GUIDELINE TO COUNTER TERRORISM ON BASIS OF DIGITAL EVIDENCE (BIOMETRICS) IN PAKISTAN

By: Muhammad Ali Zafar

Roll No : UET–13F- MEM-CASE-40

Supervisor

Dr Asim Nisar

DEPARTMENT OF ENGINEERING MANAGEMENT
CENTRE FOR ADVANCED STUDIES IN ENGINEERING
UNIVERSITY OF ENGINEERING AND TECHNOLOGY
TAXILA

Fall 2014

Guideline to counter terrorism on basis of digital evidence (Biometrics) in Pakistan

A report submitted in partial fulfillment of the requirements for the M.Sc. Thesis

By: Muhammad Ali Zafar

Roll No : UET–13F- MEM-CASE-40

Approved by:

_____
Supervisor:

Dr Asim Nisar

_____
External Examiner:

DEPARTMENT OF ENGINEERING MANAGEMENT
CENTRE FOR ADVANCED STUDIES IN ENGINEERING
UNIVERSITY OF ENGINEERING AND TECHNOLOGY TAXILA

Fall 2014

DECLARATION

The substance of this thesis is the original work of the author and due references and acknowledgements have been made, where necessary, to the work of others. No part of this thesis has been already accepted for any degree, and it is not being currently submitted in candidature of any degree.

_____

Name Muhammad Ali

Roll No : UET–13F- MEM-CASE-40

M.Sc. Thesis Scholar

Countersigned:

_____

Name Dr Asim Nisar

Thesis Supervisor

DEDICATION

This work is dedicated to my supervisor, family, my co-workers, and friends and above all to the people of Pakistan. This is an endeavor to help and guide all my brothers and sisters who are working to fight for peace and prosperity of Pakistan.

ACKNOWLEDGEMENT

In the name of Allah Almighty who is the most Gracious, most Merciful and Creator of Universe. I am grateful to God almighty who has given me the strength and ability to understand and bring out best of my abilities as bestowed by him unto me to accomplish my thesis work on time and in best of my abilities.

I would like to thank and express my sincerest gratitude towards my supervisor Dr Asim Nisar, for his guidance, support, motivation, encouragement, optimistic attitude towards my research work and motivation throughout the thesis work. It was really a nice experience to work under his supervision.

I am very thankful to my family for supporting, understanding and realizing the importance of the work I am doing for the wellbeing of my country. I am thankful to my parent who have prayed and wished me good luck in my thesis work.

I am also very thankful to all my colleagues and friends who have helped me understanding the issues and rectifying me at the time when it was dire required to be on the focused and candid approach towards my research question.

I am grateful to my seniors for helping and guiding me in my thesis research. I am grateful to all who are working in specialized setups and are doing their best to counter the menace of terrorism in Pakistan.

ABSTRACT

Currently state of Pakistan is facing extreme ideological threats. Sectarian clashes, terrorism and political rift amongst different political parties is giving rise to this threat. Terrorists are group of individuals who consider their self-fabricated ideology more authoritative than the sovereignty and ideology of Pakistan. They want power to implement their ruthless Laws. They are trying to take over the country by killing civilians, policeman, army men through sabotage, subversion and crippling the political and economic standing of the country globally.

In response, Law Enforcement Agencies (LEA) in Pakistan are trying to apprehend these terrorists. In doing so use of Digital Evidence (Biometrics) can help and lead to higher success. Currently the existing investigation procedures of the criminals and terrorists are not very effective as on Dec 1, 2013 Tehrik-i-Taliban Pakistan claimed responsibility of killing four policemen on Nov 27, 2013 at Hyderabad. Yet police was unable to prove them guilty. The terrorist's cases last for many years without final verdict by the judge. This is mostly because of poor investigation and lack of Digital evidence (Biometrics) against the terrorists to prove them guilty in court of Law. This problem exists because of non-availability of digital evidence against terrorists and lack of crime data.

This paper aims at bringing up guidelines for use of digital evidence (Biometrics) to counter terrorism in Pakistan. Biometric evidence can help in providing sufficient pieces of evidence. These pieces of Evidence are sufficient to prove suspected individuals guilty in court of Law. Also, to invoke the need to understand and modify the existing judiciary process against terrorists.

Keywords: Digital Evidence, Biometrics, Criminals, Terrorists, Investigation Procedure

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS & ACRONYMS

LEA Law Enforcement Agencies

FIA Federal Investigation Authority

ISI Inter service Intelligence

FC Frontier Constabulary

THESIS KEYWORDS

Digital Evidence

Biometrics

Criminals

Terrorists

Investigation Procedures

LIST OF USEFUL WEBSITES

http://www.bmgi.com

http://www.allpklaws.com/

https://www.google.com.pk/?gws_rd=cr,ssl&ei=vR1OVJ_jIernygPz74LYDQ#q=biometric+definition+

https://www.google.com.pk/?gws_rd=cr,ssl&ei=vR1OVJ_jIernygPz74LYDQ#q=digital+evidence+definition

https://www.youtube.com/watch?v=fmF0jZtZCRQ&hd=1 (Reliability Test, Cronbach's Alpha)

https://www.youtube.com/watch?v=VOI5IlHfZVE&hd=1 (Pearson Correlation-SPSS)

https://www.youtube.com/watch?v=0AGLdgUtIJg&hd=1 (Linear regression Part 1)

https://www.youtube.com/watch?v=VEQPX6d-EQw&src_vid=0AGLdgUtIJg&feature=iv&annotation_id=annotation_494077&hd=1 (Linear Regression) Part 2

https://www.youtube.com/watch?v=LPoy_dfuTFU (Part 3)

https://www.youtube.com/watch?v=LPoy_dfuTFU&hd=1 (Part 4)

http://punjabpolice.gov.pk/crimesstatistics (Punjab Police)

http://www.pbs.gov.pk/content/data-request-form (Bureau of statistics)

https://www.youtube.com/watch?v=hdsqMVY118U&hd=1 (NVIVO audio coding)

BACKGROUND

On 11th September 2001 terrorists attacks on United States (US) in which thousands of innocent lives were lost. Followed by the invasion of US in Afghanistan has inter-mingled the political, security and democratic issues between Pakistan and US. This incident had led Pakistan to an unwanted and undesired war which was led by US. Pakistan has fought well in this war, its contribution to eliminate the terrorists is commendable. Having said so, Pakistan has also become a victim of terrorism. It has been estimated that cost of this war both on direct and indirect fronts have been approximated to US$ 35 billion (caci analyst, n.d.).

There has been a constant increase in number of terrorists attack on Pakistani soil. Thousands of Pakistanis have suffered causalities and hundreds of them have lost their lives in this fight against terrorism. According to statistics, number of fatalities in war against terrorism in Pakistan have reached to a death toll of 19702 civilians and 6003 security forces personel (satp.org, n.d.) From 2003 to Nov 2014. This also includes assassination attempts on Prime Minister of Pakistan Benazir Bhutto and former head of Pakistan's Army Special Services Group, Maj. Gen. (Rtd) Ameer Faisal Alvi.

It is also important to understand that Pakistan has diversification in its population. We have four provinces representing different sects, cultures, ethnic values and lifestyle. Religious practices which are being performed in pakistan varies throughout, yet we all follow and believe in Almighty Allah as it needs to be. Pakistan is also falling apart when it comes to economic statistics. Fighting a war which has never been owned by Pakistan is causing huge tangible and intangible loses to Pakistan. Pakistan is paying a very high price for fighting in this war to counter terrorism. Currently unemployment, political unrest, lack of justice and prolonged justice, health issues, lawlessness are also contributing towards economic downfall of the country.

Keeping in view the current economic and political instability in country. Many splinter groups and street criminals are being funded to carry out unrest activities in the country. Different organizations and jihadist movements are taking advantage of the current wobbly state of our country. They are hiring individuals from these groups to do their dirty work (caci analyst, n.d.). They are causing subversion and are sabotaging the political hierarchical system. They are inflicting causalities to law enforcement agencies by bombing, killing innocent Pakistanis,

thrashing the justice system of Pakistan by threatening judges and lawyers. It is a high time indeed that Pakistan should take corrective action in its policy making. Pakistan should address the root causes to eliminate the terrorism which has deeply rooted in Pakistan, otherwise it will not only persist but also get worse with time.

Currently, Pakistan is taking many counter measures to address the issue of countering these terrorist organizations. It has been training its force on special lines to seek advantage over these terrorists. Some reforms in judicial system has been formulated in black and white only, however their implementation is not fully practiced to address the issue. Centralizing the data base of NADRA to keep a check on the population growth, is a good step in this regard. It will help in monitoring the population by their family tree and also to keep the track of population growth. However still there is margin of doing more to tackle the lawless ness created by these terrorist organizations. Collection and use of evidence collected from the blast scenes is very rear in this regard. Collection of evidence from blast scene has many benefits like, if evidence is collected from blast scene, it can contain information like, how blast has occurred, what was used in the blast, how much explosives have been used, how the bomb was planted, how the terrorist has approached the blast scene and biometric data like DNA of the suicidal can be collected from the blast scene. Now the data collected can be used for future purposes as well. It can be stored centrally for easy access between different agencies for cross referencing during the investigation process of terrorists.

In doing so there are many problem areas which are hampering the evidence collection and its processing like, provision of law to accommodate the digital evidence in form of biometrics, the contamination of crime scene from unwanted people. No proper chain of custody of evidence collected is maintained. No central access of the data collected. Also the evidence collected from these terrorists hide outs by security forces and at times by police is not fully gathered and stored at a centralized location for further analysis and future reference.

TABLE OF CONTENTS

1 CHAPTER ONE: INTRODUCTION

1.1 Introduction and Background

The history of terrorism is referred to as the history of well-known and significant historical individuals, entities, incidents associated with it, whether they are right or wrong, with terrorism. The literature available and scholars agree that terrorism is a disputed term, and those who are labelled terrorists describe themselves as such. It is very common for the opponents in a violent conflict to describe the other side as terrorists or practicing terrorism. (Reynold, 2005)

How broadly the term terrorism can be defined, the roots and practice of terrorism can be traced back to the 1st Century AD Sicari Zealots. The term Sicari in Latin can be translated as the "dagger man" (Goodman, 2008). The term was applied immediately the decades preceding the destruction of Jerusalem in 70 CE, to an extremist splinter group (Goodman, 2008) of Jewish Zealots, who attempted to banish the Romans and their partisans from the Roman province of Judea (Goodman, 2008) was in fact terrorists. First ever use in English language of the term terrorism occurred during the French revolution's Reign of Terror, where the Jacobins, who were ruling a revolutionary state, employed violence, including mass executions by guillotine, this was to compel obedience to the state and intimidate regime enemies. This association of the term with state violence lasted till mid-nineteenth century. After this period the term started to emerge with non-governmental groups. Some examples like Anarchism, often in league with rising nationalism and anti-monarchism, they were the most prominent ideologies which were linked with terrorism.

At the end of nineteenth century anarchist groups or individuals committed assassinations of a Russian Tsar and US president as well. While in twentieth century the term terrorism continued to be associated with a vast array of anarchist, socialist, fascist and national groups, many of them are engaged in third world anti-colonial struggles.

1.1.1 Modern day terrorism

Terrorism is associated with the Reign of terror in France until in mid-nineteenth century. After that the term was associated with non-governmental groups like anarchism, mostly rising with nationalism, a prominent ideology which is linked with terrorism. In nineteenth century more powerful, stable and affordable explosives were developed. Globalization has reached to an unprecedented level and mostly radical political movement became widely influential. The use of dynamite, in particular, inspired anarchists and it centralised their strategic thinking as well.

1.1.2 Brief history of terrorism stricken Countries

There are many example of country who have been a victim of terrorism or served as a cradle for the terrorism to nourish. Modern terrorists techniques started to emerge from Ireland. They fought against years of years of English rule, the famous Fenian Brotherhood and it's off shoot the Irish republican brotherhood were founded in 1858 as a revolutionary and militant nationalist groups. In United States, prior to civil war john brown (1800-1859) advocated and practiced armed opposition to slavery, leading several attacks between 1856 and 1859. A biographer of Brown was written that brown's purpose was to force the nation into a new political pattern by creating terror (Scott). Then in Ottoman Empire the Armenian Revolutionary Federation used violence against the government. In early 20th century the concept of revolutionary political violence against western colonial powers continued to its peaks. In Palestine different groups fought British in 1930s. The women suffrage movement had committed terrorist attacks prior to First World War. Then in 1916 the Easter Rising seized the Dublin post office and several other building claiming the freedom of the Irish Republic. During the resistance in Second World War, destruction of railways and communication infrastructure of western France was organised by special services executives. After math of the Second World War led to the anti-colonial campaigns against the collapsing European empires. Then during the cold war both US and Russia have shifted to proxy wars against each other in a covertly manner. In Middle East different organisation have formed at different periods started from 1928 to present day. All of them were working under the umbrella of government. National Liberation front, popular front for the Liberation of Palestine, Democratic front for the Liberation of Palestine, peoples mujahidin of Iran, Khomeini revolution, Armenian secret army for Liberation of Armenia during the Lebanese Civil War are some of the active organisation who have been carrying out acts of violence. Likewise there have been violence in Asia, Europe, Africa which has been organised by the sitting governments at times and at times by the people who are working against the government.

1.1.3 Terrorism in 20th Century

Major event which took place after September 11 attacks on US soil are Moscow theatre siege, Istanbul bombings, Madrid train bombing, Beslan school hostage crisis, London bombing in 2005, New Delhi bombings, Mumbai hotel siege and Norway attacks. Formation of Al-Qaeda in 1988, many terrorist act in and outside US have been carried out by this organisation, which includes bombings of two US embassies in Africa, USS Cole bombing, September 11, 2001 twin tower attack, attack on Pentagon. After this, series of terrorist's events have started with in invasion of US on Afghanistan.

The attacks on world trade centre and the pentagon had begun a new concept of evolution in the definition of word terrorism. Terrorism is the result of extremism which results in different form of manifestation of violence. The ultimate sufferers are the innocent peoples who have actually nothing to do with the new and complex world order. Terrorism is the tree and extremism provides the food and necessary nourishing ingredient for it to grow. There is a very famous saying that ***One Man's terrorist is another man's freedom fighter.*** This off-repeated statement reflects genuine doubts about what constitutes terrorism.

1.1.4 Terrorism in Pakistan

Pakistan is a very vibrant country. It has traditions and culture, which distinguishes it from the rest of the world. Pakistan is located at a very important geo-strategic location as far as south Asia is concerned. Pakistan is the future industrial hub which has both the access to warm waters and also the ground trade route to several neighbouring countries. Pakistan enjoys its relationship with its neighbours. Internal and external stability of the Pakistan is highly influenced with the stability of its neighbouring countries. With the invasion of United States on Afghanistan and terrorism against the US forces in Afghanistan at its peak it, the unstable Afghanistan both politically and internally is always a threat to the sovureniety of Pakistan.

Although the acts of terrorism are visible everywhere in world. Yet, Pakistan is facing this menace of terrorism directly and severely as a social problem. Pakistan has been a prime victim of terrorism. Pakistan right now is in front line state among international community working and fighting against terrorism, which is leading directly the people of Pakistan to face its outrage in shape of terrorists acts killing civilians every day. Pakistan is playing its role very effectively to curb terrorism and militant groups. This terrorism has many devastating effects on people of Pakistan. Sense of insecurity prevails everywhere in the country. Terrorism has enhanced intolerance and fear amongst masses. Terrorism is the biggest social evil these days in Pakistan. Terrorism has hit negatively to Pakistan's economy, society, socio-economic and political problems. The social workers who are considered to be the catalytic chain for social changes are badly effected in this war against terrorism.

Pakistan in response to these terrorists' activities is preparing its forces and building up the resources to counter it. Pakistan Armed Forces are currently involved in extensive operations against these terrorist in many parts of the country. More than fifty (50) thousand causalities of civilians, armed personel have occurred up till now. Security forces of Pakistan, Law enforcement agencies LEAs, intelligence agencies, police department are carrying out extensive apprehension and investigation of these terrorists. These terrorists are put to trial in front of courts for conviction. There have been many instances when these terrorist, who have

committed innocent killing and are involved in the various activities which are against the sovureniety of the pakistan are set free in our judicial system. It is very sad to know that, all the effort which has been put in arresting them and carrying out operations on extensively large scale by Pakistan forces are multiplied with zero.

1.2 Purpose

Currently state of Pakistan is facing extreme ideological threats. Sectarian clashes, Terrorism and Political rift amongst different political parties is giving rise to this threat. Terrorist are group of individuals who consider their self-fabricated ideology more authoritative than the sovereignty and ideology of Pakistan. They want power to implement their ruthless Laws. They are trying to take over the country by killing civilians, policemen, army men through sabotage, subversion and crippling the political and economic standing of the country globally.

In response, Law enforcement Agencies (LEA) in Pakistan are trying to apprehend these terrorists. In doing so use of Biometric technology can help and lead to higher success. Currently the existing investigating procedures of the criminals and terrorists are not very effective as on Dec 1, 2013 Tehrik-i-Taliban Pakistan claimed responsibility of killing four policemen on Nov 27, 2013 at Hyderabad. Yet Police was unable to prove them guilty (Dawn, n.d.) The Terrorists cases lasts for many years without final verdict by the judge (Times, n.d.). This is mostly because of poor investigation and lack of evidence against the terrorists to prove them guilty in court of Law. This problem exists because of non-availability of evidence against terrorists and lack of crime data (Ozgul Faith, 2007)

Biometrics refers to the identification of human beings by their physical characteristics or traits. Several different techniques are used in Biometrics which are Facial Recognition (based on measuring change in Facial Expression), IRIS (it is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil) , Study of finger and Thumb Impressions, Identifying Deoxyribonucleic acid (DNA) patterns (it refers to a molecule that encodes the genes used in the development and functioning of all known living organisms), study of blood and hair samples of individuals.

