2016

Analysis Of Data Stratification In A Multi-Sensor Fingerprint Dataset Using Match Score Statistics

Loukhya Kakumanu

Analysis Of Data Stratification In A Multi-Sensor Fingerprint Dataset Using Match Score Statistics

Loukhya Kakumanu

Thesis submitted to the Benjamin M. Statler College of Engineering and Mineral Resources at
West Virginia University

In partial fulfillment of the requirements for the degree of
Master of Science in Electrical Engineering

Jeremy Dawson, Ph.D., Chairperson
Bojan Cukic, Ph.D.
Matthew C. Valenti, Ph.D.

Lane Department of Computer Science and Electrical Engineering

Morgantown, West Virginia
2016

Keywords: Biometrics, Data Stratification, Fingerprints, Match Score, ROC curve, Statistical Distance Measures

ABSTRACT

Biometric data is an essential feature employed in testing the performance of any real time biometric recognition system prior to its usage. The variations introduced in the match performance critically determine the authenticity of the biometric data to be able to be used in an everyday scenario for the testing of biometric verification systems. This study in totality aims at understanding the impact of data stratification of such a biometric test dataset on the match performance of each of its stratum. In order to achieve this goal, the fingerprint dataset of the West Virginia University's 2012 BioCOP has been employed which is a part of the many multimodal biometric data collection projects that the University has accomplished. This test dataset has been initially segmented based on the scanners employed in the process of data acquisition to check for the variations in match performance with reference to the acquisition device. The secondary stage of data stratification included the creation of stratum based on the demographic features of the subjects in the dataset.

The main objectives this study aims to achieve are:

- *Developing a framework to assess the match score distributions of each stratum.*
- *Assessing the match performance of demographic strata in comparison to the total dataset.*
- *Statistical match performance evaluation using match score statistics.*

Following the generation of genuine and imposter match score distributions, Receiver Operating Characteristic Curves (ROC) were plotted to compare the match performance of each demographic stratum with respect to the total dataset. The divergence measures Kullback Leibler Divergence (KLD) and Jensen Shannon Divergence (JSD) have been calculated which signify the amount of variation between the match score distributions of each stratum. With the help of these procedures, the task of estimating the effect of data stratification on the match performance has been accomplished which serves as a measure of understanding the impact of this fingerprint dataset when used for biometric testing purposes.

To my loving parents and sister

ACKNOWLEDGEMENT

First of all, I would like to thank my graduate advisor Dr. Jeremy Dawson for his enormous support, invaluable advice and positive encouragement throughout the course of my research. I will forever be thankful to him for giving me this opportunity. Thanks to Dr. Bojan Cukic and Dr. Matthew C. Valenti for their willingness to serve on the final committee.

I would also like to thank my colleagues Ms. Mounika Kamireddy, Ms. Nikitha Nadiminti and Ms. Rupindrani Aila for their immense support and professional advice throughout my research.

I would like to whole heartedly thank my parents, sister and friends for their constant guidance and motivation without whom this would not have been possible.

Lastly, I would like to thank Mr. Randall Wickline and Mr. Sarang Amin for their assistance while working on my thesis.

Table of Contents

List of Figures

List of Tables

CHAPTER 1 - INTRODUCTION

The science of authenticating the identity of a person based on their physical, chemical or biological attributes is referred to as biometrics. Biometrics, or biometric recognition, employs a variety of physical or behavioral characteristics such as fingerprints, facial structure, hand geometry, iris patterns, signature, gait, palm print, voice and ear shape for establishing an individual's identity. In the biometric literature, these characteristics are referred to as traits or modalities. However, due to desirable features such as high degree of uniqueness and ease of capture, fingerprints have been one of the most extensively used biometric modality. Thanks to the usability and reliability of biometric systems based on fingerprints, it is now the main means of biometric authentication in numerous applications worldwide. This throws light on the need to understand why fingerprint matching is critical. Fingerprints are by and large characterized through particular elements called minutiae. Verification process using a probe and a gallery of fingerprint images require the matching of the minutiae in a probe image against the minutiae of other fingerprints in the gallery. Hence, fingerprint matching is a key process in biometric verification.

Human age, gender and ethnicity are valuable demographic information about a population. These measures are also considered important soft biometric traits for human recognition or search. In a study, Jonathan Philips et al [1] documented the effect of racial and gender demographics on the accuracy of algorithms that match identity in pairs of face images. This study shows that identity match accuracy differs substantially when the non-match identity population were varied by race. The results obtained indicate the importance of the demographic strata of the facial dataset in predicting the accuracy of the face recognition algorithm. According to Mumtaz Kamala and Fahad Al- Harby [2], the effects of gender differences in the acceptance of fingerprint biometric systems is highly significant. This study included 306 Saudi participants who were involved in a large scale experiment, consisting of men and women between the ages of 18 and 55. This experiment also included the testing of a fingerprint authentication system in order to understand its response to the difference in the data employed. Thomas Bergmuiller et al [3] have proposed a method that investigates the influence of sensor ageing on iris recognition by

simulative ageing of the participants of an iris test database. This study also reveals, how the iris dataset has impacted the sensor performance over a period of 4 years.

The research studies discussed above clearly indicate a prominent need to understand how the different strata of data of a biometric modality could impact the overall matching results which is the motivation behind this research.

1.1 Statement of Problem

This study uses the fingerprint dataset of the West Virginia University's 2012 BioCOP (Biometric Collection Project) which has been stratified based on the age, gender and ethnicity of the subjects. The WVU 2012 BioCOP project has 1200 subjects enrolled in it and this project has been carried out in a controlled environment using standardized acquisition techniques. The variations introduced in the fingerprints acquired from various demographic classes propagate from the acquisition subsystem all the way to the matching subsystem. These variations ultimately affect the performance rates of the fingerprint matching component. So, the question this research aims to answer is, how such a data stratification would influence the results of tests of the biometric system and the algorithms implemented using this dataset. There is need to understand the effect of strata dependency on the match performance not just from an evaluation perspective, but also from a technology usage perspective.

1.2 Purpose of Study

The fingerprint dataset of the WVU 2012 BioCOP has been acquired from 3 standard optical scanners and from a mixed set of subjects belonging to different age and ethnic groups. The purpose of this research has been to examine whether the data stratification of the fingerprint images acquired has had an impact on the performance of a particular sensor or a demographic cohort under study. This study also examines the possible extent to which the test results would be skewed had this dataset been used to test a real time biometric verification system. Examining the difference in matching error rates of the original and demographic strata was the focal point of analysis. The outcome of such a study will be useful in understanding why a particular stratum

is more susceptible to errors and also helps in providing an insight into the characteristics of the fingerprint dataset. To further augment the study, statistical analysis of the matching measures has been performed to be able to quantitatively understand the difference in match performance of each stratum and its impact on the test results of the fingerprint verification system.

1.3 Research Goals and Objectives

The goal of this study is to understand how demographic strata such as age, gender and ethnicity have an impact on the match performance through the use of multiple templates of a fingerprint impression. In principle, availability of multiple templates would allow us to examine intraclass variations and interclass similarities of fingerprints. We have three main objectives to achieve our goal which are listed below:

1. Developing a framework to understand the difference in match performance of all the fingerprint stratum.

As a primary goal, an effort has been made to customize the functionality of the software development kit in a way that it could be used to generate genuine and impostor match scores as an initial measure of qualitatively assessing the match performance of each of the stratum in the fingerprint dataset WVU 2012 BioCOP collection.

2. Evaluation of match score distributions to check for the match performance of each stratum.

As already mentioned, the data set was segmented based on the age, ethnicity and gender of the subjects enrolled in the collection. After this, through the analysis of the genuine and imposter distributions it was checked to see if a particular stratum of study has significant differences in its match performance.

3. Comparative performance evaluation of matching by statistical analysis.

A set of measures comprising of ROC curves, biometric error rates and divergence distances has been formulated using MATLAB. These measures have served as a critical source of

understanding the impact of the match performance of the various demographic strata when used for the real time testing of a verification system.

1.4 Overview of Biometrics

A biometric system is fundamentally a pattern recognition system that acquires biometric data from an individual and extracts significant features that it uses for comparison against the feature set in the database. Post comparison, the biometric system then executes an action based on the result of comparison. This action that the biometric system executes becomes very critical in establishing the identity of a person and so biometric recognition systems have become an integral part of numerous applications in today's interconnected society. Biometric recognition systems have been able to provide answers to a number of questions like *"Is he/she really who he/she claims to be?", "Is this person approved of access to a particular facility?"* which are the scenarios we come across on a day-to-day basis.

1.4.1 Applications of Biometrics

Biometrics is being widely used in forensics such as criminal identification and prison security, and has a very strong potential to be widely adopted in a broad range of civilian applications [4]. The heightened concerns about security and the enhanced need for trusted user authentication has paved way for biometrics to be used in many government and commercial applications as well. These applications can be widely categorized into three main categories which have been tabulated below.

Table 1.1: Applications of Biometrics

GOVERNMENT	FORENSIC	COMMERCIAL
Welfare disbursement	Criminal Investigation	Access Control, Computer Login
Border Crossing	Corpse Identification	Mobile Phones
National ID Card	Parenthood Determination	ATM
Driver's License, Voter Registration	Missing Children	Internet Banking, Smart Card, E-Commerce

1.4.2 Biometric Characteristics

It is a well-known fact that not all human mannerisms and features can be used as a biometric modality. The biometric measures most commonly [4] used have been illustratively shown in the Figure 1.1.

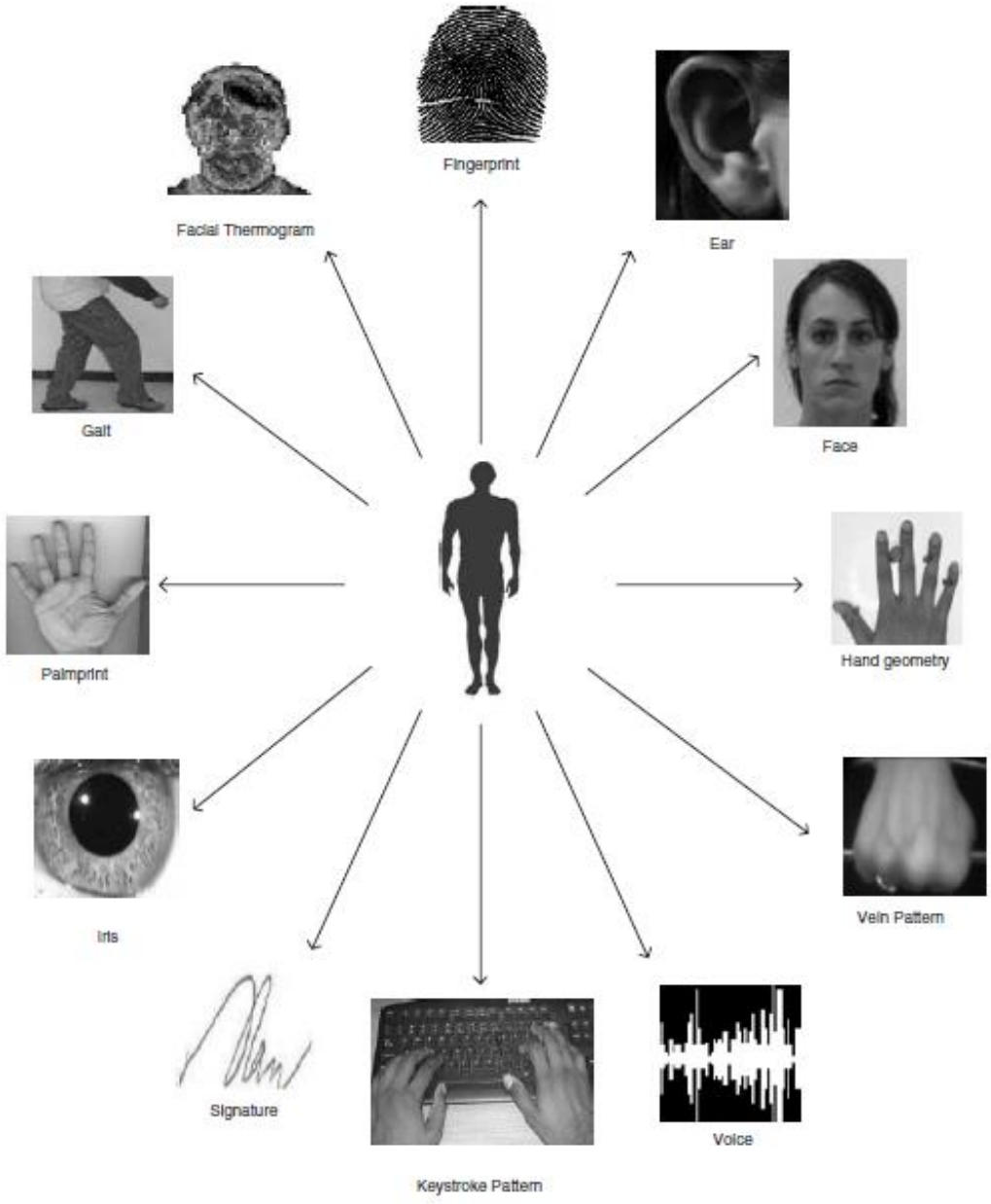


Figure 1.1: An illustration of the various biometric modalities

A human feature can be certified to be a biometric measure only if it possesses certain characteristics [6]. However, only some of these characteristics may affect the match performance statistics. These characteristics have been briefly discussed below

Table 1.2: Characteristics of a Biometric that influence match performance

		Characteristics
1.	Collectability	It is defined as the ability to obtain or extract the required biometric information from a subject which helps in having a large sample test dataset.
2.	Uniqueness	It is defined as the ability of a human element to vary over a given population thereby ensuring that each individual has his/her own distinctive version of the element. This can lead to varied match performance of the dataset.
3.	Permanence	It may be explained as the ability of a human trait or element to retain itself over a long period of time. This characteristic may also lead to consistency in matching scores when tested periodically.
4.	Live-ness	The biometric measure is expected to be live enough in order to be able to circumvent fake templates of the trait.
5.	One-way transform	The ease with which the computational procedures used in the biometric template may be inverted trait makes it more feasible to be used in data stratification tests.

6.	Performance	An ideal biometric characteristic would be the one whose performance is not affected by the manner in which the biometric is collected or processed. This ensures consistency in match performance.
7.	Sample Size	Often, the match performance of a test is inclined towards a sample that is larger in its size in comparison to another stratum under study. Thus, sample size is seen to have a considerable effect on the match performance of a biometric stratum.
8.	Quality	Low quality templates tend to produce low matching scores due to insufficient amount of biometric information. This can lead to a variation in the match scores generated while using these images.

1.5 Fingerprints as an Effective Biometric

Every individual has fingerprints except for those who have severely-damaged fingers or certain genetic defects. Over time, fingerprints have been shown to be relatively distinct as no two identical/indistinguishable fingerprints have ever been discovered. It has also been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person. This high level of uniqueness is what makes fingerprints the prime source of human identity verification [7]. There also exist several models of the individuality of fingerprints which show they are more than suitable for verification purposes and so fingerprints are an excellent choice for a differentiating characteristic in a biometric system. There are several applications of biometric systems which could only work using fingerprints, and which would not be achievable with any other biometric.

Table 1.3: Comparison of various biometric identifiers

Biometric Identifier	Acceptability	Circumvention	Collectability	Distinctiveness	Performance	Permanence	Universality
DNA	L	L	L	H	H	H	H
Ear	H	M	M	M	M	H	M
Face	H	H	H	L	L	M	H
Facial thermogram	H	L	H	H	M	L	H
Fingerprint	M	M	M	H	H	H	M
Gait	H	M	H	L	L	L	M
Hand Geometry	M	M	H	M	M	M	M
Hand Vein	M	L	M	M	M	M	M
Iris	L	L	M	H	H	H	H
Keystroke	M	M	M	L	L	L	L
Odor	M	L	L	H	L	H	H
Palmprint	M	M	M	H	H	H	M
Retina	L	L	L	H	H	M	H
Signature	H	H	H	L	L	L	L
Voice	H	H	M	L	L	L	M

With regard to Table 1.3 [7] it can be understood that fingerprints score higher points when the biometric characteristics such as uniqueness, performance and permanence are being considered. The ease of acquiring fingerprints paves the way for a number of biometric applications of which many modern techniques only require that a finger be pressed against a sensor which prevents the need to use the traditional ink-and-paper family of fingerprint collection methods. Many of the fingerprint-based biometric systems in use today are extremely efficient, and can offer results in seconds (except in special cases like the Integrated Automated Fingerprint Identification Systems (IAFIS) which takes 10 minutes on an average to retrieve results). Thus, it can be seen that in comparison with most other biometric identifiers fingerprints do possess the characteristics of an efficient biometric modality.

1.5.1 Advantages of Fingerprint Biometrics

Among all biometrics, fingerprint biometrics has proved itself the most promising and cost-effective solution in security systems. It's lower cost and accuracy has brought itself in the leading position of all biometric solutions [8]. Although other biometric technologies are gaining popularity, fingerprint is likely to maintain its leading position in the near future. At present, nearly half of the biometric solutions are being implemented using fingerprint biometrics.

The main reasons for the popularity of fingerprint biometrics are listed below:

- Success in various applications in the forensic, government, and civilian domains.
- The fact that fingerprint is an important key for the purpose of investigation.
- The existence of large legacy databases.
- The availability of compact and relatively inexpensive fingerprint readers.
- The ease of access and the low power consumption makes fingerprint based authentication systems a low cost implementation.
- Need of a fairly small storage space results in a reduced database size.

1.5.2 Challenges in Fingerprint Recognition

Although fingerprints have proved to be a vital source in the biometric arena, there are still a number of issues [9] that need to be addressed in order to improve the accuracy and performance of fingerprint based authentication systems. Most of these shortcomings can be attributed to the acquisition process as discussed here.

Small overlapping area and nonlinear distortion

In the consumer based electronic devices fingerprint sensors seem to have a small sensing area and the improper placement of the user's finger on the sensor in an unsupervised condition may result in a limited overlapping area within two impressions of the same finger. This leads to an inadequate number of minutiae in the overlapping area and so it would be difficult to determine if both the fingerprints are of the same finger.

Irreproducible contact

Injuries inflicted to the finger can permanently damage the skin of the finger. In such cases, the impression of the finger may depict a different portion of it and this may introduce additional spurious minutiae.

Non-uniform contact

Factors such as dryness of the skin, shallow or worn-out features, skin diseases, sweat, dirt and humidity in the air can result in a non-ideal contact situation. In such a case the features would not be able to attain a proper sensing surface leading to an imperfect impression of the fingerprint [9]. Inappropriate inking of the fingers in the case of inked fingerprints may also lead to noisy low contrast images causing spurious or missing minutiae.

Inconsistent contact

The projection of the finger onto the image acquisition surface maps a two dimensional impression of the three dimensional finger. This is determined by the pressure and the contact of the finger on the glass platen of the sensor [10]. If these factors are not precisely controlled, different impressions of a finger can be created by various transformations. The result of inconsistent contact of finger with the sensor can result in elastic distortion where different portions of the finger are displaced by different magnitudes in different directions.

Altered/Fake fingerprints

Criminals often cover their fingerprints by artificial fingerprints or they can mutilate their fingers in order to not be identified by automated systems. Any unauthorized user [10] may use a fake finger that imitates a legitimate user's fingerprint to access a computer system or pass security checks.

Interoperability

Interoperability [10] is a big issue in a multivendor environment because different sensor types such as optical, capacitive, RF produce images that are variant in resolution, size, distortion, background noise and contrast. This could be a matter of concern as it can occur in any module

of a fingerprint based biometric system. The difference in encoding the image into binary components may result in varying definition of the same feature. This miscellany makes it difficult to build a fingerprint system with its principal components sourced from different vendors.

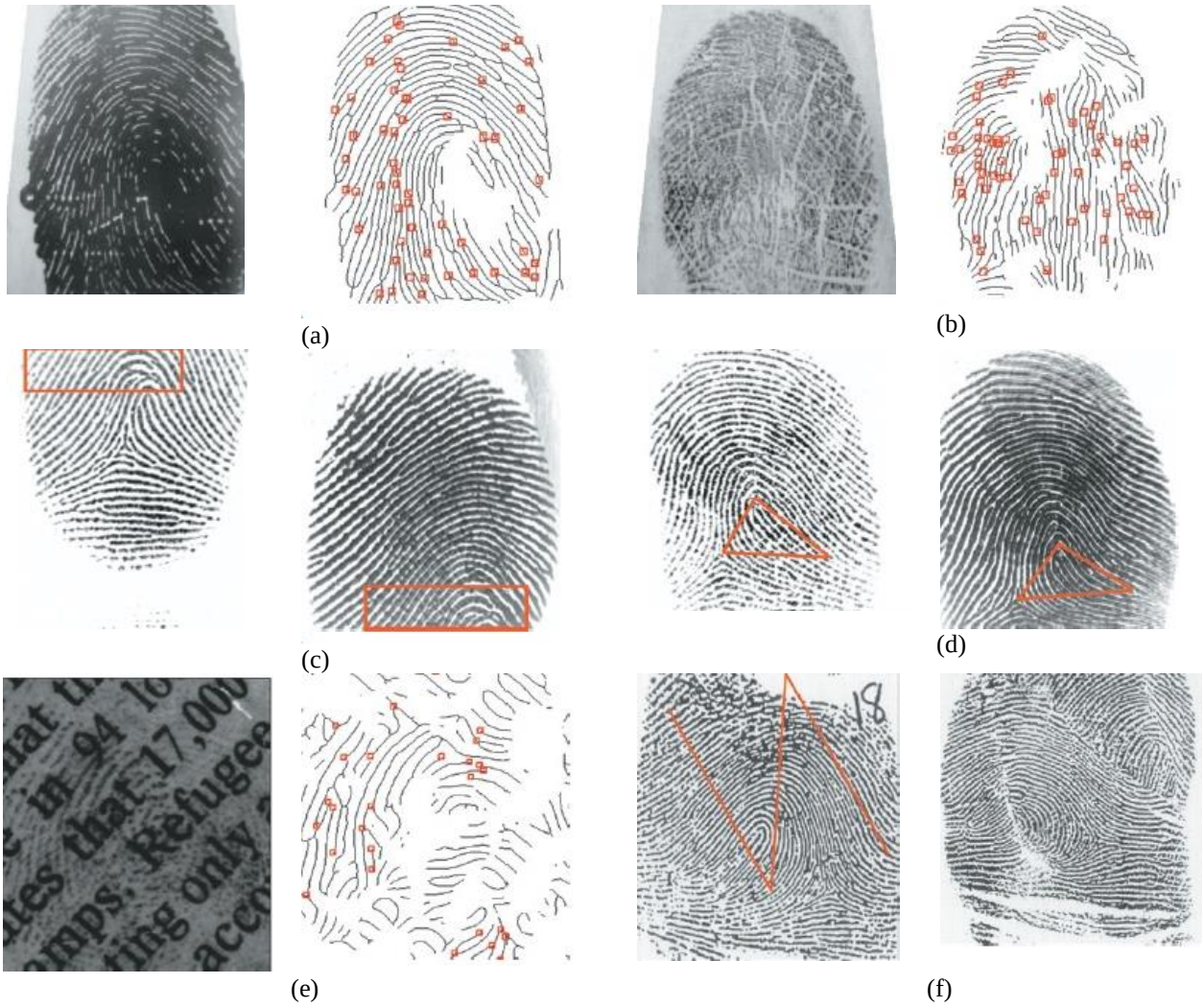


Figure 1.2: Challenges in automated fingerprint processing

(a) Wet fingerprint (left) and extracted features (right) (b) Fingerprint with many cuts (left) and extracted features (right) (c) Small overlapping area as marked by rectangles (d) Large nonlinear distortion in fingerprint patterns as indicated by the corresponding triangles (e) Latent fingerprint with overlapping letters (left) and the extracted features (right) (f) Altered fingerprint: a criminal made a Z-shaped incision into each of his fingers (left), switched two triangles, and stitched them back into the finger (right) [9].

Feature extraction errors

Most feature extraction algorithms often tend to introduce measurement errors [10]. Errors may be made during any of the feature extraction stages (e.g. estimation of orientation and frequency images, detection of the number, type, and position of the singularities, segmentation of the fingerprint area from the background, etc.). Also, enhancement algorithms may introduce conflicting biases that perturb the location and orientation of the reported minutiae from their gray-scale counterparts. The minutiae extraction is another key process of a biometric system which may introduce a large number of spurious minutiae and may not be able to detect all the true minutiae in the case of low-quality fingerprint images.

Considering all the challenges that fingerprint biometrics pose and with regard to the Figure 1.2 we do arrive at a conclusion that they have a serious impact on the performance of a fingerprint biometric authentication system and could significantly affect the matching rates leading to falsified results. Thus, it is of prime importance to tackle these issues in order to ensure a highly productive biometric matching system.

1.5.3 Overcoming the Challenges in Fingerprint Recognition

Improving data acquisition quality

Biometrics sensors that can acquire high quality biometric data will be required to facilitate the significantly higher level of matching accuracy required in a wide range of applications. Resolution of the fingerprint impressions may also be enhanced by employing fingerprint sensors that facilitate the use of extended features for more accurate performance. Similarly, biometrics sensors that can simultaneously acquire 2D/3D data can evolve as an essential component of many applications. Current biometrics systems are predominantly focused on 2D imaging and the use of 3D image acquisition [11] has not delivered its promise due to technological limitations posed by speed, cost, resolution, and size of 3D imagers/scanners as well as the representation and matching issues. Therefore, continued design and development of multimodal biometric sensors that can simultaneously acquire 2D and 3D images would prove extremely beneficial in the development of biometric technologies.

Handling Poor Quality Data

To improve the matching accuracy, extended fingerprint feature set (EFS) has been utilized in addition to minutiae. However, manually marking EFS is very tedious and therefore robust automatic extraction algorithms are being developed for this purpose. The increased capabilities to handle poor quality data for biometric identification is not only required for improving latent matching accuracy but is also essential for a range of biometric systems employed for commercial applications [11]. The failure to enroll rate (FTE) and the achievable throughput from the deployed biometrics system can also be further improved by imparting new capabilities that can handle poor quality biometric data. New user enrolments in a large-scale biometric system will typically require periodic re-training or updating of the matcher. Therefore, another aspect of an adaptive biometric system is online learning, which can periodically update the matcher. The likelihood ratio-based fusion can effectively handle the problem of missing biometric modality/data, which could also be perceived as an user preference in adaptive multimodal biometric systems. New user enrolments in a large-scale biometric system will typically require periodic re-training or updating of the matcher.

Fingerprint Mosaicking

In cases where there is only a small overlapping area between two impressions, a feasible solution to overcome the issue would be fingerprint mosaicking which combines multiple smaller images into a larger image [9]. More ergonomic and intuitive interfaces can guide users to properly place the central area of their finger on the sensor. Also, using local minutiae descriptors before the global aggregation of local matches may be considered while matching fingerprints locally.

Liveness Detection

To detect a mutilated finger, a mutilation detector can be added and effort should be made to identify the subject either by restoring the original fingerprints or using the only unaltered areas of the fingerprint. To recognize fake fingerprints, the hardware based liveness detection technique can be adopted which measures and analyzes various vital signs of the live finger such

as pulse, perspiration and deformation. The use of multibiometrics has also proved to be a solution to tackle altered fingerprints.

Improving interoperability

As a solution aimed at improving the interoperability among multiple fingerprint systems, international standardization organizations have established standards for sensors, templates and systems testing. This includes image quality specifications for fingerprint sensors and data exchange formats for minutiae templates. However, the proprietary templates have exhibited superiority in matching accuracy compared to the standard templates in NIST MINEX testing [10]. Hence, it is to be understood that the existing standards still have a scope of improvement.

System on Device

Security issues such as tampering or modification of hardware/software components and interception of fingerprint data passing through the communication channels can be of serious concern especially when in commercial applications. This problem can be overcome by employing system-on-device technology in which the sensor, feature extractor, matcher, and even the templates reside on a tamper-resistant device [10]. Cryptographic tools can be leveraged to prevent interception and alteration of fingerprint information. These methods ensure that the information about a user's fingerprint never leave the device and it is only the matching that is securely transmitted.

Template Security

Applying a noninvertible mathematical transformation to the fingerprint template and storing only the transformed template could be an efficient way of securing the templates. Using this transformation even if the fingerprint template is revealed the original fingerprint cannot be gleaned easily [10]. The same fingerprint can be used to generate a new template by applying a varied transformation and so it is referred to as a cancellable fingerprint. Employing biometric cryptosystems and generating cryptographic keys based on biometric samples is another promising solution to enhance template security.

1.5.4 Applications of Fingerprint

A vast number of a security and commercial applications today depend on fingerprint as their primary source of identification. Fingerprints are used for the purpose of information security and also in National ID systems for voter registration and identification. Identification of suspects and identification of missing children using their fingerprint data has also been an important application which has helped national agencies such as the FBI (Federal Bureau of Investigation) [4]. Fingerprints have also been used to provide biometric security thereby restricting the access to secure areas or systems such as ATM, at airports etc. Identifying the deceased victims of major disasters or amnesia victims by having their fingerprints on file has been extremely helpful at the time of calamities. Conducting a background check (including applications for government employment, defense security clearance, concealed weapon permits, etc.) in most cases also use fingerprint as the key for the purpose of verification.

(a)

(b)

(c)

Figure 1.3: Applications of Fingerprints

(a) The US-VISIT program currently employs two-print information to validate the travel documents of visitors to the United States [http://www.aci-na.org]. (b) Shows the Immigration and Naturalization

Service Accelerated Service System (INSPASS) installed at major airports in the U.S which is based on fingerprint verification technology developed by Recognition Systems, Inc. and significantly reduces the immigration processing time [7] (c) A fingerprint verification system manufactured by Digital Persona Inc. used for computer and network login [7].

1.6 Fingerprint Evaluations

The single most critical resource needed to successfully evaluate a biometric system is data and this is true for any pattern recognition application. Unavailability of a large dataset limits the scope of evaluation and the testing of new algorithms. Beyond sheer quantity, it is also crucial to understand the type and quality of biometric data changes between data sources. A number of such factors apply to fingerprints which have an impact on the performance of the biometric system [8]. These include capture type: were the images of fingerprints generated by scanning paper cards of inked fingerprints, or were they generated using a live scan device? There is impression type: are the fingerprints rolled nail-to-nail, or are they a plain (flat) impression? Other attributes such as the image quality, minutiae count detection etc. are also factors that assist in testing the credibility of the dataset and the biometric system.

With years of FBI collaboration, NIST has acquired and distributes the largest publicly available collection of federal law enforcement fingerprint images. NIST has considerably added to its fingerprint image repository [13], including operational data from federal agencies, state and county jurisdictions, and Department of Defense (DOD) applications. Nearly all this new data is considered sensitive but unclassified. Hence, it is not available to the general public.

The datasets described below are carefully sampled and utilized by NIST to test fingerprint matching algorithms and systems. These experiments are conducted and the results are reported based on the elemental requirement that a biometric system reports which is a similarity score when two biometric templates are compared to each other. In general, the higher the score, the more likely it is that the two templates belong to the same person. This fundamental concept is also the underlying idea that forms the base in the science of fingerprint matching.

Listed below are some of the multijurisdictional datasets at the National Institute of Standards and Technology (NIST) [13] that have been tested for quality based on the type of impression.

Table 1.4: Multijurisdictional datasets at NIST

NAME	SCAN TYPE	PLAIN	ROLL	TESTS	SIZE	QUALITY
US-VISIT: Jan 04 -Feb 04	Live	Index		Plain: Plain	34×10^3 matched 1.7×10^6 subjects	Good
US - VISIT Mar 04-Jun 04	Live	Index		Plain :Plain	3.7×10^6 subjects	Good
SD 29	Ink	10	10	Roll: Roll, Plain: Plain, Plain: Roll	216 card pairs	Medium
IAFIS	Ink w/Live		10	Roll: Roll, Plain: Roll	1.2×10^6 cards	Operational
SD 14 (V2)	Ink w/Live		10	Roll: Roll	2700 card pairs	Medium
INS INDEX	Live(DFR-90)	Index		Plain: Plain	620×10^3 subjects	Operational
INS Benefits	96% Live , 4% rescan	10		Roll: Roll, Plain: Plain, Plain: Roll	640×10^3 subjects	Operational
DOS-BCC	Live(DFR-90)	Index		Plain: Plain	6×10^6 subjects 240×10^3 matched	Operational Office
INS CARD	Ink	10	10	Plain: Roll	100×10^3 cards	Operational
TX	60% Ink, 40% Live	10	10	Plain: Roll	1×10^6 cards	Operational
ESD	Live	10	10	Plain: Roll	3×10^3 cards	Good
LA County	90% Live; 10% rescan	10	10	Roll: Roll, Plain: Plain, Plain: Roll	1.5×10^6 subjects 100×10^3 matched	Good
FBI 12K	Ink w/Live	10	10	Plain: Roll	12×10^3 subjects	Operational

Fingerprint Vendor Technology Evaluation (FpVTE)

This fingerprint vendor test was designed to measure the accuracy of fingerprint matching (identification, and verification systems) [16] and identify the most accurate fingerprint matching

systems. It also determines the viability of fingerprint systems for near-term deployment in large-scale identification systems and evaluates the effect of a wide variety of variables on matcher accuracy.

Software Development Kit (SDK) Tests

The NIST SDK fingerprint matcher tests are a medium scale evaluation of one-to-one verification [13]. Goals of these tests include determining the feasibility of verification matching in US-VISIT and DOS application clients, evaluating vendor accuracy variability and vendor sensitivity to image quality. Furthermore, these tests were used to scale evaluations in FpVTE.

US - VISIT CERTIFICATION

There are three main biometric functions provided by the DHS US-VISIT system which include watch list checking at the time of enrollment, duplicate identification checks for visa holders and one-to-one verification for enrolled travelers. Table 1.5 and Table 1.6 [16] refer to the standard fingerprint evaluated datasets

Table 1.5: Some standard evaluated datasets in the history of fingerprint matching

NAME	DATABASE SIZE	ALGORITHMS EVALUATED	RESULTS
FVC 2004	4 databases, each containing 800 fingerprints from 100 fingers	Open Category: 41 Large Scale Test (LST): 13 Evaluated Light Category:26	Best average EER: 2.07% (in the Open Category)
FpVTE 2003	48,105 fingerprint sets from 25,309 subjects	Large Scale Test (LST): 13 Evaluated Light Category:26 Medium Scale Test (MST):18 Small Scale Test (SST): 3 (SST only)	Best EER on MST: 0.2% (MST is the FpVTE2003 test closest to FVC2004).

Table 1.6: Comparison between FVC2004 and FpVTE2003

	FVC2004	FpVTE2003
Data collection	All the data were acquired for this event	Data coming from existing U.S. Government sources
Fingerprint format	Single finger flat impressions acquired through low-cost commercial fingerprint scanners (including small area and sweeping sensors	Mixed formats (flat, slap, and rolled from different sources; scanned paper cards, and from FBI-complaint fingerprint scanners)
Subject population	Students (24 years old on the average)	Operational fingerprint data from a variety of U.S. Government sources including low-quality fingers and low-quality sources
Anonymous participation	Allowed	Not allowed
Evaluation type	Independent strongly supervised	Independent supervised
Database availability	Databases are available to the scientific community	Databases are not available due to data protection and privacy issues
Perturbations	Deliberately exaggerated perturbations (rotation, distortion, dry/wet fingers)	Difficulties mainly due to intrinsic low-quality fingers of some subjects and sometimes due to non-cooperative users

1.7 Thesis Outline

In Chapter 2 we describe the nature of biometric systems and the basic tasks of a generic biometric system. We also discuss the various components of a fingerprint matching system and the process used by fingerprint recognition systems for matching fingerprints. We also review the strategies and algorithms used in different matching techniques based on fingerprint biometrics. We also review the statistical methods that could be used for analytical purposes. Discussion of the various error rates that determine the performance of a biometric system and statistical divergence measures form the central part of this chapter.

In Chapter 3 we discuss about the fingerprint dataset under study and its features such as demographics and the scanners employed while acquiring these images.

In Chapter 4 we describe the overall features of our fingerprint matching system. We cover the various aspects of its design and implementation also specifying how each component of our system matches with an explanation of each of its functions. We also discuss the file formats supported and the tools and libraries used to accomplish the task of matching.

In Chapter 5 we discuss the various results obtained after the experimentation with illustrations and an in-detailed explanation of its implication.

In chapter 6 we elaborate the conclusions arrived at in this study and also discuss its prospective potential.

CHAPTER 2 - THEORETICAL BACKGROUND

2.1 Generic Biometric System

In totality, a biometric authentication system consists of five major functional subsystems. These subsystems primarily perform the functions of data collection, transmission, signal processing, decision and data storage [12].

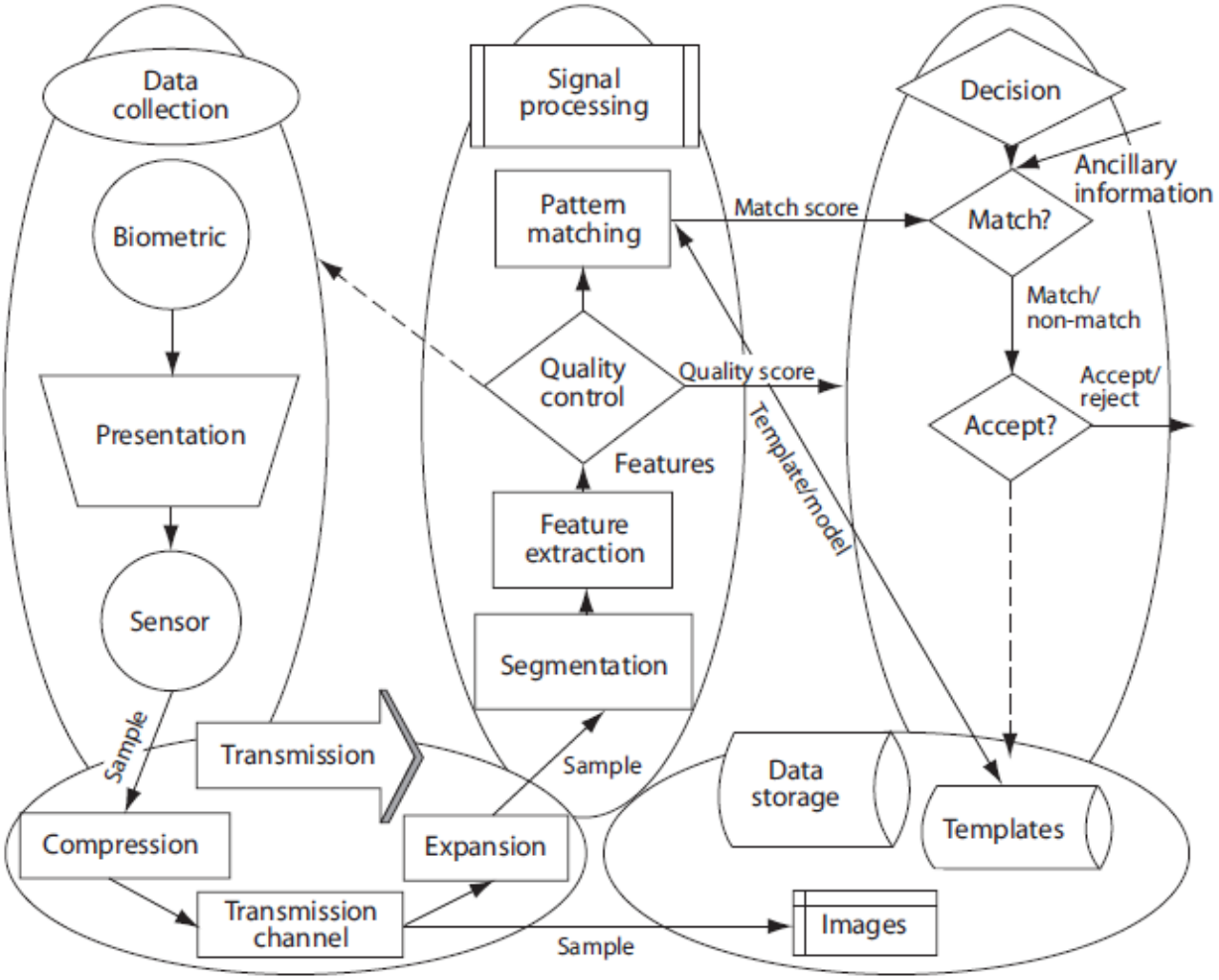


Figure 2.1 : Generic biometric system

Data Collection Module

The data collection subsystem samples the unprocessed biometric data and the data acquisition sensor converts this data into an electronic representation that is then used by the transmission

subsystem. In cases, where a great amount of data is involved, compression may be required before transmission to conserve bandwidth and storage space.

Transmission Module

The transmission subsystem transports the electronic representation of the raw biometric data to the signal processing subsystem.

Signal Processing Module

With reference to Figure 2.1 the signal processing subsystem executes four major tasks namely segmentation, feature extraction, quality control and pattern matching. Segmentation is the process of finding the required biometric pattern within the transmitted signal. After segmentation, the extraction of features is needed which a form of non-reversible compression. This means that the original biometric image cannot be reconstructed from the extracted features. The non-controllable distortions and any non-distinctive or redundant elements are removed from the biometric pattern while at the same time preserving those qualities that are distinctive and repeatable [12]. After feature extraction or sometimes before, it is essential to check if the signal received from the data collection subsystem is of good quality. If the features extracted are insufficient in quality in some way, then it can be concluded that the received signal was defective and a new sample may be requested from the data collection subsystem while the user is still at the sensor. The processed feature is then sent to the pattern matching process for comparison with one or more previously stored feature templates or models. The pattern matching process compares a presented feature sample to the stored data and sends a quantitative measure of the comparison to the decision subsystem.

Decision Making Module

The decision subsystem determines the "matches" or "non-matches" based on the similarity measures received from the pattern matcher and ultimately makes the "accept/reject" based on the system decision policy. This decision policy is specific to the operational and security requirements of the system. In most cases, lowering the number of false non- matches can be traded against raising the number of false matches. The most favorable policy in this regard

depends upon both the statistical characteristics of the comparison distances coming from the pattern matcher and the relative penalties for matching error rates within the system. In any case, it is necessary to decouple the performance of the signal processing subsystem from the policies implemented by the decision subsystem.

Storage Module

There can be multiple ways of storage depending upon the structural orientation of the biometric system [12]. For the purpose of verification which is nothing but "one-to-one" matching the database may be distributed on optically read cards, magnetic stripe cards carried by each enrolled user. The means of storage may be centralized if the system performs one-to-N matching with N greater than one as in the case of identification.

2.1.1 Tasks of a Biometric System

Based on the environment of application a biometric system may function either in the verification mode or identification mode .However, irrespective of the application context, a biometric system compares the feature set from the acquired data against the template in the database which is its chief functionality in both the verification and identification modes of operation.

In the verification mode of operation the biometric system aims at preventing multiple people from using the same identity. The system validates a person's identity by comparing the captured data with his/her own data templates in the storage subsystem [5]. A person who wishes to be recognized by the system claims an identity usually by means of a personal identification or name and the system conducts a one-to-one comparison to verify the truth of the claim. Thus, the verification mode of operation enables positive recognition.

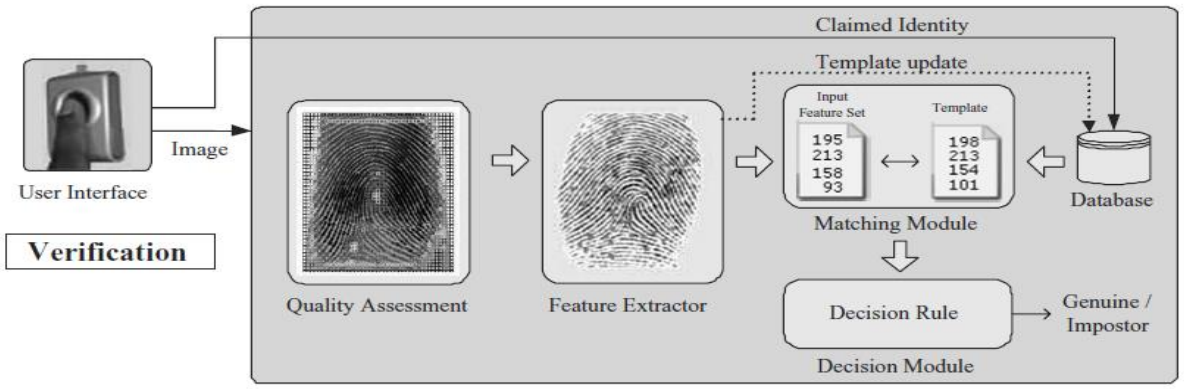


Figure 2.2 : Verification mode of a biometric system

In the identification mode of operation the biometric system aims at preventing a single person from using multiple identities. The system recognizes an individual by conducting a one-to-many comparison with all the users in the database for a match [5]. Hence, identification becomes critically important in negative recognition applications where the system implicitly or explicitly states whether the person is who he/she denies to be. For convenience, identification may also be used in positive recognition applications where the user is not required to claim an identity.

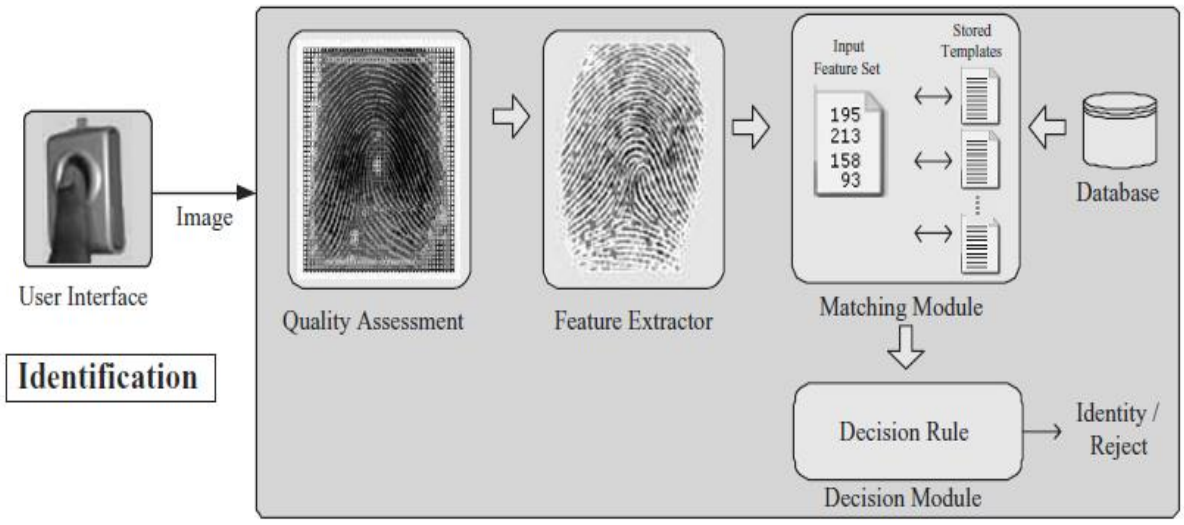


Figure 2.3 : Identification mode of a biometric system

2.2 Fingerprint Based Biometric System

Owing to the efficacy of fingerprints as a biometric modality fingerprint recognition systems have now become an integral part of many day-to-day applications. Automatic fingerprint

recognition systems also seem more advantageous in terms of performance and its low cost availability.

In the following sections the main components of a fingerprint based biometric system are introduced which is also schematically seen in Figure 2.4. The three stages of fingerprint recognition consist of sensing, feature extraction and matching.

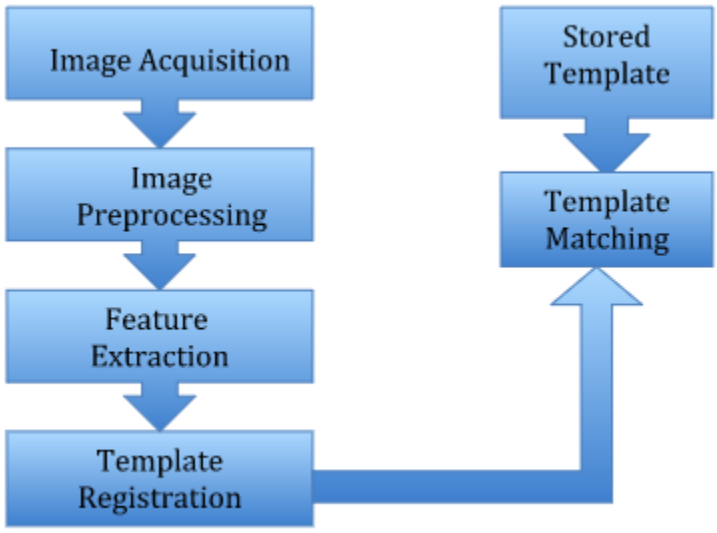


Figure 2.4: Schematic diagram of a fingerprint recognition system

2.2.1 Fingerprint Acquisition Technologies (Sensing)

Fingerprint acquisition is the most important part of a biometric recognition process as it is the component where the fingerprint image is formed. This is the enrollment phase [5] during which the sensor scans the user's fingerprint and converts it into a digital image.

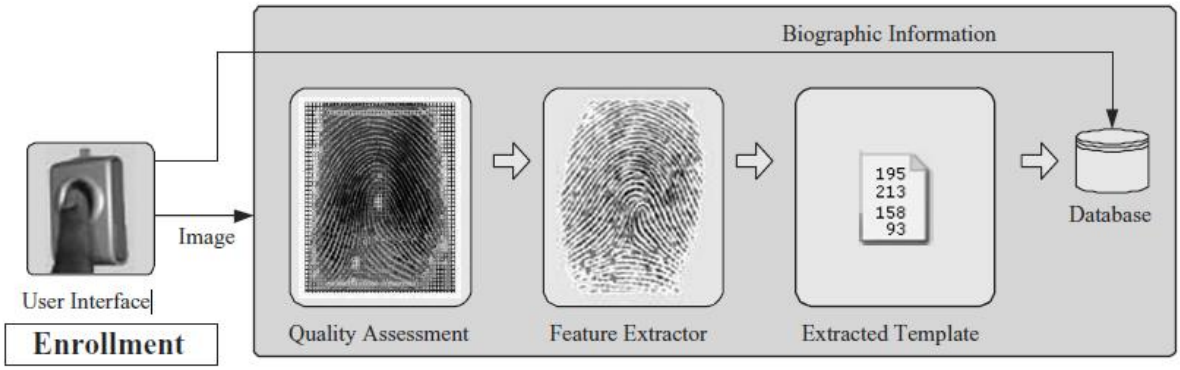
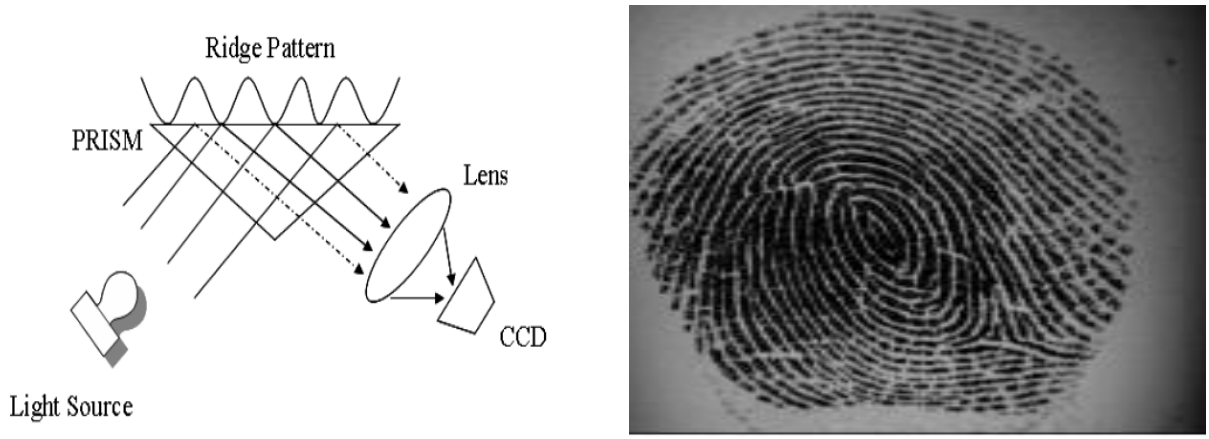


Figure 2.5 : Enrollment phase of a fingerprint biometric system

Almost all the existing fingerprint sensors belong to one of the three families of sensors: optical, solid-state, and ultrasound.

Optical Sensors

The sensors employed in this study work on the principles of optical sensing. Optical Sensors have the longest history of all fingerprint image acquisition devices. The optical sensors function on the principle of Frustrated Total Internal Reflection (FTIR) [19] as shown in Figure 2.6. The finger touches the top side of a glass prism. While the ridges (curved dark lines) enter in contact with the surface of the prism the valleys (bright areas) remain at a certain distance. The light entering the prism is absorbed at the ridges and reflected at the valleys. The difference in reflective ability allows the ridges to be differentiated from the valleys. The features sensed would then be focused onto a CCD or CMOS image sensor and the light rays exit from the prism. The major advantages of the optical fingerprint sensor technologies are low cost and its strength to the prevention of Electro Static Discharge (ESD). Optical sensors contain the following technologies: Optical reflection, Optical transmission, Optical Sweep, Optical touch less, Optical TFT and Electro-Optical. Refer to figure 2.6 [19] for the illustration showing the working of an optical sensor.



(a) (b)

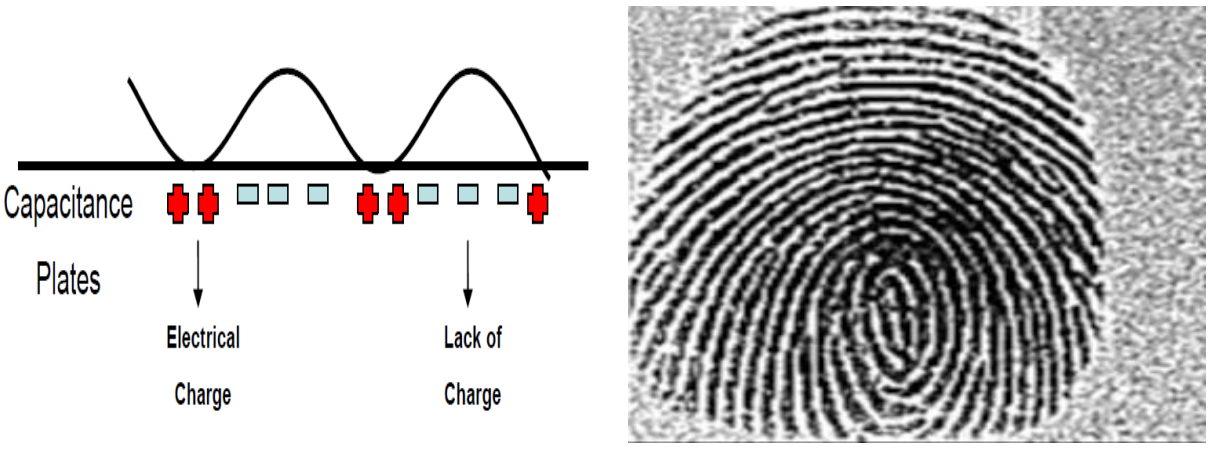
Figure 2.6 : Optical Sensor Technology

(a) Working principle (b) Image captured using an optical sensor

Solid State Sensors

Capacitive sensors have also been employed for acquiring images of the fingerprint dataset and so it is necessary to understand how they work. All silicon-based sensors consist of an array of pixels wherein each pixel is a tiny sensor itself. In this mode of fingerprint acquisition technology the user directly touches the surface of the silicon which implies that neither optical components nor external CCD/CMOS image sensors are needed. Four main effects have been proposed to convert the physical information into electrical signals namely capacitive, thermal, piezoelectric and electric [19]. Of these, the most commonly employed solid state sensor technologies have been discussed here.

Capacitive sensors use the electrical property of "capacitance" to make measurements as shown in Figure 2.7 [19]. Capacitance is a property that exists between any two conductive surfaces within some reasonable proximity. The measurement of the capacitance between the skin and the pixel is the most physical effect used to acquire fingerprints. Where there is a ridge or a valley, the distance varies, as does the capacitance. The sensors use small sensing surfaces and as result are positioned close to the targets. The measured capacitance values are then used to distinguish between fingerprint ridges and valleys. The advantages of the capacitive silicon fingerprint sensor technologies are small in size, low power consumption and work for almost everyone. The significant drawbacks are vulnerability to strong external electrical fields, the most dangerous being ESD and the high cost of the silicon area sensors.



(a) (b)

Figure 2.7: Solid State Capacitive Sensor Technology

(a)Working principle (b) Image captured using a capacitive sensor

2.2.2 Fingerprint Image Quality Assessment

The capability of a biometric system to detect and handle samples of varied quality levels is a significant contributor in estimating its proficiency as a biometric recognition system. Automated and consistent quality assessment of input samples is an important component of any biometric system which also holds true for fingerprint recognition systems. The term 'quality' [20] is used in three different contexts as it relates to biometric sample quality (ISO, 2006) which have been listed below:

1. *Fidelity*: reflects the accuracy of a sample's representation of the original source.
2. *Character*: reflects the expression of inherent features of the source.
3. *Utility*: reflects the observed or predicted positive or negative contribution of the biometric sample to the overall performance of a biometric system.

Quality assessment algorithms compute the quality score of a biometric image using fidelity, character, utility or a combination of the three. Existing image quality assessment algorithms may be subdivided into four broad categories:

1. Based on local features.
2. Based on global features.
3. Based on classifiers.

4. Hybrid algorithms based on local and global features.

These algorithms have been termed based on the component of the image employed in the course of assessment. In the local feature quality algorithms the fingerprint image is subdivided into blocks followed by the quality score computation for each block. This type of analysis takes into account specific local features. The global feature quality assessment algorithms search for abrupt changes in ridge orientation [19]. These algorithms tend to use 2-D discrete Fourier transform and energy concentration analysis of global structure to assess the image quality of fingerprints. The third category of quality assessment algorithms is based on the premise that a quality measure should define a degree of separation between match and non-match distributions of a fingerprint. Using a relatively large dataset, classifiers can be trained using a degree of separation as a response variable based on a vector of predictors and then map the degree of separation to a quality index. Hybrid algorithms are the ones which use an aggregation of local and global feature analysis to compute a quality index.

2.2.3 Fingerprint Feature Extraction

A fingerprint is an impression of the epidermal ridges of a human fingertip. A hierarchy of three levels of features, namely, Level 1 (pattern), Level 2 (minutiae points) and Level 3 (pores and ridge shape) are used for recognition purposes. Level 1 features refer to the overall pattern shape of the unknown fingerprint—a whorl, loop or some other pattern. This level of detail cannot be used to individualize, but it can help narrow down the search. Level 2 features refers to specific friction ridge paths — overall flow of the friction ridges and major ridge path deviations (ridge characteristics called minutiae) like ridge endings, lakes, islands, bifurcations, scars, incipient ridges, and flexion creases. Level 3 detail refers to the intrinsic detail present in a developed fingerprint — pores, ridge units, edge detail, scars, etc. Figure 2.9 [20] shows the various levels of fingerprint features used for matching.

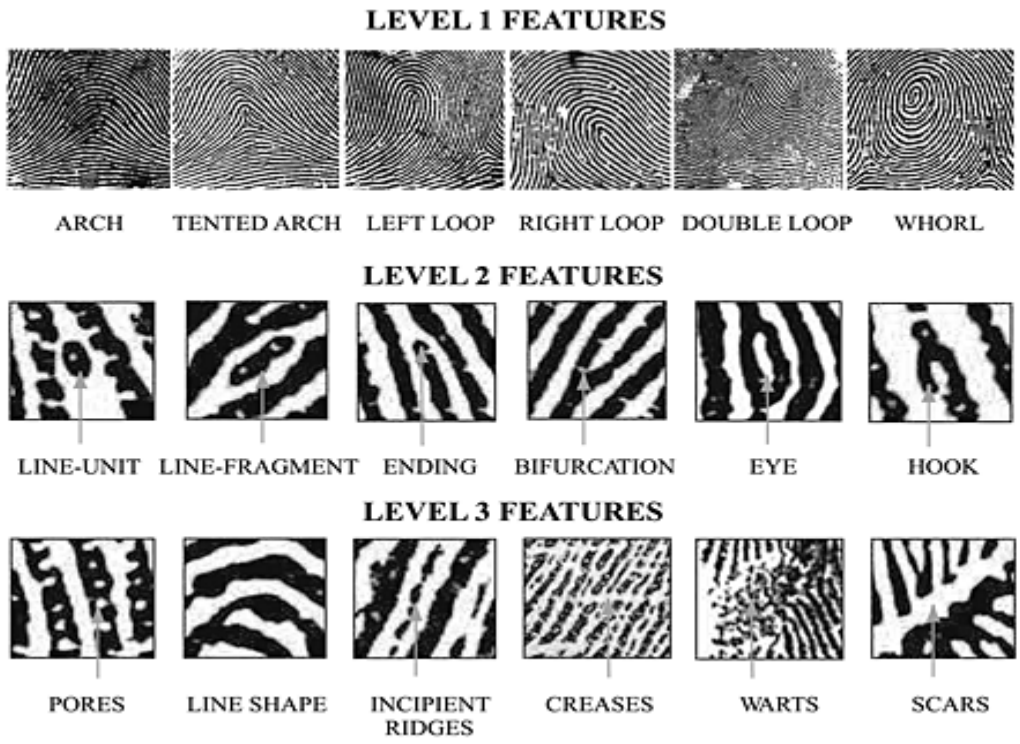


Figure 2.8 : Categorization of fingerprint features

Fingerprint feature extraction is the process of extracting useful features for identification and/or authentication from the biometric. The phase of feature extraction is tied to the process of image enhancement and it is always an area of concern to determine where the image enhancement process ceases and the feature extraction begins.

Figure 2.9 [16] below provides a graphical representation of the main feature extraction steps and their interrelations.

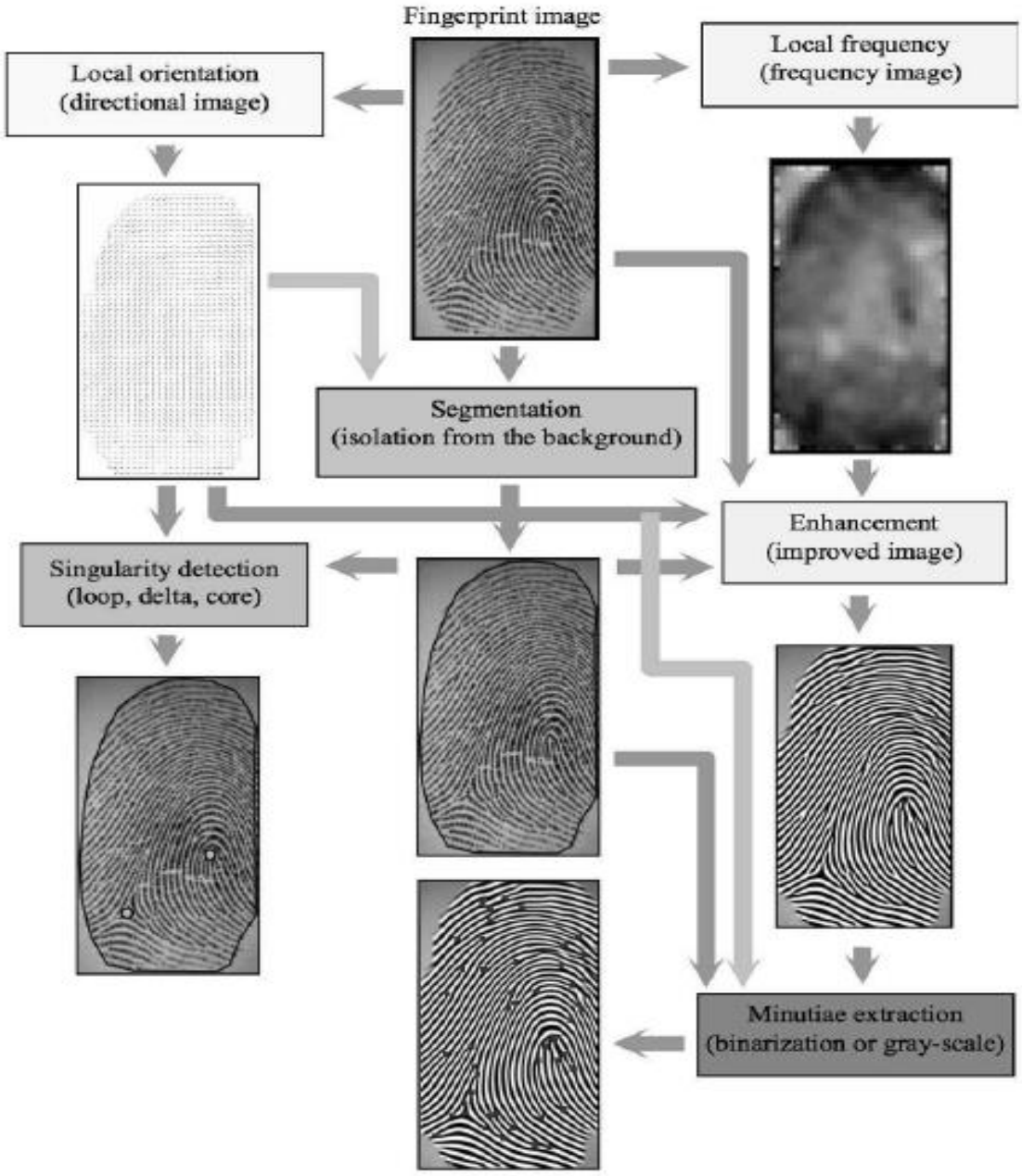


Figure 2.9: Graphical representation of fingerprint feature extraction steps and their interrelations

Local Ridge Orientation Estimation

The fingerprint image is typically separated into small regions and the gradient is analyzed to estimate the average direction of the ridges contained within that particular section. In order to make the estimate as accurate as possible the regions can be reduced in size. The local ridge orientation at a point (x, y) is given by the angle θ_{xy} which is the arbitrary small neighborhood that the fingerprint ridges forms with the horizontal axis. The local ridge density (or frequency)

f_{xy} at a point (x, y) can be defined as the number of ridges per unit length along a hypothetical segment centered at (x, y) and perpendicular to the local ridge orientation θ_{xy} . The local ridge frequency may also be computed by counting the average number of pixels between two consecutive peaks of gray - levels along the direction normal to the local ridge orientation [21].

