Figure 15 – Subject Decay Error Estimation Values Plot, Vendor 1

Figure 16 – Subject Decay Error Estimation Values Plot, Vendor 2

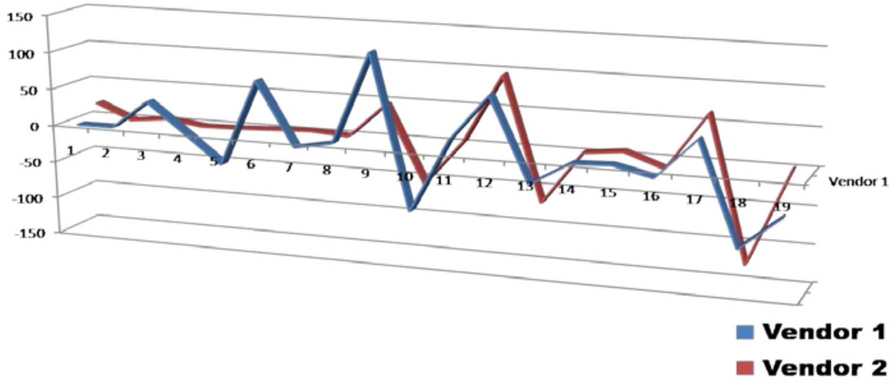


Figure 17 – Subject Decay Error Estimation Values Plot, Vendor 1 and Vendor 2

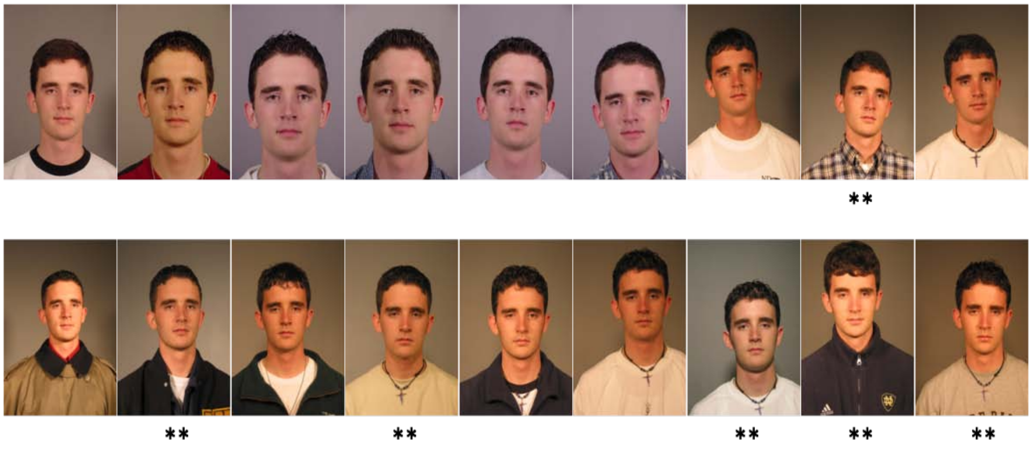


Figure 18 – Subject's Image Facial Aging Sequence [FlB07]

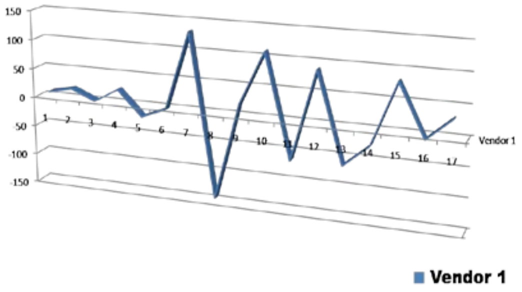


Figure 19 – Subject Decay Error Estimation Values Plot, Vendor 1

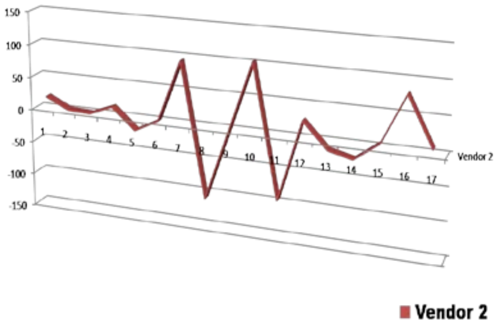


Figure 20 – Subject Decay Error Estimation Values Plot, Vendor 2

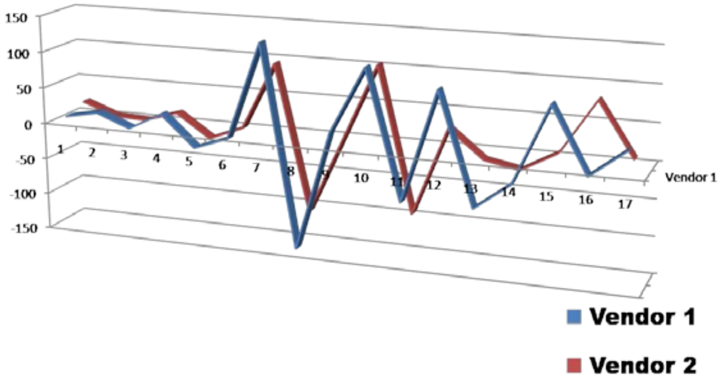


Figure 21 – Subject Decay Error Estimation Values Plot, Vendor 1 and Vendor 2

The match score prediction validation of the CTARP Framework was accomplished through phases. The first validation phase consisted of establishing a baseline with a simple linear prediction. The next phase increased the simple linear baseline from two scores to three scores, then four scores for prediction. This provides a verification baseline to measure against future modifications of the CTARP Framework. The match score prediction is then modified and implemented using neural-networks. The neural-networks provide improved match score prediction capabilities.

To provide validation to the neural-networks, the swapping of training data and verification data is performed. The data separated is such that the training data becomes the verification data and verification data becomes the training data. This is accomplished by using even-numbered rows for training, starting with the fourth row. The odd-numbered rows are used for validation of the neural-network, starting with the second row.

3.12 Summary

This chapter presented the methodology for the development of the Carls Template Aging and Renewal Prediction Framework for biometric-based authentication systems, and addressed the lack of a template aging and renewal prediction framework. The motivation for developing the CTARP Framework, along with the validity of employing a template aging and renewal prediction framework for a biometric-based authentication system was presented. Additionally, the prediction algorithms and metrics that were collected and analyzed were defined in this chapter as well. This chapter concluded with the simulation environment and equipment, model verification, and validation.

IV. Performance Results and Analysis

4.1 Chapter Overview

This chapter discusses the modeling and simulation performance results. Analysis of the results confirms the CTARP Framework maintains or improves error rates, the security of biometric verification systems and user acceptability; ultimately reducing fraud, theft, and loss of resources from unauthorized personnel. Various simulations are presented with their corresponding performance results, along with analysis and discussion. Finally, the performance results are summarized.

4.2 Model Scenarios

The simulations and scenarios are presented in the sequence to provide the ability for analysis and discussion in a logical manner. The first model scenario provides justification of template aging by showing the degradation of match scores over an extended period of time using the facial datasets and algorithms. The next scenario models the match score prediction frameworks along with the comparison of the match prediction accuracy performance rates. Discussion follows on the final prediction algorithm. This is followed by the template renewal prediction model scenario results and discussion. The final discussion reveals how the overall improvements are made to the biometric-based verification system.

4.2.1 Dataset Template Aging Environment

Demonstration of the template aging model and experiment is accomplished using the following process. First, the subjects were divided into subdirectories containing individual images of the same subject. This allows the algorithm to run facial matches against all the subject's images. The algorithms/SDKs were run on the sub-directories to create the PMSM. The PMSMs are totaled together to collect dataset match scores over an extended period of time. The match scores were combined and averaged over the image sequence. Ideal match scores should be near one over the entire duration of time. As depicted in Figure 22, the average match scores for ND 'B' gradually dropped off from one over time, although the score variance is relatively equal. As depicted in Figure 23, the average match scores for MORPH have a greater drop in score early and then trails off, although the score variance is relatively equal. This is believed to be due to the greater distances of time between images in MORPH than in ND 'B', as annotated in Table 2. The horizontal red line at match score of 0.7 provides a comparison reference point for Figure 22 and Figure 23 to depict the changes in match scores between the databases and aiding visualization of the lowering match scores over time. The trending match scores translates into an increasing error rate over time for both ND 'B' and MORPH, as indicated in Figure 24 and Figure 25, respectively. The horizontal red line at error score 0.2 provides a comparison reference point for Figure 24 and Figure 25 to depict the changes in error scores between the databases as well as visualization aid of the increasing error scores over time. Although there is no significance to 0.7 for match scores or 0.2 for error scores, this demarcation of trending scores could be used to establish a threshold level for renewal based on the image database and algorithm combination.

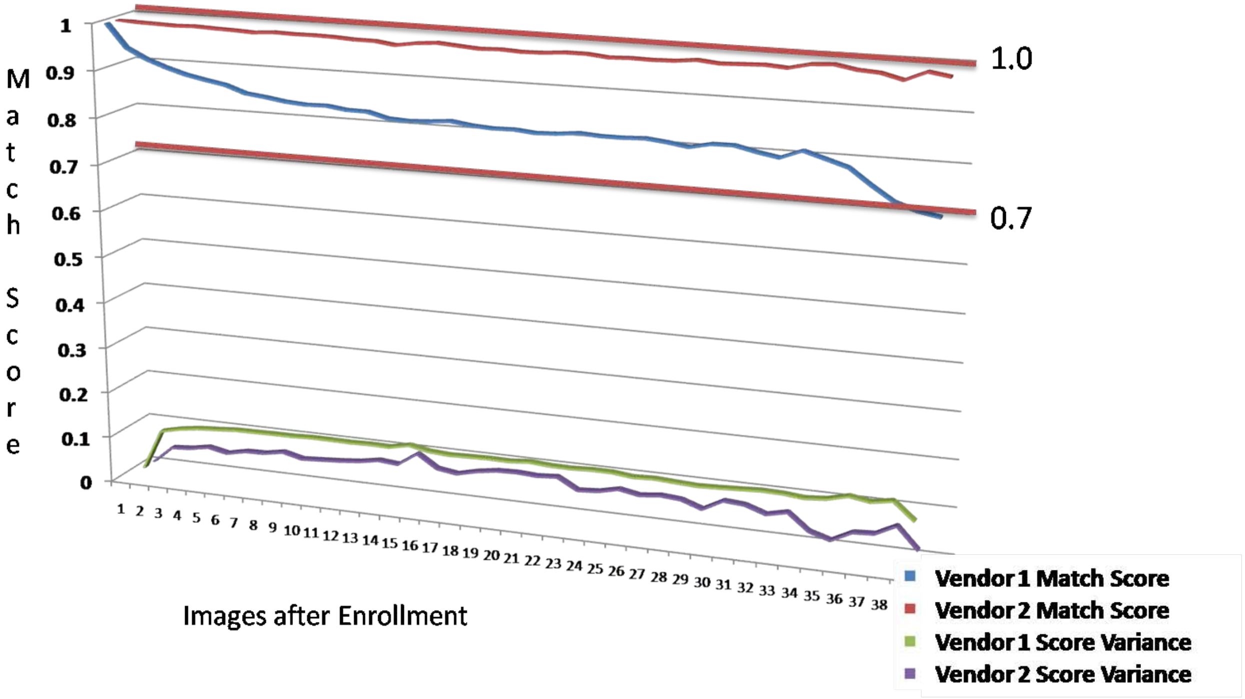


Figure 22 - ND 'B' Average Match Scores

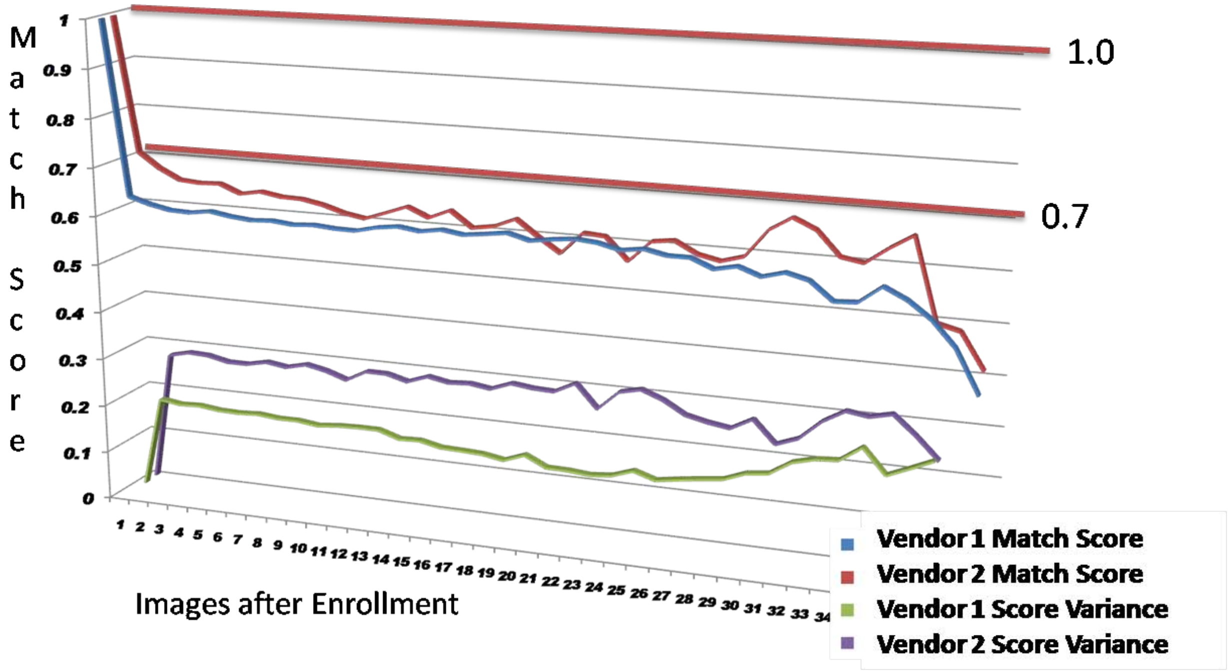


Figure 23 – MORPH Average Match Scores

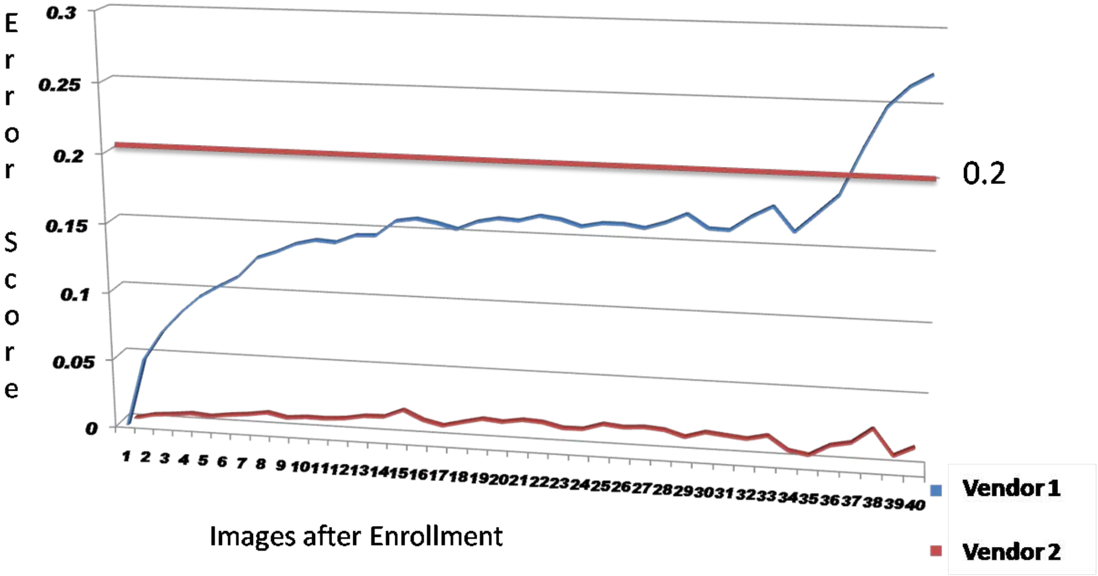


Figure 24 – ND 'B' Average Error Scores

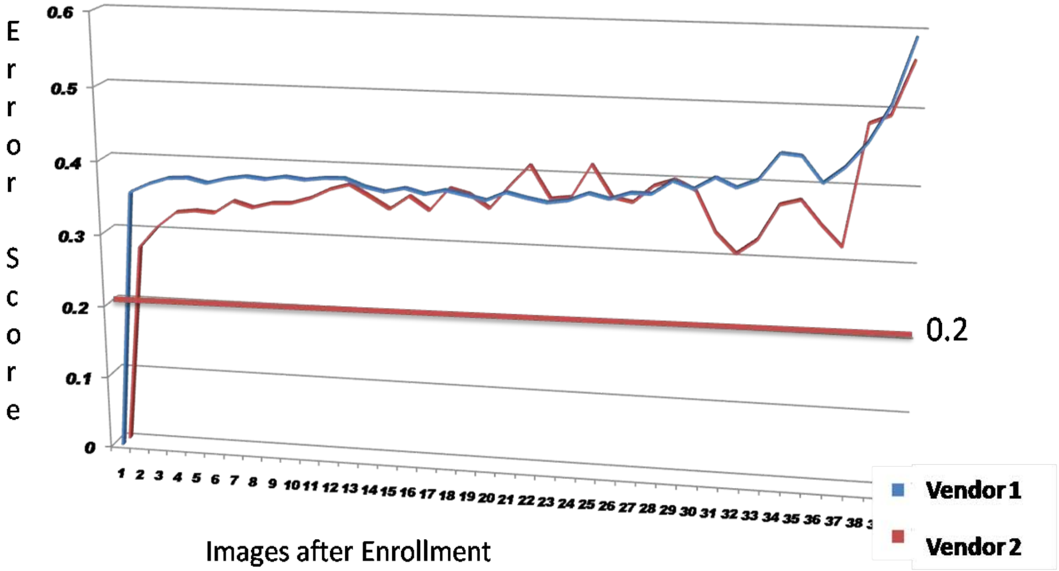


Figure 25 – MORPH Average Error Scores

Next, all the subjects were re-enrolled with new templates after the tenth verification attempt. The tenth verification attempt was chosen due to this being half the average number of images in MORPH, the smaller of the datasets, as annotated in Table 2. This “half the average” number should not be considered the re-enrollment default value. Some subject may require 14 or 20 images in a sequence before renewal is required. The match scores are re-totaled together to collect dataset match scores over an extended period of time after the renewal. Again, the match scores were combined and averaged over the image sequence with the renewal after the tenth image in the ‘aging’ sequence. Ideal match scores should be near one over the entire duration of time. As depicted in Figure 26, the average match scores for ND ‘B’ gradually dropped off from one over time. The renewal allows for the match scores to return to one. However, the scores again gradually drop off over time. As depicted in Figure 27, the same trends occur for the MORPH database. The significance of the scores resetting to one and then dropping over time provides evidence of a smaller opportunity for a false match to occur. This is related to when is the appropriate time to renew a password to prevent a hacker from running a password cracking program to break into the system. Once renewed, the old password is no longer valid and is not an access threat to the system. With the subject re-enrolled and the template renewed, it is less likely that a false match will occur.