Biometric Technology is very helpful in this regard. Biometric Evidence can help in providing sufficient pieces of evidence. These pieces of Evidence are sufficient to prove suspected individual guilty in court of Law. DNA technique of biometric collection has led to new twist in unsolved Terror Case of Ex-Red Army Faction (RAF) member Verena Becker in murder of West Germany's Chief Federal Prosecutor Siegfried Buback on April 7, 1977. (International, n.d.)

1.3 Scope of Work

The thesis work comprises on exploring the use of digital evidence especially biometric during the investigation and apprehension process of the criminals/terrorists in Pakistan. This research work contains both the qualitative and quantitative data to analyze the working of different investigating departments of Pakistan. Data obtained from qualitative and quantitative techniques have been analytically analyzed and interpreted on SPSS and NVIVO tools respectively. Quantitative data was used to evaluate the general consensus of the target sample population about the use of biometric technology in investigation and apprehension of terrorists/criminals. Analysis is performed on the results obtained by using statistical methods in SPSS. The target population is general public, students, investigating officers both from police and intelligence departments, lawyers and Law Enforcement Agency (LEA) people.

However qualitative approach for data collection was used to find out in depth and underlying problems faced by different tires of investigation process both from police and intelligence departments, lawyers and Law Enforcement Agency (LEA) people. Data collected is empirical. To collect this data interviews have been conducted and analyzed in tool NVIVO. Different themes originating from the data collected have been transmuted on various nodes to see the relationship between different themes. Then models are generated from these themes to identify the problems and legal issues faced by the people who are arresting and apprehending the terrorists. Basing on the problems and legal issues highlighted, guidelines have been formulated for the use of biometrics as digital evidence in Pakistan.

In the end results obtained from both research methodologies have been super imposed to find the perfect solution in form of guidelines. These guidelines have been proposed to facilitate the working of different intelligence departments and LEA's.

1.4 Research Title

The Research title for thesis is

Guideline to counter terrorism on basis of digital evidence (Biometrics) in Pakistan

1.5 Significance of the Study

There are many concerns regarding the criminals/terrorists which are been apprehended by Pakistani law enforcement agencies, intelligence agencies and police. To understand these, it's important to understand firstly, the working dynamics and present security situation of Pakistan. Pakistan is currently facing a huge sectarian clash between different communities which are present in Pakistan. The security and lawlessness situation in Pakistan is at its peak.

Political unrest in the country is also disturbing the working environment of different government organizations which are covertly and overtly working in Pakistan.

Keeping in view, internationally recognized and esteemed involvement of Pakistan in war against terrorism and present deranged internal affairs. There are many questions as to why these apprehended terrorists are not being convicted and punished in court of law. There can be many reasons to this question. One of the reasons is the lack of digital evidence in form of biometrics against these terrorists/criminals. Evidence can play a vital role in investigation and apprehension of these terrorists/criminals. With use of digitized evidence in biometric form will lead to greater number of apprehension and successful investigations of the criminals /terrorists.

Nowadays advancement of technology has led to a web of different and new technological forms of evidences. Digital Evidence in form of biometric is one of those. Digital Evidence is all digital information that may be used as evidence in a case. The collection and gathering of digital information may be carried out by confiscating any storage media (data carrier), tapping or monitoring any visual imagery or making of any digital copies like forensic images etc. Biometric technology is very effective in use. Use of biometric based evidence has advantages in the investigation and authentication over the conventional investigation and authentication methods (Wayman, 2008). Biometric technology provides greater security and convenience in investigating and authenticating as compared to traditional methods (Wayman, 2008)

This study has investigated the use of digital evidence in form of biometrics during the investigation and apprehension process of criminals/ terrorists in Pakistan. Basing on the results of the data collected certain guidelines have been proposed. These guidelines can help different investigation and apprehension departments, in effectively and successfully executing their methods, drills and procedures. This study is also important and unique in its existing because we as a nation are suffering from the unwanted and undesired menace of terrorism. We as nation should execute a coordinated effort at government level to counter this ill. This study will help and guide the government, state departments, intelligence agencies, police, LEAs and Armed forces of Pakistan to analyze their existing methods and procedures for putting coordinated and effective effort to counter terrorism.

1.6 The Major Research Questions of the Study

1.6.1 Aims and Objectives

This research is aimed at providing the guidelines to counter terrorism on basis of digitized evidence in form of biometrics. This research work will facilitate the LEA's, different investigating and intelligence agencies and police departments.

To fulfill the desired aim there are certain objectives, which are required to be achieved.

1. Identification of using biometric technology as digitized evidence
2. Identifying and analyzing main problems which are hampering and influencing the process of investigating terrorists/criminals
3. Analyzing the personnel's experiences and concerns who are actively involved in the investigating the terrorists/criminals.
4. Analyzing the opinions which are considered important by the persons who are apprehending these terrorists.
5. Identifying and analyzing main legal issues faced by the persons who are apprehending and investigating terrorists/criminals cases by using digital evidence (Biometrics) in Pakistan.

1.6.2 Research Questions

In order to achieve the aims and objectives listed above, Research questions have been formulated. These research questions, if answered, will lead me to achieve the objectives and later achieving the aim.

1.6.3 Research Question 1

Q.1 How biometric technology can be used as digital evidence?

Solution Methodology: The research question Q1 will be answered from the literature part. The biometric technology is study in detailed in context to its use as digitized evidence for distinguishing different individuals. The identification of different individuals is on basis of their behavioral and physiological traits. Different techniques have been studied for use of biometric data of and individual like Fingerprints, DNA, IRIS identification, Foot print pattern, gait traits, facial recognition, voice recognition etc. The issues, peculiarities and understanding of biometrics as digitized evidence are also studied and highlighted.

1.6.4 Research Question 2

Q.1 Can digital Evidence (biometrics) be used in apprehension and investigation of terrorists to counter terrorism in Pakistan?

Solution Methodology: The research question Q2 is linked with the research question Q1. It will be answered from the literature and questionnaire. The questionnaire part is to get the opinion of people who are performing the duties of apprehension and investigation currently in Pakistan.

1.6.5 Research Question 3

Q.1 What are the main problems and legal issues faced by the persons who are apprehending and investigating terrorists/criminals cases by using digital evidence (Biometrics) in Pakistan?

Solution Methodology: This research question will be addressed in three candid linked steps. Firstly identification of personel who are eligible and can investigate and apprehend terrorists/criminals both from literature and observation. Second step is to understand the problems which these individuals are facing actually in the field and determine, either biometrics as digitized evidence can help them or not. Questionnaire is used to have the understanding of people's opinion in this regard. The third step is to know in person what all are the problems and legal issues with the use biometrics as digitized evidence by interviewing individuals who are actively performing the duties of investigating and apprehending the individuals. The research question 1 and 2 provides the base for the research question 3. Identifying the use of Biometric technology as digital evidence, problems and legal issues faced. This will get a deeper understanding of problems and legal issues faced which will further help to propose guidelines to counter terrorism on basis of digital evidence (biometrics) in Pakistan.

1.6.6 Relationship between Research Questions and Objectives

The relationship between the research question and objectives in mentioned in the Figure – 1. The figure explains how the objectives are connected with the research question and how each objective contributes to achieve the aim.

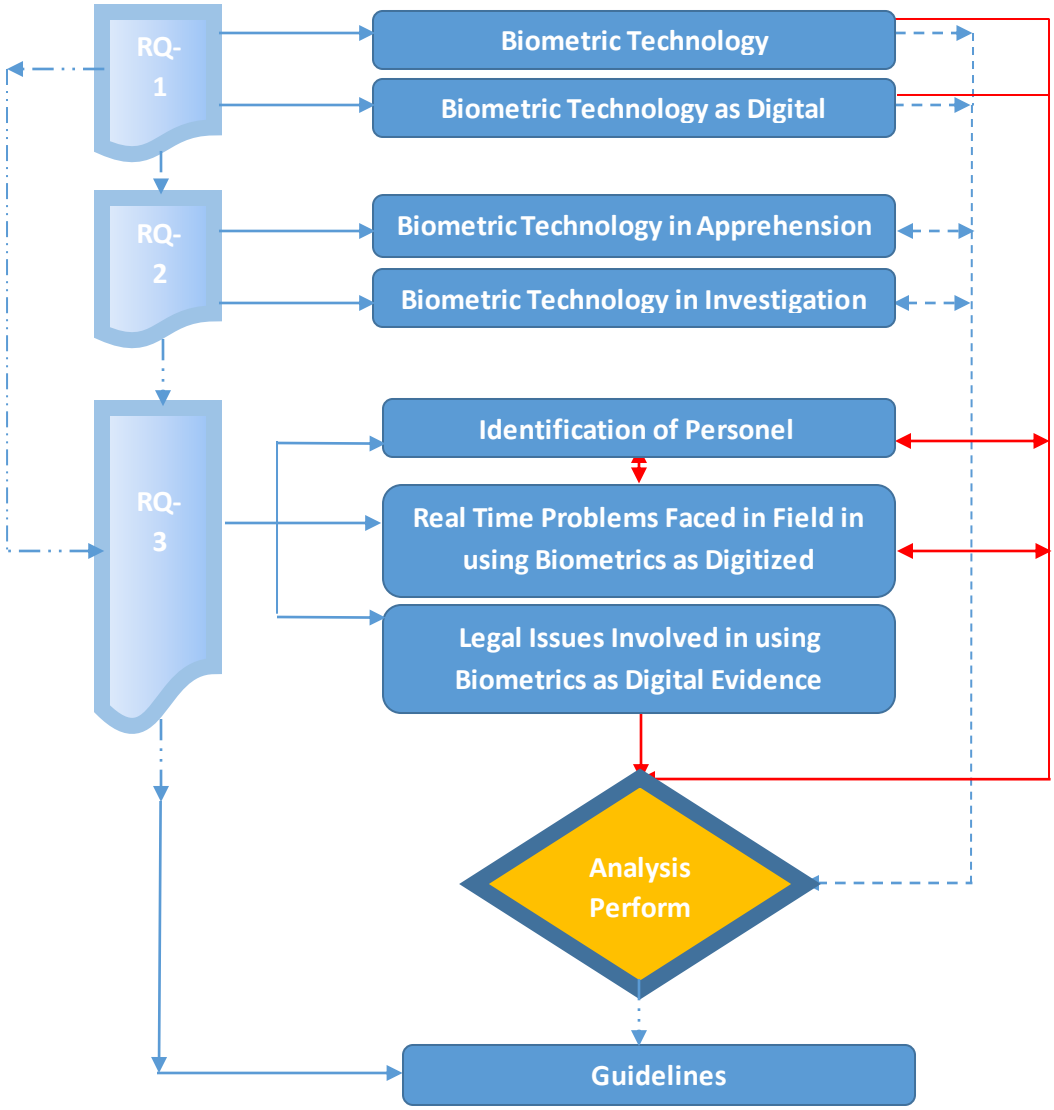

Figure 1 - Relationship between research questions

1.6.7 Research Expected Outcome

Studying the research problems and answering the research questions will enable me to formulate guidelines for effective use of biometrics technology as digital evidence to counter terrorism in Pakistan. Research work will provide following possible outcomes.

1. Brief and articulate information about biometric technology with an emphasis on its strength and weaknesses.

2. Factors which are affecting the use of biometric technology as digitized evidence by the people who are apprehending and investigating terrorists/criminals.
3. The research will provide sufficient basis for use of biometric technology in investigation and apprehension procedures of terrorists/criminals
4. This research will highlight the legal issues which are hampering the process of investigation and apprehension.
5. This research will highlight as to why the terrorists which are being apprehended and investigated, are set free during trial at Pakistani courts.
6. This research will help in proposing guidelines for you of biometric technology as digitized evidence to countering terrorism.

1.6.8 Research Motivation

I am currently working as explosive forensic analyst and Pakistan Army. I have been extensively involved in apprehension and collection of evidence from the crime scenes. I have analysed numerous incidents and proposed different counter strategies to counter the terrorist tactics, since 2008 till today.

Currently state of Pakistan is facing extreme ideological threats. Sectarian clashes, Terrorism and Political rift amongst different political parties is giving rise to this threat. Terrorist are group of individuals who consider their self-fabricated ideology more authoritative than the sovereignty and ideology of Pakistan. They want power to implement their ruthless Laws. They are trying to take over the country by killing civilians, policemen, army men through sabotage, subversion and crippling the political and economic standing of the country globally

Since the last decade Pakistan has been involved in war against terrorism. Pakistan's effort in fighting and eliminating the menace of terrorism has been commendable both at national and international forums. Pakistani security force are carrying out raids and fighting up in the front line with these miscreants. In response to Pakistani security forces the terrorist's organizations are bombing different places in Pakistan. These terrorists are targeting civilians, LEAs personnel's, security forces and destroying and sabotaging the infrastructure and the writ of Pakistani government respectively in the country. In context to these events intelligence and state departments are carrying gout extensive apprehensions of suspects and criminals

In response, Law enforcement Agencies (LEA), intelligence and state departments are carrying gout extensive apprehensions of suspects and criminals in Pakistan. . In the process there are many individuals who have been set free because of lack of evidence during the investigation process and further in the trials being conducted at Anti-terrorist Courts (ATC). Use of

Biometric technology as digitised evidence can help and lead to higher success. Currently the existing investigating procedures of the criminals and terrorists are not very effective as on Dec 1, 2013 Tehrik-i-Taliban Pakistan claimed responsibility of killing four policemen on Nov 27, 2013 at Hyderabad. Yet Police was unable to prove them guilty (Dawn, n.d.)The Terrorists cases lasts for many years without final verdict by the judge (Times, n.d.). This is mostly because of poor investigation and lack of evidence against the terrorists to prove them guilty in court of Law. This problem exists because of non-availability of evidence against terrorists and lack of crime data (Ozgul Faith, 2007)

Biometric Technology is very helpful in this regard. Biometric Evidence can help in providing sufficient pieces of evidence. These pieces of Evidence are sufficient to prove suspected individual guilty in court of Law. DNA technique of biometric collection has led to new twist in unsolved Terror Case of Ex-Red Army Faction (RAF) member Verena Becker in murder of West Germany's Chief Federal Prosecutor Siegfried Buback on April 7, 1977. (International, n.d.)

Based upon above discussion it would be of great importance that digital evidence based on biometrics must be collected, stored and processed. This digitized evidence must be used throughout the entire procedure of apprehension, investigation and trials of these terrorists and criminals. This study could be of immense importance because the study results will provide a deeper understanding into the use of biometrics as digitized evidence, which will help different LEAs, police and intelligence departments during the investigation and apprehension of the terrorists/criminals. This study will be a positive step contributing towards successful investigation and apprehension of the terrorists/criminals in Pakistan.

1.6.9 Demarcation and Focus

The main focus and concern of this thesis is to conduct a study which will highlight the causes and elaborate the factors which are hampering and preventing the successful investigation and trial of terrorists in court of law. What all are the reasons as to why the terrorist keep getting out of pakistani prisons once they are involved in killing of innocent Pakistanis. They are being investigated and apprehended by our security forces, LEA's, intelligence departments and policemen yet why they find refuge and safe umbrella in our judicial system.

1.6.10 Audience

This master thesis will be of great interest and immense importance for the Law Enforcement Agencies, police, Security forces, all Intelligence agencies who are working under the umbrella

of government. All these departments can get assistance for possible deployment of biometric technology in investigation and apprehension process. It can help these government tentacles in successfully investigating and apprehending the criminals. It can also act as base for future research work focusing on use of biometric technology in countering terrorism.

1.7 Research Methodology

There are different research methodologies in the literature which can be used as a guideline to conduct the study i.e Quantitative (Hazzan, et al., 2006; Seaman, 1999), Qualitative and Mixed methodologies (Creswell, 2002). It is always important to understand and know the important factors which are involved in these methodologies, when it is required to select a specific and suitable research methodology. Selecting the suitable method for research always leads to a quality research both in context to results and research contribution. Therefore it is very necessary to be absolutely clear about the pro and cons of the research method to be chosen in context to the research work being carried out.

Procedure for doing the research must be divided into approaches i.e Qualitative, Quantitative and mixed methods, which must have the elements of enquiry, knowledge claims, strategies and methods. The choice of selecting the research technique is then transformed into various processes which are involved in the main research design process (Creswell, 2002). While adopting a specific research approach, it is important to understand mainly three factors i.e Research problem, personel experience of the researcher and most importantly the audience which will be befitted from research work. Understanding of all these factors helps in focusing the research which leads to successful and candid conclusions in the research work. (Creswell, 2002).