Segmentation

Segmentation is the process of separating the foreground regions in the image from the background regions. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information .When minutiae extraction algorithms are applied to the background regions of an image, it results in the extraction of noisy and false minutiae. Thus, segmentation is employed to discard these background regions, which facilitates the reliable extraction of minutiae. In a fingerprint image, the background regions generally exhibit a very low grey-scale variance value, whereas the foreground regions have a very high variance. Hence, a method based on variance thresholding can also be used to perform the segmentation [21].

Fingerprint Image Enhancement and Binarization

The goal of fingerprint enhancement is to perk up the precision of the ridge structures in the recoverable regions and mark the unrecoverable regions as too noisy for further processing. The most commonly used technique for image enhancement is based on contextual filters. In this method, the filter characteristics vary according to the local context defined by local ridge orientation θ_{xy} and local ridge frequency f_{xy} [16]. Employing a band pass filter i.e. tuned to the corresponding frequency and orientation can effectively remove the undesired noise and preserve the true ridge and furrow structures. The fingerprint image is then passed through the filtering stage. Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains. Therefore, it is appropriate to use Gabor filters as band pass filters to remove the noise and preserve true ridge/valley structures.

Binarization is the process that converts a grey level image into a binary image. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates

the extraction of minutiae. Usually grayscale image is converted into binary image using a global threshold. The binarization process involves examining the grey-level value of each pixel in the enhanced image, and, if the value is greater than the global threshold, then the pixel value is set to a binary value one; otherwise, it is set to zero. The outcome is a binary image containing two levels of information, the foreground ridges and the background valleys [22].

Let I (x, y) represent the intensity value of enhanced grayscale image at pixel position (x, y). Let T_P be the threshold value [16]. In case of fingerprint images T_P represents the differentiating intensity between the background pixels and ridge pixels. BW(x, y) represent the binary image obtained by the equation.

$$BW_{(X,Y)} = \begin{matrix} 1, \text{ if I (x, y)} \geq T_P \\ 0, \quad \text{Otherwise} \end{matrix} \qquad \text{Eq (2.1)}$$

Thinning

Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide [23] seen in Figure 2.10 [20].The application of the thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeletonized version of the binary image. Each sub-iteration begins by examining the neighborhood of each pixel in the binary image, and based on a particular set of pixel-deletion criteria, it checks whether the pixel can be deleted or not. These sub-iterations continue until no more pixels can be deleted. This skeleton image is then used in the subsequent extraction of minutiae.

Minutiae Extraction

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood with reference to Table 2.1 and Table 2.2 [24], [25]. According to Rutovitz the crossing number for a ridge pixel is given by the equation:

$$\text{CN} = \sum_{i=1}^{8} | P_i - P_{i-1} | , P_9 = P_1 \qquad \text{Eq (2.2)}$$

Where Pi is the pixel value in the neighborhood of P. For a pixel P, its eight neighboring pixels are scanned in an anti-clockwise direction as follows:

Table 2.1 : 3×3 window for searching minutiae

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

The pixel can then be classified according to the property of its CN value. Using the properties of the CN it may be classified into one of the following types:

Table 2.2 : Properties of Crossing Number

CN Value	Property
0	Isolated point
1	Ridge ending point
2	Continuing ending point
3	Bifurcation point
4	Crossing point

(a) (b) (c) (d)

Figure 2.10: Feature extraction in a fingerprint

(a) A fingerprint gray-scale image (b) The image obtained after enhancement and binarization (c) The image obtained after thinning (d) Termination and bifurcation minutiae detected through the pixel-wise computation of the crossing number.

2.2.4 Fingerprint Matching

Once all the required features have been extracted, matching can be achieved. Matching algorithms are broad and varied in their approaches, techniques, and methodologies, and employ

many different strategies in an attempt to increase their efficiency, to increase their match-speed, to reduce the memory footprint, or to improve accuracy. Most methods of fingerprint matching follow a similar pattern involving an orientation estimation, segmentation of the fingerprint image, ridge detection and thinning, and finally, the minutiae detection [26].

Correlation Based Matching

In this class of fingerprint matching two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations). Fourier transform may then be used to speed up the correlation computation [16]. The mathematical formulation for this method is discussed below:

Let $\boldsymbol{I}^{(\Delta x,\Delta y,\theta)}$ represent a rotation of the input image **I** by an angle Ɵ around the origin shifted by Δx and Δy pixels in directions x and y respectively. The similarity between these two images may then be computed as

$$\mathrm{S}\ (\mathbf{T},\ \mathbf{I}) = \max_{\Delta x,\Delta y,\theta} CC\ (\boldsymbol{T}, I^{(\Delta \boldsymbol{x},\Delta \boldsymbol{y},\boldsymbol{\theta})}) \qquad \text{Eq (2.3)}$$

where CC(**T,I) =** $\boldsymbol{T^T}$ **I** is the cross- correlation between **T** and **I** where **T** is the template and **I** is the image**.** The cross correlation technique of fingerprint matching proves to be advantageous as an efficient measure of image similarity. Also, the maximization obtained from the mathematical formulation above allows the fingerprint matching system to find an optimal registration. However, in comparison to other matching approaches this technique suffers from certain drawbacks which necessitates the need to employ other techniques in the course of fingerprint matching.

Minutiae Based Matching

Two fingerprints match if their minutiae points match. This approach of minutiae based fingerprint matching is also the backbone of the currently available fingerprint recognition products and forms the most extensively employed technique of fingerprint matching. Minutiae (i.e., ridge ending and ridge bifurcation) are extracted from the registered fingerprint image and the input fingerprint image, and the number of corresponding minutiae pairings between the two images is used to recognize a valid fingerprint image [27]. Figure 2.11 [27] shows the various

fingerprint extraction techniques. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Most common minutiae matching algorithms consider each minutia as a triplet m ={x, y,θ} that indicates the (x, y) minutia location coordinates and the minutia angle.

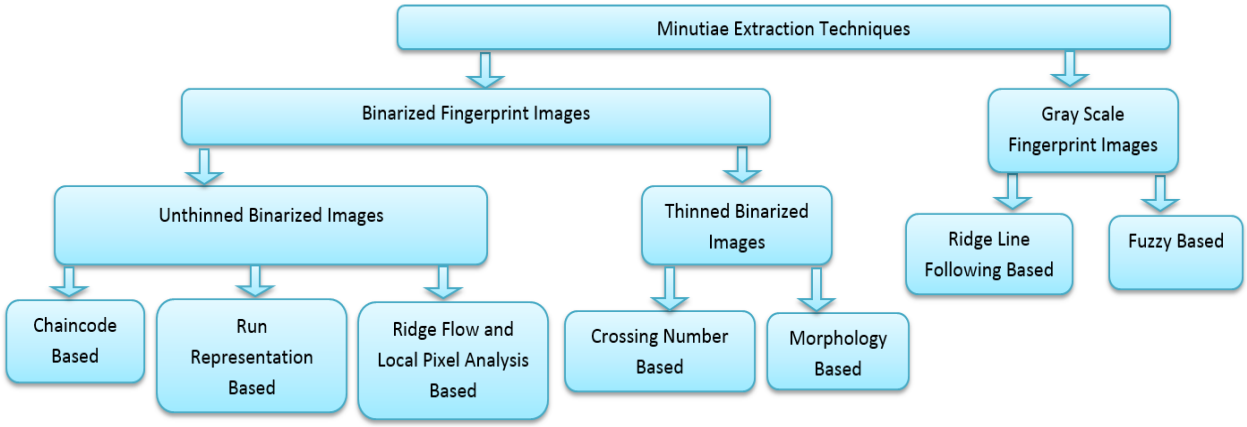


Figure 2.11 : Minutiae based extraction techniques

The matching algorithms may be roughly categorized into two groups based on the scope of their respective matching techniques. These two groups are commonly referred to as "global matching techniques" and "local matching techniques". There are significant differences in the way these two types of matching algorithms are typically designed, in what contexts they are used, and how they treat or process their data. The trade-offs between local and global techniques include: algorithm complexity, computational complexity, distortion tolerance, and discriminatory power.

Pattern-based (or Image-based) Matching

Pattern based algorithms compare the basic fingerprint patterns (e.g., local orientation and frequency, ridge shape, texture information) between a previously stored template and a candidate fingerprint [27]. The images need to be aligned in the same position, about a central point on each image. The candidate fingerprint image is then graphically compared with the template to determine the degree of match. The image-based techniques include both optical as well as computer-based image correlation techniques.

Non-Minutiae Feature-Based Matching

Minutiae extraction is difficult in extremely low-quality fingerprint images. While some other features of the fingerprint ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, their distinctiveness as well as persistence is generally lower. The approaches [10] belonging to this family compare fingerprints in terms of features extracted from the ridge pattern. In principle, correlation-based matching could be conceived of as a subfamily of non-minutiae feature-based matching, in as much as the pixel intensities are themselves features of the finger pattern.

2. 3 Comparison of Various Fingerprint Matching Techniques

Table 2.3 : Comparison of various fingerprint matching techniques

Class	Advantages	Disadvantages
Correlation Based	• Effective image similarity. • Optimal registration of the fingerprint image.	• Non- linear distortion. • Computationally expensive.
Minutiae Based	• Extensively applicable for a wide variety of fingerprint based commercial products • Ease in acquiring the desired level of accuracy in matching.	• Difficulty while extracting minutiae from poor quality images. • Time consuming. • Additional components may be needed.
Non - minutiae (ridge feature based)	• Enhancement of the overall system performance. • Effective even for low quality fingerprint images.	• Conjunction with minutiae may be required. • Computationally complex

Table 2.3 [16] lists the advantages and disadvantages of each set of matching techniques. The choice of the method to be employed is totally dependent on the fingerprint feature level being used.

2.4 Literature Review

Vendor SDK Fingerprint Matching

The science of fingerprint recognition using a wide variety of matching techniques in entirety involves algorithms which revolve around the concepts that have been discussed in section 2.3. The real time implementation of these algorithms includes the extensive use of a commercial platform that brings together all the different components of fingerprint authentication. These products are called fingerprint matchers and are often referred to as *fingerprint recognition SDK's*. They are presently being sourced from a number of vendors worldwide. A brief review of such SDK based fingerprint verification experiments has been given below.

For Testing

NIST has conducted testing of one-to-one SDK based on fingerprint matching systems to evaluate the accuracy of one-to-one matching used in the US-VISIT program. Fingerprint matching systems from eleven vendors not used in US-VISIT were also evaluated to insure that the accuracy of the matcher tested was comparable to the most accurate available Commercial Off The Shelf matchers (COTS) products. The SDK based matching application was tested on 20 different single finger data sets of varying difficulty. The average true accept rate (TAR) at a false accept rate (FAR) of 0.01% was better than 98% for the two most accurate systems while the worst TAR at a FAR of 0.01% was greater than 94% [29].

For Performance Evaluation

COTS are often used in fingerprint image synthesis. In a certain study two such matchers were used for performance evaluation. The results indicated that COTS1 had a higher matching accuracy than COTS2 on the standard minutiae templates generated from the ground truth minutiae. The study also leads to an understanding of the performance of each matching system which were given different test datasets [29]**.**

For Experimentation

Among the many areas of fingerprint science, reconstructing fingerprint images from various classes of fingerprint features has been a significant one. Often, commercial fingerprint matchers

have been employed in such studies for experimentation. The salient feature of such a study is its ability to preserve the minutiae at specified locations in the reconstructed feature map. Experiments using a commercial fingerprint matcher suggest that the reconstructed ridge structure bears close resemblance to the parent fingerprint. It has been demonstrated that three levels of information about the parent fingerprint can be elicited from a given minutiae template: the orientation field, the fingerprint class, and the friction ridge structure [30].

2.5 Biometric System Errors

Decision Error Rates

The performance of a biometric system may be stated in terms of the decision error rates viz. "false acceptance rate" and "false rejection rate".

False Acceptance Rate (impostor acceptance)

The fraction of transactions with wrongful claims of identity (in a positive ID system) or non-identity (in a negative ID system) that are incorrectly confirmed is referred to as the false acceptance rate of the biometric system [31]. A transaction may consist of one or more wrongful attempts dependent on the decision policy. In the mathematical terminology the false acceptance rate is also referred to as the Type II error. It can be computed using the relation below

$$\text{FAR} = \frac{impostor\ scores\ exceeding\ threshold}{all\ imposter\ scores} \qquad \text{Eq (2.4)}$$

False Rejection Rate (genuine rejection)

The fraction of transactions that with truthful claims of identity (in a positive ID system) or non-identity (in a negative ID system) that are incorrectly denied is referred to as the false rejection rate of the biometric system. A transaction may contain one or more truthful attempts dependent upon the decision policy. In the mathematical terminology the false rejection rate is also referred to as the Type I error [31]. It can be computed using the relation below

$$\text{FRR} = \frac{genuine\ scores\ falling\ below\ the\ threshold}{all\ genuine\ scores} \qquad \text{Eq (2.5)}$$

The performance of a biometric system is specified in terms of false acceptance rate (FAR). The decision scheme should establish a decision boundary which minimizes the false rejection rate

(FRR) for the specified FAR. There is a tradeoff between the two types of errors. If a higher threshold is chosen, the genuine rejection rate is lower but the false accept rate may be higher, and vice versa. The given biometric application dictates the FAR and FRR requirements. For example, access to an ATM machine generally needs a small FRR, but access to a military installation requires a very small FAR. Different decision thresholds lead to different FAR and FRR.

Matching Errors

Considering the scenario of a single comparison of a submitted sample against a single enrolled template, the matching errors of a biometric authentication system may be discussed as follows:

False Match Rate (FMR)

Mistaking biometric measurements from two different persons to be from the same person results in a false match. Therefore, the false match rate is the probability that a sample will be falsely declared to match a single randomly selected "non-self" template [31]. It is sometimes also referred to as the false positive rate.

False Non-Match Rate (FNMR)

Mistaking two biometric measurements from the same person to be from two different persons results in a false non-match. Therefore, the false non-match rate is the probability that a sample will be falsely declared not to match a template of the same measure of the same user supplying the sample. It is sometimes also referred to as the false negative rate. Figure 2.12 [7] refers to the various operating points of typical biometric applications.

Non-Self

This explicitly means that the samples used for matching are genetically different. Comparison of genetically identical biometric characteristics (for instance, biometric samples of identical twins) yield different score distributions than comparison of genetically different characteristics. Consequently, such genetically similar comparisons should not be considered while computing the false match rate [31].

It is to be noted that both FMR and FNMR are functions of the system threshold. If the threshold is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if the threshold *is* raised to make the system more secure, then FNMR increases accordingly.

Equal Error Rate (EER)

The EER operating point is a computation which is generally regarded as an obvious choice to judge the quality of a fingerprint matcher. The EER is the operational point where FNMR=FMR. A lower EER value, therefore, indicates better performance.

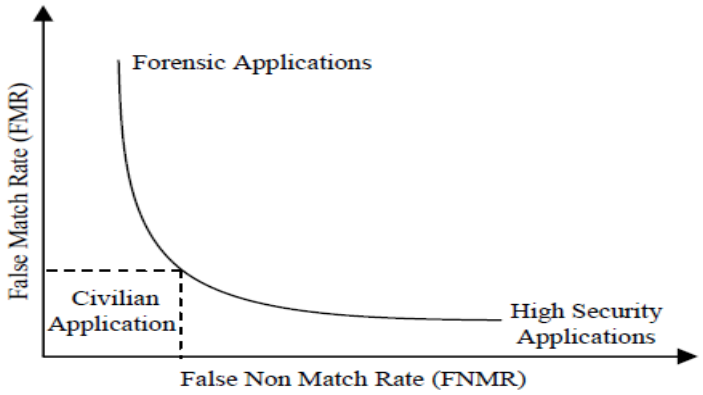


Figure 2.12 : Typical operating points of different biometric applications

Image Acquisition Errors

Failure To Enroll Rate (FTE)

The failure to enroll rate is the expected fraction of biometric transactions for which the system is unable to generate repeatable templates. This comprises of all those transactions wherein the user was unable to present the required biometric feature, the image that the user provided was insufficient in its quality at the time of enrollment, the user is unable to reliably match his/her template in attempts to confirm that the enrollment is usable [31]. The failure to enroll rate will depend on the enrollment policy.

Failure To Acquire Rate (FTA)

The failure to acquire rate is defined as the fraction of biometric transactions for which the system is unable to capture or locate an image or signal of sufficient quality [31]. This image acquisition error depends on the adjustable thresholds for image or signal quality.

2.6 Identity Claims in a Biometric System

Genuine Claim of Identity

A genuine attempt is a single good faith attempt by a user to match his or her own stored template. In a genuine biometric transaction the user truthfully claims to be him/herself thereby leading to the comparison of a sample with a truly matching template [31]. Such pairs of biometric samples generating scores higher than or equal to the threshold are inferred to as mate pairs (i.e., belonging to the same person). The distribution of scores generated from pairs of samples from the same person is called the genuine distribution.

Impostor Claim of Identity

An impostor attempt is a single trial by a user to match his/her template with a non-matching template. In an impostor biometric transaction the user falsely claims to be someone else thereby leading to the comparison of a sample with a mismatched template [31]. Such pairs of biometric samples generating scores lower than the threshold are inferred to as non-mate pairs (i.e., belonging to different persons). The distribution of scores generated from pairs of samples from different persons is called the impostor distribution. Figure 2.13 [32] is an illustration of the genuine and imposter match score distributions also indicating the FMR and FNMR curves.

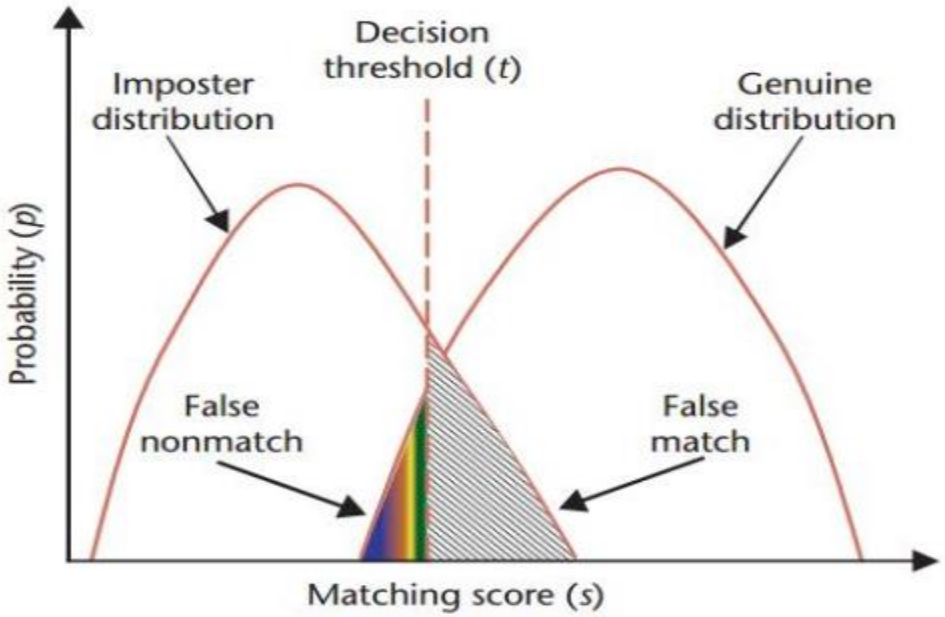


Figure 2.13: Representation of a typical genuine and impostor score distribution

2.7 Receiver Operating Characteristic Curves

A receiver operating characteristic (ROC) curve is a plot of genuine acceptance rate (1-FRR) against false acceptance rate for all possible system operating points (i.e., matching threshold) and measures the overall performance of the system. Each point on the curve corresponds to a particular decision threshold. In the ideal case, both the error rates, i.e., FAR and FRR should be zero and the genuine distribution and imposter distribution should be disjoint. In such a case, the "ideal" ROC curve is a step function at the zero false acceptance rate [13]. On the other extreme, if the genuine and imposter distributions are exactly the same, then the ROC is a line segment with a slope of 45 degrees with an end point at zero false acceptance rate. In practice, the ROC curve behaves in between these two extremes. Figure 2.14 [13] is an illustration of sample ROC Curves.

ROC (T) = (FAR (T), GAR (T)) where T is the threshold Eq (2.6)

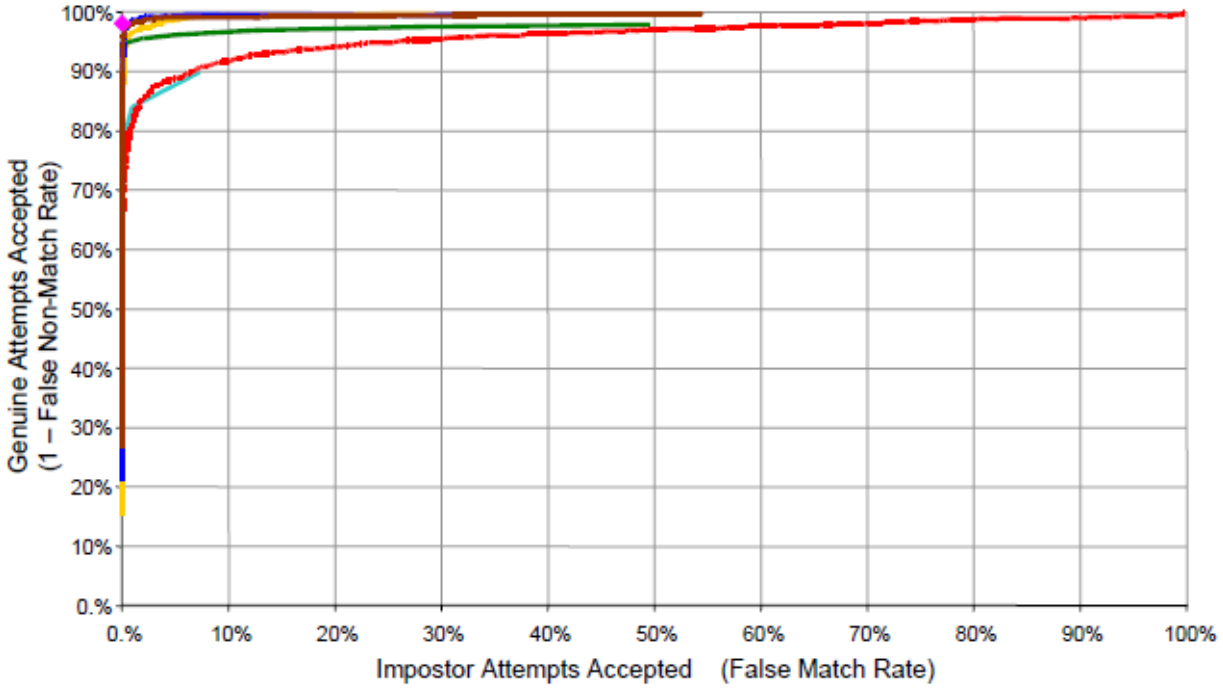


Figure 2.14 : Sample ROC Curves

An ROC curve demonstrates several things [32] which have been listed below:

- It shows the tradeoff between sensitivity and specificity (any increase in sensitivity will be accompanied by a decrease in specificity).
- The closer the curve follows the left-hand border and then the top border of the ROC space, the more accurate the test.
- The closer the curve comes to the 45-degree diagonal of the ROC space, the less accurate the test.
- The slope of the tangent line at a cut point gives the likelihood ratio (LR) for that value of the test.
- The area under the curve (AUC) is a measure of performance accuracy. An area of 1 represents a perfect test while an area ≤ 0.5 represents a worthless test.

2.8 Information- Theoretic Divergence Measures

In probability theory, a f-divergence is a function $D_f(\mathrm{M} \,||\, \mathrm{N})$ that measures the difference between two probability distributions M and N. It helps the intuition to think of the divergence as an average, weighted by the function *f*, of the odds ratio given by M and N. The Kullback Leibler Divergence is one such measure that belongs to the family of *f*-divergences [38]. It is also called as the discrimination information**,** information divergence, relative entropy, KLIC or KL divergence.

Kullback- Leibler Divergence

The Kullback Leibler Divergence or KLD, as we call it in this study, is not symmetric in M and N. In applications, M typically represents the "true" distribution of data, observations, or a precisely calculated theoretical distribution, while N typically represents a theory, model, description, or approximation of M. For two discrete probability distributions M and N the Kullback Leibler Divergence from N to M is defined by the following mathematical relation

$$D_{KL}\,(M \parallel N) = \sum_i M(i) \log \frac{M(i)}{N(i)} \qquad \text{Eq (2.7)}$$

In words, it is the expectation of the logarithmic difference between the probabilities M and N, where the expectation is taken using the probabilities of M [38]. The Kullback–Leibler divergence is defined only if N (i) =0 which implies M (i) =0, for all i (absolute continuity).

Whenever M (i) is zero the contribution of the i-th term is interpreted as zero because $\lim_{x\to 0} x\log(x) = 0$.

Properties of KLD

- A very essential property of this divergence will be that the K-L divergence is always non-negative, i.e.

$$D_{KL}(M \parallel N) \geq 0 \qquad \text{Eq (2.8)}$$

- The equality is reached when both distribution coincides, i.e. M (x) = N (x) for all values of x.
- The Kullback Leibler Divergence is not symmetrical and does not satisfy the triangular inequality [38]. So, the KLD is not really a metric, but a premetric. Hence, it specifies a topology.

$$\text{D}(M \parallel N) \neq \text{D}(N \parallel M) \qquad \text{Eq (2.9)}$$

To address the symmetry problem, the Jeffrey's Divergence [39] which is another form of f-divergence can be employed which is obtained by "averaging" two Kullback-Leibler distances. The J - divergence equals the average of the two possible Kullback-Leibler distances between the two probability distributions and hence results in a symmetric version of the KLD. Assuming the component Kullback-Leibler distances exist, it may be mathematically expressed as

$$\text{J}(M, N) = \frac{D(M \parallel N) + D(N \parallel M)}{2} \qquad \text{Eq (2.10)}$$

Relation between the Kullback Leibler Divergence and Jeffrey's Divergence

The Kullback Leibler Divergence may be expressed as half of its symmetric version which is Jeffrey's Divergence.

$$K(\text{M} \parallel \text{N}) = \frac{1}{2}\,\text{J}(\text{M} \parallel \text{N}) \qquad \text{Eq (2.11)}$$

Jensen- Shannon Divergence

The Jensen Shannon Divergence or JSD, as we call it in our study, is the smoothed version of the Kullback Leibler Divergence. It is also called as the information radius or total information to the average [37]. The square root of the Jensen Shannon Divergence is known as the Jensen Shannon distance which serves as the information theoretic measure in this study. Mathematically, the Jensen Shannon Divergence is given as

$$\text{JSD}\ (\text{M} \parallel \text{N}) = \frac{1}{2} D(M \parallel P) + \frac{1}{2} D(N \parallel P) \qquad \text{Eq (2.12)}$$

$$\text{where P} = \frac{1}{2}(M + N) \qquad \text{Eq (2.13)}$$

Properties of Jensen Shannon Divergence

- JSD is symmetric and it is always a finite value.
- The Jensen–Shannon divergence is bounded by 1 for two probability distributions, given that the base 2 algorithm is being used.

$$0 \leq \text{JSD}\ (\text{M} \parallel \text{N}) \leq 1 \qquad \text{Eq (2.14)}$$

- The Jensen Shannon Divergence when computed with respect to log base e has the upper bound as ln(2)

$$0 \leq \text{JSD}\ (\text{M} \parallel \text{N}) \leq \ln(2) \qquad \text{Eq (2.15)}$$

- The Jensen–Shannon divergence gives the mutual information between a random variable X associated to a distributive mixture between M and N and a binary indicator variable Y that is used to shift between M and N to produce the mixture [37].

$$I(X; Y) = \text{JSD}\ (\text{M} \parallel \text{N}) \qquad \text{Eq (2.16)}$$

- The closer the distributions lesser would be the value of JSD.

CHAPTER 3 - EXPERIMENTAL DATA

3.1 Data Acquisition

Over the past few years, West Virginia University (WVU) in collaboration with the Federal Bureau of Investigation (FBI) has been involved in a number of large scale multimodal biometric collections. The West Virginia University's BIOCOP 2012 is one such assortment that has been employed for analysis in our study. The fingerprint subset of this collection consists of images that have been acquired from 1200 participants belonging to various age and ethnic groups.

Table 3.1 : Description of the fingerprint scanners employed in WVU BIOCOP 2012

Scanner	**Properties**	**Enrollment**	**No: of images captured**
CrossMatch Verifier 300LC	It is an optical USB 2.0 fingerprint scanner. The scanner is an improved version of Verifier 300 LC with USB 2.0 support, faster frame rate and an infrared filter to improve ambient light rejection.	Captures the image of only one finger in a single trial of enrollment.	34911
CrossMatch Verifier 310 LC	It is a FIPS 201 approved dual fingerprint capture device. Enhanced accuracy, reduced time for enrollment are the major advantages of this scanner.	Can be employed to capture the image of two or more fingers or varied combinations of multiple fingers in a single trial of enrollment.	38368
Upek Eikon Touch 700	It is a FIPS 201 certified capacitive USB 2.0 fingerprint scanner.	Captures the image of only one finger in a single trial of enrollment.	34810

Using the scanners listed below fingerprint images were captured of all the ten fingers. However, this study is confined to the analysis of genuine and impostor score distributions for the right

thumb and right index fingers. The specifications of these images as captured by the various scanners has been listed in Table 3.2.

Table 3.2 : Specifications of the fingerprint images in WVU BIOCOP 2012

Specification	CrossMatch Verifier 300 LC	CrossMatch Verifier 310	Upek Eikon Touch 700
No: of Images	Right Thumb - 3491 Right Index- 3491	Right Index- 3480 (segmented)	Right Thumb - 3481 Right Index- 3481
Image Format	Bitmap (.bmp)	Bitmap (.bmp)	Bitmap (.bmp)
Size	586 kb	586 kb	91 kb
Bit depth	8	8	8
Color	Grayscale	Grayscale	Grayscale
Original resolution (in pixels)	800 × 750	800 × 750	256 × 360
Modified resolution (while verification)	500 × 500	500 × 500	500 500

3.2 Demographic Distribution of the Fingerprint Data

While one section of this study revolves around the genuine and impostor score distributions of the total fingerprints captured by each of the scanners, the crux of this study is totally oriented towards analyzing the fingerprints based on the demographic feature they belong to. The three demographic features that this study aims to examine are Age, Gender and Ethnicity. Table 3.3 shows the demographic distribution of the BIOCOP 2012 fingerprint dataset.

Table 3.3 : Demographic distribution of the BIOCOP 2012 fingerprint dataset

Demographic	No: of Participants	Reason for variations in matching score
Age	Age 18-19 :138 Age 20-30: 886 Age 31-49: 113 Age 50-70: 59 Age 71-79: 4	Decreased skin firmness Loose and dry aging skin resulting in poor quality
Gender	Male- 705 Female- 495	Difference in pattern of the ridge structure Varying ridge breadth and minutaie count
Ethnicity	Caucasian - 727 Asians - 105 Asian Indians - 137 African Americans - 76 Middle Eastern - 61 Hispanics - 56 Africans - 20 Other Pacific Islanders - 4 Others - 14	Difference in ridge structure

The main goal of analyzing the effect of data stratification takes into account the key fact that fingerprint images acquired from different subjects present different information to the system which results in a significant variation in matching score. The reason for these variations in the fingerprints has been described in Table 3.3.

CHAPTER 4 - METHODOLOGY

4.1 Experimental Set Up

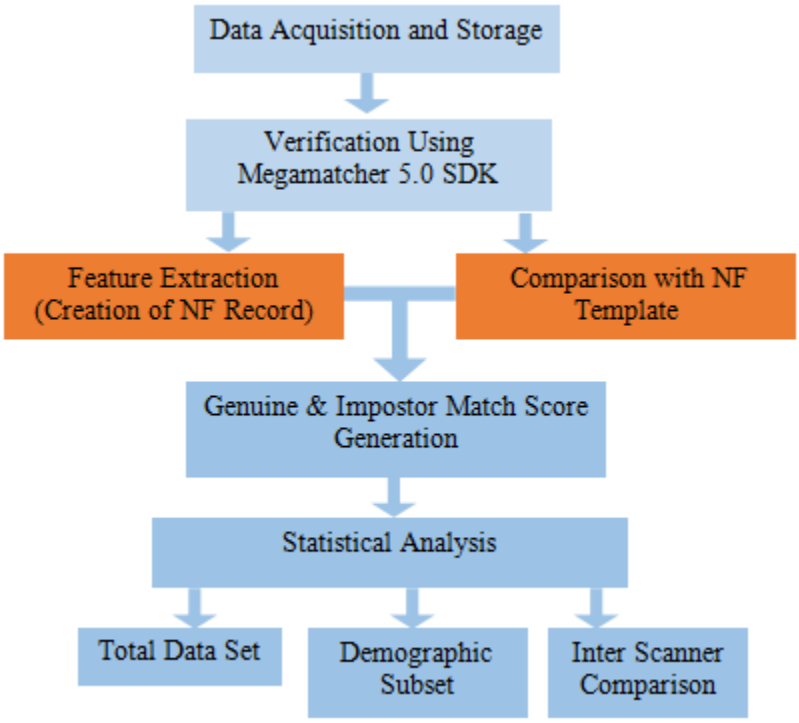


Figure 4.1: Algorithmic view of the overall experimental set up

Figure 4.1 gives us an illustrative view of the matching and analysis algorithm that has been implemented in this study. MegaMatcher 5.0 SDK was installed and matching functions were employed using a JAVA based platform in an Eclipse Integrated Development Environment (IDE). Post-matching the genuine and impostor scores were stored in Comma Separated Variable (CSV) files and were used for statistical analysis using MATLAB.

4.2 Matching System

4.2.1 MegaMatcher SDK

MegaMatcher technology [41] is designed for large-scale AFIS (Automatic Fingerprint Identification System) and multi-biometric systems developers. The technology ensures high reliability and speed of biometric identification even when using large databases. MegaMatcher

is available as a software development kit that allows development of large-scale single- or multi-biometric fingerprint, face, voice, iris and palm print identification products for Microsoft Windows, Linux, Mac OS X, iOS and Android platforms.

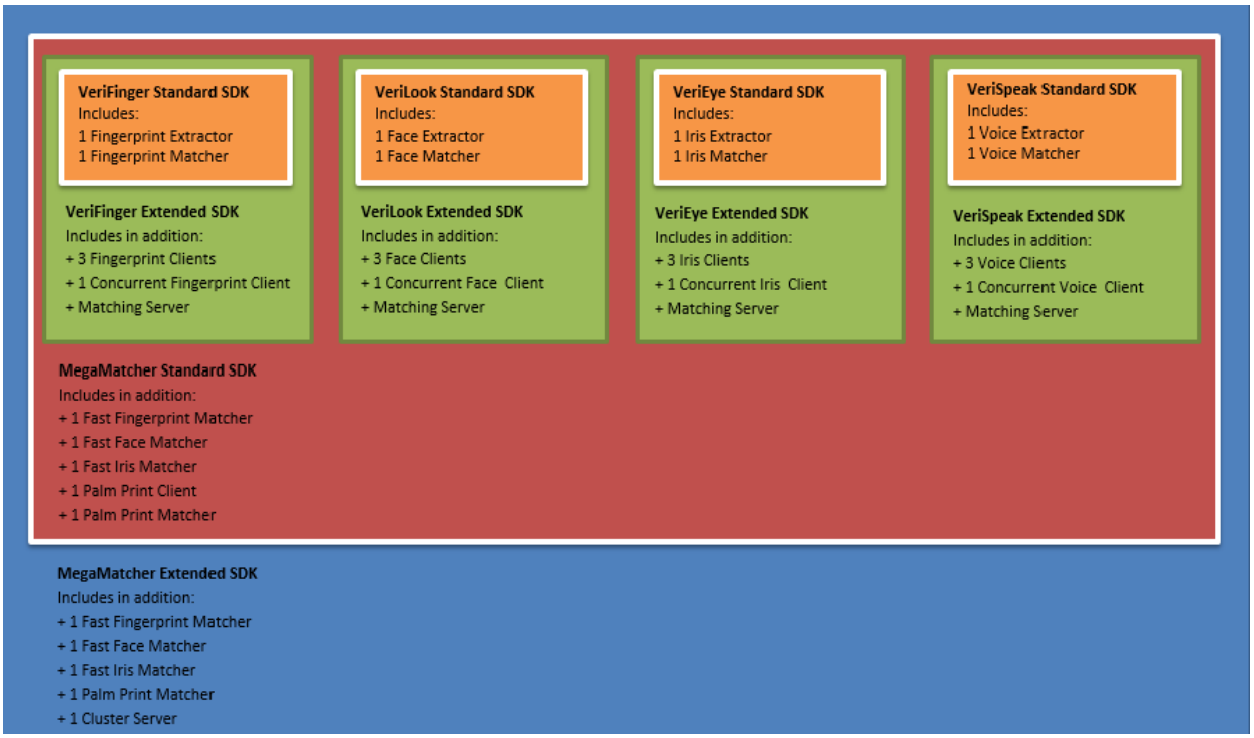


Figure 4.2 : Schema of Megamatcher SDK

Features of MegaMatcher SDK

- It also endures high productivity and efficiency are supported by a fused algorithm that contains fingerprint, face, iris, palmprint and voice recognition engines. Integrators can use the fused algorithm for better results or any of these engines separately.
- The fault-tolerant scalable cluster software [41] allows to perform fast parallel matching, processes high number of requests and handles databases with practically unlimited size.
- MegaMatcher includes server software for local multi-biometrical systems and cluster software for large-scale multibiometrical products development. .NET and Java components for rapid development of client side software are also included with MegaMatcher.
- To ensure system compatibility with other software, WSQ library is included, as well as modules for conversion between MegaMatcher template and other biometrical standards.

4.2.2 VERIFINGER 7.0

VeriFinger [41] is a fingerprint authentication algorithm intended for biometric systems developers and integrators. The technology assures system performance with fast, reliable fingerprint matching in one-to-one and one-to-many modes. VeriFinger fingerprint engine performance and reliability has been recognized by NIST as MINEX compliant.

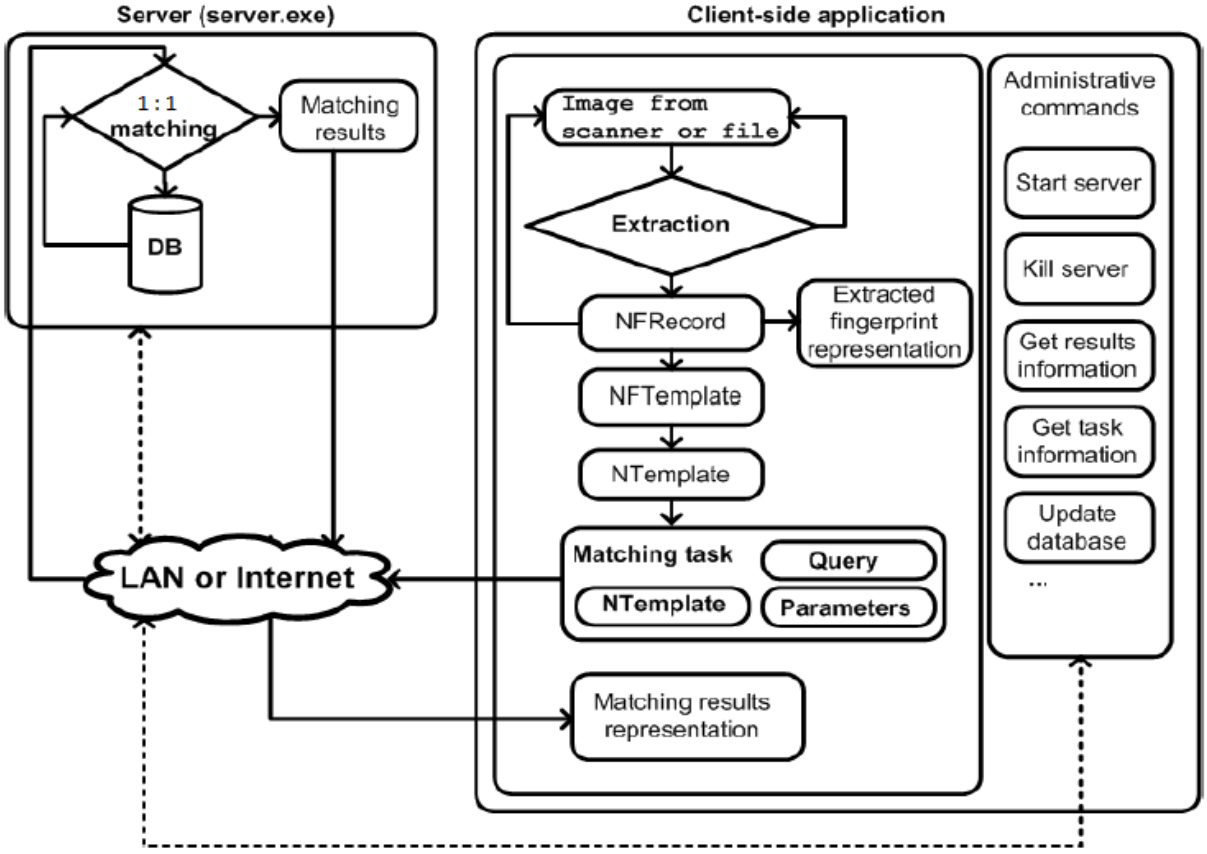


Figure 4.3 : Client-Server Architecture of VeriFinger

4.2.2.1 SDK Fingerprint Components

Fingerprint Matcher

The Fingerprint Matcher [42] performs fingerprint template matching in one-to-one (verification) and one-to-many (identification) modes. Also the Fingerprint Matcher component includes fused matching algorithm that allows to increase template matching reliability by:

- Matching templates that contain 2 or more fingerprint records (note that the Fingerprint Segmenter and the Fingerprint Client components are required to perform template extraction from images that contain more than one fingerprint)
- Matching templates that contain fingerprint, face, voiceprint and/or iris records (note that matching faces, irises and voiceprints requires to purchase Face Matcher, Iris Matcher and Voice Matcher components correspondingly).

The Fingerprint Matcher component matches 40,000 fingerprints per second and is designed to be used in desktop or mobile biometric systems, which run on PCs or laptops with at least Intel Core 2 Q9400 (2.67 GHz) processor.

Fingerprint Client

The Fingerprint Client [42] component is a combination of the Fingerprint BSS (Biometric Standard Support), Fingerprint Segmenter and Fingerprint WSQ (Wavelet Scalar Quantization) components. It is intended for the systems that need to support most or all functionality of the mentioned components on the same PC. The Fingerprint Client extracts a single fingerprint template in 0.6 seconds. The specified performance requires a PC or laptop with at least Intel Core 2 Q9400 (2.67 GHz) processor.

Fingerprint Segmenter

The Fingerprint Segmenter [42] components separates fingerprints if an image contains more than one fingerprint. This component also enables the Fingerprint Extractor component to process fingerprints from scanned ten print card or image captured using scanners that allow to scan two or more fingers at a time.

Table 4.1 : Fingerprint Engine Specifications

MegaMatcher 5.0 Fingerprint Engine Specifications (PC Based Platform)		
Template Extraction Components	Fingerprint Extractor	Fingerprint Client
Template Extraction time (in seconds)	1.34	0.6
Template Matching Component	Fingerprint Matcher	
Template Matching Speed (fingerprints per second)	40,000	
Single fingerprint record size in a template (in bytes)	700- 6,000 (configurable)	

4.2.2.2 Biometric Functionalities

MegaMatcher 5.0 is comprised of a number of tutorials each of which includes a small program that demonstrates specific functionality [41] of Neurotechnology libraries. The section below would give a brief description about the biometric libraries used in this study.

Table 4.2 : Biometric Function Files

Biometrics	**Description**
EnrollFingerFromImage	Demonstrates how to extract features from fingerprint image and enroll to database.
EvaluateFingerQuality	Demonstrates fingerprint image quality evaluation.
SegmentFingers	Demonstrates how to use fingerprint features segmentation.
ShowTemplateContent	Demonstrates how to retrieve information about a template.
VerifyFinger	Demonstrates how to use 1:1 fingerprint matching.

4.2.2.3 Task Specific Attributes

Table 4.3 : Task Specific Attributes used for Matching, Segmentation and Minutiae extraction

For Matching	
NBiometricOperation	Defines the biometric operation to be performed in the task.
NBiometricStatus	Returns the status of the biometric task.
NBiometricTask	Used to define a new biometric task.
NFinger	Provides methods for the biometric engine to deal with fingerprint templates.
NMatchingSpeed	Defines the matching speed to be low, medium or high.
NSubject	Represents a person and contains the biometric information related to that person.
NBiometricClient	Represents a biometric client which provides functions for biometric data capture and its transfer through various connections.

NImage	Provides functionality for managing images.
Segmentation and Quality Score generation	
NF Position	Specifies finger position.
NFIQ Quality	Specifies the quality of a fingerprint image
For Minutiae Extraction	
NFCore	Represents a core in the fingerprint image.
NFDelta	Represents a delta in a fingerprint image.
NFDoubleCore	Represents a double core in a fingerprint image.
NFMinutia	Represents a minutia point in a fingerprint image.
NFMinutiaFormat	Specifies the format of the minutiae in the fingerprint image.
NFRecord	Provides the functionality for packing, unpacking and editing Neurotechnology finger records.

Table 4.3 [41] lists out the various task specific attributes that have been used in the course of experimentation in this study.

4.3 Matching of fingerprints

The templates can be compared with the aim to check if they belong to the same person. The result of such comparison is the similarity score. The higher score suggests the higher probability that features collections are obtained from the same person. This score is mapped to yes/no answer with the matching threshold [41]. Using the NMatcher component of the matching system, each finger from the query template is matched with the database template in the following way:

- If query of finger position is unknown it is matched with all fingers from database template and the match with maximal score is selected.
- If query of finger position is known it is matched with all fingers from database template that have the same finger position or have unknown finger position and the match with maximal score is selected.

Table 4.4 : Matching threshold for various FAR

FAR (false acceptance rate)	Matching threshold (score)
100 %	0
10 %	12
1 %	24
0.1 %	36
0.01 %	48
0.001 %	60
0.0001 %	72
0.00001 %	84
0.000001 %	96

Table 4.5 gives the set of FAR's for various levels of thresholding as stated by Megamatcher 5.0 SDK which could also be determined using the relation

$$\text{Threshold} = -12 * \log10\,(\text{FAR}) \qquad \text{Eq (4.1)}$$

where FAR is NOT percentage value (e.g. 0.1% FAR is 0.001).

The returned score should be interpreted as the probability that the false acceptance happened. The score is retuned by using such algorithm – if the matching score is equal or higher than the set matching threshold, then it means that modality has matched and score is returned. If the score is lower than the matching threshold, then "0" value is returned and it means that the modality did not match. There is no maximum value for the matching score which implies that bigger the score lower is the probability that false acceptance has happened.

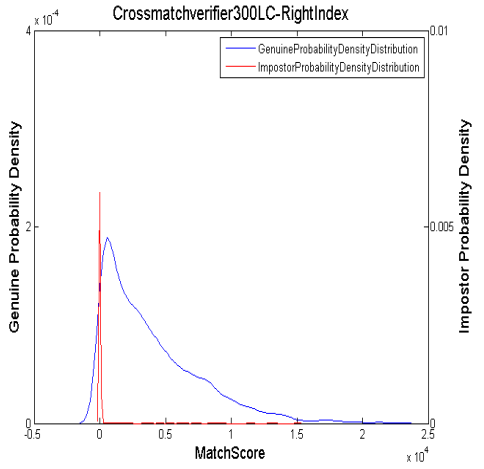
CHAPTER 5 - EXPERIMENTAL RESULTS

5.1 Fingerprint Image Match Score Analysis

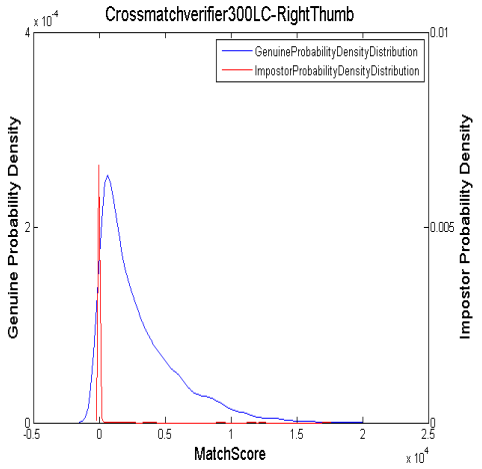
VeriFinger component contained in the MegaMatcher software SDK has been used as the matching platform. The fingerprint feature extractor component extracts a template of the original fingerprint image which serves as the probe image. The fingerprint matcher component then matches this probe image against the set of images in the gallery. In order to generate the genuine scores, a probe image of a subject is matched against all other fingerprint images of the same subject which forms the gallery. However, in order to generate the imposter scores the probe image of a subject is matched against that particular set of images of all the subjects in the dataset which forms the gallery in this case. In both the cases, the probe image has not been included in the gallery. For both the experiments the horizontal and vertical resolution of the fingerprint images has been set to 500 pixels per inch (ppi) in order to avoid the error of 'invalid sample resolution' which occurred while trying to perform experiments with the original resolution of the images. Also, while experimentation the matching speed was maintained at a low level and the matching threshold was kept zero in order to allow maximum possible matches. Each experiment resulted in a genuine or imposter match score list obtained in the form of comma separated variable (csv) files which were then imported into Matlab to generate the imposter and genuine score distributions. Table 5.1 shows the maximum and minimum values of the genuine and imposter scores generated by the matcher for each of the sensors.

Table 5.1: Range of match scores of the WVU 2012 BioCOP fingerprint dataset

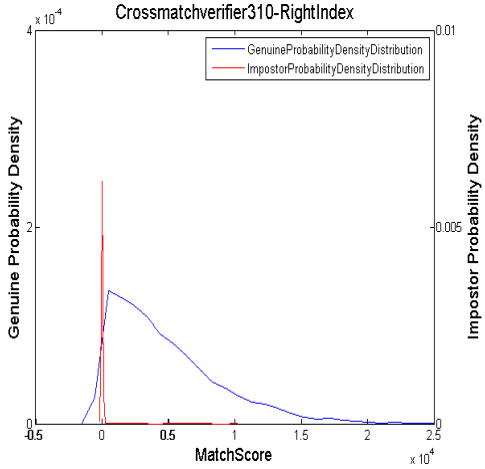
Sensor	Finger	Genuine Maximum score	Genuine Minimum Score	Imposter Maximum Score	Imposter Minimum Score
CrossMatch Verifier 300LC	Right Thumb	18492	0	17391	0
	Right Index	22179	0	15140	0
CrossMatch Verifier 310	Right Index	94154	0	10017	0
Upek Eikon Touch 700	Right Thumb	23760	0	10089	0
	Right Index	31277	0	9470	0



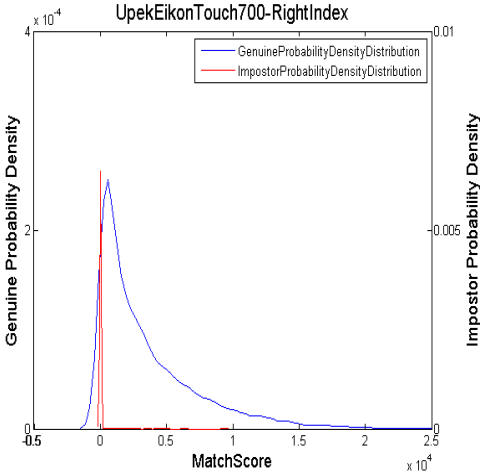
(a)



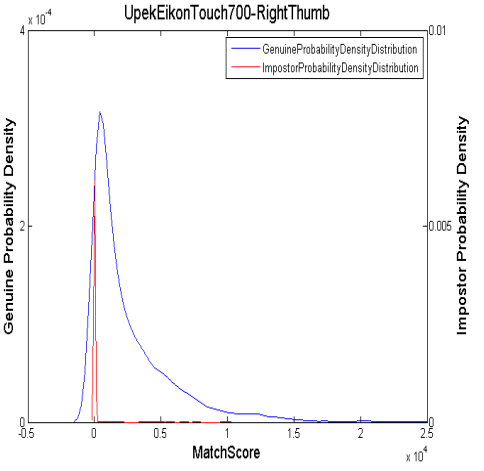
(b)



(c)



(d)



(e)

(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

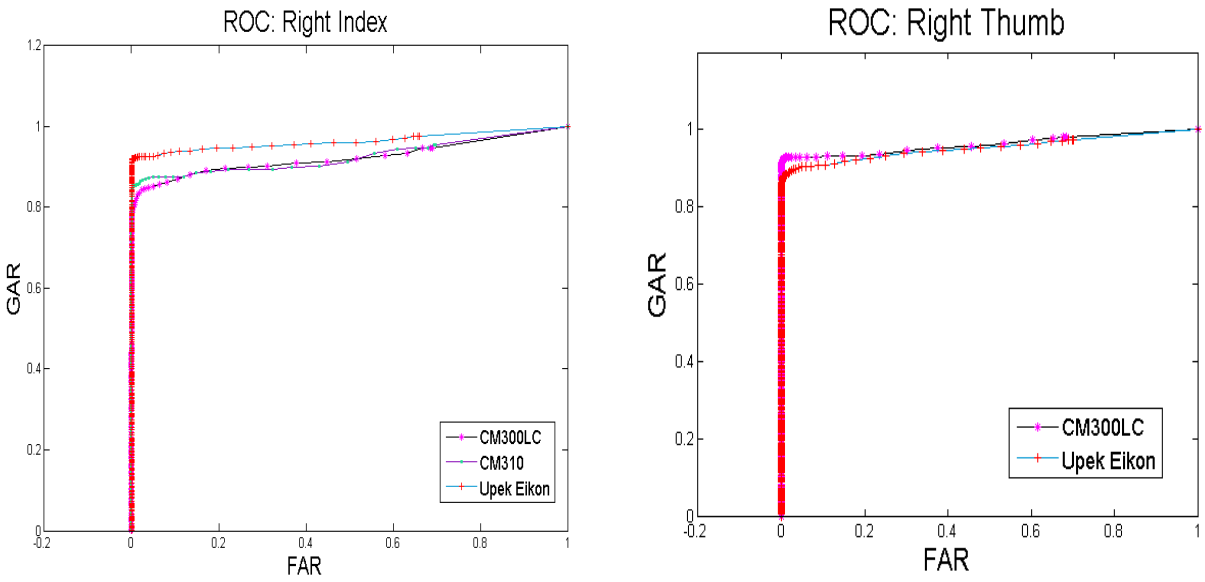
Figure 5.1 : Genuine and imposter score distributions for thumb and index fingerprint images

5.1.1 ROC Curves of the WVU 2012 BioCOP Fingerprint Dataset

ROC curves were plotted in order to better understand the performance of the sensors employed. These performance curves can be seen in Figure 5.2. The area under the curve values (AUC) for these curves have been tabulated in Table 5.2. From these values it can be understood that the scanners CrossMatch Verifier 300LC and Upek Eikon Touch 700 have been on the same level in terms of match performance.

Table 5.2 : Summary of AUC values of the WVU 2012 BioCOP fingerprint dataset

Finger	Scanner	Area under Curve
Right Thumb	Cross Match Verifier 300LC	0.9535
	Upek Eikon Touch 700	0.9381
Right Index	Cross Match Verifier 300LC	0.9035
	Cross Match Verifier 310	0.8856
	Upek Eikon Touch 700	0.9651



(a) (b)

Figure 5.2 : ROC Curves for WVU 2012 BioCOP Fingerprint Dataset

(a) Right Index (b) Right Thumb

5.1.2 Divergence Measure Distributions

The Kullback Leibler and Jensen Shannon Divergence measures have been listed in Table 5.3.

From these values it can be inferred that the range of the KLD and JSD scores varies between 0.3928 and 0.0571. As discussed in Section 2.5, the more a divergence score is closer to zero the more ideal it would be. However, with reference to the divergence measure properties, this range of variation in divergence is not very significant to state that a particular sensor exhibits a change in its match performance as a result of data stratification.

Table 5.3 : KLD and JSD Scores for the Right Index and Right Thumb fingerprint images

Scanner - Finger	Reference Scanner - Finger	KLD Genuine	KLD Imposter	JSD Genuine	JSD Imposter	JD Genuine	JD Imposter
Upek Eikon Touch-Right Thumb	Cross Match Verifier 300LC - Right Thumb	**0.3928**	0.5516	0.4839	0.2332	0.7855	1.1032
Cross Match Verifier 310 - Right Index	Cross Match Verifier 300LC - Right Index	0.2398	0.1153	0.5211	**0.0571**	0.4795	0.2306
Upek Eikon Touch-Right Index	Cross Match Verifier 300LC - Right Index	0.2786	0.283	0.5076	0.1366	0.5572	0.5661

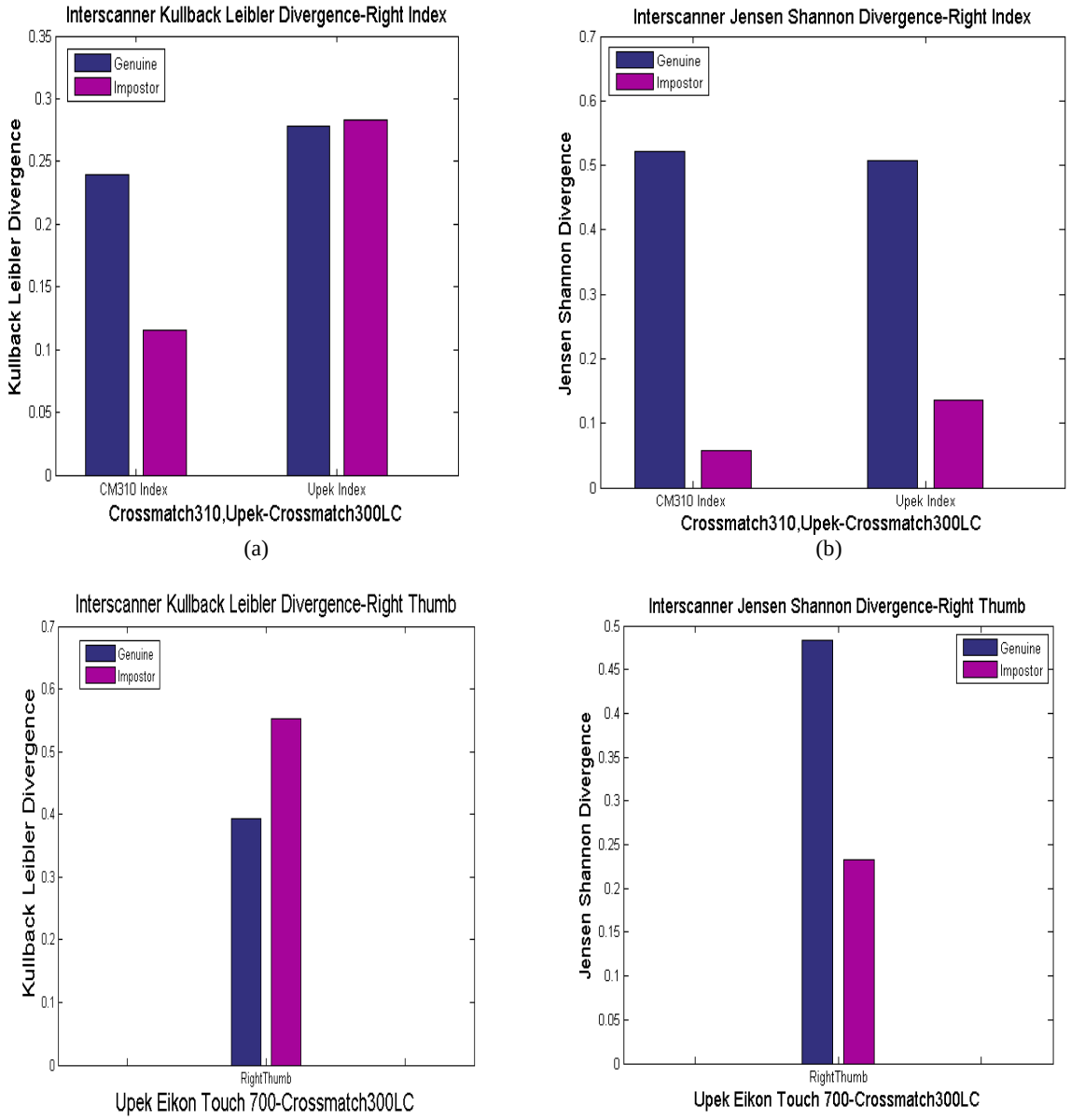


Figure 5.3 : KLD and JSD Distributions of Right Index and Right Thumb Fingerprint Images

(a) Bar graph of KLD scores of right index images. (b) Bar graph of JSD scores of right index images. (c) Bar graph of KLD scores of right thumb images. (d) Bar graph of JSD scores of right thumb images.

5.2 Demographic Based Distributions

The major objective this study is oriented towards is understanding the influence of the demographic strata on the match performance of each stratum and in comparison with the total fingerprint dataset. In order to accomplish this task the test dataset under study has been divided into three demographic strata viz. gender, age and ethnicity. Sections 5.2.1, 5.2.2, 5.2.3 describe the experimental results that have been obtained in each of these sections respectively.

5.2.1 Gender Based Test Results

The fingerprint dataset of the WVU 2012 BioCOP consists of 705 males and 495 females belonging to different age and ethnic groups. The sections below focus on the difference in match performance between the male and female strata with reference to the ROC curves and the statistical divergence measures.

5.2.1.1 Match Score Analysis

Table 5.4 : Maximum and Minimum match scores of the gender strata

Demographic	Scanner	Finger	Genuine		Imposter	
			Maximum	Minimum	Maximum	Minimum
Male	Cross Match Verifier 300LC	Right Thumb	16558	0	9325	0
		Right Index	21819	0	13299	0
	Cross Match Verifier 310LC	Right Index	94154	0	6396	0
	Upek Eikon Touch 700	Right Thumb	23760	0	9820	0
		Right Index	31277	0	998	0
Female	Cross Match Verifier 300LC	Right Thumb	18492	0	17391	0
		Right Index	22179	0	15140	0
	Cross Match Verifier 310LC	Right Index	24724	0	10017	0
	Upek Eikon Touch	Right Thumb	20938	0	10089	0
		Right Index	25701	0	3975	0

Figure 5.4 and Figure 5.5 show the match score distributions of each scanners for the gender stratum under study. It needs to be mentioned that the overlap area of the genuine and impostor

distribution is very small indicating a very less error region. These results hold good for all the distributions. Hence, it can be seen that there is not much of variation in the match score distributions of the gender strata with respect to the total dataset which is again a sign of minimal data stratification effect. Refer to Section A of the appendix for the individual genuine and imposter score distributions.

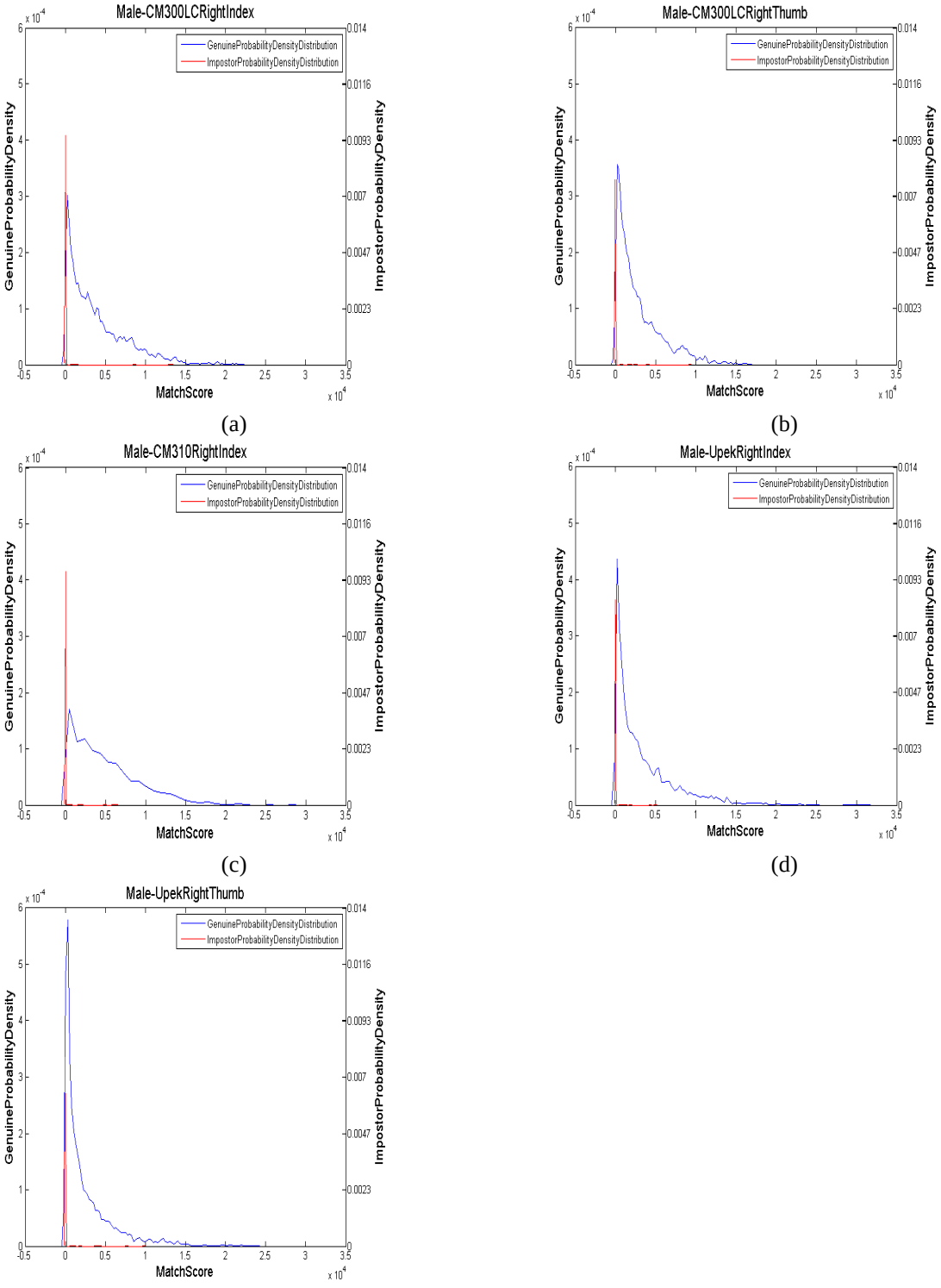
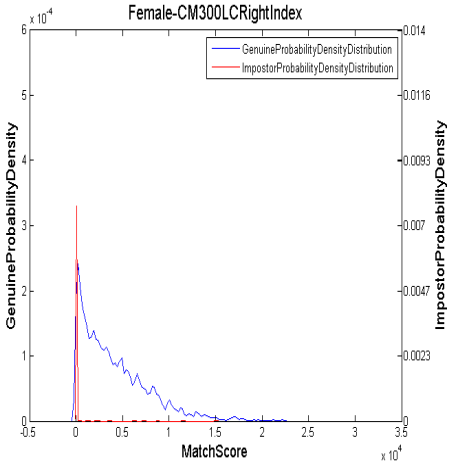
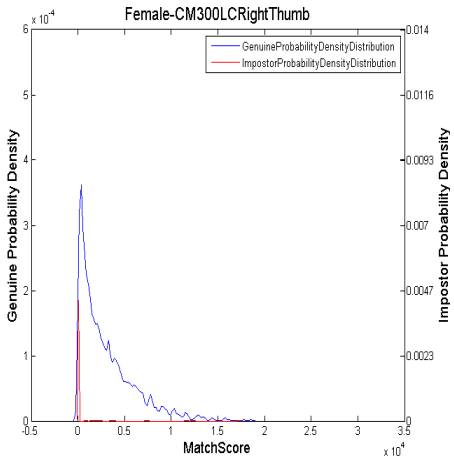


Figure 5.4 : Genuine and imposter match score distributions for male fingerprint images.