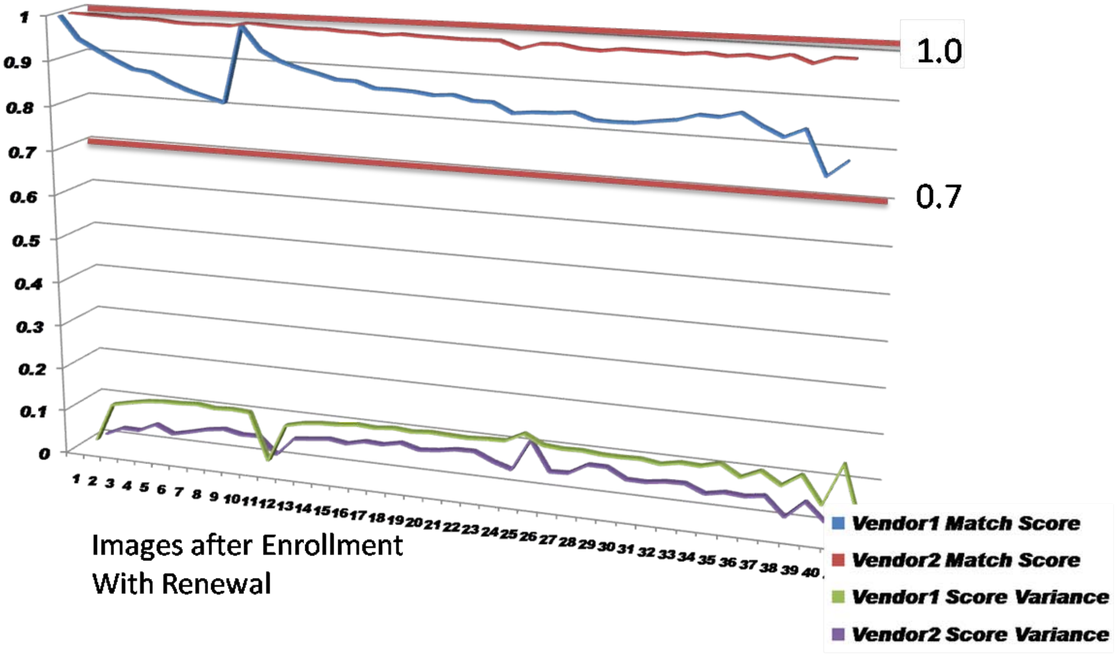


Figure 26 – ND 'B' Average Match Scores with Renewal

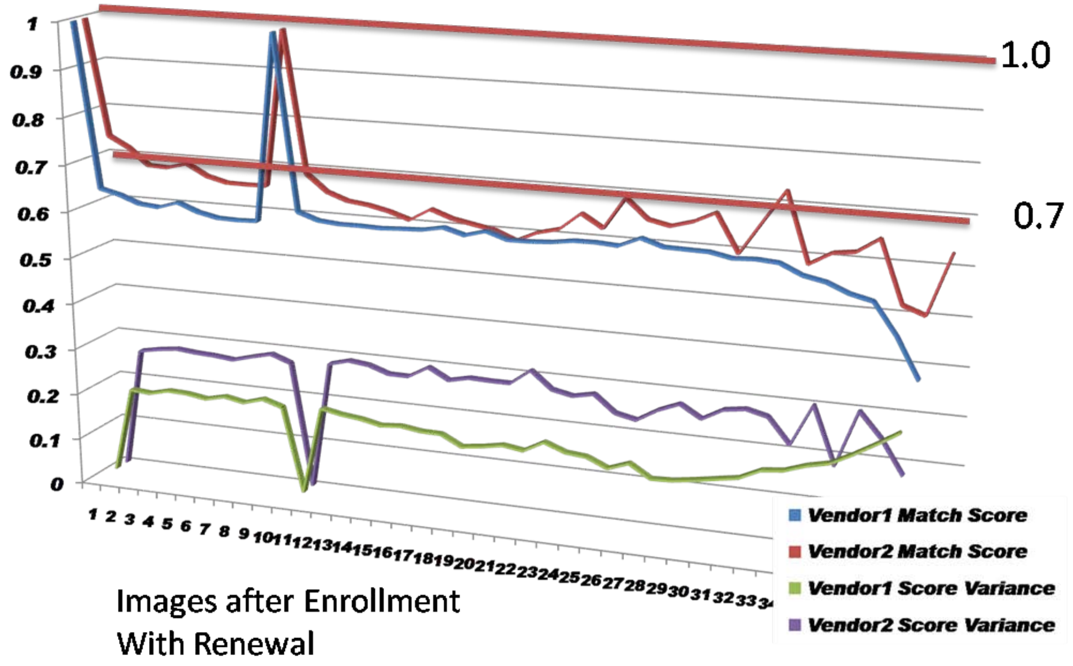


Figure 27 – MORPH Average Match Scores with Renewal

Finally, to get the full understanding of the template aging and need for renewal, the match scores from both datasets were combined. Then the combined re-enrolled subject scores are re-totaled together to collect dataset match scores over an extended period of time after the renewal. Again, the match scores were combined and averaged over the image sequence with the renewal after ten images in the 'aging' sequence. As stated, ideal match scores should be near one over the entire duration of time. However, as depicted in Figure 28 and Figure 29, the average match scores follow the same trends as seen for the individual databases. Similarly, re-enrollment decreases the false match likelihood. For example, a subject's aging image sequence has an average match score of 0.765 (without renewal). However, the subject's aging image sequence averaged match score with the renewal increases to 0.896. This is an increase of the averaged match score of 0.131, which is a 17.1% increase. This increase in the average match score yields an improvement in security, although very difficult to make it quantifiable for one subject. Although the previous example is an increase for one subject, an increase for all subjects results in an overall improvement to the security of the biometric-based authentication system. This increase in security is therefore preventing a lower opportunity for a false acceptance to occur. This translation ultimately improves the performance error rates.

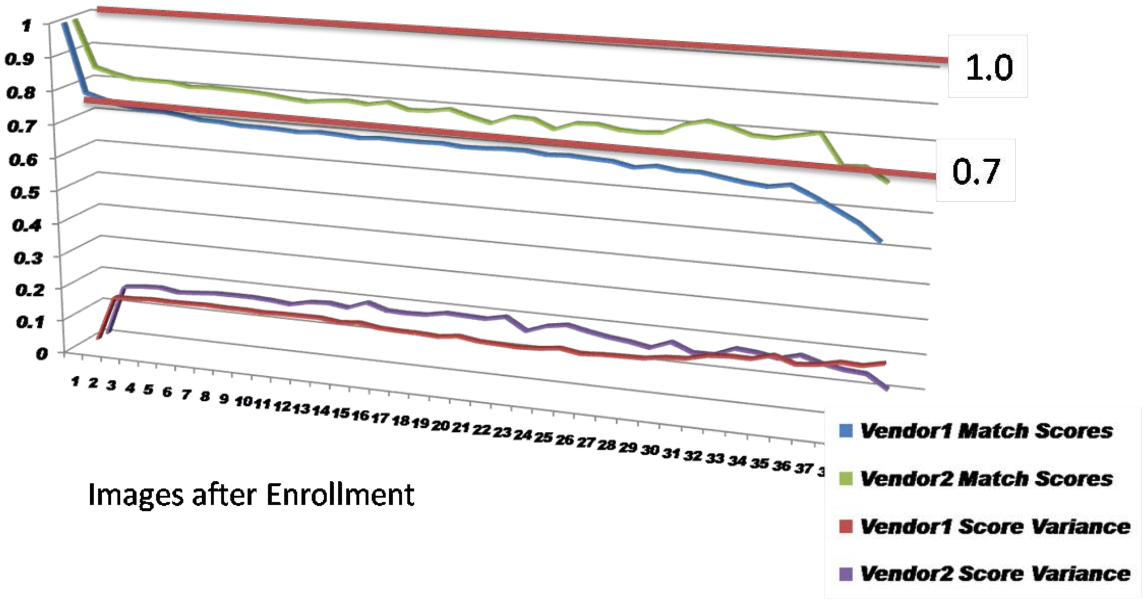


Figure 28 – Combined Datasets Average Match Scores, Variance over Time

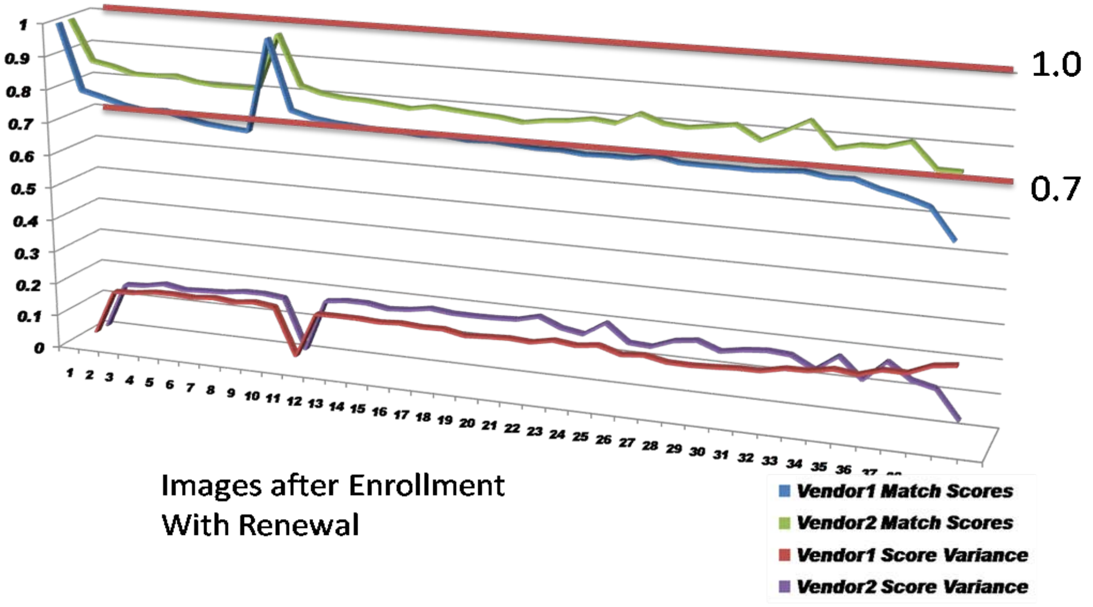


Figure 29 – Combined Datasets Average Match Scores, Variance over Time with Renewal

The decreasing of match scores over time provides proof that some type of renewal is needed to ascertain higher error rates in biometric-based verification systems. The renewal of templates provides opportunity to improve error rates. Although this example is not the prime or a prime renewal point, the ability to predict a renewal point allows for improvements in error rates therefore increasing security in the biometric-based validation system.

4.2.2 Match Score Prediction Framework Models

To determine the best MPA performance of the CTARP Framework among the baseline, linear, and neural-network prediction frameworks, several simulations are developed and analyzed. For each scenario, the prediction framework models are the same as those discussed in Chapter 3. The models are changed for each scenario, as noted in the scenario discussion below. Linear and neural-network predictions are performed on each of the subjects. These linear and multiple neural-network/transfer configurations are tested to determine which performed best. The divided sections, have either three or four inputs.

Match prediction accuracy rate is separated into two categories for comparison among the linear and neural-network configurations. The two match prediction accuracy percentages calculated are: 1) Within one percent, and 2) Within two percent. Although there are no known studies for comparison of match prediction accuracy, the two arbitrarily categories chosen provide a measurable comparison factor for the different neural-networks against each other. This measurable comparison provides the ability to form a basis on a logical assessment on which neural-network to choose for the final

CTARP Framework. The first match category (within one-percent accuracy) is defined as $\left|prediction - score\right| \leq 0.01$. The second match category (within two-percent accuracy) is defined as $\left|prediction - score\right| \leq 0.02$. The correct number predicted within the accuracy rate category yields the match prediction accuracy (MPA) rate percentage, such that $MPA = \frac{\#correct}{\#\,predictions} * 100$.

4.2.2.1 Linear Match Score Prediction Framework Models

The linear prediction model algorithms are performed on each of the subjects. These linear configurations are tested to determine which performed best. The linear combinations tested are: Baseline 2, 3, and 4. The configurations have two, three, or four inputs. The baseline linear prediction is labeled L2 in the tables below. The three-node linear prediction is labeled L3 in the tables below. The four-node linear prediction is labeled L4 in the tables below. The predictions are plotted against the actual scores. For example, Figure 30 is a single linear match prediction plot compared to the original scores. As depicted, there is one matching point, which falls within the one percentage category (this is with the eigth image). There are no matching points within the two percentage category and multiple non-matching points along the plot. The number of matched points is one and the number of possible predictions is 29, yielding a 1% MPA rate of 3.45% and a 2% MPA rate of 3.45%. A match at 1% MPA corresponds to a match at 2% MPA, but a match at 2% MPA is not reciprical to a match at 1% MPA. The objective is to have as high of a MPA rate as possible. The closer to this perfect match prediction accuracy rate, the better the prediction of the re-enrollment point will be.

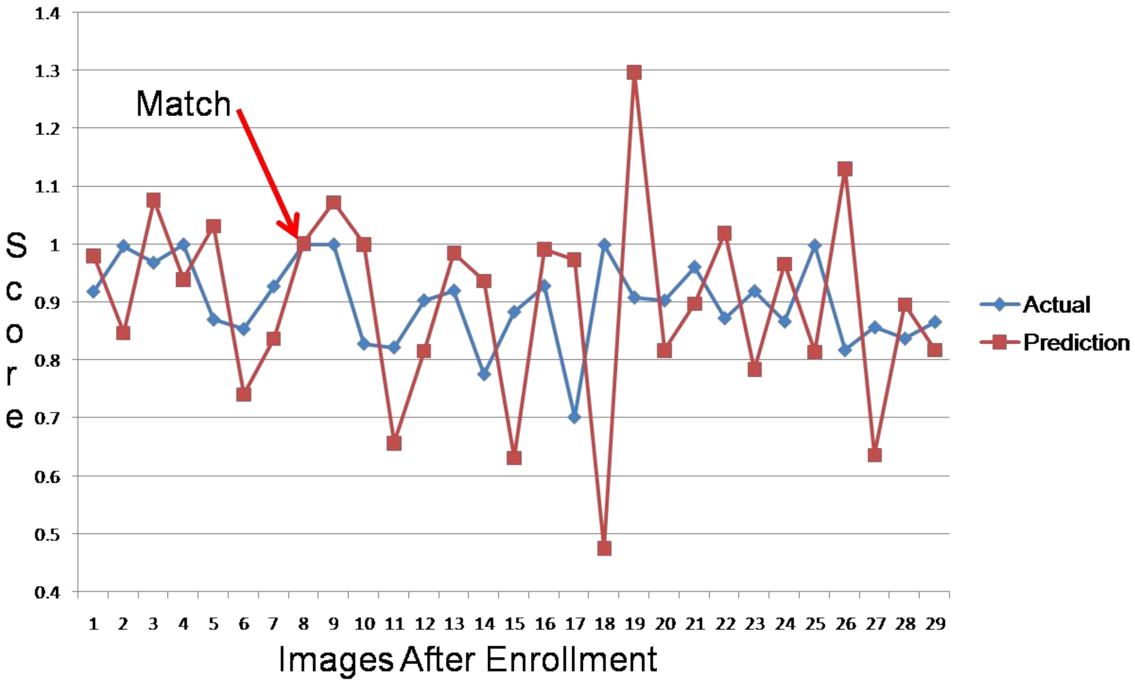


Figure 30 – Single Subject Linear Match Prediction Plot

4.2.2.2 Neural-Network Match Score Prediction Framework Models

Each of the different neural-network predictions are performed on each of the subjects. There are multiple neural-network/transfer configurations tested to determine which performed best. The combinations have either three or four inputs with one or two hidden layers and one output. The different transfers of Tansig (T), Logsig (L), and Purelin (P) are utilized to create ten different neural-network/transfer configurations. The neural-network combinations tested are: TL31, LL31, TTL331, LLL331, TTP331, TL41, LL41, TTL441, LLL441, and TTP441 and labeled as such in the tables below. The predictions are plotted against the original scores. For example, Figure 31 is a single TTL331 neural-network match prediction plot compared to the original scores. As depicted, there are five matching points, four which fall within the one-percentage category. There is one matching point within the two-percentage category and multiple non-matching points along the plot. The number of matched points is five and the number of predictions is 28, yielding a 1% MPA rate of 14.29% and a 2% MPA rate of 17.86%. Therefore this example has a low performance rate, but improved over the linear example stated previously. The objective is to have as high of a MPA rate as possible. The closer to this perfect match prediction accuracy rate, the better the prediction of the re-enrollment point will be, therefore producing a successful CTARP Framework allowing a subject's template to be renewed before false rejections start to occur. Too many false rejections lowers the user's acceptability of the biometric-based authentication system.

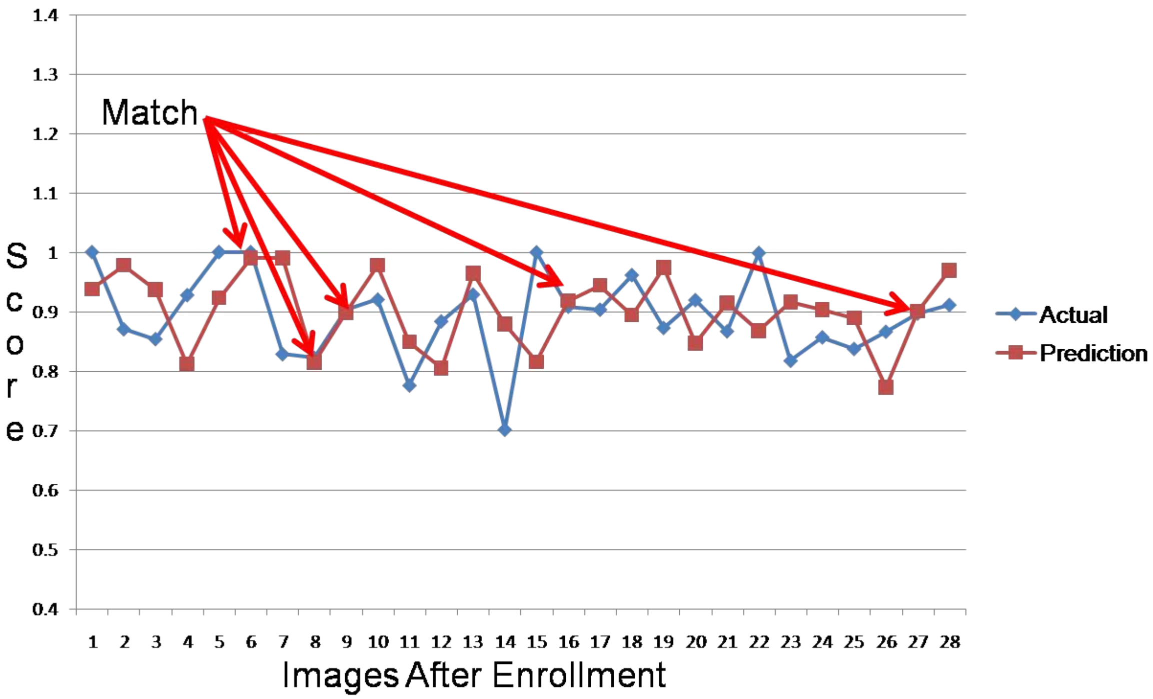


Figure 31 – Single Subject Neural-Network Prediction Accuracy Plot

4.2.3 Neural-Network Prediction Experimental Results

Implementation of a neural-network is utilized due to their predictive abilities, as discussed above. The renewal prediction step of the CTARP Framework determines opportunities for renewal of the subject's template before the next verification attempt. Previously described was the predicted 'next match score', which is entered in the DE estimate. This predicted 'next match score' and 'predicted DE estimate' provides the advantage of knowing if there is a possibility of renewal on the next verification. If the next 'actual' verification attempt yields a matching score that results in a DE estimate above the Re-Enrollment Point threshold, then an advantage has been gained in knowing that a re-enrollment needs to be accomplished with the current verification. For example, a neural-network prediction of 'next match scores' is compared to the actual match scores of a subject (after training of the neural-network) is shown in Figure 32. As depicted, the circled 'next match score' prediction is 0.1693. This results in a predicted decay error estimation score of 111.702 (depicted in Figure 33), indicating a re-enrollment point (which is greater than the defined threshold level of 100, as discussed below). As circled in Figure 32, the actual subject's next match score is 0.4964. This results in a decay error estimation score of 124.0889 (circled in Figure 33), confirming the predicted re-enrollment point.