The research approach helps in identifying different scenarios which are employed by the researchers and investigators to focus their research question. Qualitative approach is used when certain phenomenon or concepts are little known or it needs to be discovered (Creswell, 2002). Qualitative research is suitable when researcher is working with new topic or when the topic is studied for the first time with the population or group in hand (Creswell, 2002). Likewise when there is a need to test or explain a theory quantitative approach is used (Creswell, 2002). Quantitative technique is suitable when there is a need to express the scientific knowledge in quantities, measuring units and scales, mathematical relations, tables and graphs (Rijgersberg, et al., 2009)

1.8 Quantitative Part

The approach which is used to carryout research work is both qualitative and quantitative as shown in Figure - 2. In Quantitative approach, a questionnaire was formulated to carry out the data. It is said that questionnaire is a well-known technique to collect demographic data and user's opinion (Preece, et al., 2002). Questionnaire was made by listing the factor for variables i.e. Digital Evidence (Biometrics) and Investigation of terrorists from the literature. Questionnaire was divided in three parts.

1. In Part-I the information regarding respondent is asked which includes name, age, gender and experience in their own particular field.
2. In Part-II the questions regarding digital evidence (biometrics) have been asked to know the general understanding of the terminologies. Also to get the opinion of the respondents and factors about the use of biometric technology as digitized evidence.
3. In Part-III the questions regarding terrorist investigation have been asked. Use of biometric technology as digitized evidence, factors and legal issues involved in the use of biometric technology as digitized evidence during investigation of terrorists have been asked. These questions have been designed in a way to know the respondents opinion and their understanding of the issue.

Questionnaire underwent face validity and for content validity factors have been listed. Pilot study was conducted to further evaluate the content validity. After this, reliability analysis has been conducted to check the unrelated sub factors who are not contributing sufficiently to variables. Exploratory factor analysis have also been conducted to check the under lying construct validity of instrument. This was very important as to see whether it is collecting the data it is required to. Results of factor analysis were effective thereby making instrument valid. Data was collected on questionnaire in order to find out the opinion of using digital evidence (Biometrics) from people who are involved in investigating and apprehended terrorists/criminals on routine basis in different investigating agencies, intelligence departments, law enforcement agencies, police and army. Likert scale has been used for questionnaire. The scaling technique is used to get the opinion of the people about the use of digital evidence in form of biometrics during the investigation of terrorists/criminals etc. Pilot study was conducted to check the validity of the questionnaire on twenty sample (n=20). After that mean of variables have been computed. Co-relation of variable's mean was also checked which came out to be positive. Reliability analysis of the variables is also carried out. Results of the Cronbach's alpha were found to be in permissible limits. Exploratory factor analysis has

also been carried out to further check the validity of questionnaire through SPSS. The values of determinant and KMO were also in permissible limits.

1.9 Qualitative Part

In qualitative approach, interviews have been conducted for data collection (Hove & Anda, 2005). According to Creswell (2002) interviews and observations are considered to be most effective and important data collection method used in ethnographic studies. After performing literature review unstructured interviews have been conducted for data collection. A total of thirty (n=30) individuals were interviewed. Individuals who were interviewed are performing the duties of investigating and apprehended terrorists/criminals on routine basis in different investigating agencies, intelligence departments, law enforcement agencies, police and army. Interviews were conducted in order to have interviewee's opinion about the use of digital evidence in form of biometrics during the investigation of terrorists/criminals etc. In order to avoid involving any inaccurate data collected from interviews which could lead to invalid results (Creswell 1998). Audio recording and noting down of interviews have been preferred to avoid any inaccurate collection of data.

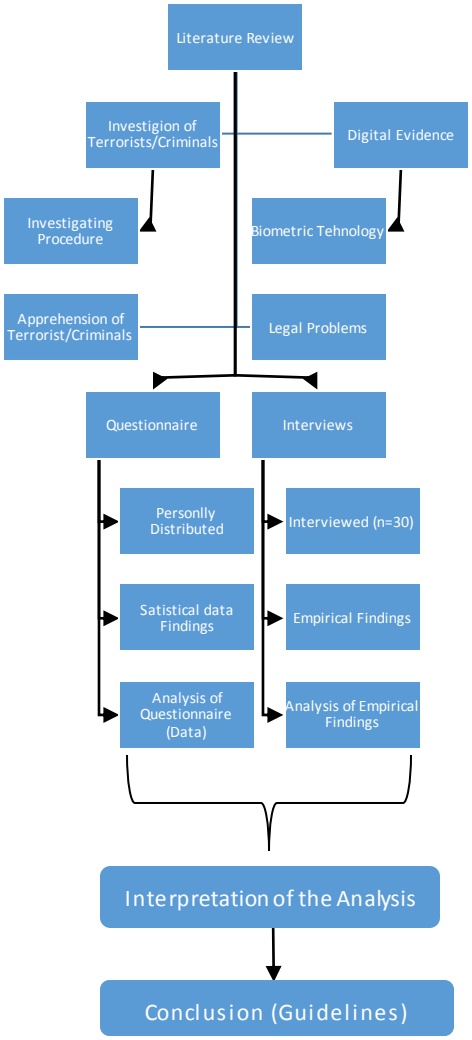

Figure 2 - Research Methodology

1.9.1 Research Process

Figure - 3 shown below elaborates the research process of the study.

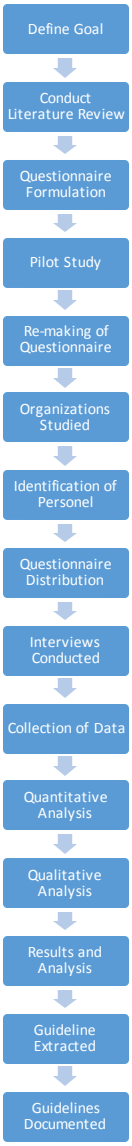

Figure 3 - Research Process of study

1.9.2 Sources of Primary Data

The primary sources for data are as follows.

1.9.2.1 Questionnaire

Questionnaire has been made on the likert scale. Ranging from 1 to 5 with 1 being strongly agree, 2 Agree, 3 neutral, 4 disagree and 5 being strongly disagree.

1.9.2.2 Interview

Total of thirty (30) interviews have been conducted which includes six (6) unstructured and twenty four (24) structured interviews from the concerned people who are involved in the phenomenon.

1.9.3 Data Collection Method(s)

There are generally two major approaches for collection of information about a particular situation, person, problem or phenomenon. There are certain times when data is already available and there is a need to only extract it. Meanwhile there are times when it is required to collect data as well. Based upon these broad approaches to information gathering, data is categorized as, primary data and secondary data. Figure – 4 shows different data collection methods.

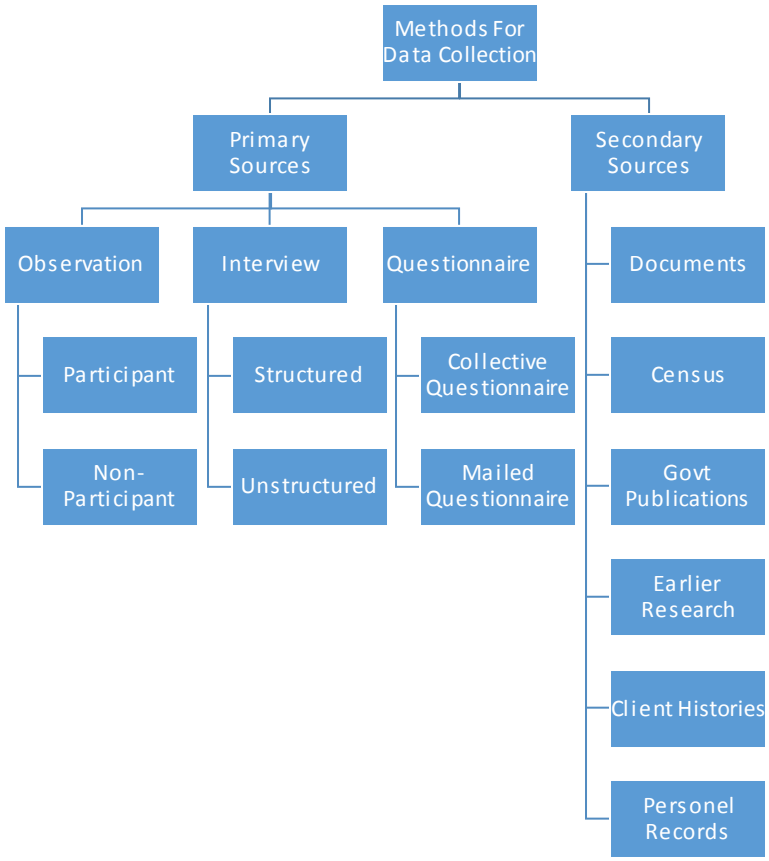

Figure 4 - Data Collection Methods

The methods which have been highlighted above will not give a 100 percent accurate and reliable information. There are many factors which define the data collection. However the data collection methods which have been used for this research work are

1. Questionnaire
2. Interviews

1.9.4 Data Analysis Method(s)

For my data analysis both qualitative and quantitative, data has been recorded in tool NVIVO for my qualitative data analysis. In NVIVO free nodes have been made of all the emerging themes which are present in the interviews. Open coding technique has been used to make free nodes. Once these nodes have been made they are further categorized by axial coding

technique. In which relationships have been given to the various nodes. After that, selective coding has been done to identify and further answer research questions and research objectives respectively. After that models are generated to show and highlight main factors and legal issues currently being faced by the personel who are actively involved in apprehension and investigation of criminals.

In quantitative part data is recorded in tool SPSS for quantitative data analysis. Data gathered is first hand data from people who are practically performing the duties in the field. Questionnaire has been validated by firstly doing content analysis. Pilot study has been conducted for questionnaire. After doing that construct validity has been carried out of the questionnaire in SPSS and the results were within permissible limits. Correlation of variables has also been checked which came out to be positive. Further hypothesis is also tested in SPSS. Reliability test, exploratory factor analysis of questionnaire, ANOVA tests have also been carried out. Lastly responses of respondents is shown in form of graphs to identify and analyze the main factors in the use of biometrics as digitized evidence. .

1.9.5 Classification

There are many different types of research which can be classified according to

1. The purpose of the research – the reason why they are being conducted
2. The process of the research–the way data is collected and analyzed
3. The logic of the research– whether you are moving from general to specific
4. The outcome of the research– whether you are trying to solve a particular problem or making a general contribution to knowledge

This research study is classified as descriptive and analytical.

1.9.5.1 Descriptive Research

Descriptive research ids the one which describes the phenomenon as it exist in actuality. It is used to identify and obtain information on the characteristics of a pertinent problem or issue. The descriptive study may answer the question starting with what. In this study research question 3 which is as, what are the main problems and legal issues faced by the persons who are apprehending and investigating terrorists/criminals cases by using digital evidence (Biometrics) in Pakistan? So in order to identify the problem areas and main legal issues, this study can be classified as Descriptive Research.

1.9.5.2 Analytical Research

Analytical research is a continuation of descriptive research. The researcher goes beyond merely describing the characteristics, to analyzing and explaining why or how it is happening.

This analytical study may answer the question staring with how. In this study research question 1, 2 and 4 which are as, how biometric technology can be used as digital evidence? , How use of Digital Evidence (Biometrics) in apprehension and investigation of terrorists can counter terrorism in Pakistan?, How legal issues and problems faced by the persons who are apprehending and investigating terrorists/criminals cases can be solved by use of digital evidence (Biometrics) in Pakistan?

1.9.6 Limitations of the Study

With regards to this thesis work, there are certain guidelines which have been proposed. Basing on the data collected, analysis and interpretation carried out on problem area and legal issues faced by the personel who are performing the duties of investigation and apprehension of terrorists/criminals in different intelligence, Police, LEAs and state security departments. These guidelines are believed to be quite helpful for effective use of biometric technology as digitized evidence in countering terrorism in Pakistan.

1. Identification of main factors and legal issues which are being faced in the use of biometrics as digitized evidence in counter terrorism in Pakistan. However, it will also be very necessary to study the technical aspects involved in the use of biometrics as digitized evidence.
2. This study was limited to only Rawalpindi, Islamabad and Karachi. It would be of great importance that this study must be conducted in other parts of the country in order to understand the more factors and legal issues being faced in different parts of the country.
3. Questionnaire was distributed to only hundred persons, this number should be increased to five hundred (500) to thousand (1000) to further refine the research.

1.10 Hypothesis

In this research, null hypothesis is, *Use of digital Evidence (Biometrics) in investigation of terrorists, cannot reduce terrorism in Pakistan*. The ANOVA test performed to check the null hypothesis, results were significant, clearly showing that null hypothesis is rejected.

Alternate hypothesis is *Use of digital Evidence (Biometrics) in investigation of terrorists, can reduce terrorism in Pakistan*. As per ANOVA test alternate hypothesis stands corrected.

1.11 Theoretical Framework

Theoretical frame work constitutes of an independent variable as *Digital Evidence (Biometrics)* and a dependent variable *Terrorist Investigation*. Graphically it can be shown as

2 CHAPTER TWO: LITERATURE REVIEW

2.1 Preface

The literature review plays a very important role in carrying out the research process. It is not merely one simple step to be performed in the research process but in reality it is an iterative feedback process which keeps on looping throughout the research process. It helps in defining, redefining and refinement of undefined research problem. Literature review helps in solving and identifying the research problem which is intended to be solved. Literature review is on existing work which is carried out in subject area. This work has helped me a lot to understand the concepts and procedures involved in the investigation of terrorists/criminals worldwide. Currently research work in investigating terrorists is very limited.

Detailed literature review has been studied to perform and understand the concepts and procedural methodologies for employing biometric technology. The application of biometric technology in different sectors like commercial industry, national security departments, use in government installations, e-banking, registration of population, crime scene investigation etc.. In context to this study focus is on use of biometrics as digital evidence in investigation processes of terrorists/criminals currently used in Pakistan. To counter terrorism on basis of digital evidence especially biometrics during the investigation of the terrorists/criminals is explored.

It is important to define the search strategy i.e how search from literature review has been conducted. Different search engines have been used to carry out search effectively. Electronic databases i.e. IEEE (Institute of Electrical and Electronic Engineers), Science Direct, Springer Link, Digital Library, IJDE (International Journal of Digital Evidence) and Elsevier were used in searching relevant data. In addition to mentioned databases, manual searching was performed using Google, Bing and Google Scholar.

2.2 Venn diagram

When the set theory was born out of the need to put the mathematicians, scientists and physicists on a firm and logical foundation. Language of set theory allowed these individuals to make precise definition, replacement of unsatisfactory and fuzzy language with more exact and precise language of sets. In order to understand and illustrate the concepts of set theory, different types of logical diagrams emerged. Most famous of all is the well-known Venn diagram. Venn diagram was invented by john Venn. He was a graduate of Cambridge. He was a priest and resigned priesthood and became lecturer at Cambridge. He taught Moral Sciences.

Venn diagram is also used to illustrate the relationship between different sets, groups of different objects that have and are sharing something in common. Usually Venn diagrams are used to depict the intersection of sets. Venn diagram is used in scientific and engineering presentations, in theoretical mathematics, in computer application, and in statistics. Venn diagrams can also be used in the market research, in science, etc. It can also be used to collect and store the overlapping information as well.

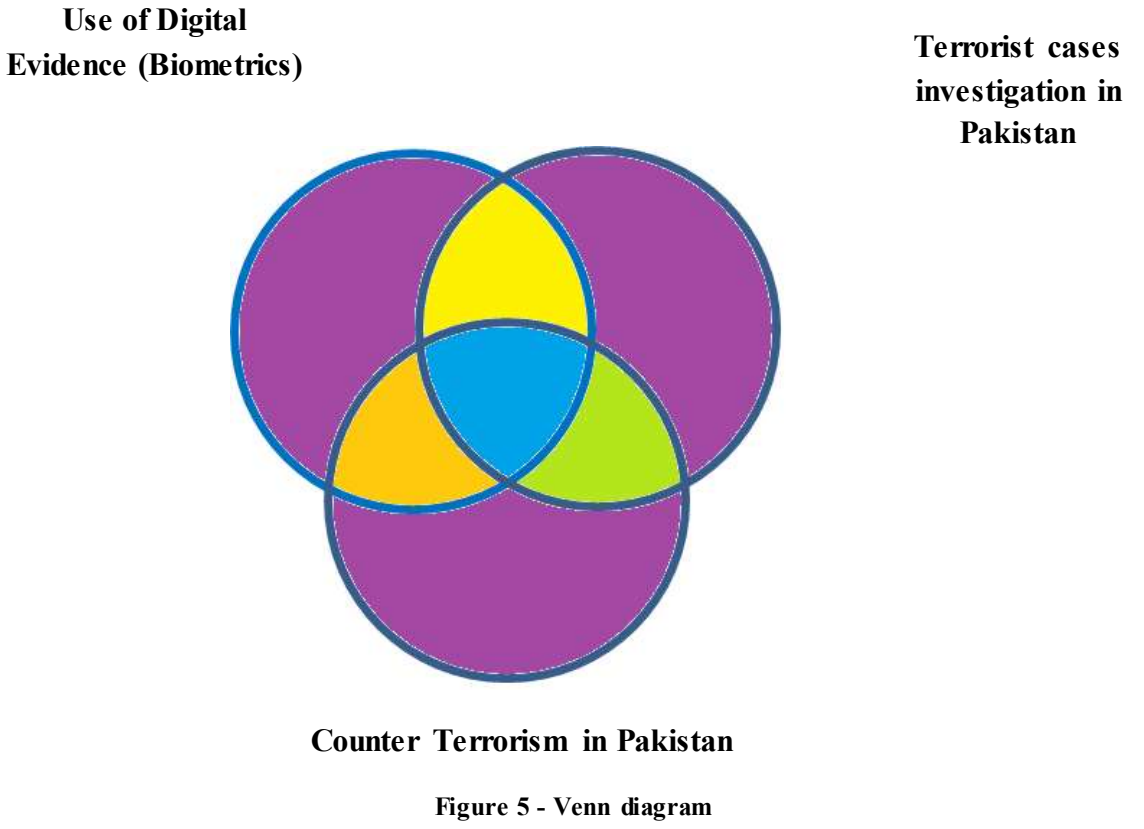

Figure 5 - Venn diagram

- *Digital Evidence in countering Terrorism in Pakistan*
- *Terrorist cases investigation to counter terrorism*
- *Digital evidence in terrorist cases investigation*
- *Digital Evidence in terrorist investigation cases to counter terrorism*

2.3 Introduction

Literature review has been conducted keeping in mind subject area which is biometric technology. There are many fields in which biometric application are being used like E-banking, E-commerce, biometrics in courts and justice system, biometrics in security application, biometrics in health care, biometrics in registering and monitoring application, use of biometric application in identification and scanning application of individuals, biometrics in

national security departments and agencies and many more but focus has been on its(biometrics) role as digitized evidence in countering terrorism in Pakistan. Sub area of subject area is role of biometric is counter terrorism. Then research questions have been formulated. Basing on research questions research objectives have been formulated. Different publications have been studied in this regard and Venn diagram has been formulated which is shown above.