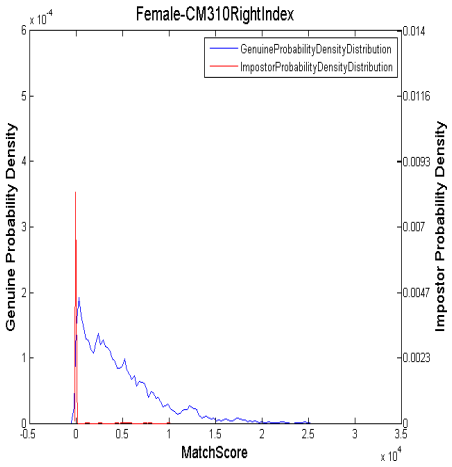
(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb



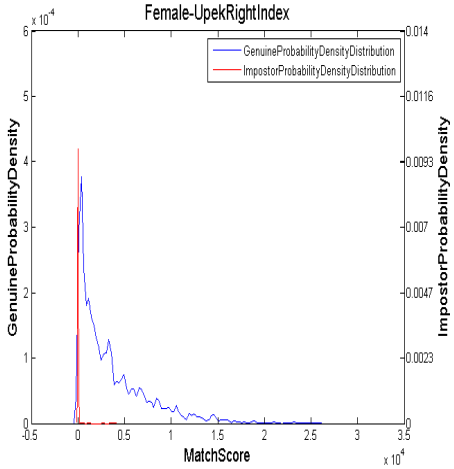
(a)



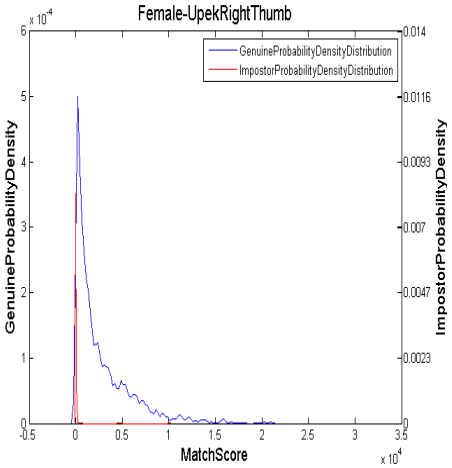
(b)



(c)



(d)



(e)

Figure 5.5 : Genuine and imposter match score distributions for female fingerprint images.

(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb

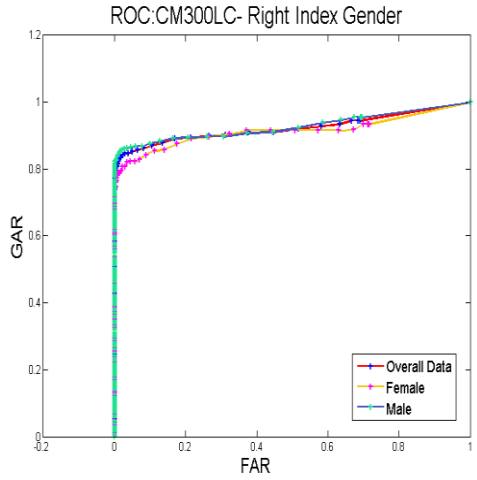
5.2.1.2 Receiver Operating Characteristic Curves

Table 5.5 lists the AUC Values obtained from the receiver operating characteristic curves. It can be seen that the gender strata has been quite close in its performance to the total data set. This signifies that a majority of the data set has been quite invariant in terms of the match performance under the influence of data stratification. However, it can also be noticed that the gender stratum has been consistent in its match performance throughout.

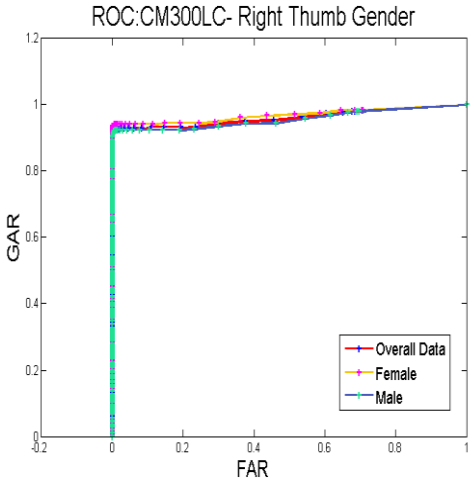
Table 5.5 : Gender Based AUC Values

Scanner	Finger	Gender	Area Under Curve
Cross Match Verifier 300LC	Right Thumb	Main	0.9535
		Male	0.9457
		Female	0.968
	Right Index	Main	0.9197
		Male	0.9244
		Female	0.9088
Cross Match Verifier 310	Right Index	Main	0.8656
		Male	0.8261
		Female	0.9257
Upek Eikon Touch 700	Right Thumb	Main	0.9374
		Male	0.9263
		Female	0.9616
	Right Index	Main	0.9640
		Male	0.9639
		Female	0.9600

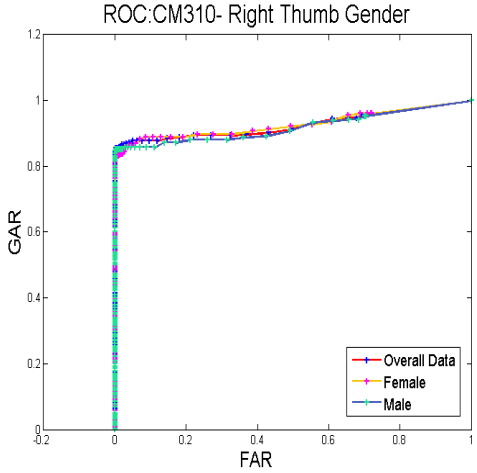
Using the minutiae extraction feature of the VeriFinger component the count of minutiae has been generated for each set of male and female fingerprint images acquired from all the scanners. It has been observed that the average count of extracted minutia is comparatively more for the fingerprint images obtained using CrossMatch Verifier 300LC for both male and female strata. This can be understood from the boxplots in Figure 5.7. The center line of the box plot indicates the median of the minutiae count generated which is seen to be higher in the case of CrossMatch Verifier 300LC in comparison with CrossMatch Verifier 310 and Upek Eikon Touch 700. Thus, the images acquired using CrossMatch verifier 300LC show a higher rate of success from the point of feature extraction.



(a)

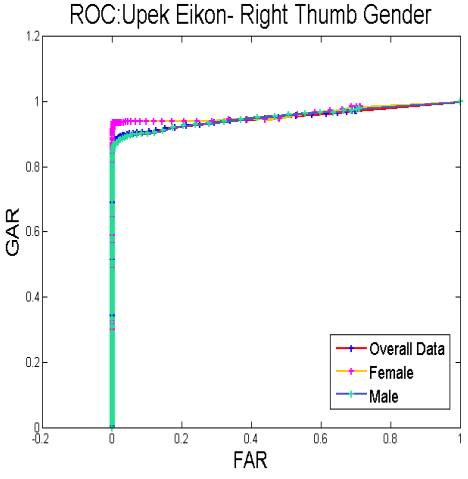


(b)



(c)

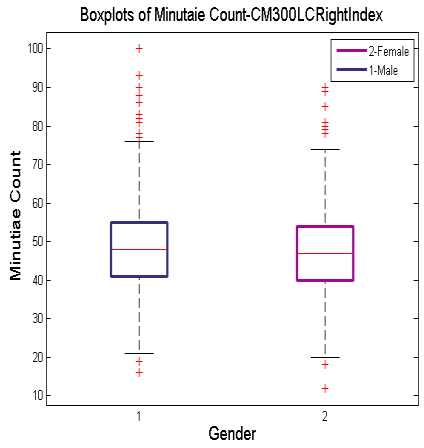
(d)



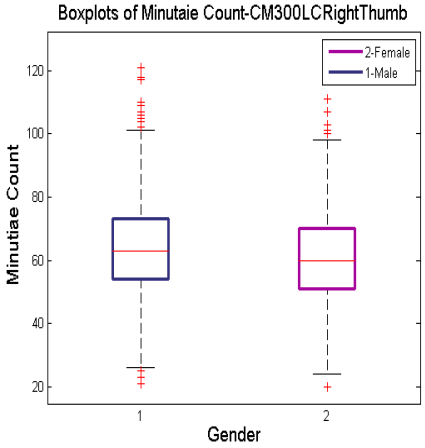
(e)

Figure 5.6 : Gender Based ROC Curves

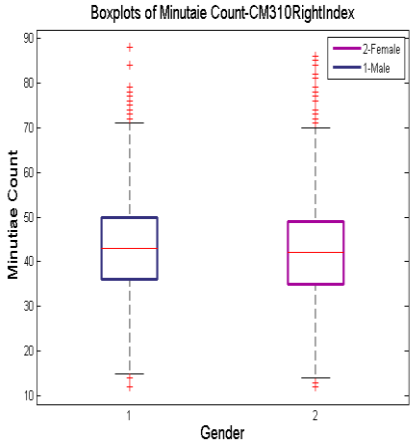
(a) CrossMatch 300LC right index .(b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index .(e) Upek Eikon Touch right thumb



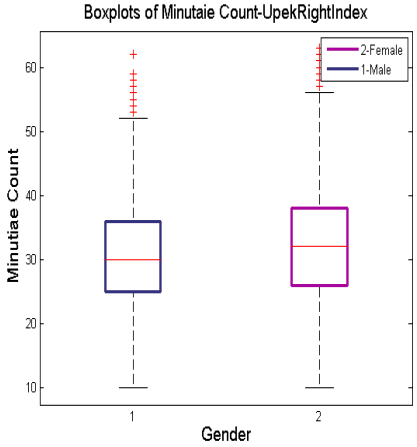
(a)



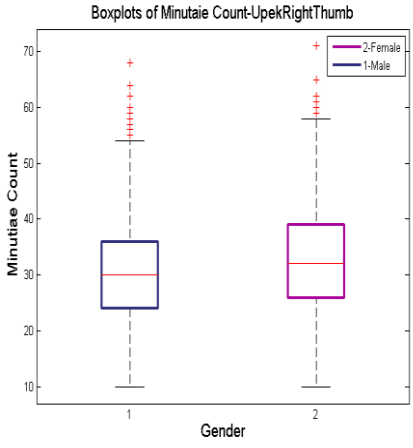
(b)



(c)



(d)



(e)

Figure 5.7 : Gender Based Minutiae Count Representation

(a) Boxplots of minutiae of right index images from Crossmatch Verifier 300LC. (b) Boxplots of minutiae of right thumb images from Crossmatch Verifier 300LC. (c) Boxplots of minutiae of right index

images from Crossmatch Verifier 310. (d) Boxplots of minutiae of right index images from Upek Eikon Touch 700. (e) Boxplots of minutiae of right thumb images from Upek Eikon Touch 700.

5.2.1.3 Divergence Measure Distributions

Table 5.6 lists the divergence distance measures between the male and female stratum. Both the KLD and JSD distributions validate the conclusions arrived at in the section 5.2.1.2. It can be seen that the maximum divergence score obtained is 0.577 while the minimum score is 0.013. Again, this variation in the divergence score values does not present a significant separation between the match score distributions. Hence, it can be concluded that the match performance of each of the gender demographic strata has not been influenced by the effect of data stratification. Refer to figure 5.8 for the bar graphs of the KLD and JSD scores obtained for the male and female stratum.

Table 5.6 : Gender Based KLD and JSD Values

Sensor Name	Gender	Finger	KLD Genuine	KLD Imposter	JSD Genuine	JSD Imposter	JD Genuine	JD Imposter
Cross Match Verifier 300 LC	Male	Right Index	0.3796	0.0274	0.2773	**0.0137**	0.7592	0.0548
	Male	Right Thumb	0.3667	0.0369	0.2573	0.0184	0.7334	0.0737
	Female	Right Index	0.5472	0.1236	0.4105	0.0614	1.0945	0.2472
	Female	Right Thumb	0.5075	0.121	0.3783	0.0601	1.0149	0.242
Cross Match Verifier 310 LC	Male	Right Index	0.3829	0.0326	0.285	0.0163	0.7658	0.0652
	Female	Right Index	0.5508	0.1268	0.422	0.063	1.1016	0.2537
Upek	Male	Right Index	0.3694	0.0274	0.2687	**0.0137**	0.7388	0.0548
	Male	Right Thumb	0.3602	0.0603	0.2545	0.0301	0.7204	0.1206
	Female	Right Index	0.5354	**0.577**	0.398	0.0288	1.0707	0.1154
	Female	Right Thumb	0.5149	0.0418	0.3751	0.0209	1.0297	0.835

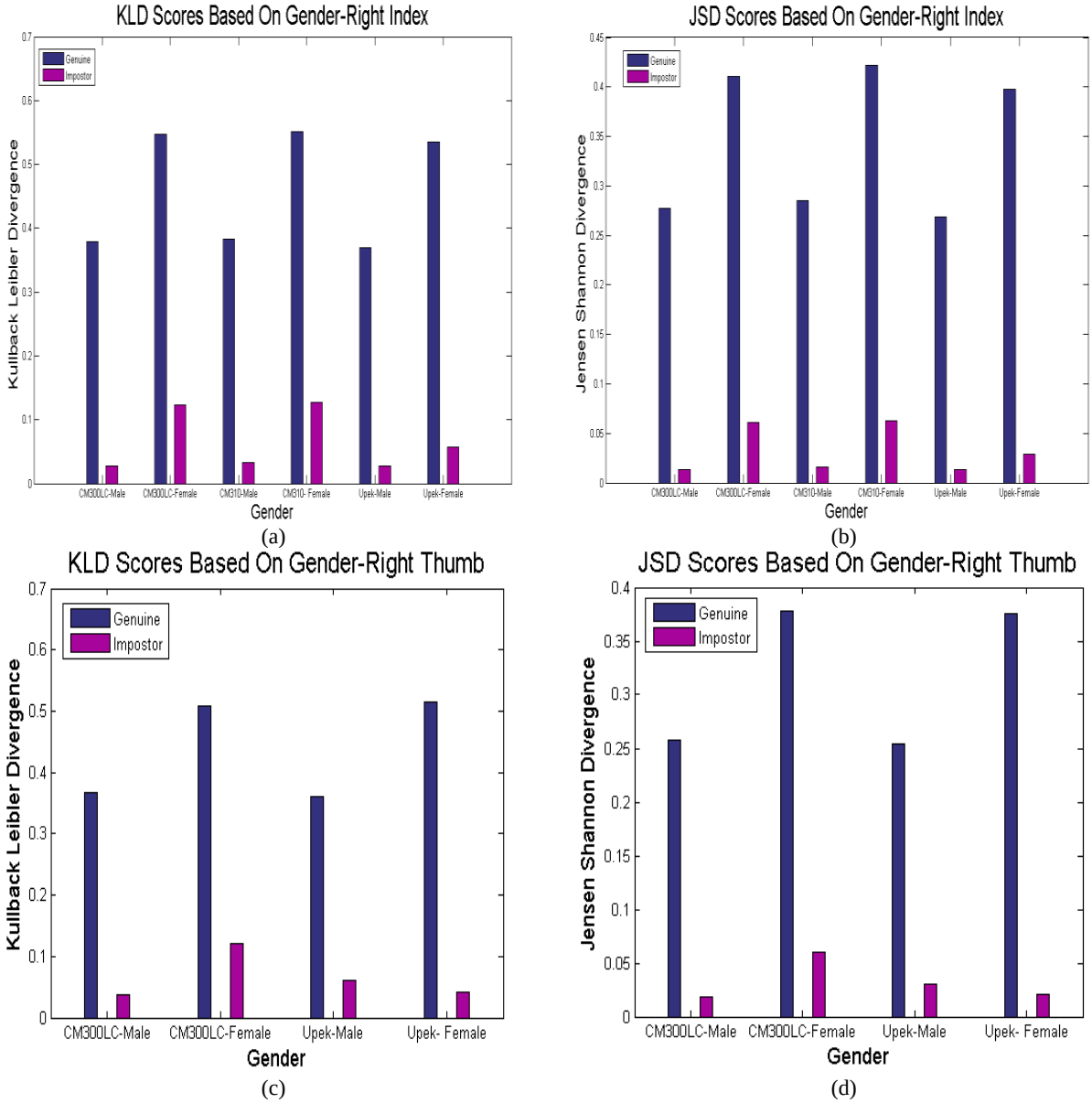


Figure 5.8 : Gender Based KLD and JSD Distributions

(a) Bar graph of KLD scores of right index images. (b) Bar graph of JSD scores of right index images. (c) Bar graph of KLD scores of right thumb images. (d) Bar graph of JSD scores of right thumb images.

5.2.2 Age Based Test Results

The fingerprint dataset of the WVU 2012 BioCOP consists of subjects belonging to five age groups viz. Age 18-19, Age 20-30, Age 31-49, Age 50-70, Age 71-79. The sections below focus on the difference in match performance between the various age groups with reference to the ROC curves and the statistical divergence measures.

5.2.2.1 Match Score Analysis

Figure 5.9, 5.10, 5.11 shows the match score distributions of each scanners for each of the major age stratum under study. It needs to be mentioned that the overlap area of the genuine and impostor distribution is very small indicating a very less error region. Also, the performance of the three age groups has been quite close to the match performance of the total dataset. This results holds good for all the distributions of the three major age groups Age 20-30, Age 31-49, Age 50-70. Refer to the Section B of appendix for the individual genuine and imposter score distributions.

Table 5.7 : Maximum and Minimum match scores of the three major age groups

Demographic	Scanner	Finger	Genuine		Imposter	
			Maximum	Minimum	Maximum	Minimum
20-30	Cross Match Verifier 300LC	Right Thumb	57288	0	7432	0
		Right Index	21819	0	15140	0
	Cross Match Verifier 310LC	Right Index	28609	0	7011	0
	Upek Eikon Touch	Right Thumb	23760	0	5781	0
		Right Index	31277	0	9470	0
31-49	Cross Match Verifier 300LC	Right Thumb	14002	4	17391	0
		Right Index	14859	0	11629	0
	Cross Match Verifier 310LC	Right Index	94154	0	10017	0
	Upek Eikon Touch	Right Thumb	22681	0	6795	0
		Right Index	22992	42	1323	0
50-70	Cross Match Verifier 300LC	Right Thumb	12877	0	34	0
		Right Index	14472	0	41	0
	Cross Match Verifier 310LC	Right Index	20369	0	51	0
	Upek Eikon Touch	Right Thumb	12983	0	52	0
		Right Index	18444	0	56	0

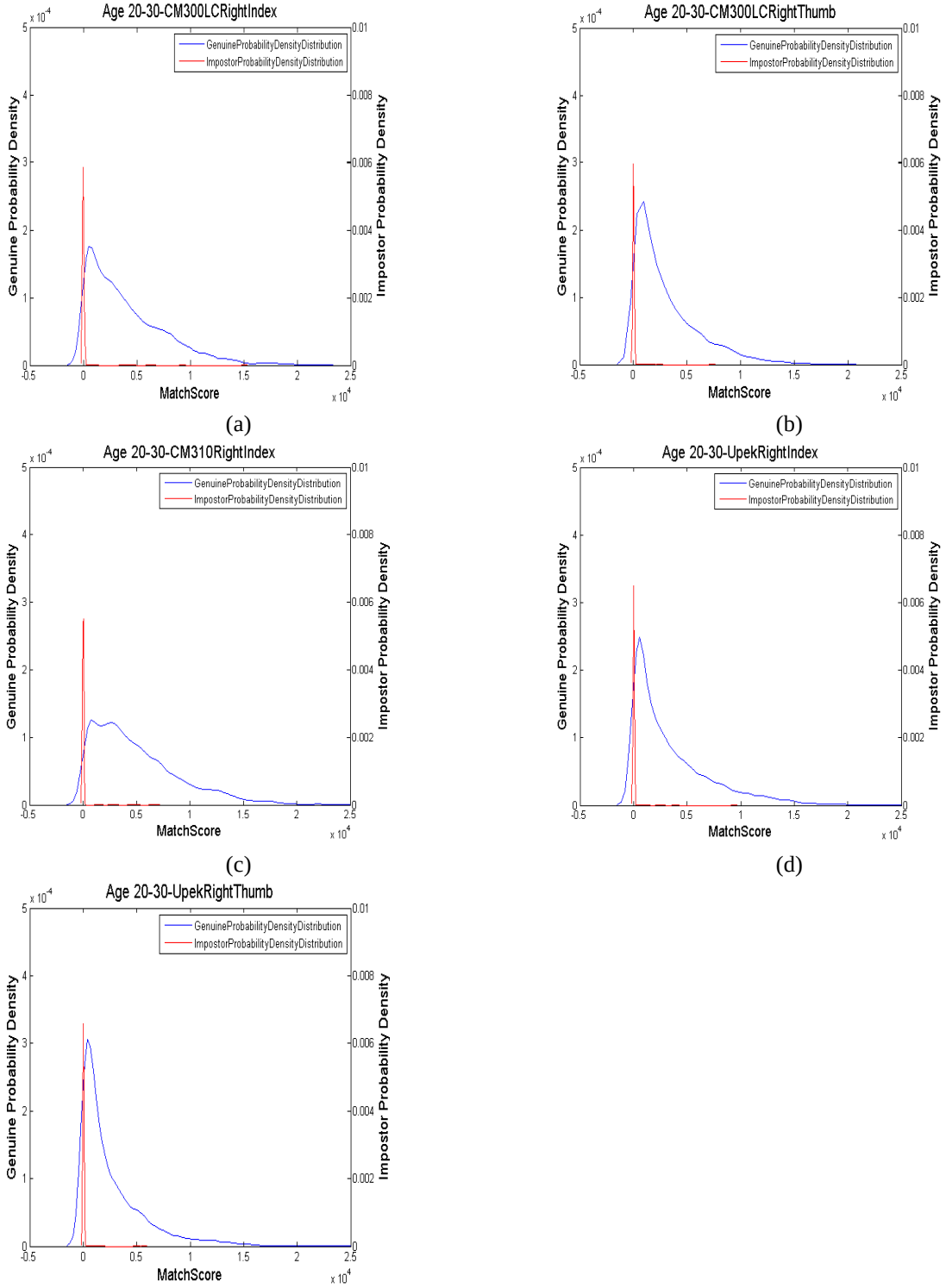
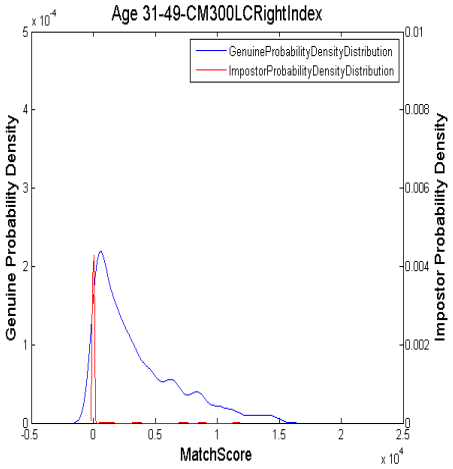
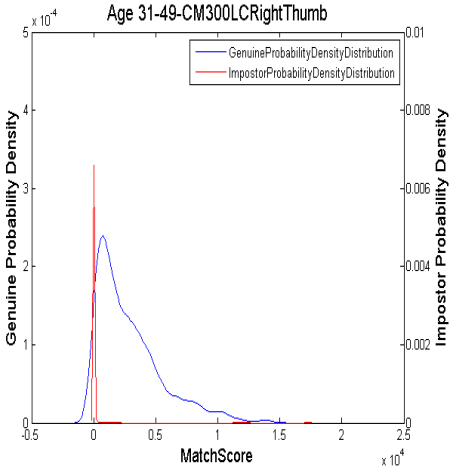


Figure 5.9 : Genuine and imposter match score distributions for Age group 20-30.

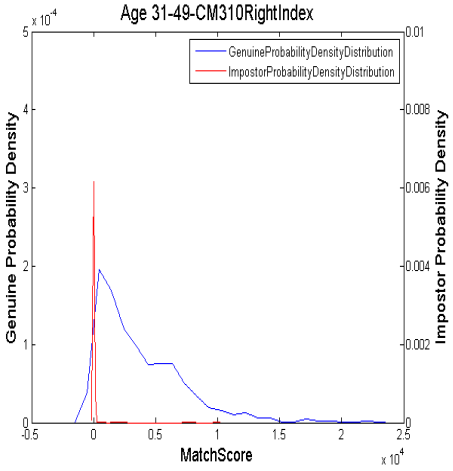
(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.



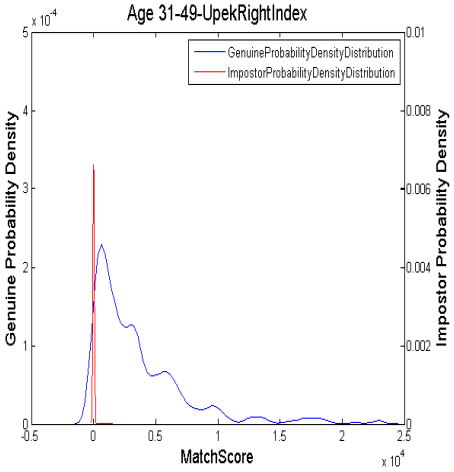
(a)



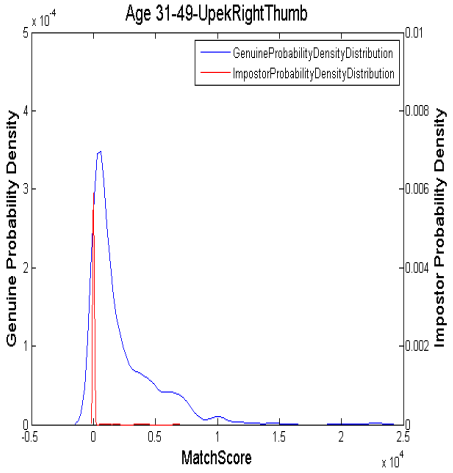
(b)



(c)



(d)



(e)

Figure 5.10: Genuine and imposter match score distributions for Age group 31-49.

(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

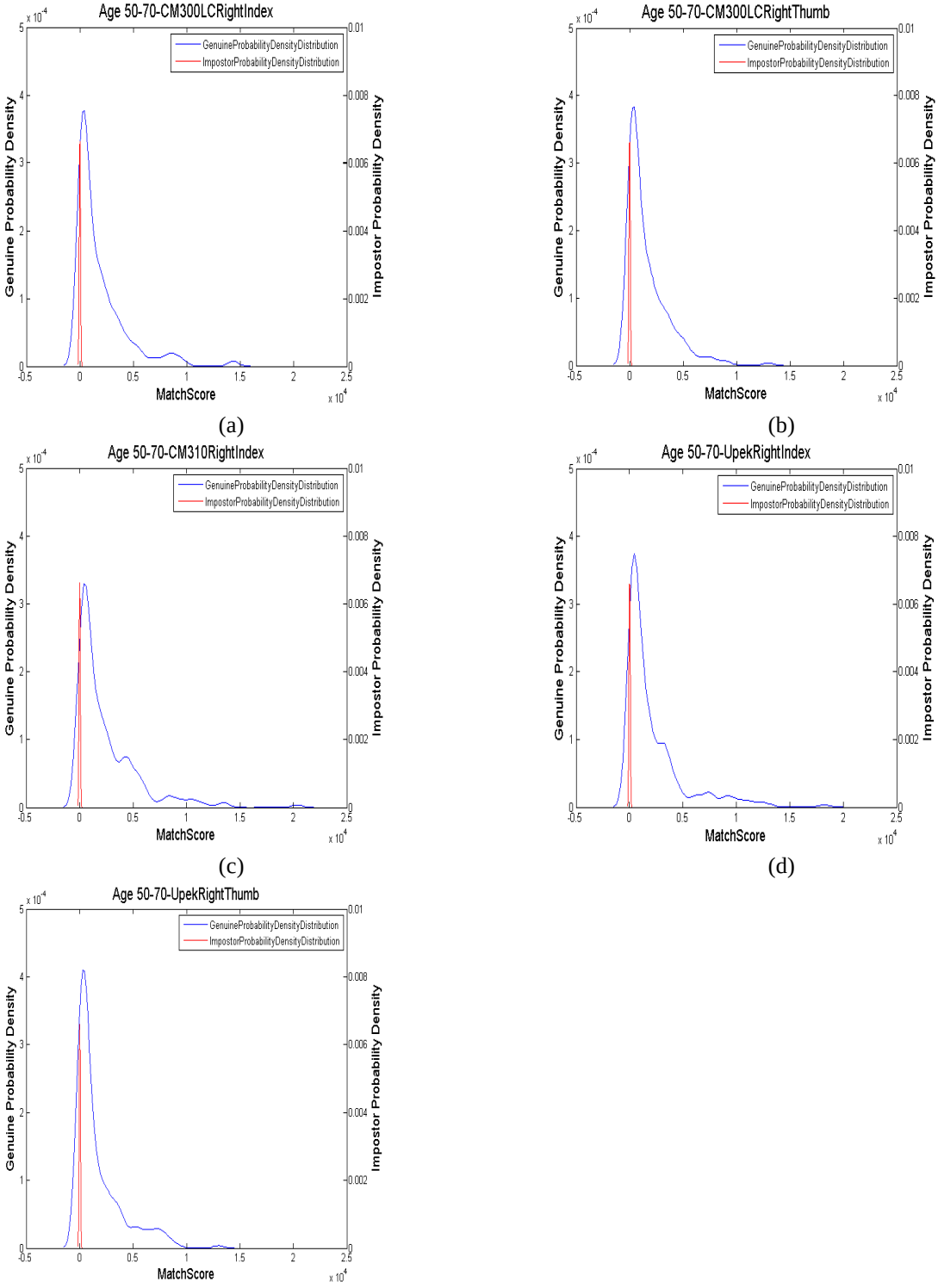


Figure 5.11 : Genuine and imposter match score distributions for Age group 50-70.

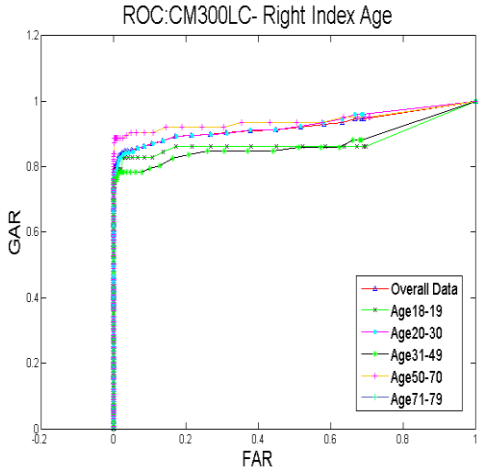
(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

5.2.2.2 Receiver Operating Characteristic Curves

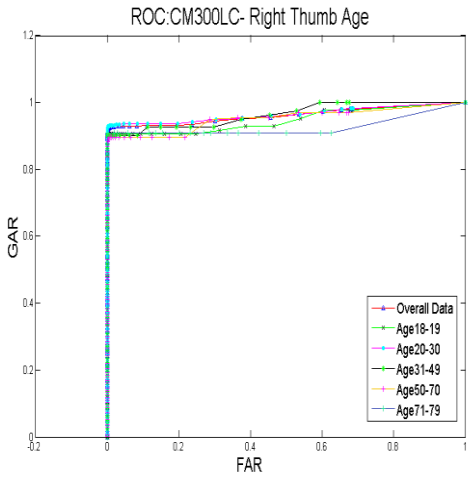
Table 5.8 lists the AUC Values obtained from the receiver operating characteristic curves. It can be noticed that the age group 20-30 has been close in its match performance to the total dataset owing to the similarity in sample size as the subjects belonging to this group constitute a major section of the age demographic strata.

Table 5.8 : Age Based AUC Values

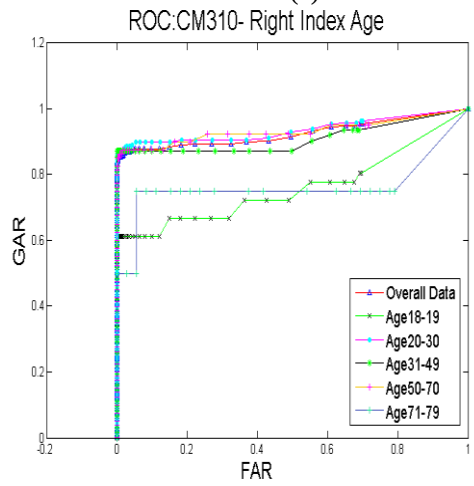
Scanner	Finger	Age	Area Under Curve
Cross Match Verifier 300LC	Right Thumb	Main	0.9535
		18-19	0.9456
		20-30	0.9528
		31-49	0.9642
		50-70	0.9505
		71-79	0.915
	Right Index	Main	0.9197
		18-19	0.8671
		20-30	0.924
		31-49	0.861
		50-70	0.938
		71-79	0.9216
Cross Match Verifier 310	Right Index	Main	0.8656
		18-19	0.5358
		20-30	0.8754
		31-49	0.9041
		50-70	0.9293
		71-79	0.7455
Upek Eikon Touch 700	Right Thumb	Main	0.9381
		18-19	0.928
		20-30	0.9352
		31-49	0.9845
		50-70	0.8985
		71-79	0.8617
	Right Index	Main	0.9635
		18-19	0.9441
		20-30	0.9606
		31-49	1
		50-70	0.9366
		71-79	0.9927



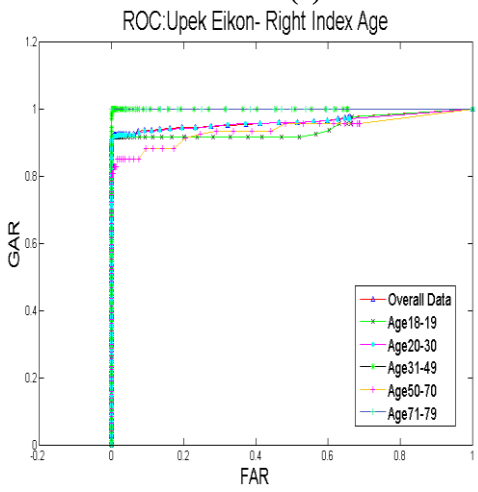
(a)



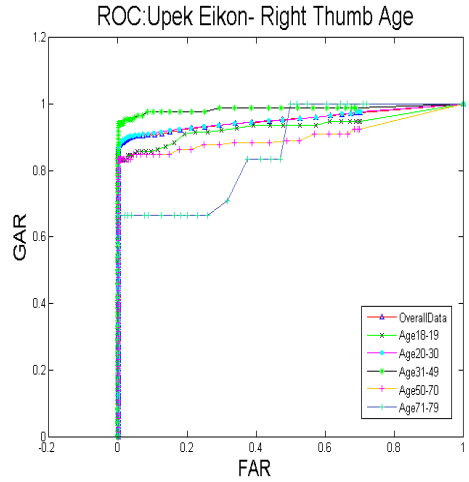
(b)



(c)



(d)



(e)

Figure 5.12 : Age Based ROC Curves

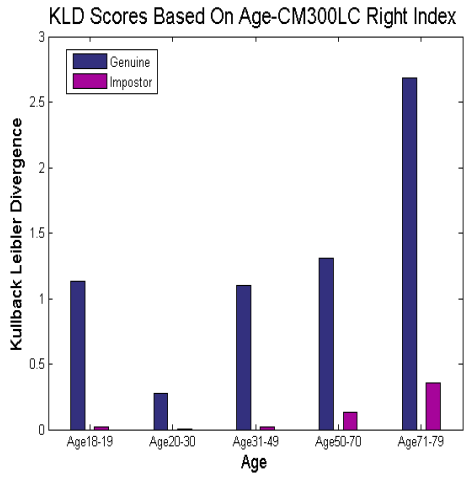
(a) CrossMatch 300LC right index. (b) CrossMatch300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

5.2.2.3 Divergence Measure Distributions

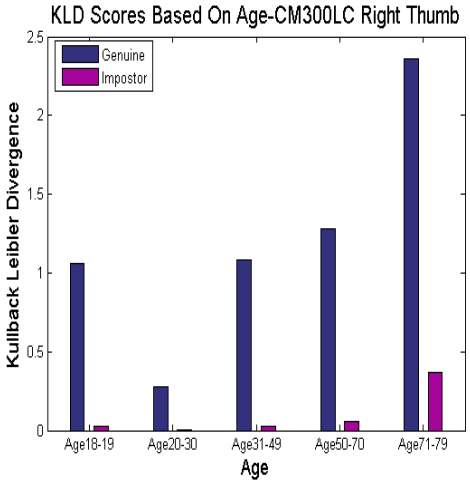
Table 5.9 : Age Based KLD and JSD Values

Sensor Name	Age	Finger	KLD Genuine	KLD Imposter	JSD Genuine	JSD Imposter	JD Genuine	JD Imposter
Cross Match Verifier 300 LC	18-19	Right Index	1.136	0.0177	0.6633	0.0089	2.2632	0.0354
		Right Thumb	1.0565	0.0274	0.6344	0.0137	2.1131	0.0544
	20-30	Right Index	0.2799	0.0075	0.1921	0.0037	0.5597	0.015
		Right Thumb	0.2764	0.0069	0.1838	0.0035	0.5527	0.0139
	31-44	Right Index	1.0967	0.0207	0.6533	0.0102	2.1934	0.0415
		Right Thumb	1.084	0.0261	0.6485	0.0129	2.168	0.0523
	50-70	Right Index	1.311	0.1318	0.687	0.0654	2.622	0.2637
		Right Thumb	1.2817	0.0591	0.6818	0.0295	2.5633	0.1183
	71-79	Right Index	**2.6869**	0.3538	0.6783	0.2451	5.3738	0.7076
		Right Thumb	2.3618	0.3656	0.6098	0.1836	4.7236	0.7313
Cross Match Verifier 310	18-19	Right Index	1.1354	0.091	0.6675	0.0095	2.2709	0.0382
	20-30	Right Index	0.2824	0.009	0.1982	0.0045	0.5644	0.0179
	31-44	Right Index	1.1481	0.0389	0.6696	0.0192	2.2963	0.0774
	50-70	Right Index	1.384	0.1229	0.6964	0.061	2.768	0.2459
	71-79	Right Index	2.5021	0.5289	0.6822	0.2582	5.0041	1.0578
Upek Eikon Touch 700	18-19	Right Index	1.0958	0.0195	0.6521	0.0097	2.1917	1.039
		Right Thumb	1.0414	0.0267	0.6306	0.0133	2.0829	0.0534
	20-30	Right Index	0.2791	0.004	0.1877	**0.002**	0.5582	0.0079
		Right Thumb	0.2809	0.0082	0.1765	0.0041	0.5475	0.0165
	31-44	Right Index	1.0962	0.0212	0.653	0.0106	2.1925	0.0425
		Right Thumb	0.915	0.0345	0.6621	0.0172	1.0435	0.069
	50-70	Right Index	1.2886	0.1423	0.6812	0.0707	2.5771	0.2847
		Right Thumb	2.178	0.1098	0.664	0.0543	2.4201	0.2196
	71-79	Right Index	2.4818	0.3271	0.6894	0.2026	4.9636	0.6542
		Right Thumb	2.0999	0.35	0.6938	0.1736	4.1997	0.7

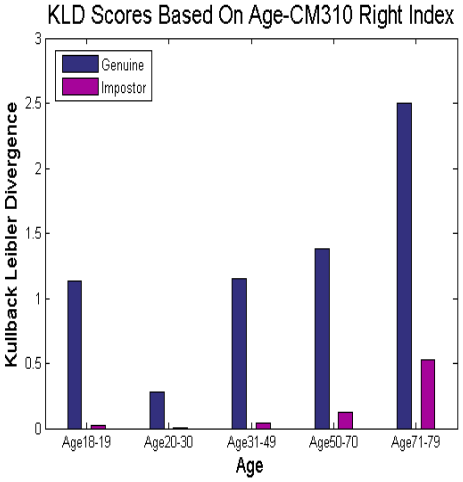
Table 5.9 lists the divergence distance measures between the various age stratums. Both the KLD and JSD distributions validate the conclusions arrived at in the section 5.2.2.2. For the age strata the maximum divergence score obtained is 2.6869 while the minimum score obtained is 0.002. It is to be noticed that there is considerably higher variation in the match scores of the age strata in comparison with the overall dataset. However, yet again, this variation is not significant enough to conclude that the match performance of the age strata has been influenced by the data stratification. This phenomenon in the match performance has remained constant for data acquired from all the scanners and for both the thumb and index fingers. Refer to figure 5.13 for the bar graphs of the KLD and JSD scores obtained for the various age groups.



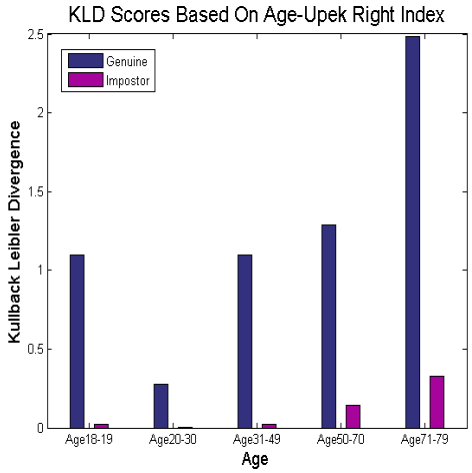
(a)



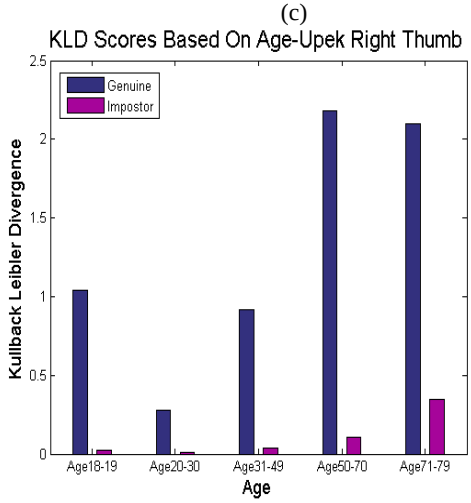
(b)



(c)



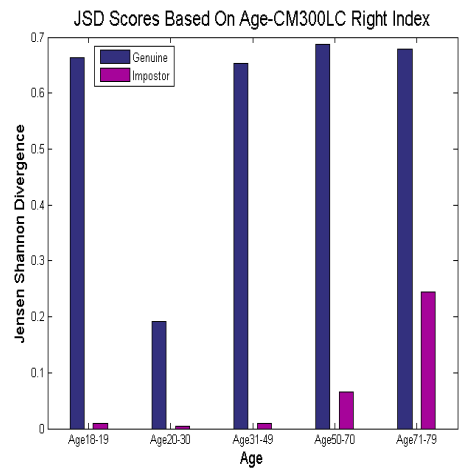
(d)



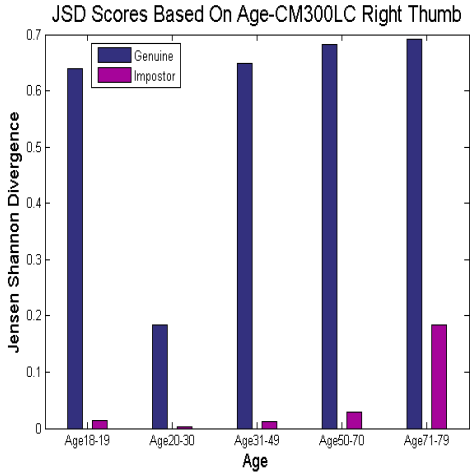
(e)

Figure 5.13 : Age Based KLD Distributions.

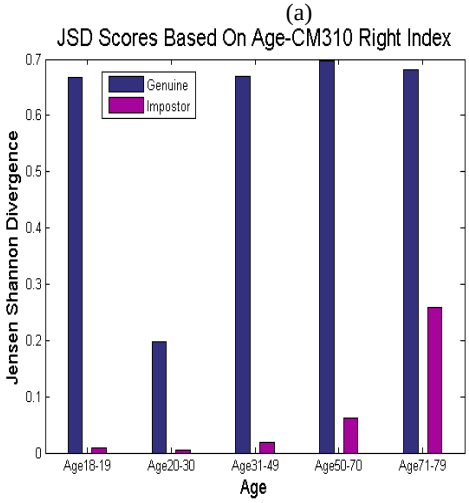
(a) Bar graph of KLD scores of right index images from Crossmatch Verifier 300LC. (b) Bar graph of KLD scores of right thumb images from Crossmatch Verifier 300LC. (c) Bar graph of KLD scores of right index images from Crossmatch Verifier 310. (d) Bar graph of KLD scores of right index images from Upek Eikon Touch 700. (e) Bar graph of KLD scores of right thumb images from Upek Eikon Touch 700.



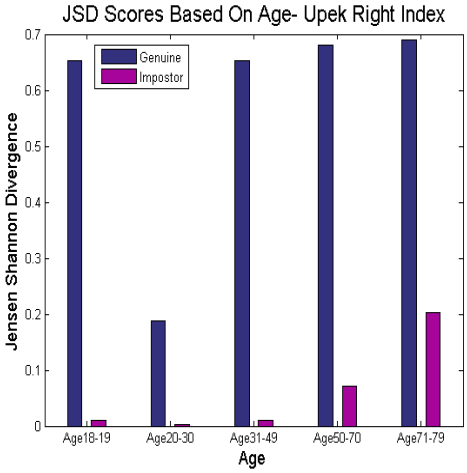
(a)



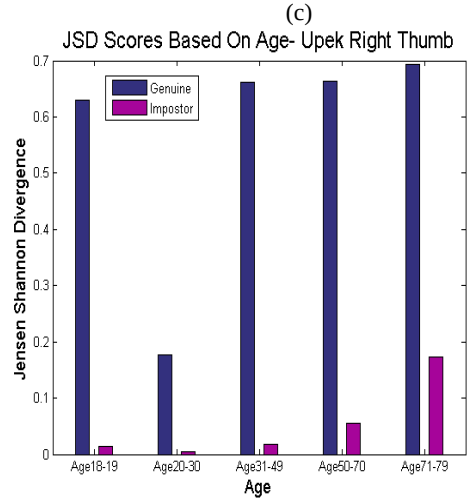
(b)



(c)



(d)



(e)

Figure 5.14 : Age Based JSD Distributions

(a) Bar graph of KLD scores of right index images from Crossmatch Verifier 300LC. (b) Bar graph of KLD scores of right thumb images from Crossmatch Verifier 300LC. (c) Bar graph of KLD scores of right index images from Crossmatch Verifier 310. (d) Bar graph of KLD scores of right index images from Upek Eikon Touch 700. (e) Bar graph of KLD scores of right thumb images from Upek Eikon Touch 700.

5.2.3 Ethnicity Based Test Results

The fingerprint dataset of the WVU 2012 BioCOP consists of subjects belonging to 8 ethnic groups of which Caucasians, Asian Indians and Asians are the three major stratum. The sections below focus on the difference in match performance between the various ethnic groups.

5.2.3.1 Match Score Analysis

The genuine and imposter distributions shown below indicate a similarity in match performance of all the major groups. Refer to section B of the appendix for the individual genuine and imposter score distributions for the other ethnic groups.

Table 5.10 : Maximum and Minimum scores of the major ethnic groups

Demographic	Scanner	Finger	Genuine		Imposter	
			Maximum	Minimum	Maximum	Minimum
Caucasian	Cross Match Verifier 300LC	Right Thumb	17750	0	17931	0
		Right Index	21445	0	11269	0
	Cross Match Verifier 310LC	Right Index	28609	0	10017	0
	Upek Eikon Touch 700	Right Thumb	23760	0	6795	0
		Right Index	31277	0	1323	0
Asian	Cross Match Verifier 300LC	Right Thumb	18942	0	7432	0
		Right Index	19050	0	15140	0
	Cross Match Verifier 310LC	Right Index	94154	0	7011	0
	Upek Eikon Touch 700	Right Thumb	12269	0	5781	0
		Right Index	18708	0	9470	0
Asian Indian	Cross Match Verifier 300LC	Right Thumb	16185	4	37	0
		Right Index	20705	0	49	0
	Cross Match Verifier 310LC	Right Index	22155	90	63	0
	Upek Eikon Touch 700	Right Thumb	21074	0	64	0
		Right Index	2105	0	89	0

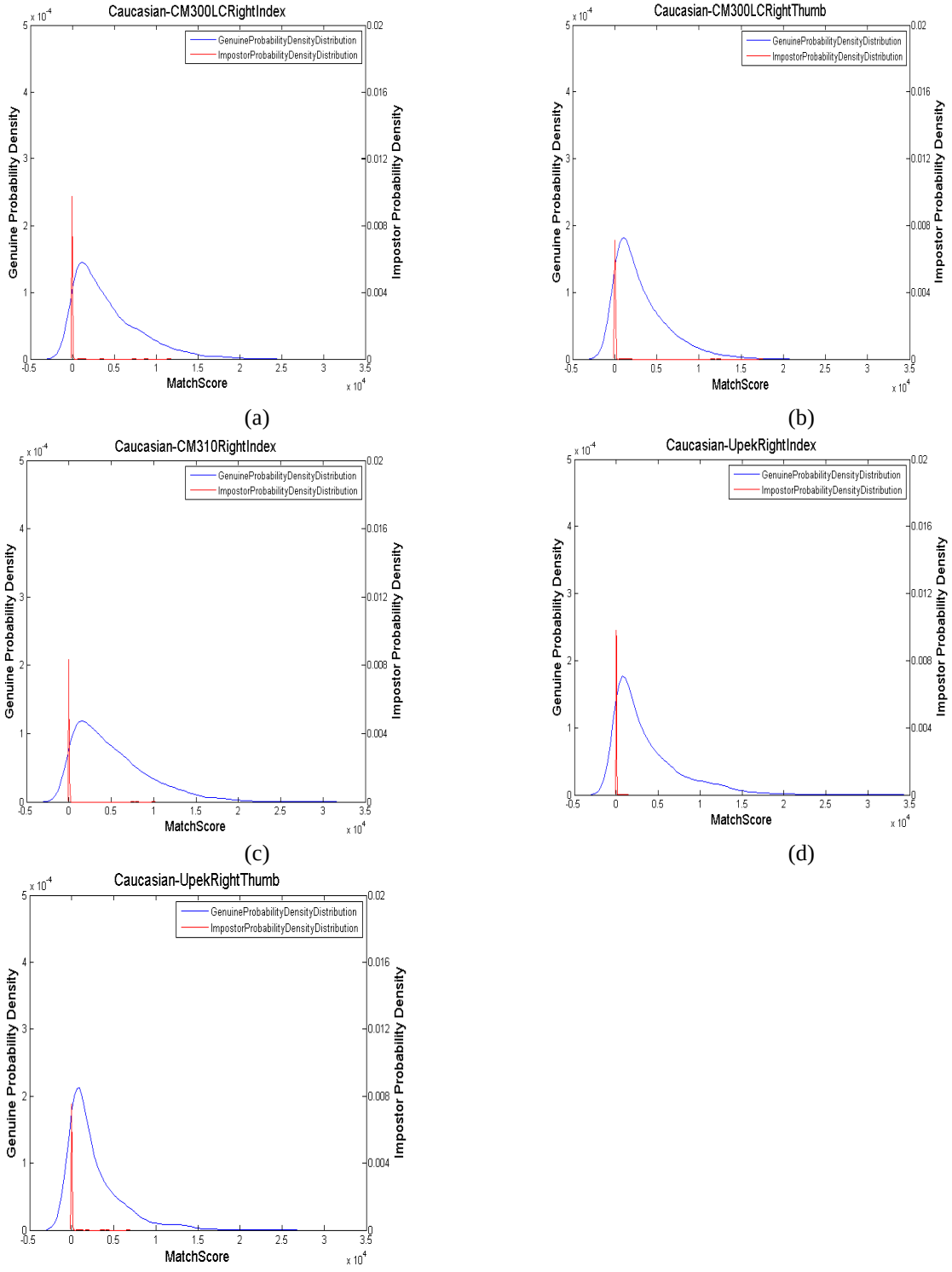


Figure 5.15 : Genuine and imposter match score distributions for Caucasian ethnicity.

(a) CrossMatch 300LC right index. (b) CrossMatch 300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

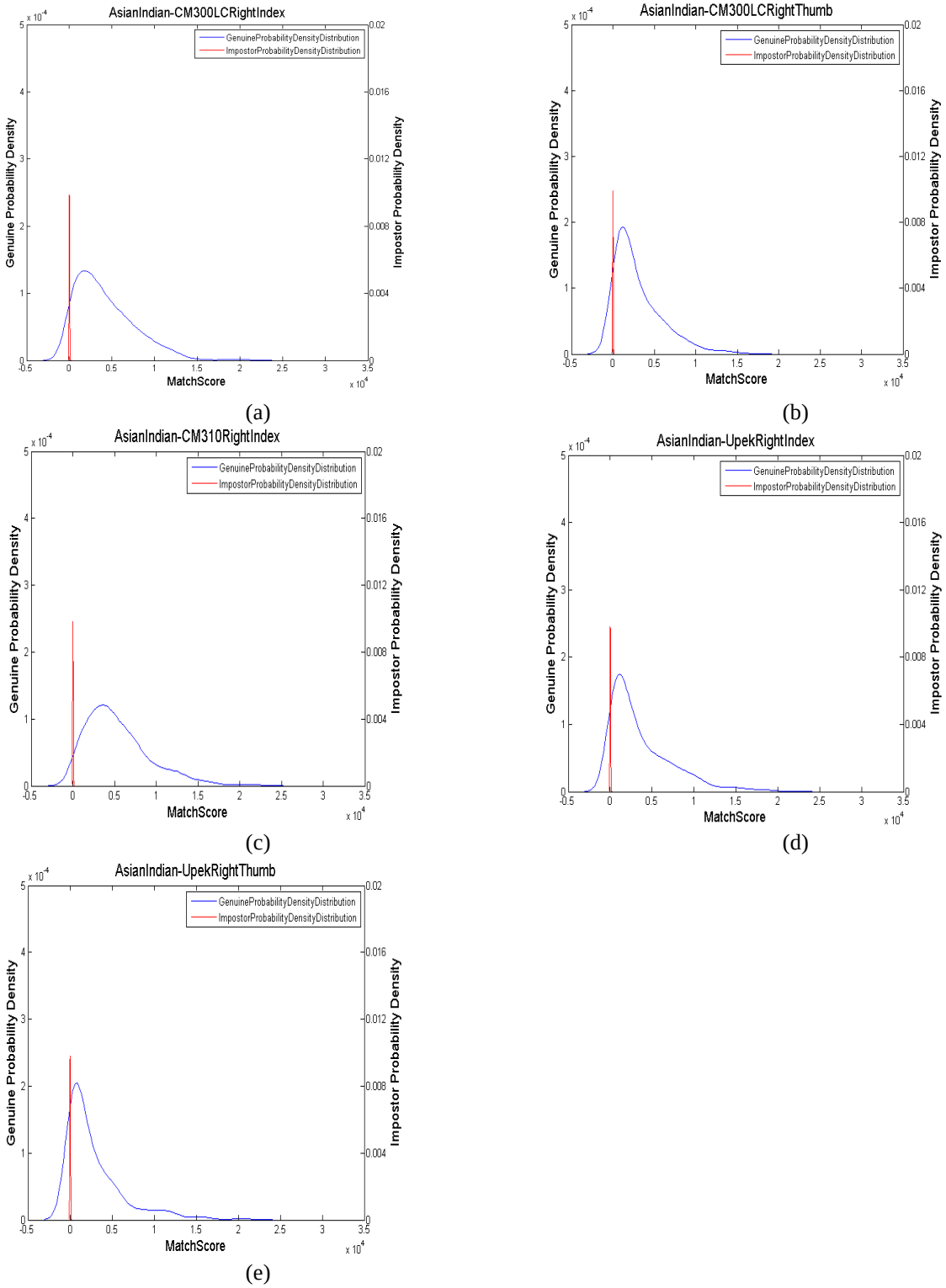


Figure 5.16 : Genuine and imposter match score distributions for Asian Indian ethnicity.

(a) CrossMatch 300LC right index. (b) CrossMatch 300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

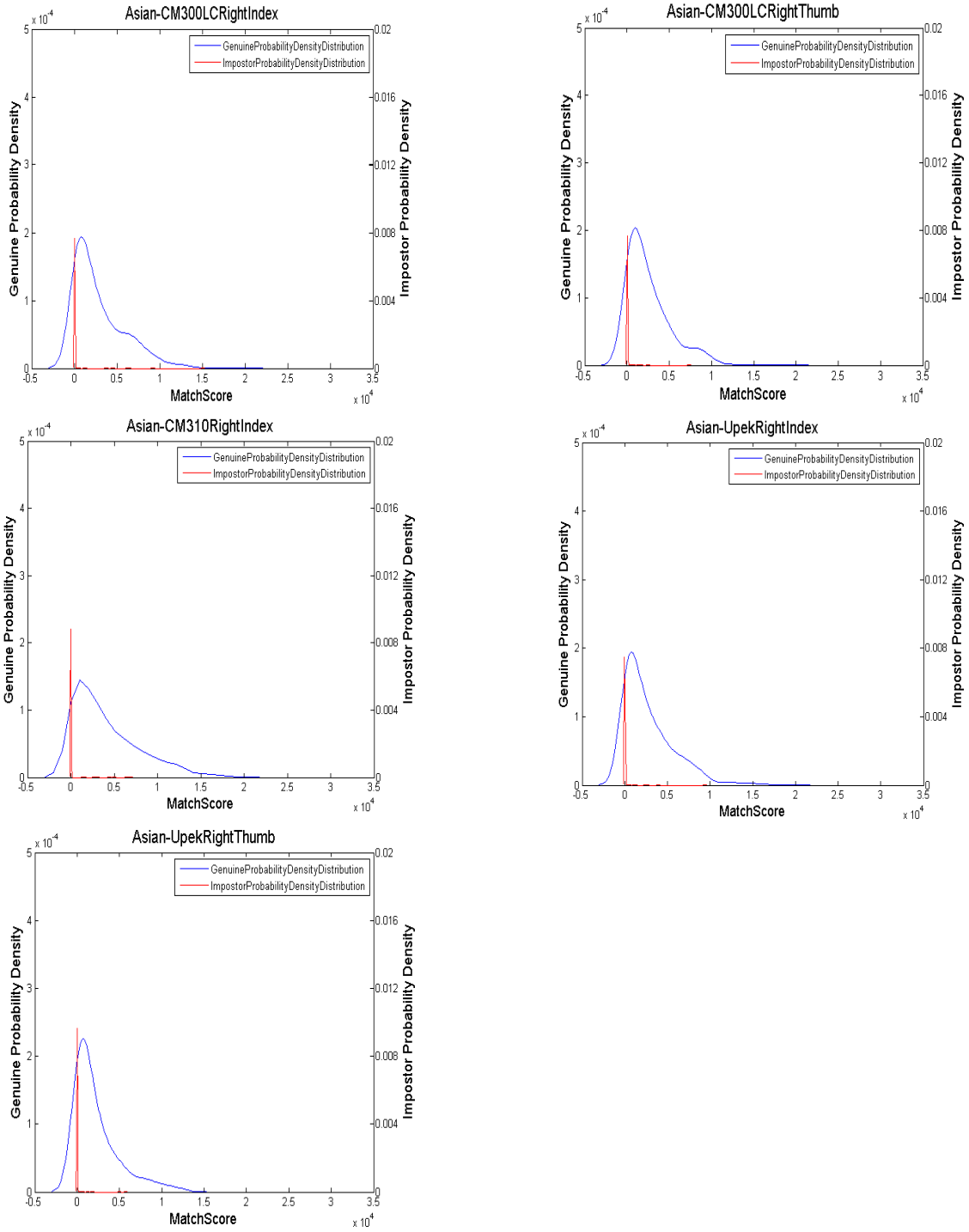


Figure 5.17 : Genuine and imposter match score distributions for Asian ethnicity.

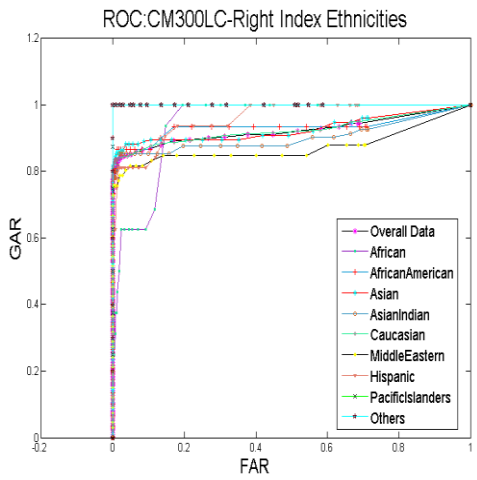
(a) CrossMatch 300LC right index. (b) CrossMatch 300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

5.2.3.2 Receiver Operating Characteristic Curves

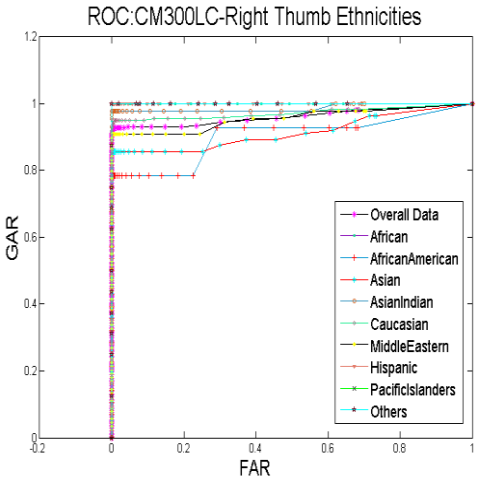
Table 5.11 lists the AUC Values obtained from the receiver operating characteristic curves.

Table 5.11 : Ethnicity Based AUC Values

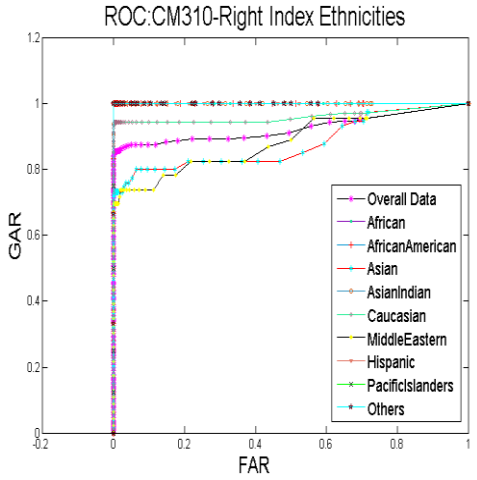
Scanner	Finger	Ethnicity	Area Under Curve
Cross Match Verifier 300LC	Right Thumb	Full data	0.9197
		African	0.9453
		African American	0.9286
		Asian Indian	0.9257
		Asian	0.8951
		Caucasian	0.9215
		Middle Eastern	0.8656
		Hispanic	0.9595
		OPF	0.9989
		Others	0.9989
	Right Index	Full data	0.9535
		African	0.999
		African American	0.8978
		Asian Indian	0.912
		Asian	0.9866
		Caucasian	0.9713
		Middle Eastern	0.9543
		Hispanic	1
		OPF	0.996
		Others	0.9993
Cross Match Verifier 310	Right Index	Full data	0.8656
		African	1
		African American	1
		Asian Indian	0.5378
		Asian	1
		Caucasian	0.9593
		Middle Eastern	0.8827
		Hispanic	1
		OPF	0.9984
		Others	0.9991
Upek Eikon Touch 700	Right Thumb	Full data	0.9381
		African	0.9999
		African American	0.909
		Asian Indian	0.7931
		Asian	0.9629
		Caucasian	0.9633
		Middle Eastern	0.9636
		Hispanic	0.9424
		OPF	0.9966
		Others	0.9971
	Right Index	Full data	0.9540
		African	0.9999
		African American	1
		Asian Indian	0.8896
		Asian	0.9812
		Caucasian	0.9729
		Middle Eastern	0.909
		Hispanic	0.994
		OPF	0.9988
		Others	0.998



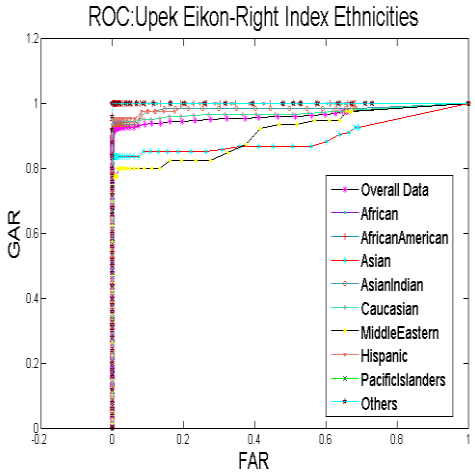
(a)



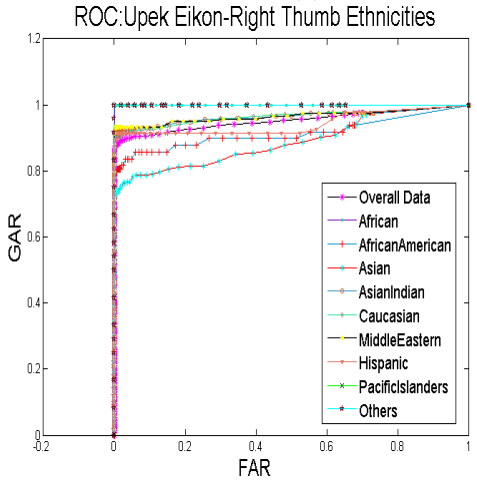
(b)



(c)



(d)



(e)

Figure 5.18 : Ethnicity Based ROC Curves.