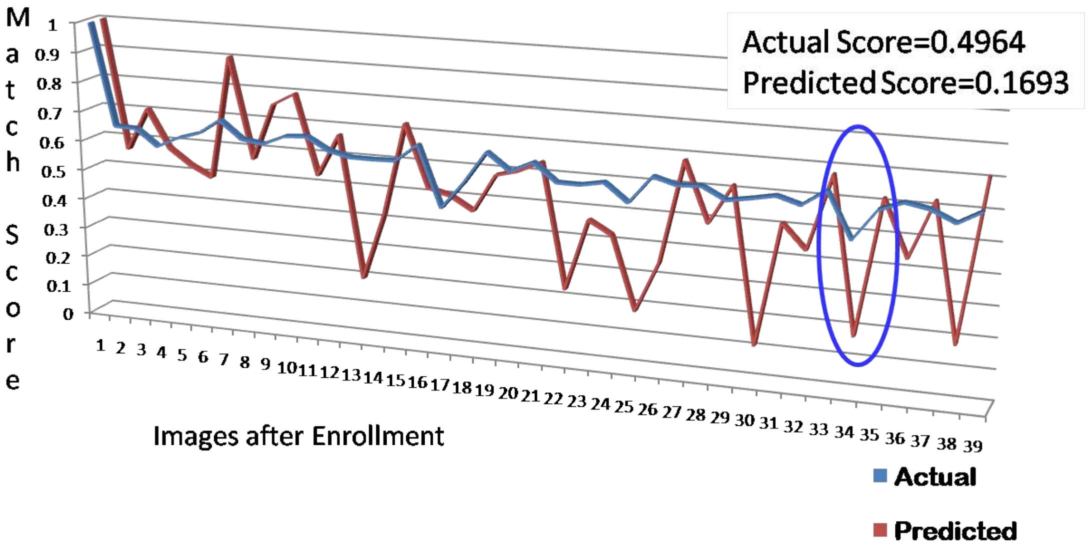


Figure 32 – Single Predicted versus Actual 'Next Match Score' Plot

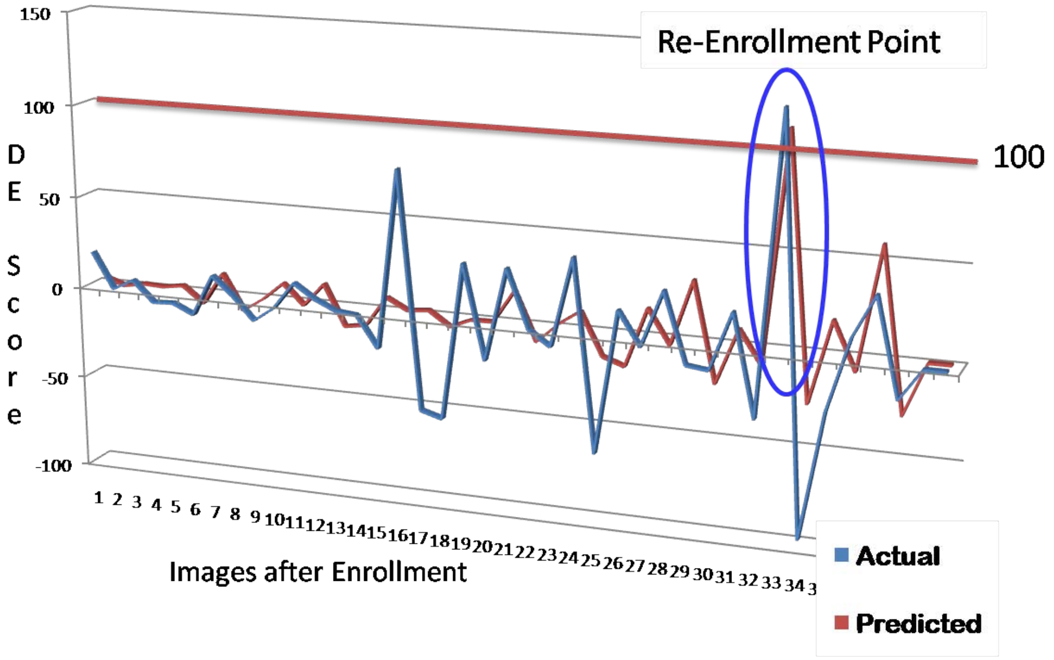


Figure 33 – Single Predicted versus Actual 'Next Match Score' Re-Enrollment Point Plot

Additionally, the match prediction accuracy for this subject was 24.14% at the 1% MPA Rate and 42.86% at the 2% MPA Rate, as described previously. An increase in the accuracy rate translates into an increase in the predictability of when it is time for a subject's template re-enrollment based on the renewal predictions. The experiments demonstrate how the 'next match score' prediction with the predicted decay error estimation method provides an advantage of pre-determing the template re-enrollment point opportunities. With the addition of the foresight to determine template re-enrollment point opportunities, this will aide in improving the security by knowing when a subject may require re-enrollment. This will improve the false rejection rate by preventing a subject from being falsely rejected due to the subject needing to re-enroll due to the changes over time.

4.2.4 Predictive Re-Enrollment Points

The next step of the CTARP Framework determines opportunities for re-enrollment of the subject. The decay error estimation is used in the prediction of the re-enrollment points based on the threshold level set within the biometric-based authentication system. The points indicate change (error) from the previous verification. A large change (greater than 100) signifies a re-enrollment opportunity. This is called a "Re-Enrollment Point" (REP), as defined in Chapter III. The value of 100 for the initial thresholding value for re-enrollment signifies a change greater than 10% in the match score. For example, a subject's running match scores over time of: [1, ..., 1, 0.887, 0.917, 0.959, ..., 0.936, 0.709] has an averaged error slope score of 0.00056. The match score change is from 0.936 to 0.709, a difference of 0.291, greater than a 10% change.

The error slope score of the last two images is 0.227. This results in a decay error estimation score of 405.357, indicating a re-enrollment point, which is greater than the threshold level of 100. The experiments demonstrate how the decay error estimation method predicts the template re-enrollment point opportunities. A subject's decay error estimations over time is plotted in Figure 34 with a predicted re-enrollment point of opportunity. As depicted in Figure 34, a threshold is delineated, there are points with large errors, and one point significantly larger (circled) than the rest (a re-enrollment opportunity). This point indicates an inferior match from the previous verification to the current verification, or an error score change of 10% or greater. Additionally, this is evidence of a significant change from the enrollment template used in the comparison match used for validation. There are points with negative values. This is due to that image having a significantly less error, or closer match, to the enrollment template than the previous image.

The predicted re-enrollment point of opportunity plot in Figure 34 is representative of one algorithm/SDK. To have valid predictive re-enrollment points, the points should be very similar for both algorithms/SDKs. The predicted re-enrollment point plot of the second algorithm/SDK produces closely related results. As indicated in Figure 35, the re-enrollment point plot is depicted using both commercial vendor's algorithm/SDKs. The two algorithms/SDKs results are plotted side-by-side for visual comparison. The matching re-enrollment point is circled in the sample subject's plot.

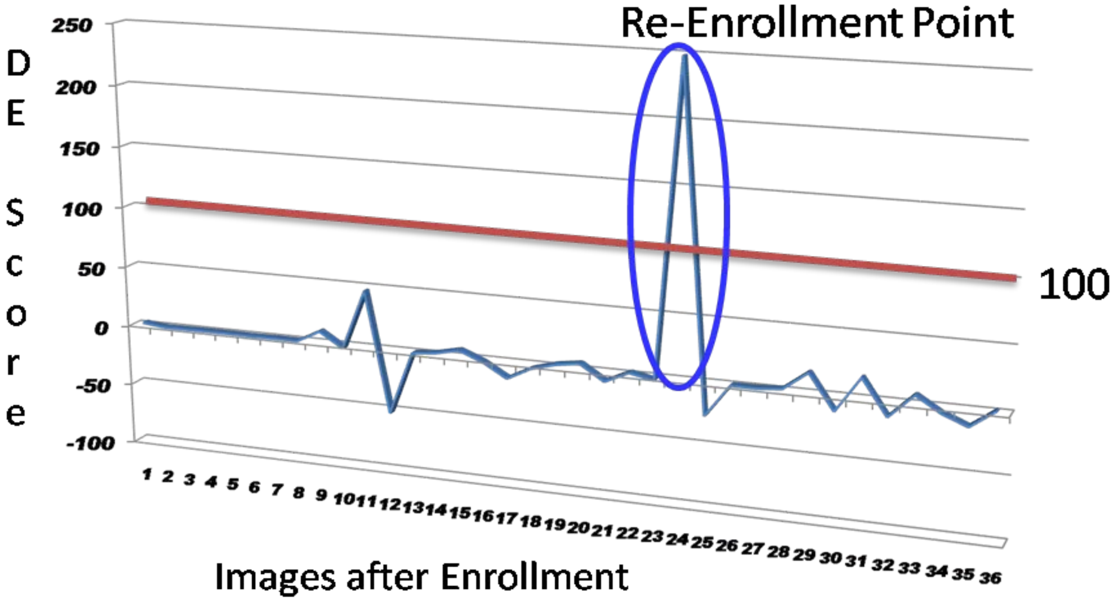


Figure 34 – Single Algorithm/SDK Subject Predictive Re-Enrollment Point Plot

4.3 Performance Conclusions

Improving the Type I/II error rates (false rejection / false acceptance, respectively) in biometric-based authentication systems to increase security was one focus for this research. A second focus was to predict when to renew an aged enrollment template (and hence increasing accuracy and user acceptability) for the individual user.

First and foremost, regardless of the simulation or scenario, the CTARP Framework always maintained, at a minimum, the current state of error rates and security established on the biometric-based authentication systems. Over 20% of the time (30 out of 147 Subjects), the implemented CTARP Framework improved the error rates and security due to a predicted re-enrollment point and template renewal. Of the remaining subjects, there were not any predictions for renewal, therefore not changing the security posture level for those subjects. This supports insufficient aging data (no longevity of data collection) lending to the necessity of template aging and renewal prediction research. Had the CTARP Framework not been implemented, security would have eventually declined over time. Insinuating that by not having re-enrolled any new subjects, the subject's match scores will eventually drop below the acceptance threshold, as defined by a static template in Chapter 3. Therefore, the subject would be prevented authentication through false-rejections or possibly allowing a false-acceptance of an imposter to access the system. With either occurrence, the security of the system is degraded.

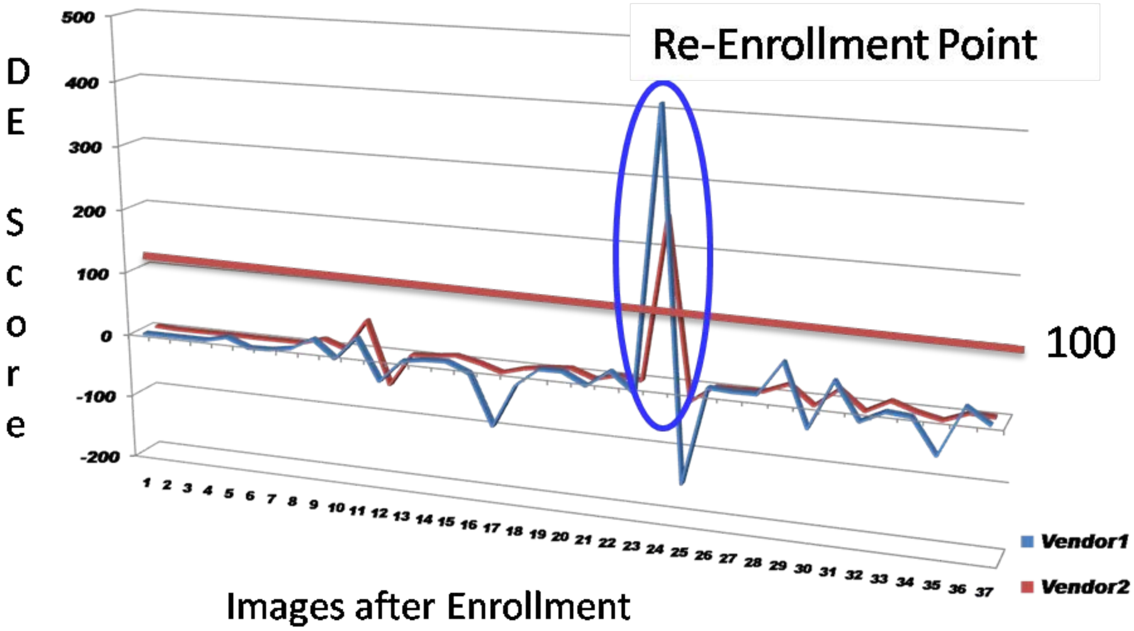


Figure 35 – Algorithm/SDK Side-by-Side Subject Predictive Re-Enrollment Point Plot

4.3.1 Linear versus Neural-Network Performance Results

As expected, the neural-network predictive performance is improved over the linear models. Comparative results are summarized in Table 6. This table provides an example of one subject's match prediction accuracy rate data. The baseline linear MPA rate calculated for this subject is 5.41% at one percent and increases to 10.81% for two percent. The three-node linear MPA rate calculated for this subject is 2.78% at one percent and increases to 5.56% for two percent. The four-node linear MPA rate calculated for this subject is 2.86% at one percent and increases to 11.43% for two percent. The decrease in the MPA rate for the three-node linear is due to the difference in linear calculations between two points, three points, and four points. The neural-networks provide increases over the linear MPA. The neural-network predictive performances are more than double the accuracy rate over their respective three-node and four-node linear predictions. A three-node example, the TL31 MPA increases to 17.24% and 34.48% for one percent and two percent, respectively. A four-node example, the TL41 MPA is increased to 14.29% and 25.0% for one percent and two percent, respectively.

The 147 subjects' simulation MPA results are compiled and further summarized in Table 7. In the table, the compiled MPA rates for the examined subjects are reported. Again, overall, the neural-networks provided MPA rate increases over the linear MPA rates. For example, the TL31 MPA is increased to 47.17% and 53.23% for one percent and two percent, respectively. That results in increases of 71.8% and 56.4%, 84.0% and 80.1%, 71.7% and 54.3%, over the baseline, three-node linear, and four-node linear, respectively. These results provide evidence to utilize neural-networks for match score prediction in the CTARP Framework. During the testing, there were multiple neural-networks that provided improvements to the linear MPA. However, there was not one that performed better than another. Following the rule of thumb on training data to inputs ratio of 9:1 and 12:1 on three-node and four-node neural-networks, only the three-input, three-node neural-network configuration met the criteria. The neural-network configuration of four-input, four-node results in an input weight of 12. The smallest set of training data for one subject with a four-input, four-node neural-network is 120. This results in a ratio of 10:1, which below the required 12:1 rule of thumb for training data. Although this does not invalidate the data and simulations, it defines that the four-input, four-node neural-network configurations cannot satisfy the CTARP Framework for all subjects. The neural-network configuration of three-input, three-node results in an input weight of nine. The smallest set of training data for one subject with a three-input, three-node neural-network is 108. This results in a ratio of 12:1, clearly above the required 9:1 rule of thumb for training data. Therefore, this narrows the neural-network configurations to TL31, TTL331, LL31, LLL331, and TTP331. The three-input, three-node neural-network with the highest MPA rate is TL31. Therefore, the final neural-network configuration is TL31 for the CTARP Framework.

Table 6 – Sample Subject MPA Results

Type	#Pred	1%	Accuracy	2%	Accuracy
L2	37	2	5.41%	4	10.81%
L3	36	1	2.78%	3	5.56%
L4	35	1	2.86%	4	11.43%
TL31	29	5	17.24%	10	34.48%
TTL331	29	4	13.79%	8	27.59%
TL41	28	4	14.27%	7	25.00%
TTL441	28	4	14.27%	5	17.86%
LL31	29	3	10.35%	6	20.69%
LLL331	29	4	13.79%	5	17.24%
LL41	28	3	10.71%	4	14.29%
LLL441	28	4	14.27%	5	17.86%
TTP331	29	3	10.35%	7	24.14%
TTP441	28	4	14.27%	4	14.29%

Table 7 – Comparison of MPA Results

Type	Pred#	1%	Accuracy	2%	Accuracy
L2	3350	922	27.52%	1140	34.03%
L3	3238	830	25.63%	970	29.56%
L4	3125	858	27.46%	1078	34.50%
TL31	2294	1082	47.17%	1221	53.23%
TTL331	2294	1050	45.77%	1208	52.66%
TL41	2168	940	43.36%	1103	50.86%
TTL441	2168	971	44.79%	1100	50.74%
LL31	2294	1012	44.12%	1162	50.65%
LLL331	2294	1075	46.86%	1224	53.36%
LL41	2168	1026	47.33%	1122	51.75%
LLL441	2168	991	45.71%	1117	51.52%
TTP331	2294	993	43.29%	1153	50.26%
TTP441	2168	882	40.68%	1025	47.28%

4.3.2 Decay Error Estimation Experimental Results

The last step of the CTARP Framework determines opportunities for renewal of the subject’s template through examination of the re-enrollment point as predicted by the decay error estimation. Although the renewal prediction of the re-enrollment point is based on a threshold level set within the biometric-based authentication system, the threshold level is adjustable based on the desired accuracy rate. The large change value (greater than 100) signifying a re-enrollment opportunity was determined through the results of the testing. Although this point indicates a significant error, it does not necessarily mean the subject needs to be renewed. The renewal is based on the biometric-based authentication system threshold level that is set by the system administrator [WaJ05]. For example, if the match threshold level is set at 0.80, this may result in one single re-enrollment point. A lower threshold level allows for a greater amount of error between the enrollment template and the current verification template being used for the match comparison. This translate into longer periods of time before a re-enrollment may be needed for the subject. Figure 36 is representative of an 80-percent matching threshold where only one re-enrollment point is valid for renewal, as circled. Although the match threshold is decreased in the example, the Decay Error score threshold can be increased to produce the same desired affect of the re-enrollment point.

However, if the matching threshold level is increased and set at 0.90, this may result in multiple re-enrollment points. A higher threshold level allows for less error between the enrollment template and the current verification template being used for the match comparison. This translate into shorter periods of time before re-enrollment that will be needed for the subject. Figure 37 is representative of a 90-percent matching threshold level that resulted in multiple valid re-enrollment points for renewal, as circled. Although the match threshold is increased in the example, the Decay Error score threshold can be lowed to achieve the same desired change affect to the re-enrollment point.