2.4 Related Work

Literature review is divided in three different parts to study in detail about the biometric technology, its uses and usage as digitized evidence and its role in successful investigation. Also these parts constitutes Venn diagram as shown in Figure – 5.

2.4.1 Criminal Investigation

Criminal investigation is one of the ancient science that may have roots as far back as in the writings of the Code of Hammurabi. In the code it is suggested that both the accuser and accused had the right to present evidence they collected (Ann Wolbert Burgess, 2009). In the modern era criminal investigations are most often done by government police forces. Private investigators are also commonly hired to complete or assist in criminal investigations.

Criminal Investigation is an applied science that involves the study of facts, used to identify, locate and prove the guilt of a criminal. A complete criminal investigation can include searching, interviewing and interrogating individuals. It also includes Evidence collection its preservation and various methods of investigation. (O'Hara, 1994) Modern day criminal investigations commonly employ many modern scientific techniques known collectively as forensic science.

The word forensic comes from the Latin forēnsis, meaning "of or before the forum" ("Forensics". TheFreeDictionary.com., n.d.). In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story. The individual with the best argument and delivery would determine the outcome of the case. This origin is the source of the two modern usages of the word forensic – as a form of legal evidence and as a category of public presentation. In modern use, the term "forensics" in the place of "forensic science" can be considered correct as the term "forensic" is effectively a synonym for "legal" or "related to courts". However, the term is now so closely associated with the scientific field that many dictionaries include the meaning that equates the word "forensics" with "forensic science".

Forensic science (often mistakenly shortened to forensics which refers to public speaking) is the scientific method of gathering and examining information about the past. This is especially important in law enforcement where forensics is done in relation to criminal or civil law,[5] but forensics are also carried out in other fields, such as astronomy, archaeology, biology and geology to investigate ancient times. In Medical field it is also used to investigate criminal cases involving murders. Time of murder and how murder is done can be known by the help of Biology Forensics. Other fields of forensics are Forensic accounting, Forensic animation, Forensic anthropology, Forensic chemistry, Forensic economics, Forensic engineering, Forensic entomology, Forensic facial reconstruction, Forensic identification, Forensic linguistics, Forensic materials engineering, Forensic photography, Forensic polymer engineering, Forensic profiling, Forensic psychiatry, Forensic psychology, Forensic seismology, Forensic video analysis and Forensic Biometrics.

2.4.2 Why Biometrics

Privacy and security have remained one the prime concerns of human society. The history shows that different measures were adopted by humans to ensure those. Walls were built, huge forts were made and people were assigned task to strengthen security and privacy. As the human social infrastructure kept changing with time, also there appeared some changes in the security methods. If we quote from modern day world, we find passwords, user names and token used for ensuring security and privacy. All the above mentioned tools used for ensuring security and privacy are authentication techniques. The authentication process is based on what you have (like cards and tokens) and what you know (passwords and pins). Passwords and ID cards are known as conventional means of authentication (O'Gorman, 2003). With passage of time certain limitations i.e. passwords could be forgotten, shared or hacked and cards could be stolen and lost, were experienced in the conventional means of authentication (Jain, et al., 2006). So the need for a more robust authentication system was thought, something covering the limitations of the previous conventional methods of authentication. It was thought that the new mechanism should base on the methodology of what you are i.e. some part of the human body or some behavioral characteristics of the human body (O'Gorman, 2003).

2.4.3 Biometrics Technology as Remedy

Biometrics technology is said to be an authentication technique that measures the physical or behavioral characteristics of an individual and then compares it with the stored template in the database in order to identify that individual (Woodward, 1997). According to Woodward (1997) biometrics solutions involve scanning of unique human characteristics i.e. physical and behavioral, which are measured and then integrated into a computer system for the process of

recognition. According to Jain et al. (2006) biometrics based authentication system is more reliable and powerful than traditional authentication system as it cannot be lost, difficult to forge, difficult to copy and needs person to be present at time of authentication. Stanley et al. (2009) rates biometrics as the most secure and convenient tool for authentication process of individuals. According to Stanley et al. (2009) biometric authentication is gaining acceptance and popularity in large numbers of applications i.e. from governmental programs (ID card system, Visa system) to personal applications for logical and physical access control.

2.4.3.1 Working of Biometrics

The biometrics recognition process, according to (Vielhauer, 2005; Bhargav-Spantzel, et al., 2006) consist of two operational steps i.e. Enrollment and Authentication (see Fig.4). Enrollment involves the extraction and storage of unique feature of individual i.e. fingerprint, hand, iris etc. While the authentication mode comprise of authentication process (comparison of extracted features, at authentication point, with the saved template in data base) in order to authenticate the individual. According to figure no 4 the enrollment process is performed by data acquisition module after that feature extractor module process involves extracting biometric data feature then enrolling the individual's biometric template in database. The enrolled biometric data is then used to compare with the biometric sample at the time of recognition. The authentication process is performed when the user gets authenticated by the biometric system. Here the user gives his biometrics sample, already enrolled in the database, in order to get authenticated. The biometric sample submitted, is compared with the enrolled biometric template and authentication is performed as shown in Figure – 6.

Biometrics refers to the identification of human beings by their physical characteristics or traits. Several different techniques are used in Biometrics which are Facial Recognition (based on measuring change in Facial Expression), IRIS (it is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil) , Study of finger and thumb Impressions, Identifying Deoxyribonucleic acid (DNA) patterns (it refers to a molecule that encodes the genes used in the development and functioning of all known living organisms), study of blood and hair samples of individuals.

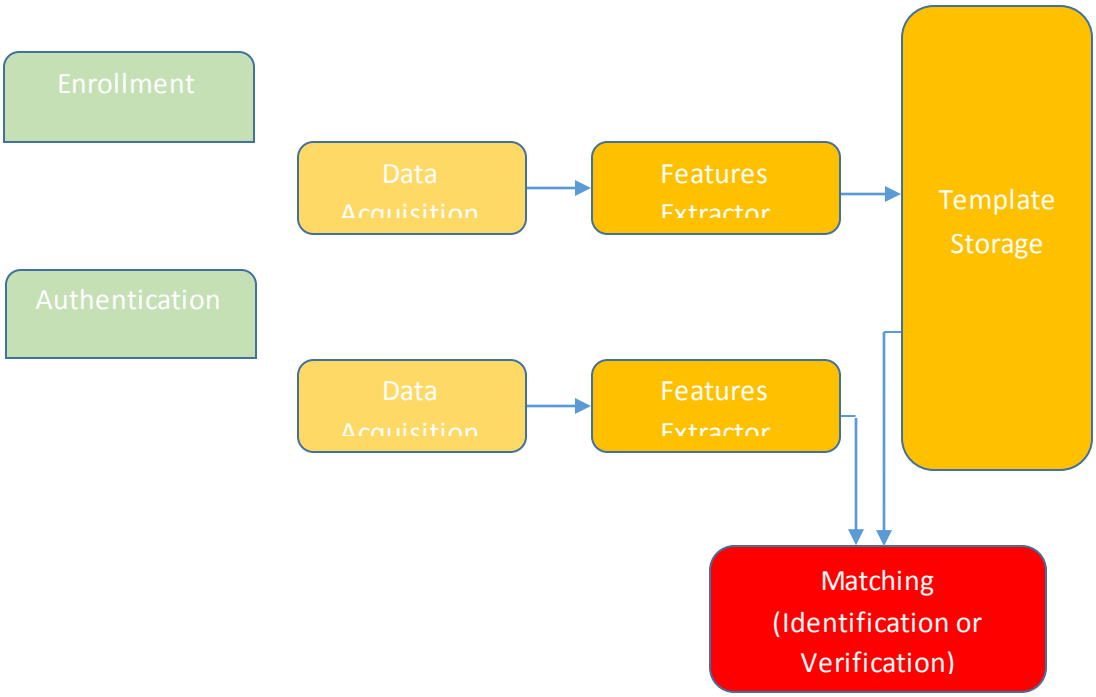

Figure 6 - Enrollment and Authentication of Biometric System, Adopted from (Bhargav-Spantzel, et al., 2006, p.65)

An elaborate, more comprehensive detail and step wise explanation of biometric technology recognition process is given by Liu and Silverman (2001) shown in Figure - 7. It is explained as follows.

1. First step is choosing the biometric characteristics i.e. finger print or face scan to be used in biometrics recognition system.
2. After this step biometric characteristics are processed by the biometric device and these characteristics are extracted and enrolled in the data base as biometric template.
3. After the storage of biometric template, the process of scanning the template of suspect with the stored template in biometric system for recognition purposes.
4. After the scanning process, the biometric characteristic are processed and a template of suspect is extracted, which will then be used to compare the already enrolled template in the biometric system.
5. After the matching and scanning process is complete the results are displayed i.e suspect gets authenticated or rejected.
6. Then the matching results are available to be used in any application, depending on why the matching was performed.

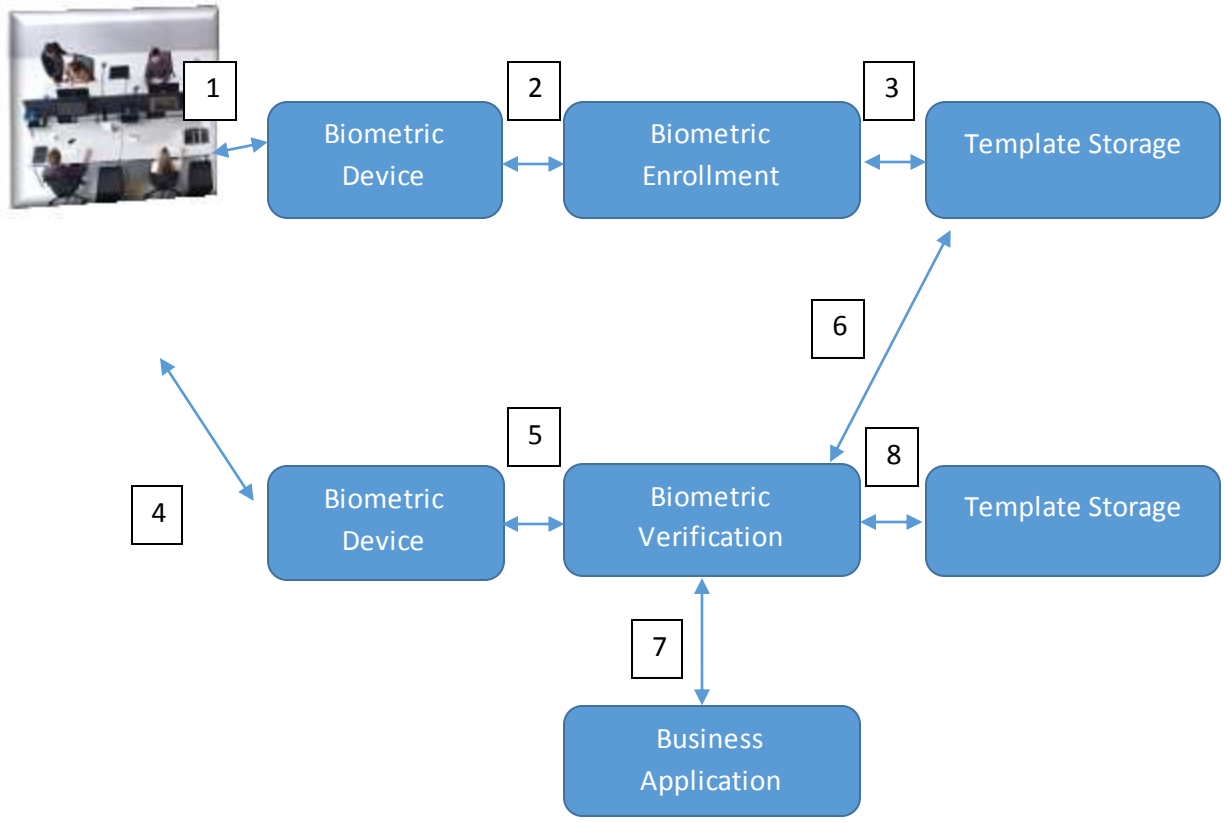

Figure 7 - Biometric Process Model. Adopted from (Liu and Silverman, 2001, p.28)

2.4.4 Verification and Identification

According to Jain, Ross, et al., (2004) there are two modes, a biometric system can operate in i.e. verification mode and identification mode. In verification mode the biometric system verifies that the person is the one who he claims to be by comparing the captured biometric data with the template that is stored in data base. In verification process (see Fig. 8) the user claims his identity "I am xxx" and the biometric system performs 1:1 comparison in order to find out that the person is the one who he claims to be (Jain, Ross, et al., 2004; Davrondzhon, et al., 2006; Bala, 2008). Identity verification is mostly used to perform positive recognition with the purpose of preventing multiple people to use same identity (Wayman, 2001).The identification mode as shown in Figure – 9 operates with the aim to identify an individual among large number of people. In identification process an individual gives his or her biometric sample to the system and the system compares it with the large list of templates that are stored in database. Here 1: N numbers of comparisons are involved (Gregory & Simon, 2008). Identification plays a very important role in negative recognition applications where the system ensures that the person is one who he or she denies to be (Jain, Ross et al. 2004).

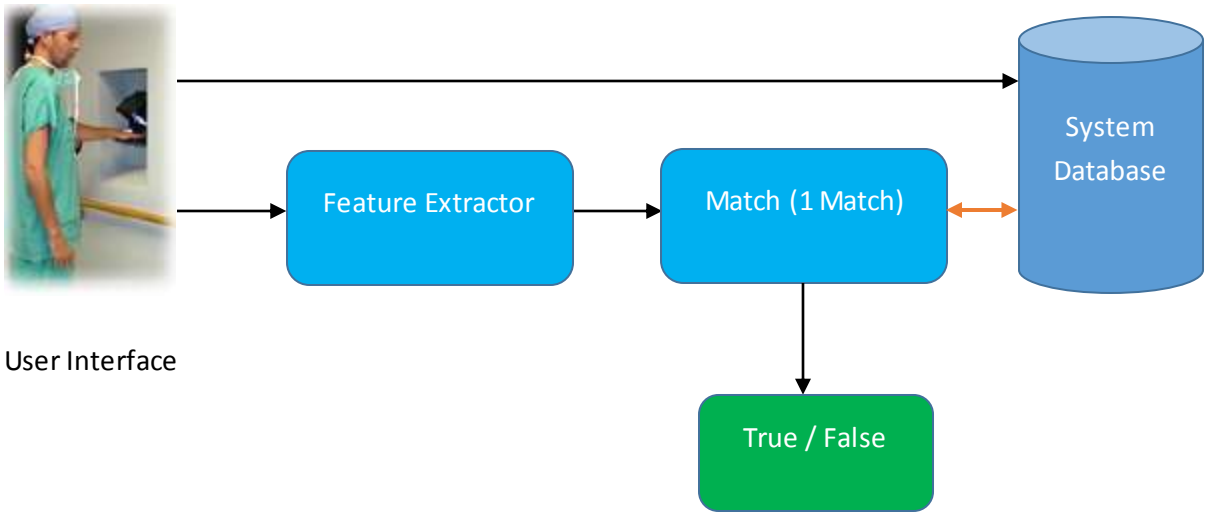

Figure 8 - Verification mode of Biometric System, Adopted from (Jain, Ross et al. 2004, p.5)