(a) CrossMatch 300LC right index. (b) CrossMatch 300LC right thumb. (c) CrossMatch 310 right index. (d) Upek Eikon Touch right index. (e) Upek Eikon Touch right thumb.

It can also be noticed that the three major ethnic groups have close resemblance in the match performance characteristics with respect to the total dataset as an indication of minimum data stratification effect.

5.2.3.3 Divergence Measure Distributions

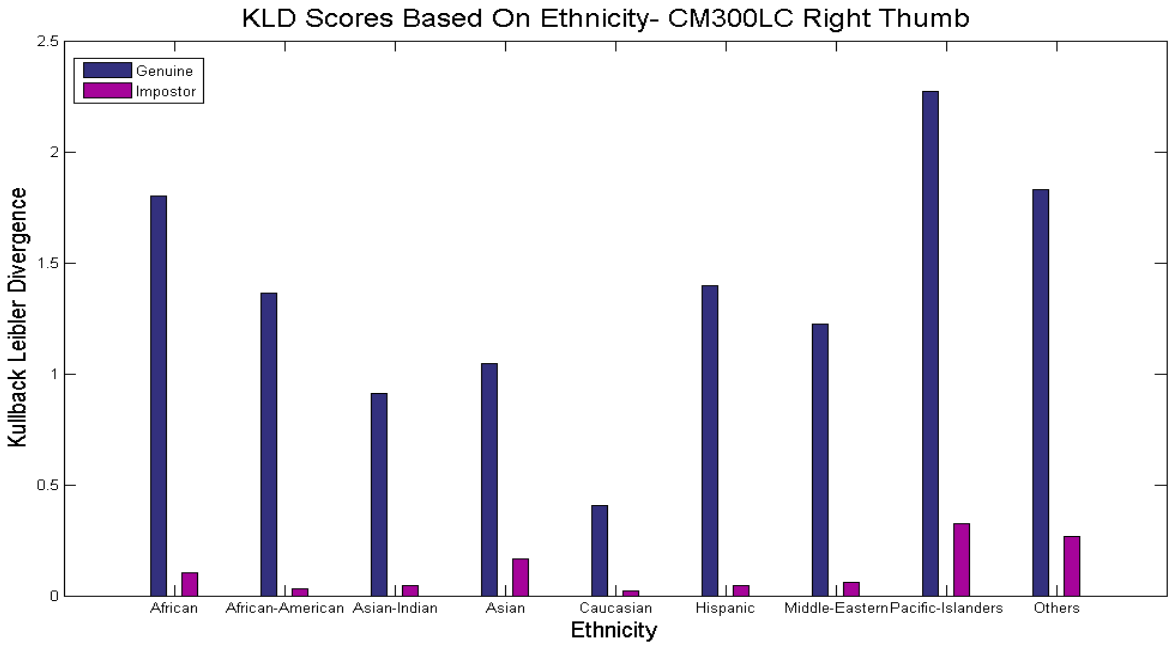
Table 5.12 : Ethnicity Based KLD and JSD values for the right index fingerprints

Sensor Name	Ethnicity	KLD Genuine	KLD Imposter	JSD Genuine	JSD Imposter	JD Genuine	JD Imposter
Cross Match Verifier 300 LC	African	1.83	0.07	0.71	0.04	3.66	0.13
	African American	1.41	0.06	0.70	0.03	2.82	0.12
	Asian Indian	0.96	0.08	0.62	0.05	1.91	0.17
	Asian	1.09	0.09	0.66	0.05	2.20	0.20
	Caucasian	0.42	0.005	0.31	0.003	0.83	0.02
	Hispanic	1.45	0.04	0.67	0.022	2.90	0.09
	Middle Eastern	1.285	0.06	0.68	0.03	2.57	0.12
	Others	1.92	0.9	0.71	0.05	3.83	0.18
	Pacific Islanders	1.57	0.41	0.70	0.22	3.15	0.80
Cross Match Verifier 310 LC	African	1.92	0.11	0.71	0.06	3.82	0.20
	African American	1.45	0.05	0.70	0.02	2.90	0.09
	Asian Indian	0.99	0.11	0.63	0.05	1.97	0.21
	Asian	1.13	0.08	0.67	0.04	2.26	0.16
	Caucasian	0.52	0.09	0.34	0.005	1.03	0.02
	Hispanic	1.49	0.07	0.70	0.04	2.98	0.15
	Middle Eastern	1.35	0.054	0.69	0.03	2.69	0.106
	Others	1.92	0.13	0.71	0.07	3.84	0.27
	Pacific Islanders	**2.50**	0.50	0.69	0.24	5.007	0.98
Upek	African	1.91	0.01	0.706	0.05	3.83	0.20
	African American	1.92	0.15	0.70	0.072	2.83	0.29
	Asian Indian	0.94	0.07	0.61	0.04	1.88	0.13
	Asian	1.06	0.09	0.65	0.05	2.11	0.18
	Caucasian	0.40	0.02	0.30	**0.001**	0.80	0.04
	Hispanic	1.45	0.05	0.69	0.02	2.91	0.09
	Middle Eastern	1.30	0.04	0.68	0.02	2.59	0.07
	Others	1.77	0.16	0.71	0.08	3.54	0.31
	Pacific Islanders	2.25	0.34	0.71	0.19	4.51	0.68

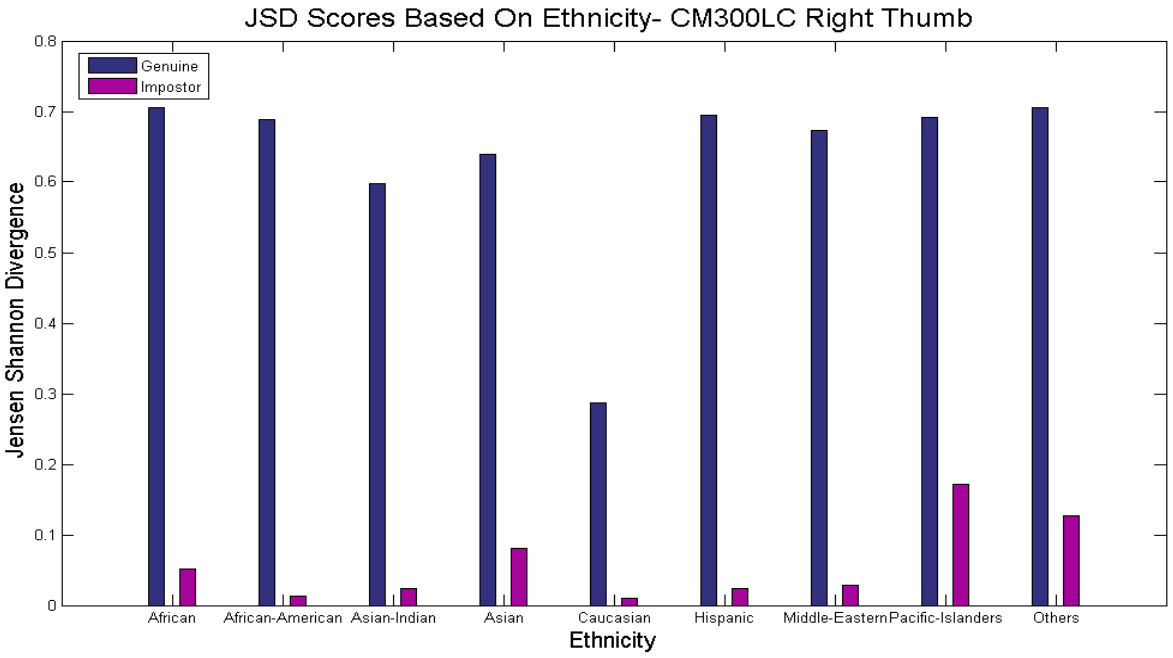
Table 5.13 : Ethnicity Based KLD and JSD values for the right thumb fingerprints

Sensor Name	Ethnicity	KLD Genuine	KLD Imposter	JSD Genuine	JSD Imposter	JD Genuine	JD Imposter
Cross Match Verifier 300 LC	African	1.80	0.11	0.71	0.05	3.60	0.21
	African American	1.36	0.027	0.69	**0.01**	2.73	0.06
	Asian Indian	0.91	0.05	0.60	0.02	1.82	0.01
	Asian	1.05	0.16	0.64	0.09	2.09	0.33
	Caucasian	0.40	0.02	0.29	**0.01**	0.81	0.04
	Hispanic	1.40	0.05	0.70	0.02	2.78	0.01
	Middle Eastern	1.22	0.06	0.70	0.03	2.45	0.12
	Others	1.83	0.27	0.70	0.13	3.66	0.54
	Pacific Islanders	**2.28**	0.32	0.70	0.18	4.55	0.65
Upek	African	1.88	0.18	0.71	0.09	3.76	0.36
	African American	1.35	0.12	0.69	0.08	2.68	0.32
	Asian Indian	0.89	0.07	0.58	0.04	1.78	0.15
	Asian	0.99	0.03	0.62	0.13	1.99	0.06
	Caucasian	0.40	0.02	0.28	**0.01**	0.80	0.02
	Hispanic	1.36	0.03	0.69	0.017	2.71	0.07
	Middle Eastern	1.12	0.04	0.66	0.02	2.40	0.07
	Others	1.81	0.17	0.71	0.08	3.62	0.34
	Pacific Islanders	2.20	0.36	0.70	0.12	4.38	0.71

Both the KLD and JSD distributions validate the conclusions arrived at in the section 5.2.3.2. The maximum and minimum divergence scores for the right index images are 2.5 and 0.001 respectively, while these values are 2.28 and 0.01 for the right thumb images. These values indicate that the match performance has not been affected by the data stratification as they present only a minor variation in the divergence distributions in comparison with the total dataset and in the case of both sets of fingerprint images.



(a)



(b)

Figure 5.19 : Ethnicity Based KLD and JSD Match Score Distributions of the right thumb fingerprint images.

5.3 Pairwise Comparison for Equal Sample Sized Strata

In order to revalidate the results that have been obtained in the previous sections, the divergence measures have been calculated considering stratum equal in size. From the values obtained, it

can be understood that the sample size of the stratum under study has not influenced the divergence measure values as the range of values in Table 5.14 present an insignificant change. Hence, it can be concluded that the effect of data stratification remains minimum even when equal sample sized strata are tested.

Table 5.14: KLD and JSD values for equal sample sized stratum

Demographic Pair	Distribution	KLD	JSD
Male-Female	Genuine	0.03	0.65
	Imposter	0.12	0.06
Age 20-30; Age 50-70	Genuine	0.01	0.67
	Imposter	0.06	0.03
Age 20-30; Age 31-49;	Genuine	0.02	0.67
	Imposter	0.05	0.03
Caucasian-Asian	Genuine	0.02	0.67
	Imposter	0.13	0.07
African-African American	Genuine	0.09	0.69
	Imposter	0.23	0.11
Hispanic- Asian Indian	Genuine	0.02	0.67
	Imposter	0.07	0.04
Middle Eastern- Asian	Genuine	0.01	0.68
	Imposter	0.30	0.14

5.4 Statistical Error Rates

Table 5.15 and Table 5.16 present the false rejection rates calculated at a false acceptance rate of 1%. With reference to the matching threshold, which was zero while performing matching, the range of FRR values has been around 1%-5%. However, a majority of these values lie close to each other which again reiterates the similarity in the match score distributions. Hence, it can be stated again that the effect of data stratification on this fingerprint dataset has been considerably insignificant.

Table 5.15 : FRR values at FAR 1% for all the age and gender strata

Demographic/ Attribute	Finger	Scanner	FRR at 1% FAR
Total data set	Right Thumb	Cross Match Verifier 300LC	0.86
		Upek Eikon Touch 700	2.46
	Right Index	Cross Match Verifier 300LC	1.80
		Cross Match Verifier-310	0.86
		Upek Eikon Touch 700	1.1
Female	Right Thumb	Cross Match Verifier 300LC	2.1
		Upek Eikon Touch 700	1.8
	Right Index	Cross Match Verifier 300LC	2.08
		Cross Match Verifier-310	1.09
		Upek Eikon Touch 700	1.09
Male	Right Thumb	Cross Match Verifier 300LC	0.84
		Upek Eikon Touch 700	2.80
	Right Index	Cross Match Verifier 300LC	1.68
		Cross Match Verifier-310	0.80
		Upek Eikon Touch 700	1.10
Age 18-19	Right Thumb	Cross Match Verifier 300LC	1
		Upek Eikon Touch 700	3.36
	Right Index	Cross Match Verifier 300LC	1.50
		Cross Match Verifier-310	1.76
		Upek Eikon Touch 700	1
Age 20-30	Right Thumb	Cross Match Verifier 300LC	0.69
		Upek Eikon Touch 700	2.24
	Right Index	Cross Match Verifier 300LC	2
		Cross Match Verifier-310	0.60
		Upek Eikon Touch 700	1.13
Age 31-49	Right Thumb	Cross Match Verifier 300LC	1
		Upek Eikon Touch 700	1.30
	Right Index	Cross Match Verifier 300LC	2.70
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0
Age 50-70	Right Thumb	Cross Match Verifier 300LC	3.26
		Upek Eikon Touch 700	5.50
	Right Index	Cross Match Verifier 300LC	3.27
		Cross Match Verifier-310	2.61
		Upek Eikon Touch 700	3.71
Age 71-79	Right Thumb	Cross Match Verifier 300LC	4.70
		Upek Eikon Touch 700	2.70
	Right Index	Cross Match Verifier 300LC	0
		Cross Match Verifier-310	1
		Upek Eikon Touch 700	0

Table 5.16 : FRR at FAR 1% for the ethnicity stratum

Ethnicity	Finger	Scanner	FRR AT FAR=1%
African	Right Thumb	Cross Match Verifier 300LC	0
		Upek Eikon Touch 700	0
	Right Index	Cross Match Verifier 300LC	7.20
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0
African-American	Right Thumb	Cross Match Verifier 300LC	1.50
		Upek Eikon Touch 700	5
	Right Index	Cross Match Verifier 300LC	1.55
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0
Asian	Right Thumb	Cross Match Verifier 300LC	2
		Upek Eikon Touch 700	6.70
	Right Index	Cross Match Verifier 300LC	2.70
		Cross Match Verifier-310	2.50
		Upek Eikon Touch 700	2.70
Asian-Indian	Right Thumb	Cross Match Verifier 300LC	0.18
		Upek Eikon Touch 700	1.60
	Right Index	Cross Match Verifier 300LC	1.38
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0.70
Caucasian	Right Thumb	Cross Match Verifier 300LC	0.57
		Upek Eikon Touch 700	1.90
	Right Index	Cross Match Verifier 300LC	1.55
		Cross Match Verifier-310	0.35
		Upek Eikon Touch 700	0.77
Middle-Eastern	Right Thumb	Cross Match Verifier 300LC	1.67
		Upek Eikon Touch 700	1.73
	Right Index	Cross Match Verifier 300LC	3.33
		Cross Match Verifier-310	2.98
		Upek Eikon Touch 700	3.85
Hispanic	Right Thumb	Cross Match Verifier 300LC	0
		Upek Eikon Touch 700	2.28
	Right Index	Cross Match Verifier 300LC	2.22
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0.57
Other Pacific Islanders	Right Thumb	Cross Match Verifier 300LC	0
		Upek Eikon Touch 700	0
	Right Index	Cross Match Verifier 300LC	0
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	0
Others	Right Thumb	Cross Match Verifier 300LC	0
		Upek Eikon Touch 700	0
	Right Index	Cross Match Verifier 300LC	0
		Cross Match Verifier-310	0
		Upek Eikon Touch 700	1.55

CHAPTER 6 - CONCLUSION AND FUTURE WORK

6.1 Conclusions

With reference to all the graphs and values listed in Chapter 5, we arrive at the following conclusions after experimentation.

Table 6.1 : Conclusions

Task	Conclusion
Match Score Distributions Of The Total Dataset	Average match performance of all the scanners has been quite similar. The divergence values range between *0.3928* and *0.0571*.
Gender Based Study	The male stratum has been able to closely match its performance to that of the total fingerprint dataset. The maximum and minimum divergence values are *0.577* and *0.0137* respectively indicating a minor variation in match performance with respect to the total dataset. Thus, it can be concluded that the gender demographic strata has presented a minor difference in its performance as a result of data stratification.
Minutiae Extraction	The minutiae extraction has been best for the fingerprint images acquired from CrossMatch Verifier 300LC for both the genders. This also indicates that this scanner has been able to provide more information for matching to the biometric verification system.
Age Based Study	The match performance of Age group 20-30 bears close resemblance to that of the total dataset owing to the similarity in sample size. The maximum and minimum divergence values are *2.6869* and *0.002* respectively. In this case, even though the values seem to be a little more variant they still present a minor variation in match performance with respect to the total dataset. Thus, it can be concluded that the age demographic strata has also presented a minor difference in its performance as a result of data stratification.
Ethnicity Based Study	The match performance of Caucasian ethnic group bears close resemblance to that of the total dataset owing to the similarity in sample size. The maximum and minimum divergence values are *2.5*, *0.001* for right index and *2.28*, *0.*01 for right thumb respectively. Again in this case, even though the values seem to be a little more variant they still present a minor variation in match performance with respect to the total dataset. Thus, it can be concluded that the ethnicity demographic strata, similar to the age and gender stratum, has also

	presented a minor difference in its performance as a result of data stratification.
Equal Sample Sized Stratum Study	The KLD and JSD values vary slightly when samples of equal size are tested for the effect of data stratification.
Statistical Error Rates	The range of FRR values at FAR 1% lie close to each other restating the minor performance change of the demographic strata with respect to the total dataset.

Considering the conclusions stated in the above sections, it is necessary to know why data stratification has not been phenomenal in this study. The fingerprint dataset of the WVU BioCOP has been acquired in a controlled environment under the supervision of trained operators. Standard acquisition techniques have been employed for obtaining the fingerprint images. Another major factor that has played an important role in determining the effect of data stratification is that the data is concentrated in a particular ethnic and age group. These factors reduce the variation in match performance. Studies [42] show that certain ethnic groups such as Africans and African Americans could be fundamental in influencing the match performance characteristics. However, in this dataset, these ethnic groups are very small in number which leads to the conclusion that the lack of more subjects belonging to such ethnic groups may have contracted the effect of data stratification.

6.2 Future Work

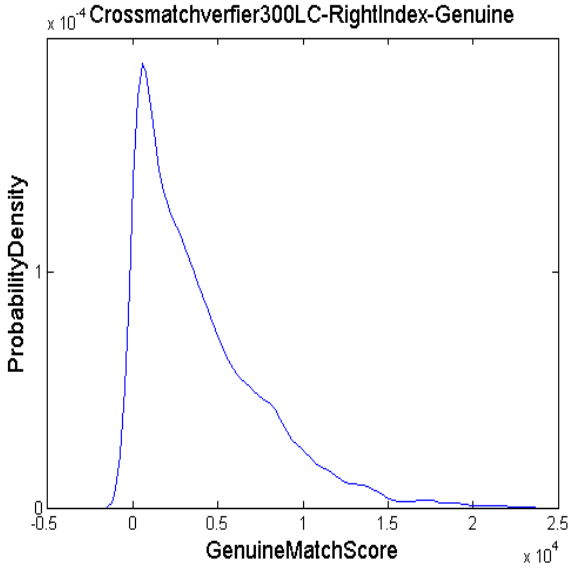
All the conclusions listed above are based on the match score values that have been obtained from a single matcher. However, in order to prove the authenticity of these results it is necessary to perform these experiments using another matching system. Although the changes in match performance have been minor in this study, the effect of applying such a framework to larger datasets could lead to highly significant performance variations. This dataset consists of 1200 subjects, so a 1% difference in performance rate accounts to the data of only 12 subjects whereas applying the same methodology to a larger dataset would drastically increase the count of subjects thereby amplifying the variation in performance. Hence, employing a large dataset could be a productive extension for this study. Using statistical measures that could more effectively validate slight quantitative changes may serve as an extension of the performance analysis. Also, experimentation with this dataset as a part of a multibiometric study can help in testing its

usability. Further study could also include, understanding the match score distributions for the left hand fingers to check for any similarities in the match performance.

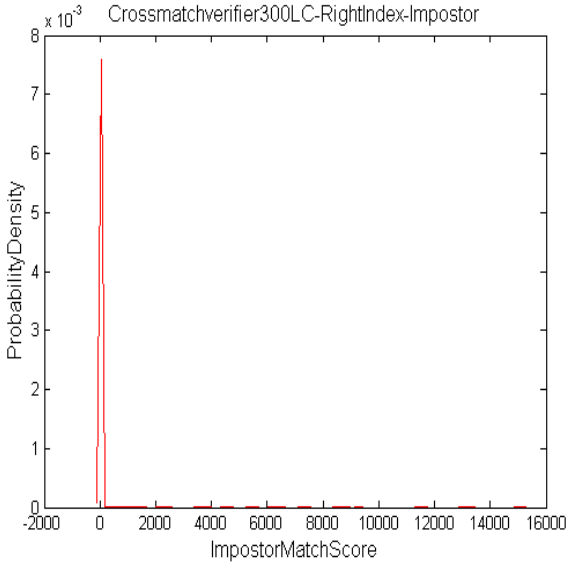
APPENDIX

[A] FINGERPRINT MATCH SCORE DISTRIBUTIONS OF THE TOTAL DATA SET

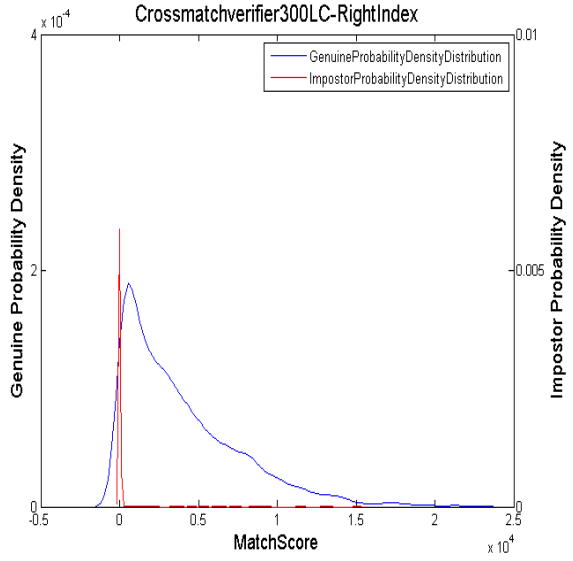
(i) Crossmatchverifier 300LC- Right Index



(a)



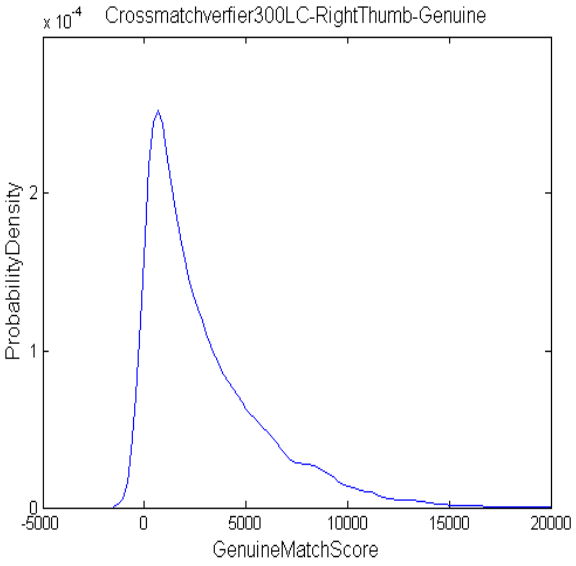
(b)



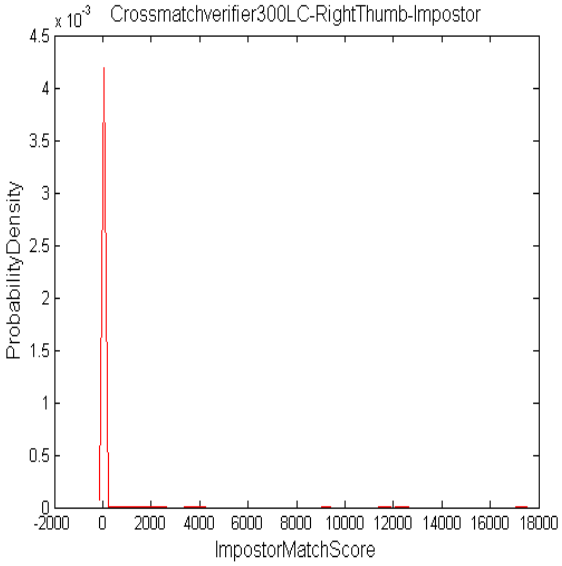
(c)

Figure A (i): Match score distributions of right index images captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

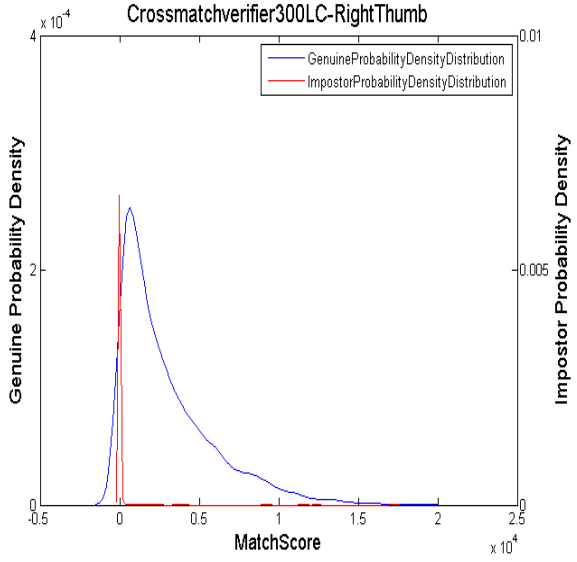
(ii) Crossmatchverifier300LC – Right Thumb



(a)



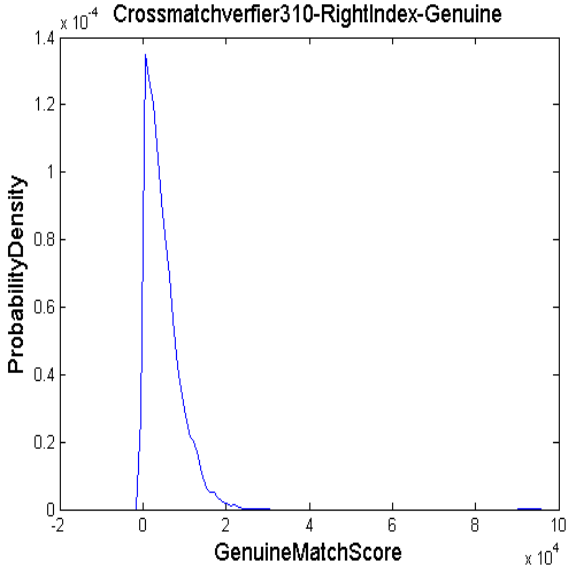
(b)



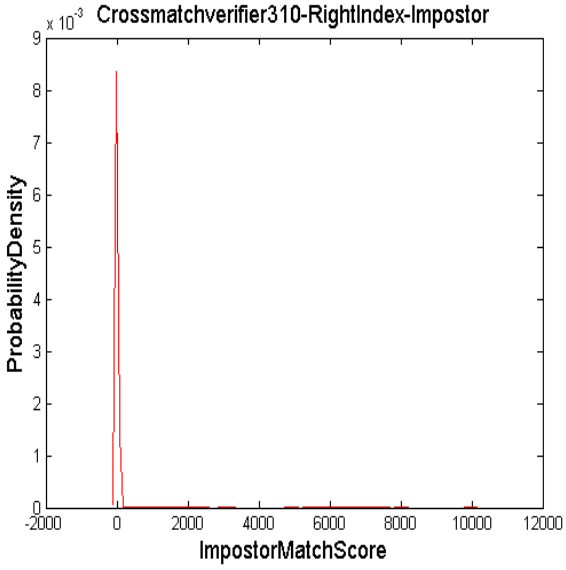
(c)

Figure A (ii): Match score distributions of right thumb images captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

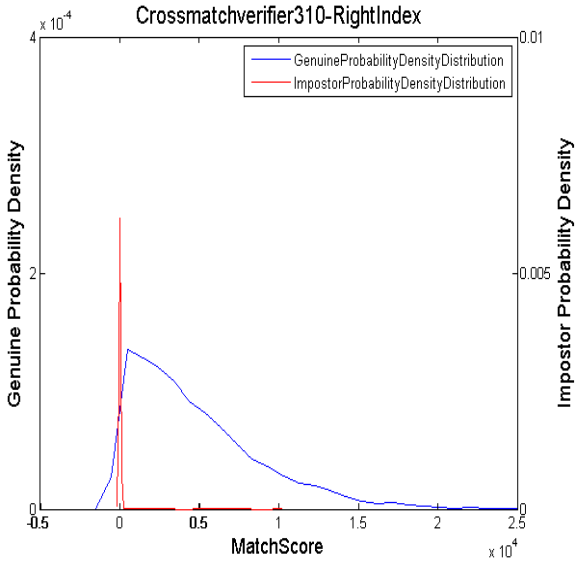
(iii) Crossmatchverifier 310 – Right Index



(a)



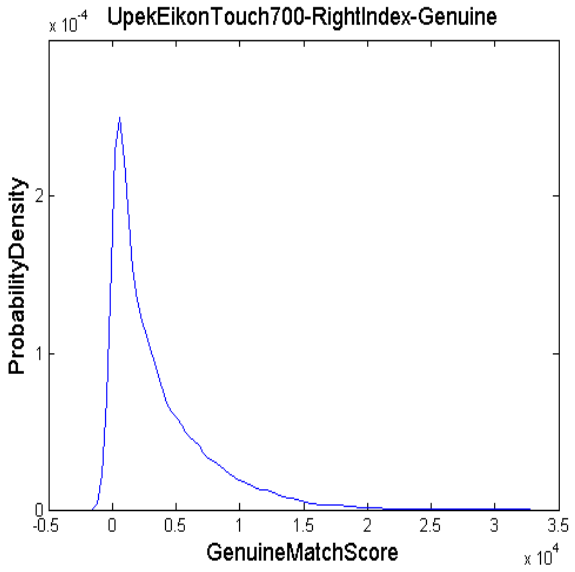
(b)



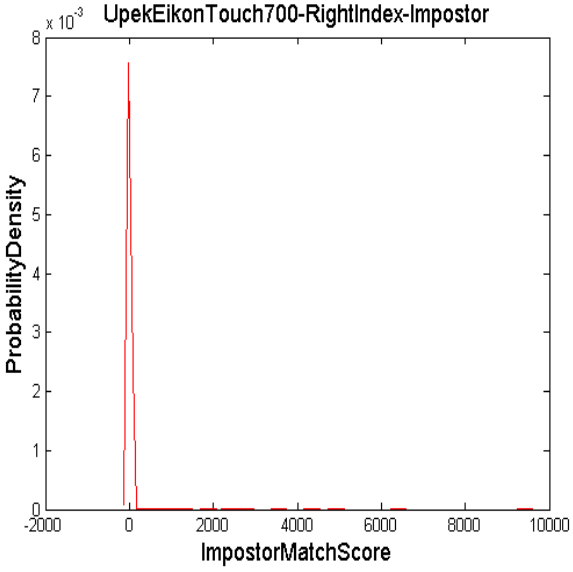
(c)

Figure A (iii): Match score distributions of right index images captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

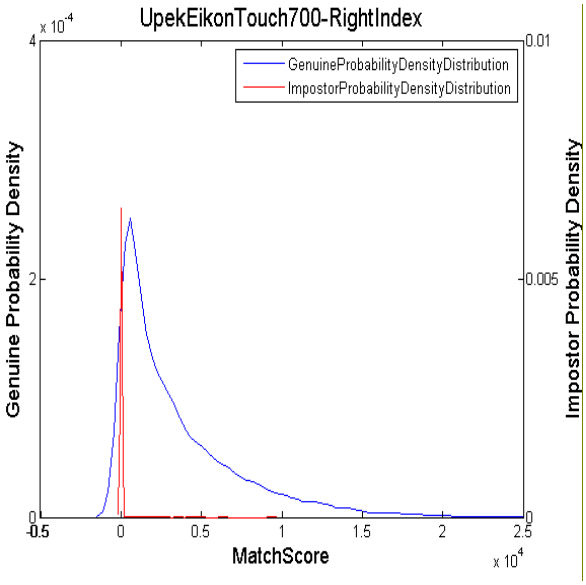
(iv) Upek Eikon Touch 700 – Right Index



(a)



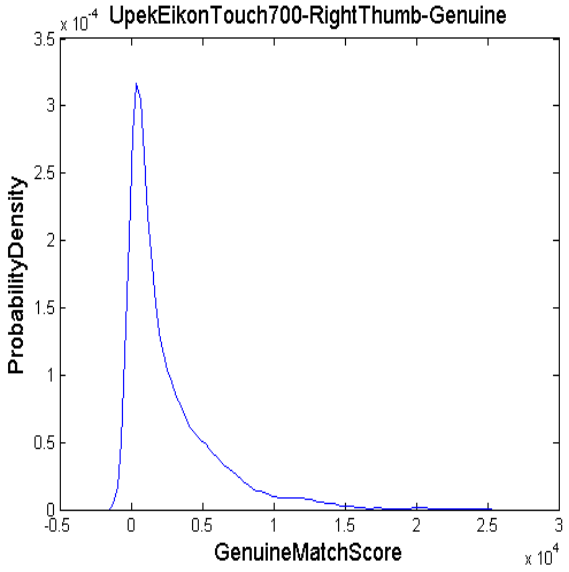
(b)



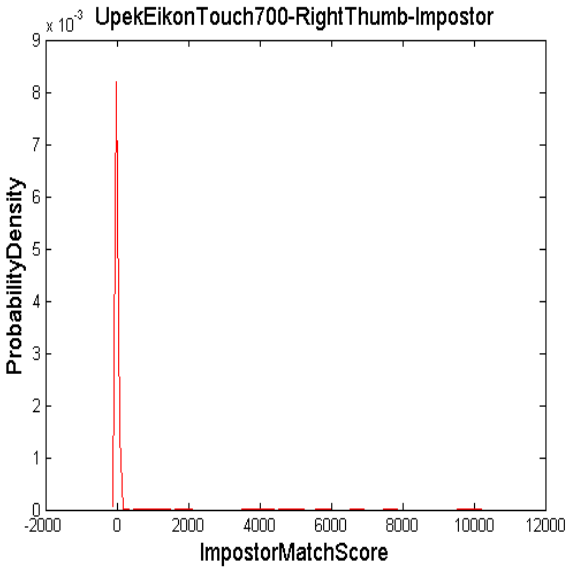
(c)

Figure A (iv): Match score distributions of right index images captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

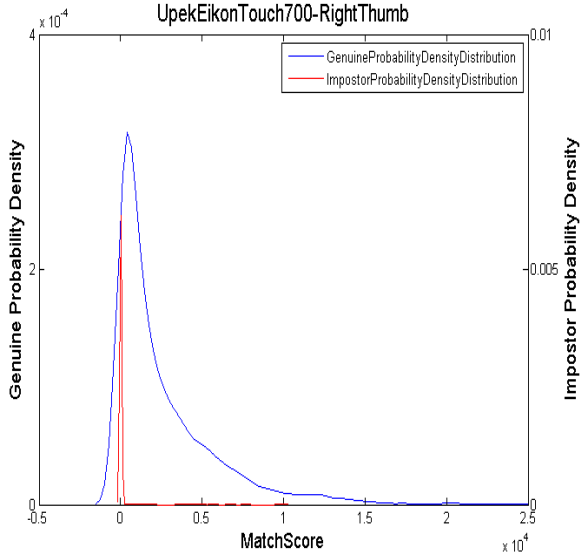
(v) Upek Eikon Touch 700- Right Thumb



(a)



(b)



(c)

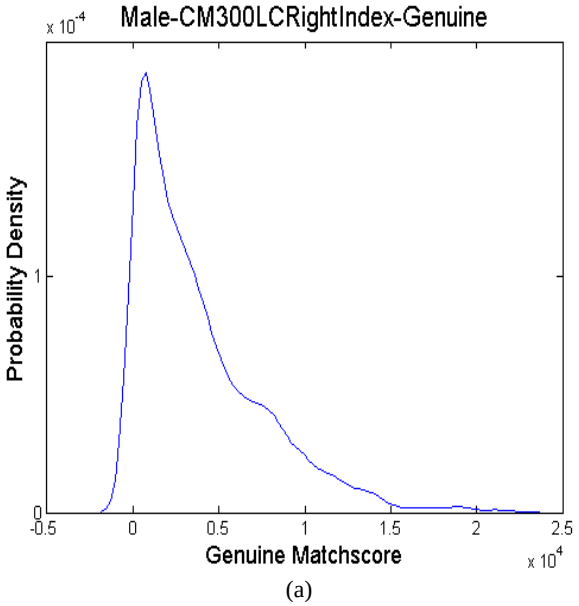
Figure A. (v): Match score distributions of right thumb images captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

[B]DEMOGRAPHIC BASED DISTRIBUTIONS

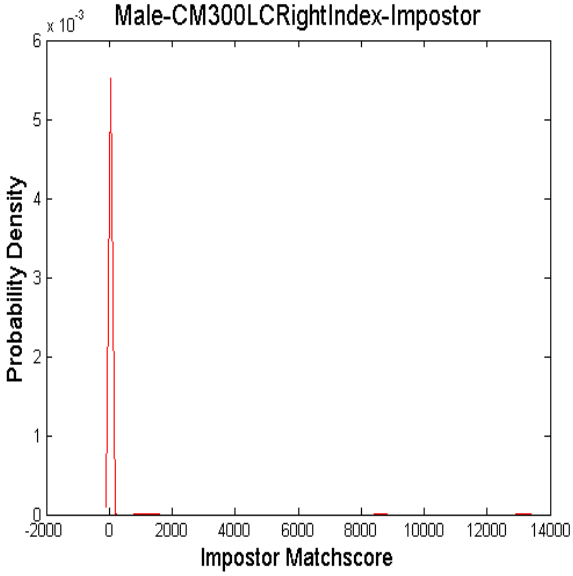
GENDER BASED FINGERPRINT MATCH SCORE DISTRIBUTIONS

B.1) Male

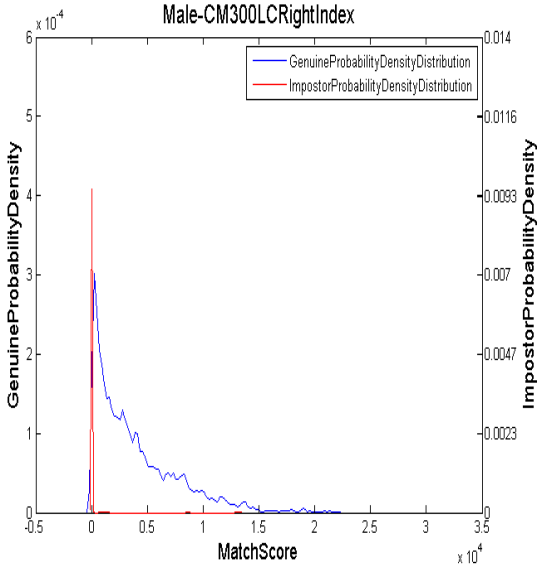
B.1. (i) Crossmatchverifier 300LC- Right Index



(a)



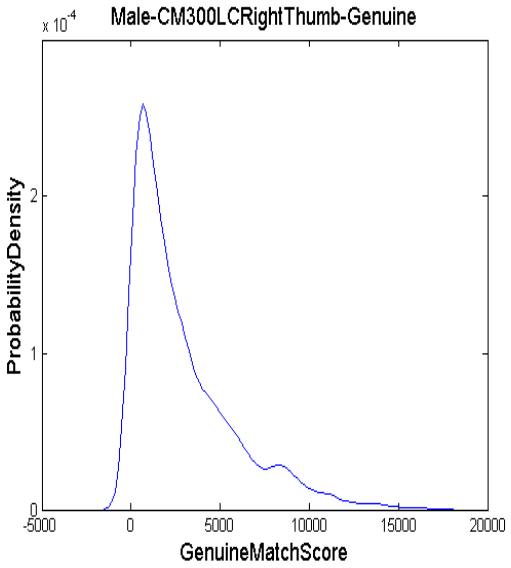
(b)



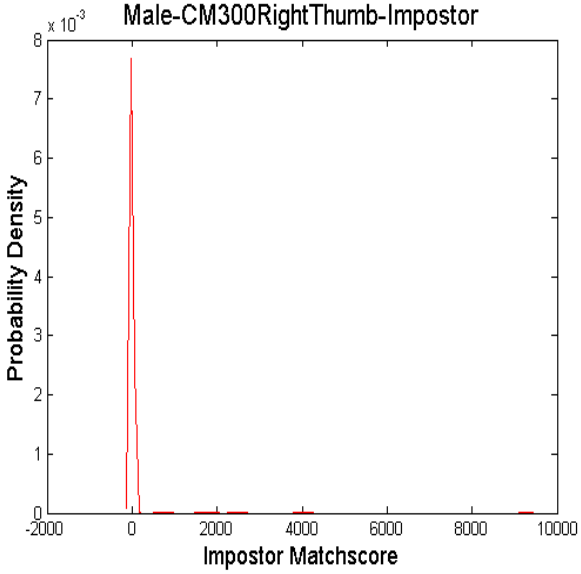
(c)

Figure B.1 (i): Match score distributions of right index images of male's captured using the Crossmatch Verifier 300LC sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

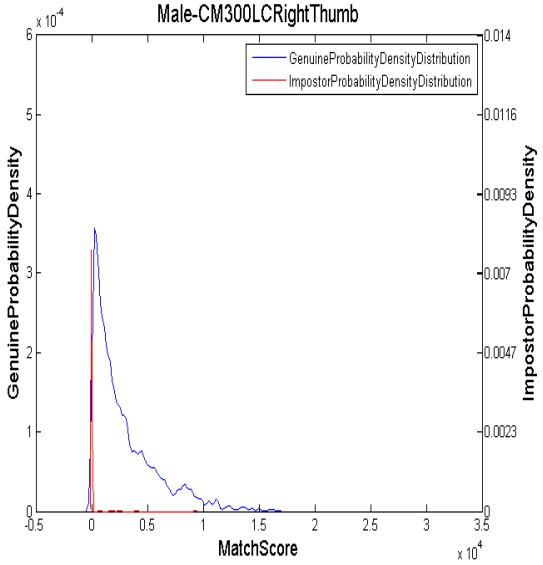
B.1. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



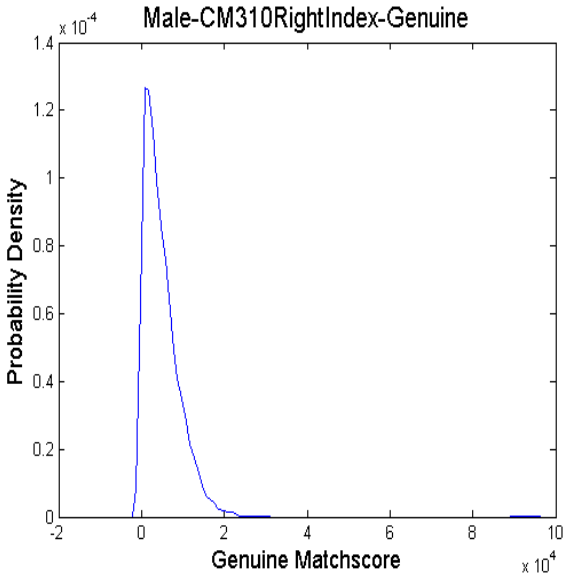
(b)



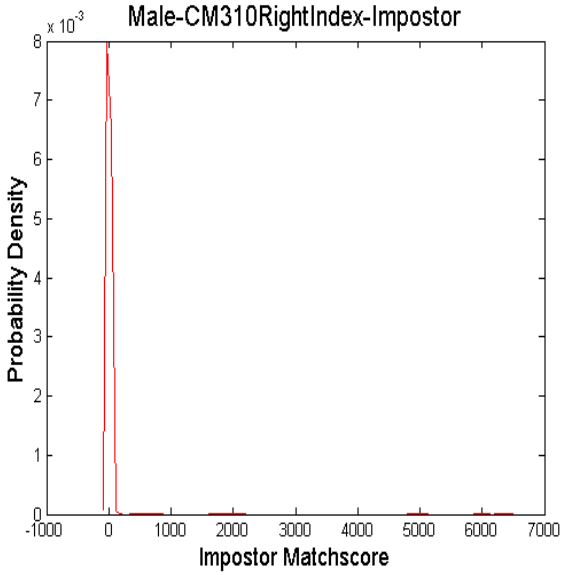
(c)

Figure B.1 (ii): Match score distributions of right thumb images of male's captured using the Crossmatch Verifier 300LC sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

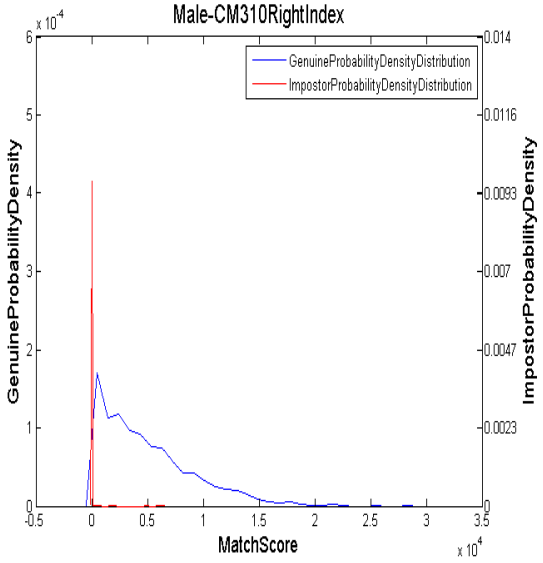
B.1. (iii) Crossmatchverifier 310 – Right Index



(a)



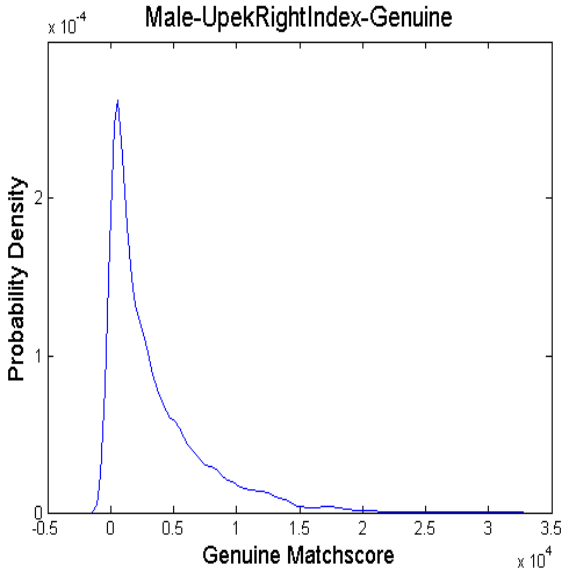
(b)



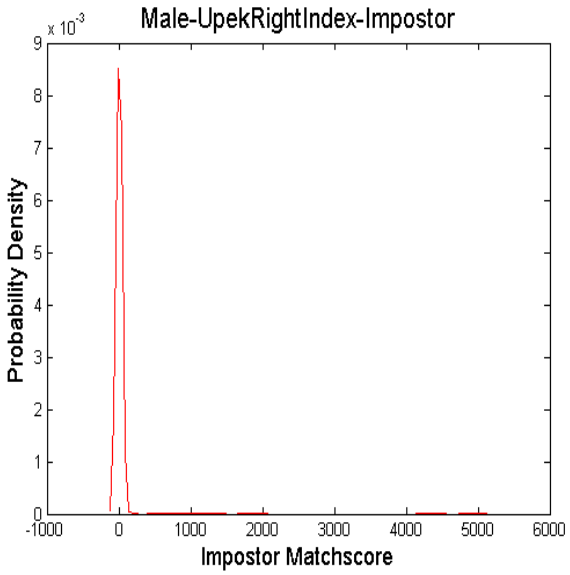
(c)

Figure B.1 (iii): Match score distributions of right index images of male's captured using the Crossmatch Verifier 310 sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

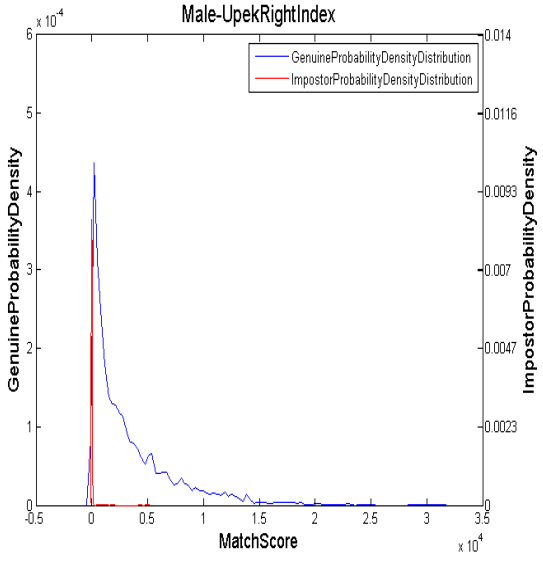
B.1. (iv) Upek Eikon Touch 700- Right Index



(a)



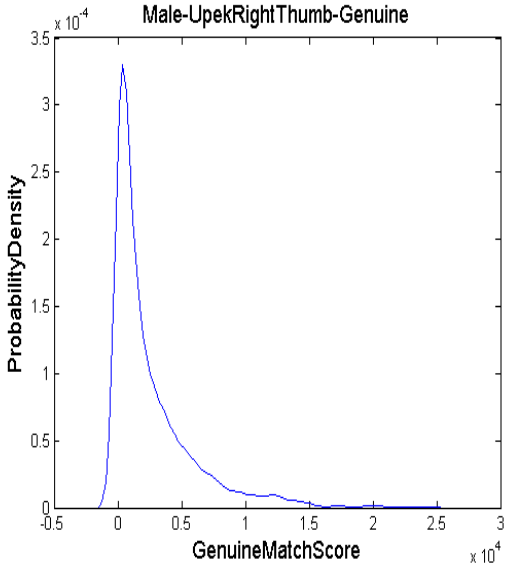
(b)



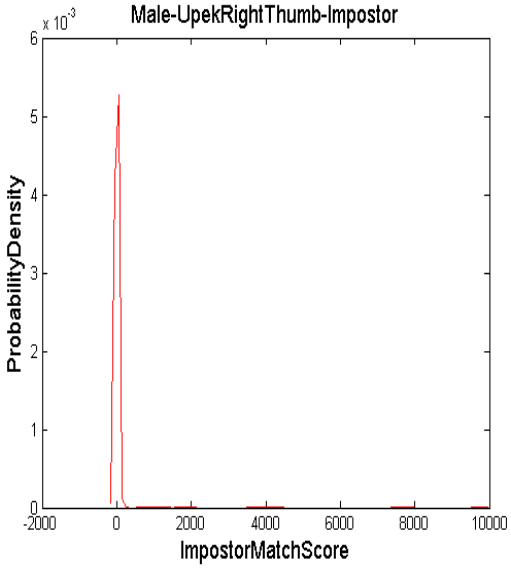
(c)

Figure B.1 (iv): Match score distributions of right index images of male's captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

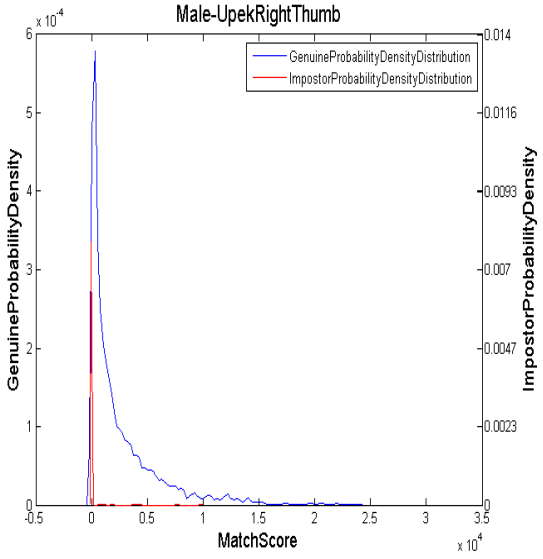
B.1. (v). Upek Eikon Touch 700 – Right Thumb



(a)



(b)

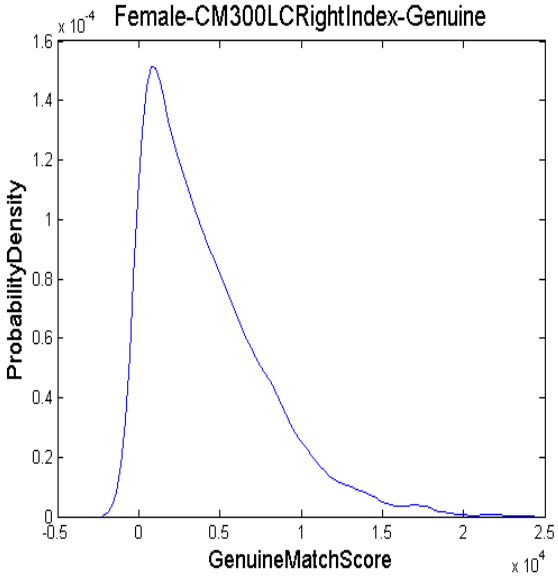


(c)

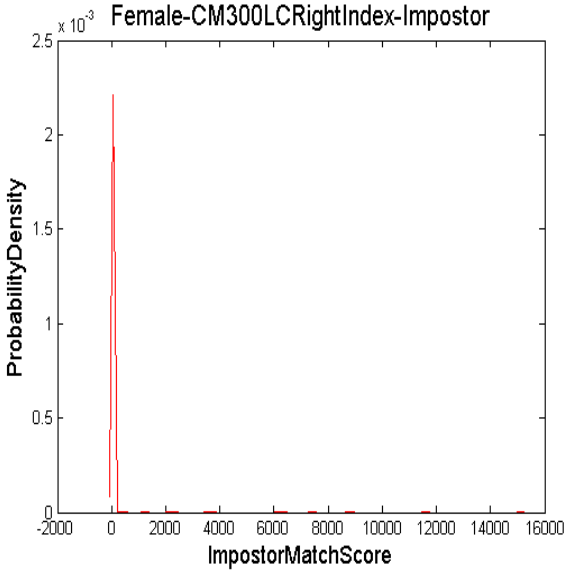
Figure B.1 (v): Match score distributions of right thumb images of male's captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.2) Gender - Female

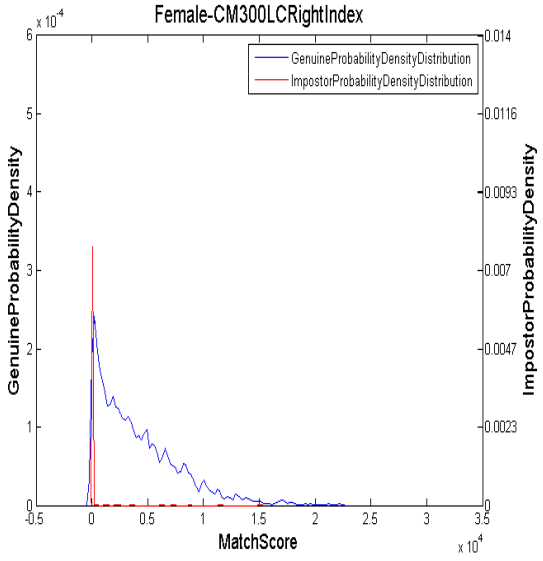
B.2. (i) Crossmatchverifier 300LC- Right Index



(a)



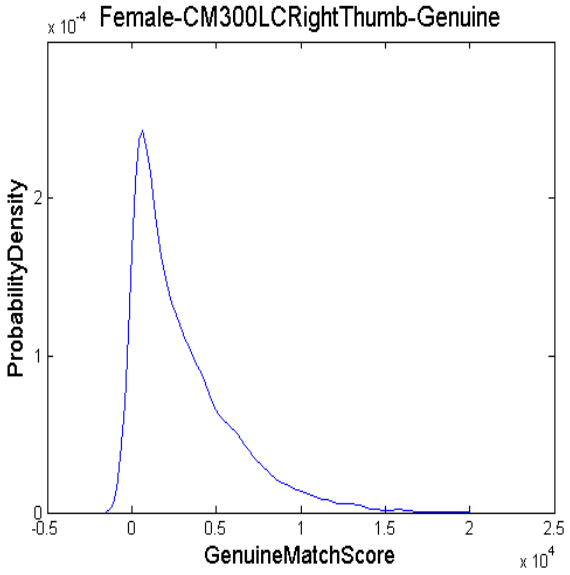
(b)



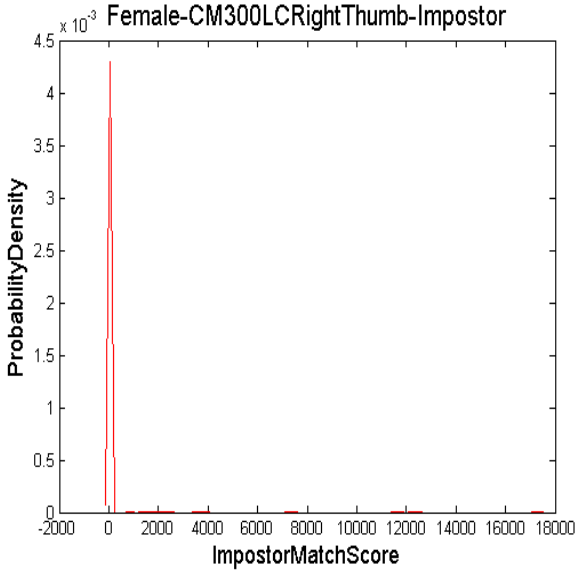
(c)

Figure B.2 (i): Match score distributions of right index images of female's captured using the Crossmatch Verifier 300LC sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

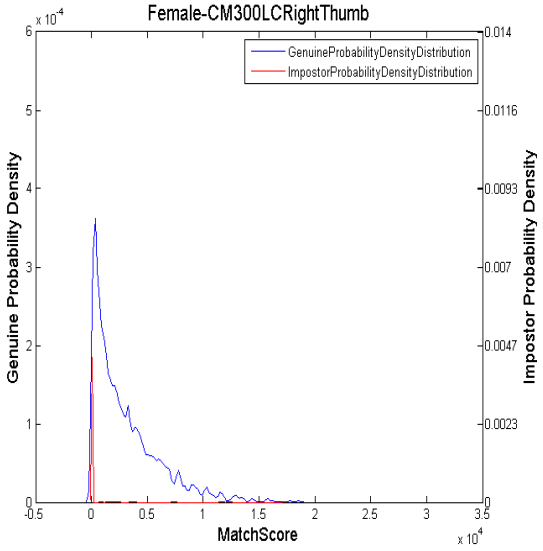
B.2. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



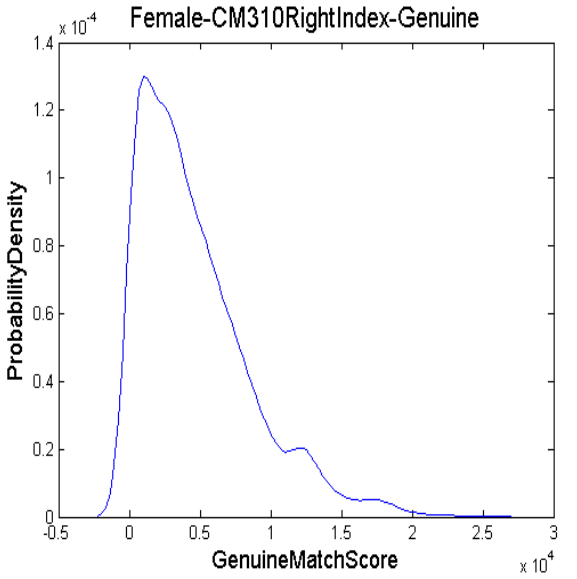
(b)



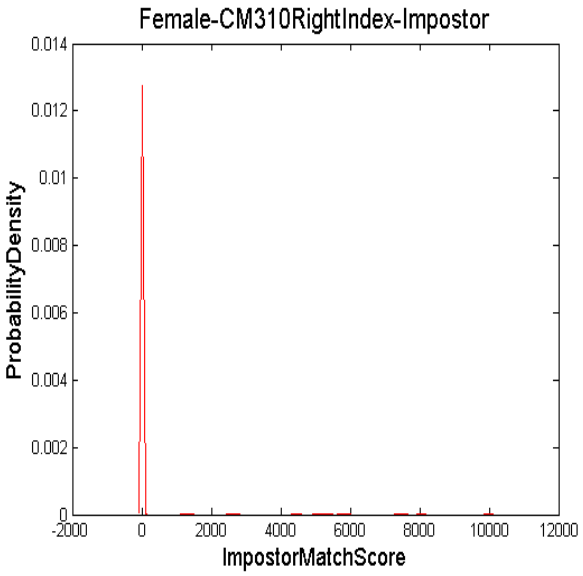
(c)

Figure B.2 (ii): Match score distributions of right thumb images of female's captured using the Crossmatch Verifier 300LC sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

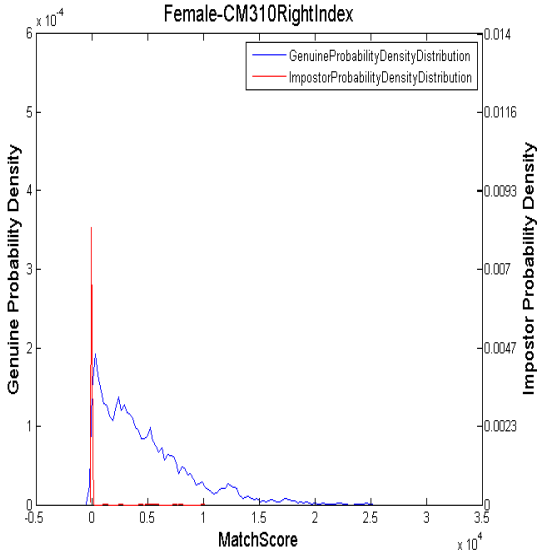
B.2. (iii) Crossmatchverifier 310 – Right Index



(a)



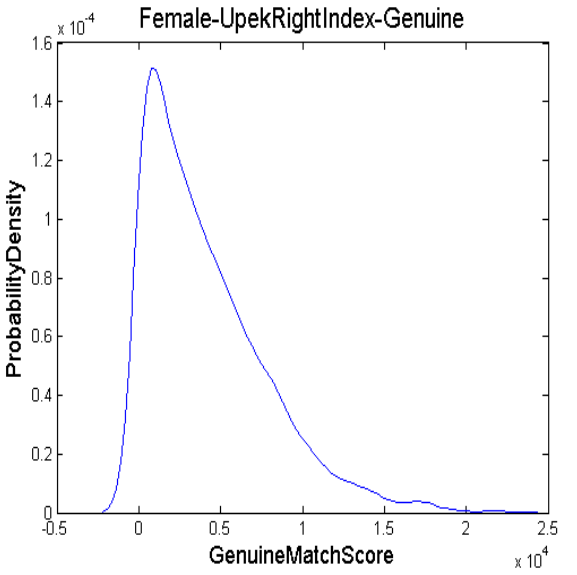
(b)



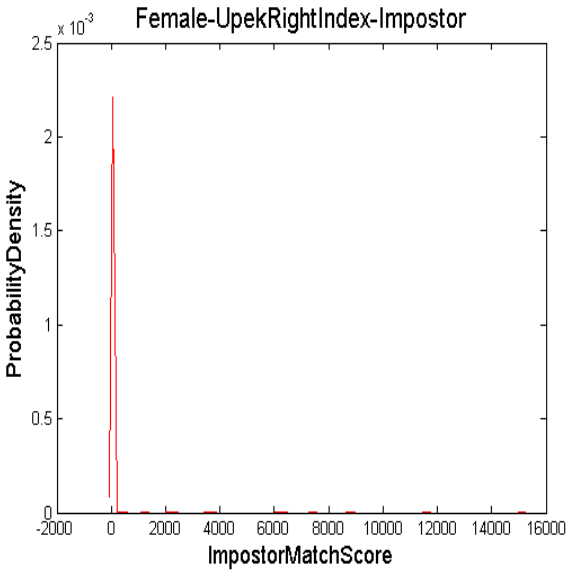
(c)

Figure B.2 (iii): Match score distributions of right index images of female's captured using the Crossmatch Verifier 310 sensor.(a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

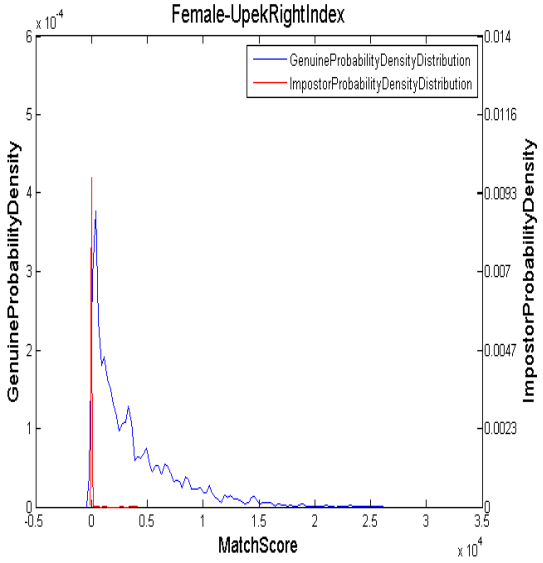
B.2. (iv) Upek Eikon Touch 700 – Right Index



(a)