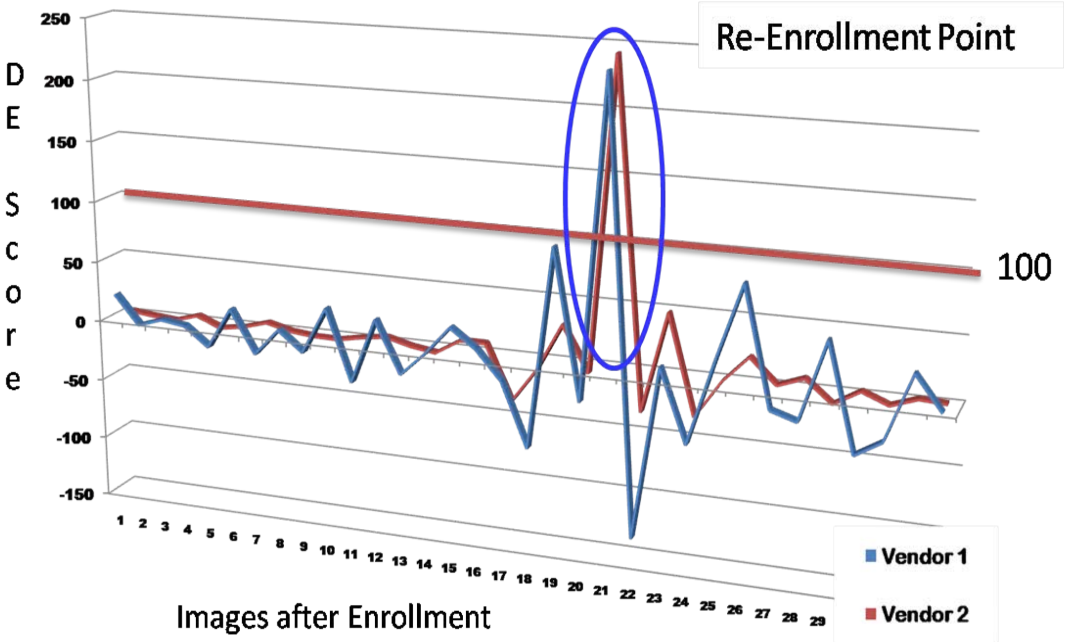


Figure 36 – 80-Percent Threshold Subject Predictive Re-Enrollment Point Plot

The simulation results are further summarized in Table 8. In the table, reported is a sampling of representative example subjects that have re-enrollment points with decay error estimates greater than 100. As a scenario is executing the CTARP Framework and going through the iterations of the template-aged steps, a subject's image is added to the CTARP Framework one at a time, simulating the verifications and aging over time. A 'next' match score prediction and corresponding 'next' error score prediction is calculated. This new error score is then entered in the template renewal prediction algorithm (TRPA) to determine the DE estimate. If the DE estimate is greater than the threshold, this indicates a predicted possible re-enrollment opportunity. For example, the Subject with ID number 02463 and Image Number 256 is the 24th image of 38 in the series. This subject's match score has changed (aged) enough from enrollment for the decay error estimate to cross the set threshold level, therefore indicating a favorable opportunity for template renewal.

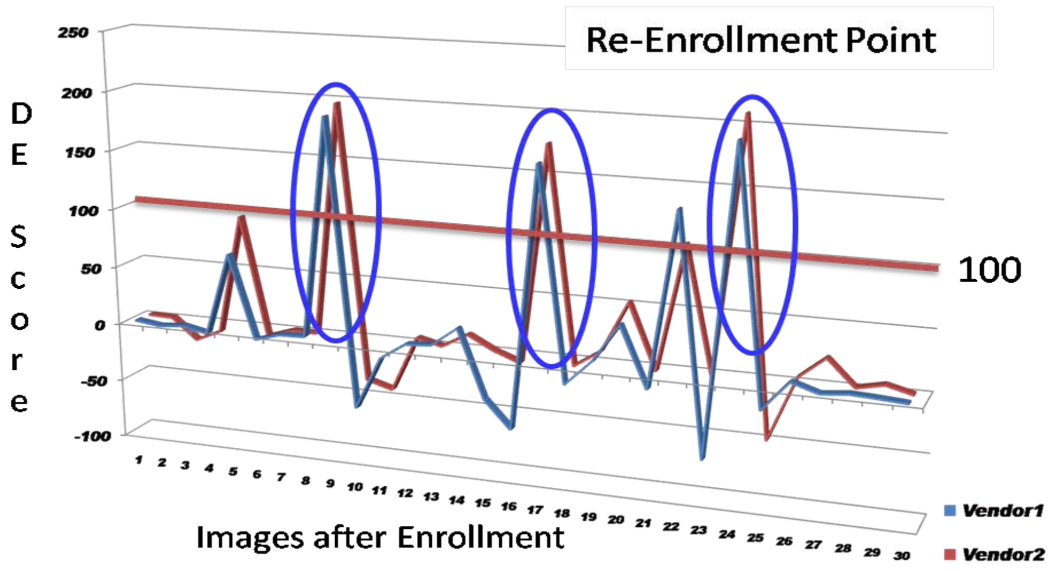


Figure 37 – 90-Percent Threshold Subject Predictive Re-Enrollment Point Plot

Table 8 – Subject Error Prediction and Re-Enrollment Results

SubjectID	Image#	Sequence#	Prediction	Ave Slope	DE	CrossThreshold
02463	256	24 of 38	0.166	0.0020	103	Yes
02463	309	32 of 38	0.246	0.0020	119	Yes
04211	138	24 of 35	0.227	0.0005	418	Yes
04212	166	23 of 30	0.352	0.0004	835	Yes
04222	162	32 of 36	0.179	0.0002	731	Yes
04233	64	12 of 30	0.210	0.0009	239	Yes

The simulation results of the CTARP Framework and decay error estimation, or re-enrollment points, have similar results from both commercial vendor algorithms, as further summarized in Table 9. In the table, only a few representative example subjects are reported, although there were multiple subjects (30 out of 147, or 20%) with decay error estimate values indicating renewal from both commercial algorithms/SDKs. For example, the Subject with ID number 04213 and Image Number 64 is a predictive re-enrollment point matched by both algorithms/SDKs. The decay error estimate for Vendor 1 is 167 and the decay error estimate for Vendor 2 is 191. This subject has decay error estimates that cross the set threshold and have results closely related although different algorithms are used. Therefore, this subject's example indicates a possible opportunity for template renewal is predicted through the CTARP Framework using the TRPA and the DE estimate.

Table 9 – Verified Subject Error Prediction and Re-Enrollment Results

Subject ID	Image #	Seq #	CrossThreshold	V1 DE est.	V2 DE est.
04212	138	24	Y	417	249
04213	64	12	Y	167	191
04233	167	24	Y	270	204
68158	21M41	22	Y	105	592
69975	17M52	18	Y	164	175

4.4 Summary

Analysis was performed on two different publicly available datasets simulating an aging environment and using two commercially available facial matching algorithms with associated software development kits. In all simulated cases, the CTARP Framework demonstrated template aging and prediction ability of template renewals. As the template aging increased over time without renewal, eventually, there would have been an increase false rejection rates. With the template renewal being predicted and then the subject being re-enrolled, the false rejection rates have improved, prolonging the degradation of the false rejection rates. This was accomplished even with a higher threshold level where the false rejection rates would increase more quickly than if the threshold level was at a lower level. The CTARP Framework primary objectives of improving security and being able to predict when it is now time to renew an aging template was achieved, as demonstrated by the template aging and renewal prediction followed by re-enrollment as opposed to waiting for the subject to start receiving false rejections to the biometric-based authentication system.

V. Conclusion

5.1 Summary of Research

Relatively few research efforts are aimed at solving the biological aging issue as it pertains to biometric systems or even the biometric template aging process. Most research being pursued in biometrics is related to improving recognition or matching algorithms, improving modality recognition, or delving into new modalities. None of the known research, though, specifically addressed a template aging and renewal prediction environment, nor do they completely address the issues facing a structured process or framework to deal with template aging.

After a rigorous search through the literature to survey the history and determine the state-of-the-art of biometrics, template aging, and template renewal and predictions, this research provides a structured approach to template aging and renewal prediction by developing the novel Carls Template Aging and Renewal Prediction (CTARP) Framework.

This research is the leading edge of solving issues related to biometric template aging. This research has the potential of having long-term ramifications with the ability to apply the CTARP Framework to all biometric modalities as well as future ones. This fusion of template aging and renewal prediction factors can be combined to make biometric applications more readily reliable, improving biometric system performance. If most advantageous periodic renewals to the template are determined, this will have an overall improvement in the error rates without the higher cost of continuous renewal or decreased error rates of static templates. This will ultimately enhance the security of the biometric system.

5.2 Research Contributions

The CTARP Framework provides improved biometrics security through template renewal and decreasing the number of false rejections in a biometric-based authentication infrastructure. This research produced a novel framework that can be applied to numerous biometric-based authentication systems. The CTARP Framework provides an improved renewal method over the current continuous or static renewal methods, which translates into the availability of more resources. Improved (decreased) error rates mean fewer false rejections, which translates to higher user acceptability. Higher user acceptability translates into more users willing to adopt the technology of biometric-based authentication systems over the less secure knowledge-based counterparts.

5.3 Publications

To date, two papers have been accepted and published in international conferences. Additionally, one draft conference paper and one draft journal article are prepared for submission and review. Specific titles and publication venues are listed at the end of this chapter.

5.4 Recommendations for Future Research

5.4.1 Adapt CTARP Framework to Other Modalities

With relatively minor adjustments, the CTARP Framework can be applied to other biometric modalities. All biometrics deal with an aging challenge, although some modalities age more rapidly than other modalities. The more rapidly changing behavioral biometric modalities, such as keystroke, handwriting, voice, or gait, would benefit immediately from the CTARP Framework, where the less rapidly changing biological modalities, such as fingerprint and iris, would need further research and adjustments to adopt the CTARP Framework.

5.4.2 Incorporate Features from the Template Aging or Renewal Prediction Concepts

Another area of potential interest is to make use of the template aging or the renewal prediction frameworks. The concept of the Perfect Match Score Matrix provides a means to demonstrate template aging and prediction of the next match score. This can aide in decision-making on how to proceed with the next verification attempt for the subject. With the incorporation of a time domain, this conceptual methodology can be developed and applied to all biometric modalities. The concept of the Error Score Matrix and template renewal prediction and its associated algorithm can be improved upon producing a higher accuracy rate on the prediction of re-enrollment opportunities. While these concepts do not improve upon or develop matching algorithms, its application to other modalities needs to be further studied. The Template Renewal Prediction Algorithm of the Decay Error estimation (associated with the Error Score Matrix and template renewal prediction) can be improved upon by determining a true time delta instead of using image indexes to represent a time delta. With additional research, time differential concerns and the inconsistencies between the modalities can be addressed within the TRPA. While these concepts do not improve upon or develop matching algorithms, its application to other modalities needs to be further studied.

5.4.3 Incorporate Fuzzy Logic into Template Aging or Renewal Prediction Concepts

One further area of potential interest is to incorporate fuzzy logic into the template aging, the renewal prediction concepts, and/or the CTARP Framework. Using the concept of fuzzy logic provides an alternative means to demonstrate template aging and prediction of the next match score. Using additional factors such as age groups (at certain periods of age, the face changes more rapidly, such as people in their mid-20's, mid 30's, and 50's [RiB05, TaS00]), time of separation from enrollment, race, or gender. This can aide in decision-making on how to proceed with the next verification attempt for the subject.

5.4.4 Adapt CTARP Framework for False Acceptance Rate improvement

Supplementary potential interest is to cultivate and extend CTARP to address false acceptance rates, similarly to the false rejection rates discussed. The separating drift of one's template through aging addressed the false rejection rate. However, additional research needs to address false acceptance rates. One potential solution would be to research the possible narrowing drift of one's template towards another in the system allowing a potential increase in false acceptance rates. An increase in false acceptance rates can cause undue security problems, therefore requiring further research.

Publications

Published (2):

[CaR08a] John W. Carls, Richard A. Raines, Michael R. Grimaila, Steven K. Rogers, "Biometric Security Enhancements Through Template Aging Match Score Analysis", *Proceedings of the 3rd International Conference on Information Warfare and Security,* Omaha, NE (Approximately 50% Acceptance Rate)

[CaR08b] John W. Carls, Richard A. Raines, Michael R. Grimaila, Steven K. Rogers, "Biometric Enhancements: Template Aging Error Score Analysis", *Proceedings of the 8th IEEE International Conference on Automatic Face and Gesture Recognition*, Amsterdam, Netherlands (Special Session Invitation)

Drafted (2):

[CaR08c] John W. Carls, Richard A. Raines, Michael R. Grimaila, Steven K. Rogers, "Improved Biometric Score Predictions using Neural Networks", Carnegie Mellon CyLab ROBUST Workshop, *Proceedings of ROBUST 2008: The Robust Biometrics: Understanding the Science and Technology Workshop*, Honolulu, HI. Submission Deadline: September 10, 2009. Conference Date: November 2-5, 2008.

[CaR09] John W. Carls, Richard A. Raines, Michael R. Grimaila, Steven K. Rogers, "Biometric Enhancements: Template Aging and Renewal Prediction ", *Proceedings of IEEE Systems Journal Special Issue on "Biometrics Systems"*. Submission Deadline: January 15, 2009. Publication Date: August 2009.

VI. Appendix

This section presents the modified C++ source code, where not copyright protected or proprietary, and printout of the MatLab® code. A sample printout of the MatLab® code for the neural-networks is also attached in this section. Numerous versions of the C++ and MatLab® code were used throughout development. Within each version, the neural-network variations of the code were modified as needed to accommodate the parameter changes for each scenario. The core architectural portion of the code, however, was not modified after verification and validation, and was carried through in each version unaltered.

6.1 Verilook Code

This is the modified code used to generate the score comparison table matrix.

```
/**
 * Class CMainFrame, implements application main window.
 *
 * Copyright (C) 2003-2007 Neurotechnologija
 */

// adding file operations
#include <iostream>
using std::ios;
#include <fstream>
using std::ofstream;
// end of add file operations

/**
 * Outputs message to right log window.
 * @param      msg    message text
 *                    v       similarity value
 */
void CMainFrame::LogMessageRight
{
        // adding text file output
        ofstream outfile;
        outfile.open("MatchScore.txt", ios::app);
        // adding score to outfile
        outfile << v << ", ";
        outfile.close();
        // end add to outfile
}

/**
 * Matches face to entire face database.
 */
void CMainFrame::OnJobsMatch()
{
               // adding linefeed to text file output
               ofstream outfile;
               outfile.open("MatchScore.txt", ios::app);
               // adding End of Line marker to outfile
               outfile << "EOL \n ";
               outfile.close();
               // end add to outfile

}

void CMainFrame::DoEnroll(void* features, const string & newFaceID)
{
               //Adding Enrollment Filename to MatchScore.txt
               ofstream outfile;
               outfile.open("MatchScore.txt", ios::app);
               // adding filename to outfile
               outfile << faceID.c_str() << ", ";
               outfile.close();
               // end add to outfile
}

void CMainFrame::DoMatch(void* features, bool forceSingleMatch)
{
                              // adding similarity score to outfile
                              // outfile << lst[i].similarity << ", ";
                              // end adding similarity score to outfile
        // close outfile("MatchScore.txt")
        // outfile.close();
        // end add to outfile
}
```

6.2 Cognitec Code

Call_Enroll.bat

```
CD .\Subj_001
CALL enroll.bat
cd ..
```

Call_Match.bat

```
CD .\Subj_004
CALL match.bat > Cog_Score.txt
cd ..

for   %%f   in   (*.jpg)   do   G:\FVSDK_6_3_0\examples\cpp_original\x86_32\enroll
G:\FVSDK_6_3_0\bin\x86_32\frsdk.cfg  %%f.fir %%f

for     %%f     in     (*.fir)     do     (for     %%g     in     (*.fir)     do
(G:\FVSDK_6_3_0\examples\cpp_original\x86_32\match
G:\FVSDK_6_3_0\bin\x86_32\frsdk.cfg %%f %%g))

// Program to read in Cog_Score file and output scores
#include <iostream>
#include <fstream>
#include <string>
using namespace std;
using std::string;
using std::getline;

int main()
{
  ifstream inFile;
  ofstream outFile;
```

```
          string text_line;
          char ch;
          int score;

          ifstream inFile("Cog_Score.txt", ios::in);

          if (! inFile){
             cout << " Unable to open inFile" << endl;
                exit(1);
          }

          outFile.open("Cog_Score_Matrix.txt");

          if (! outFile){
             cout << " Unable to open out file" << endl;
                exit(1);
          }

          while (!inFile.eof())
          {
               inFile.ignore(100, '#');
               inFile.ignore(6, ':');
               inFile.get(score);
            ofstream outFile(score, ", ", ios::app);
            // outFile.put(score, ', ');
          }
          inFile.close();
          outFile.close();
        }
```