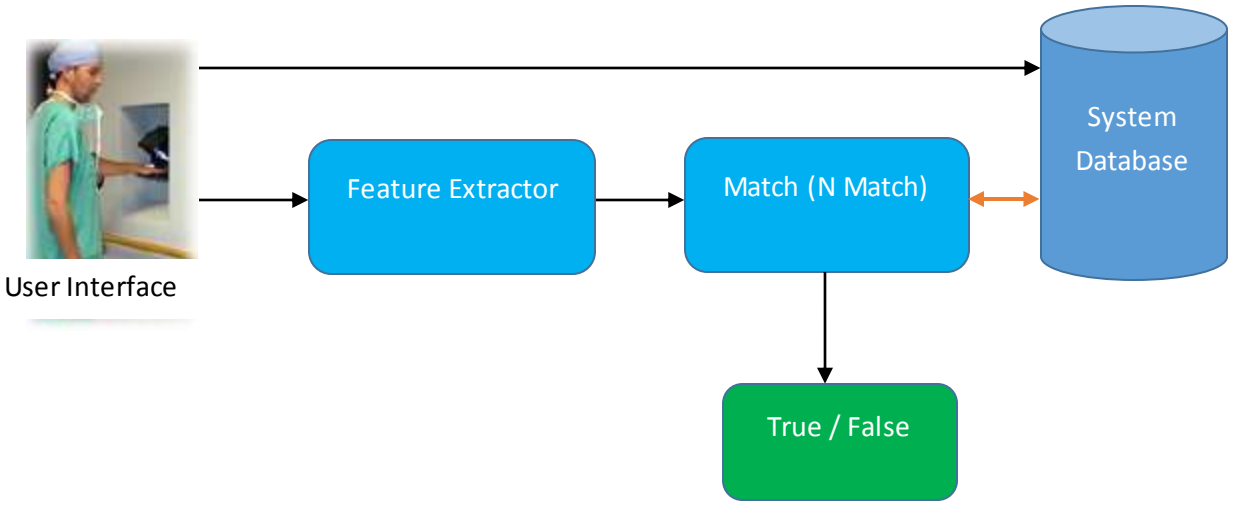

Figure 9 - Identification mode of Biometric System, Adopted from (Jain, Ross et al. 2004, p.5)

2.4.5 Characteristics of Biometric System

The recognition process, facilitated by the biometric system, is based on the physical and behavioral characteristics of individuals (Stanley, et al., 2009). One can question "what human characteristics i.e. physical and behavioral, can be used as biometric trait?" According to (Gregory, 2008; Jain, Ross, et al., 2004) any human physiological and behavioral characteristics can be used as biometrics characteristics if it satisfies the following requirements i.e. universality, uniqueness (distinctiveness), permanence and collectability (Gregory, 2008; Jain, Ross, et al., 2004). These are explained below

1. **Universality:** It means that the characteristic that is chosen as biometric trait is universal in selected domain e.g. if finger print biometrics is to be selected in some office domain then it is very important that all the employs has at least one finger to use the biometrics system.
2. **Uniqueness:** The chosen biometric characteristics, is unique i.e. no two individuals have exactly the same characteristics.
3. **Permanence:** It means that the characteristics are permanent in nature or they change very slowly with time. The face changes over time but DNA remains permanent for whole life. So for a characteristic to be used in biometric system it is important to have permanency.
4. **Collectability*:*** This means that how easy it is to measure the characteristics quantitatively i.e. in numbers for the computer. We can say it refers to the collection of that biometric characteristic.

According to Jain, Ross, et al., (2004) there are some other issues that need to be considered when there is a need to characterize the biometric systems. The issues are performance, acceptability and circumvention (Jain, Ross, et al., 2004). These are explained below.

1. **Performance:** Performance of the biometric system means that how much time, equipment and calculations are done in order to achieve the accuracy and speed of the biometric recognition.
2. **Acceptability:** This characteristic of the biometric system shows that either the biometric systems will be acceptable to the users or not. The acceptability of the biometrics technology, mostly, depends upon the individuals perceptions of biometrics technology.
3. **Circumvention:** Circumvention means that how easy it is to forge the system i.e. how easy it is to fool the biometric system.

2.4.6 Evaluation of Biometric System

Evaluation of biometrics technology is an important aspect of biometrics technology. Different types of evaluation methods exists however some of the evaluations methods are listed below.

There are three types of biometric technology evaluations i.e. technology, scenario and operational evaluations. Technology evaluation prime goal is the comparison of competing algorithms from a single technology. Determination of the overall system performance in simulated application is the goal of the scenario evaluation while the operational evaluation is

a tool to conclude the performance of the biometric system in specific environment and with specific group of population (Phillips, et al., 2000; Mansfield & Wayman, 2002).

Two measures i.e. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used for the evaluation of biometric systems as shown in Figure - 10. Incorrectly accepting the biometric trait is called false acceptance and the rate this false acceptance can or may occur for any biometric system is called False Acceptance Rate (FAR) while the incorrect rejection of the biometrics trait is called false rejection and the percentage this false rejection may occur for any biometrics system is called False Rejection Rate (FRR) (Liu, et al., 2001; Moskovitch, et al., 2009).

According to Liu and Silverman (2001) both the measures i.e. FAR and FRR are used to allow limited entry to authorized users however these measures vary scenario to scenario. In some case you need tight security and for that the false acceptance is minimized but at the same time the false rejection rate increases also. The two measures are interrelated to each other and that's why it will be a good idea to go for a balanced approach. The FAR and FRR are plotted against each other in the below diagram. The points on the plot show the hypothetical performance of the system at different sensitivity settings. Crossover Error Rate (CER), a comparison metrics that is used to find the reliability and accuracy of biometric systems, can be determined by comparing the FAR and FRR on the plot. The point having lowest value of CER (Crossover Error Rate) is the point where the system can work more accurately (Liu and Silverman, 2001)

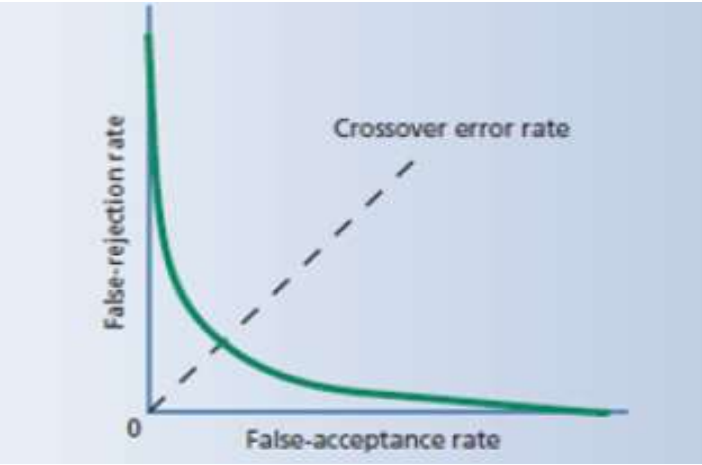

Figure 10 - Cross over Error Rate Attempts to Combine with Two Measures of Biometric Accuracy, Liu & Silverman, 2001, p.32

2.4.7 Benefits of Biometric Technology

As biometrics technology is now widely preferred for use around the world. It can be seen from building access control to the passports and from schools to hospitals. While there has been recorded some concerns about the privacy issues related to biometric technology but still it is

in use in many parts of the world. Gregory & Simon (2008) listed some of the benefits that are associated with the biometrics technology. The benefits associated with the biometrics technology are listed below

1. **Cooperation Not Required:** Most of the time the biometric recognition is performed without any cooperation required from the user e.g. placing a camera on the entrance can do facial and gate (recognition of individual from his/her walking style) authentication without any effort required from the user. It requires fewer efforts from the user as compared to passwords and cards.
2. **Guarantees Physical Location:** It means that at the authentication time, the subject is present at the place. As anyone can use my card or password but only i can use my finger or face for authentication. This is the benefit of the biometric technology that it makes sure that the subject is present at authentication point.
3. **High-Throughput:** Biometrics technology gives high throughput when there is some danger of fraud or some false identification. It is considered suitable than password in such situations.
4. **Unforgettable:** People have many passwords to remember which indeed a tricky thing is. On the other hand biometrics is difficult to forget as it involves any physical or behavioral characteristic of humans for authentication purpose.
5. **Unlosable:** There are problems with the authentication schemes like they get stolen or lost e.g. cards and keys etc. The biometric has strength that it can be lost or stolen. It would sound strange to say " I found human finger in the train or I lost my finger in the hotel room"
6. **Unsharable:** The common problem with password is they get shared for some reasons. The biometrics, on the other hand, cannot be shared with anyone. This benefit of the biometrics improves and enhances the authentication process and auditing.
7. **Cost Reduction:** Biometrics systems believed to increase the cost but if the system is implemented properly then it can achieve cost reduction i.e. it confirms people's entrance to organization which means that no fake card punching for other employees can work. This ensures the quality work which certainly pays back i.e. minimizing the cost. Secondly the expenses done on the help desk, dealing with the passwords and cards problems, can be reduced to maximum level which again is a step towards cost reduction.
8. **Compliance:** Access control is used to make sure the data protection and it is made sure by one or two factor authentication. The problems related with other authentication

schemes make, biometrics technology, a fit choice as the access control can be enhanced by authenticating the user from his physical and behavioral characteristics.

9. **Emergency Identification:** In some scenarios persons need to be identified very carefully and very quickly. Let's take example of a man lying unconsciously on the road having no identity cards with him. As he needs quick medication but the problem is how to recognize him. Biometrics works here as it can identify the person from his fingerprint or any other biometric characteristics which is enrolled in the biometric system.
10. **No Identity Theft:** Identity theft is big problem to solve. Biometrics technology is a nice option to reduce identity theft as if there is some one bad enough to use my credit card to buy something; he will be facing a problem when there is biometrics authentication required to use the credit card.

2.4.8 Various uses of Biometric Technology

Biometrics technology can be seen in many different organizations and departments all around the world. The organizations, where there is need to authenticate the users, looking forward to biometrics technology for authentication. Gregory & Simon (2008) describe the following industries where the biometrics could have an effective role in performing and facilitating the authentication process.

1. **Health Care:** Biometrics technology can be used in health care in order to secure the physical assets and the logical assets i.e. data security in the health care systems.
2. **Food and Drugs Administration:** The food and drugs industry has a certain potential for the biometrics systems as the administration in these industries can be made effective through the use of biometric technology.
3. **Law Enforcement:** The law enforcement agencies can use biometrics systems to apprehend terrorist/criminals by identifying them from their physical and behavioral characteristics.
4. **Banking and Finance:** The banking and finance section also needs certain level of identification for the transactions. To have a robust identification and to minimize the fraud, there is a greater possibility for the biometrics systems to help banking and finance section in authenticating the individuals.
5. **And all other Companies and Organizations that has use of credit cards:** Apart from the above mentioned areas, there are many other areas where there are credit cards involved. All such companies having credit cards involvement can have the biometric system for identification when it comes to the usage of credit cards.

Nanavati, et al., (2002) have also explained the usage of biometrics systems in different industries and markets. The following industries and markets have a potential use for biometrics technology (Nanavati, et al., 2002).

1. **Criminal Detection:** Biometrics technology can be used to identify the criminals and suspects. After 9/11 the suspects and bad people identification was a challenge. Biometrics technology is used to meet this challenge.
2. **E commerce / Telephony:** E-commerce has great potential for the biometrics technology. As the remote transactions, done by the users, need to be verified and biometrics can play an important role in this sort of remote verification.
3. **Retail Market:** Retail market also has a potential for biometrics technology. While buying commodities needs verification for many reasons. The card verification is to be replaced by the biometrics technology.
4. **Computer / Network Access:** When accessing computers and networks, mostly passwords were used before. But now thanks to biometrics technology, as we have laptops with fingerprint scanners. It will be a nice move to get identified when it comes to accessing the networks and the computers.
5. **Time Attendance / Physical Access:** Time and attendance mechanism can be revolutionized with biometrics technology. It would be a good practice to identify people with biometrics technology for checking attendance. Also there are greater chances that the physical access to resources and different portions of the organization is given after biometric identification.
6. **Citizen's Identification:** Citizens can be identified very effectively while using the biometrics technology. There are certain governmental programs where citizen's identification is required e.g. voting and social benefit schemes.
7. **Intelligence acquiring and Surveillance:** The surveillance can be made easy with the usage of biometrics technology. The governmental organizations responsible for keeping things ok in the area needs surveillance and it would be a good idea to use biometrics technology i.e. face recognition and gate.

2.4.9 Biometrics in Law Enforcement

Nowadays biometric technology is extensively used by the Law enforcement people for its inquisitive race with criminals. The systematic search of digital devices for pertinent evidence is on the peak (Mark Reith, 2002).

Law enforcement Agencies (LEA) in Pakistan are trying to apprehend the terrorists. Currently the existing investigating procedures of the criminals and terrorists are not very effective as on

Dec 1, 2013 Tehrik-i-Taliban Pakistan claimed responsibility of killing four policemen on Nov 27, 2013 at Hyderabad. Yet Police was unable to prove them guilty [6] The Terrorists cases lasts for many years without final verdict by the judge [7]. This is mostly because of poor investigation and lack of evidence against the terrorists to prove them guilty in court of Law. This problem exists because of non-availability of evidence against terrorists and lack of crime data [8]

Biometric Technology is very helpful in this regard. Biometric Evidence can help in providing sufficient pieces of evidence. These pieces of Evidence are sufficient to prove suspected individual guilty in court of Law. DNA technique of biometric collection has led to new twist in unsolved Terror Case of Ex-Red Army Faction (RAF) member Verena Becker in murder of West Germany's Chief Federal Prosecutor Siegfried Buback on April 7, 1977. [9]

2.4.10 Biometric Technology in Criminal Investigation

Criminal investigation is one of the ancient science that may have roots as far back as in the writings of the Code of Hammurabi. In the code it is suggested that both the accuser and accused had the right to present evidence they collected.[2] In the modern era criminal investigations are most often done by government police forces. Private investigators are also commonly hired to complete or assist in criminal investigations.

Criminal Investigation is an applied science that involves the study of facts, used to identify, locate and prove the guilt of a criminal. A complete criminal investigation can include searching, interviewing and interrogating individuals. It also includes Evidence collection its preservation and various methods of investigation.[3] Modern day criminal investigations commonly employ many modern scientific techniques known collectively as forensic science.

The word forensic comes from the Latin forēnsis, meaning "of or before the forum."[4] In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story. The individual with the best argument and delivery would determine the outcome of the case. This origin is the source of the two modern usages of the word forensic – as a form of legal evidence and as a category of public presentation. In modern use, the term "forensics" in the place of "forensic science" can be considered correct as the term "forensic" is effectively a synonym for "legal" or "related to courts". However, the term is now so closely associated with the scientific field that many dictionaries include the meaning that equates the word "forensics" with "forensic science".

Forensic science (often mistakenly shortened to forensics which refers to public speaking) is the scientific method of gathering and examining information about the past. This is especially important in law enforcement where forensics is done in relation to criminal or civil law,[5] but forensics are also carried out in other fields, such as astronomy, archaeology, biology and geology to investigate ancient times. In Medical field it is also used to investigate criminal cases involving murders. Time of murder and how murder is done can be known by the help of Biology Forensics. Other fields of forensics are Forensic accounting, Forensic animation, Forensic anthropology, Forensic chemistry, Forensic economics, Forensic engineering, Forensic entomology, Forensic facial reconstruction, Forensic identification, Forensic linguistics, Forensic materials engineering, Forensic photography, Forensic polymer engineering, Forensic profiling, Forensic psychiatry, Forensic psychology, Forensic seismology, Forensic video analysis and Forensic Biometrics.

2.5 Biometric Techniques

There are many biometrics techniques available nowadays in the market. Some of them are quite mature, already in use in industry, i.e. (fingerprint, hand geometry, iris, retina, facial recognition, voice, signature dynamics and typing rhythm) while others are still in the pipeline (odor biometrics) (Stanley et al., 2009).

There are strengths and weaknesses associated with each technique and selection of a specific technique depends on the application. It is very rare for a single biometric technique to fulfill the requirements of all applications (Deriche, 2008). The techniques cannot be categorized as best or bad biometrics techniques, all what matters in labeling these techniques depends on what we want to achieve, with whom we want to achieve and what conditions do we have to achieve our goal (Julian, 2002).

The question arises here, what is most appropriate technique that can be used for robust authentication? It is very important to decide on what is the basis for selecting biometric techniques among many techniques on hand. According to Nanavati, et al., (2002) to be able to select the best biometric technique among many, it is very important that some of the important questions are answered regarding these techniques. These questions help in evaluating the biometric technology for choosing the best alternative. The questions such as, which technology is more able to reject the false attempts? Which technology is most opposing to spoofing? Which technology is least expensive in deployment? Which technology ensures maximum privacy? (Nanavati, et al., 2002).

As this study is to suggest guidelines for using biometrics as digitized evidence to counter terrorism in pakistan that's why the different biometrics techniques are discussed below with their strengths and weaknesses so that it would help in formulating guide lines.

2.5.1 Finger Print Biometrics

Fingerprint biometrics is the most popular and most used biometric technique used for biometric identification (Gregory & Simon, 2008). The recent usage of fingerprints can be traced back to 1960s when the law enforcement agencies used it to identify individuals (Stanley, et al., 2009). Figure – 11 explains that Fingerprint is the pattern of valleys and ridges on fingertip surface which are formed during the first seven months of fetal development. In identification process, the fingerprints have the greater matching accuracy (Jain, et al., 2006). The fingerprint biometrics involves pattern comparison of ridges and furrows, as well as the minutiae points (characteristics of ridges that happen when at some point the ridge ends or it divides in to two). The points i.e. ridges, furrows and minutiae points are the points that comparison is based on in fingerprint identification process (Deriche, 2008).

Figure 11 - Fingerprint Impression, Adopted from (Draper, et al. 2007, p.4)

Strengths of fingerprint biometrics:

1. Fingerprint scanner has low cost (Gregory, 2008; Jain, Ross et al. 2006; Moore, 2005).
2. Fingerprint provides good convenience in usage (Gregory, 2008; Nanavati, et al. 2002, Biometrics: Newsportal.com, 2009).
3. Fingerprint is not intrusive (Biometrics: Newsportal.com, 2009).