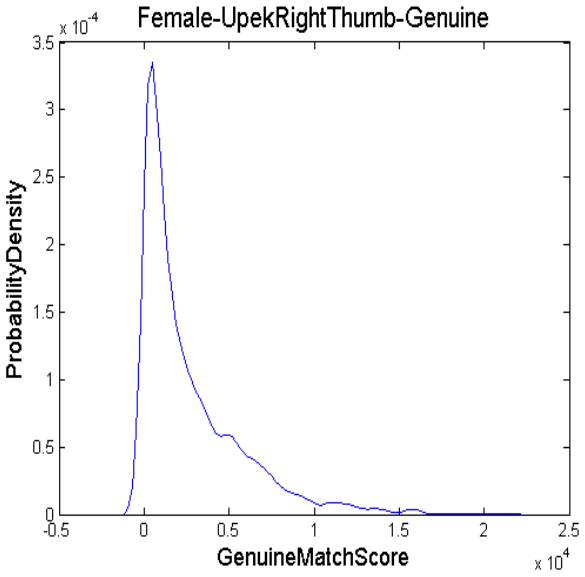
(b)



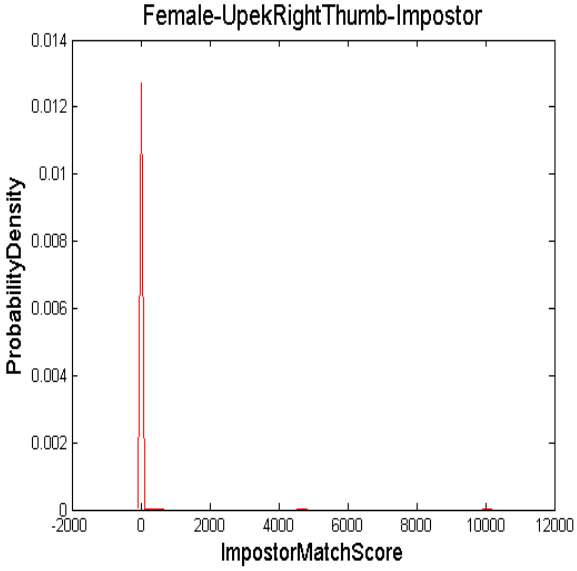
(c)

Figure B.2 (iv): Match score distributions of right index images of female's captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

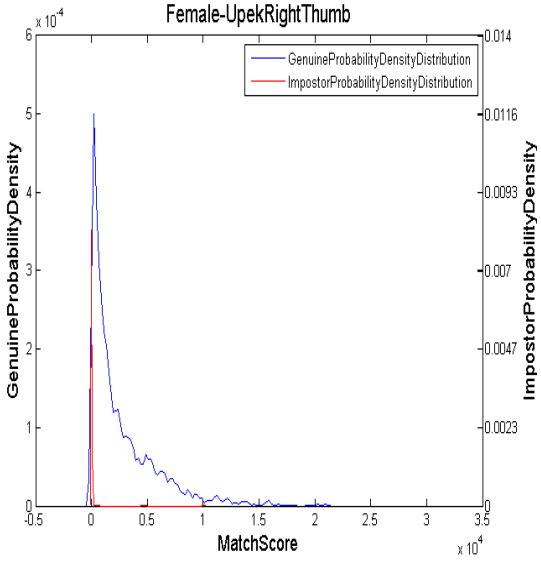
B.2. (v) Upek Eikon Touch 700 – Right Thumb



(a)



(b)



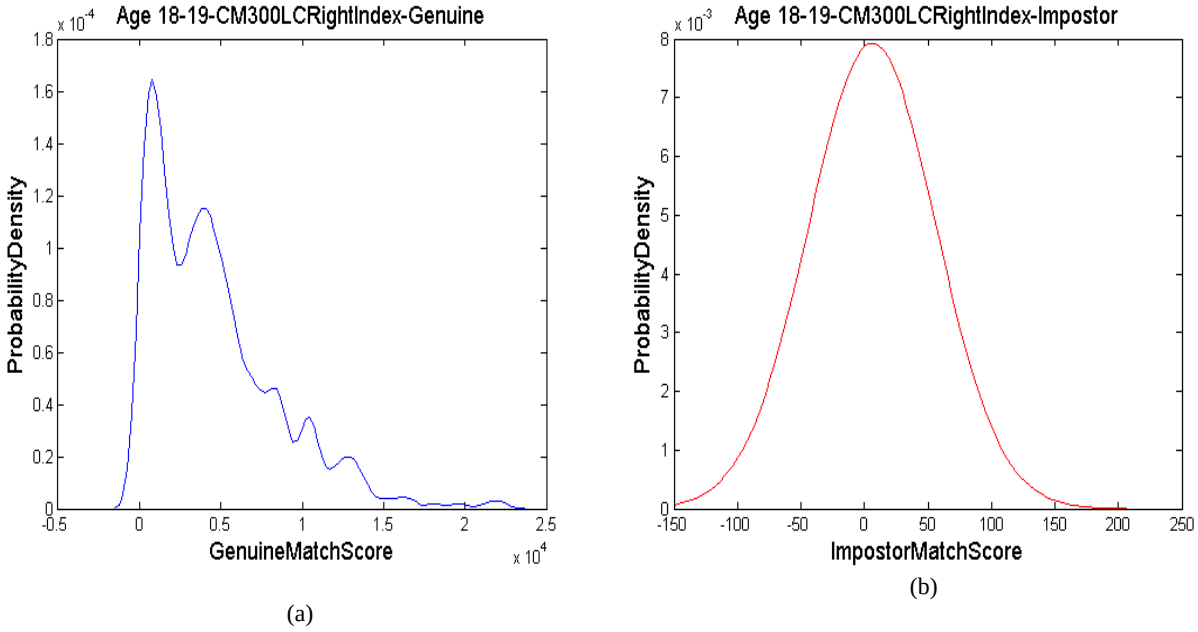
(c)

Figure B.2 (v): Match score distributions of right thumb images of female's captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

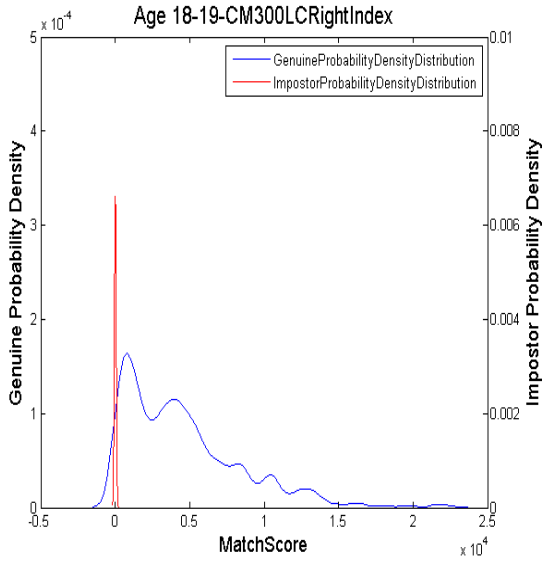
AGE BASED FINGERPRINT MATCH SCORE DISTRIBUTIONS

B.3) Age 18-19

B.3. (i) Crossmatchverifier 300LC – Right Index



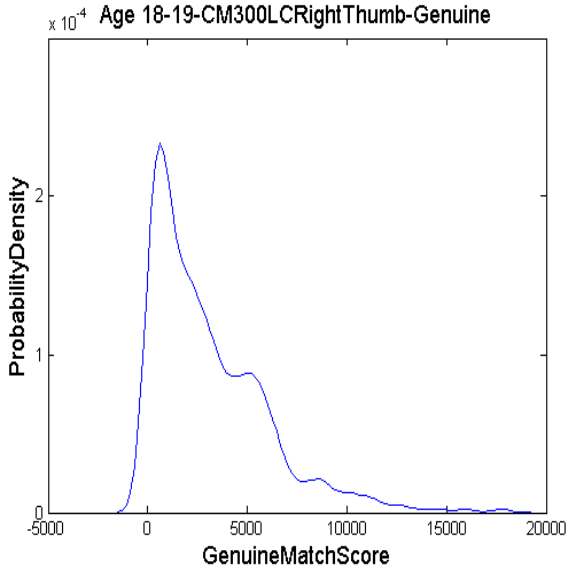
(a) (b)



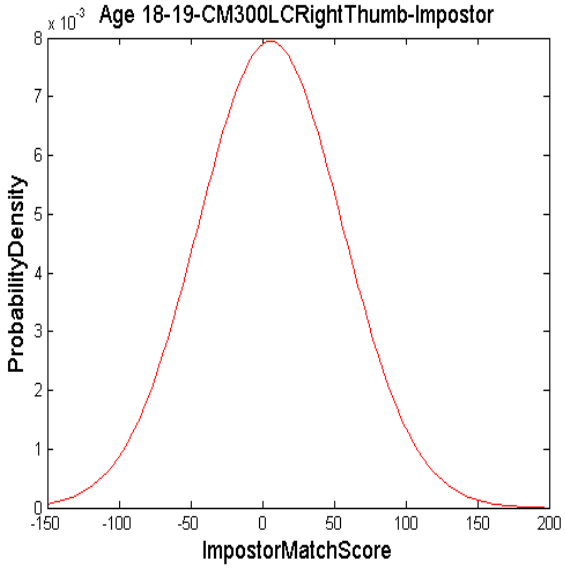
(c)

Figure B.3 (i): Match score distributions of right index images of the age group 18-19 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

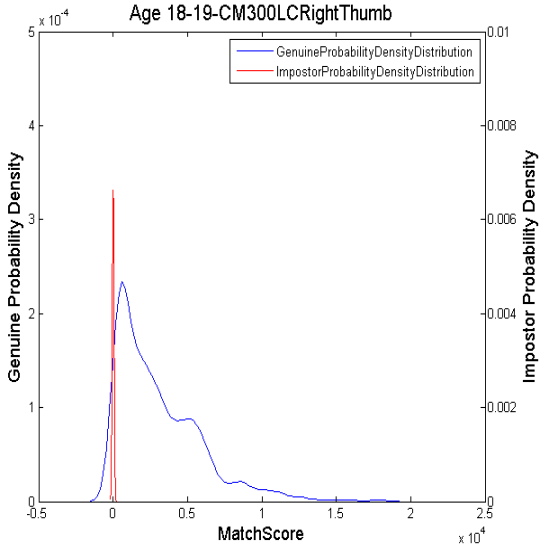
B.3. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



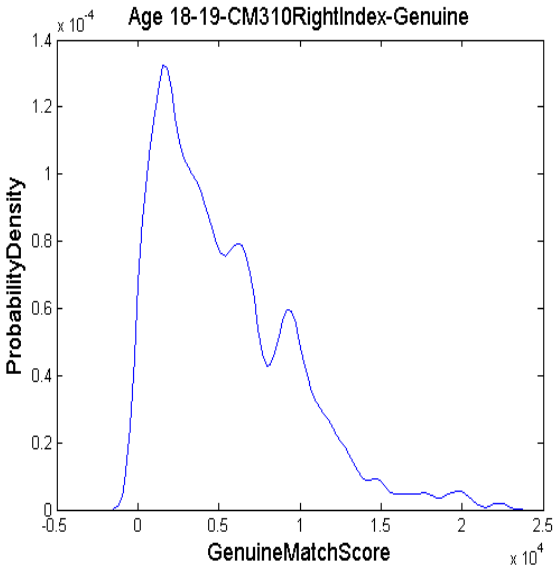
(b)



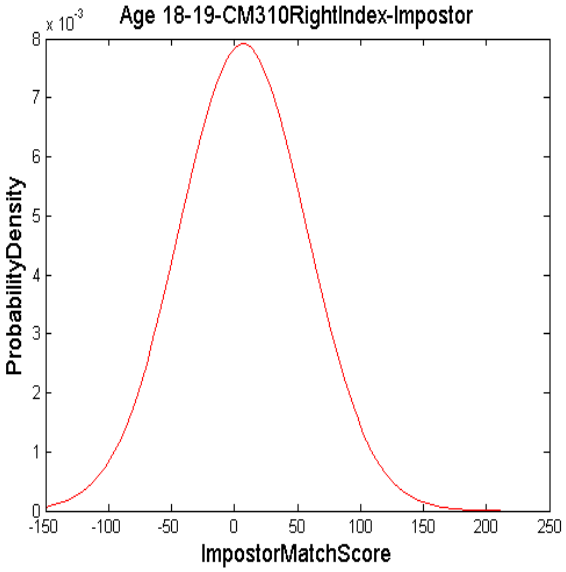
(c)

Figure B.3 (ii): Match score distributions of right thumb images of the age group 18-19 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

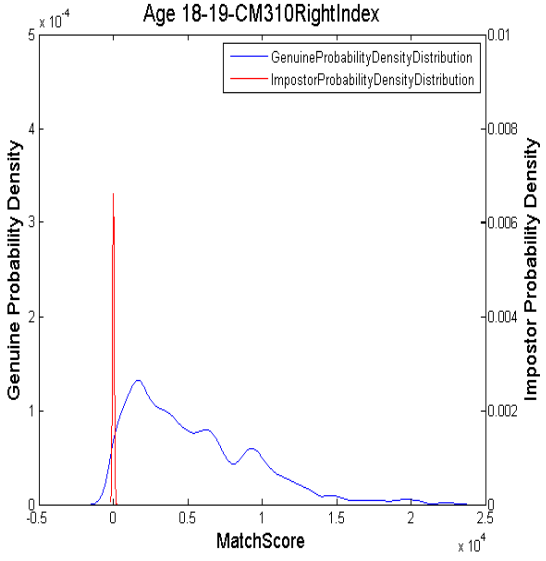
B.3. (iii) Crossmatchverifier 310- Right Index



(a)



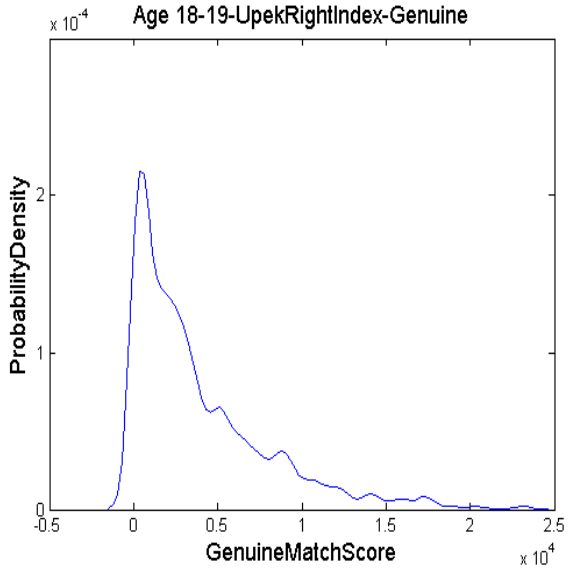
(b)



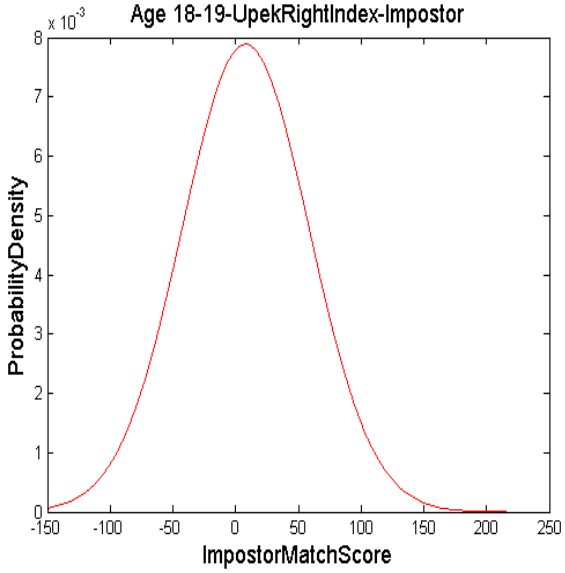
(c)

Figure B.3 (iii): Match score distributions of right index images of the age group 18-19 captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

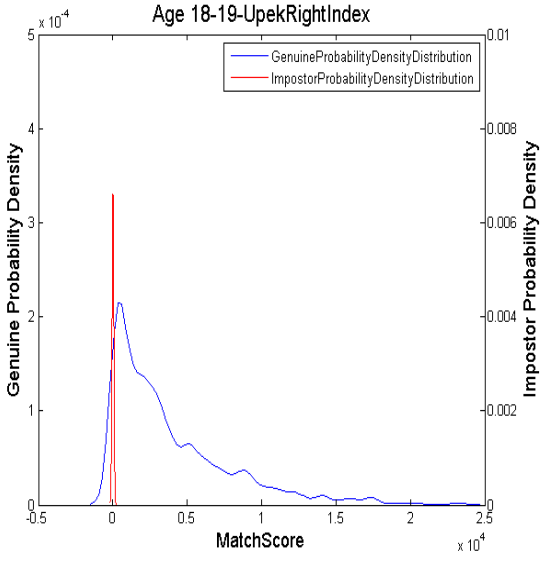
B.3. (iv) Upek Eikon Touch 700- Right Index



(a)



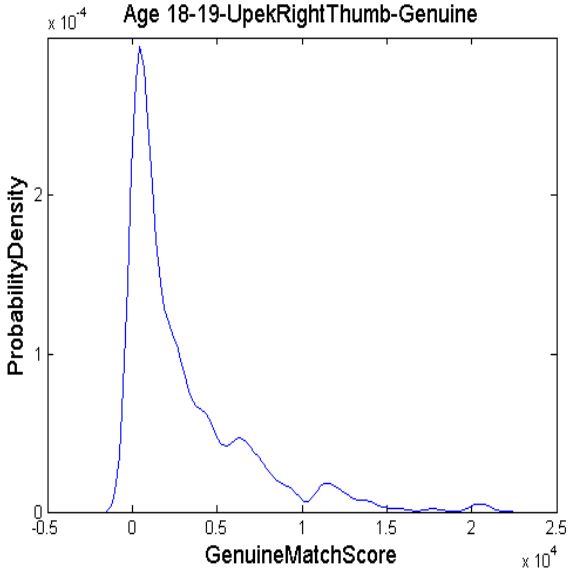
(b)



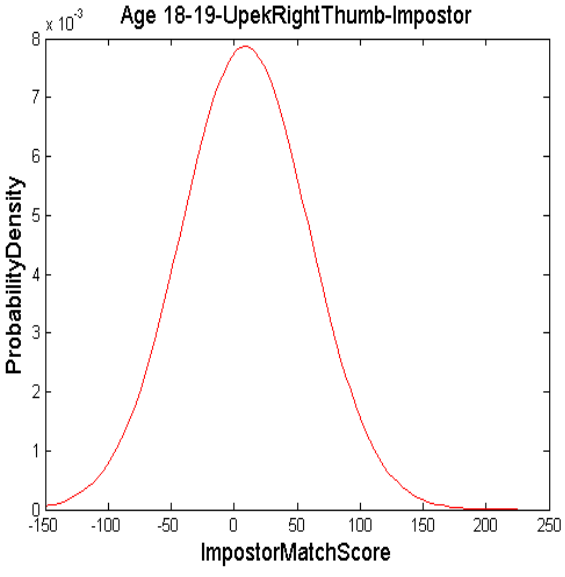
(c)

Figure B.3 (iv): Match score distributions of right index images of the age group 18-19 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

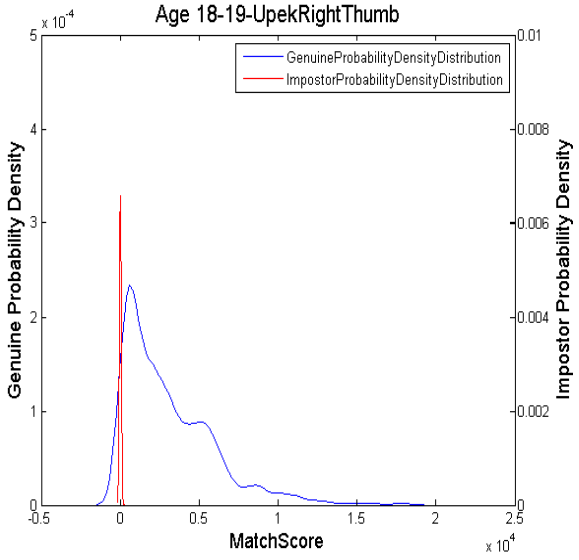
B.3. (v) Upek Eikon Touch 700- Right Thumb



(a)



(b)

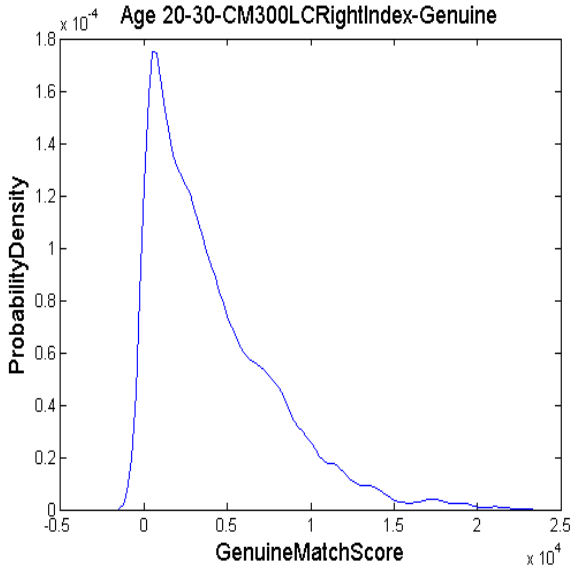


(c)

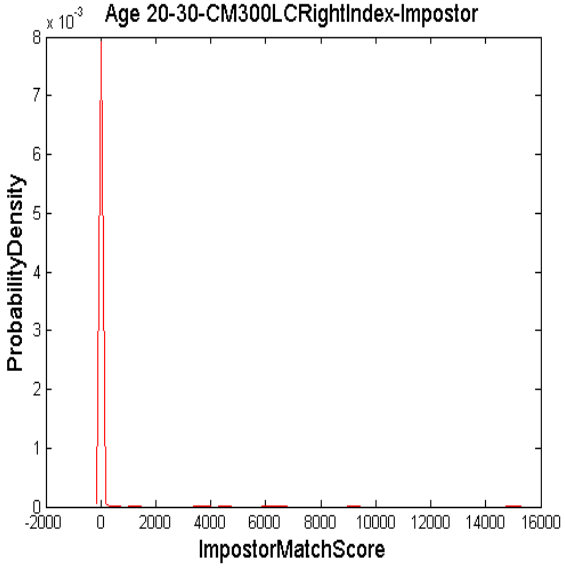
Figure B.3 (v): Match score distributions of right thumb images of the age group 18-19 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.4) Age 20-30

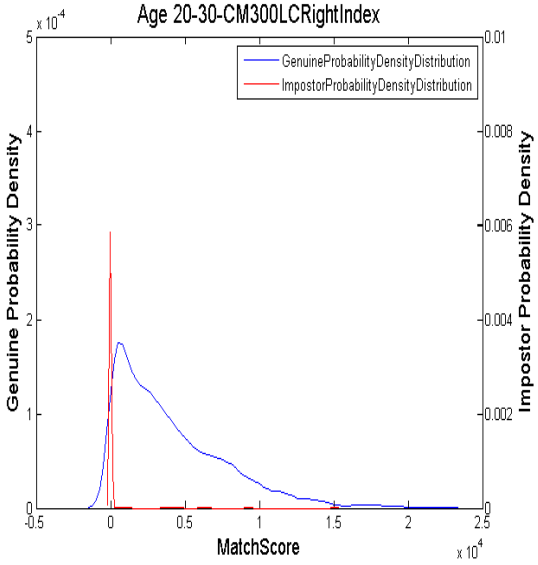
B.4. (i) Crossmatchverifier 300LC- Right Index



(a)



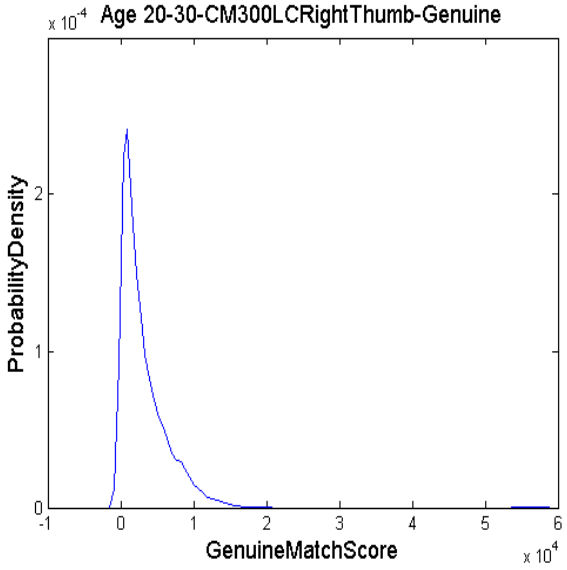
(b)



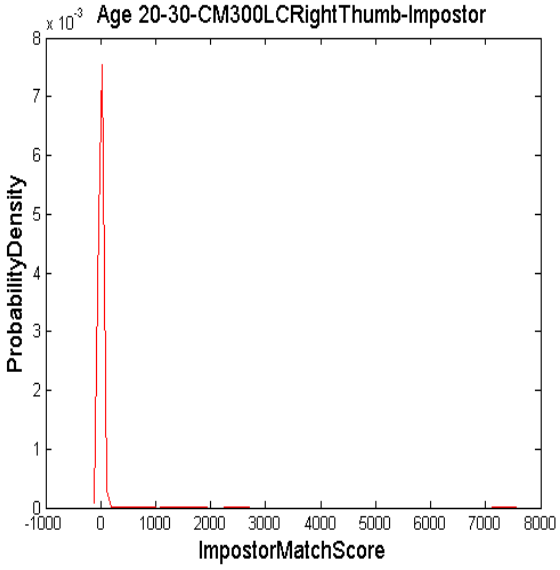
(c)

Figure B.4 (i): Match score distributions of right index images of the age group 20-30 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

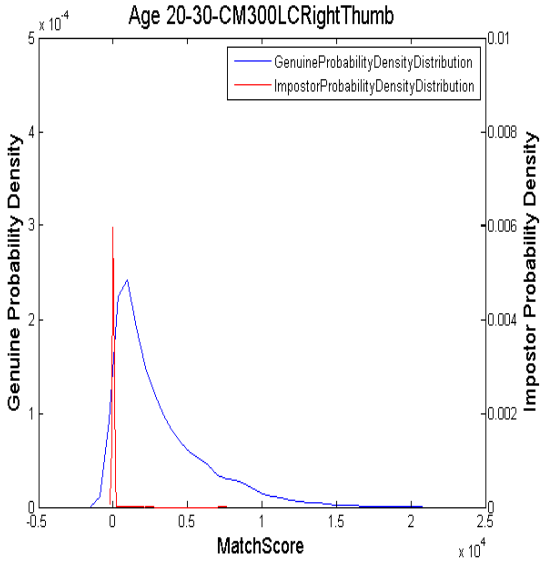
B.4. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



(b)



(c)

Figure B.4 (ii): Match score distributions of right thumb images of the age group 20-30 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.4. (iii) Crossmatchverifier 310 – Right Index

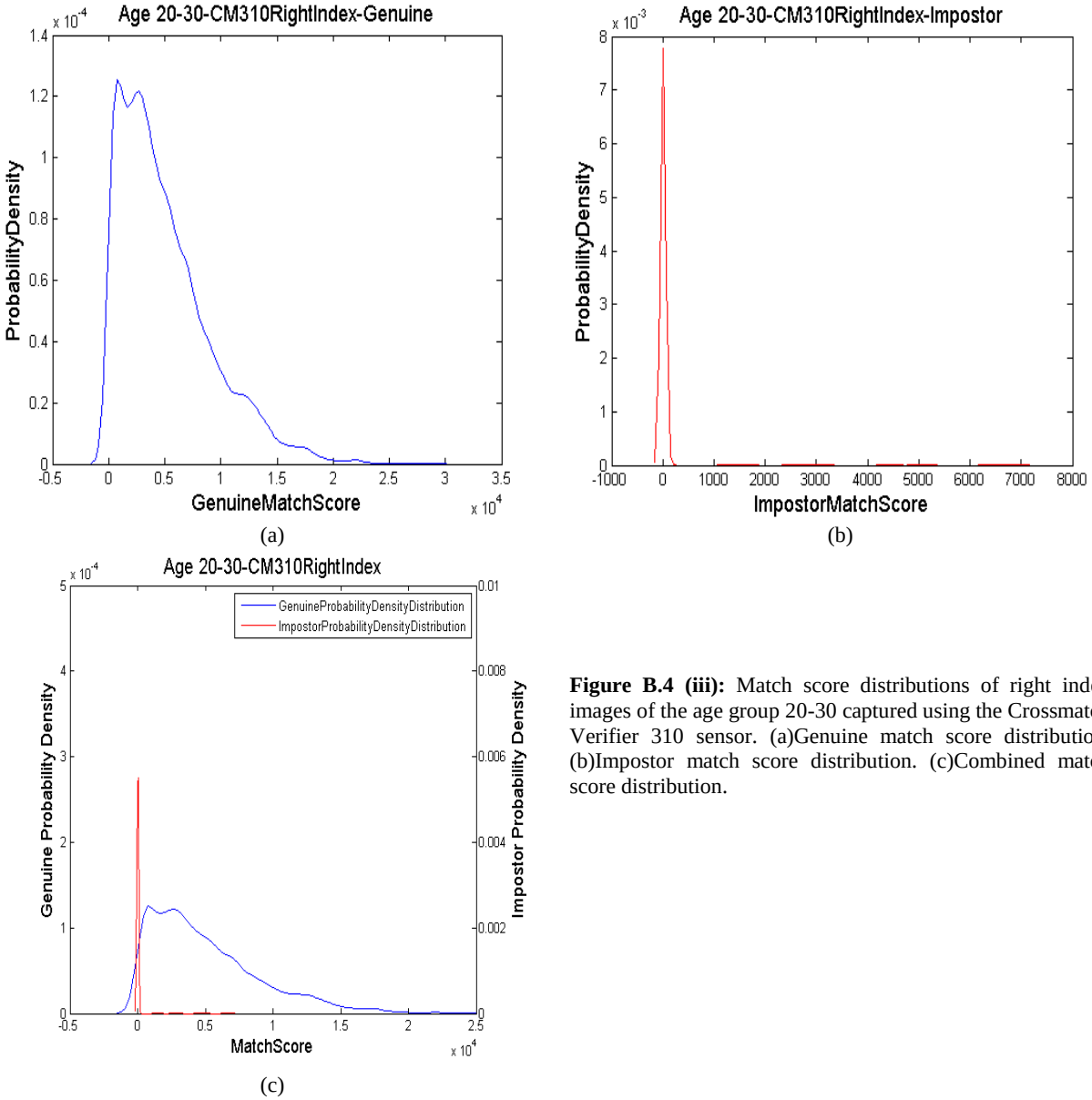


Figure B.4 (iii): Match score distributions of right index images of the age group 20-30 captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.4. (iv) Upek Eikon Touch 700- Right Index

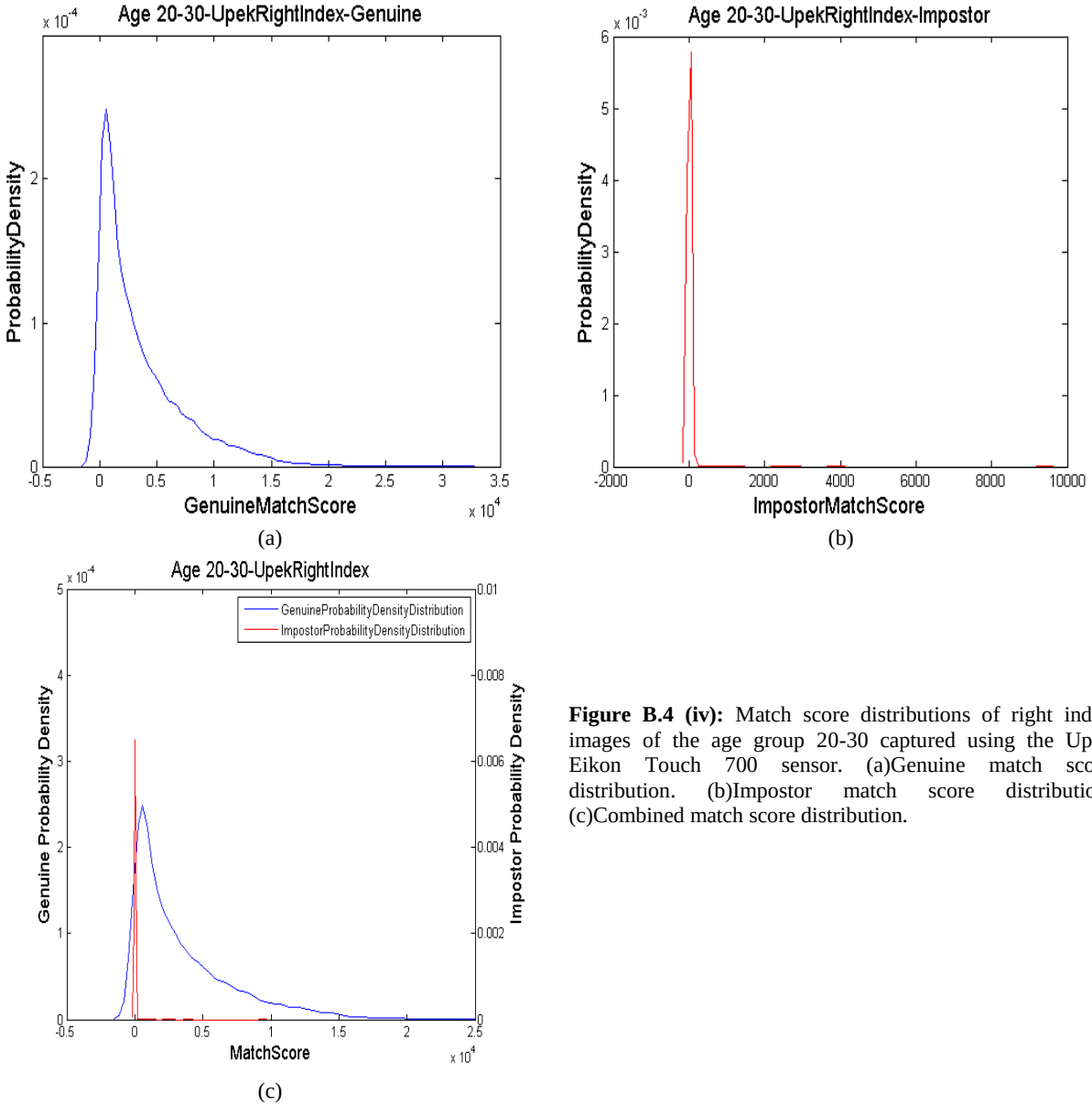
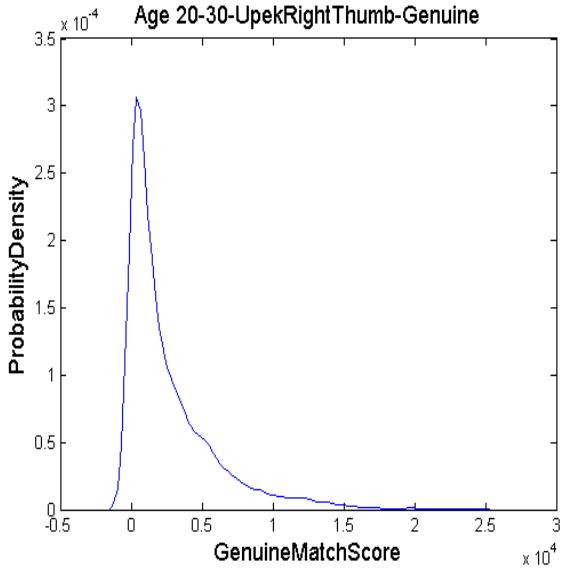
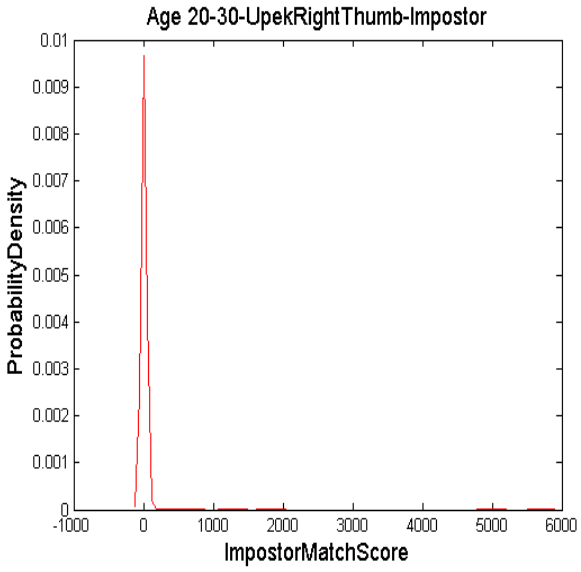


Figure B.4 (iv): Match score distributions of right index images of the age group 20-30 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

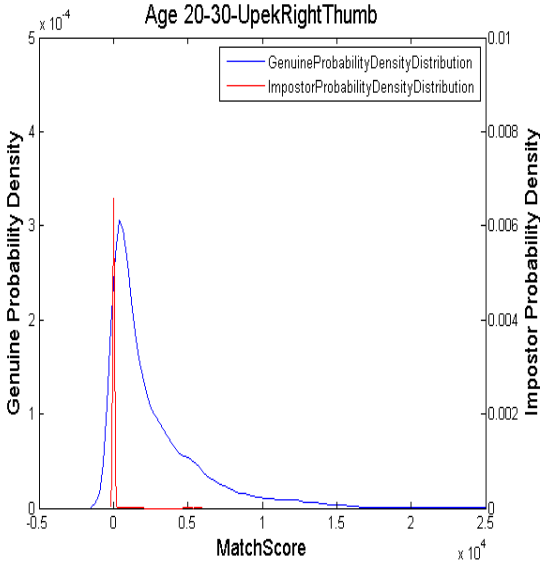
B.4. (v) Upek Eikon Touch 700- Right Thumb



(a)



(b)

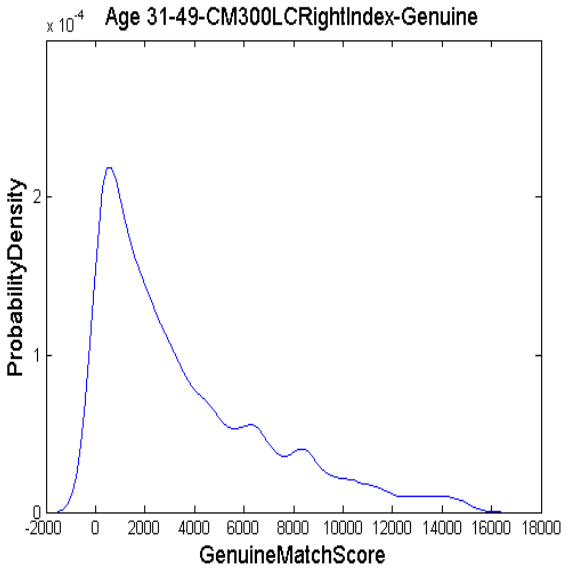


(c)

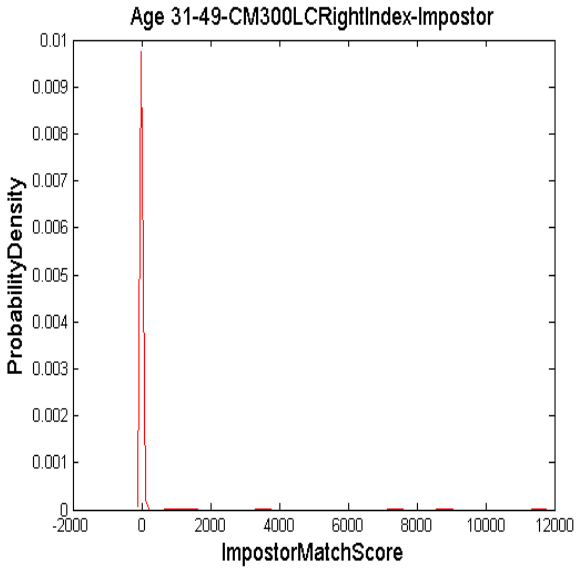
Figure B.4 (v): Match score distributions of right thumb images of the age group 20-30 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.5) Age 31-49

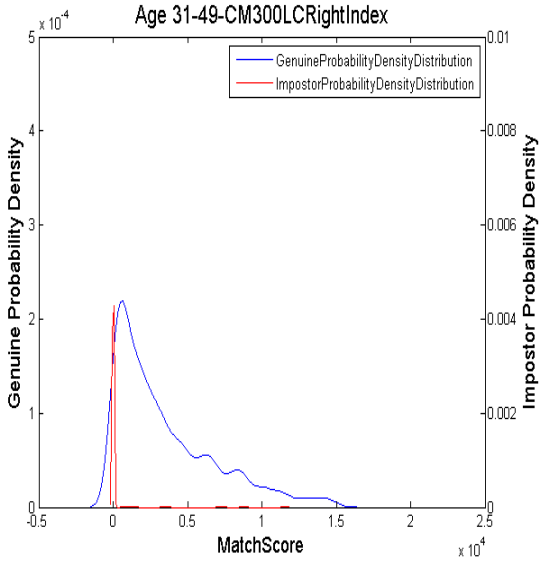
B.5. (i) Crossmatchverifier 300LC- Right Index



(a)



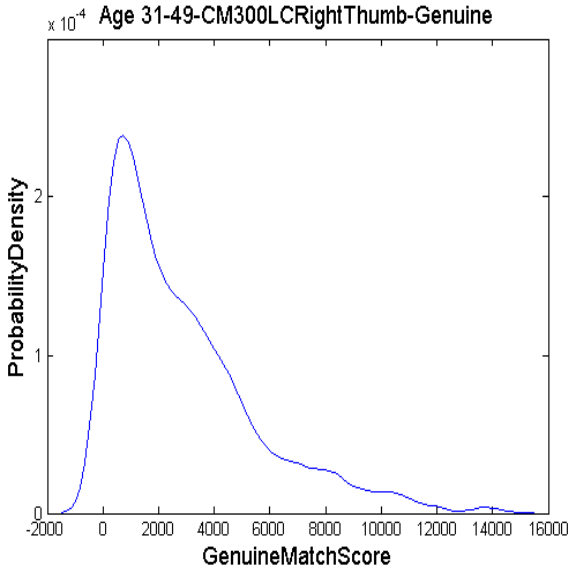
(b)



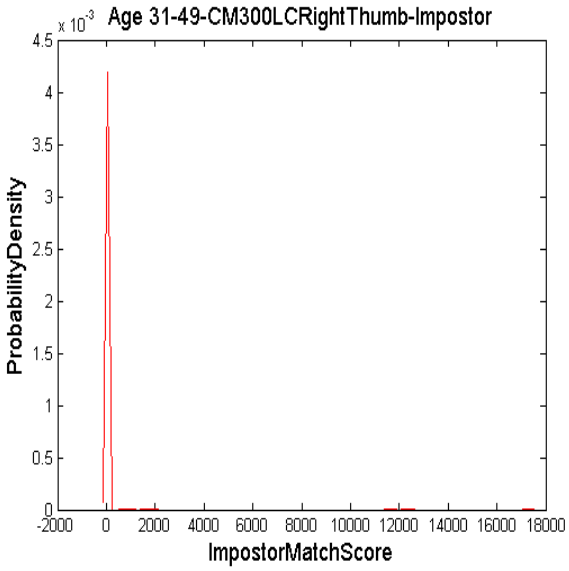
(c)

Figure B.5 (i): Match score distributions of right index images of the age group 31-49 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

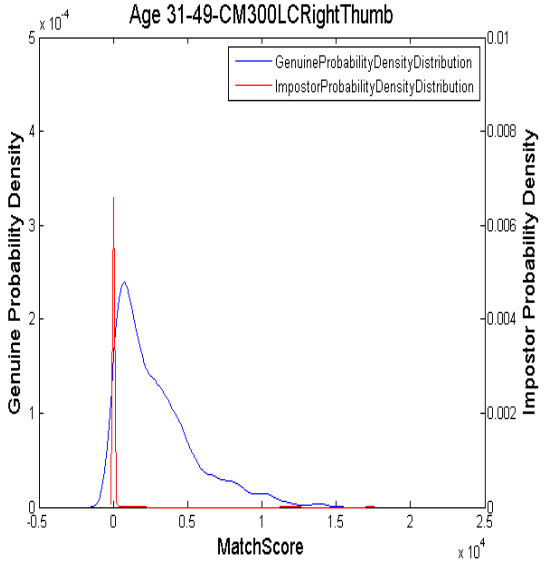
B.5. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



(b)



(c)

Figure B.5 (ii): Match score distributions of right thumb images of the age group 31-49 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.5. (iii) Crossmatchverifier 310-Right Index

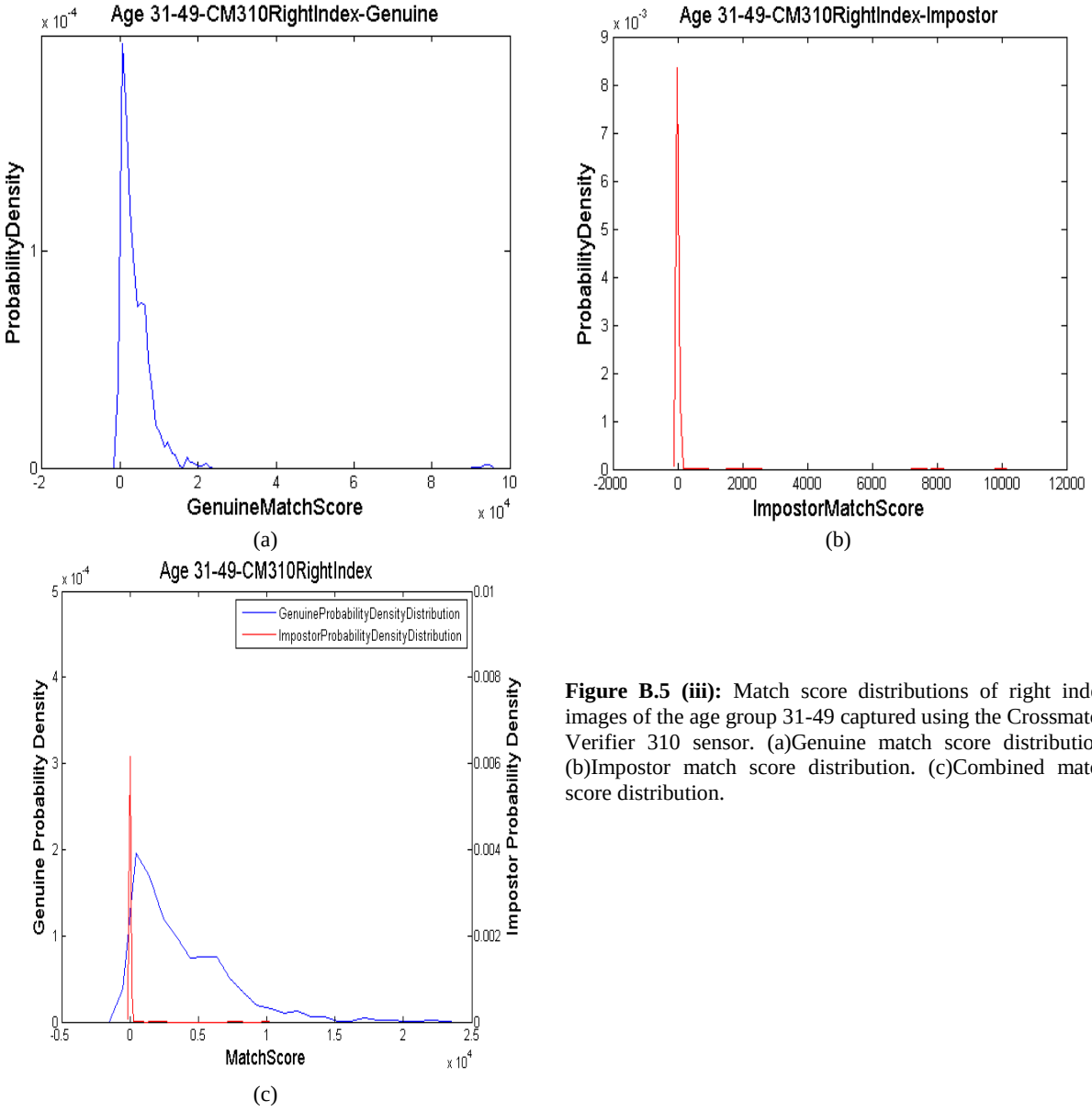
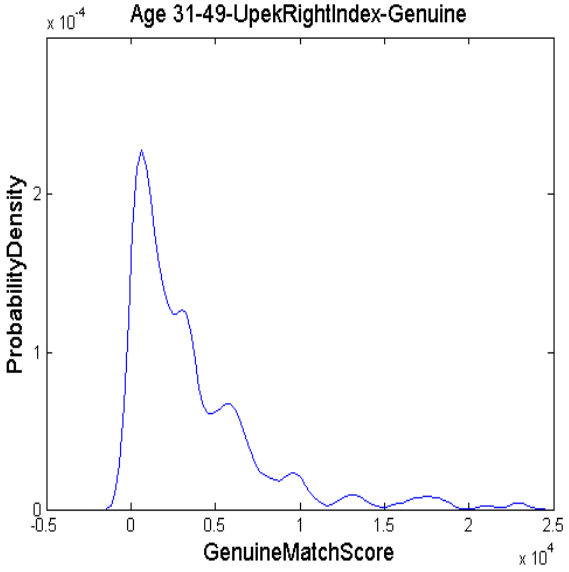
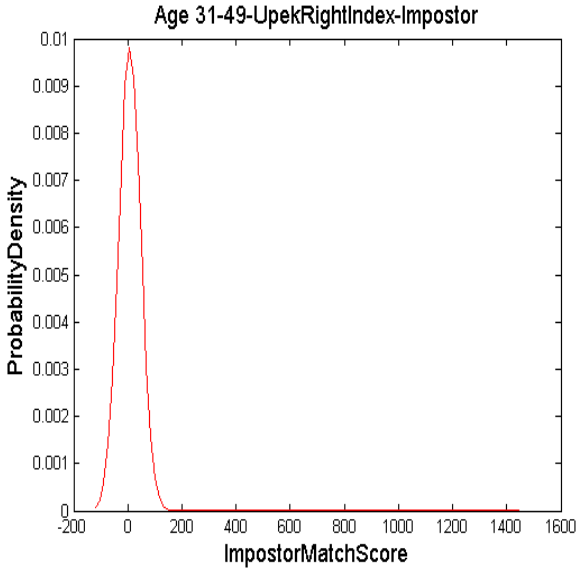


Figure B.5 (iii): Match score distributions of right index images of the age group 31-49 captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

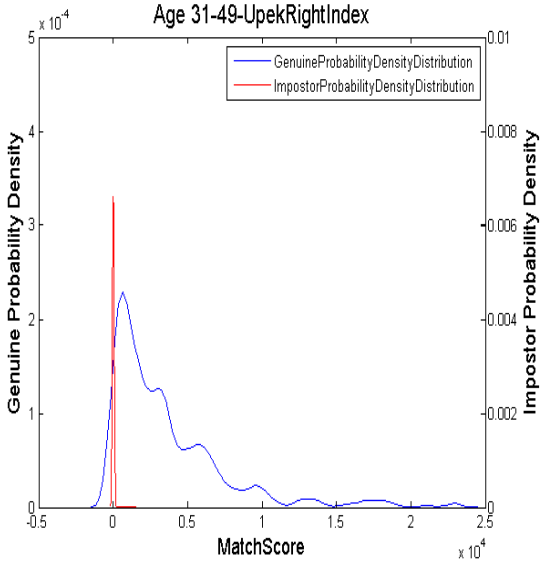
B.5. (iv) Upek Eikon Touch 700-Right Index



(a)



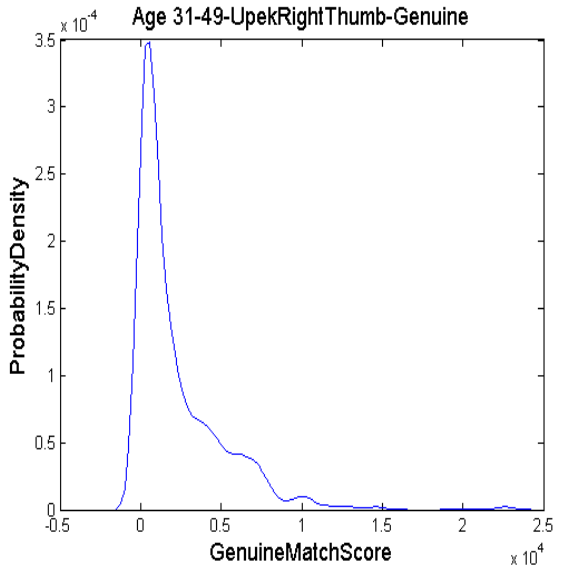
(b)



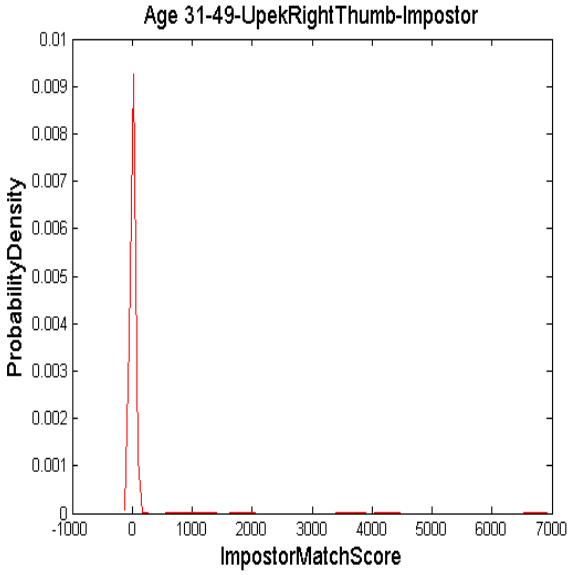
(c)

Figure B.5 (iv): Match score distributions of right index images of the age group 31-49 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

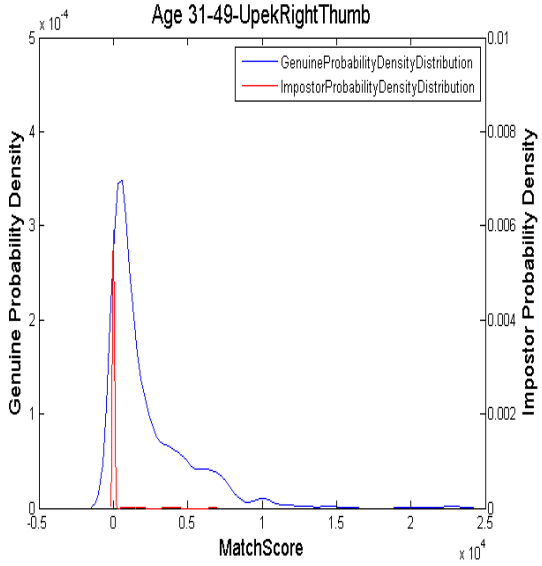
B.5. (v) Upek Eikon Touch 700-Right Thumb



(a)



(b)

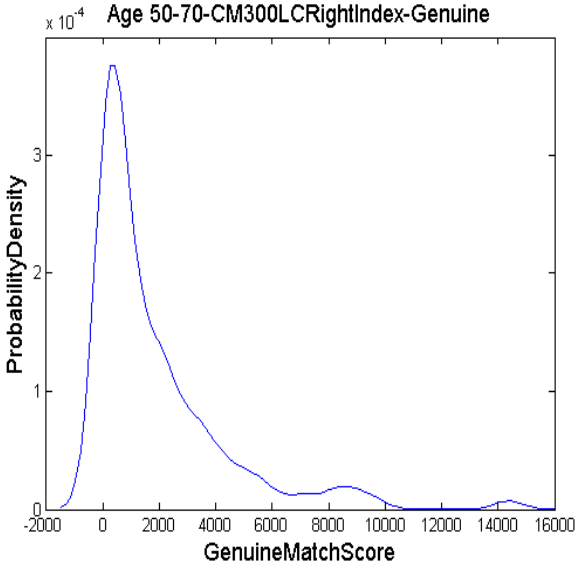


(c)

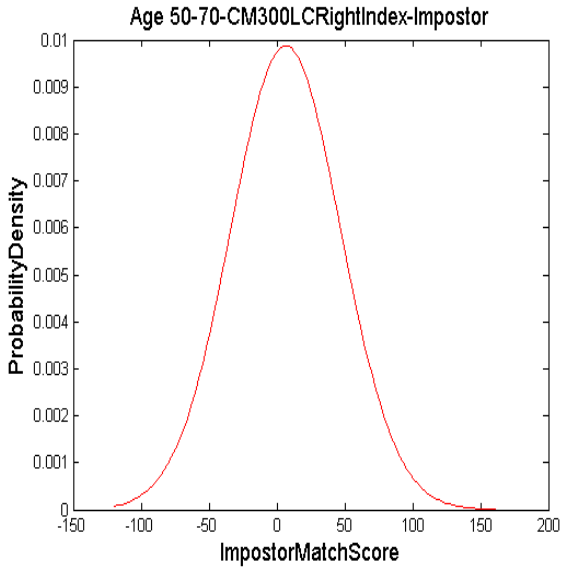
Figure B.5 (v): Match score distributions of right thumb images of the age group 31-49 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.6) Age 50-70

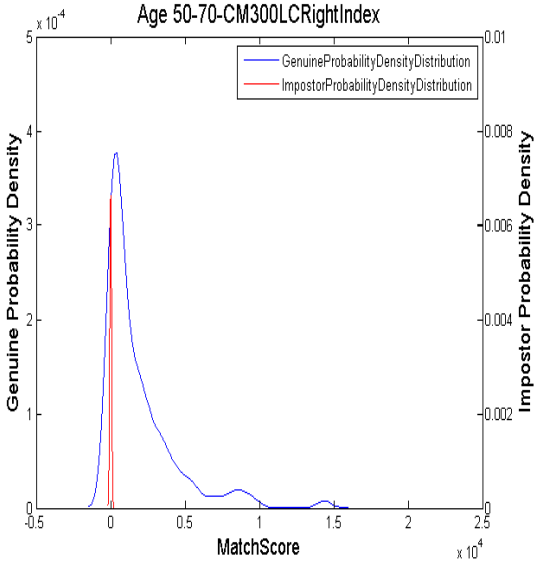
B.6. (i) Crossmatchverifier 300LC-Right Index



(a)



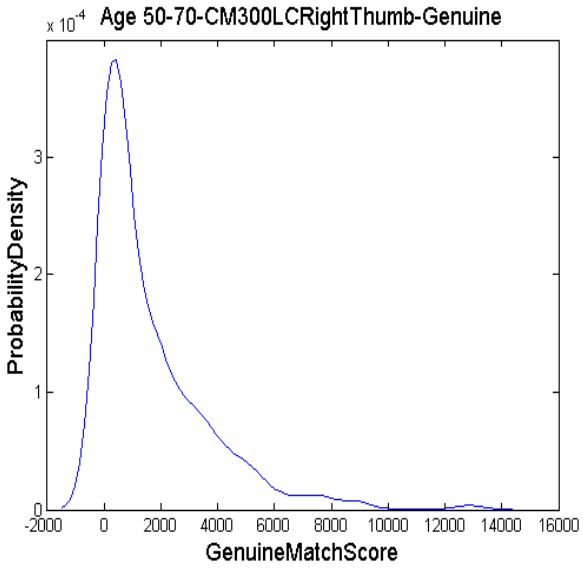
(b)



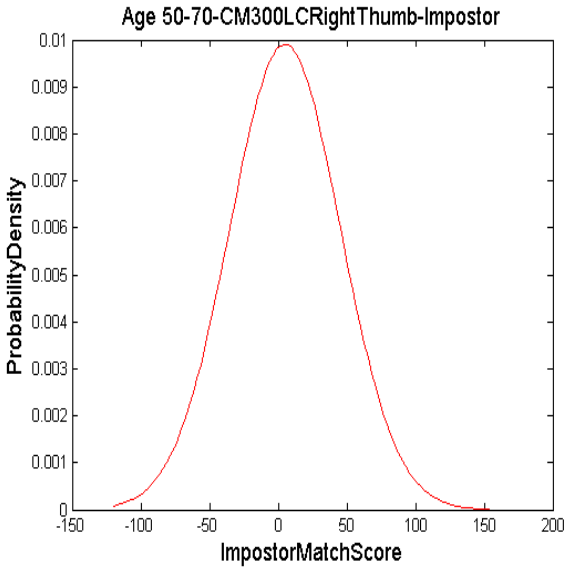
(c)

Figure B.6 (i): Match score distributions of right index images of the age group 50-70 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

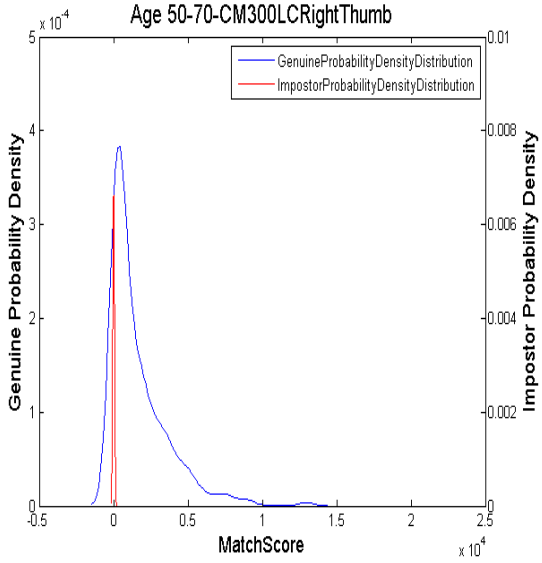
B.6. (ii) Crossmatchverifier 300LC-Right Thumb



(a)



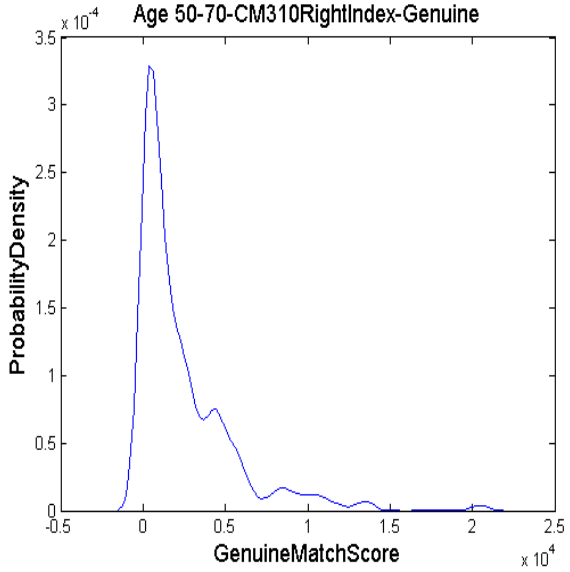
(b)



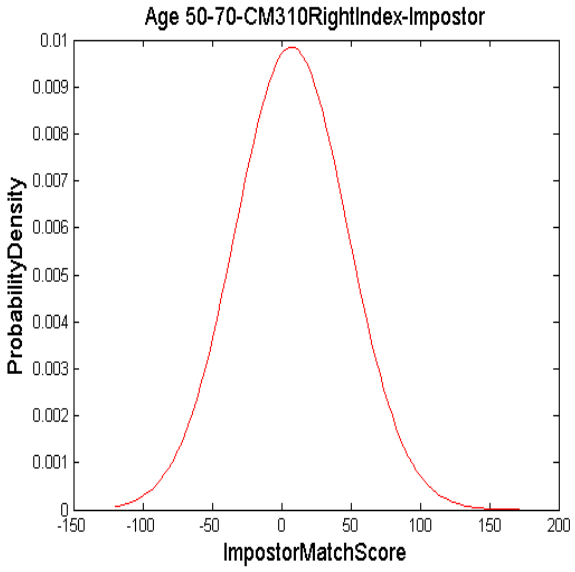
(c)

Figure B.6 (ii): Match score distributions of right thumb images of the age group 50-70 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

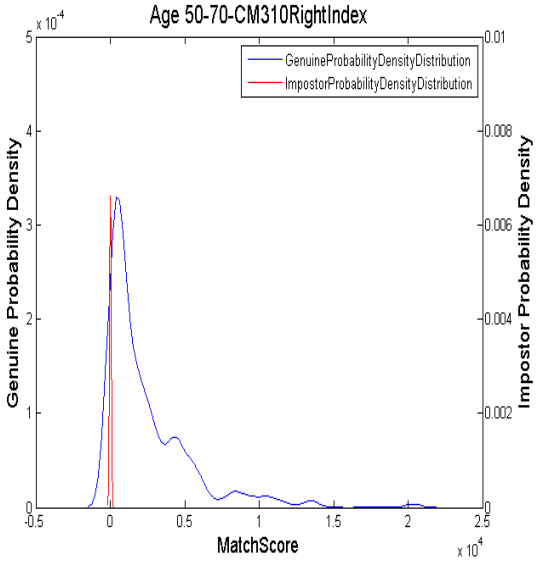
B.6. (iii) Crossmatchverifier 310-Right Index



(a)



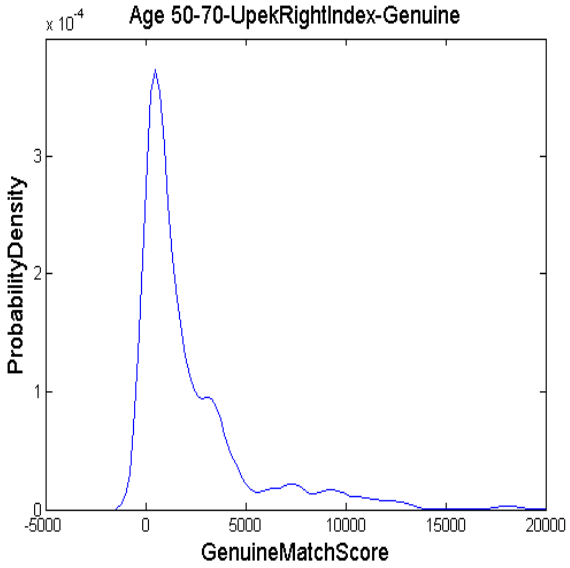
(b)