6.3 MATLAB Code

```
% Neural Net Feed Fwd 3 node predictor
% LCDR John W. Carls, USN
% This file is used to read in matching scores and predict the next score
% using a feed-forward neural network prediction.
% Training Inputs [1x3], Targets [1x1] are from Even Rows
% Validation Inputs [1x3], Targets [1x1] are from Odd Rows
% Prediction Inputs [1x3] are from First Row
% Prediction Results [1x1] are from Trained Neural Net
% an compared against Actual Scores [1x1] from First Row
% Structure:
%           Test_Subj: scores    [square]
%                      t_inputs  [X x 3] = training inputs
%                      t_targets [X x 1] = training targets
%                      v_inputs  [X x 3] = validation inputs
%                      v_targets [X x 1] = validation targets
%                      v_results [X x 1] = validation results
%                      p_inputs  [X x 3] = prediction inputs
%                      p_results [X x 1] = prediction results
%                      a_results [X x 1] = actual results
%
close all;
clear;
clc;

% Read in files
files = dir('Subj_*.xls');
% for i = 1 : numel(files)
%     Test_xls = files(i).name
% end
% Loop through files in directory
for i = 1 : numel(files)
    % Load Test Subject
    % Subj = 'Subj_04207';
    % Subj_xls = [Subj,'.xls'];
    Subj_xls = files(i).name;
    Test_Subj.t_inputs = xlsread(Subj_xls,'V_3_Node','S2:U37');
    Test_Subj.t_targets = xlsread(Subj_xls,'V_3_Node','V2:V37');
    Test_Subj.v_inputs = xlsread(Subj_xls,'V_3_Node','W2:Y29');
    Test_Subj.v_targets = xlsread(Subj_xls,'V_3_Node','Z2:Z29');
    Test_Subj.p_inputs = xlsread(Subj_xls,'V_3_Node','AA2:AC14');
    Test_Subj.a_results = xlsread(Subj_xls,'V_3_Node','AD2:AD14');

    % v_size = 72;
    [v_size,y] = size(Test_Subj.v_inputs);
    % p_size = 29;
    [p_size,y] = size(Test_Subj.p_inputs);
    epochs = 200;

    %Copy structure
    V_X1 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    V_net1 = newff([min(V_X1.t_inputs)' max(V_X1.t_inputs)'],[3 1],{'tansig' 'logsig'});
    V_net1.trainParam.epochs = epochs;
    % Train neuralnet
    V_net1 = train(V_net1,V_X1.t_inputs',V_X1.t_targets');
    % Validate neuralnet
    V_X1.v_results = sim(V_net1,V_X1.v_inputs');
    % Predictions
    V_X1.p_results = sim(V_net1,V_X1.p_inputs');
%               figure,    plot(1:v_size,V_X1.v_results,'.-c',1:v_size,V_X1.v_targets','.-
b',1:p_size,V_X1.p_results,'.-r',1:p_size,V_X1.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('V Neural Net Tansig Logsig 3 1')
    xlswrite(Subj_xls,V_X1.v_inputs,'V_Tan_Log_3_1','A2')
    xlswrite(Subj_xls,V_X1.v_targets,'V_Tan_Log_3_1','E2')
    xlswrite(Subj_xls,V_X1.v_results','V_Tan_Log_3_1','F2')
    xlswrite(Subj_xls,V_X1.p_inputs,'V_Tan_Log_3_1','G2')
    xlswrite(Subj_xls,V_X1.p_results','V_Tan_Log_3_1','K2')
    xlswrite(Subj_xls,V_X1.a_results,'V_Tan_Log_3_1','L2')

    %Copy structure
    V_X2 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    V_net2 = newff([min(V_X2.t_inputs)' max(V_X2.t_inputs)'],[3 1],{'logsig' 'logsig'});
    V_net2.trainParam.epochs = epochs;
    % Train neuralnet
    V_net2 = train(V_net2,V_X2.t_inputs',V_X2.t_targets');
    % Validate neuralnet
    V_X2.v_results = sim(V_net2,V_X2.v_inputs');
    % Predictions
    V_X2.p_results = sim(V_net2,V_X2.p_inputs');
%               figure,    plot(1:v_size,V_X2.v_results,'.-c',1:v_size,V_X2.v_targets','.-
b',1:p_size,V_X2.p_results,'.-r',1:p_size,V_X2.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('V Neural Net Logsig Logsig 3 1')
    xlswrite(Subj_xls,V_X2.v_inputs,'V_Log_Log_3_1','A2')
    xlswrite(Subj_xls,V_X2.v_targets,'V_Log_Log_3_1','E2')
    xlswrite(Subj_xls,V_X2.v_results','V_Log_Log_3_1','F2')
    xlswrite(Subj_xls,V_X2.p_inputs,'V_Log_Log_3_1','G2')
    xlswrite(Subj_xls,V_X2.p_results','V_Log_Log_3_1','K2')
    xlswrite(Subj_xls,V_X2.a_results,'V_Log_Log_3_1','L2')

    %Copy structure
    V_X3 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    V_net3  =  newff([min(V_X3.t_inputs)'  max(V_X3.t_inputs)'],[3  3  1],{'tansig'  'tansig'
'purelin'});
    V_net3.trainParam.epochs = epochs;
    % Train neuralnet
    V_net3 = train(V_net3,V_X3.t_inputs',V_X3.t_targets');
    % Validate neuralnet
    V_X3.v_results = sim(V_net3,V_X3.v_inputs');
    % Predictions
    V_X3.p_results = sim(V_net3,V_X3.p_inputs');
%               figure,    plot(1:v_size,V_X3.v_results,'.-c',1:v_size,V_X3.v_targets','.-
b',1:p_size,V_X3.p_results,'.-r',1:p_size,V_X3.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('V Neural Net Tansig Tansig Purelin 3 3 1')
    xlswrite(Subj_xls,V_X3.v_inputs,'V_Tan_Tan_Pur_3_3_1','A2')
    xlswrite(Subj_xls,V_X3.v_targets,'V_Tan_Tan_Pur_3_3_1','E2')
    xlswrite(Subj_xls,V_X3.v_results','V_Tan_Tan_Pur_3_3_1','F2')
    xlswrite(Subj_xls,V_X3.p_inputs,'V_Tan_Tan_Pur_3_3_1','G2')
    xlswrite(Subj_xls,V_X3.p_results','V_Tan_Tan_Pur_3_3_1','K2')
    xlswrite(Subj_xls,V_X3.a_results,'V_Tan_Tan_Pur_3_3_1','L2')

    %Copy structure
    V_X4 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    V_net4  =  newff([min(V_X4.t_inputs)'  max(V_X4.t_inputs)'],[3  3  1],{'tansig'  'tansig'
'logsig'});
    V_net4.trainParam.epochs = epochs;
    % Train neuralnet
    V_net4 = train(V_net4,V_X4.t_inputs',V_X4.t_targets');
    % Validate neuralnet
    V_X4.v_results = sim(V_net4,V_X4.v_inputs');
    % Predictions
    V_X4.p_results = sim(V_net4,V_X4.p_inputs');
%               figure,    plot(1:v_size,V_X4.v_results,'.-c',1:v_size,V_X4.v_targets','.-
b',1:p_size,V_X4.p_results,'.-r',1:p_size,V_X4.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('V Neural Net Tansig Tansig Logsig 3 3 1')
    xlswrite(Subj_xls,V_X4.v_inputs,'V_Tan_Tan_Log_3_3_1','A2')
    xlswrite(Subj_xls,V_X4.v_targets,'V_Tan_Tan_Log_3_3_1','E2')
    xlswrite(Subj_xls,V_X4.v_results','V_Tan_Tan_Log_3_3_1','F2')
    xlswrite(Subj_xls,V_X4.p_inputs,'V_Tan_Tan_Log_3_3_1','G2')
    xlswrite(Subj_xls,V_X4.p_results','V_Tan_Tan_Log_3_3_1','K2')
    xlswrite(Subj_xls,V_X4.a_results,'V_Tan_Tan_Log_3_3_1','L2')

    %Copy structure
    V_X5 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    V_net5  =  newff([min(V_X5.t_inputs)'  max(V_X5.t_inputs)'],[3  3  1],{'logsig'  'logsig'
'logsig'});
    V_net5.trainParam.epochs = epochs;
    % Train neuralnet
    V_net5 = train(V_net5,V_X5.t_inputs',V_X5.t_targets');
    % Validate neuralnet
    V_X5.v_results = sim(V_net5,V_X5.v_inputs');
    % Predictions
    V_X5.p_results = sim(V_net5,V_X5.p_inputs');
%               figure,    plot(1:v_size,V_X5.v_results,'.-c',1:v_size,V_X5.v_targets','.-
b',1:p_size,V_X5.p_results,'.-r',1:p_size,V_X5.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('V Neural Net Logsig Logsig Logsig 3 3 1')
    xlswrite(Subj_xls,V_X5.v_inputs,'V_Log_Log_Log_3_3_1','A2')
    xlswrite(Subj_xls,V_X5.v_targets,'V_Log_Log_Log_3_3_1','E2')
    xlswrite(Subj_xls,V_X5.v_results','V_Log_Log_Log_3_3_1','F2')
    xlswrite(Subj_xls,V_X5.p_inputs,'V_Log_Log_Log_3_3_1','G2')
    xlswrite(Subj_xls,V_X5.p_results','V_Log_Log_Log_3_3_1','K2')
    xlswrite(Subj_xls,V_X5.a_results,'V_Log_Log_Log_3_3_1','L2')

    % Repeat for Cognitec
    Test_Subj.t_inputs = xlsread(Subj_xls,'C_3_Node','S2:U37');
    Test_Subj.t_targets = xlsread(Subj_xls,'C_3_Node','V2:V37');
    Test_Subj.v_inputs = xlsread(Subj_xls,'C_3_Node','W2:Y29');
    Test_Subj.v_targets = xlsread(Subj_xls,'C_3_Node','Z2:Z29');
    Test_Subj.p_inputs = xlsread(Subj_xls,'C_3_Node','AA2:AC14');
    Test_Subj.a_results = xlsread(Subj_xls,'C_3_Node','AD2:AD14');

    %Copy structure
    C_X1 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    C_net1 = newff([min(C_X1.t_inputs)' max(C_X1.t_inputs)'],[3 1],{'tansig' 'logsig'});
    C_net1.trainParam.epochs = epochs;
    % Train neuralnet
    C_net1 = train(C_net1,C_X1.t_inputs',C_X1.t_targets');
    % Validate neuralnet
    C_X1.v_results = sim(C_net1,C_X1.v_inputs');
    % Predictions
    C_X1.p_results = sim(C_net1,C_X1.p_inputs');
%               figure,    plot(1:v_size,C_X1.v_results,'.-c',1:v_size,C_X1.v_targets','.-
b',1:p_size,C_X1.p_results,'.-r',1:p_size,C_X1.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('C Neural Net Tansig Logsig 3 1')
    xlswrite(Subj_xls,C_X1.v_inputs,'C_Tan_Log_3_1','A2')
    xlswrite(Subj_xls,C_X1.v_targets,'C_Tan_Log_3_1','E2')
    xlswrite(Subj_xls,C_X1.v_results','C_Tan_Log_3_1','F2')
    xlswrite(Subj_xls,C_X1.p_inputs,'C_Tan_Log_3_1','G2')
    xlswrite(Subj_xls,C_X1.p_results','C_Tan_Log_3_1','K2')
    xlswrite(Subj_xls,C_X1.a_results,'C_Tan_Log_3_1','L2')

    %Copy structure
    C_X2 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    C_net2 = newff([min(C_X2.t_inputs)' max(C_X2.t_inputs)'],[3 1],{'logsig' 'logsig'});
    C_net2.trainParam.epochs = epochs;
    % Train neuralnet
    C_net2 = train(C_net2,C_X2.t_inputs',C_X2.t_targets');
    % Validate neuralnet
    C_X2.v_results = sim(C_net2,C_X2.v_inputs');
    % Predictions
    C_X2.p_results = sim(C_net2,C_X2.p_inputs');
%               figure,    plot(1:v_size,C_X2.v_results,'.-c',1:v_size,C_X2.v_targets','.-
b',1:p_size,C_X2.p_results,'.-r',1:p_size,C_X2.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('C Neural Net Logsig Logsig 3 1')
    xlswrite(Subj_xls,C_X2.v_inputs,'C_Log_Log_3_1','A2')
    xlswrite(Subj_xls,C_X2.v_targets,'C_Log_Log_3_1','E2')
    xlswrite(Subj_xls,C_X2.v_results','C_Log_Log_3_1','F2')
    xlswrite(Subj_xls,C_X2.p_inputs,'C_Log_Log_3_1','G2')
    xlswrite(Subj_xls,C_X2.p_results','C_Log_Log_3_1','K2')
    xlswrite(Subj_xls,C_X2.a_results,'C_Log_Log_3_1','L2')

    %Copy structure
    C_X3 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    C_net3  =  newff([min(C_X3.t_inputs)'  max(C_X3.t_inputs)'],[3  3  1],{'tansig'  'tansig'
'purelin'});
    C_net3.trainParam.epochs = epochs;
    % Train neuralnet
    C_net3 = train(C_net3,C_X3.t_inputs',C_X3.t_targets');
    % Validate neuralnet
    C_X3.v_results = sim(C_net3,C_X3.v_inputs');
    % Predictions
    C_X3.p_results = sim(C_net3,C_X3.p_inputs');
%               figure,    plot(1:v_size,C_X3.v_results,'.-c',1:v_size,C_X3.v_targets','.-
b',1:p_size,C_X3.p_results,'.-r',1:p_size,C_X3.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('C Neural Net Tansig Tansig Purelin 3 3 1')
    xlswrite(Subj_xls,C_X3.v_inputs,'C_Tan_Tan_Pur_3_3_1','A2')
    xlswrite(Subj_xls,C_X3.v_targets,'C_Tan_Tan_Pur_3_3_1','E2')
    xlswrite(Subj_xls,C_X3.v_results','C_Tan_Tan_Pur_3_3_1','F2')
    xlswrite(Subj_xls,C_X3.p_inputs,'C_Tan_Tan_Pur_3_3_1','G2')
    xlswrite(Subj_xls,C_X3.p_results','C_Tan_Tan_Pur_3_3_1','K2')
    xlswrite(Subj_xls,C_X3.a_results,'C_Tan_Tan_Pur_3_3_1','L2')

    %Copy structure
    C_X4 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    C_net4  =  newff([min(C_X4.t_inputs)'  max(C_X4.t_inputs)'],[3  3  1],{'tansig'  'tansig'
'logsig'});
    C_net4.trainParam.epochs = epochs;
    % Train neuralnet
    C_net4 = train(C_net4,C_X4.t_inputs',C_X4.t_targets');
    % Validate neuralnet
    C_X4.v_results = sim(C_net4,C_X4.v_inputs');
    % Predictions
    C_X4.p_results = sim(C_net4,C_X4.p_inputs');
%               figure,    plot(1:v_size,C_X4.v_results,'.-c',1:v_size,C_X4.v_targets','.-
b',1:p_size,C_X4.p_results,'.-r',1:p_size,C_X4.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('C Neural Net Tansig Tansig Logsig 3 3 1')
    xlswrite(Subj_xls,C_X4.v_inputs,'C_Tan_Tan_Log_3_3_1','A2')
    xlswrite(Subj_xls,C_X4.v_targets,'C_Tan_Tan_Log_3_3_1','E2')
    xlswrite(Subj_xls,C_X4.v_results','C_Tan_Tan_Log_3_3_1','F2')
    xlswrite(Subj_xls,C_X4.p_inputs,'C_Tan_Tan_Log_3_3_1','G2')
    xlswrite(Subj_xls,C_X4.p_results','C_Tan_Tan_Log_3_3_1','K2')
    xlswrite(Subj_xls,C_X4.a_results,'C_Tan_Tan_Log_3_3_1','L2')

    %Copy structure
    C_X5 = Test_Subj;
    % Define Neural Network using FeedFwd
    % Parameters for newff( [min max], [#neurons, output],{txfunc, txfunc})
    C_net5  =  newff([min(C_X5.t_inputs)'  max(C_X5.t_inputs)'],[3  3  1],{'logsig'  'logsig'
'logsig'});
    C_net5.trainParam.epochs = epochs;
    % Train neuralnet
    C_net5 = train(C_net5,C_X5.t_inputs',C_X5.t_targets');
    % Validate neuralnet
    C_X5.v_results = sim(C_net5,C_X5.v_inputs');
    % Predictions
    C_X5.p_results = sim(C_net5,C_X5.p_inputs');
%               figure,    plot(1:v_size,C_X5.v_results,'.-c',1:v_size,C_X5.v_targets','.-
b',1:p_size,C_X5.p_results,'.-r',1:p_size,C_X5.a_results','.-g')
%    legend('V Scores','V Target','Pred Scores','Actual Score')
%    title('C Neural Net Logsig Logsig Logsig 3 3 1')
    xlswrite(Subj_xls,C_X5.v_inputs,'C_Log_Log_Log_3_3_1','A2')
    xlswrite(Subj_xls,C_X5.v_targets,'C_Log_Log_Log_3_3_1','E2')
    xlswrite(Subj_xls,C_X5.v_results','C_Log_Log_Log_3_3_1','F2')
    xlswrite(Subj_xls,C_X5.p_inputs,'C_Log_Log_Log_3_3_1','G2')
    xlswrite(Subj_xls,C_X5.p_results','C_Log_Log_Log_3_3_1','K2')
    xlswrite(Subj_xls,C_X5.a_results,'C_Log_Log_Log_3_3_1','L2')
end
exit

       %
       close all;
       clear;
       clc;
       % 1 percent
       VTanLog31_1p = 0;
       VTanTanLog331_1p = 0;
       VTanLog41_1p = 0;
       VTanTanLog441_1p = 0;
       VLogLog31_1p = 0;
       VLogLogLog331_1p = 0;
       VLogLog41_1p = 0;
       VLogLogLog441_1p = 0;
       VTanTanPur331_1p = 0;
       VTanTanPur441_1p = 0;
       CTanLog31_1p = 0;
       CTanTanLog331_1p = 0;
       CTanLog41_1p = 0;
       CTanTanLog441_1p = 0;
       CLogLog31_1p = 0;
       CLogLogLog331_1p = 0;
       CLogLog41_1p = 0;
```

```
CLogLogLog441_1p = 0;
CTanTanPur331_1p = 0;
CTanTanPur441_1p = 0;
% 2 percent
VTanLog31_2p = 0;
VTanTanLog331_2p = 0;
VTanLog41_2p = 0;
VTanTanLog441_2p = 0;
VLogLog31_2p = 0;
VLogLogLog331_2p = 0;
VLogLog41_2p = 0;
VLogLogLog441_2p = 0;
VTanTanPur331_2p = 0;
VTanTanPur441_2p = 0;
CTanLog31_2p = 0;
CTanTanLog331_2p = 0;
CTanLog41_2p = 0;
CTanTanLog441_2p = 0;
CLogLog31_2p = 0;
CLogLogLog331_2p = 0;
CLogLog41_2p = 0;