Weaknesses of fingerprint biometrics:

1. Can be easily spoofed (Biometrics: Newsportal.com, 2009).
2. In identification mode, it requires large amount of computational resources (Jain, et al., 2006).

2.5.2 Face Recognition

Face recognition is the most common biometric system among humans used for personal recognition (Jain, et al., 2006). Humans have different faces from each other. The unique dimensions, proportions and physical attributes of a person face form bases for face recognition biometrics (Biometrics: Newsportal.com, 2009). Face recognition is based on the analysis of facial characteristics (Deriche, 2008). The user image is obtained by a camera which is further used for the authentication process as shown in Figure - 12. The acquired facial image is stored as template and when the authentication is required then the newly facial image of the user is compared with the template (Deriche, 2008).

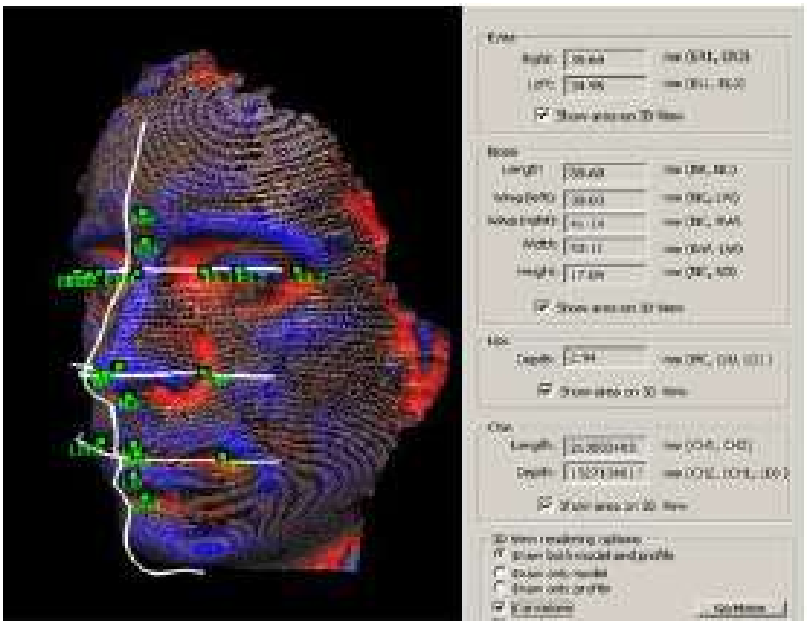

Figure 12 - Face Recognition Biometrics, Adopted -Figure image of face, 2009

Strengths of face recognition biometrics:

1. Similar to human process of authentication (Gregory & Simon, 2008).
2. The convenience to use facial biometrics is excellent (Gregory & Simon, 2008; Nanavati, et al., 2002).
3. Facial biometrics is mature technology (Gregory & Simon, 2008).
4. Face recognition can use the existing image capturing devices i.e. cameras (Nanavati, et al., 2002).

Weaknesses of face recognition biometrics:

1. Most people are uncomfortable with taking pictures taken with the fair that it will cause privacy abuse (Nanavati, et al. 2002; Biometrics: Newsportal.com, 2009).
2. Accuracy can be reduced with changes in characteristics of the face i.e. hair style and make up (Nanavati, et al. 2002; Biometrics: Newsportal.com, 2009).
3. More suited for authentication than identification because it's easy to change the proportions of one's face by wearing mask (Biometrics: Newsportal.com, 2009).
4. The accuracy can also be reduced by the light and angels (Nanavati, et al. 2002).

2.5.3 Retina Biometrics

There are blood vessels at the back of eye which are unique from eye to eye and person to person (Biometrics: Newsportal.com, 2009). Dr Carleton Simon and Dr Isodore Goldstein, in 1935, discovered that the patterns of the blood vessels of retina are unique and can be used for the identification of individuals (Gregory & Simon, 2008). Retina based biometrics system works on the principal of analyzing the layer of blood vessels which are present on the back of eye as shown in Figure - 13. A light source of low intensity through optical coupler is used for the scanning purpose of patterns of retina. (Deriche, 2008). Retina biometrics is used in places where high security is needed (Deriche, 2008; Nanavati, et al. 2002).

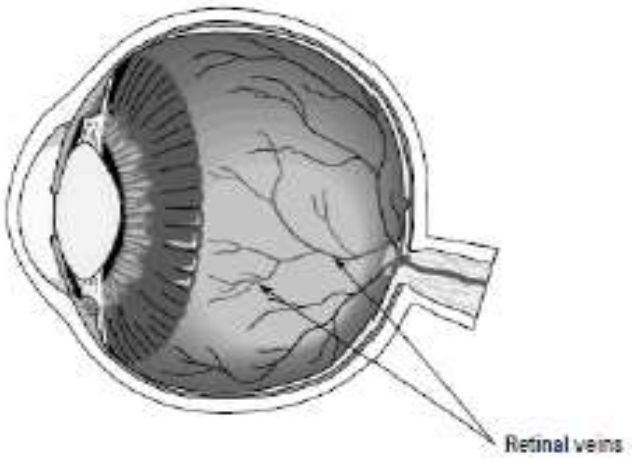

Figure 13 - Retina Scan Biometrics, Gregory & Simon, 2008, p.91

Strengths of the Retina scan biometrics:

1. Its highly accurate technology (Gregory & Simon, 2008; Deriche, 2008; Nanavati, et al. 2002; Biometrics: Newsportal.com, 2009).
2. Provides most security in authentication (Gregory & Simon, 2008; Deriche, 2008).
3. It is difficult to spoof (Nanavati, et al. 2002).

Weaknesses of Retinal scan biometrics:

1. Enrolment and scanning are slow and intrusive to individuals (Gregory & Simon, 2008; Biometrics: Newsportal.com, 209).
2. Limited use of the retina biometrics because of demanding efforts from user (Nanavati, et al. 2002).
3. Expensive technology i.e. high cost (Gregory & Simon, 2008).

2.5.4 IRIS Biometrics

The iris is an annular region that is surrounded by the pupil and the sclera from all sides (Jain, et al., 2006). The iris is elastic, pigmented and connective tissue controlling the pupil as shown in the Figure - 14. It is developed at the early stages of morphogenesis and after development iris remains stable for the whole life. The iris of each and every human is different from one another i.e. unique (Biometrics: Newsportal.com, 2009). The iris patterns are unique and even the iris patterns of the twins or the right and left eye are not same (Deriche, 2008). Frank Bunch was the one who proposed the idea that iris is so unique that it can be used for identification process (Gregory & Simon, 2008). The iris biometrics involves analysis of almost 200 point of iris i.e. rings, furrows, freckles and the corona and then compares it with the previously recorded template, stored in database (Biometrics: Newsportal.com, 2009).

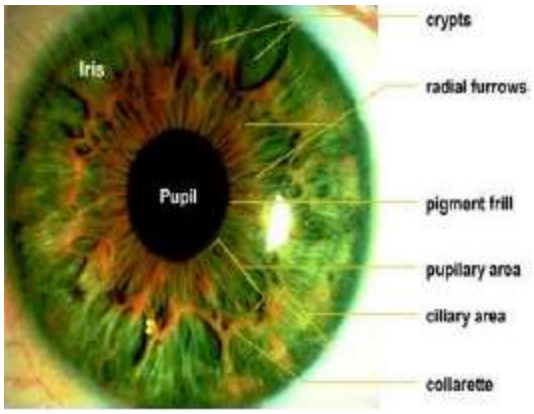

Figure 14 - IRIS Biometrics, Dawson, 2002

Strengths of Iris biometrics:

1. Most accurate technology (Gregory & Simon, 2008; Deriche, 2008; Nanavati, et al., 2002).
2. Iris biometrics is not intrusive and is hygienic (no physical contact) (Deriche, 2008; Biometrics: Newsportal.com, 2009).
3. Iris biometrics has low false acceptance rate (Jain, A.K. et al., 2006).
4. Iris biometrics has promising processing speed (Jain, A.K. et al., 2006).
5. The patterns of iris remain stable for all the life (Nanavati, et al., 2002; Iridian technologies, 2009).

Weaknesses of Iris Biometrics:

1. Less convenience in usage (Nanavati, et al., 2002; Biometrics: Newsportal.com, 209).
2. Less competition in market because of few vendors (Gregory & Simon, 2008).

2.5.5 Hand Geometry Biometrics

Hand geometry biometrics involves a number of measurements of the human hand i.e. shape of the hand, palm size, and lengths and widths of the fingers (Sanchez-Reillo, et al., 2000). It is one of the established technologies that are used mostly for the physical access controls (Nanavati, et al., 2002). The operation of hand geometry biometrics involves the template development of the hand geometric characteristics as shown in the Figure - 15. The template is stored which is then used for comparison with subsequent hand readings of an individual (Deriche, 2008). The hand geometry biometrics measure up to 90 parameters of human hand for identification process (Biometrics: Newsportal.com, 2009; Salavati, 2006). Some organizations use the hand geometry biometrics systems to control time and attendance (Deriche, 2008; Liu, et al. 2001).

Figure 15 - Hand Geometry, (Libin, 2005)

Strengths of Hand geometry biometrics:

1. It's easy to use (Gregory & Simon, 2008; Deriche, 2008; Liu, et al., 2001).
2. Hand geometry biometrics is Non-intrusive (Biometrics: Newsportal.com, 2009).
3. Hand geometry biometrics can operate in challenging and rough environments (Nanavati, et al., 2002).
4. It is an established and reliable technology (Nanavati, et al., 2002).
5. Hand geometry biometrics has low failure to enroll (FTE) rate (Biometrics: Newsportal.com, 2009).

Weaknesses of Hand geometry biometrics:

1. It's not a mature technology (Gregory & Simon, 2008).

2. Lack of satisfactory accuracy results (Nanavati, et al. 2002; (Biometrics: Newsportal.com, 2009).
3. Relatively high rate of FAR (false acceptance rate) and FRR (false rejection rate) rate (Bolle, et al., 2003).
4. Jewelry on hands may propose challenges in scanning the hand geometry (Jain, et al., 2000).

2.5.6 Voice Biometrics

Voice is said to be a combination of behavioral and physical biometrics. Shape and size of the appendages (vocal tracks, mouth, nasal cavities and lips), used in sound generation, form the basis for individual voice features (Campbell, 1997). Almost every individual has unique voice features from other individual. The Texas Instruments were the first, who worked on voice identification technology (Deriche, 2008) in 1970s by developing a prototype that was tested by the U.S. Air force and MITRE Corporation (Gregory & Simon, 2008). An image of the instrument interface is shown in Figure – 16. It operates on the same principal of enrolling and storing a voice template which is used for identification when an individual uses the voice biometrics for identification purpose.

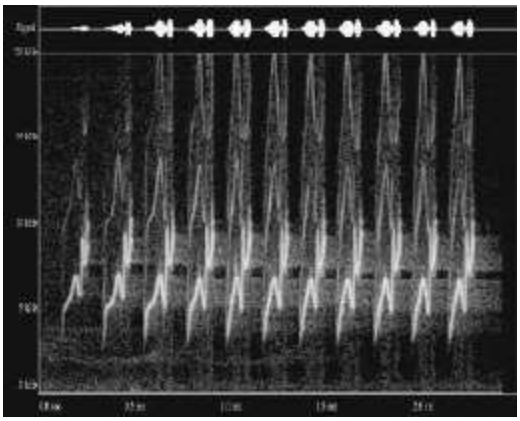

Figure 16 - Voice Biometrics, Gregory & Simon, 2008, p.102

Strengths of Hand geometry biometrics:

1. There is no need for some extra new devices for voice biometrics (Deriche, 2008; Biometrics: Newsportal.com, 2009; Liu & Silverman, 2001).
2. Voice biometrics is low cost biometrics (Gregory & Simon, 2008).
3. Its usage is convenient (Gregory & Simon, 2008).
4. With low invasiveness (Biometrics: Newsportal.com, 2009).

Weaknesses of Hand geometry biometrics:

1. The accuracy can be affected with serious illness or some problems in throat (Deriche, 2008).
2. High rate of false non match (Biometrics: Newsportal.com, 2009).
3. Because of poor devices generating echoes (Nanavati, et al. 2002).
4. Voice biometrics can be easily spoofed (Gregory & Simon, 2008).

2.5.7 Signature Biometrics

The way in which an individual signs his or her name is the unique characteristics of that individual (Nalwa, 1997). Signature biometrics deals with the signature patterns of an individual for identification purpose (Nanavati, et al. 2002). Signature biometrics involves the analysis of the way in which user signs his or her name and other signing features i.e. speed, velocity and pressure experienced while signing. Figure – 17 show signature analyzer which is used to analysis of signatures. The least three (speed, velocity and pressure) are of the same importance as the finished static signature in signature biometric identification (Deriche, 2008).

Figure 17 - Signature Biometrics, Digital Signature, 2009

Strengths of Hand geometry biometrics:

1. Signature biometrics has wide acceptance in public (Deriche, 2008; Liu & Silverman, 2001).
2. Signature biometrics has reasonable accuracy ration in operations (Deriche, 2008) resulting low false acceptance rate (Biometrics: Newsportal.com, 2009).
3. The signature biometrics is noninvasive in nature (Nanavati, et al. 2002; Biometrics: Newsportal.com, 2009).

Weaknesses of Hand geometry biometrics:

1. Professionals can forge signatures to fool the system (Jain, A.K. et al., 2006).

2. Same individual can have inconsistent signature (Nanavati, et al. 2002; Biometrics: Newsportal.com, 2009).
3. Signature of individual changes with passage of time (Deriche, 2008).
4. Signature biometrics has very limited market (Nanavati, et al. 2002).

2.5.8 Key Stroke Biometrics

A keystroke is behavioral biometric technique, the keystroke biometric offers sufficient discriminatory information when each individual type on a keyboard in a characteristic way (Jain, Ross et al. 2004). Mike was the first who took notice of the typing and argued that different people type differently from each other and that typing are somehow unique characteristics of individuals (Gregory & Simon, 2008). The typing dynamics may not be interesting to many of us for identification but the studies have revealed that the two factors i.e. inter-character timing and the dwell (a time for which the key stays pressed in typing) can give us 99% accurate identification of the person who is typing (Gregory & Simon, 2008) as shown in Figure - 18.

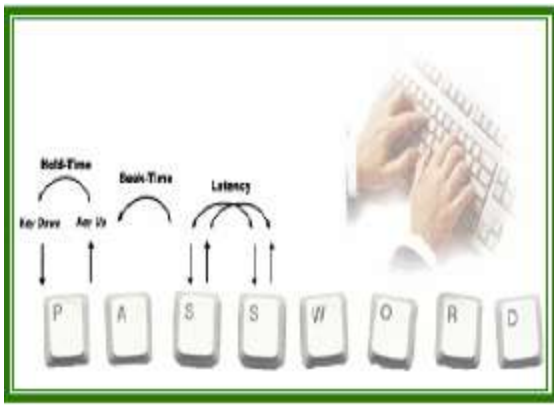

Figure 18 - Key Stroke Biometrics (Figure image of key stroke, 2009)

Strengths of Keystroke biometrics:

1. Low cost (Gregory & Simon, 2008).
2. Do not need any new sensors and can be used with existing hardware (Gregory & Simon, 2008, Nanavati, et al. 2002).

Weaknesses of Keystroke biometrics:

1. It's not a mature technology (Nanavati, et al. 2002).
2. It has less convenience in use (Nanavati, et al. 2002).

2.5.9 Gait Biometrics

Gait is defined as the coordinated and cyclic combinations of movements that are caused by human locomotion (Boyd & little, 2005). Humans have certain styles when they walk and that characteristics of humans can be used to identify humans. Gait biometrics is not a very unique characteristic of human but it can be used to identify individuals in relatively low security applications (Jain, Ross et al. 2004) as shown in Figure - 19. According to Gregory & Simon (2008) gait is a biometric entity that can be classified as physical and behavioral biometrics. The explanation is given that the way human do walk is known to be a behavioral biometric. The gait is physical biometrics in a way that human's physical structure of the feet and body weight can affect the gait (Gregory & Simon, 2008).

Figure 19 - Gait Biometrics, BenAbdelkader, et al. 2004, p.538

Strengths of Gait biometrics:

1. Convenience of the gait biometrics (Gregory & Simon, 2008).
2. Gait is easily acquired from distance (Gregory & Simon, 2008).

Weaknesses of gait biometrics:

1. Not much accurate (Gregory & Simon, 2008).
2. Gait is not invariant as with time gait can be possibly changed (Jain, Ross et al. 2004).
3. Requires more computations and that's why its computations expensive (Jain, Ross et al. 2004).

2.5.10 DNA Biometrics

DNA (Deoxyribonucleic acid) is present in side each living cell of the human body as shown in Figure - 20. It is the basic blue print for the living things. Watson and Crick, in 1953, published the DNA model that was based on the X-ray images of Rosalind Franklin. The DNA in the individuals is totally unique from each other except twins (Gregory & Simon, 2008). The DNA can be used to identify individuals except twins as twins have the same DNA structure. DNA is used mostly in forensic applications to identify individuals (Jain, Ross et al. 2004).