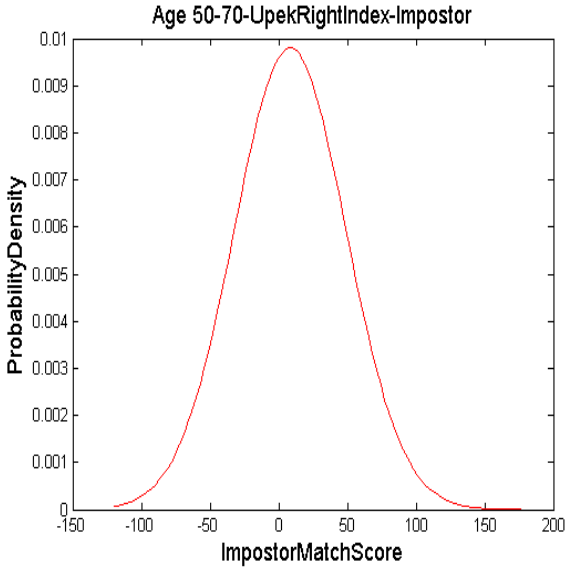
(c)

Figure B.6 (iii): Match score distributions of right index images of the age group 50-70 captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

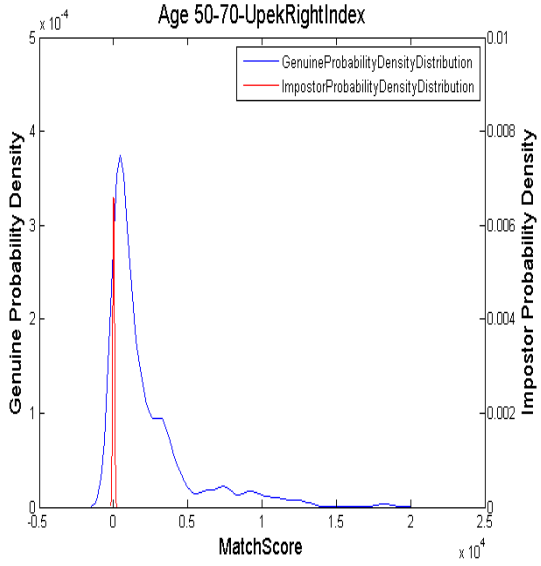
B.6. (iv) Upek Eikon Touch 700-Right Index



(a)



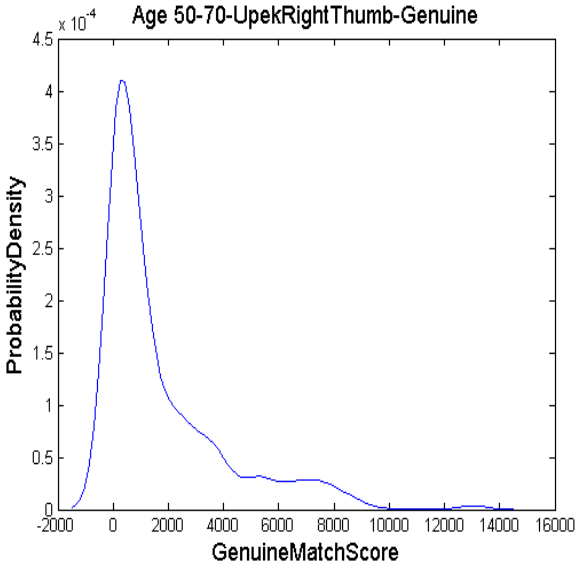
(b)



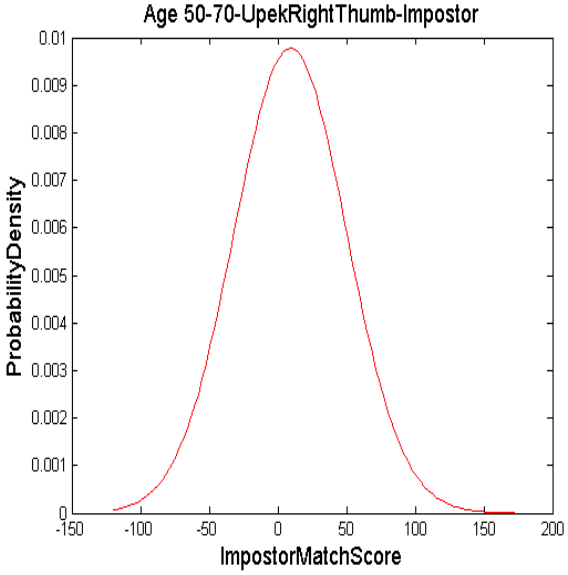
(c)

Figure B.6 (iv): Match score distributions of right index images of the age group 50-70 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

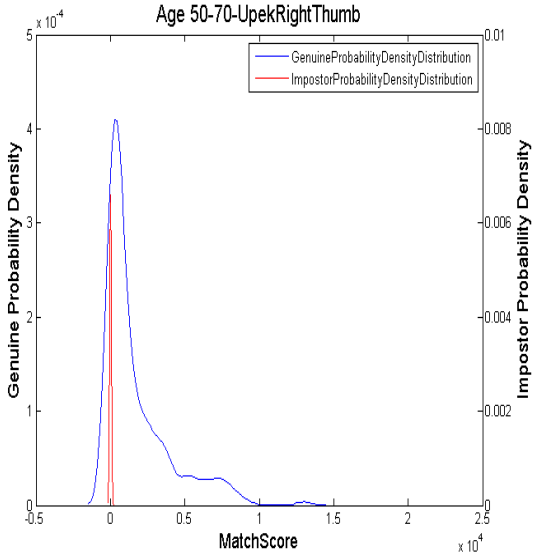
B.6. (v) Upek Eikon Touch 700-Right Thumb



(a)



(b)

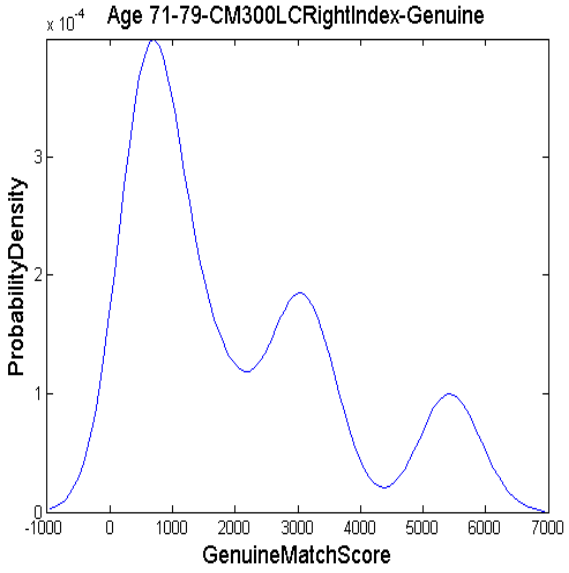


(c)

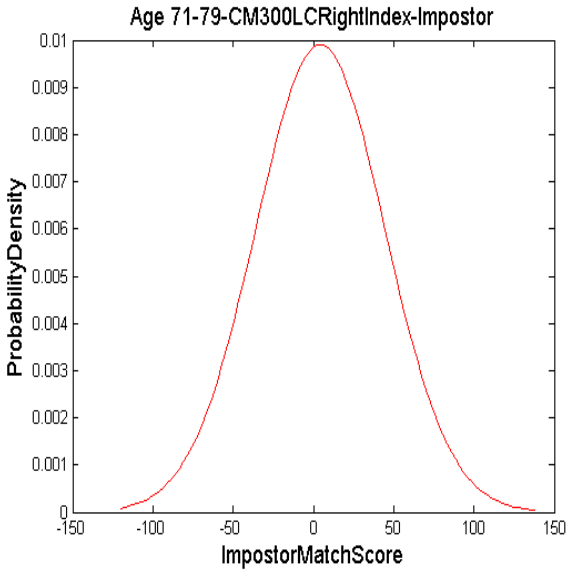
Figure B.6 (v): Match score distributions of right thumb images of the age group 50-70 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.7) Age 71-79

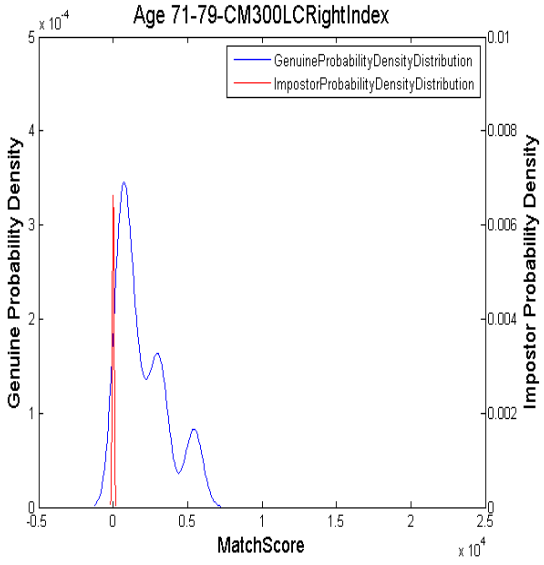
B.7. (i) Crossmatchverifier 300LC- Right Index



(a)



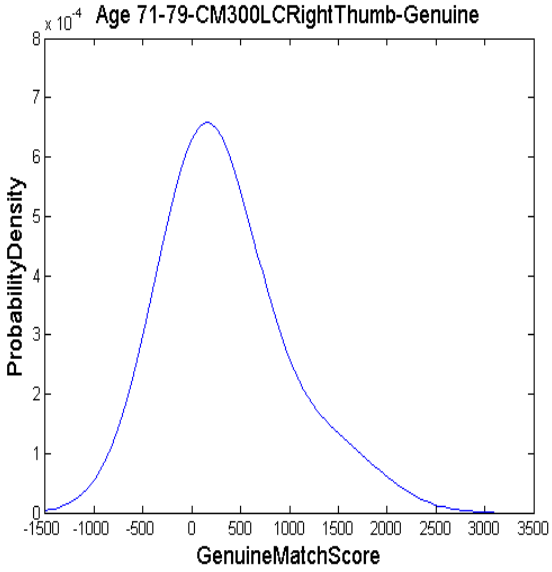
(b)



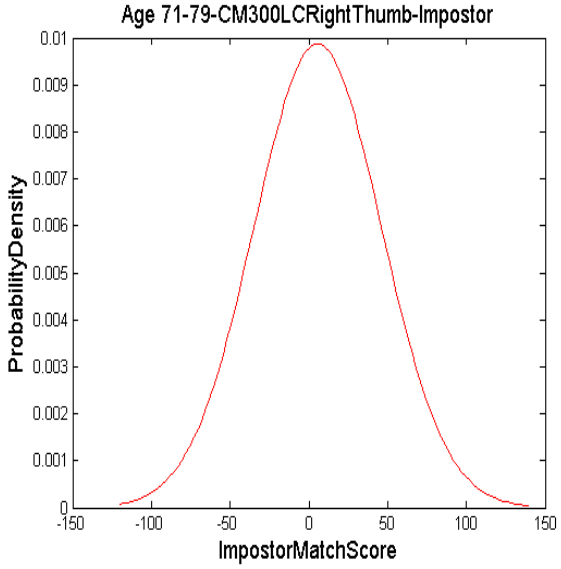
(c)

Figure B.7 (i): Match score distributions of right index images of the age group 71-79 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

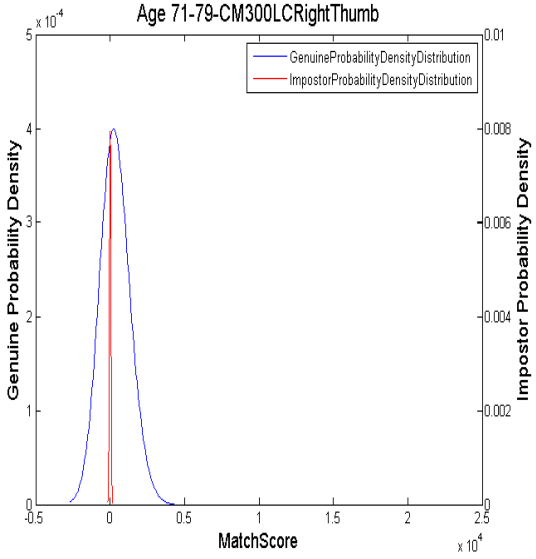
B.7. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



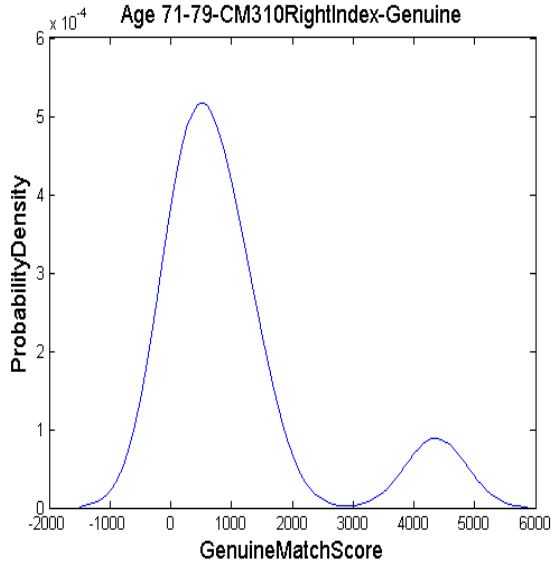
(b)



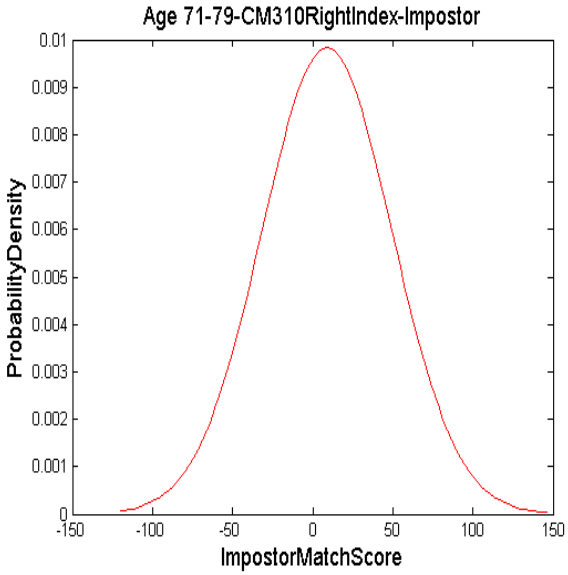
(c)

Figure B.7 (ii): Match score distributions of right thumb images of the age group 71-79 captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

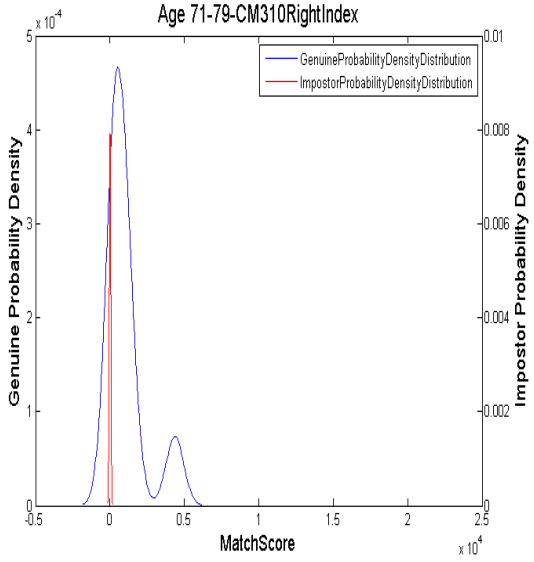
B.7. (iii) Crossmatchverifier 310- Right Index



(a)



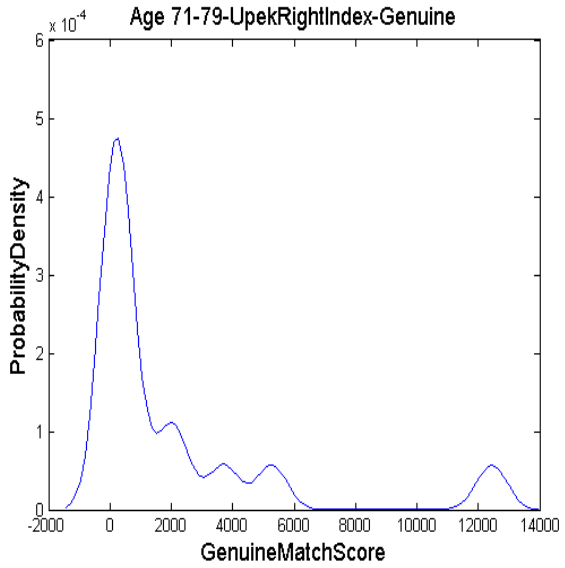
(b)



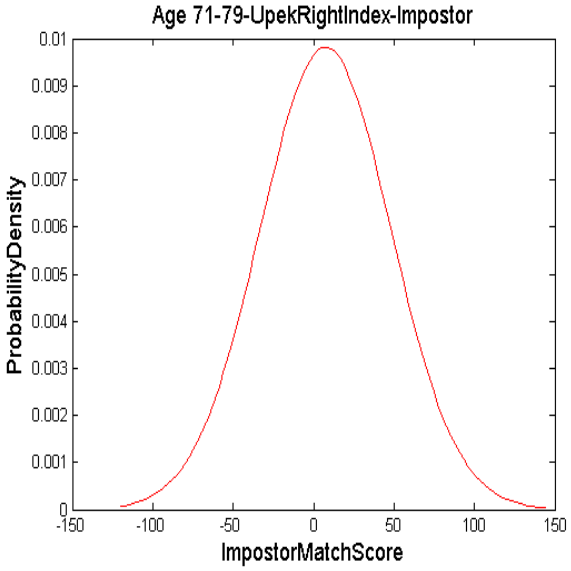
(c)

Figure B.7 (iii): Match score distributions of right index images of the age group 71-79 captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

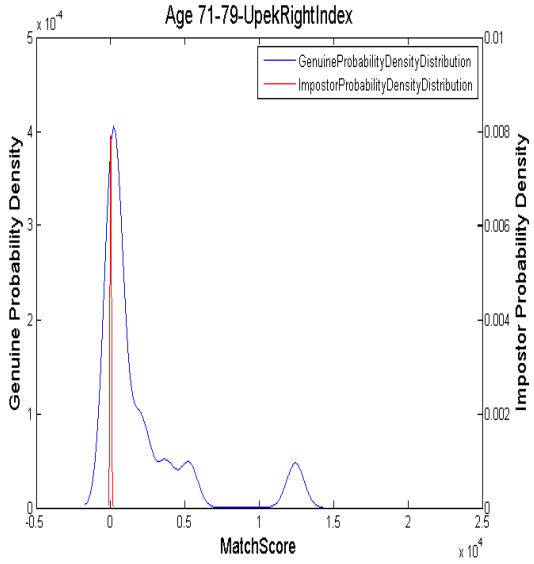
B.7. (iv) Upek Eikon Touch 700- Right Index



(a)



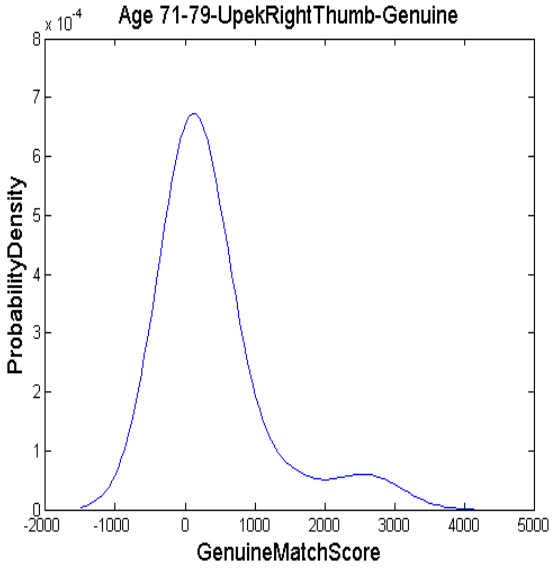
(b)



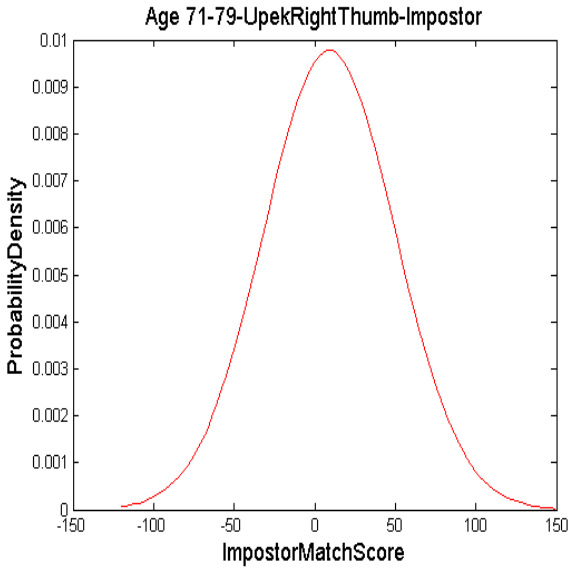
(c)

Figure B.7 (iv): Match score distributions of right index images of the age group 71-79 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

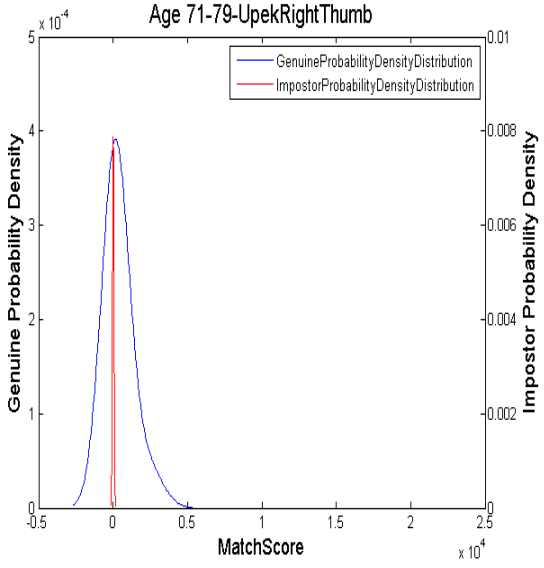
B.7. (v) Upek Eikon Touch 700- Right Thumb



(a)



(b)



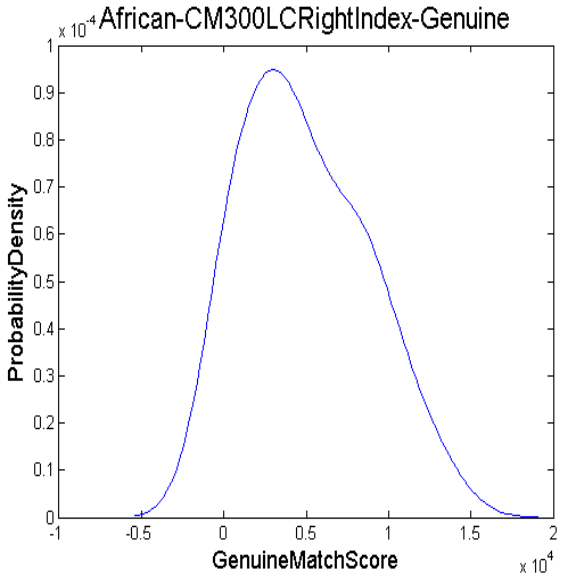
(c)

Figure B.7 (v): Match score distributions of right thumb images of the age group 71-79 captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

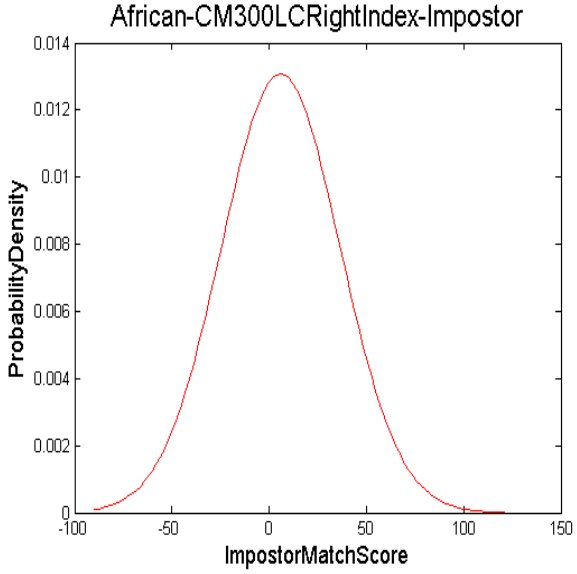
ETHNICITY BASED FINGERPRINT MATCH SCORE DISTRIBUTIONS

B.8) African

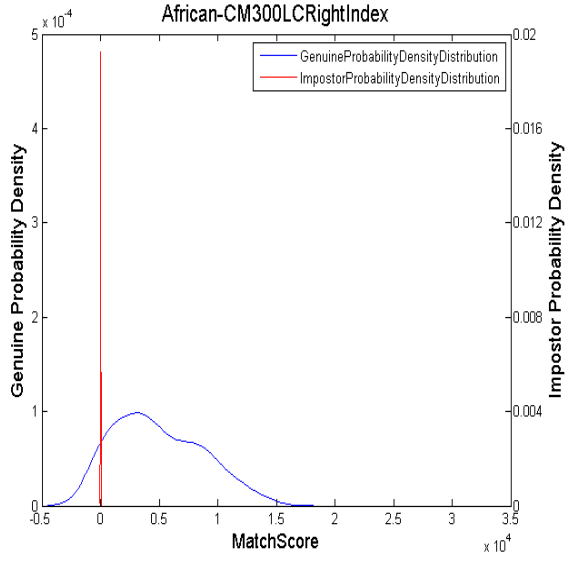
B.8. (i) Crossmatchverifier 300LC-Right Index



(a)



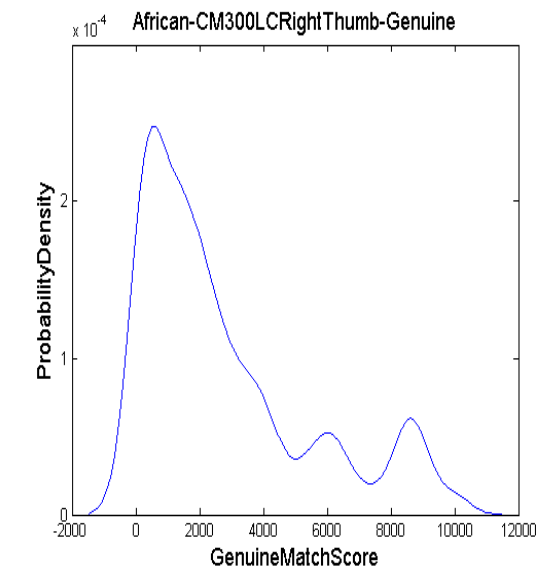
(b)



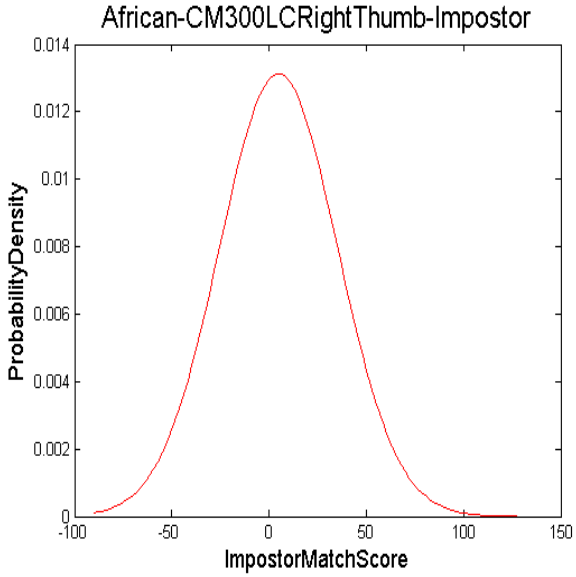
(c)

Figure B.8 (i): Match score distributions of right index images of African ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

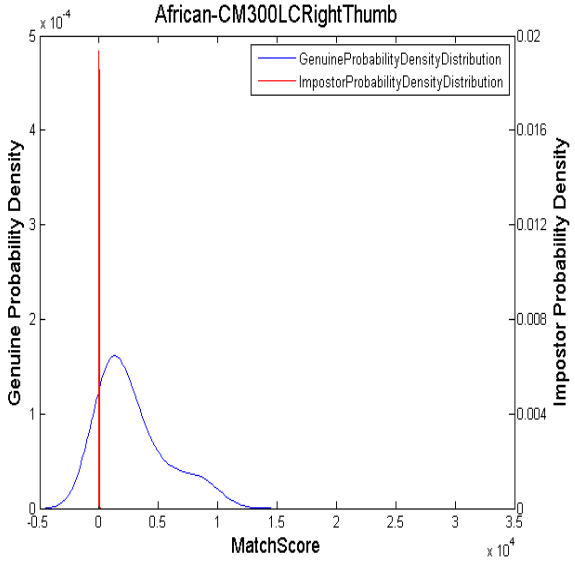
B.8. (ii) Crossmatchverifier 300LC-Right Thumb



(a)



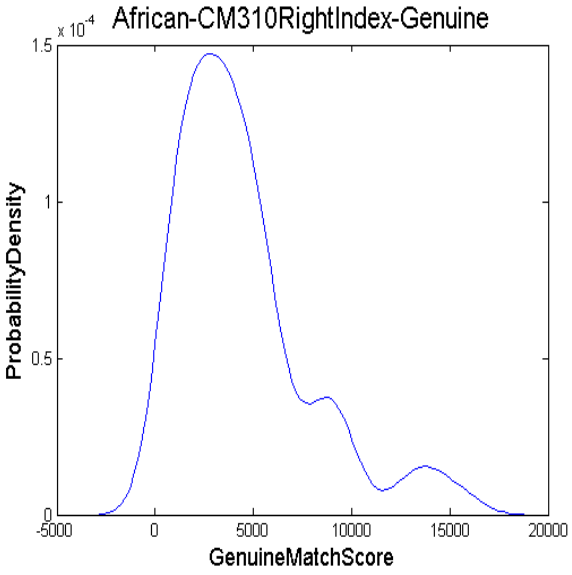
(b)



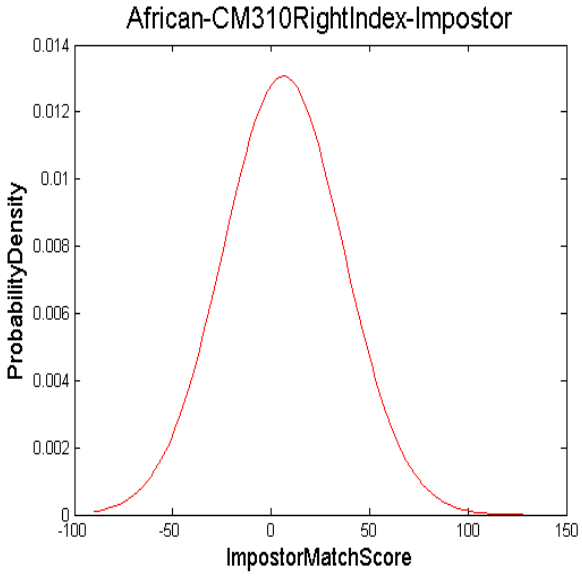
(c)

Figure B.8 (ii): Match score distributions of right thumb images of African ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

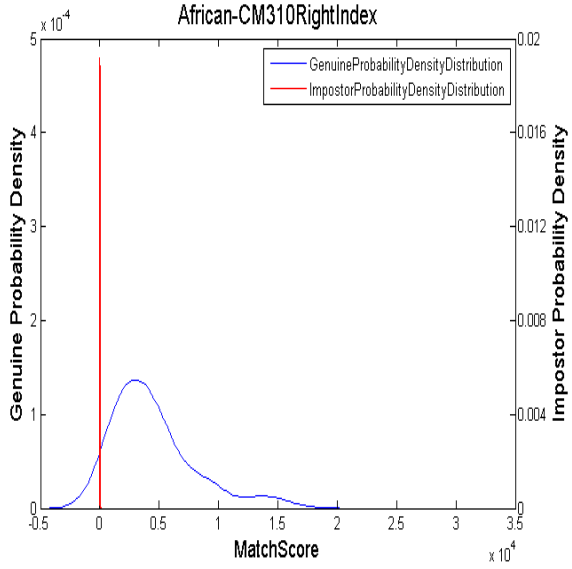
B.8. (iii) Crossmatchverifier 310-Right Index



(a)



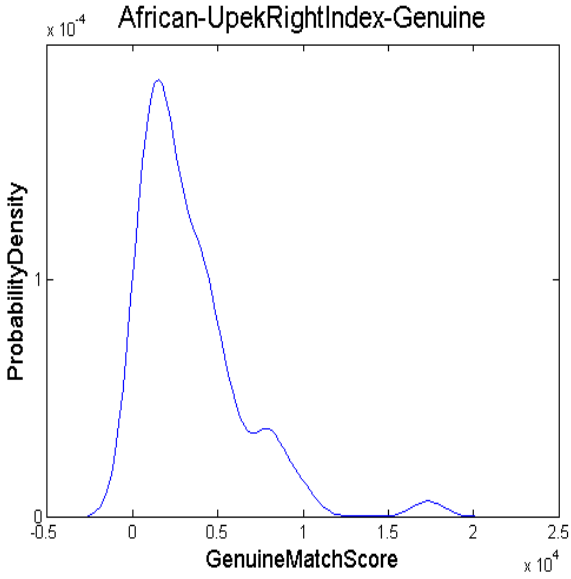
(b)



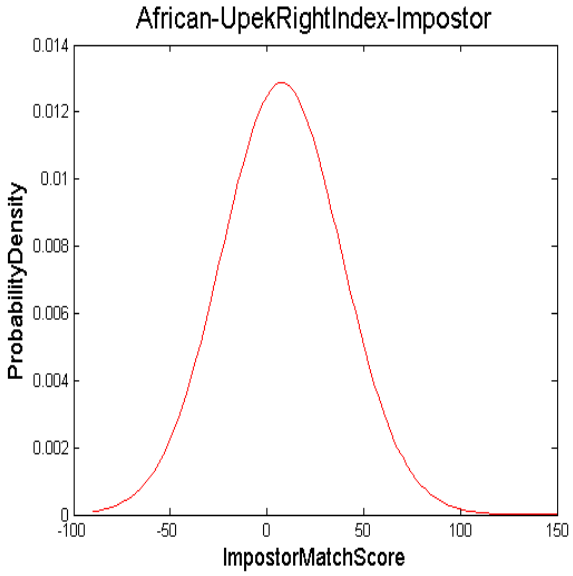
(c)

Figure B.8 (iii): Match score distributions of right index images of African ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

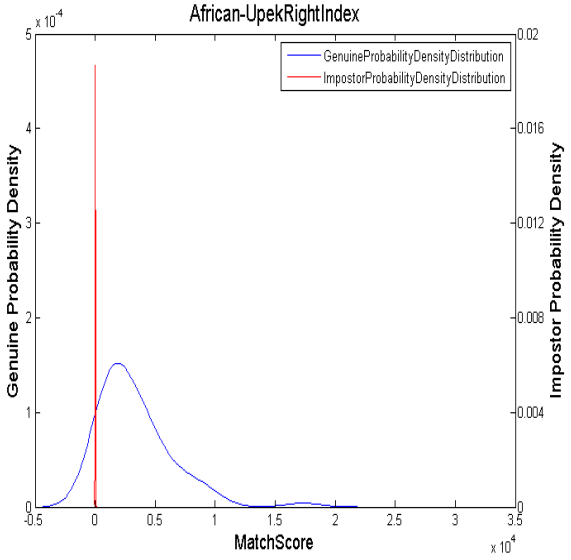
B.8. (iv) Upek Eikon Touch 700-Right Index



(a)



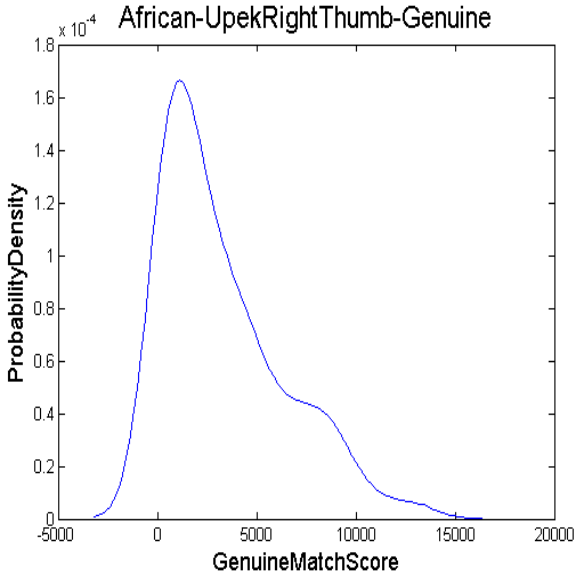
(b)



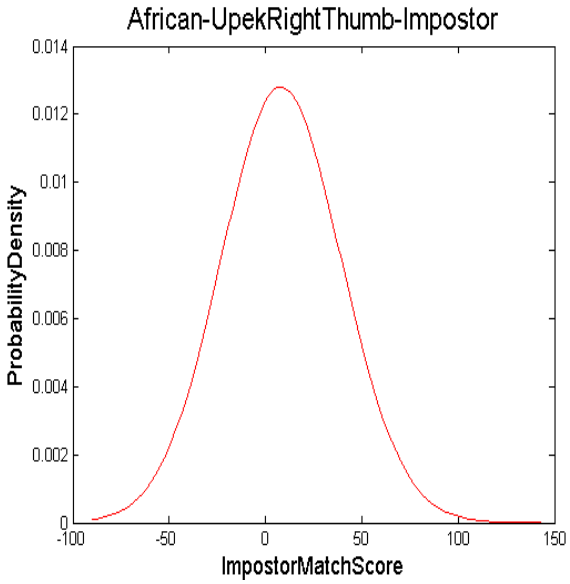
(c)

Figure B.8 (iv): Match score distributions of right index images of African ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

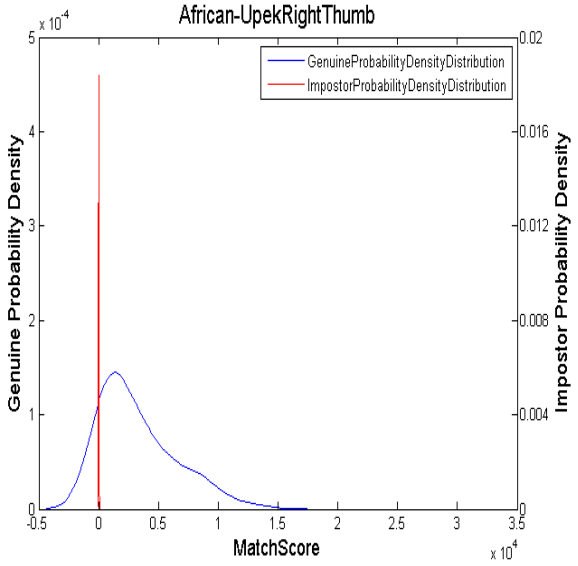
B.8. (v) Upek Eikon Touch 700-Right Thumb



(a)



(b)

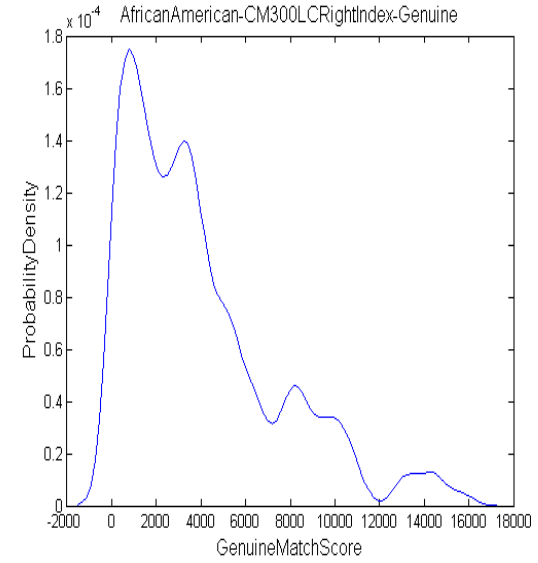


(c)

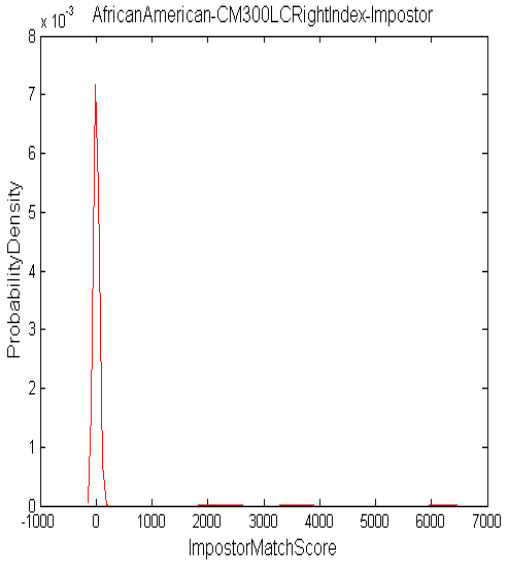
Figure B.8 (v): Match score distributions of right thumb images of African ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.9) African American

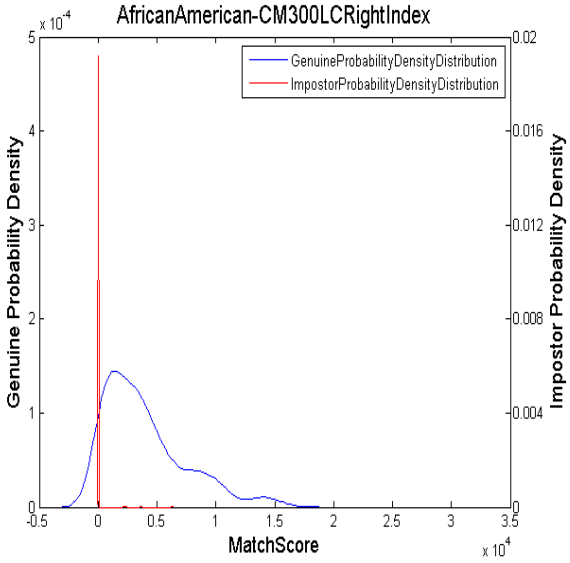
B.9. (i) Crossmatchverifier 300LC- Right Index



(a)



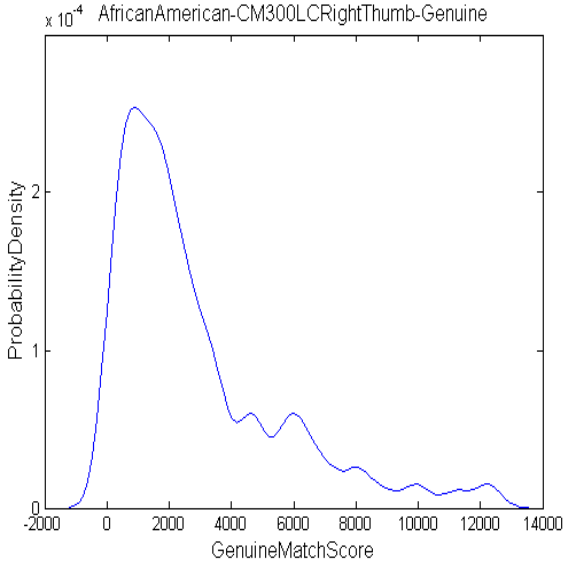
(b)



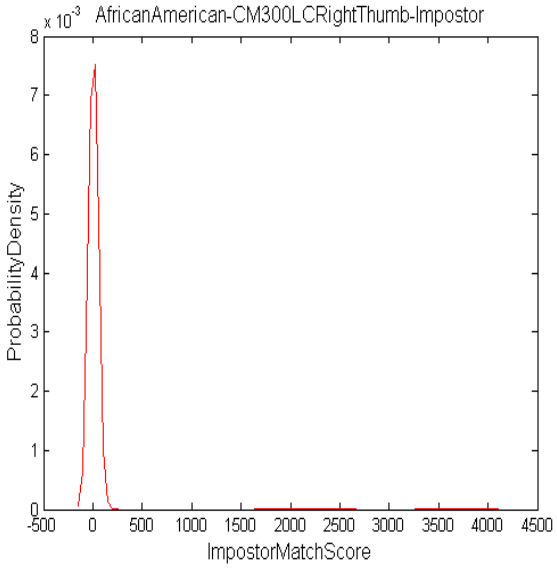
(c)

Figure B.9 (i): Match score distributions of right index images for African American ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

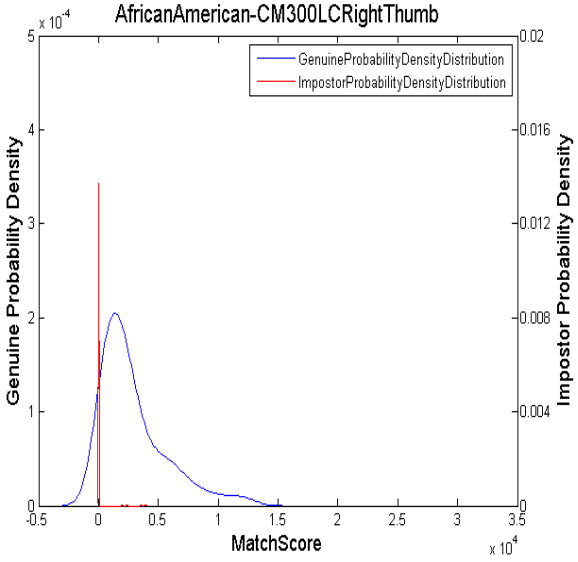
B.9. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



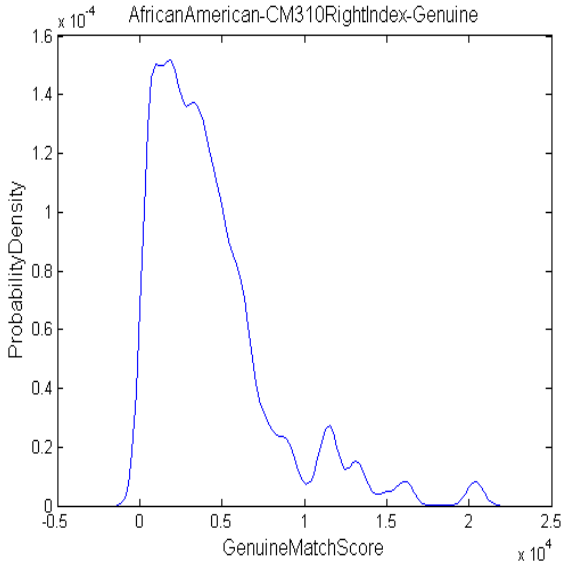
(b)



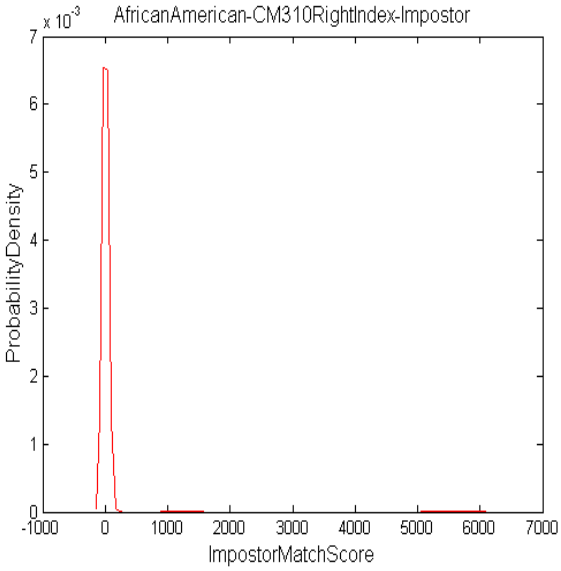
(c)

Figure B.9 (ii): Match score distributions of right thumb images for African American ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

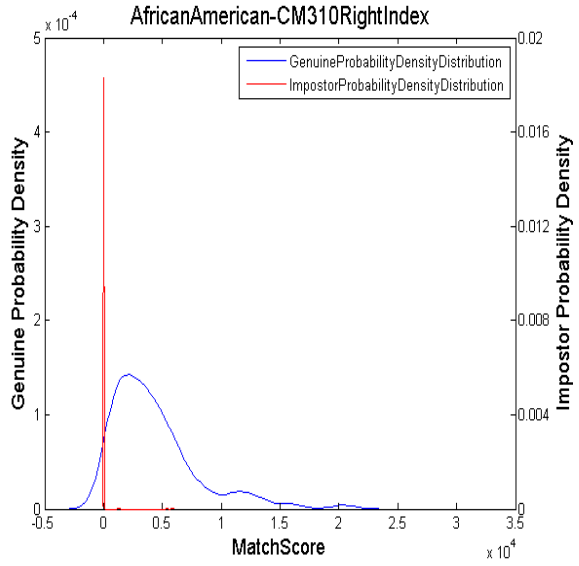
B.9. (iii) Crossmatchverifier 310- Right Index



(a)



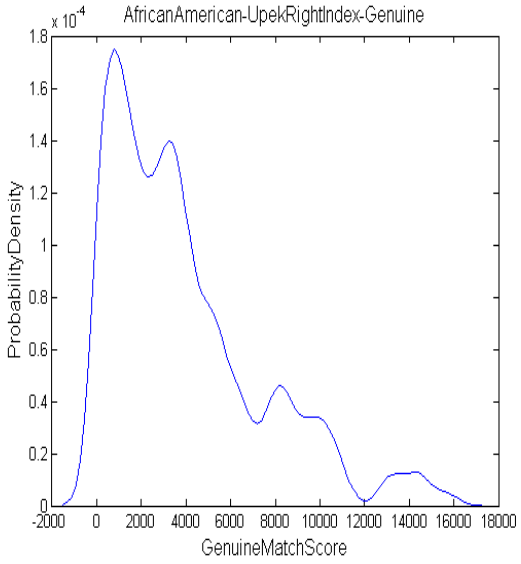
(b)



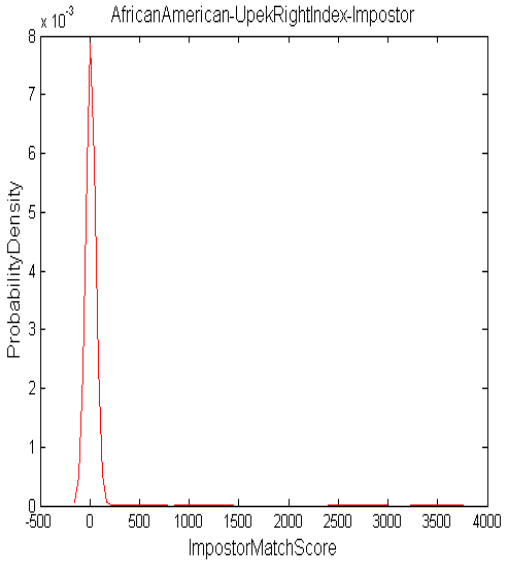
(c)

Figure B.9 (iii): Match score distributions of right index images for African American ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

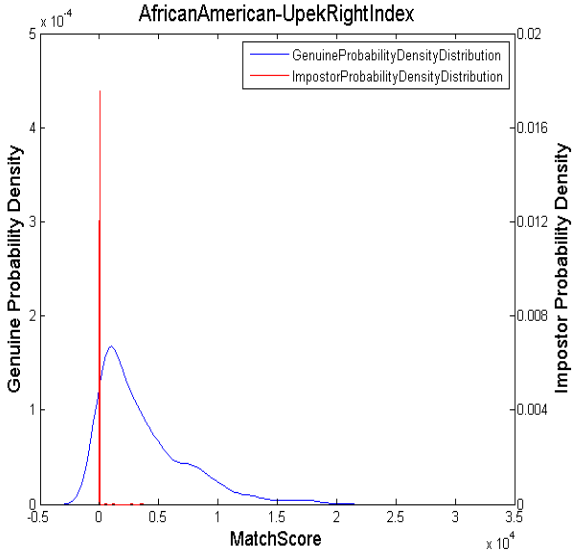
B.9. (iv) Upek Eikon Touch 700- Right Index



(a)



(b)



(c)

Figure B.9 (iv): Match score distributions of right index images for African American ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.9. (v) Upek Eikon Touch 700- Right Thumb

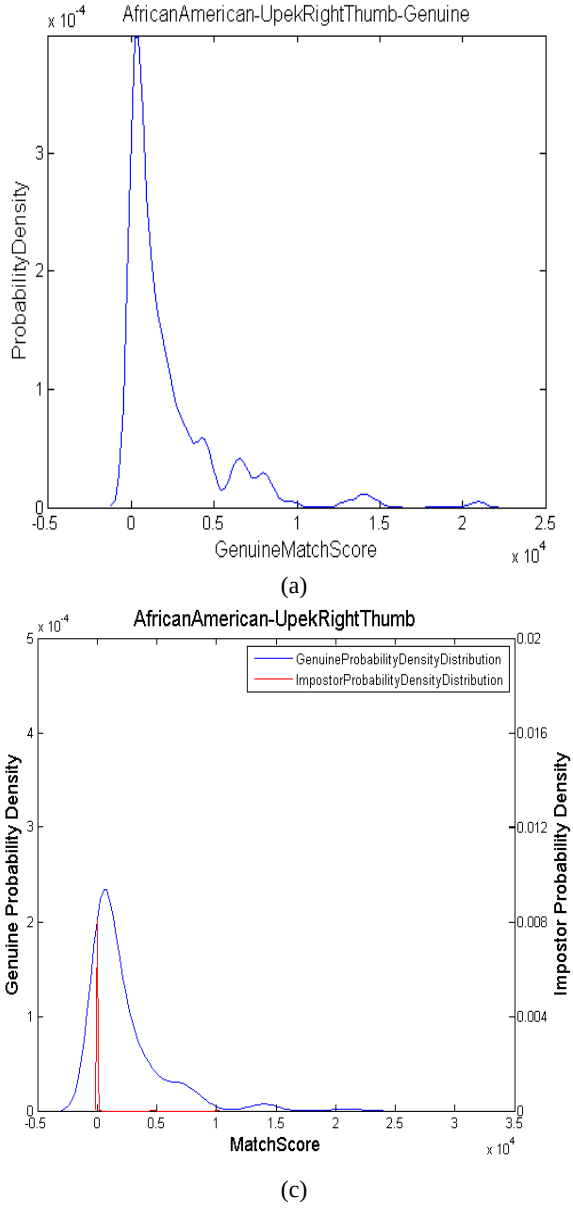
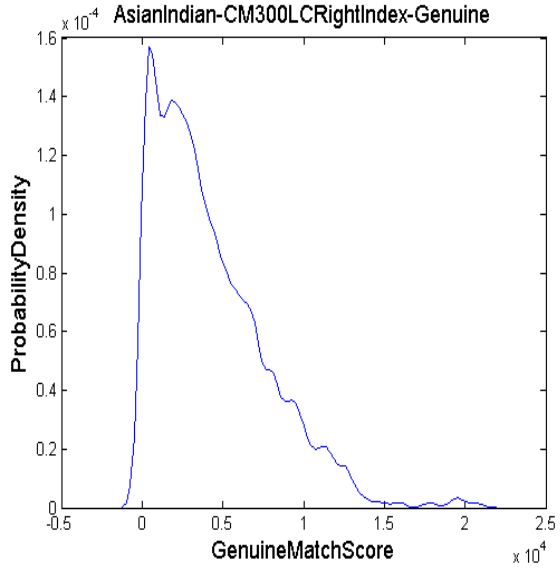


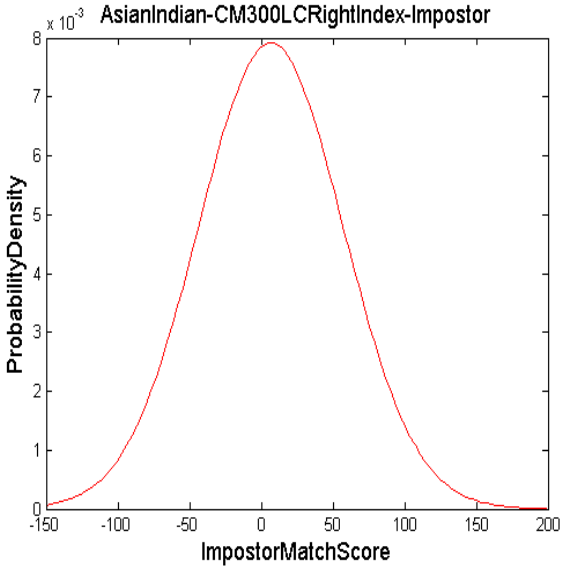
Figure B.9 (v): Match score distributions of right thumb images for African American ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.10) Asian Indian

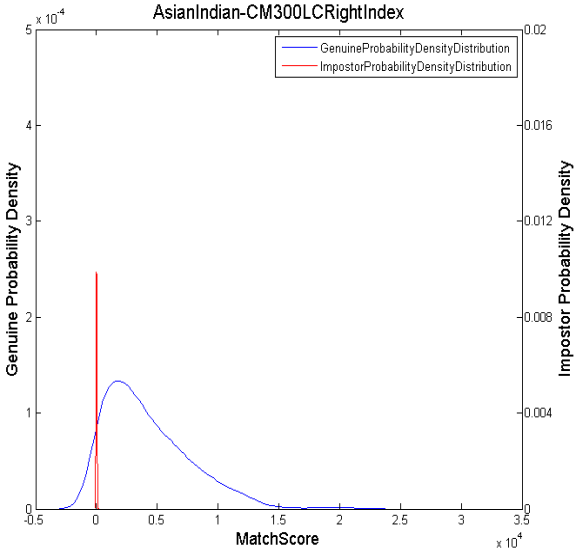
B.10. (i) Crossmatchverifier 300LC-Right Index



(a)



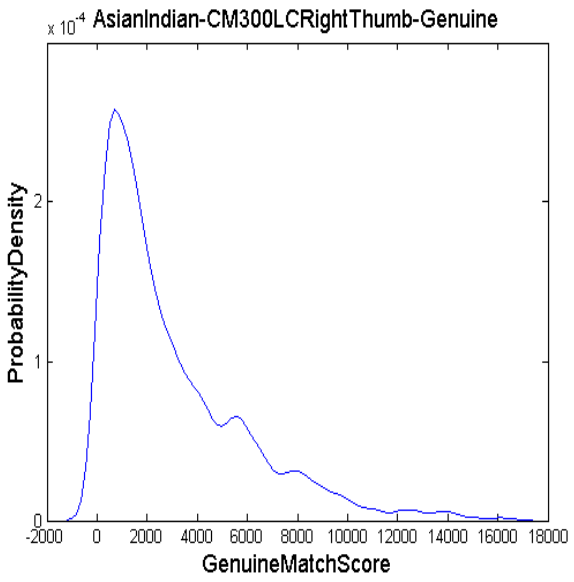
(b)



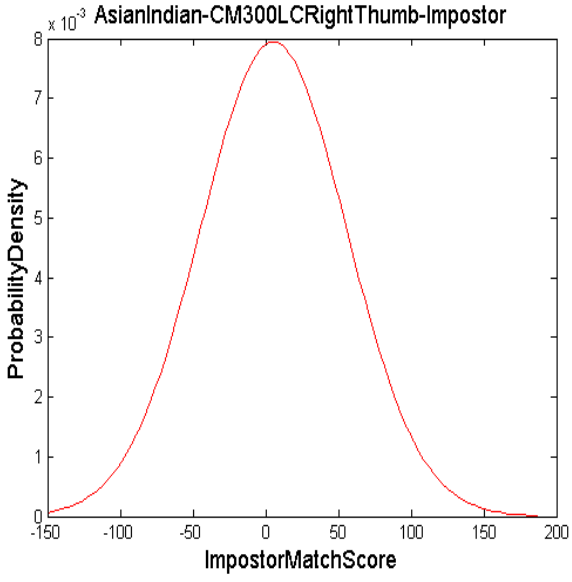
(c)

Figure B.10 (i): Match score distributions of right index images for Asian Indian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution (c) Combined match score distribution.