CLogLogLog441_2p = 0;
CTanTanPur331_2p = 0;
CTanTanPur441_2p = 0;
% Predictions
VTanLog31_p = 0;
VTanTanLog331_p = 0;
VTanLog41_p = 0;
VTanTanLog441_p = 0;
VLogLog31_p = 0;
VLogLogLog331_p = 0;
VLogLog41_p = 0;
VLogLogLog441_p = 0;
VTanTanPur331_p = 0;
VTanTanPur441_p = 0;
CTanLog31_p = 0;
CTanTanLog331_p = 0;
CTanLog41_p = 0;
CTanTanLog441_p = 0;
CLogLog31_p = 0;
CLogLogLog331_p = 0;
CLogLog41_p = 0;
CLogLogLog441_p = 0;
CTanTanPur331_p = 0;
CTanTanPur441_p = 0;

% Read in files
Totals_xls = 'Totals17.xls';
files = dir('Subj_*.xls');
fsize = numel(files);
for i = 1 : numel(files)
    % 1 percent
    Subj_xls = files(i).name;
    VTanLog31_1p = VTanLog31_1p + xlsread(Subj_xls,'Totals','C4');
    VTanTanLog331_1p = VTanTanLog331_1p + xlsread(Subj_xls,'Totals','C6');
    VTanLog41_1p = VTanLog41_1p + xlsread(Subj_xls,'Totals','C8');
    VTanTanLog441_1p = VTanTanLog441_1p + xlsread(Subj_xls,'Totals','C10');
    VLogLog31_1p = VLogLog31_1p + xlsread(Subj_xls,'Totals','C12');
    VLogLogLog331_1p = VLogLogLog331_1p + xlsread(Subj_xls,'Totals','C14');
    VLogLog41_1p = VLogLog41_1p + xlsread(Subj_xls,'Totals','C16');
    VLogLogLog441_1p = VLogLogLog441_1p + xlsread(Subj_xls,'Totals','C18');
    VTanTanPur331_1p = VTanTanPur331_1p + xlsread(Subj_xls,'Totals','C20');
    VTanTanPur441_1p = VTanTanPur441_1p + xlsread(Subj_xls,'Totals','C22');
    CTanLog31_1p = CTanLog31_1p + xlsread(Subj_xls,'Totals','I4');
    CTanTanLog331_1p = CTanTanLog331_1p + xlsread(Subj_xls,'Totals','I6');
    CTanLog41_1p = CTanLog41_1p + xlsread(Subj_xls,'Totals','I8');
    CTanTanLog441_1p = CTanTanLog441_1p + xlsread(Subj_xls,'Totals','I10');
    CLogLog31_1p = CLogLog31_1p + xlsread(Subj_xls,'Totals','I12');
    CLogLogLog331_1p = CLogLogLog331_1p + xlsread(Subj_xls,'Totals','I14');
    CLogLog41_1p = CLogLog41_1p + xlsread(Subj_xls,'Totals','I16');
    CLogLogLog441_1p = CLogLogLog441_1p + xlsread(Subj_xls,'Totals','I18');
    CTanTanPur331_1p = CTanTanPur331_1p + xlsread(Subj_xls,'Totals','I20');
    CTanTanPur441_1p = CTanTanPur441_1p + xlsread(Subj_xls,'Totals','I22');
    % 2 percent
    VTanLog31_2p = VTanLog31_2p + xlsread(Subj_xls,'Totals','D4');
    VTanTanLog331_2p = VTanTanLog331_2p + xlsread(Subj_xls,'Totals','D6');
    VTanLog41_2p = VTanLog41_2p + xlsread(Subj_xls,'Totals','D8');
    VTanTanLog441_2p = VTanTanLog441_2p + xlsread(Subj_xls,'Totals','D10');
    VLogLog31_2p = VLogLog31_2p + xlsread(Subj_xls,'Totals','D12');
    VLogLogLog331_2p = VLogLogLog331_2p + xlsread(Subj_xls,'Totals','D14');
    VLogLog41_2p = VLogLog41_2p + xlsread(Subj_xls,'Totals','D16');
    VLogLogLog441_2p = VLogLogLog441_2p + xlsread(Subj_xls,'Totals','D18');
    VTanTanPur331_2p = VTanTanPur331_2p + xlsread(Subj_xls,'Totals','D20');
    VTanTanPur441_2p = VTanTanPur441_2p + xlsread(Subj_xls,'Totals','D22');
    CTanLog31_2p = CTanLog31_2p + xlsread(Subj_xls,'Totals','J4');
    CTanTanLog331_2p = CTanTanLog331_2p + xlsread(Subj_xls,'Totals','J6');
    CTanLog41_2p = CTanLog41_2p + xlsread(Subj_xls,'Totals','J8');
    CTanTanLog441_2p = CTanTanLog441_2p + xlsread(Subj_xls,'Totals','J10');
    CLogLog31_2p = CLogLog31_2p + xlsread(Subj_xls,'Totals','J12');
    CLogLogLog331_2p = CLogLogLog331_2p + xlsread(Subj_xls,'Totals','J14');
    CLogLog41_2p = CLogLog41_2p + xlsread(Subj_xls,'Totals','J16');
    CLogLogLog441_2p = CLogLogLog441_2p + xlsread(Subj_xls,'Totals','J18');
    CTanTanPur331_2p = CTanTanPur331_2p + xlsread(Subj_xls,'Totals','J20');
    CTanTanPur441_2p = CTanTanPur441_2p + xlsread(Subj_xls,'Totals','J22');
    % predictions
    VTanLog31_p = VTanLog31_p + xlsread(Subj_xls,'Totals','E4');
    VTanTanLog331_p = VTanTanLog331_p + xlsread(Subj_xls,'Totals','E6');
    VTanLog41_p = VTanLog41_p + xlsread(Subj_xls,'Totals','E8');
    VTanTanLog441_p = VTanTanLog441_p + xlsread(Subj_xls,'Totals','E10');
    VLogLog31_p = VLogLog31_p + xlsread(Subj_xls,'Totals','E12');
    VLogLogLog331_p = VLogLogLog331_p + xlsread(Subj_xls,'Totals','E14');
    VLogLog41_p = VLogLog41_p + xlsread(Subj_xls,'Totals','E16');
    VLogLogLog441_p = VLogLogLog441_p + xlsread(Subj_xls,'Totals','E18');
    VTanTanPur331_p = VTanTanPur331_p + xlsread(Subj_xls,'Totals','E20');
    VTanTanPur441_p = VTanTanPur441_p + xlsread(Subj_xls,'Totals','E22');
    CTanLog31_p = CTanLog31_p + xlsread(Subj_xls,'Totals','K4');
    CTanTanLog331_p = CTanTanLog331_p + xlsread(Subj_xls,'Totals','K6');
    CTanLog41_p = CTanLog41_p + xlsread(Subj_xls,'Totals','K8');
    CTanTanLog441_p = CTanTanLog441_p + xlsread(Subj_xls,'Totals','K10');
    CLogLog31_p = CLogLog31_p + xlsread(Subj_xls,'Totals','K12');
    CLogLogLog331_p = CLogLogLog331_p + xlsread(Subj_xls,'Totals','K14');
    CLogLog41_p = CLogLog41_p + xlsread(Subj_xls,'Totals','K16');
    CLogLogLog441_p = CLogLogLog441_p + xlsread(Subj_xls,'Totals','K18');
    CTanTanPur331_p = CTanTanPur331_p + xlsread(Subj_xls,'Totals','K20');
    CTanTanPur441_p = CTanTanPur441_p + xlsread(Subj_xls,'Totals','K22');
end
% 1 percent
xlswrite(Totals_xls,VTanLog31_1p,'Totals','C8');
xlswrite(Totals_xls,VTanTanLog331_1p,'Totals','C12');
xlswrite(Totals_xls,VTanLog41_1p,'Totals','C16');
xlswrite(Totals_xls,VTanTanLog441_1p,'Totals','C20');
xlswrite(Totals_xls,VLogLog31_1p,'Totals','C24');
xlswrite(Totals_xls,VLogLogLog331_1p,'Totals','C28');
xlswrite(Totals_xls,VLogLog41_1p,'Totals','C32');
xlswrite(Totals_xls,VLogLogLog441_1p,'Totals','C36');
xlswrite(Totals_xls,VTanTanPur331_1p,'Totals','C40');
xlswrite(Totals_xls,VTanTanPur441_1p,'Totals','C44');
xlswrite(Totals_xls,CTanLog31_1p,'Totals','I8');
xlswrite(Totals_xls,CTanTanLog331_1p,'Totals','I12');
xlswrite(Totals_xls,CTanLog41_1p,'Totals','I16');
xlswrite(Totals_xls,CTanTanLog441_1p,'Totals','I20');
xlswrite(Totals_xls,CLogLog31_1p,'Totals','I24');
xlswrite(Totals_xls,CLogLogLog331_1p,'Totals','I28');
xlswrite(Totals_xls,CLogLog41_1p,'Totals','I32');
xlswrite(Totals_xls,CLogLogLog441_1p,'Totals','I36');
xlswrite(Totals_xls,CTanTanPur331_1p,'Totals','I40');
xlswrite(Totals_xls,CTanTanPur441_1p,'Totals','I44');
% 2 percent
xlswrite(Totals_xls,VTanLog31_2p,'Totals','D8');
xlswrite(Totals_xls,VTanTanLog331_2p,'Totals','D12');
xlswrite(Totals_xls,VTanLog41_2p,'Totals','D16');
xlswrite(Totals_xls,VTanTanLog441_2p,'Totals','D20');
xlswrite(Totals_xls,VLogLog31_2p,'Totals','D24');
xlswrite(Totals_xls,VLogLogLog331_2p,'Totals','D28');
xlswrite(Totals_xls,VLogLog41_2p,'Totals','D32');
xlswrite(Totals_xls,VLogLogLog441_2p,'Totals','D36');
xlswrite(Totals_xls,VTanTanPur331_2p,'Totals','D40');
xlswrite(Totals_xls,VTanTanPur441_2p,'Totals','D44');
xlswrite(Totals_xls,CTanLog31_2p,'Totals','J8');
xlswrite(Totals_xls,CTanTanLog331_2p,'Totals','J12');
xlswrite(Totals_xls,CTanLog41_2p,'Totals','J16');
xlswrite(Totals_xls,CTanTanLog441_2p,'Totals','J20');
xlswrite(Totals_xls,CLogLog31_2p,'Totals','J24');
xlswrite(Totals_xls,CLogLogLog331_2p,'Totals','J28');
xlswrite(Totals_xls,CLogLog41_2p,'Totals','J32');
xlswrite(Totals_xls,CLogLogLog441_2p,'Totals','J36');
xlswrite(Totals_xls,CTanTanPur331_2p,'Totals','J40');
xlswrite(Totals_xls,CTanTanPur441_2p,'Totals','J44');
% predictions
xlswrite(Totals_xls,VTanLog31_p,'Totals','E8');
xlswrite(Totals_xls,VTanTanLog331_p,'Totals','E12');
xlswrite(Totals_xls,VTanLog41_p,'Totals','E16');
xlswrite(Totals_xls,VTanTanLog441_p,'Totals','E20');
xlswrite(Totals_xls,VLogLog31_p,'Totals','E24');
xlswrite(Totals_xls,VLogLogLog331_p,'Totals','E28');
xlswrite(Totals_xls,VLogLog41_p,'Totals','E32');
xlswrite(Totals_xls,VLogLogLog441_p,'Totals','E36');
xlswrite(Totals_xls,VTanTanPur331_p,'Totals','E40');
xlswrite(Totals_xls,VTanTanPur441_p,'Totals','E44');
xlswrite(Totals_xls,CTanLog31_p,'Totals','K8');
xlswrite(Totals_xls,CTanTanLog331_p,'Totals','K12');
xlswrite(Totals_xls,CTanLog41_p,'Totals','K16');
xlswrite(Totals_xls,CTanTanLog441_p,'Totals','K20');
xlswrite(Totals_xls,CLogLog31_p,'Totals','K24');
xlswrite(Totals_xls,CLogLogLog331_p,'Totals','K28');
xlswrite(Totals_xls,CLogLog41_p,'Totals','K32');
xlswrite(Totals_xls,CLogLogLog441_p,'Totals','K36');
xlswrite(Totals_xls,CTanTanPur331_p,'Totals','K40');
xlswrite(Totals_xls,CTanTanPur441_p,'Totals','K44');
% 1 percent
xlswrite(Totals_xls,VTanLog31_1p/fsize,'Totals','C6');
xlswrite(Totals_xls,VTanTanLog331_1p/fsize,'Totals','C10');
xlswrite(Totals_xls,VTanLog41_1p/fsize,'Totals','C14');
xlswrite(Totals_xls,VTanTanLog441_1p/fsize,'Totals','C18');
xlswrite(Totals_xls,VLogLog31_1p/fsize,'Totals','C22');
xlswrite(Totals_xls,VLogLogLog331_1p/fsize,'Totals','C26');
xlswrite(Totals_xls,VLogLog41_1p/fsize,'Totals','C30');
xlswrite(Totals_xls,VLogLogLog441_1p/fsize,'Totals','C34');
xlswrite(Totals_xls,VTanTanPur331_1p/fsize,'Totals','C38');
xlswrite(Totals_xls,VTanTanPur441_1p/fsize,'Totals','C42');
xlswrite(Totals_xls,CTanLog31_1p/fsize,'Totals','I6');
xlswrite(Totals_xls,CTanTanLog331_1p/fsize,'Totals','I10');
xlswrite(Totals_xls,CTanLog41_1p/fsize,'Totals','I14');
xlswrite(Totals_xls,CTanTanLog441_1p/fsize,'Totals','I18');
xlswrite(Totals_xls,CLogLog31_1p/fsize,'Totals','I22');
xlswrite(Totals_xls,CLogLogLog331_1p/fsize,'Totals','I26');
xlswrite(Totals_xls,CLogLog41_1p/fsize,'Totals','I30');
xlswrite(Totals_xls,CLogLogLog441_1p/fsize,'Totals','I34');
xlswrite(Totals_xls,CTanTanPur331_1p/fsize,'Totals','I38');
xlswrite(Totals_xls,CTanTanPur441_1p/fsize,'Totals','I42');
% 2 percent
xlswrite(Totals_xls,VTanLog31_2p/fsize,'Totals','D6');
xlswrite(Totals_xls,VTanTanLog331_2p/fsize,'Totals','D10');
xlswrite(Totals_xls,VTanLog41_2p/fsize,'Totals','D14');
xlswrite(Totals_xls,VTanTanLog441_2p/fsize,'Totals','D18');
xlswrite(Totals_xls,VLogLog31_2p/fsize,'Totals','D22');
xlswrite(Totals_xls,VLogLogLog331_2p/fsize,'Totals','D26');
xlswrite(Totals_xls,VLogLog41_2p/fsize,'Totals','D30');
xlswrite(Totals_xls,VLogLogLog441_2p/fsize,'Totals','D34');
xlswrite(Totals_xls,VTanTanPur331_2p/fsize,'Totals','D38');
```

```
        xlswrite(Totals_xls,VTanTanPur441_2p/fsize,'Totals','D42');
        xlswrite(Totals_xls,CTanLog31_2p/fsize,'Totals','J6');
        xlswrite(Totals_xls,CTanTanLog331_2p/fsize,'Totals','J10');
        xlswrite(Totals_xls,CTanLog41_2p/fsize,'Totals','J14');
        xlswrite(Totals_xls,CTanTanLog441_2p/fsize,'Totals','J18');
        xlswrite(Totals_xls,CLogLog31_2p/fsize,'Totals','J22');
        xlswrite(Totals_xls,CLogLogLog331_2p/fsize,'Totals','J26');
        xlswrite(Totals_xls,CLogLog41_2p/fsize,'Totals','J30');
        xlswrite(Totals_xls,CLogLogLog441_2p/fsize,'Totals','J34');
        xlswrite(Totals_xls,CTanTanPur331_2p/fsize,'Totals','J38');
        xlswrite(Totals_xls,CTanTanPur441_2p/fsize,'Totals','J42');
        % predictions
        xlswrite(Totals_xls,VTanLog31_p/fsize,'Totals','E6');
        xlswrite(Totals_xls,VTanTanLog331_p/fsize,'Totals','E10');
        xlswrite(Totals_xls,VTanLog41_p/fsize,'Totals','E14');
        xlswrite(Totals_xls,VTanTanLog441_p/fsize,'Totals','E18');
        xlswrite(Totals_xls,VLogLog31_p/fsize,'Totals','E22');
        xlswrite(Totals_xls,VLogLogLog331_p/fsize,'Totals','E26');
        xlswrite(Totals_xls,VLogLog41_p/fsize,'Totals','E30');
        xlswrite(Totals_xls,VLogLogLog441_p/fsize,'Totals','E34');
        xlswrite(Totals_xls,VTanTanPur331_p/fsize,'Totals','E38');
        xlswrite(Totals_xls,VTanTanPur441_p/fsize,'Totals','E42');
        xlswrite(Totals_xls,CTanLog31_p/fsize,'Totals','K6');
        xlswrite(Totals_xls,CTanTanLog331_p/fsize,'Totals','K10');
        xlswrite(Totals_xls,CTanLog41_p/fsize,'Totals','K14');
        xlswrite(Totals_xls,CTanTanLog441_p/fsize,'Totals','K18');
        xlswrite(Totals_xls,CLogLog31_p/fsize,'Totals','K22');
        xlswrite(Totals_xls,CLogLogLog331_p/fsize,'Totals','K26');
        xlswrite(Totals_xls,CLogLog41_p/fsize,'Totals','K30');
        xlswrite(Totals_xls,CLogLogLog441_p/fsize,'Totals','K34');
        xlswrite(Totals_xls,CTanTanPur331_p/fsize,'Totals','K38');
        xlswrite(Totals_xls,CTanTanPur441_p/fsize,'Totals','K42');
exit

%
close all;
clear;
clc;
% 1 percent
VTanLog1_1p = 0;
VTanTanLog331_1p = 0;
VTanLog41_1p = 0;
VTanTanLog441_1p = 0;
VLogLog31_1p = 0;
VLogLogLog331_1p = 0;
VLogLog41_1p = 0;
VLogLogLog441_1p = 0;
VTanTanPur331_1p = 0;
VTanTanPur441_1p = 0;
VLinear2_1p = 0;
VLinear3_1p = 0;
VLinear4_1p = 0;
CTanLog31_1p = 0;
CTanTanLog331_1p = 0;
CTanLog41_1p = 0;
CTanTanLog441_1p = 0;
CLogLog31_1p = 0;
CLogLogLog331_1p = 0;
CLogLog41_1p = 0;
CLogLogLog441_1p = 0;
CTanTanPur331_1p = 0;
CTanTanPur441_1p = 0;
CLinear2_1p = 0;
CLinear3_1p = 0;
CLinear4_1p = 0;
% 2 percent
VTanLog31_2p = 0;
VTanTanLog331_2p = 0;
VTanLog41_2p = 0;
VTanTanLog441_2p = 0;
```

```
VLogLog31_2p = 0;
VLogLogLog331_2p = 0;
VLogLog41_2p = 0;
VLogLogLog441_2p = 0;
VTanTanPur331_2p = 0;
VTanTanPur441_2p = 0;
VLinear2_2p = 0;
VLinear3_2p = 0;
VLinear4_2p = 0;
CTanLog31_2p = 0;
CTanTanLog331_2p = 0;
CTanLog41_2p = 0;
CTanTanLog441_2p = 0;
CLogLog31_2p = 0;
CLogLogLog331_2p = 0;
CLogLog41_2p = 0;
CLogLogLog441_2p = 0;
CTanTanPur331_2p = 0;
CTanTanPur441_2p = 0;
CLinear2_2p = 0;
CLinear3_2p = 0;
CLinear4_2p = 0;
% Predictions
VTanLog31_p = 0;
VTanTanLog331_p = 0;
VTanLog41_p = 0;
VTanTanLog441_p = 0;
VLogLog31_p = 0;
VLogLogLog331_p = 0;
VLogLog41_p = 0;
VLogLogLog441_p = 0;
VTanTanPur331_p = 0;
VTanTanPur441_p = 0;
VLinear2_p = 0;
VLinear3_p = 0;
VLinear4_p = 0;
CTanLog31_p = 0;
CTanTanLog331_p = 0;
CTanLog41_p = 0;
CTanTanLog441_p = 0;
CLogLog31_p = 0;
CLogLogLog331_p = 0;
CLogLog41_p = 0;
CLogLogLog441_p = 0;
CTanTanPur331_p = 0;
CTanTanPur441_p = 0;
CLinear2_p = 0;
CLinear3_p = 0;
CLinear4_p = 0;

% Read in files
Totals_xls = 'Totals.xlsx';
files = dir('Subj_*.xlsx');
fsize = numel(files);
for i = 1 : numel(files)
    % 1 percent
    Subj_xls = files(i).name;
    VTanLog31_1p = VTanLog31_1p + xlsread(Subj_xls,'Totals','C4');
    VTanTanLog331_1p = VTanTanLog331_1p + xlsread(Subj_xls,'Totals','C6');
    VTanLog41_1p = VTanLog41_1p + xlsread(Subj_xls,'Totals','C8');