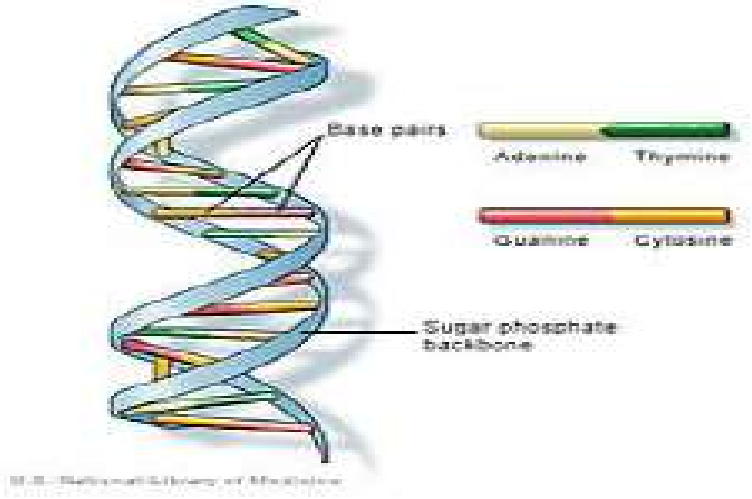

Figure 20 - DNA Biometrics, (DNA-Based Biometrics)

Strengths of DNA Biometrics:

1. It's most accurate biometrics technology (Gregory & Simon, 2008; Biometrics: Newsportal.com, 2009).

Weaknesses of DNA Biometrics:

1. High Cost (Gregory & Simon, 2008).
2. DNA biometrics has poor convenience (Gregory & Simon, 2008).
3. The processing time for DNA Biometrics is very long (Gregory & Simon, 2008).

2.5.11 Which is Best Biometric Technique

As there are many biometrics technologies in the market and it's hard to label them good, bad or best. It's very rare to say grade any biometric technology as perfect as no biometric technology is perfect (Jain, Bolle, et al., 2002). There are pros and cons associated with every technology and the selection of any biometric application defends on the application (Deriche, 2008). The Figure - 21 explains the strengths and weaknesses associated with each biometric technology. High, Medium, and low are Denoted by H, M, and L, respectively.

Biometrics Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H
DNA	H	H	H	L	H	L	L

Figure 21 - Comparison of Biometric Techniques, (Jain, Ross et al. 2004, p.11)

To summarize the discussion about the best biometric technology, it is observed and can be said that the best biometric technology is defined and is dependent on the application of the technology. As this research work is based on the formulation of guidelines for the use of biometric technology as digitized evidence to counter terrorist in pakistan, various strengths and weakness of different biometric technology have been explained in order to have a choice amongst the technology for easy employment in to the system of investigation and apprehension of the terrorists and criminals. Finger printing is most effective, once its applications and uses with regards to investigation and apprehension are concerned.

2.5.12 Use of Digital Evidence (Biometrics)

Identification of conventional procedure involved in the handing, storage and retrieval of the evidence are explored. Conventionally chain of custody of the evidence being maintained refers to chronological order in which the evidence was documented, handled, transferred, analyzed and disposed. Author has classified the evidence as both physical and electronic. Also the sanctity of the evidence must be maintained, it is of utmost importance. Author has explained that currently no procedure for standardization of evidence chains is in vogue. Current practices relies only on traditional paper documentations. The author considers that chain of evidence is a multi-component validation problem. For which he has given a framework, which includes techniques for cryptography, keystroke analysis, digital water marking and hardware source identification. The author has used real time scenarios for testing his framework.

Author has also shown related work in traditional paper based chain of evidence. Tempering of the evidence cannot be ruled out in this regard. He explains that responsibility of onus of the evidence in criminal justice system falls on many shoulders. Firstly on the top of the hierarchy are the prosecutors and down the line at bottom it is the lab technicians, evidence collecting individuals, officers supporting local, state and federal law enforcement agencies. Furthermore

author added that the integrity of the digital chain of evidence is highly sensitive issue. If the defendant alleges about an image that it has been altered then proof of the evidence becomes the responsibility of the state institutions to prove it otherwise. In the end author proposed future works in term of proposed framework. [3]

In this report, the characteristics of Deoxyribonucleic Acid (DNA) are discussed. It has been explained that DNA of each and every individual in the world is different except in the case of twins. DNA can be extracted from a number of sources, such as hair, bones, teeth, saliva and blood. This report explains the approval of building up of the national data base of DNA which has been collected since 1988s. Meanwhile the Federal Bureau of Investigation (FBI) convened a working group of federal, state, and local forensic scientists to establish guidelines for the use of forensic scientists to establish the guidelines for the use of forensic DNA analysis in laboratories. In 1994 congress gave the approval of the national DNA data base. Process in vogue is further legally covered under United States Judicial system as Federal Law (42 U.S.C 14132(a)). This law authorizes the FBI to collect and maintain national DNA database. In addition to it congress has granted various programs to provide assistance to state and local governments for forensic laboratories. Report also brings out the factual data in to lime light about the total funding of $785 being given to this program since FY 2006-12. This report also highlights the problem area of back log of cases and laboratory capacity enhancement.

The combined DNA Index system CODIS is currently in vogue in United States. This system uses Local DNA Index system (LDIS), State DNA Index System (SDIS) and National DNA Index System (NDIS) system to evaluate, process and further generates the probable investigative leads for the criminals. Since 2000 NDIS has aided in the investigation of nearly 175,000 crimes. It has also been mentioned in the report that mostly matches occur between forensic and offender profiles stored in SDIS rather than in NDIS. This report also highlights causes of the backlog of criminal cases. One of the aspect is that the evidence in the possession of Law Enforcement agencies is not incorporated in the statistics. Around 40% of unanalyzed cases contains DNA in different murder and rape cases, of which around 2,000 cases have been with the LEA, which can be helpful if included for investigation.

Processing time of the DNA case has been discussed in detail. Where different percentages have been shown to conclude the processing speed of 145 laboratories available in USA. In this report it is highlighted that priorities have been set to process the case for the DNA collection and building of the database. Further it is discussed that the leads generated for further investigation at times is limited to the personel and resources available with agencies

who have initiated the case for DNA profiling. This report also highlights the congressional issues, legislative issues and quality concerns of the DNA and evidence profiling. [4]

Explanation and definition regarding digital forensic analysis tools followed by a discussion of abstraction layers is discussed. Paper aims at identifying the analysis of Digital Forensics by abstraction layer. Theory of abstraction layer explains the purpose and goals of digital forensic analysis tools. Author explains that the use of abstraction layer is not a new concept but their usage is not very well documented. It also explains that the investigator can make use of different operating systems and forensic software to view a suspect system. This paper explains that with current use of results produced by digital forensic tool are successfully used in prosecutions, but the legality of the results lacks forensic science design. Abstraction layers and their errors have been explained in detail in this paper. Four characteristic of the abstraction layer have been explained in this paper. A Lossy Layer is the one which has greater than zero margins of abstraction error associated with it. With the use of this layer the there is a possibility of increase in investigator using data reduction techniques to manage the increasing number of logs, networks packets and files. A lossless Layer is one that has a zero margin of abstraction error. After that major categories of digital forensics are defined with the help of conception of abstraction layers. Which are physical Media Analyst, Media management Analysis, File system analysis, Application analysis, Network Analysis and memory analysis. [5]

It is important to have a clear understanding of the biometrics and its identifiers. It also explains the methods which are currently used for biometrics. Author says that information used in this work is from multiple internet resources, TV reports, magazines and newspapers and books. Also in this paper methods of data collection, content analysis are applied. This paper explain the history of biometrics, its development process. Also the advantages and disadvantages of using biometrics. Its characteristics, methods and types of biometric identifiers have also been explained in this paper. The author explains that the history of biometrics dates back to ancient times even the Babylonians make use of fingerprints to finalized their business deals. Then author talks about the uniqueness of the biometrics its measurability, permanence, measurability etc. Then biometric identifiers have been explained. First is the physiological and behavioral. Physiological types includes fingerprints, IRIS recognition, DNA, Palm printing, Hand geometry, Odour, facial Recognition etc. Behavioral type includes Gait, Voice recognition, Typing rhythm, Footprints etc. [7]

This study identifies the importance and effectiveness of biometric technology in enhanced and robust authentication security systems all over the world. This also explains the categories and characteristics of biometrics that is both physical and behavioral. It also highlights the causes,

that why this biometric technology with its so useful benefits is not implemented in so many countries. Cost effect, human perception about the biometric technology are the main hurdles in implying biometric technology. This paper also highlights the issue of human privacy and security concerns of human beings, as biometrics is the management of the human identification. Human perception about the concept of deployment of biometric technology must be addressed first in this regard. This study is limited to only Blekinge health care system to analyze the human perception and cost effects involved in the deployment of biometric technology. Author explains that the understanding of the biometric technology needs to be focused first as in case of the Blekinge Health care system. Once this source issues is established then only the true effects and befits from the technology can be seen and enjoyed. Author used different techniques to conduct his research. He used web based surveys, questionnaire, conducted interviews to analyze the perception of the people. In his study he determines that the most of the issues are because of the lack of understanding of the biometric technology. [8]

Corroborative evidences are those who have dual functions in its arguments. Firstly it has the direct supporting of the main conclusion. Secondly it has the bolstering function/effect which would relatively increase the probative value of some other piece of evidence in the argument. Author presents a model which highlights the analysis and guides the evaluation part of the corroborative evidence as it will occur in the discussion. Author explains convergence and the corroborative evidence and their argument authenticity. Author explains about certain models which haven't work which includes corroborative as premise support, corroborative as premise support (Of unstated premise) and corroboration as convergence. [11]

Abstract model of digital forensics have been discussed and defined. The model encompasses the digital forensic process, comparison and a contrast is drawn between four forensic methodologies. This paper also explains the urgencies and perpetual race in which different Law Enforcement Agencies are into. They require digital technology and development of tools which would ease the process of search by digital devices for a particular evidence. This paper also rectifies the shortcomings of the previously used methodologies and also is advantageous with regards to:-

1. It standardizes the process of development of tool for digital forensics
2. A mechanistic approach towards the application of digital forensics in future
3. A generic tactic by the judicial members to link and present technological aspects to non-technical audience
4. Also to incorporate non-digital electronic technologies within the abstraction.

Paper also explains that the there is a need to standardize the procedure for digital forensics as the term is a synonym to computer forensics. It has been used earlier as such. Figure – 22 explains the working models of digital evidence as shown below.

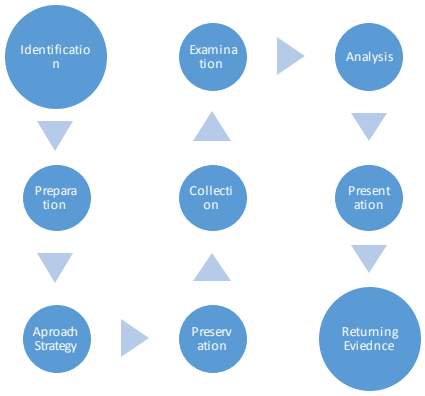

Figure 22 - Working Models of Digital Forensics

After the model has been presented the advantages and disadvantages of the abstract model are discussed in detail. At the end paper summarizes by saying that the criminals are moving ahead and ahead in the criminal activities and their practices are becoming more and more sophisticated with the evolution in the technology. However the Law Enforcement Agencies are also at a look out to counter these criminals and their activities so that the battle field remains at parity. [15]

Relationship of the biometrics and the facial recognition of the personel is discussed in subsequent paragraph. Importance of the facial recognition can be judged in context to new visa information system currently in process at a large number of systems. Author has highlighted that facial recognition needs to be developed more before it can be practically applied to high security settings and large scale applications. Author emphasis that use of facial recognition techniques must be coupled with the human supervision, as the errors detected by the humans are almost 80% which have not been comprehended by the computerized systems. Study is focused on the facial recognition with context to hair. Computer systems were falsely accepting two similar image pairs, once the hair are removed compared to when it is present. Manipulation in the hair is the most cost effective way of non-zero effort based attack on the facial recognition system. Author explains some of the issues regarding the growing security concerns of identity frauds, terror-related crimes for accessing resources and at time illegal immigration, however there is a thought that the new visa information system can address such issues. This study is focused on the two aspects of the facial recognition, false acceptance rate (FAR) and false rejection rate (FRR). Purpose explained in the study is to check the effectiveness of the facial recognition software currently being used in a setting like visa information system. [20]

Explaining the principle of identity verification of the users based on already stored behavioral and physiological traits of the sample. Based on the advancement of the biometric technology the devices has are using minutiae point matching. There are two main approaches to do this is direct grayscale and binary detection. This study presents the binary approach to minutia detection of the biometrics. There are two goals of this thesis, firstly to investigate biometric technology in context to available verification devices and to see if they can be converted into small workable mobile applications. Secondly to see that effectiveness and implementation of automated fingerprint recognition as illustrated by Figure - 23. In this paper the working of an arbitrary biometric system is discussed. [21]

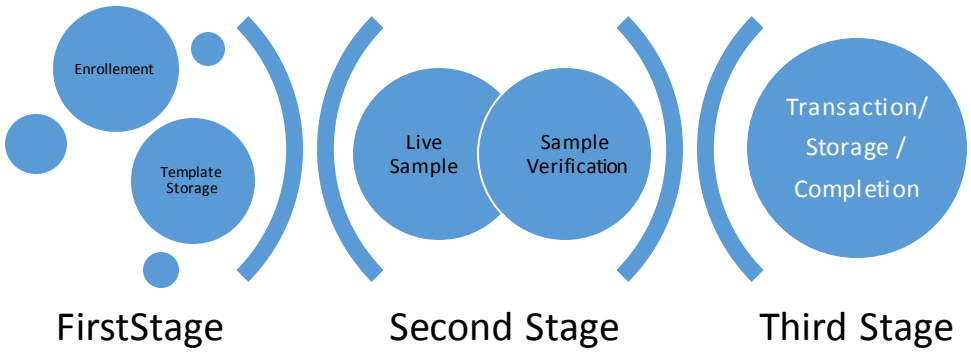

Figure 23 - Biometric Stages of Verification

Extensive literature has been carried out on the subject of biometrics. Paper discusses the identity management conducted through biometrics. Market value of the biometric technology and its prospects have been discussed in accordance to the exemplary evidences. Paper highlights that the incidents of digitized crimes and terrorists acts have been on the rise in modern age. Now the question asked is that as all these incidents have occurred, the reliability and validity of existing surveillance system is questionable. There are many questions which have been addressed in this paper keeping in view the modern security and surveillance system. Question like the efficacy of the modern security system and weather the system distinguishes between the authorized and unauthorized person also is surveillance system user friendly or not. Earlier techniques includes cryptography involving passwords and tokens to be remembered by the user himself. Then what was happening, users were not remembering/forgetting the passwords and token respectively. Then idea of the detection based on biometrics evolved, such as detection or surveillance on the features of physiological or behavioral attribute of the individual. Biometric evolution started back in 1883 from development of Bertillon's system to elementary fingerprinting recognition system by Sir John Galton in 1903. Paper also tells about the biometric acceptance criteria such as, universality,

distinctiveness, invariance, collectability, performance, acceptability and circumvention. Basic tree of biometrics is also explained in the Figure - 24.

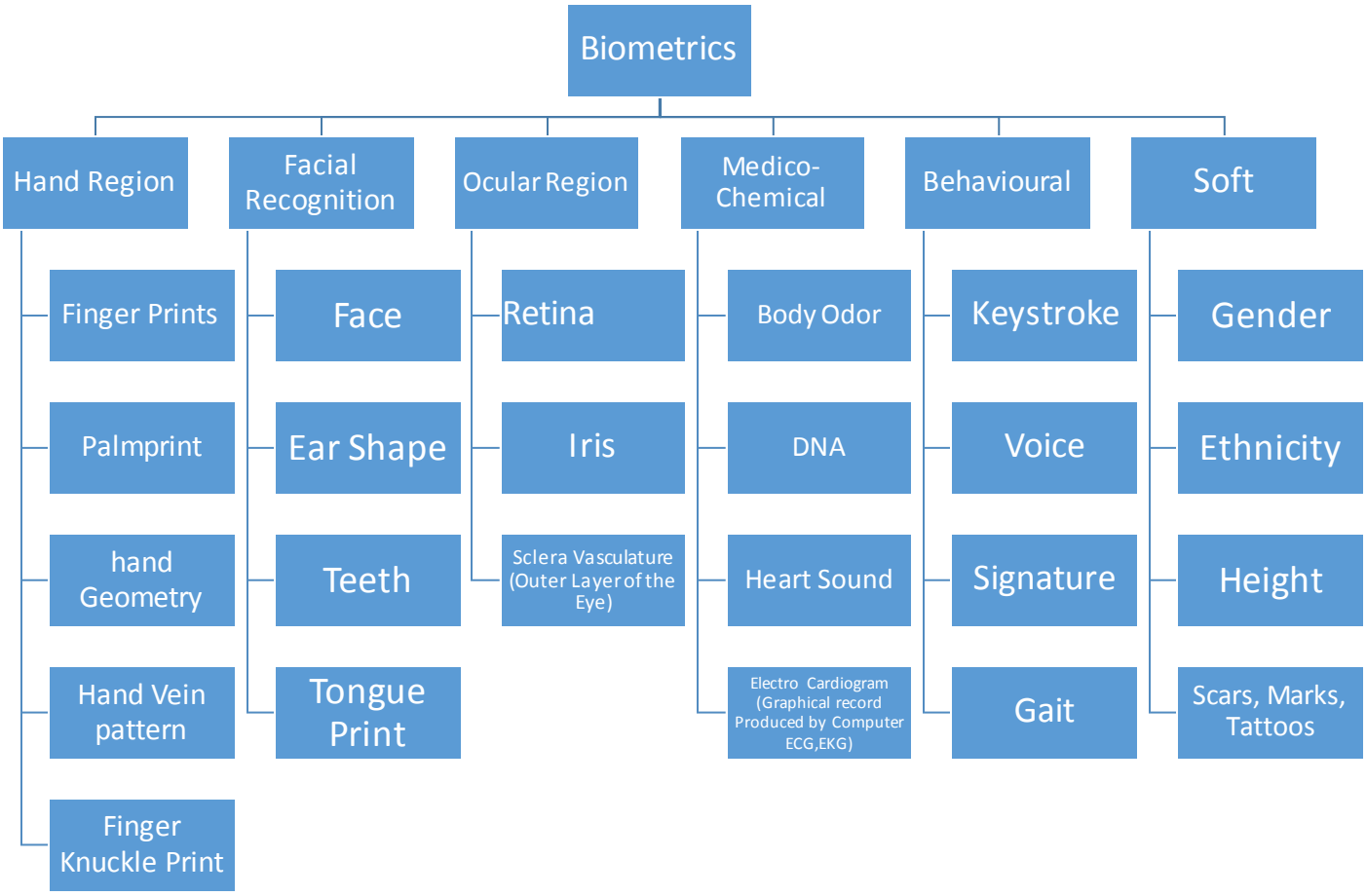

Figure 24 - Classification of Biometric Modalities

In this paper biometric system is also explained in detail. Composition of biometric system is also highlighted as shown in Figure – 25.