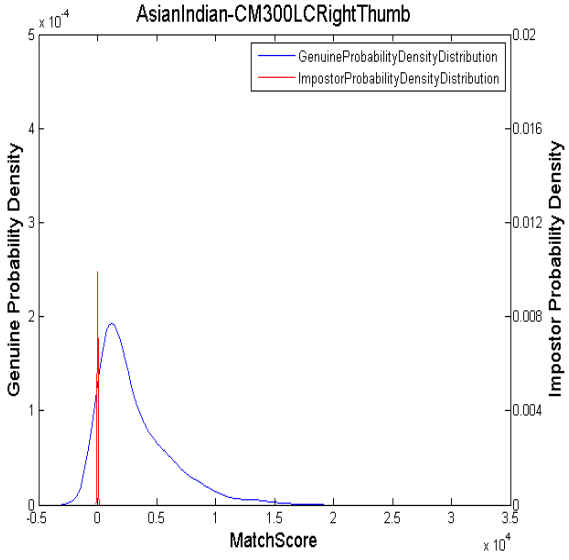
B.10. (ii) Crossmatchverifier 300LC-Right Thumb



(a)



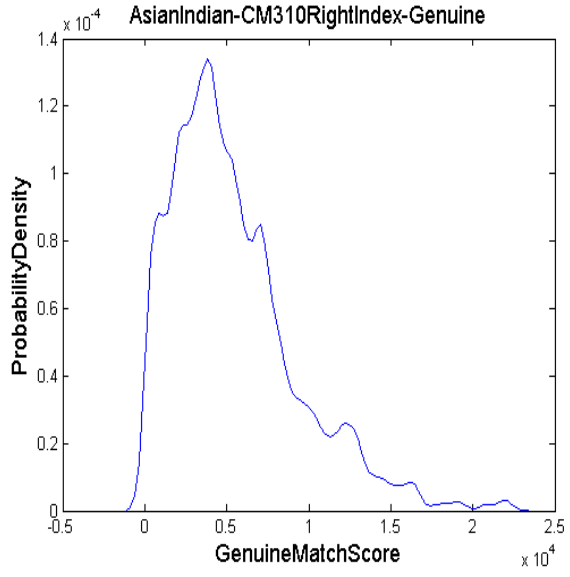
(b)



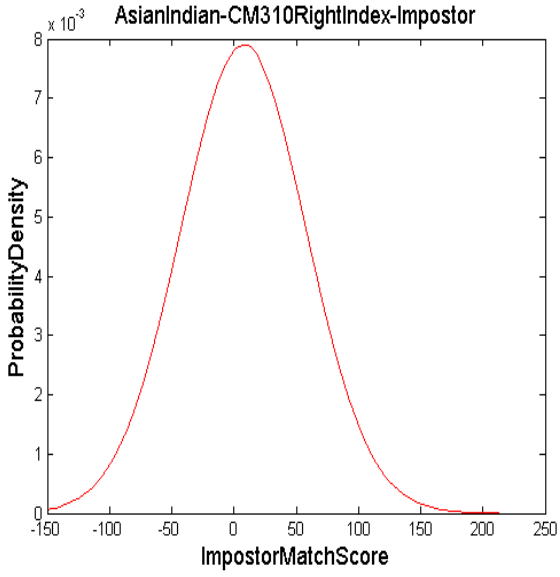
(c)

Figure B.10 (ii): Match score distributions of right thumb images for Asian Indian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

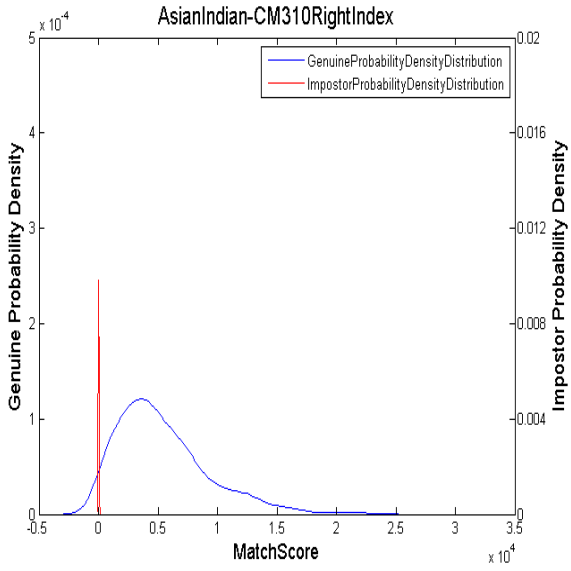
B.10. (iii) Crossmatchverifier 310-Right Index



(a)



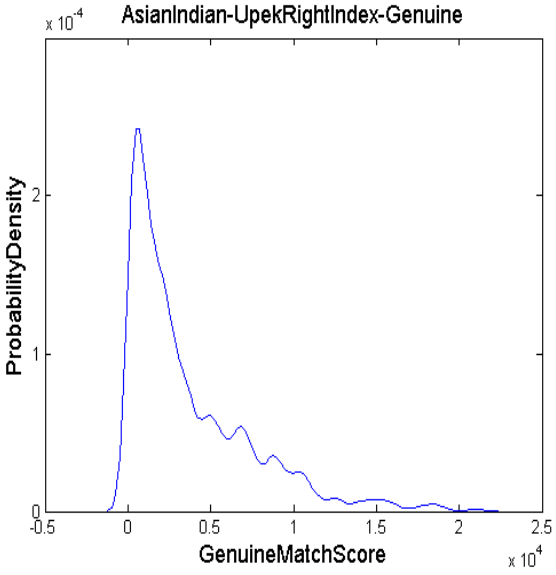
(b)



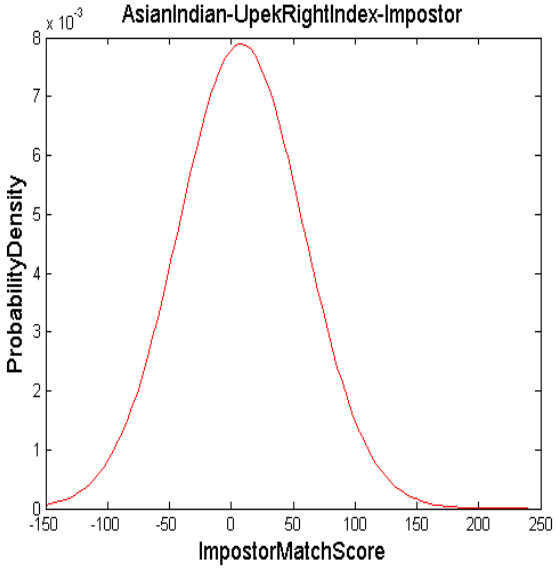
(c)

Figure B.10 (iii): Match score distributions of right index images for Asian Indian ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

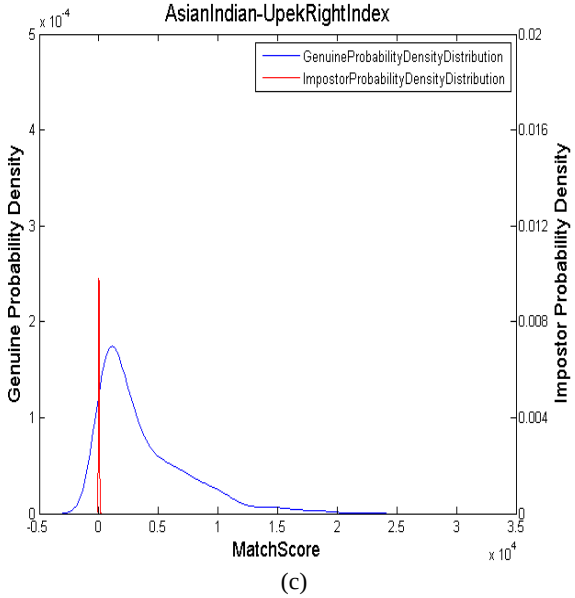
B.10. (iv) Upek Eikon Touch 700- Right Index



(a)



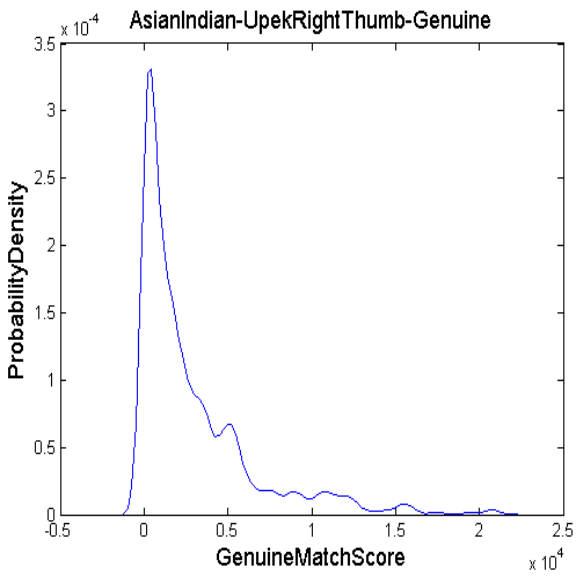
(b)



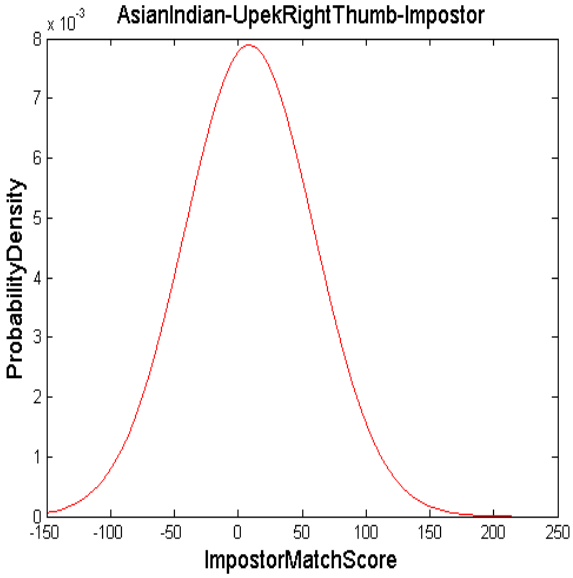
(c)

Figure B.10 (iv): Match score distributions of right index images for Asian Indian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

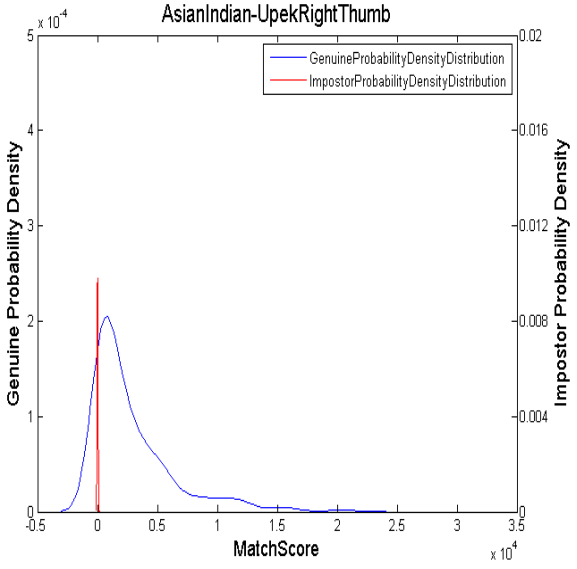
B.10. (v) Upek Eikon Touch 700- Right Thumb



(a)



(b)

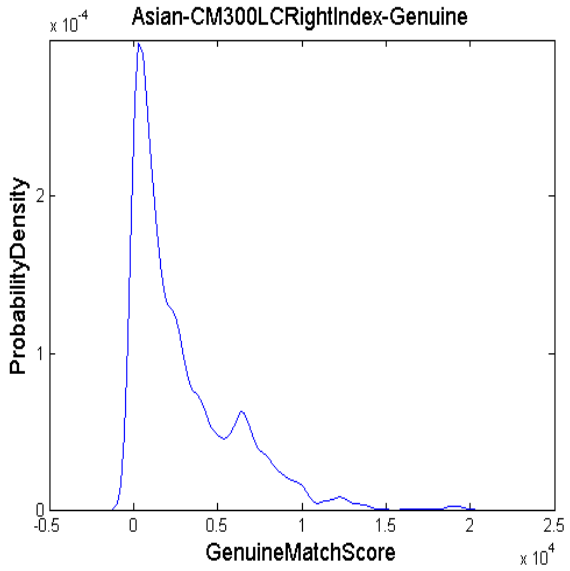


(c)

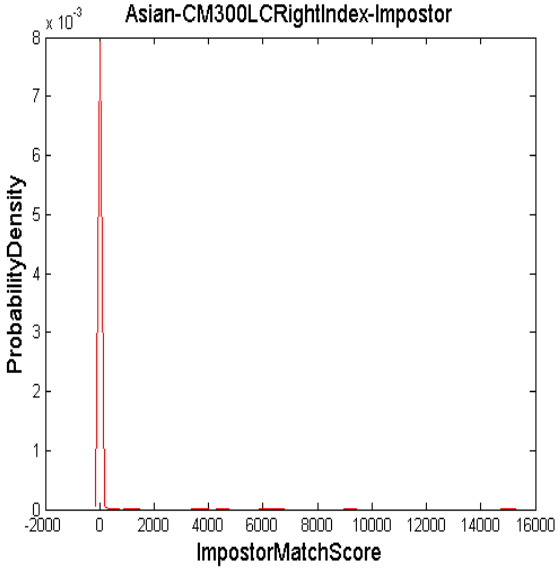
Figure B.10 (v): Match score distributions of right thumb images for Asian Indian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.11) Asian

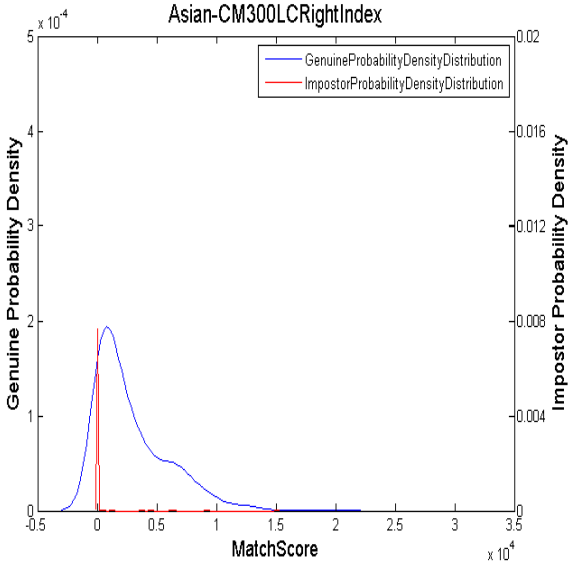
B.11. (i) Crossmatchverifier 300LC- Right Index



(a)



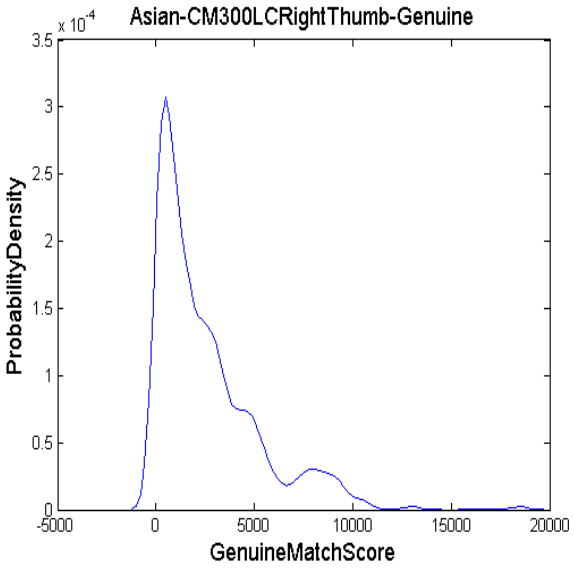
(b)



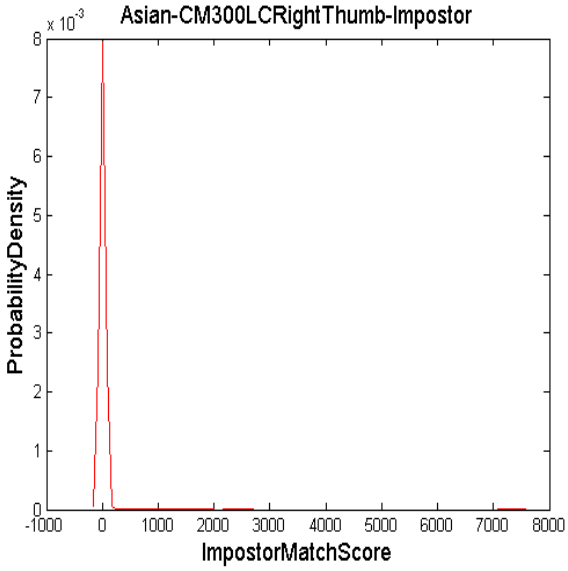
(c)

Figure B.11 (i): Match score distributions of right index images for Asian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

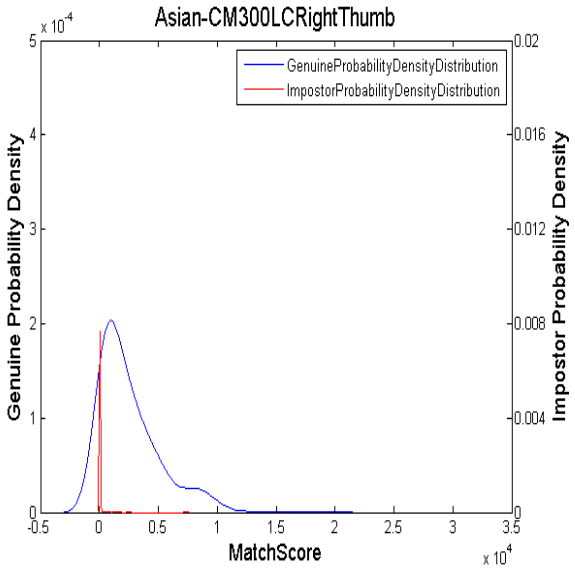
B.11. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



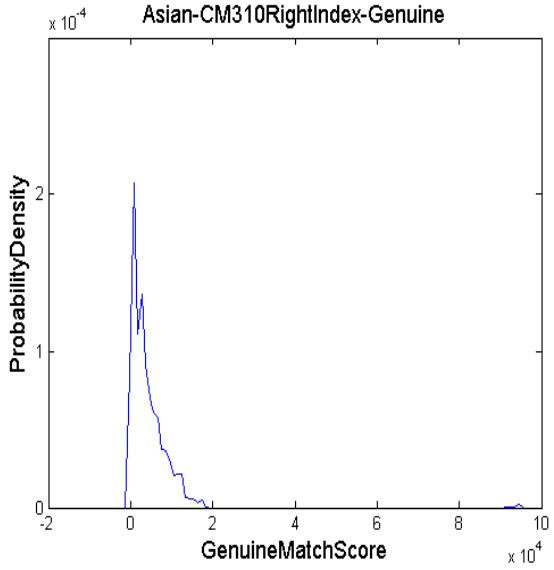
(b)



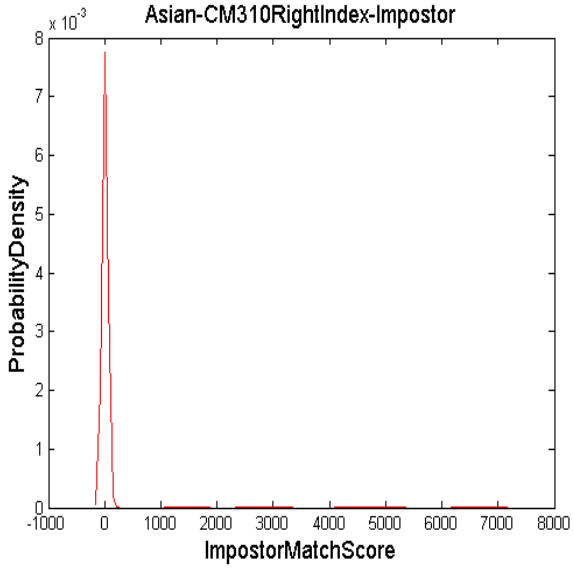
(c)

Figure B.11 (ii): Match score distributions of right thumb images for Asian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

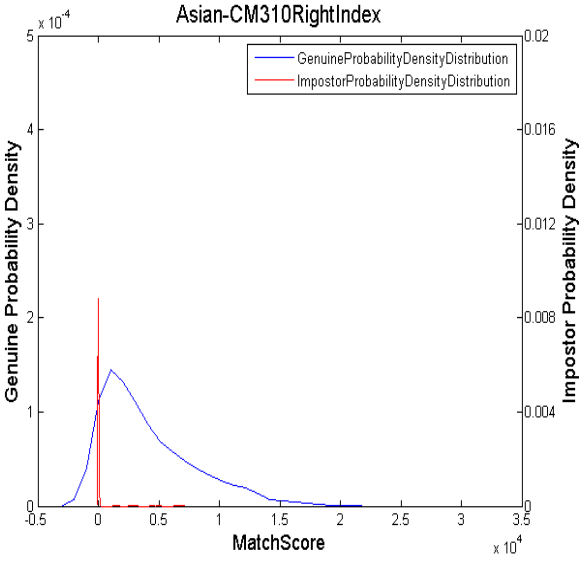
B.11. (iii) Crossmatchverifier 310- Right Index



(a)



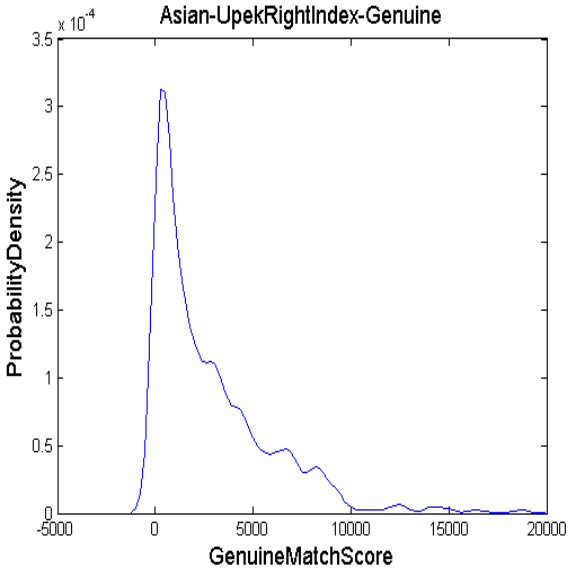
(b)



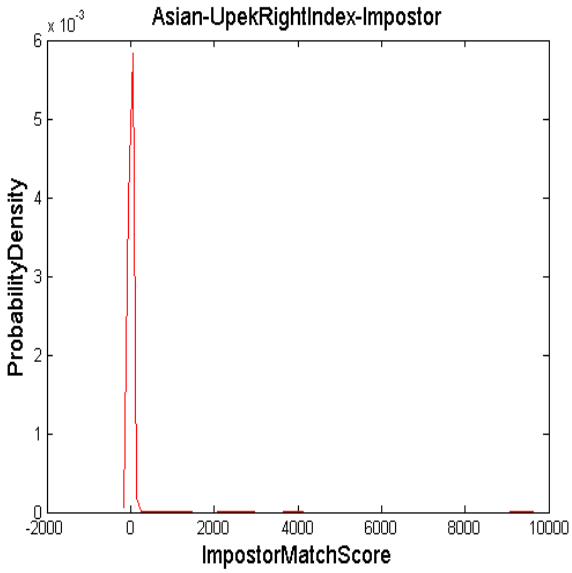
(c)

Figure B.11 (iii): Match score distributions of right index images for Asian ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

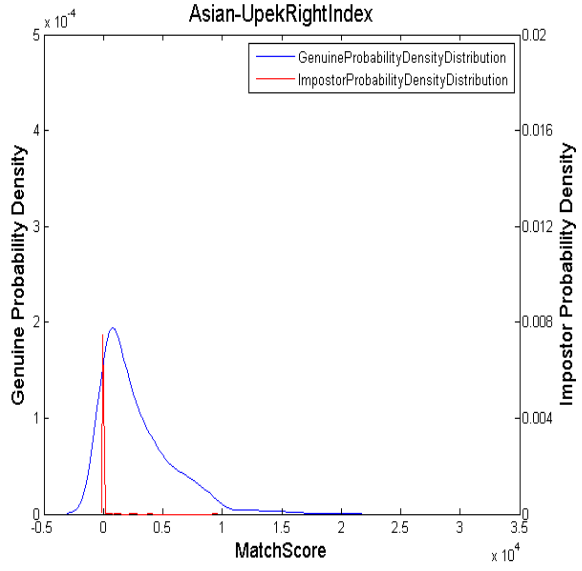
B.11. (iv) Upek Eikon Touch 700 – Right Index



(a)



(b)



(c)

Figure B.11 (iv): Match score distributions of right index images for Asian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.11. (v) Upek Eikon Touch 700- Right Thumb

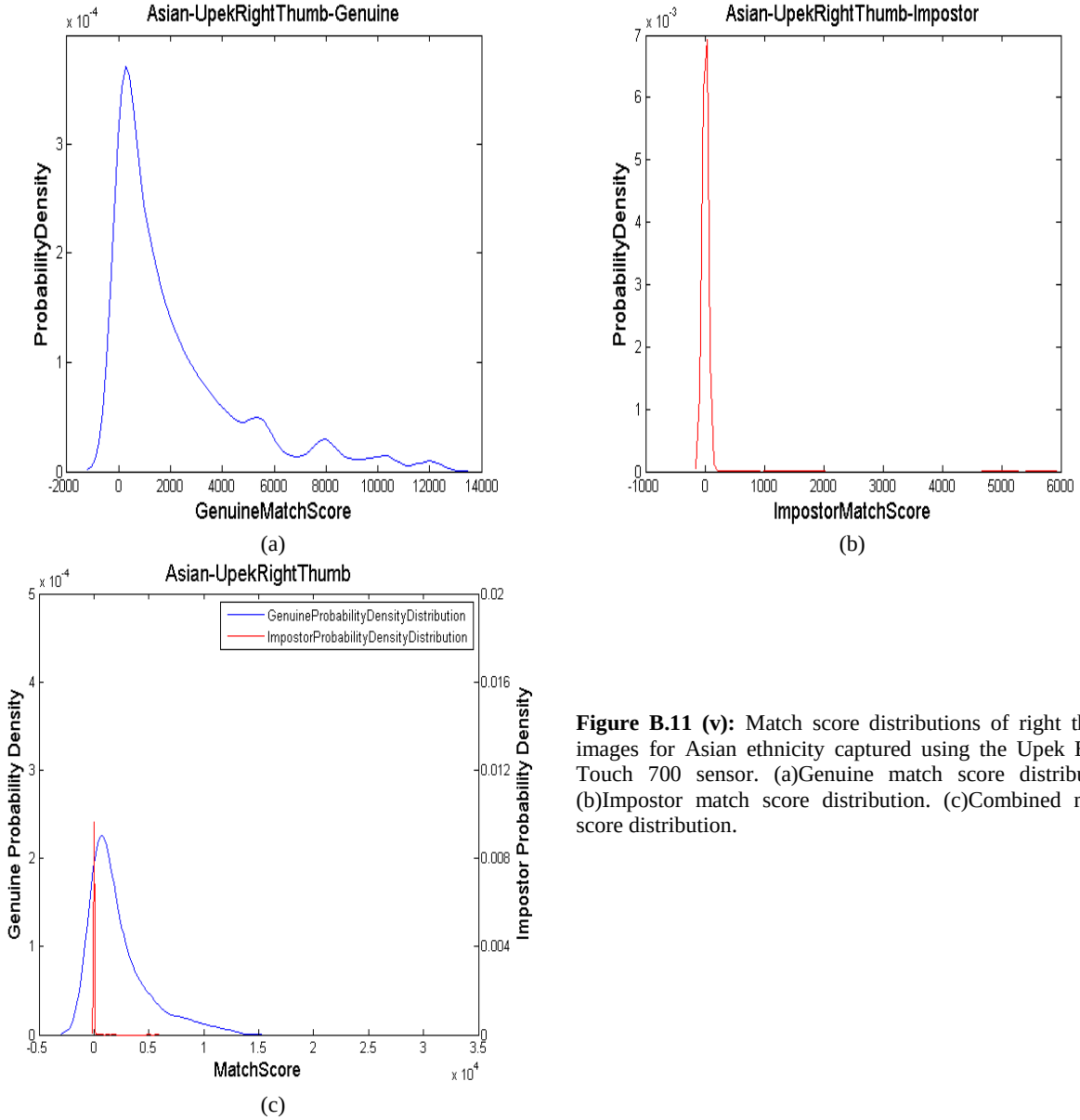
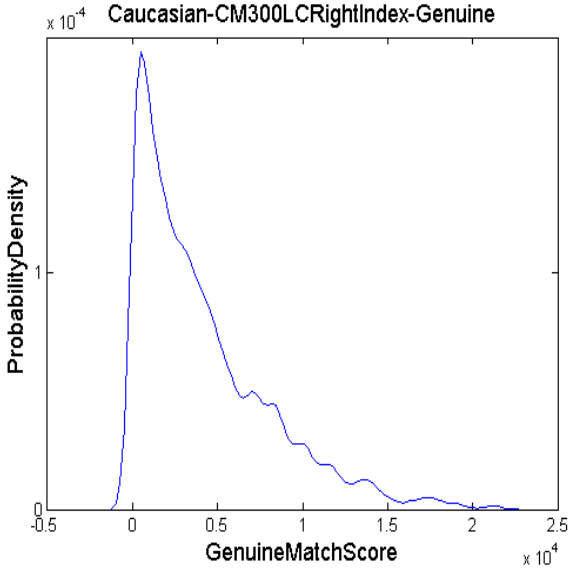


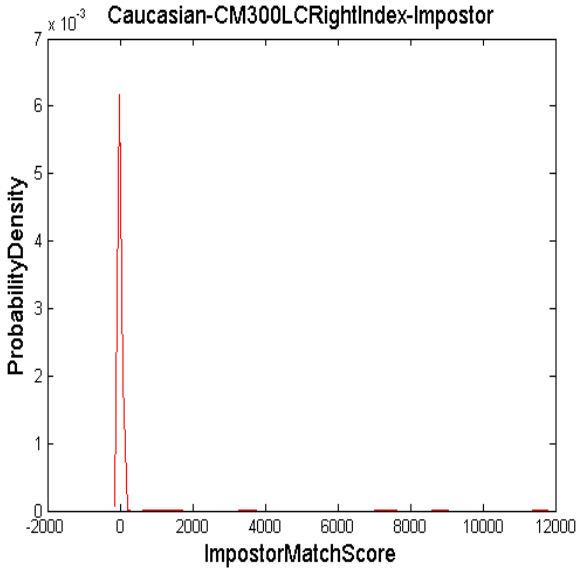
Figure B.11 (v): Match score distributions of right thumb images for Asian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.12) Caucasian

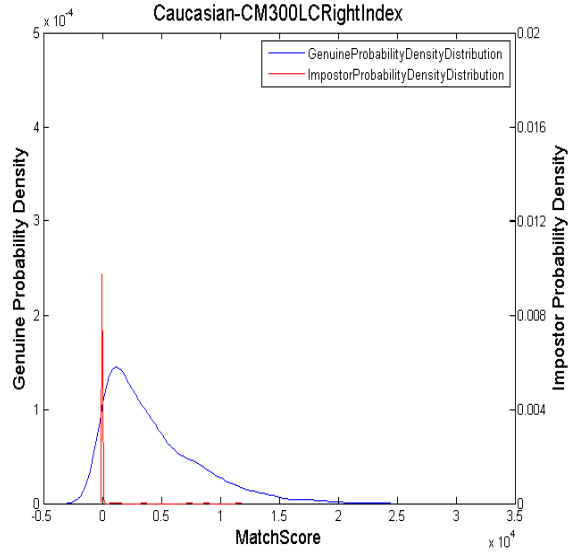
B.12. (i) Crossmatchverifier 300LC- Right Index



(a)



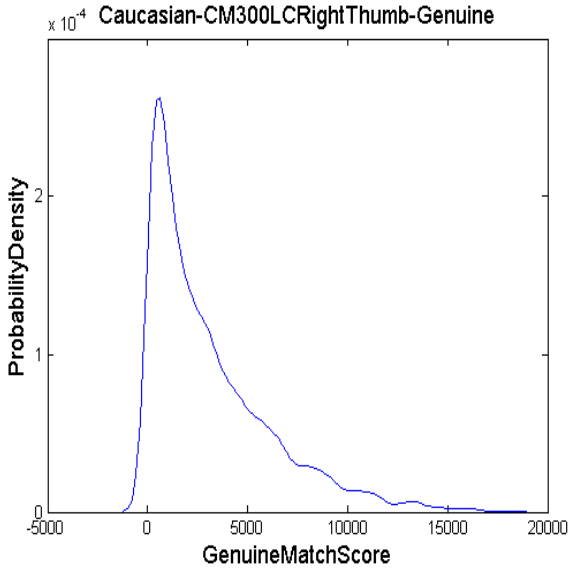
(b)



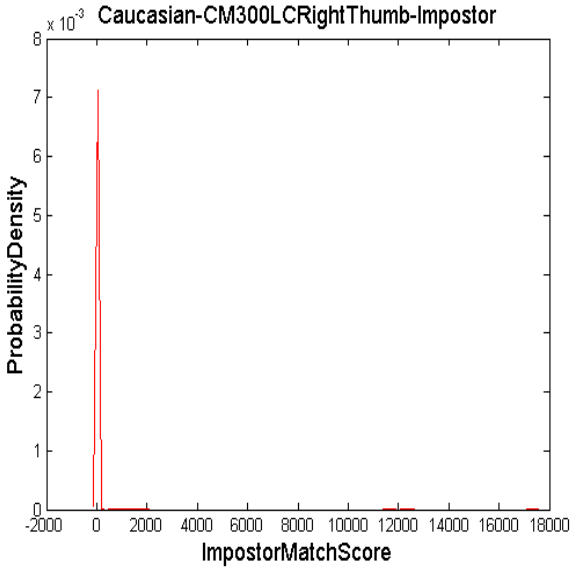
(c)

Figure B.12 (i): Match score distributions of right index images for Caucasian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

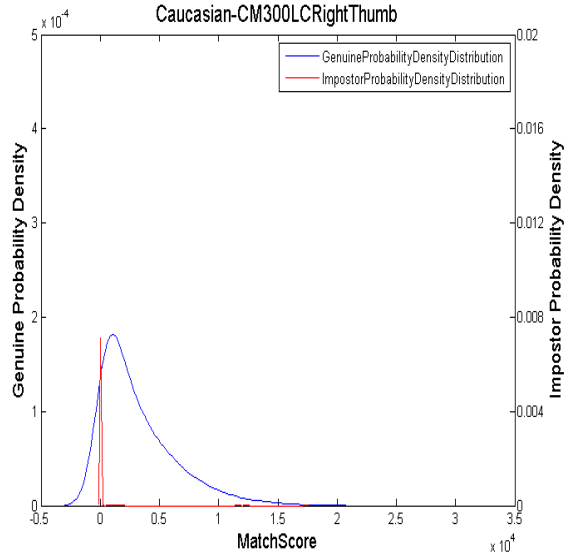
B.12. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



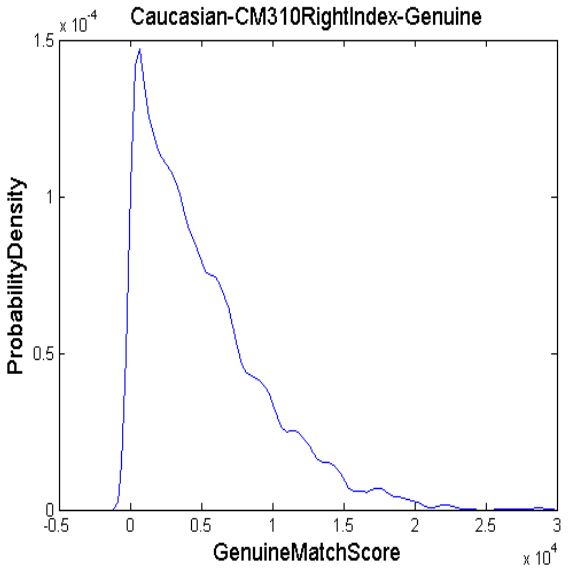
(b)



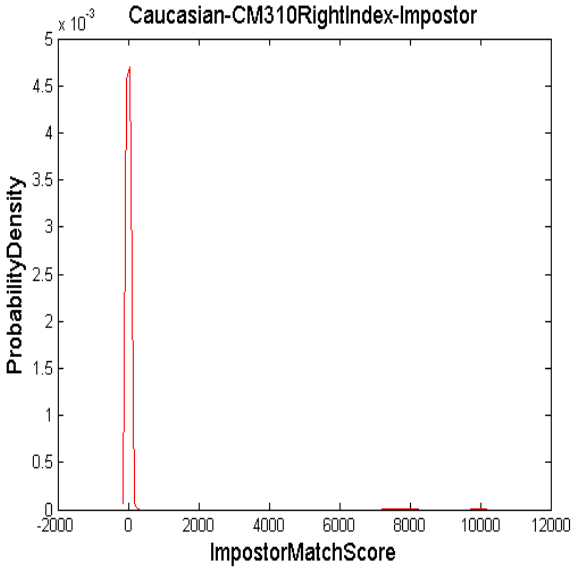
(c)

Figure B.12 (ii): Match score distributions of right thumb images for Caucasian ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

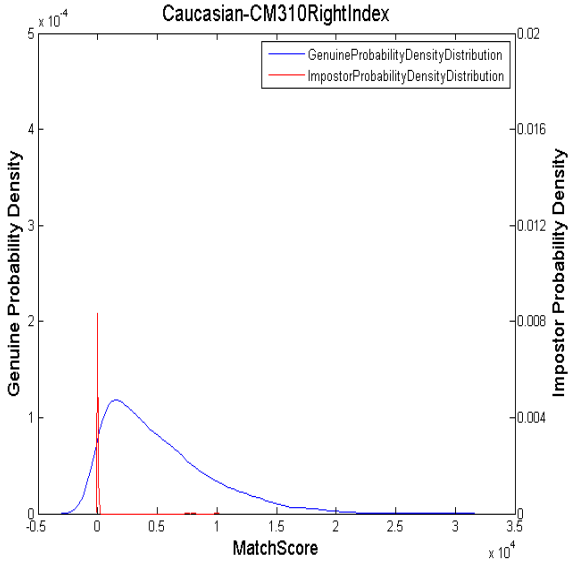
B.12. (iii) Crossmatchverifier 310- Right Index



(a)



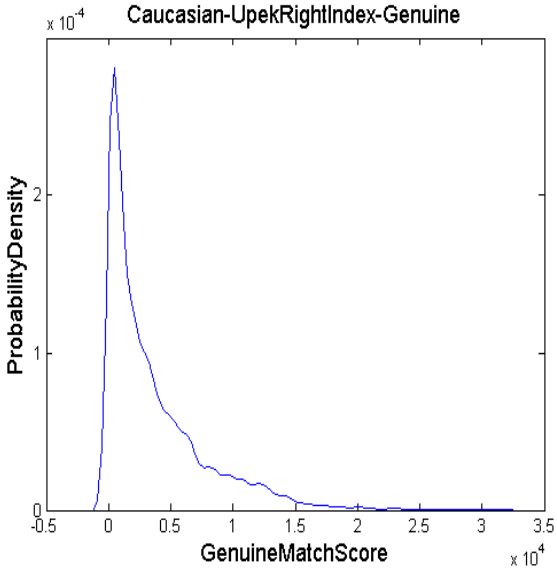
(b)



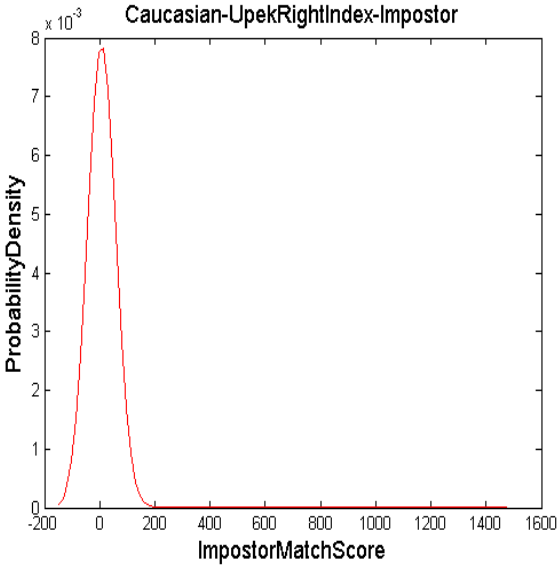
(c)

Figure B.12 (iii): Match score distributions of right index images for Caucasian ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

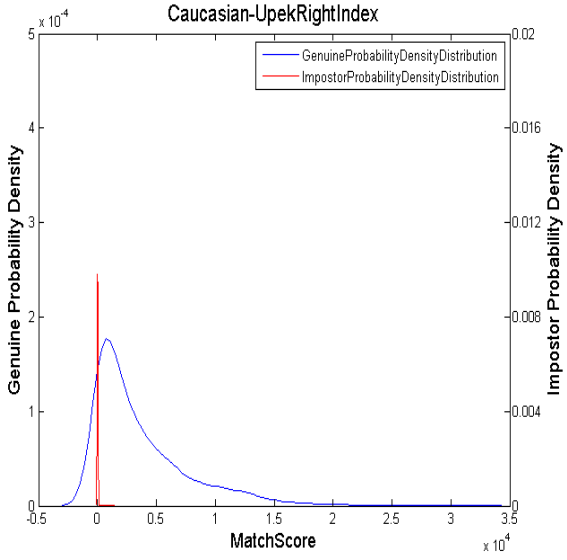
B.12. (iv) Upek Eikon Touch 700- Right Index



(a)



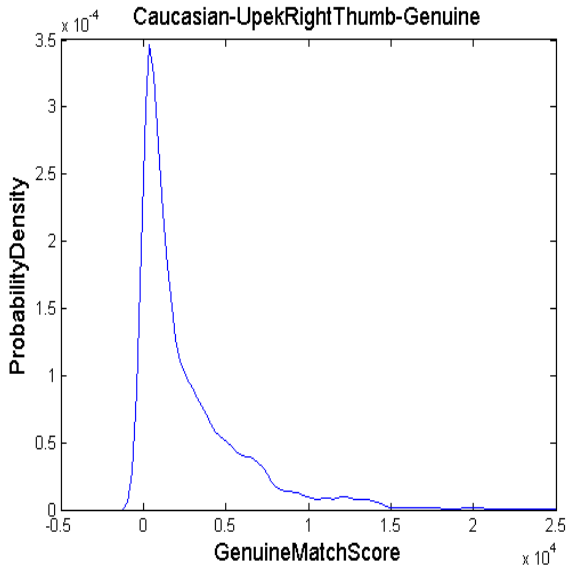
(b)



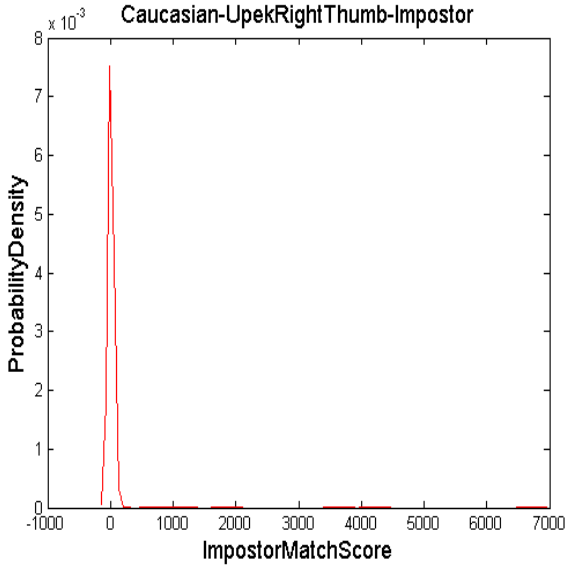
(c)

Figure B.12 (iv): Match score distributions of right index images for Caucasian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

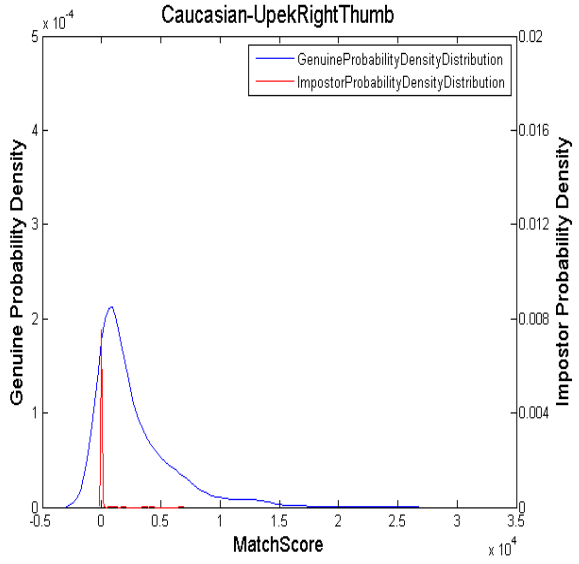
B.12. (v) Upek Eikon Touch 700- Right Thumb



(a)



(b)

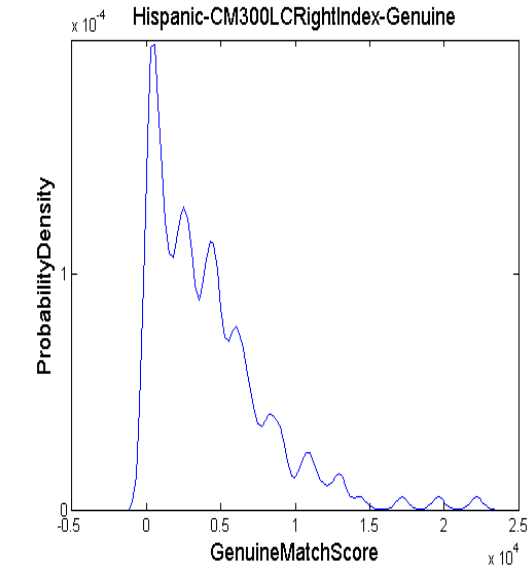


(c)

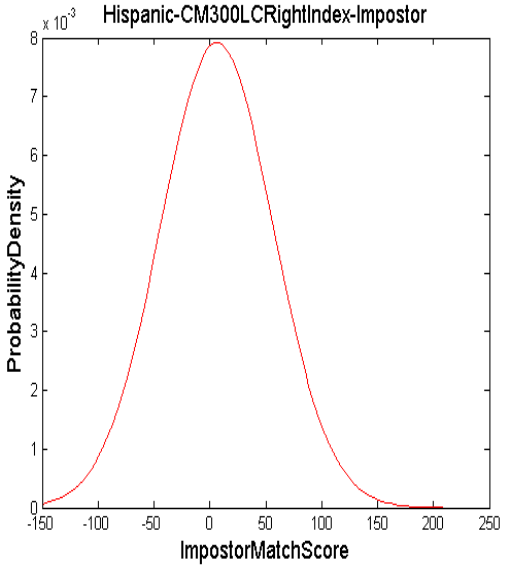
Figure B.12 (v): Match score distributions of right thumb images for Caucasian ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.13) Hispanic

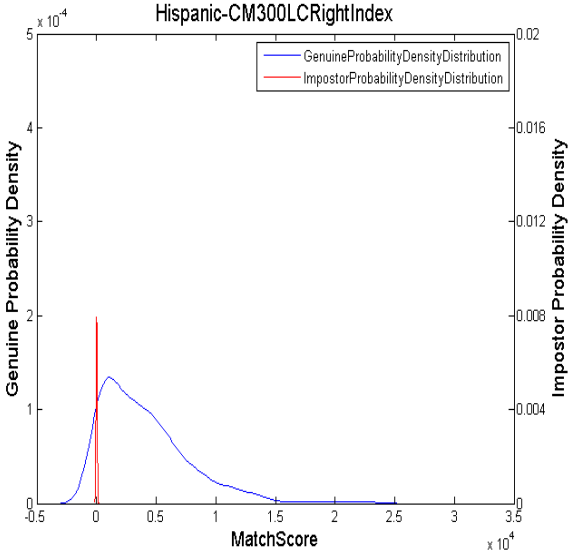
B.13. (i) Crossmatchverifier 300LC-Right Index



(a)



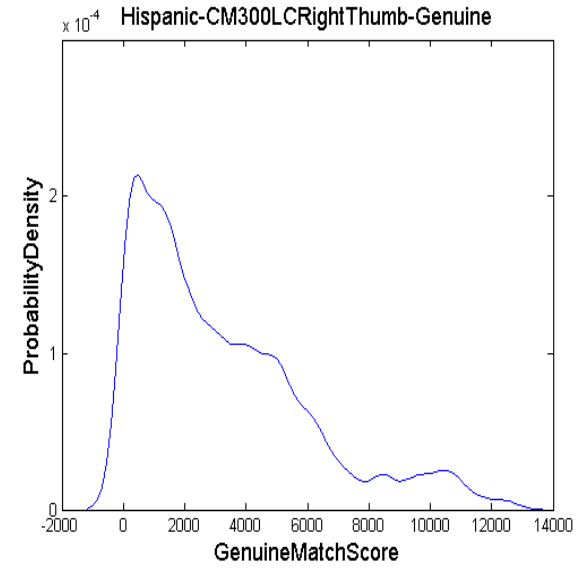
(b)



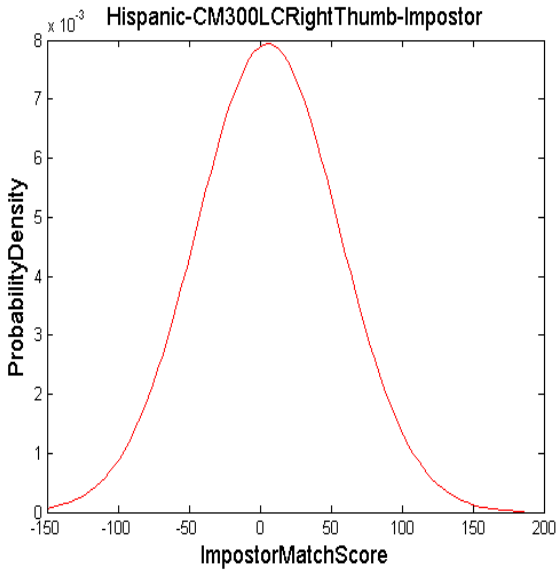
(c)

Figure B.13 (i): Match score distributions of right index images for Hispanic ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

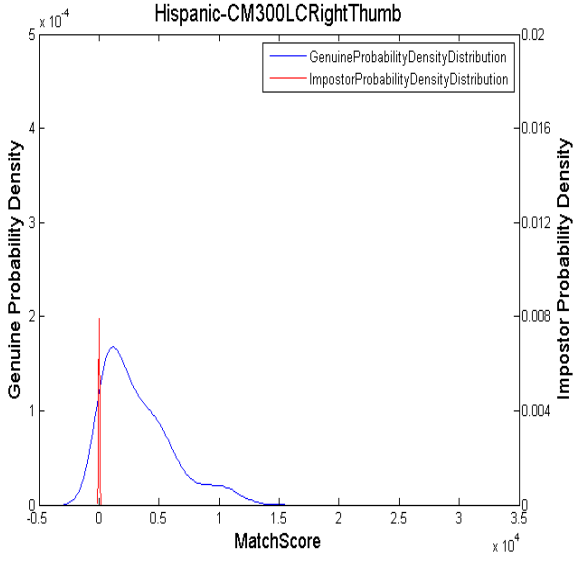
B.13. (ii) Crossmatchverifier 300LC-Right Thumb



(a)



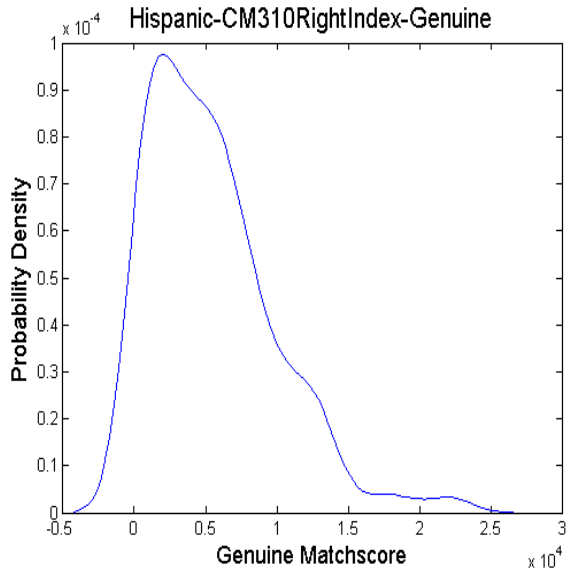
(b)



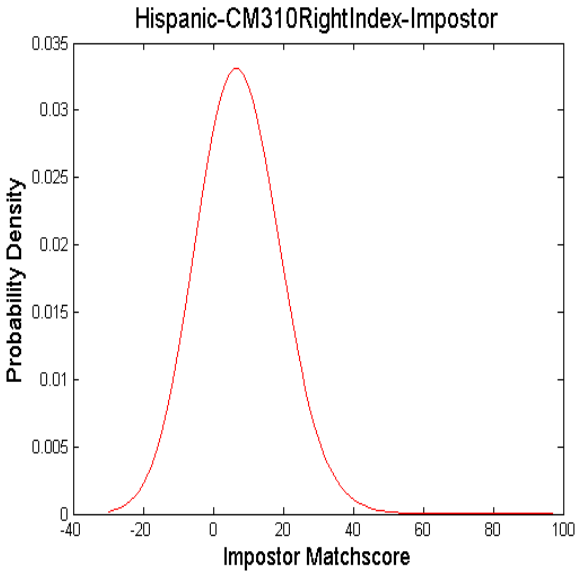
(c)

Figure B.13 (ii): Match score distributions of right thumb images for Hispanic ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

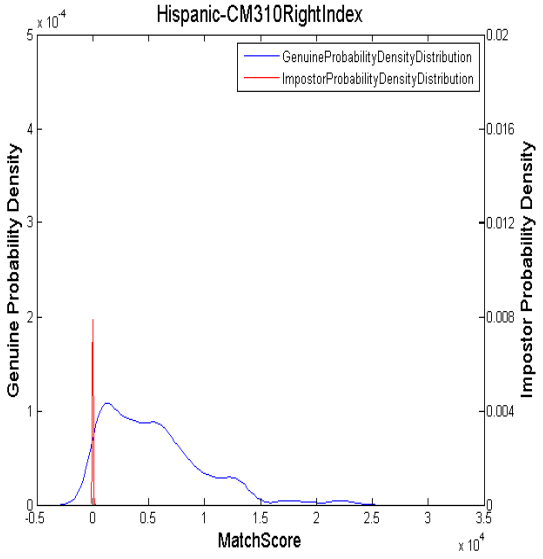
B.13. (iii) Crossmatchverifier 310-Right Index



(a)



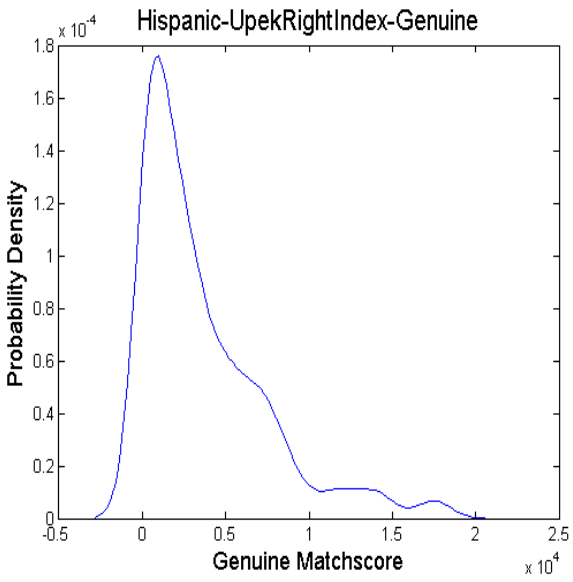
(b)



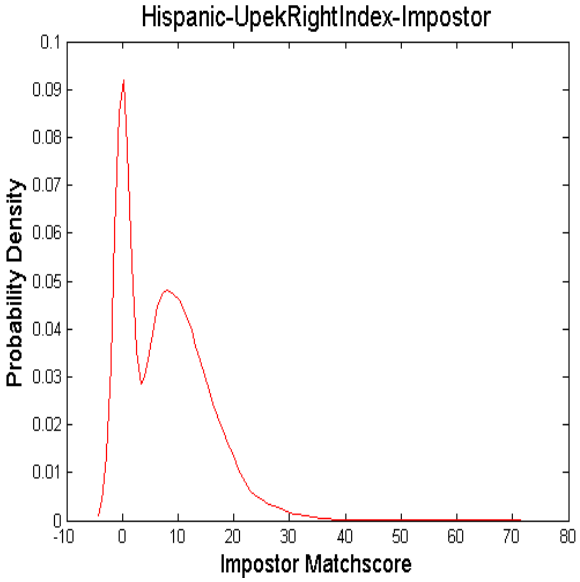
(c)

Figure B.13 (iii): Match score distributions of right index images for Hispanic ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

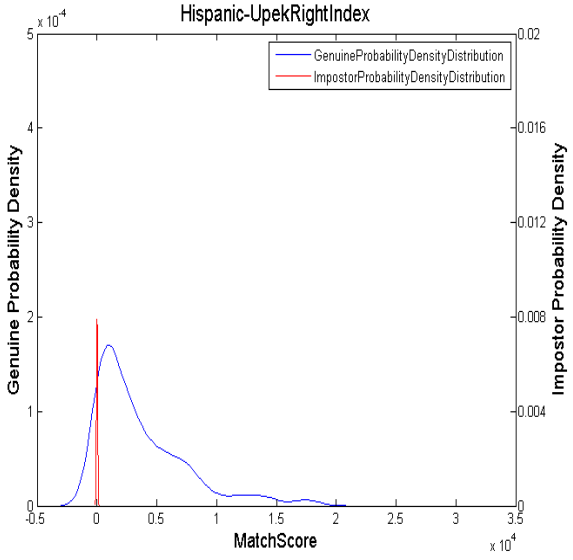
B.13. (iv) Upek Eikon Touch 700-Right Index



(a)



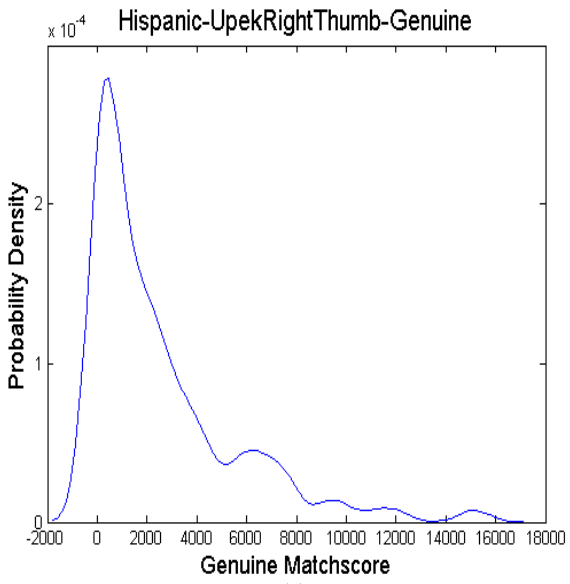
(b)



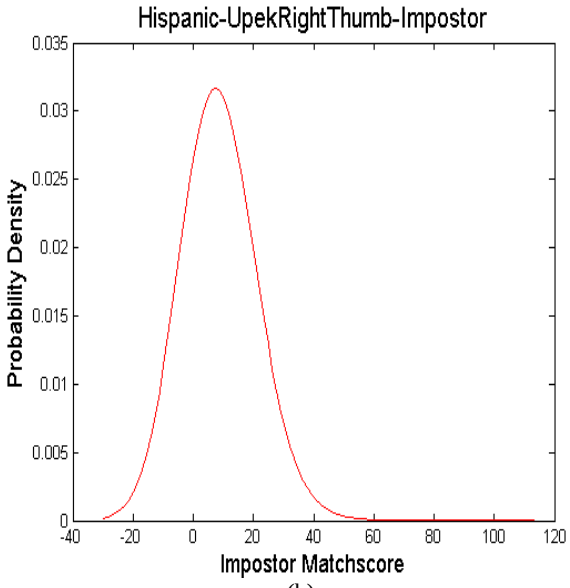
(c)

Figure B.13 (iv): Match score distributions of right index images for Hispanic ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

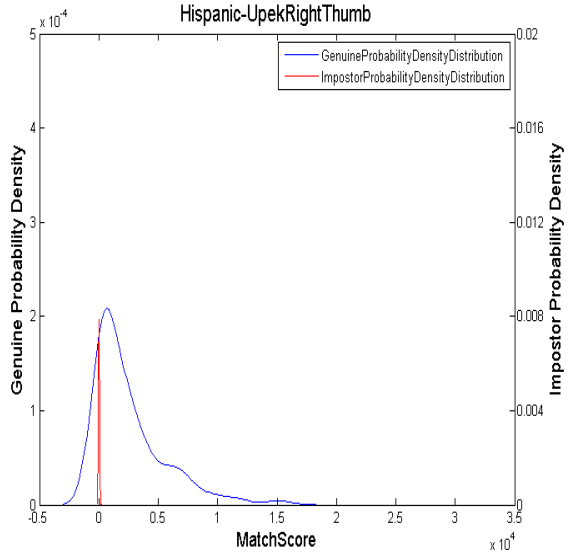
B.13. (v) Upek Eikon Touch 700-Right Thumb



(a)



(b)

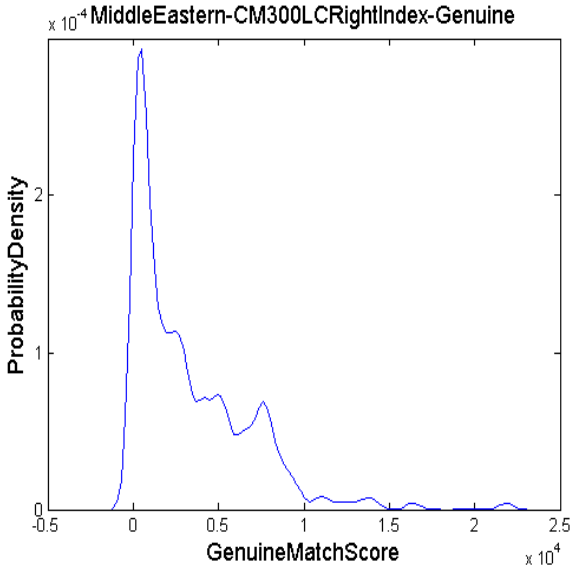


(c)

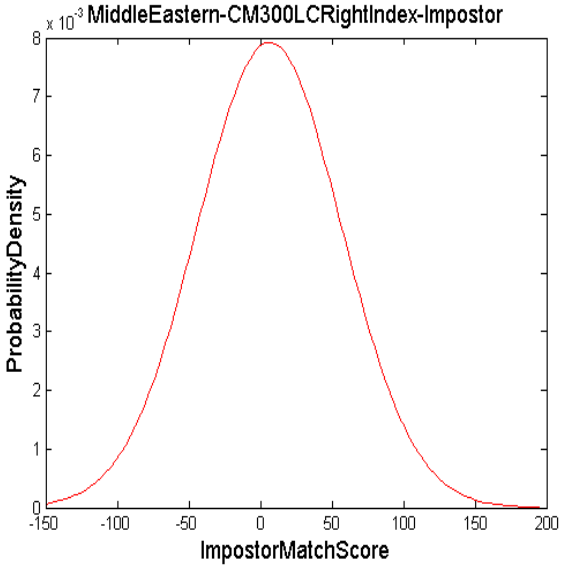
Figure B.13 (v): Match score distributions of right thumb images for Hispanic ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.14) Middle Eastern

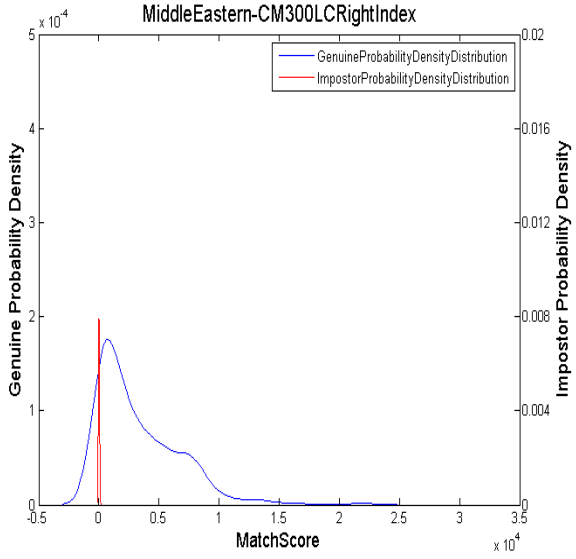
B.14. (i) Crossmatchverifier 300LC-Right Index



(a)



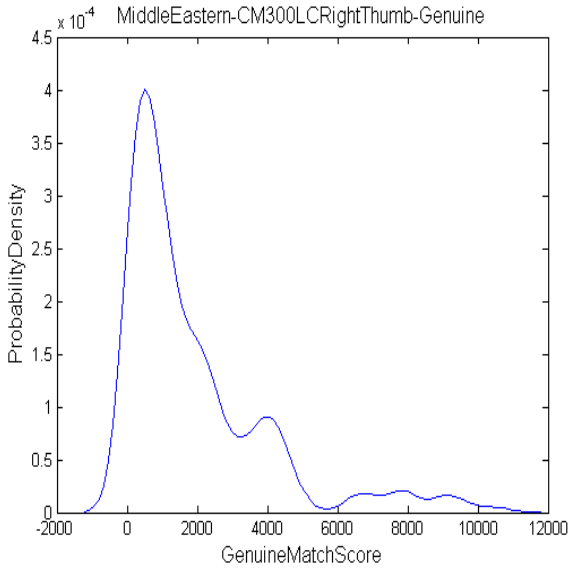
(b)



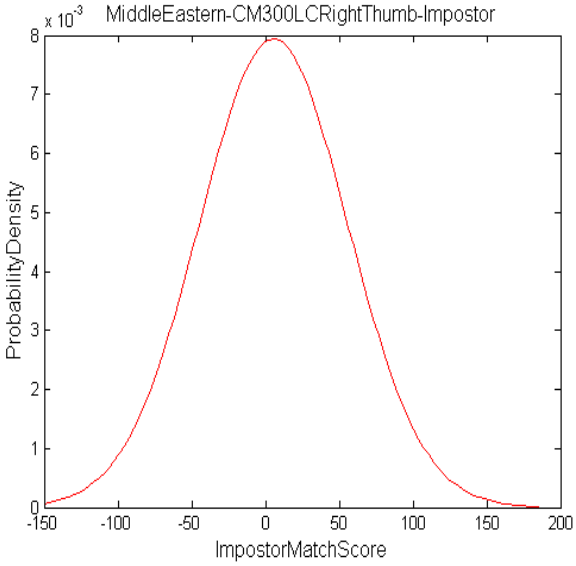
(c)

Figure B.14 (i): Match score distributions of right index images for Middle Eastern ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

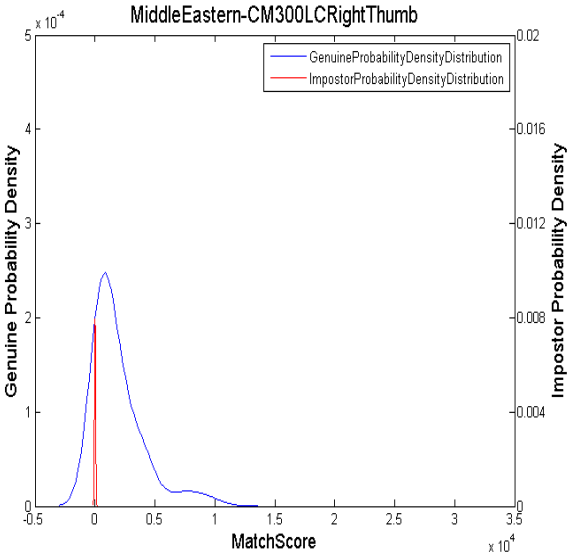
B.14. (ii) Crossmatchverifier 300LC-Right Thumb



(a)



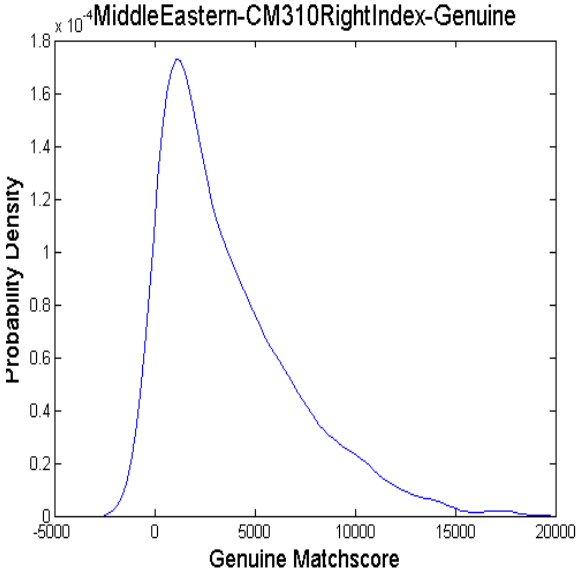
(b)



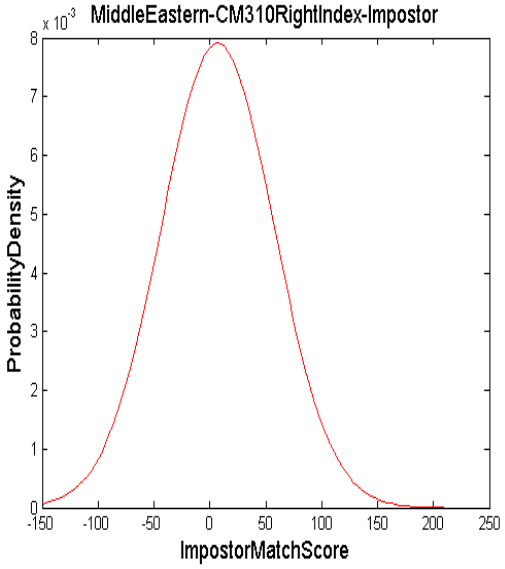
(c)

Figure B.14 (ii): Match score distributions of right thumb images for Middle Eastern ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

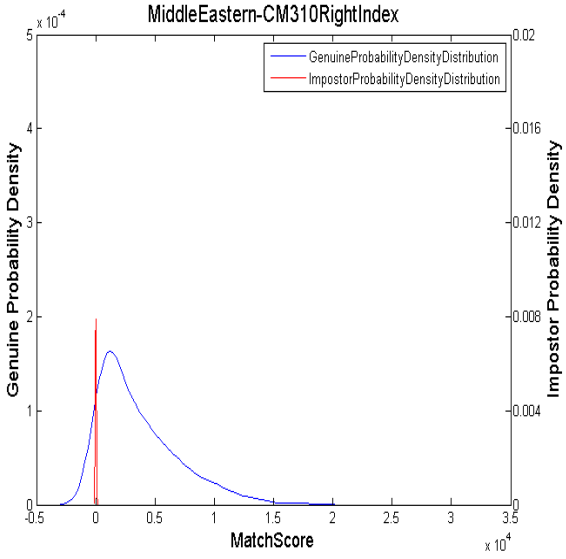
B.14. (iii) Crossmatchverifier 310-Right Index



(a)



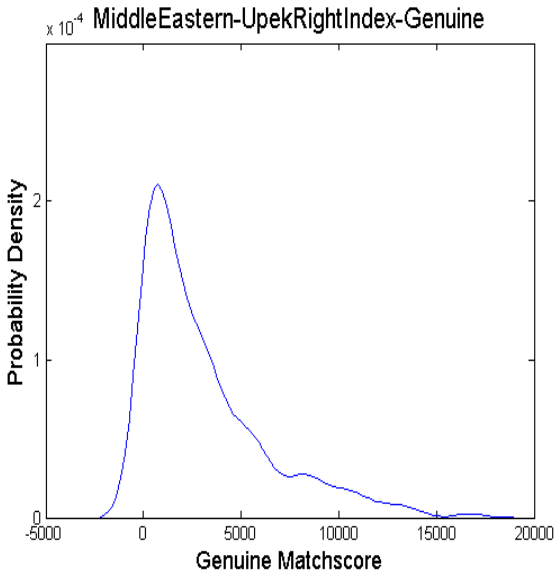
(b)