    VTanTanLog441_1p = VTanTanLog441_1p + xlsread(Subj_xls,'Totals','C10');
    VLogLog31_1p = VLogLog31_1p + xlsread(Subj_xls,'Totals','C12');
    VLogLogLog331_1p = VLogLogLog331_1p + xlsread(Subj_xls,'Totals','C14');
    VLogLog41_1p = VLogLog41_1p + xlsread(Subj_xls,'Totals','C16');
    VLogLogLog441_1p = VLogLogLog441_1p + xlsread(Subj_xls,'Totals','C18');
    VTanTanPur331_1p = VTanTanPur331_1p + xlsread(Subj_xls,'Totals','C20');
    VTanTanPur441_1p = VTanTanPur441_1p + xlsread(Subj_xls,'Totals','C22');
    VLinear2_1p = VLinear2_1p + xlsread(Subj_xls,'Totals','C29');
    VLinear3_1p = VLinear3_1p + xlsread(Subj_xls,'Totals','C32');
    VLinear4_1p = VLinear4_1p + xlsread(Subj_xls,'Totals','C35');
    CTanLog31_1p = CTanLog31_1p + xlsread(Subj_xls,'Totals','I4');
    CTanTanLog331_1p = CTanTanLog331_1p + xlsread(Subj_xls,'Totals','I6');
    CTanLog41_1p = CTanLog41_1p + xlsread(Subj_xls,'Totals','I8');
    CTanTanLog441_1p = CTanTanLog441_1p + xlsread(Subj_xls,'Totals','I10');
    CLogLog31_1p = CLogLog31_1p + xlsread(Subj_xls,'Totals','I12');
    CLogLogLog331_1p = CLogLogLog331_1p + xlsread(Subj_xls,'Totals','I14');
    CLogLog41_1p = CLogLog41_1p + xlsread(Subj_xls,'Totals','I16');
    CLogLogLog441_1p = CLogLogLog441_1p + xlsread(Subj_xls,'Totals','I18');
    CTanTanPur331_1p = CTanTanPur331_1p + xlsread(Subj_xls,'Totals','I20');
    CTanTanPur441_1p = CTanTanPur441_1p + xlsread(Subj_xls,'Totals','I22');
    CLinear2_1p = CLinear2_1p + xlsread(Subj_xls,'Totals','I29');
    CLinear3_1p = CLinear3_1p + xlsread(Subj_xls,'Totals','C32');
    CLinear4_1p = CLinear4_1p + xlsread(Subj_xls,'Totals','C35');
    % 2 percent
    VTanLog31_2p = VTanLog31_2p + xlsread(Subj_xls,'Totals','D4');
    VTanTanLog331_2p = VTanTanLog331_2p + xlsread(Subj_xls,'Totals','D6');
    VTanLog41_2p = VTanLog41_2p + xlsread(Subj_xls,'Totals','D8');
    VTanTanLog441_2p = VTanTanLog441_2p + xlsread(Subj_xls,'Totals','D10');
    VLogLog31_2p = VLogLog31_2p + xlsread(Subj_xls,'Totals','D12');
    VLogLogLog331_2p = VLogLogLog331_2p + xlsread(Subj_xls,'Totals','D14');
    VLogLog41_2p = VLogLog41_2p + xlsread(Subj_xls,'Totals','D16');
    VLogLogLog441_2p = VLogLogLog441_2p + xlsread(Subj_xls,'Totals','D18');
    VTanTanPur331_2p = VTanTanPur331_2p + xlsread(Subj_xls,'Totals','D20');
    VTanTanPur441_2p = VTanTanPur441_2p + xlsread(Subj_xls,'Totals','D22');
    VLinear2_2p = VLinear2_2p + xlsread(Subj_xls,'Totals','D29');
    VLinear3_2p = VLinear3_2p + xlsread(Subj_xls,'Totals','D32');
    VLinear4_2p = VLinear4_2p + xlsread(Subj_xls,'Totals','D35');
    CTanLog31_2p = CTanLog31_2p + xlsread(Subj_xls,'Totals','J4');
    CTanTanLog331_2p = CTanTanLog331_2p + xlsread(Subj_xls,'Totals','J6');
    CTanLog41_2p = CTanLog41_2p + xlsread(Subj_xls,'Totals','J8');
    CTanTanLog441_2p = CTanTanLog441_2p + xlsread(Subj_xls,'Totals','J10');
    CLogLog31_2p = CLogLog31_2p + xlsread(Subj_xls,'Totals','J12');
    CLogLogLog331_2p = CLogLogLog331_2p + xlsread(Subj_xls,'Totals','J14');
    CLogLog41_2p = CLogLog41_2p + xlsread(Subj_xls,'Totals','J16');
    CLogLogLog441_2p = CLogLogLog441_2p + xlsread(Subj_xls,'Totals','J18');
    CTanTanPur331_2p = CTanTanPur331_2p + xlsread(Subj_xls,'Totals','J20');
    CTanTanPur441_2p = CTanTanPur441_2p + xlsread(Subj_xls,'Totals','J22');
    CLinear2_2p = CLinear2_2p + xlsread(Subj_xls,'Totals','J29');
    CLinear3_2p = CLinear3_2p + xlsread(Subj_xls,'Totals','J32');
    CLinear4_2p = CLinear4_2p + xlsread(Subj_xls,'Totals','J35');
    % predictions
    VTanLog31_p = VTanLog31_p + xlsread(Subj_xls,'Totals','E4');
    VTanTanLog331_p = VTanTanLog331_p + xlsread(Subj_xls,'Totals','E6');
    VTanLog41_p = VTanLog41_p + xlsread(Subj_xls,'Totals','E8');
    VTanTanLog441_p = VTanTanLog441_p + xlsread(Subj_xls,'Totals','E10');
    VLogLog31_p = VLogLog31_p + xlsread(Subj_xls,'Totals','E12');
    VLogLogLog331_p = VLogLogLog331_p + xlsread(Subj_xls,'Totals','E14');
    VLogLog41_p = VLogLog41_p + xlsread(Subj_xls,'Totals','E16');
    VLogLogLog441_p = VLogLogLog441_p + xlsread(Subj_xls,'Totals','E18');
    VTanTanPur331_p = VTanTanPur331_p + xlsread(Subj_xls,'Totals','E20');
    VTanTanPur441_p = VTanTanPur441_p + xlsread(Subj_xls,'Totals','E22');
    VLinear2_p = VLinear2_p + xlsread(Subj_xls,'Totals','E29');
    VLinear3_p = VLinear3_p + xlsread(Subj_xls,'Totals','E32');
    VLinear4_p = VLinear4_p + xlsread(Subj_xls,'Totals','E35');
    CTanLog31_p = CTanLog31_p + xlsread(Subj_xls,'Totals','K4');
    CTanTanLog331_p = CTanTanLog331_p + xlsread(Subj_xls,'Totals','K6');
    CTanLog41_p = CTanLog41_p + xlsread(Subj_xls,'Totals','K8');
    CTanTanLog441_p = CTanTanLog441_p + xlsread(Subj_xls,'Totals','K10');
    CLogLog31_p = CLogLog31_p + xlsread(Subj_xls,'Totals','K12');
    CLogLogLog331_p = CLogLogLog331_p + xlsread(Subj_xls,'Totals','K14');
    CLogLog41_p = CLogLog41_p + xlsread(Subj_xls,'Totals','K16');
    CLogLogLog441_p = CLogLogLog441_p + xlsread(Subj_xls,'Totals','K18');
    CTanTanPur331_p = CTanTanPur331_p + xlsread(Subj_xls,'Totals','K20');
    CTanTanPur441_p = CTanTanPur441_p + xlsread(Subj_xls,'Totals','K22');
    CLinear2_p = CLinear2_p + xlsread(Subj_xls,'Totals','K29');
    CLinear3_p = CLinear3_p + xlsread(Subj_xls,'Totals','K32');
    CLinear4_p = CLinear4_p + xlsread(Subj_xls,'Totals','K35');
end
% 1 percent
xlswrite(Totals_xls,VTanLog31_1p,'Totals','C8');
xlswrite(Totals_xls,VTanTanLog331_1p,'Totals','C12');
xlswrite(Totals_xls,VTanLog41_1p,'Totals','C16');
xlswrite(Totals_xls,VTanTanLog441_1p,'Totals','C20');
xlswrite(Totals_xls,VLogLog31_1p,'Totals','C24');
xlswrite(Totals_xls,VLogLogLog331_1p,'Totals','C28');
xlswrite(Totals_xls,VLogLog41_1p,'Totals','C32');
xlswrite(Totals_xls,VLogLogLog441_1p,'Totals','C36');
xlswrite(Totals_xls,VTanTanPur331_1p,'Totals','C40');
xlswrite(Totals_xls,VTanTanPur441_1p,'Totals','C44');
xlswrite(Totals_xls,VLinear2_1p,'Totals','C55');
xlswrite(Totals_xls,VLinear3_1p,'Totals','C60');
xlswrite(Totals_xls,VLinear4_1p,'Totals','C65');
xlswrite(Totals_xls,CTanLog31_1p,'Totals','I8');
xlswrite(Totals_xls,CTanTanLog331_1p,'Totals','I12');
xlswrite(Totals_xls,CTanLog41_1p,'Totals','I16');
xlswrite(Totals_xls,CTanTanLog441_1p,'Totals','I20');
xlswrite(Totals_xls,CLogLog31_1p,'Totals','I24');
xlswrite(Totals_xls,CLogLogLog331_1p,'Totals','I28');
xlswrite(Totals_xls,CLogLog41_1p,'Totals','I32');
xlswrite(Totals_xls,CLogLogLog441_1p,'Totals','I36');
xlswrite(Totals_xls,CTanTanPur331_1p,'Totals','I40');
xlswrite(Totals_xls,CTanTanPur441_1p,'Totals','I44');
xlswrite(Totals_xls,CLinear2_1p,'Totals','I55');
xlswrite(Totals_xls,CLinear3_1p,'Totals','I60');
xlswrite(Totals_xls,CLinear4_1p,'Totals','I65');
% 2 percent
xlswrite(Totals_xls,VTanLog31_2p,'Totals','D8');
xlswrite(Totals_xls,VTanTanLog331_2p,'Totals','D12');
xlswrite(Totals_xls,VTanLog41_2p,'Totals','D16');
xlswrite(Totals_xls,VTanTanLog441_2p,'Totals','D20');
xlswrite(Totals_xls,VLogLog31_2p,'Totals','D24');
xlswrite(Totals_xls,VLogLogLog331_2p,'Totals','D28');
xlswrite(Totals_xls,VLogLog41_2p,'Totals','D32');
xlswrite(Totals_xls,VLogLogLog441_2p,'Totals','D36');
xlswrite(Totals_xls,VTanTanPur331_2p,'Totals','D40');
xlswrite(Totals_xls,VTanTanPur441_2p,'Totals','D44');
xlswrite(Totals_xls,VLinear2_2p,'Totals','D55');
xlswrite(Totals_xls,VLinear3_2p,'Totals','D60');
xlswrite(Totals_xls,VLinear4_2p,'Totals','D65');
xlswrite(Totals_xls,CTanLog31_2p,'Totals','J8');
xlswrite(Totals_xls,CTanTanLog331_2p,'Totals','J12');
xlswrite(Totals_xls,CTanLog41_2p,'Totals','J16');
xlswrite(Totals_xls,CTanTanLog441_2p,'Totals','J20');
xlswrite(Totals_xls,CLogLog31_2p,'Totals','J24');
xlswrite(Totals_xls,CLogLogLog331_2p,'Totals','J28');
xlswrite(Totals_xls,CLogLog41_2p,'Totals','J32');
xlswrite(Totals_xls,CLogLogLog441_2p,'Totals','J36');
xlswrite(Totals_xls,CTanTanPur331_2p,'Totals','J40');
xlswrite(Totals_xls,CTanTanPur441_2p,'Totals','J44');
xlswrite(Totals_xls,CLinear2_2p,'Totals','J55');
xlswrite(Totals_xls,CLinear3_2p,'Totals','J60');
xlswrite(Totals_xls,CLinear4_2p,'Totals','J65');
% predictions
xlswrite(Totals_xls,VTanLog31_p,'Totals','E8');
xlswrite(Totals_xls,VTanTanLog331_p,'Totals','E12');
xlswrite(Totals_xls,VTanLog41_p,'Totals','E16');
xlswrite(Totals_xls,VTanTanLog441_p,'Totals','E20');
xlswrite(Totals_xls,VLogLog31_p,'Totals','E24');
xlswrite(Totals_xls,VLogLogLog331_p,'Totals','E28');
xlswrite(Totals_xls,VLogLog41_p,'Totals','E32');
xlswrite(Totals_xls,VLogLogLog441_p,'Totals','E36');
xlswrite(Totals_xls,VTanTanPur331_p,'Totals','E40');
xlswrite(Totals_xls,VTanTanPur441_p,'Totals','E44');
xlswrite(Totals_xls,VLinear2_p,'Totals','E55');
xlswrite(Totals_xls,VLinear3_p,'Totals','E60');
xlswrite(Totals_xls,VLinear4_p,'Totals','E65');
xlswrite(Totals_xls,CTanLog31_p,'Totals','K8');
xlswrite(Totals_xls,CTanTanLog331_p,'Totals','K12');
xlswrite(Totals_xls,CTanLog41_p,'Totals','K16');
xlswrite(Totals_xls,CTanTanLog441_p,'Totals','K20');
xlswrite(Totals_xls,CLogLog31_p,'Totals','K24');
xlswrite(Totals_xls,CLogLogLog331_p,'Totals','K28');
xlswrite(Totals_xls,CLogLog41_p,'Totals','K32');
xlswrite(Totals_xls,CLogLogLog441_p,'Totals','K36');
xlswrite(Totals_xls,CTanTanPur331_p,'Totals','K40');
xlswrite(Totals_xls,CTanTanPur441_p,'Totals','K44');
xlswrite(Totals_xls,CLinear2_p,'Totals','K55');
xlswrite(Totals_xls,CLinear3_p,'Totals','K60');
xlswrite(Totals_xls,CLinear4_p,'Totals','K65');
% 1 percent
xlswrite(Totals_xls,VTanLog31_1p/fsize,'Totals','C6');
xlswrite(Totals_xls,VTanTanLog331_1p/fsize,'Totals','C10');
xlswrite(Totals_xls,VTanLog41_1p/fsize,'Totals','C14');
xlswrite(Totals_xls,VTanTanLog441_1p/fsize,'Totals','C18');
xlswrite(Totals_xls,VLogLog31_1p/fsize,'Totals','C22');
xlswrite(Totals_xls,VLogLogLog331_1p/fsize,'Totals','C26');
xlswrite(Totals_xls,VLogLog41_1p/fsize,'Totals','C30');
xlswrite(Totals_xls,VLogLogLog441_1p/fsize,'Totals','C34');
xlswrite(Totals_xls,VTanTanPur331_1p/fsize,'Totals','C38');
xlswrite(Totals_xls,VTanTanPur441_1p/fsize,'Totals','C42');
xlswrite(Totals_xls,VLinear2_1p/fsize,'Totals','C53');
xlswrite(Totals_xls,VLinear3_1p/fsize,'Totals','C58');
xlswrite(Totals_xls,VLinear4_1p/fsize,'Totals','C63');
xlswrite(Totals_xls,CTanLog31_1p/fsize,'Totals','I6');
xlswrite(Totals_xls,CTanTanLog331_1p/fsize,'Totals','I10');
xlswrite(Totals_xls,CTanLog41_1p/fsize,'Totals','I14');
xlswrite(Totals_xls,CTanTanLog441_1p/fsize,'Totals','I18');
xlswrite(Totals_xls,CLogLog31_1p/fsize,'Totals','I22');
xlswrite(Totals_xls,CLogLogLog331_1p/fsize,'Totals','I26');
xlswrite(Totals_xls,CLogLog41_1p/fsize,'Totals','I30');
xlswrite(Totals_xls,CLogLogLog441_1p/fsize,'Totals','I34');
xlswrite(Totals_xls,CTanTanPur331_1p/fsize,'Totals','I38');
xlswrite(Totals_xls,CTanTanPur441_1p/fsize,'Totals','I42');
xlswrite(Totals_xls,CLinear2_1p/fsize,'Totals','I53');
xlswrite(Totals_xls,CLinear3_1p/fsize,'Totals','I58');
xlswrite(Totals_xls,CLinear4_1p/fsize,'Totals','I63');
% 2 percent
xlswrite(Totals_xls,VTanLog31_2p/fsize,'Totals','D6');
xlswrite(Totals_xls,VTanTanLog331_2p/fsize,'Totals','D10');
xlswrite(Totals_xls,VTanLog41_2p/fsize,'Totals','D14');
xlswrite(Totals_xls,VTanTanLog441_2p/fsize,'Totals','D18');
xlswrite(Totals_xls,VLogLog31_2p/fsize,'Totals','D22');
xlswrite(Totals_xls,VLogLogLog331_2p/fsize,'Totals','D26');
xlswrite(Totals_xls,VLogLog41_2p/fsize,'Totals','D30');
xlswrite(Totals_xls,VLogLogLog441_2p/fsize,'Totals','D34');
xlswrite(Totals_xls,VTanTanPur331_2p/fsize,'Totals','D38');
xlswrite(Totals_xls,VTanTanPur441_2p/fsize,'Totals','D42');
xlswrite(Totals_xls,VLinear2_2p/fsize,'Totals','D53');
xlswrite(Totals_xls,VLinear3_2p/fsize,'Totals','D58');
xlswrite(Totals_xls,VLinear4_2p/fsize,'Totals','D63');
xlswrite(Totals_xls,CTanLog31_2p/fsize,'Totals','J6');
xlswrite(Totals_xls,CTanTanLog331_2p/fsize,'Totals','J10');
xlswrite(Totals_xls,CTanLog41_2p/fsize,'Totals','J14');
xlswrite(Totals_xls,CTanTanLog441_2p/fsize,'Totals','J18');
xlswrite(Totals_xls,CLogLog31_2p/fsize,'Totals','J22');
xlswrite(Totals_xls,CLogLogLog331_2p/fsize,'Totals','J26');
xlswrite(Totals_xls,CLogLog41_2p/fsize,'Totals','J30');
xlswrite(Totals_xls,CLogLogLog441_2p/fsize,'Totals','J34');
xlswrite(Totals_xls,CTanTanPur331_2p/fsize,'Totals','J38');
xlswrite(Totals_xls,CTanTanPur441_2p/fsize,'Totals','J42');
xlswrite(Totals_xls,CLinear2_2p/fsize,'Totals','J53');
xlswrite(Totals_xls,CLinear3_2p/fsize,'Totals','J58');
xlswrite(Totals_xls,CLinear4_2p/fsize,'Totals','J63');
% predictions
xlswrite(Totals_xls,VTanLog31_p/fsize,'Totals','E6');
xlswrite(Totals_xls,VTanTanLog331_p/fsize,'Totals','E10');
xlswrite(Totals_xls,VTanLog41_p/fsize,'Totals','E14');
xlswrite(Totals_xls,VTanTanLog441_p/fsize,'Totals','E18');
xlswrite(Totals_xls,VLogLog31_p/fsize,'Totals','E22');
xlswrite(Totals_xls,VLogLogLog331_p/fsize,'Totals','E26');
xlswrite(Totals_xls,VLogLog41_p/fsize,'Totals','E30');
xlswrite(Totals_xls,VLogLogLog441_p/fsize,'Totals','E34');
xlswrite(Totals_xls,VTanTanPur331_p/fsize,'Totals','E38');
xlswrite(Totals_xls,VTanTanPur441_p/fsize,'Totals','E42');
xlswrite(Totals_xls,VLinear2_p/fsize,'Totals','E53');
xlswrite(Totals_xls,VLinear3_p/fsize,'Totals','E58');
xlswrite(Totals_xls,VLinear4_p/fsize,'Totals','E63');
xlswrite(Totals_xls,CTanLog31_p/fsize,'Totals','K6');
xlswrite(Totals_xls,CTanTanLog331_p/fsize,'Totals','K10');
xlswrite(Totals_xls,CTanLog41_p/fsize,'Totals','K14');
xlswrite(Totals_xls,CTanTanLog441_p/fsize,'Totals','K18');
xlswrite(Totals_xls,CLogLog31_p/fsize,'Totals','K22');
xlswrite(Totals_xls,CLogLogLog331_p/fsize,'Totals','K26');
xlswrite(Totals_xls,CLogLog41_p/fsize,'Totals','K30');
xlswrite(Totals_xls,CLogLogLog441_p/fsize,'Totals','K34');
xlswrite(Totals_xls,CTanTanPur331_p/fsize,'Totals','K38');
xlswrite(Totals_xls,CTanTanPur441_p/fsize,'Totals','K42');
xlswrite(Totals_xls,CLinear2_p/fsize,'Totals','K53');
xlswrite(Totals_xls,CLinear3_p/fsize,'Totals','K58');
xlswrite(Totals_xls,CLinear4_p/fsize,'Totals','K63');
exit
```