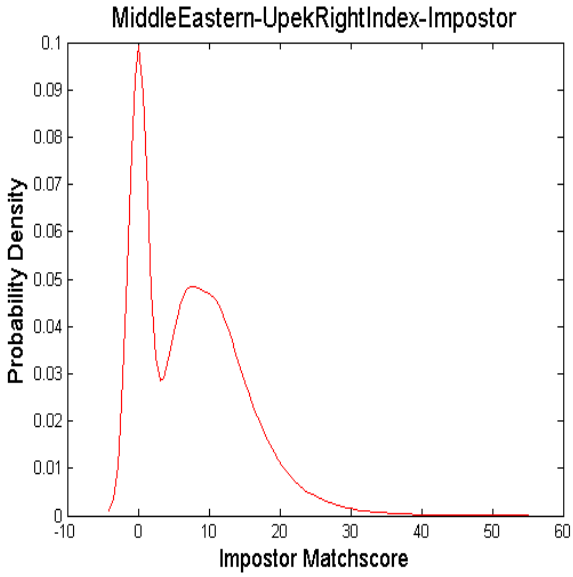
(c)

Figure B.14 (iii): Match score distributions of right index images for Middle Eastern ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

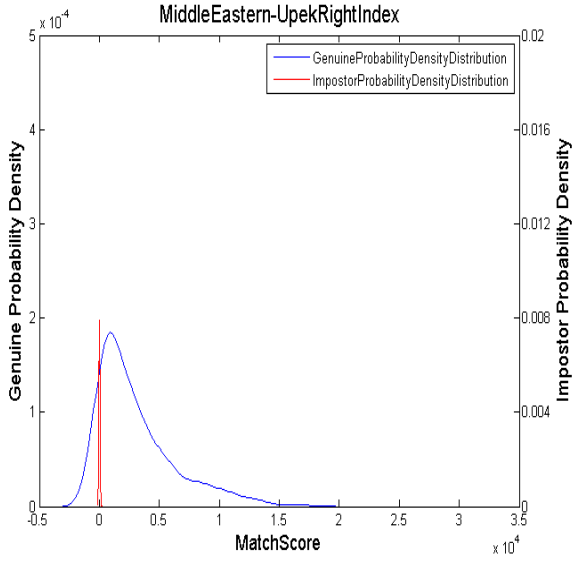
B.14. (iv) Upek Eikon Touch 700-Right Index



(a)



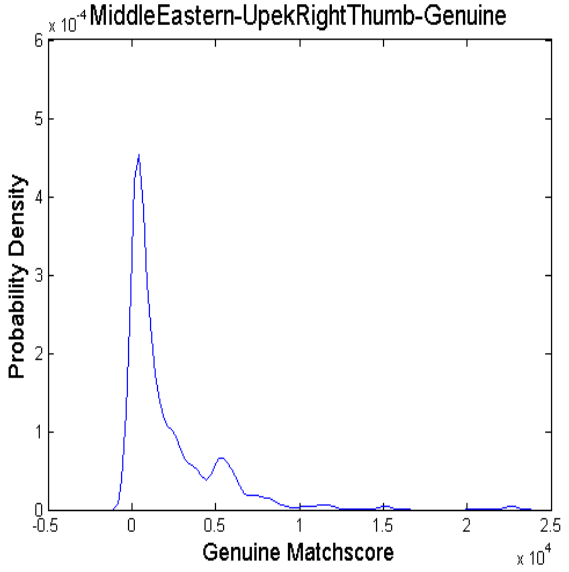
(b)



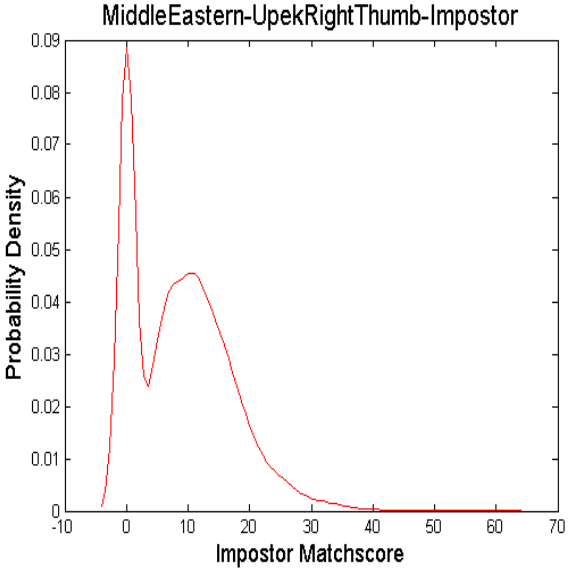
(c)

Figure B.14 (iv): Match score distributions of right index images for Middle Eastern ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

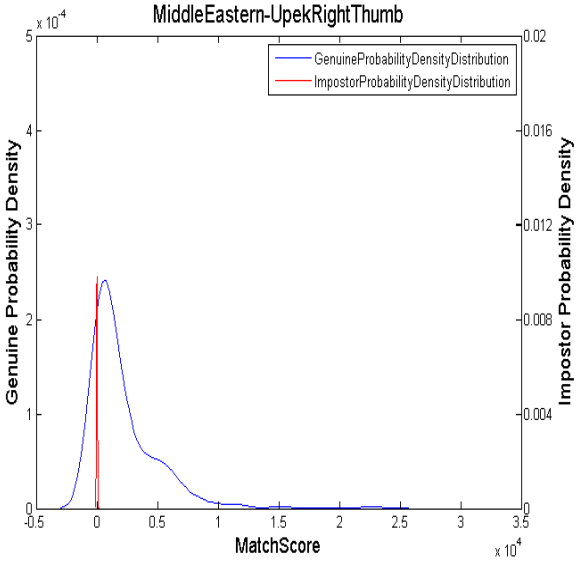
B.14. (v) Upek Eikon Touch 700-Right Thumb



(a)



(b)

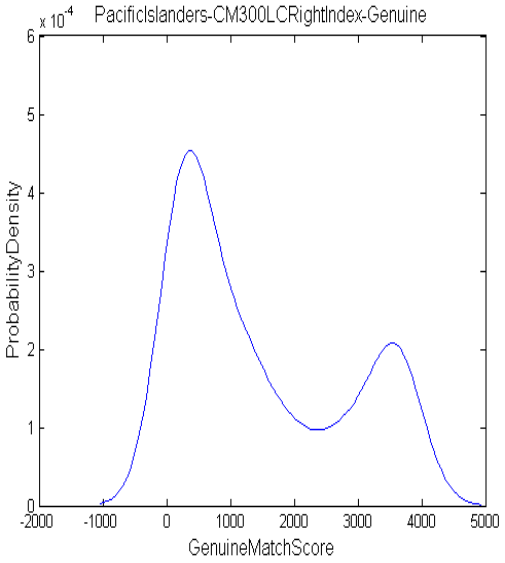


(c)

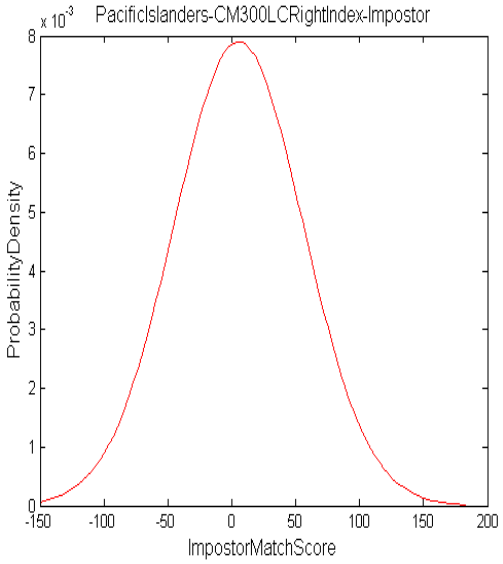
Figure B.14 (v): Match score distributions of right thumb images for Middle Eastern ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.15) Other Pacific Islanders

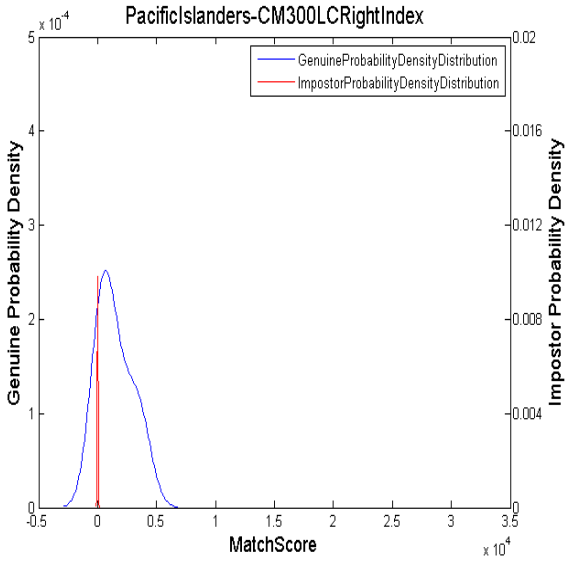
B.15. (i) Crossmatchverifier 300LC- Right Index



(a)



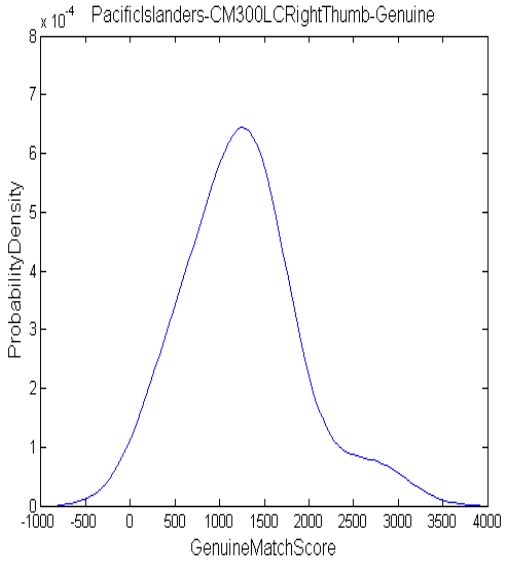
(b)



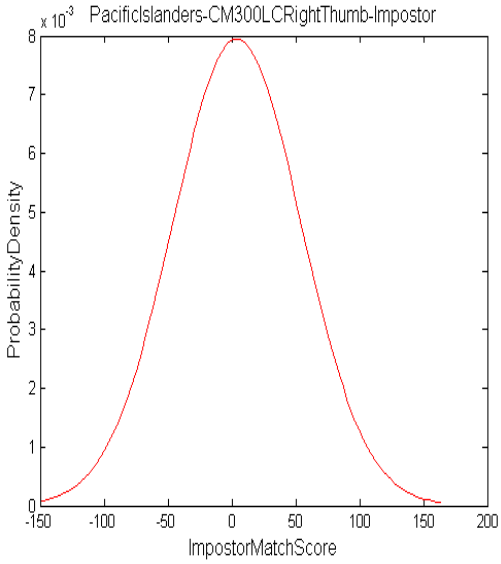
(c)

Figure B.15 (i): Match score distributions of right index images for Pacific Islanders ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

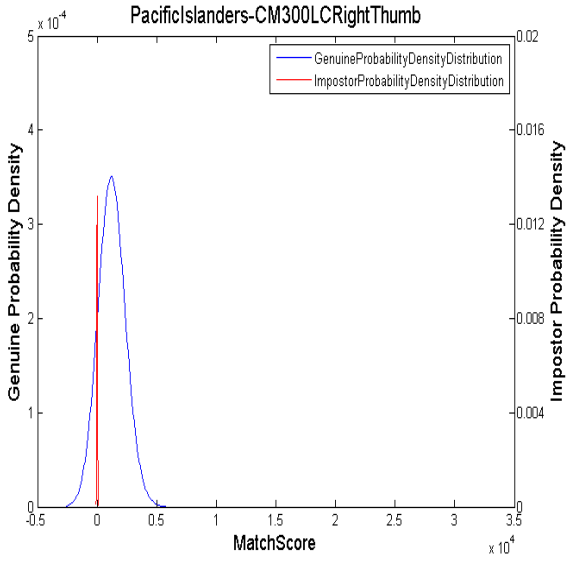
B.15. (ii) Crossmatchverifier 300LC- Right Thumb



(a)



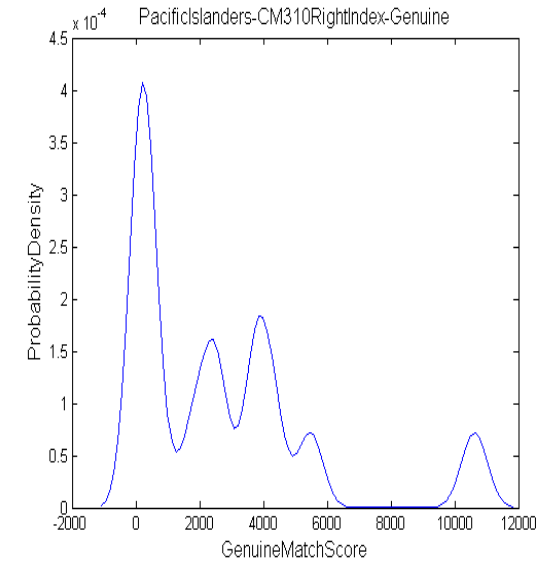
(b)



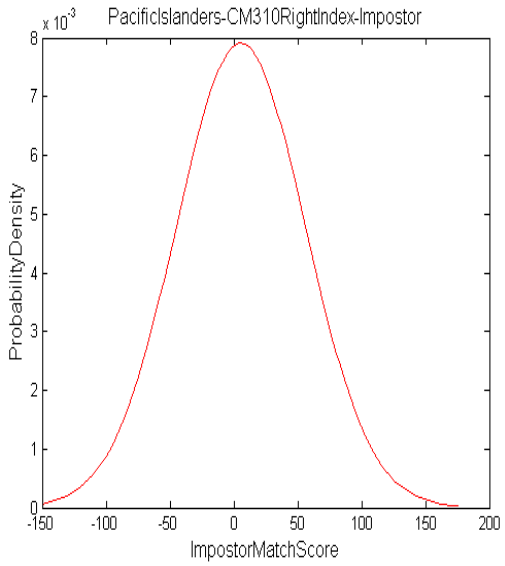
(c)

Figure B.15 (ii): Match score distributions of right thumb images for Pacific Islanders ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

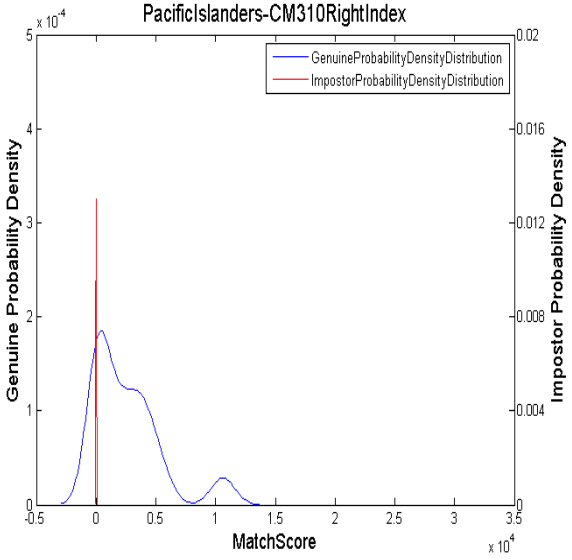
B.15. (iii) Crossmatchverifier 310- Right Index



(a)



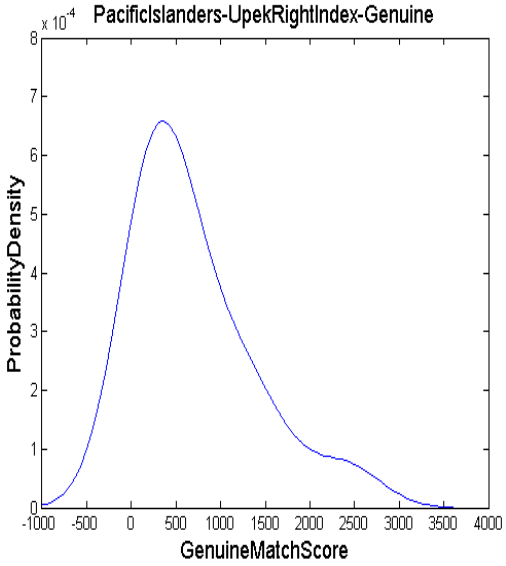
(b)



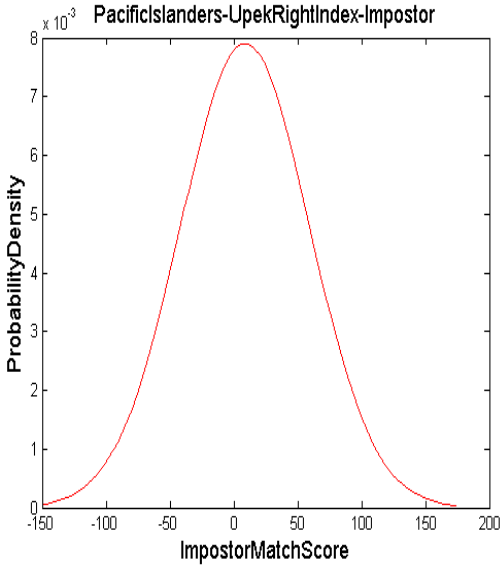
(c)

Figure B.15 (iii): Match score distributions of right index images for Pacific Islanders ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

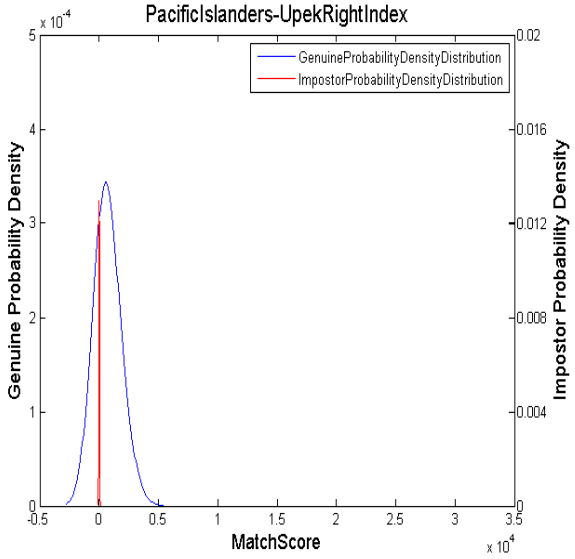
B.15. (iv) Upek Eikon Touch 700- Right Index



(a)



(b)



(c)

Figure B.15 (iv): Match score distributions of right index images for Pacific Islanders ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.15. (v) Upek Eikon Touch 700- Right Thumb

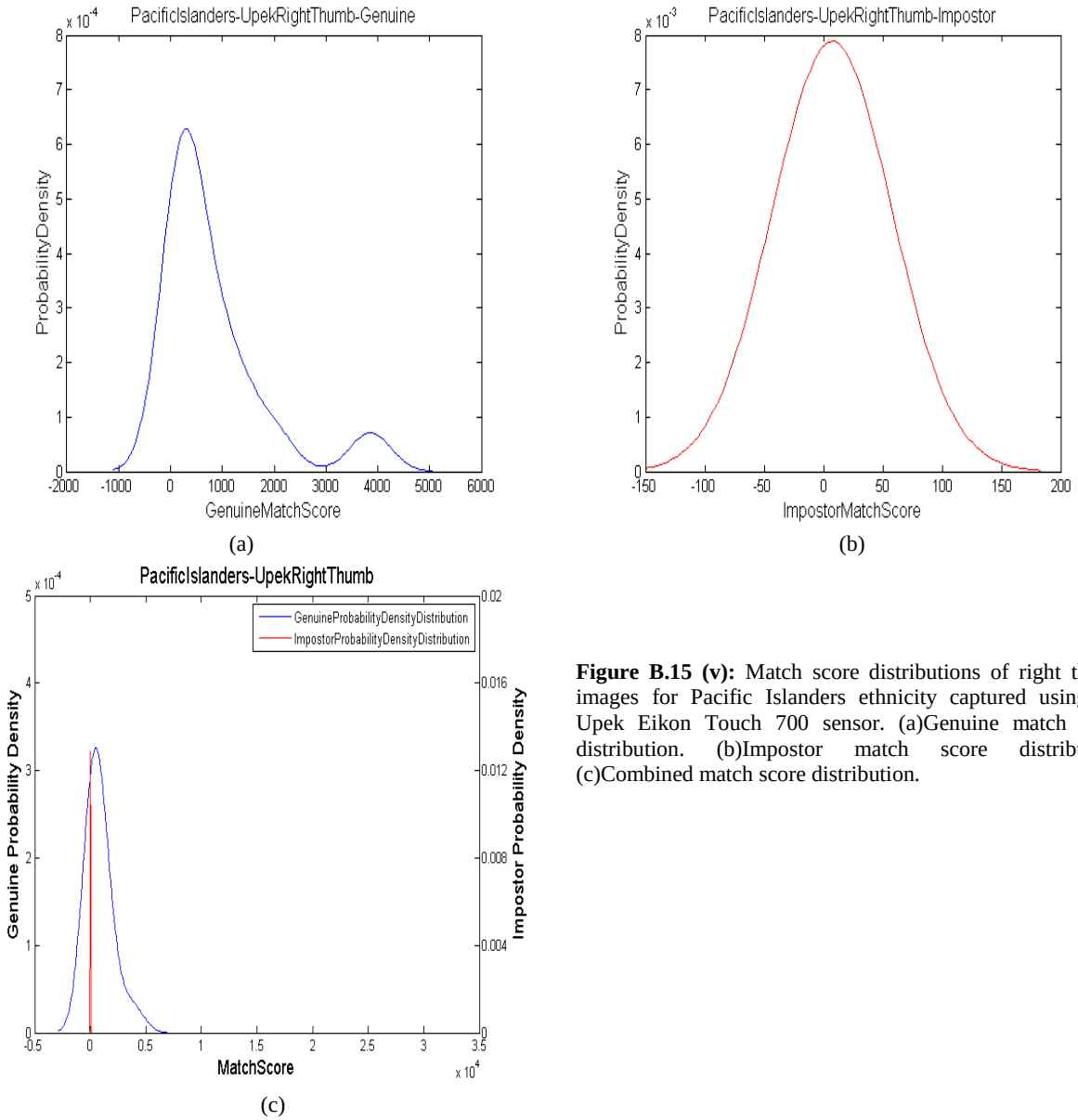
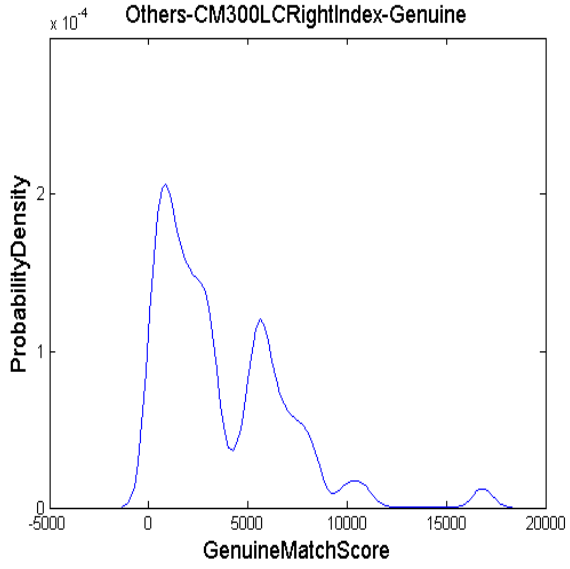


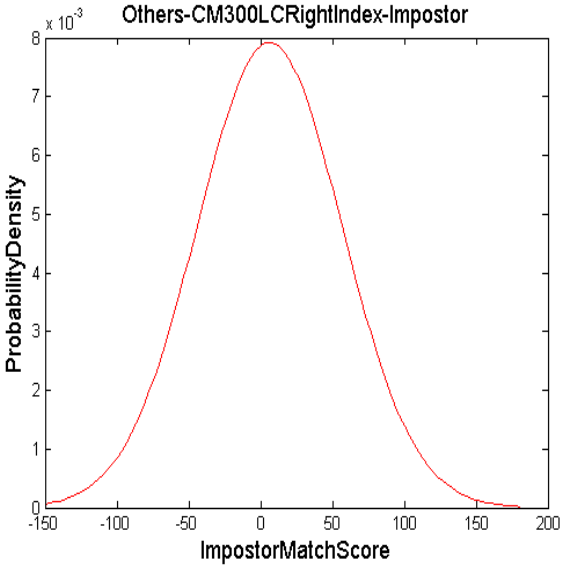
Figure B.15 (v): Match score distributions of right thumb images for Pacific Islanders ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

B.16) Others

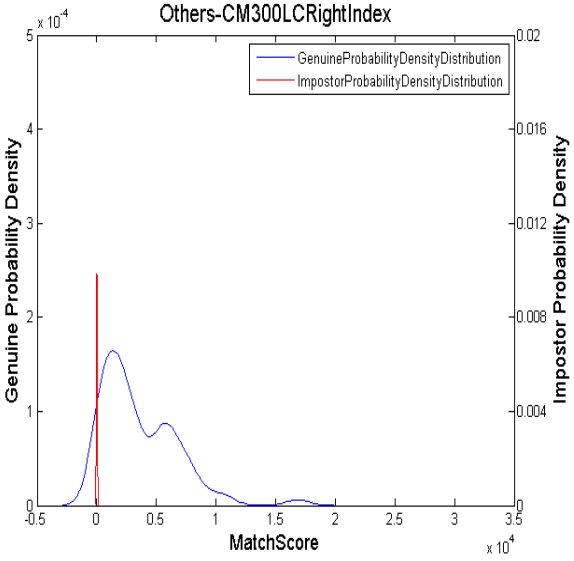
B.16. (i) Crossmatchverifier300LC – Right Index



(a)



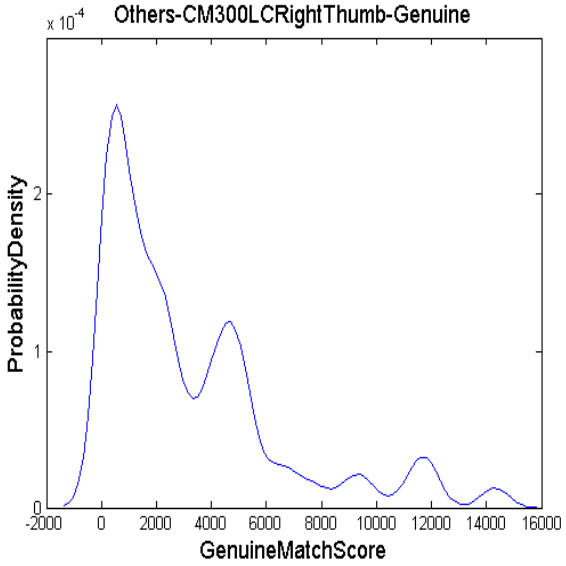
(b)



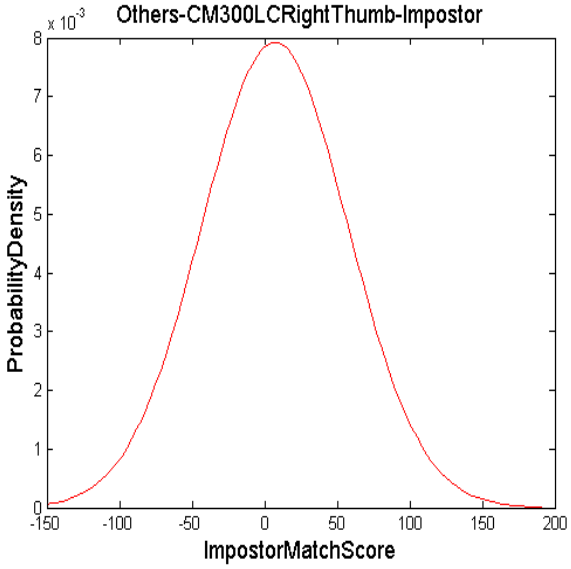
(c)

Figure B.16 (i): Match score distributions of right index images for Other ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

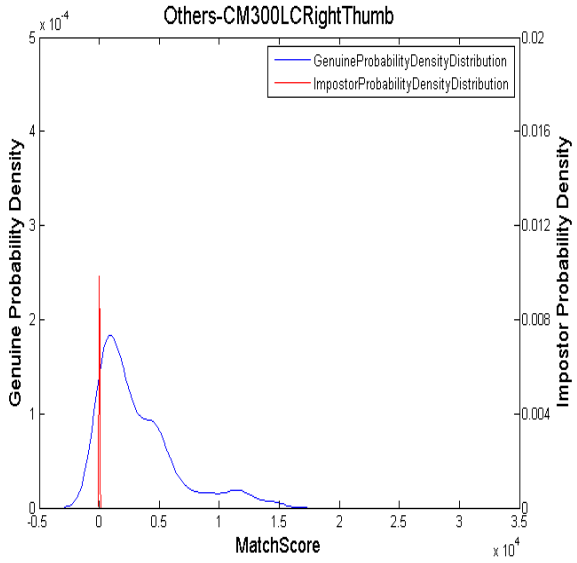
B.16. (ii) Crossmatchverifier300LC – Right Thumb



(a)



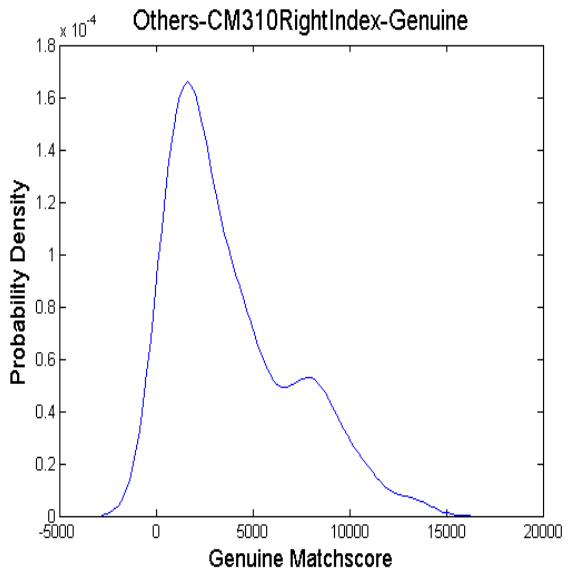
(b)



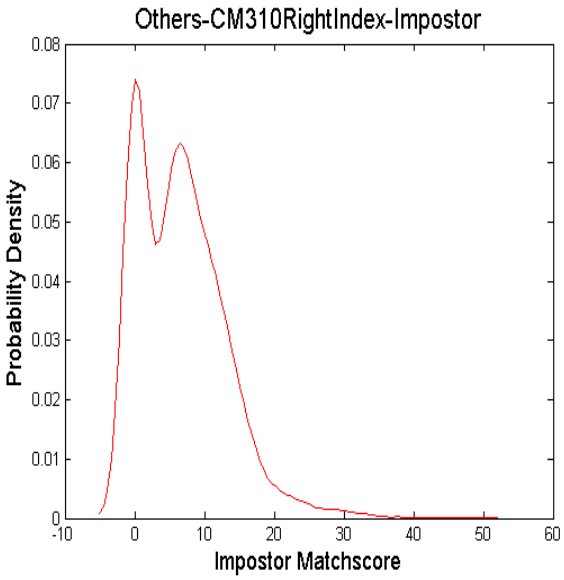
(c)

Figure B.16 (ii): Match score distributions of right thumb images for Other ethnicity captured using the Crossmatch Verifier 300LC sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

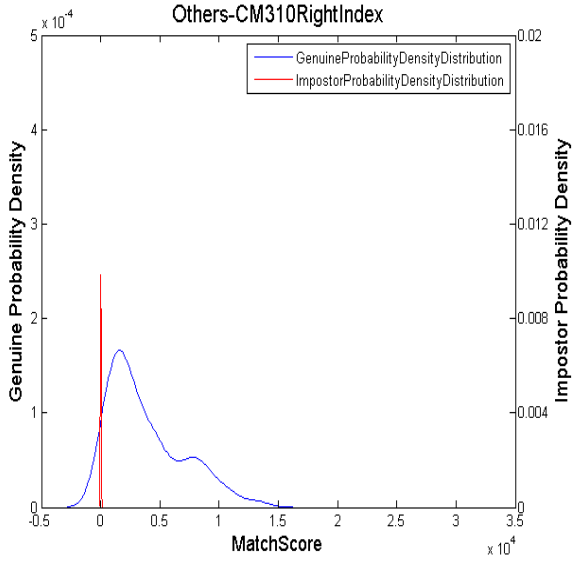
B.16. (iii) Crossmatchverifier310 – Right Index



(a)



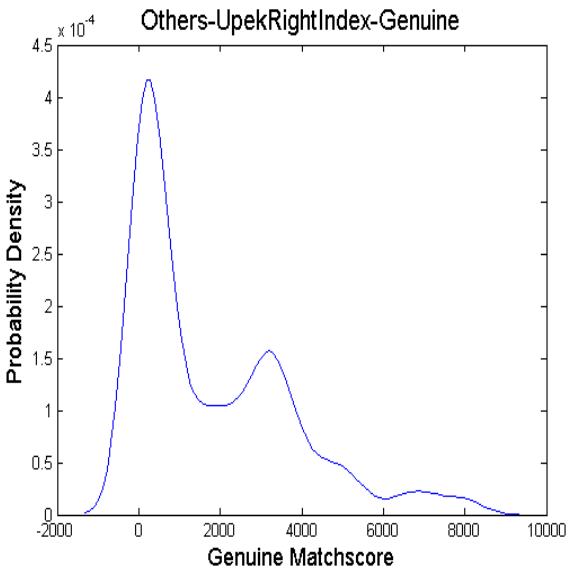
(b)



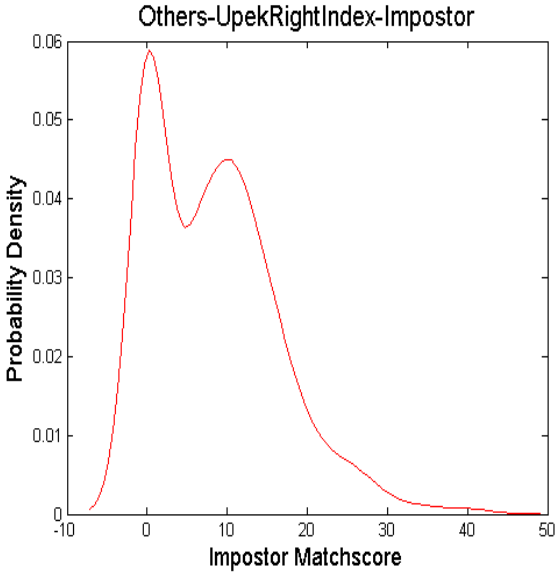
(c)

Figure B.16 (iii): Match score distributions of right index images for Other ethnicity captured using the Crossmatch Verifier 310 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

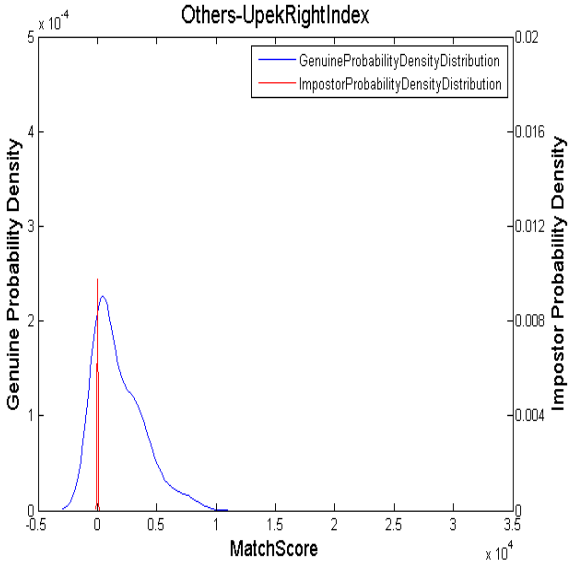
B.16. (iv) Upek Eikon Touch 700 – Right Index



(a)



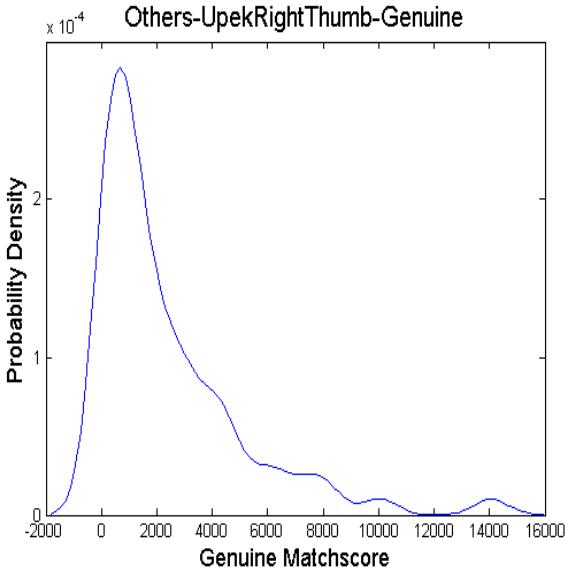
(b)



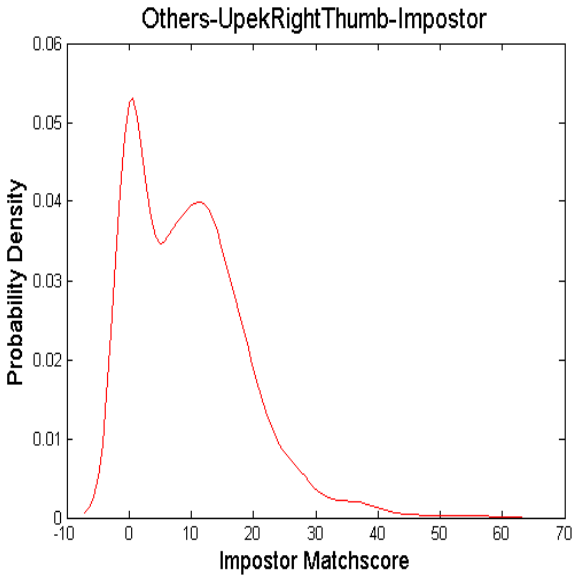
(c)

Figure B.16 (iv): Match score distributions of right index images for Other ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

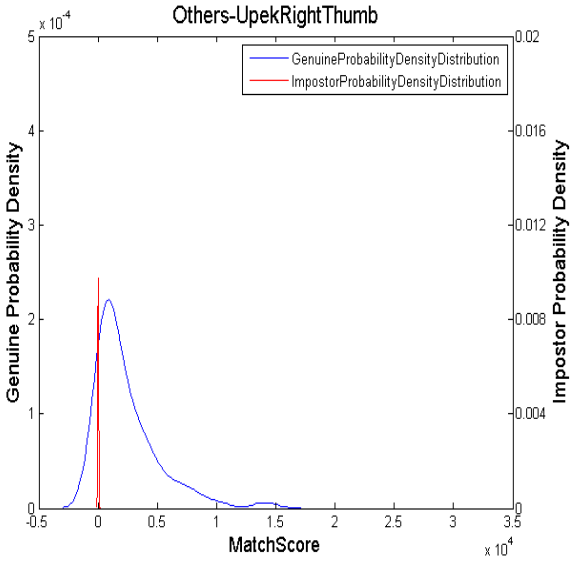
B.16. (v) Upek Eikon Touch 700 – Right Thumb



(a)



(b)

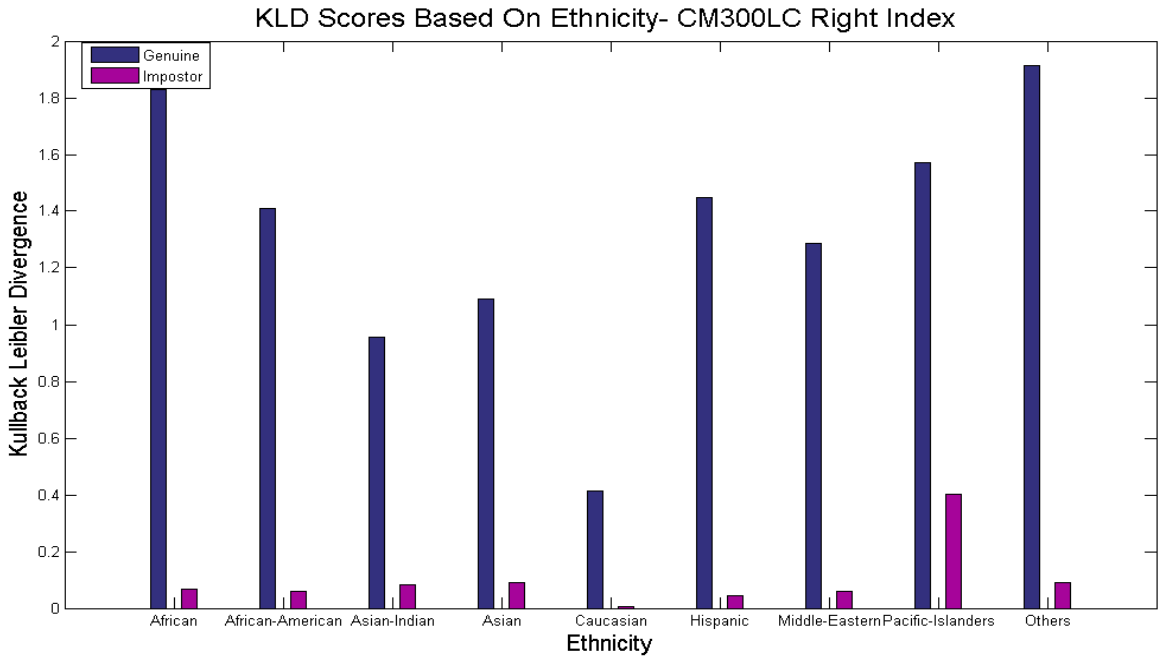


(c)

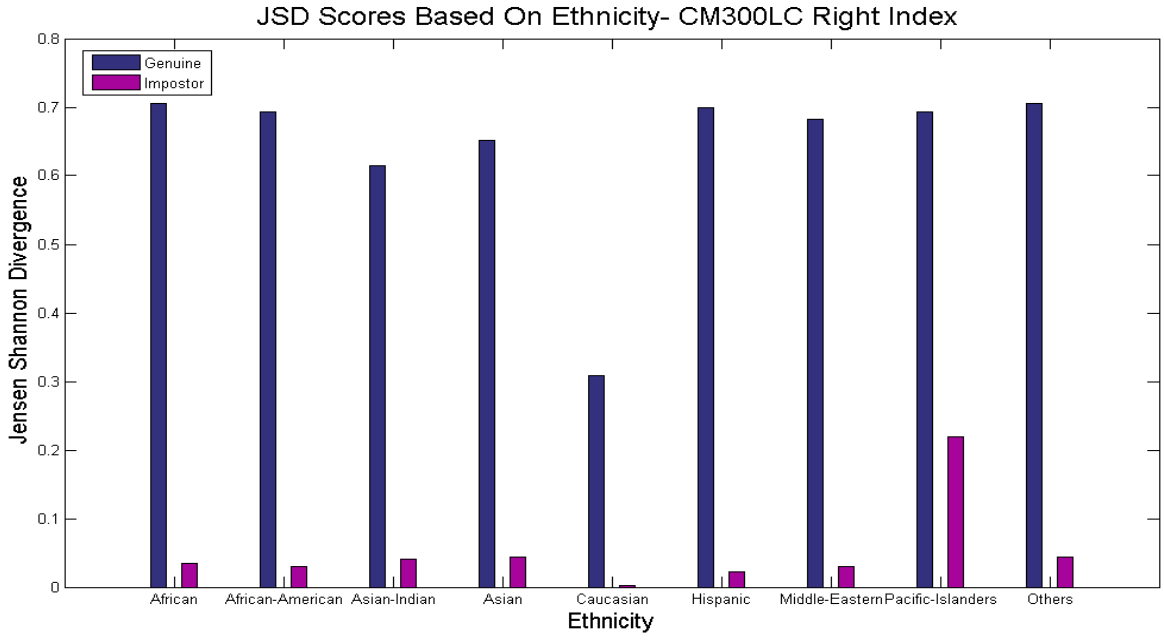
Figure B.16 (v): Match score distributions of right thumb images for Other ethnicity captured using the Upek Eikon Touch 700 sensor. (a)Genuine match score distribution. (b)Impostor match score distribution. (c)Combined match score distribution.

Ethnicity Based KLD and JSD Distributions

B.17. (i) KLD and JSD distribution for right index finger – Crossmatch Verifier 300LC



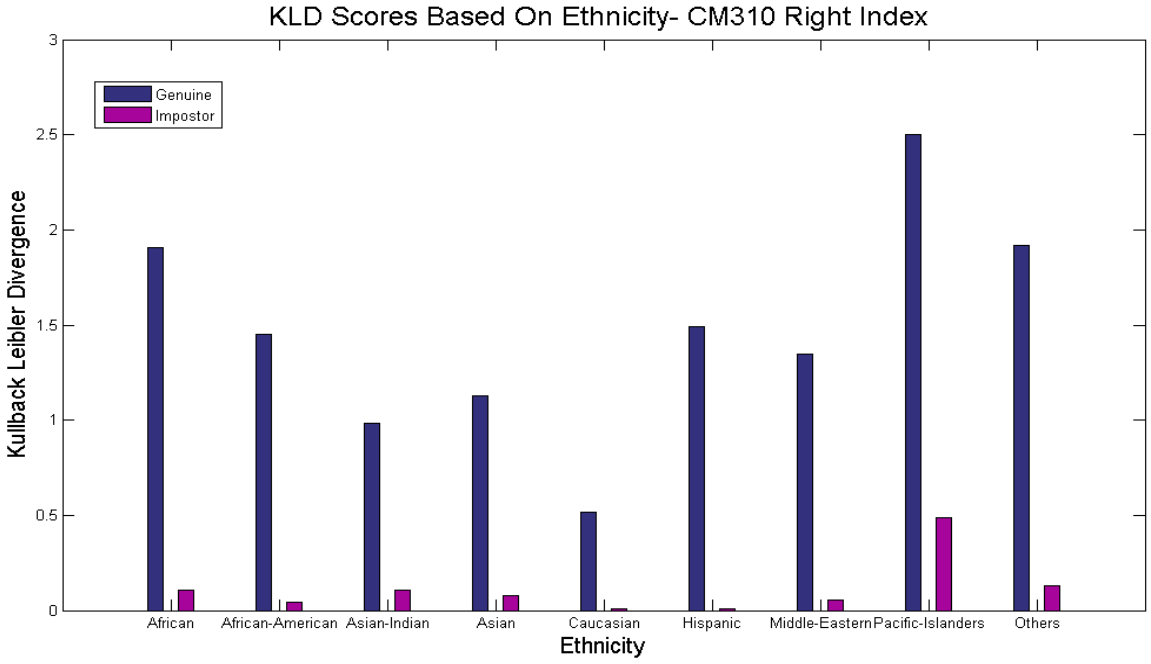
(a)



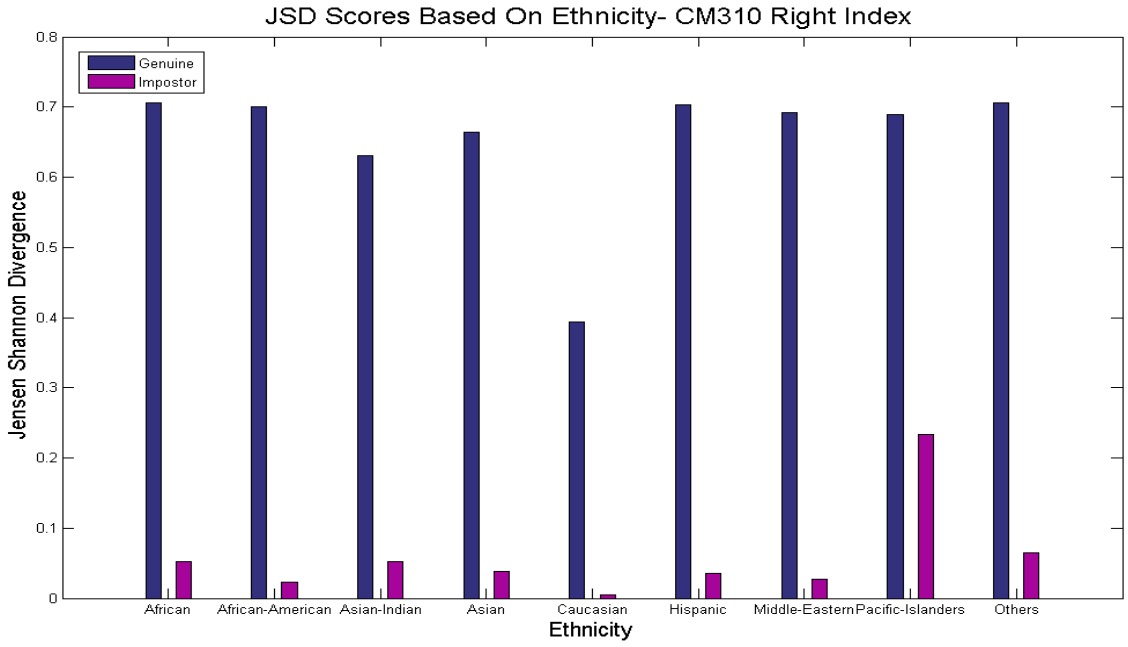
(b)

(i) KLD and JSD distributions of right index images obtained from Crossmatch Verifier 300LC

B.17. (ii) KLD and JSD distribution for right thumb finger – Crossmatch Verifier 310



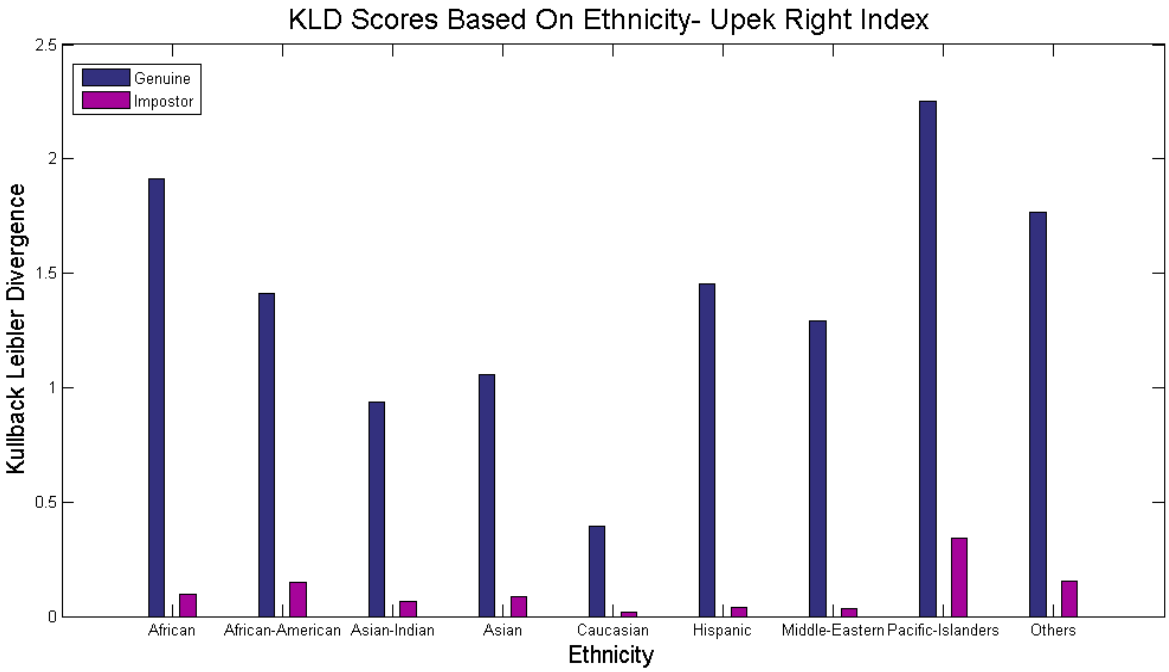
(a)



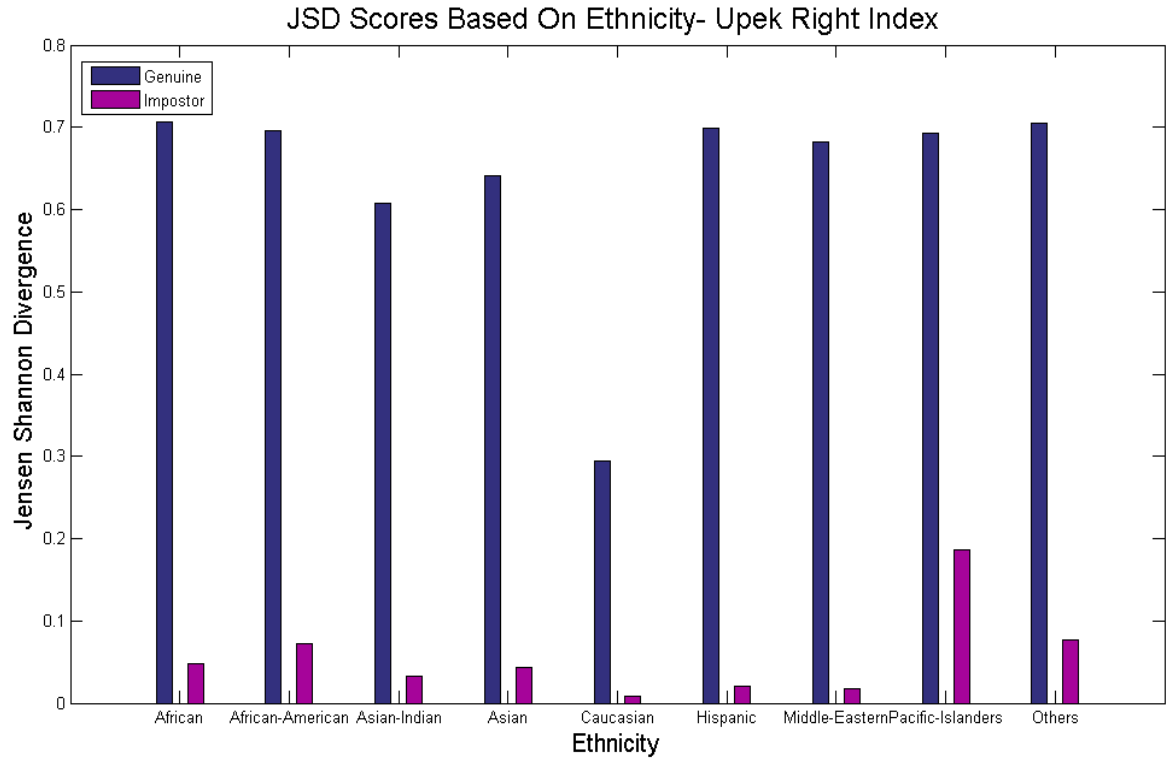
(b)

(ii) KLD and JSD distributions of right index images obtained from Crossmatch Verifier 310

B.17. (iii) KLD and JSD distribution for right index finger – Upek Eikon Touch 700



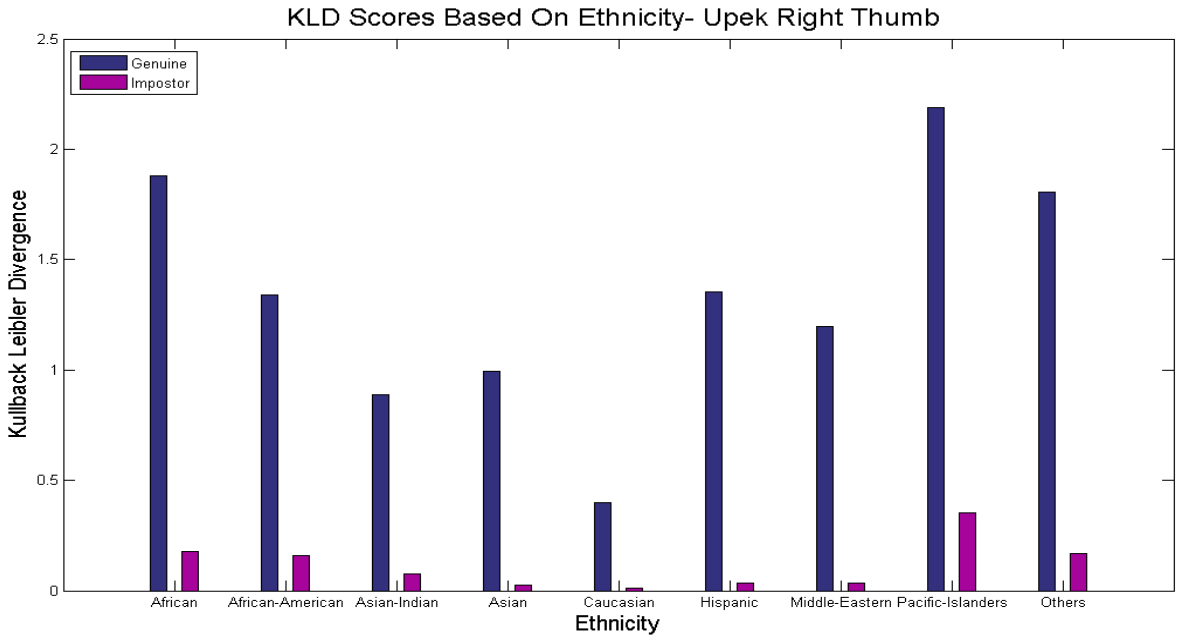
(a)



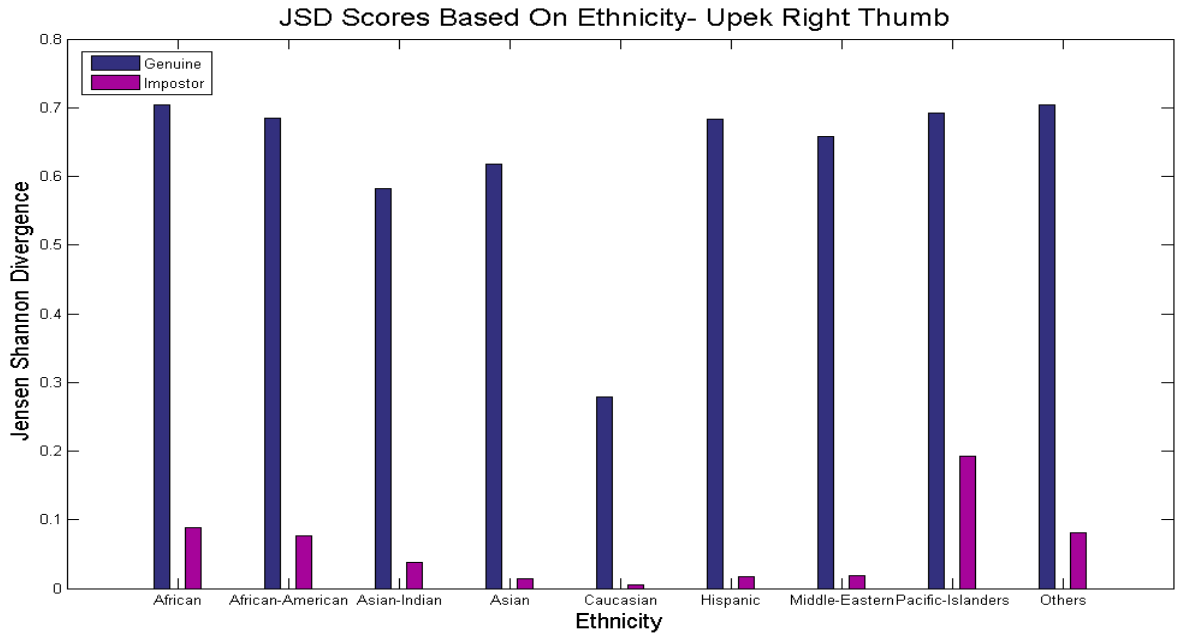
(b)

(iii) KLD and JSD distributions of right index images obtained from Upek Eikon Touch 700

B.17.(iv) KLD and JSD distribution for right thumb finger – Upek Eikon Touch 700



(a)



(b)

(iv) KLD and JSD distributions of right thumb images obtained from Upek Eikon Touch 700

References

[1] P. Jonathan. Phillips. Xiaobo An, Joseph Dunlop, Alice J.O' Toole, "Demographic Effects on Estimates of Automatic Face Recognition," in *IEEE*, 2011.

[2] Fahad Al-Harby, Rami Qahwaji, and Mumtaz Kamala, "The effects of gender differences in the acceptance of biometrics authentication," in *International Conference on CyberWorlds*, 2009.

[3] Thomas Bergmullery, Luca Debiasi ,Andreas Uhl and Zhenan Sun, "Impact of sensor ageing on iris recognition," in *IEEE*, 2014.

[4] Anil. K. Jain. and Arun Ross, "Introduction to Biometrics," in *Handbook of Biometrics*, Springer, 2007, pp. 1-20.

[5] Israa. M. Alsaadi, "Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 4, no. 12, 2015.

[6] Helen van de Haar, Darelle van Greunen and Dalenca Pottas, "The Characteristics of a Biometric," *IEEE, Information Security for South Africa*, 2013.

[7] Arun Ross, Saila Prabhakar and Anil K. Jain, "An Introduction to Biometric Recognition1," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004.

[8] Priyanka, "Fingerprint Recognition Techniques and its Applications," in *IEEE International Conference on Advances in Engineering & Technology Research*, Unnao, India, 2014.

[9] Jianjiang Feng, Karthik Nandakumar, Anil K. Jain, "FINGERPRINT MATCHING," in *The IEEE Computer Society*, 2010.

[10] Azad Noor, "A New Algorithm for Minutiae Extraction and," Brunel University, UK, Uxbridge, London, 2012.

[11] Ajay Kumar, Anil K. Jain, "Biometrics of Next Generation: An Overview," in *SECOND GENERATION BIOMETRICS*, Springer, 2010.

[12] James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric

Authentication Systems," in *Biometric Systems*.

[13] Michael D. Garris, Elham Tabassi, and Charles L. Wilson, "NIST Fingerprint Evaluations," *Proceedings of the IEEE,* vol. 94, no. 11, November 2006.

[14] Patrick J. Flynn, "Biometrics databases," in *Handbook of Biometrics*, Springer, 2007, pp. 529-547.

[15] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, "FVC2004: Third Fingerprint Verification Competition," International Conference on Biometric Authentication, Hong Kong, 2004.

[16] Davide Maltoni and Raffaele Cappelli, "Fingerprint Recognition," in *Handbook of Biometrics*, Springer, 2007, pp. 23-39.

[17] Soweon Yoon, "Fingerprint Recognition: Models and Applications," Michigan State University, Michigan, 2014.

[18] Guodong Guo, Guowang Mu ,"Joint Estimation of Age, Gender and Ethnicity: CCA vs. PLS," in *Automatic Face and Gesture Recognition, 10th IEEE International Conference and Workshops*, 2013.

[19] Shimon. K. Modi, "ANALYSIS OF FINGERPRINT SENSOR INTEROPERABILITY ON SYSTEM PERFORMANCE," Purdue University, West Lafayette, Indiana, 2008.

[20] Anil K. Jain, Yi Chen, Meltem Demirkus,"Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE,* vol. 29, no. 1, 2007.

[21] Atul S. Chaudhari, Sandip S. Patil "A Study and Review on Fingerprint Image Enhancement and Minutiae Extraction," *IOSR Journal of Computer Engineering,* vol. 9, no. 6, pp. 53-56, 2013.

[22] Lavanya B N, K B Raja, Venugopal K R and L M Patnaik, "Minutiae Extraction in Fingerprint using Gabor Filter Enhancement," in *International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 2009.

[23] Atul S. Chaudhari, Dr. Girish K. Patnaik, Sandip S. Patil, "Implementation of Minutiae Based Fingerprint Identification System using Crossing Number Concepts," *International Journal of Computer Trends and Technology (IJCTT),* vol. 8, no. 4, 2014.

[24] Feng Zhao, Xiaoou Tang, "Preprocessing and postprocessing for skeleton-based fingerprint

minutiae extraction," *The Journal Of The Pattern Recognition Society,* vol. 40, pp. 1270-1281, 2007.

[25] Tamer Uz, "Fingerprint Template Synthesis," University of Nevada, Reno, 2006.

[26] Jean-Christophe Petkovich, "A Fingerprint Identification System," Carleton University, Ottawa, Ontario, 2011.

[27] Davit Kocharyan, Hakob Sarukhanyan "Feature Extraction Techniques and Minutiae-Based Fingerprint Recognition Process," in *American V-King Scientific Publishing,* Armenia, 2010.

[28] ANIL K. JAIN, LIN HONG, SHARATH PANKANTI, RUUD BOLLE, "An Identity-Authentication System Using Fingerprints," *PROCEEDINGS OF THE IEEE,* vol. 85, no. 9, 1997.

[29] Qijun Zhao, Anil K. Jain , Nicholas G. Paulter Jr., Melissa Taylor ,"Fingerprint Image Synthesis based on Statistical Feature Models," *IEEE 5th International Conference,* 2012.

[30] Arun Ross, Member, Jidnya Shah, and Anil K. Jain , "From Template to Image: Reconstructing Fingerprints from Minutiae Points," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE,* vol. 29, no. 4, 2007.

[31] A. J. Mansfield, and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices," Centre for Mathematics and Scientific, National Physical Laboratory, Middlesex, 2002.

[32] [Online]. Available: https://semiengineering.com/biometrics-for-the-lot.

[33] M. E. Schuckers, Computational Methods in Biometric Authentication, Springer, 2010.

[34] V´aclav Maty´aˇs Jr. , Zdenˇek ˇR´ıha, Biometric Authentication Systems, University of Augsburg, 2000.

[35] RAVI. J, K. B. RAJA, VENUGOPAL. K. R, "FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING," *International Journal of Engineering Science and Technology,* vol. 1, no. 2, pp. 35-42, 2009.

[36] Craig Watson, Charles Wilson, Karen Marshall, Mike Indovina, Rob Snelick, "Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers," NIST, 2005.

[37] J. Lin, "Divergence Measures Based on the Shannon Entropy," *IEEE TRANSACTIONS ON*

INFORMATION THEORY, vol. 37, no. 1, 1991.

[38] Angel Garrido, Facultad de Ciencias de la UNED, "About some properties of the Kullback-Leibler divergence," *AMO - Advanced Modeling and Optimization,* vol. 11, no. 4, 2009.

[39] Don H. Johnson and Sinan Sinanovi´c, "Symmetrizing the Kullback-Leibler distance," Rice University, Houston, TX.

[40] Tim van Erven and Peter Harremoës,, "Rényi Divergence and Kullback–Leibler Divergence," *IEEE TRANSACTIONS ON INFORMATION THEORY,* vol. 60, no. 7, 2014.

[41] "MegaMatcher 5.0,VeriFinger 7.0, VeriLook5.5, VeriEye 2.8 and VeriSpeak 2.1 SDK Developer's Guide," Neurotechnology, 2014.

[42] "Large-scale AFIS and multi-biometric identification, Mega-Matcher SDK," Neurotechnology.