VII. Bibliography

[Ano01b] BioAPI Consortium, *BioAPI Specification Version 1.1*).

[Ano3] American National Standards Institute, *Biometric Information Management & Security*, ANSI X9:84:2003).

[Ano05a] Anonymous, "What are Biometrics, and how could you be using them?," PassUK.com, 2005.

[Ano05b] Smart Card Alliance, Smart Cards and Biometrics in Privacy-Sensitive Secure ID Systems, http://www.smartcardalliance.org/newsletter/may_2005/feature_0505.html, Accessed: November 8, 2006.

[Ano06a] National Science and Technology Council, *Biometrics Frequently Asked Questions*: September 7, 2006).

[Ano06b] National Science and Technology Council, *Biometrics Glossary*: September 14, 2006).

[Ano06c] ISO/IEC, *Information Technology - Biometric Application Programming Interface - Part 1: BioAPI Specification*).

[Ano06d] Anonymous, "Electronic Biometric Transmission Specification (EBTS)," vol. IAFIS-DOC-01078-8.0 Draft: Department of Justice Federal Bureau of Investigation, 2006.

[Ano06e] Department of Defense Biometrics Task Force, *Department of Defense Electronic Biometric Transmission Specification*).

[Ano07] U.S. Government, *Capability Development Document (CDD) For Identity Dominance System*).

[BeA07] Beveridge, J. Ross, Andres Alvarez, Jilmil Saraf, and Ward Fisher, "Face Detection Algorithm and Feature Performance on FRGC 2.0 Imagery," *Proceedings of the Biometrics: Theory, Applications and Systems*, Washington, D.C., 2007.

[Bis95] Bishop, Christopher M., *Neural Networks for Pattern Recognition*: Oxford University Press, 1995.

[CaM06] Cappelli, R., D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 28, no. 1, pp. 3-18, 2006.

[CaR08] Carls, John, Richard Raines, Michael Grimaila, and Steven Rogers, "Biometric Security Enhancements Through Template Aging Matching Score Analysis," *Proceedings of the 3rd International Conference on Information Warfare and Security*, Omaha, NE, 2008.

[Cog07] Cognitec. FaceVACS SDK. Ver. 6.3.0.0. Computer Software. 2007.

[Col06] Colbry, Dirk Joel Luchini, "Human Face Verification By Robust 3D Surface Alignment," Dissertation, Michigan State University, 2006.

[Dau02] Daugman, John, "The Importance of Being Random: Statistical Principles of Iris Recognition," *Pattern Recognition*, 2002.

[DaY06] Dass, Sarat C. , Yongfang Zhu, and Anil K. Jain, "Validating a Biometric Authentication System: Sample Size Requirements," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1902-1319, 2006.

[Dro06] Dror, Itiel, "Cognitive Science Serving Security: assuring useable and efficient biometric and technological solutions," in *Aviation Security International: The Journal of Airport & Airline Security*, vol. 12, 2006, pp. 21-28.

[ElK04] Elliott, Stephen, Eric Kukula, and Nathan Sickler, "The Challenges of the Environment and the Human / Biometric Device Interaction on Biometric System Performance," *Proceedings of the International Workshop on Biometric Techologies - Special Forum on Modeling and Simulation in Biometric Technology*, Calgery, Alberta, Canada, 2004.

[FlB07] Flynn, Patrick J and Kevin W. Bowyer, "University of Notre Dame Database Collection B," University of Notre Dame, 2007.

[Fly07] Flynn, Patrick J., "University of Notre Dame Biometrics Database Distribution," University of Notre Dame, 2007.

[FrM08] Freni, Biagio, Gian Luca Marcialis, and Fabio Roli, "Replacement Algorithms for Fingerprint Template Update," *Proceedings of the 5th International Conference on Image Analysis and Recognition (ICIAR 2008)*, 2008.

[GeZ07] Geng, Xin, Zhi-Hua Zhou, and Kate Smith-Miles, "Automatic Age Estimation Based on Facial Aging Patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 12, pp. 2234-2240, 2007.

[Gro05] Gross, Ralph, *Handbook of Face Recognition*. New York: Springer, 2005.

[HaD02] Hagan, Martin T., Howard B. Demuth, and Mark Hudson Beale, *Neural Network Design*: Martin Hagan, 2002.

[HaH06] Department of the Army Biometrics Task Force, *Biometric Collection, Transmission and Storage Standards Technical Reference*).

[HaW05] Hasse, Georg and Andreas Wolf, "Data Quality, Interoperability, Biometrics Fusion, and Template Ageing: Challenges for ePassports," *Proceedings of the The Biometric Consortium Conference 2005*, Arlington, VA, USA, 2005.

[HiS05] Hill, Catherine M., Christopher J. Solomon, and Stuart J. Gibson, "Aging the Human Face - A Statistically Rigorous Approach," *Proceedings of the The IEE International Symposium on Imaging for Crime Detection and Prevention, 2005. ICDP 2005.*, 2005.

[Hon98] Hong, Lin, "Automatic Personal Identification Using Fingerprints," Dissertation, Michigan State University, 1998.

[JaB02] Jain, Anil, Ruud Bolle, and Sharath Pankanti, *BIOMETRICS: Personal Identification in Networked Society*: Kluwer Academic Publishers, 2002.

[JaR05] Jain, A. Anil, Arun Ross, and Umut Uludag, "Biometric Template Security: Challenges and Solutions," *Proceedings of the European Signal Processing Conference (EUSIPCO)*, Antalya, Turkey, 2005.

[JaU03] Jain, Anil, Umut Uludag, and Arun Ross, "Biometric Template Selection: A Case Study in Fingerprints," *Proceedings of the 4th International Conference on Audio- and Video-Based Person Authentication (AVBPA)*, Guildford, UK, 2003.

[KeS05] Kevenaar, T. A. M., G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo, "Face Recognition with Renewable and Privacy Preserving Binary Templates," *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005.*, 2005.

[LaC07] Lanitis, Andreas and Tim Cootes, "FG-NET Aging Database," Cyprus College University of Manchester, UK, 2007.

[LaD04] Lanitis, Andreas, Chrisina Draganova, and Chris Christodoulou, "Comparing Different Classifiers for Automatic Age Estimation," *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 34, no. 1, pp. 621-628, 2004.

[LaT02] Lanitis, Andreas, Chris J. Taylor, and Timothy F. Cootes, "Toward Automatic Simulation of Aging Effects on Face Images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 4, pp. 442-455, 2002.

[Liu06] Liu, Xiaomei, "Optimizations in Iris Recognition," Dissertation, University of Notre Dame, 2006.

[Lof07] Lofton, Steve, "Phone Conversation on June 12, 2007," 2007.

[MaG05] Mansukhani, Praveer and Venu Govindaraju, "Exploring Similarity Measures for Biometric Databases," *Audio- and Video-based Biometric Person Authentication; 5th International Conference*, vol. 3546, pp. 832-eoa, 2005.

[MaM03] Maltoni, D., D. Maio, and S. Prabhakar, *Handbook of Fingerprint Recognition*: Springer, 2003.

[MaO05] Martinez, Francisco, Carlos Orrite, and Elfas Herrero, "Biometric Hand Recognition Using Neural Networks," *Proceedings of the Computational Intelligence and Bioinspired Systems; 8th International Work-Conference on Artificial Neural Networks, IWANN 2005*, Vilanova i la Geltru, Barcelona, Spain, 2005.

[Mat07] MathWorks, The. MATLAB. Ver. 7.4.0.287 (R2007a). Computer Software. 2007.

[MAT07] The MathWorks, Inc.®, MatLab, Natick, Massachusetts, http://www.mathworks.com, Accessed: July 30, 2007.

[MaW02] Mansfield, A. J. and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01," Centre for Mathematics and Scientific Computing, National Physical Laboratory *NPL Report CMSC 14/02*, August 2002, 2002.

[MuA04] Mukaida, Shigeru and Hiroshi Ando, "Extraction and Manipulation of Wrinkles and Spots for Facial Image Synthesis," *Proceedings of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition (FGR '04)*, 2004.

[Neu07] Neurotechnologija. Verilook SDK. Ver. 3.0.3.7. Computer Software. 2007.

[Nua06] Communications, Nuance. Dragon NaturallySpeaking. Ver. 9. Computer Software. 2006.

[PhG03a] DARPA/NIST, *Face Recognition Vender Test 2002: Overview and Summary*).

[PhG03b] DARPA/NIST, *Face Recognition Vender Test 2002: Evaluation Report,* NISTIR 6965).

[PhS07] Phillips, P. Jonathon, W. Todd Scruggs, Alice J. O'Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, and Matthew Sharpe, "FRVT 2006 and ICE 2006 Large-Scale Results," National Institute of Standards and Technology, Gaithersburg, MD 20899, March 2007, 2007.

[PoD01] National Institute of Standards and Technology, *Common Biometric Exchange File Format, NISTIR 6529,* NISTIR 6529: January 3, 2001).

[Pod02] Podio, Fernando L., "Personal Authentication Through Biometric Technologies," *Proceedings of the 4th International Workshop on Networked Appliances*, Gaithersburg, MD, 2002.

[RaC06a] Ramanathan, Narayanan and Rama Chellappa, "Modeling Age Progression in Young Faces," *Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06)*, 2006.

[RaC06b] Ramanathan, Narayanan and Rama Chellappa, "Face Verification Across Age Progression," *IEEE Transactions on Image Processing*, vol. 15, no. 11, pp. 3349-3361, 2006.

[RiB05] Ricanek, Karl Jr. and Edward Boone, "The Effect of Normal Adult Aging on Standard PCA Face Recognition Accuracy Rates," *Proceedings of the 2005 IEEE International Joint Conference on Neural Networks*, Montreal, QC, Canada, 2005.

[Ric07] Ricanek, Karl, "MORPH Database," University of North Carolina at Wilmington, 2007.

[RiT06] Ricanek, Karl Jr. and Tamirat Tesafaye, "MORPH: A Longitudinal Image Database of Normal Adult Age-progression," *Proceedings of the 7th International Conference on Automatic Face and Gesture Recognition, FGR 2006*, Southampton, United Kingdom, 2006.

[RoK91] Rogers, Steven K. and Matthew Kabrisky, *An Introduction to Biological and Artificial Neural Networks for Pattern Recognition* Bellingham, Wash., USA: SPIE Optical Engineering Press, 1991.

[Ros03] Ross, Arun, "Information Fusion In Fingerprint Authentication," Dissertation, Michigan State University, 2003.

[Rug02] Ruggles, Thomas, "Biometric Technical Assesment," California Welfare Fraud Prevention System, August 19, 2002, 2002.

[Sch06] Schuckers, Michael E., "Statistical Inference for Template Aging," *Proceedings of the Biometric Technology for Human Identification III,* Orlando (Kissimmee), FL, 2006.

[ScK04] Schneiderman, Henry and Takeo Kanade, "Object Detection Using the Statistics of Parts," *International Journal of Computer Vision*, vol. 56, no. 3, pp. 151-177, 2004.

[ScM07] Scheidat, Tobias, Andrey Makrushin, and Claus Vielhauer, "Automatic Template Update Strategies for Biometrics," Otto-von-Guericke University of Magdeburg, Magdeburg, Germany, May 2007, 2007.

[Shi05] Modi, Shimon K, "Keystroke Dynamics Verification Using Spontaneous Password," Thesis, Purdue University, 2005.

[Tai07] Taister, Mike, "Phone Conversation on June 14, 2007," 2007.

[TaS00] Taister, Michael A., Sandra D. Holliday, and H. I. M. Borrman, "Comments on Facial Aging in Law Enforcement Investigation," *Forensic Science Communcations*, vol. 2, no. 2, 2000.

[UlR03] Uludag, Umut, Arun Ross, and A. Anil Jain, "Biometric Template Selection and Update: A Case Study in Fingerprints," *Pattern Recognition*, vol. 37, no. 7, pp. 1533-1542, 2004.

[Ulu06] Uludag, Umut, "Secure Biometric Systems," Dissertation, Michigan State University, 2006.

[UmA04] Umut, Uludag and K. Jain Anil, "Attacks on Biometric Systems: A Case Study in Fingerprints," *Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, 2004.

[VeK06] van der Veen, Michiel, Tom Kevenaar, Geert-Jan Schrijen, Ton H. Akkermans, and Fei Zuo, "Face Biometrics with Renewable Templates," *Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, CA, 2006.

[VeN05] Veres, G. V., M. S. Nixon, and J. N. Carter, "Model-based Approaches for Predicting Gait Changes Over Time," *Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing - (ISSNIP 2005)*, Melbourne, Australia, 2005.

[ViJ04] Viola, Paul and Michael Jones, "Robust Real-Time Face Detection," *International Journal of Computer Vision*, vol. 57, no. 2, pp. 137-154, 2004.

[WaJ05] Wayman, James, Anil Jain, Davide Maltoni, and Dario Maio, *Biometric Systems: Technology, Design and Performance Evaluation*: Springer-Verlag London Limited., 2005.

[WaJ07] Wang, Peng, Qiang Ji, and James L. Wayman, "Modeling and Predicting Face Recognition System Performance Based on Analysis of Similarity Scores," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 665-670, 2007.

[WiG07] National Institute of Standards and Technology, *NIST Special Publication 800-76-1 Biometric Data Specification for Personal Identity Verification,* 800-76-1: January 2007).

[WoO03] Woodward Jr., John D., Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age*: McGraw-Hill/Osborne, 2003.

[Woo04] Woodard, Damon L., "Exploiting Finger Surface As A Biometric Identifier," Dissertation, Notre Dame, 2004.

[YaD02] Yang, Ming-Hsuan, David J. Kriegman, and Narendra Ahuja, "Detecting Faces in Images: A Survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 1, pp. 34-58, 2002.

[YaN02] Yam, Chew Yean, Mark S. Nixon, and John N. Carter, "Performance Analysis on New Biometric Gait Motion Model," *Proceedings of the Fifth IEEE Southwest Symposium on Image Analysis and Interpretation, 2002.*, Santa Fe, NM, 2002.

[YiZ05] Yin, Yilong, Bo Zhao, and Xiukun Yang, "An on-line template improvement algorithm," *Proceedings of the Biometric Technology for Human Identification II,* Orlando, FL, 2005.

VIII. Vita

Lieutenant Commander John W. Carls is a native of Allentown, PA, and graduated from Emmaus High in 1985. After attending Millersville University for two years, he enlisted in the United States Navy in 1987. Upon completion of Recruit Training, DS ‘A’ & ‘C’ schools, he reported to USS WASP (LHD 1) as an Data Systems Technician and performed additional duties as Work Center Supervisor / Assistant Leading Petty Officer for Combat Systems/CD Division. During this tour, he commissioned USS WASP (LHD 1) in July 1989, qualified ESWS, and completed deployments to the Mediterranean and Caribbean.

In February 1993, LCDR Carls attended Instructor Training at FTC, Dam Neck, VA. Upon completion, he reported to NMITC, Dam Neck, VA, and served as an Intelligence Center Maintenance Course Instructor / Supervisor. During this tour, he qualified Master Training Specialist and was selected for the Enlisted Commission Program.

In June 1996, LCDR Carls reported to the NSI in Newport, R.I., followed by NROTC Hampton Roads, VA. He attended Old Dominion University earning a degree in Bachelor of Science in Computer Science and commission in May 1998. After completing Surface Warfare Officers’ Division Officer School in Newport, R.I., he reported to USS MAHAN (DDG 72) in November 1998 as the Electrical Officer. Onboard, he qualified Surface Warfare Officer, Officer of the Deck Underway, Engineering Officer of the Watch, and completed a Mediterranean deployment.

In July 2000, he was assigned to the USS SIROCCO (PC 6) as the Weapons Officer / Supply Officer and qualified Command Duty Officer. LCDR Carls then reported to Assault Craft Unit FOUR (ACU 4) as the Facilities Manager / 1st LT. Following this, he reported as a graduate student at the Naval Postgraduate School, Monterery, CA, earning a Masters of Science in Computer Science with an emphasis on Networking and Space Information Warfare Command & Control.

In October 2003, he was assigned to the Office of Naval Intelligence as the ONI-43 Department Operations Officer / Information Assurance Officer. He earned his CISSP and was selected for the DoD Information Assurance Scholarship Program. He is currently a Doctorate of Philosophy student at the Air Force Institute of Technology, Graduate School of Engineering and Management, working on a PhD in Computer Science with a concentration on Biometrics and a minor in Information Resource Management. Upon completion of his duties at AFIT, his follow-on assignment is to report to the USS KEARSARGE (LHD 3) as the Assistant C5I Department Head.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 26-03-2009	**2. REPORT TYPE** **Doctoral Dissertation**	**3. DATES COVERED** *(From – To)* August 2005 – March 2009

4. TITLE AND SUBTITLE
A FRAMEWORK FOR ANALYZING BIOMETRIC TEMPLATE AGING AND RENEWAL PREDICTION

5a. CONTRACT NUMBER n/a

5b. GRANT NUMBER n/a

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Carls, John W., Lieutenant Commander, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/DCS/ENG/09-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory, Sensors Directorate
(Dr. Steven K. Rogers)
13th St, Bldg 620
Wright Patterson AFB OH 45433

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Biometric technology and systems are modernizing identity capabilities. With maturing biometrics in full, rapid development, a higher accuracy of identity verification is required. An improvement to the security of biometric-based verification systems is provided through higher accuracy; ultimately reducing fraud, theft, and loss of resources from unauthorized personnel. With trivial biometric systems, a higher acceptance threshold to obtain higher accuracy rates increase false rejection rates and user unacceptability. However, maintaining the higher accuracy rate enhances the security of the system. An area of biometrics with a paucity of research is template aging and renewal prediction, specifically in regards to facial aging. Through the methods presented in this research, higher accuracy rates are obtained without lowering the acceptance threshold, therefore improving the security level, false rejection rates, and user acceptability. As a proof of concept, this research develops a biometric template aging and renewal prediction framework currently absent in the biometric literature. The innovative framework is called the Carls Template Aging and Renewal Prediction Framework (CTARP Framework). The research integrates a diversity of disparate developments to provide a critical fundamental framework of significant advancement in the biometrics body of knowledge. This research presents the CTARP Framework, a novel foundational framework for methods of modeling and predicting template aging and renewal prediction based on matching score analysis. The groundwork discusses new techniques used in the template aging and renewal prediction framework, to include "perfect match score matrix", "error score matrix", and "decay error estimate" concepts. The matching scores are calculated using commercially available facial matching algorithms/SDKs against publicly available facial databases. Improving performance error rates over biometric authentication systems without a template aging and renewal prediction process is accomplished with the new CTARP framework while maintaining or improving upon the overall matching and/or rejection levels. Using such scores, timeframe predictions of when an individual needs to be renewed with a new template is feasible.

15. SUBJECT TERMS

Biometrics, Template Aging, Template Renewal Prediction

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. Richard A. Raines (ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4278 e-mail: Richard.Raines@afit.edu
U	**U**	**U**	UU	168	