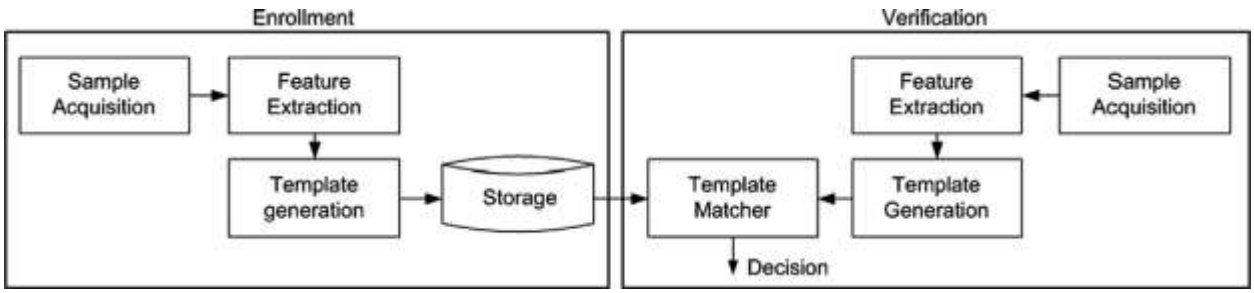

Figure 25 - Enrollment and Verification (S.Yan, 2011)

Concept of multi-modal biometrics uses different biometric trait at the same time for processing and finding out the results as shown in Figure – 26.

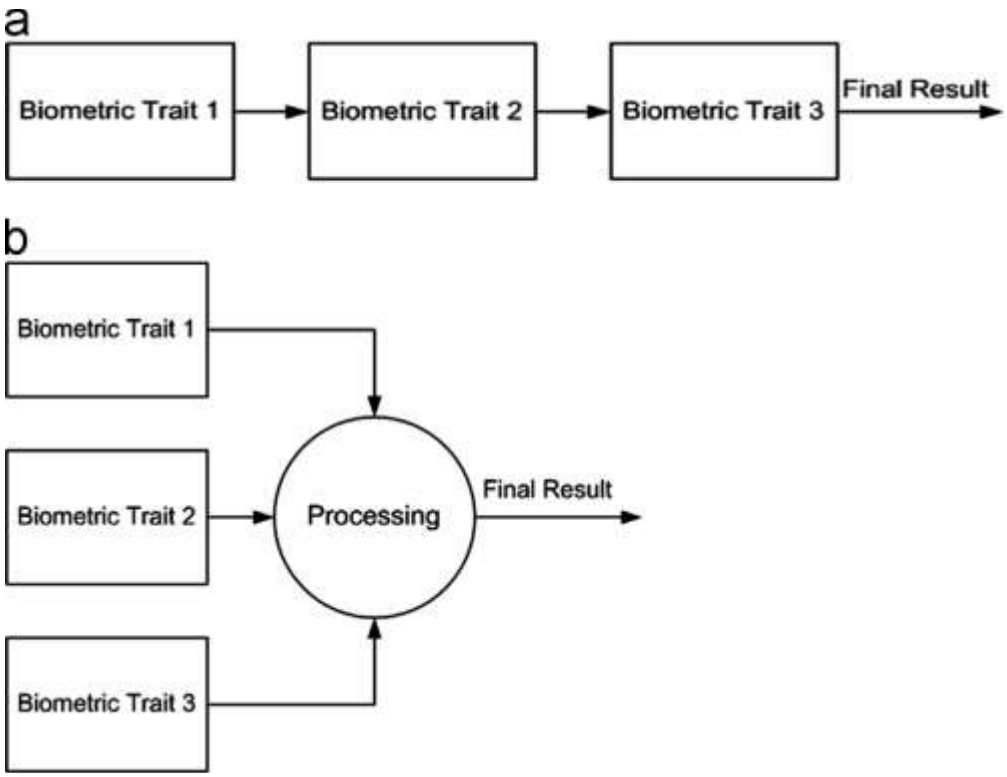

Figure 26 - Multi Modal System Architecture (M.Gudavalli A.V.Babu, March2012)

Author explains that old conventional and cryptographic methods are not very effective as they often require to remember something to process or get something. Whereas the efficacy of using equipment on distinctive features like physiological or behavioral characteristics of the individual are quite helpful and effective. Paper also draws attention to the use of biometrics in the civil sector as well as critical important security installations. [22]

Facial recognition technique is also proposed to identify different faces. Values like polynomial coefficients, covariance matrix and algorithm are based on common eigenvalues. Author explains about the advantages of the technique used id that the identification of faces is on without considering and computing the eigenvalues and eigenvectors. The technique is very simple and effective in computing and extracting the features of the image. Eventual findings in the study is that the time required to match different faces IDs very less in the technique proposed than already present methods like PCA, LDA-based methods, ERE and DCV methods.[26]

Explanation of the meanings of the biometrics in context to analyzing biological and behavioral traits of an individual to confirm his or her identity. It also explains that there are many biometric modalities which are currently being used and implemented such as fingerprints,

hand and facial geometry, Iris, vein structure, gait, voice recognition as well. This paper explores the possibilities for use of corneal technique as biometric identification attribute. Term corneal is a biological term which originates from the word cornea, which is the transparent and virtually interior part of the eye. It consists of five distinctive parts which are *epithelium, bowman's membrane, stroma, descemet's membrane and endothelium*. After that the methods which are used for the measuring the cornea have been discussed like reflection based, which has been the most reliable. This method uses the measure the reflection in the cornea. Then the working has been explained in a way that the recording, detection and processing of corneas details are explained in an elaborate manner. Then author recommends some future works with regards to the sample size. [27]

Use of biometric form, gait which any individual inherits is his or her own are also explored. Gait characteristic are unique for every individual. They are considered the unique characteristics like the finger prints of any individual. One of the application which can be observed by using gait feature of the biometrics, is that it can be very useful in surveillance applications. This study is aimed at development of robust method for identifying gait feature to automatically asses it from a low-resolution video. Two distinct approaches have been discussed one is parametric and other is non-parametric approach. Both the methods have been tested on different data sets to evaluate its effectiveness of detection based. On parametric it is 70 % accurate and on Non-Parametric it is 50% accurate and speedy as well. This framework has been tested on real time scenarios and it has achieved 85% detection and has given 12 % false alarm rate. [28]

Concept of securing the biometrics of an individual have also been analyzed .A frame work has been proposed with the name *generalized evaluation framework* for privacy and for security assessment. Framework proposed is flexible and indispensable. Different algorithms have been used for the subject framework. Future work proposed in this regard are the extension of the framework and its practical demonstration and evaluation. This framework can be used as a bench mark for further analyzing different templates. This paper also suggests that the relationship between recognition performance and security should be further analyzed. [29]

Traditional authentication system's basis: Passwords, cryptographic, tokens being used for security assistance all over the world. These systems are unable to meet strict security requirement in this digitized century. Author compares the old systems with biometric- based authentication system. Biometric based authentication is considered to be the most valid and credible piece of information. Biometrics includes like physiological, behavioral

characteristics of an individual. As the advantage between the traditional and biometric based authentication is that the biometric data cannot be lost, forgotten or guessed) where as in traditional methods the password and token are forgotten and were causing many problems in the authentication system. This paper addresses the main issues and develops the techniques to eradicate the associated and linked problems which are inherent and circumstantial as well. [30]

2.5.13 Terrorist/Criminals Cases Investigation

The design and application of a tool, OpenVL, that will not only meets the needs for speedy initial triage, but also can facilitate the review of digital evidence collected at later stages of investigation. This software is easy to understand and can readily collect and retain the forensic data. This software enables later interaction with the digital evidence safely and easily. The forensic value of the digital evidence does not degrades when OpenVL is used by the first responder for the collection of the digital evidence. Also by the use of this software the personel working in the field as first responders who does not have any specialized forensic training to review digital artifacts can record, collect and maintains the velocity of time-sensitive investigation. Also flexibility and usability of the OpenVL is discussed. It also enables easy and speedy presentation of Digital evidence in the courtroom.

Under normal procedure the first responders are told to collect the digital evidence from the crime scene. Digital evidence collected from the scene eventually forms part of the queue to be further analyzed at forensic lab. This procedure at times take long to further investigate the procedure. This software is developed for the Digital forensic Practitioners, investigators and first responders. [1]

The framework for digital forensics which includes the investigation process model on physical crime scene procedures. This paper explains that each digital device is a digital crime scene which is also included in the physical crime scene. Entire process includes the collection of digital evidence, its preservation, and reconstruction of digital crime scene. The reconstruction of the digital crime scene helps to test the developed hypothesis.

This paper also explains the concepts and definition of the digital evidence, forensic investigation, and digital analyses types. Also the framework presented has five phases. Readiness Phase, Development phases, Physical crime scene investigation phase, digital crime scene investigation phase and presentation phase. The principal used is simple cause and effect of events. In which the author has searched for the evidence that shows the cause and effect of an event and then he developed a hypothesis about the events which have occurred on the crime scene. [2]

The major focus on the problem faced by FBIs Forensic Audio, Video and Image Analysis Unit (FAVIAU). Author explain that the examinations are performed in absence of automated biometric application. By virtue of which automated biometric examination workflow has decreased. In the absences of the automated biometric application there is problem in presenting the statistics and rate of probability of criminal in the court of LAW. Initial research regarding facial, ear and hand biometrics are in the preliminary phases. However the FAVIAU have funded research projects concerning facial and ear individualization. Paper explains the working of the FAVIAU that two types of examinations are performed on the image by the examiners, photographic comparison and photogrammetry. Sources of the image has been explained that it could be any like "questioned individual" which are submitted to FBI for analyses. It can also be an evidential media ranging from different surveillance videos from a bank to film still images recovered from a suspect. It can be an image from questioned individual's computer. Author also explains that the analysis on the image is performed by methods of recognizing individuals based on their physical or behavioral characteristics and not by automation. FAVIAU has considered it very important that in order to increase the productivity and efficiency of investigators biometric development is very important. Author emphasizes that by the use of automated biometric systems which focuses on facial recognition, ear identification, hand identification, gait attributes and analysis, and the determination of height would greatly enhance the efficacy and efficiency of the forensic work currently being performed by the FBI. [9]

Different frameworks have been studied and literature Review has been conducted on twenty samples (n=20) frameworks to evaluate and highlight the preservation of digital evidence and protection of basic human rights during digital forensic investigation. He reported that only thirteen sample (n=13) were included in the study and were lacking the preservation of digital evidence and protection of basic human rights as explicit overarching umbrella principles. Author has proposed an extension to overcome this issue to Reith's abstract digital forensics model in which expounding the preservation and protection of evidence and human rights respectively as basic umbrella principles.

This also explains that digital device have become an important part of our lives. These devices record our details in so precise manner that they transform every detail into digital behavioral archives of respective user. Paper also explains that the research is being conducted in two fronts with regards to Digital Forensics (DF) and Digital forensic Science (DFS). Technical part of research covers the development of tools which will aid in systematic Digital forensics (DF) investigation. Theoretical part of the research focuses on the area of (DFS). Theoretical

part of the research focuses on development of theories and methodologies including processes, frameworks and models to conduct DF investigation. Author has used the Reith's work [1] as base and extended it to the level which has both the elements of preservation and protection of digital evidence and human rights respectively as shown in Figure – 27. Which explains the entire process of digital forensic model under protection and preservation. [12]

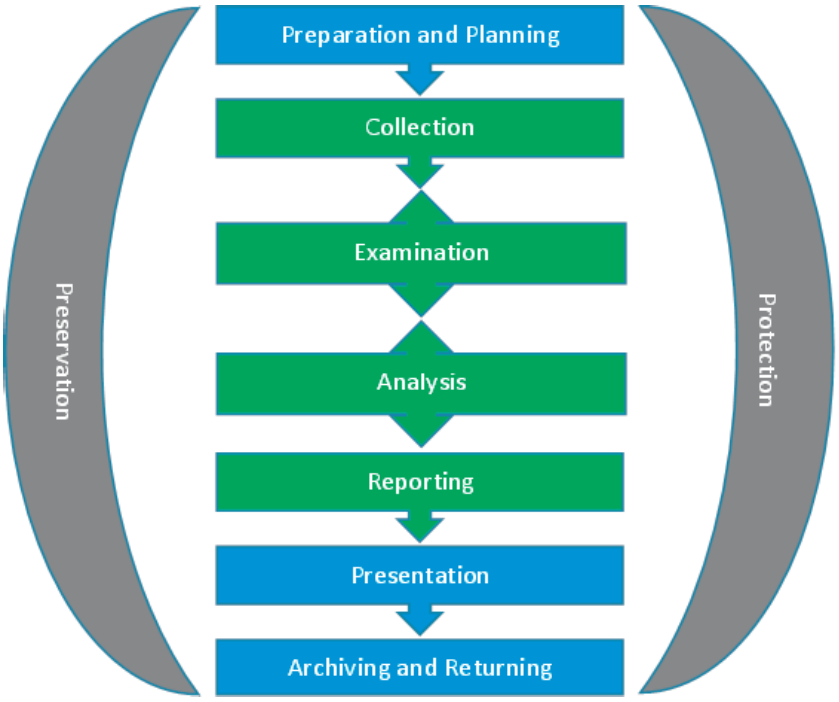

Figure 27 - Digital Forensic Models (Reith M, 2002)

Author explains about the forensic investigation of digital evidence, as a phenomenon which in general is understood as post-event response to an important occurring with vital piece of information security. Paper also explains about the benefits which an organization can get, once it is interested in gathering and preserving digital evidence about various occurring's. Author highlights the definition of forensic readiness in context to cost effect of conducting an investigation, whilst maximizing potential use of the digital evidence. Author emphasis about the cost and benefits of such approach as humongous. Paper also bring out the necessary ingredients for use of digital evidence such as enhanced computer systems, staff monitoring, technical aspects involved, physical and procedural means to secure data to evidential standards of admissibility, processing, admissibility, processes and procedures to be doubly ensured by the staff, legal issues involved in the process of evidence, appropriate legal advices to get involved with the law enforcement. This paper is very important to understand that if any organization is interested or willing to implement the forensic readiness, a ten step process is proposed for the implementation. Author also explains about the understanding and need of the forensic readiness is a risk assessment. He also explains that risk assessment for something like

this would inculcate BS 7799 or ISO 17799 to be a valid starting point, but it will not asses all those situations where digital evidence may be required. The author lists all the ten points, which includes Defining the business scenarios in which digital evidence is required. Identification of all available resources. Defining the requirement of digital evidence collection. Establishment of capability of legal issues. Need for storage and retrieval of the information. Staff Monitoring. Issues concerning the investigation process. Training of the individuals involved. Documentation involved in the process of evidence and scene reconstruction. Legal aspects of different actions involved in response of any incident. [14]

Norwegian information security laboratory used the technique of Approximate Hash Based Matching (AHBM). This paper explains that this technique is used to identify complex and unstructured byte-level similarity. Papers aims at to help the investigators in different Law Enforcement Agencies to organize and analyze digital evidence using approximate matching. Author also highlights that there are tools which are being used to match the data which have any bit of similarity in them. Tools which are used by approximate matching are in use for quite some time but are not being integrated with more technological advanced digital investigation tools. Paper also explains the type of Approximate Matching (AM). There are three mainly three types, Perceptual, content, and hash based matching. Content and Hash matching is utilized by the computer to identify the data on similarities. However the perceptual method identifies similar objects on the basis of the human beings. With the help of perceptual method similar pictures and video can be identified. In case of hash and content the identification is done on the basis of binary codes i.e documents, executable. All these hash, content and perceptual techniques all are considered important and have importance with respect to digital investigation. [17]

In this paragraph enhanced capability of forensic analysis techniques by imparting partial and full automation of the investigative process is discussed. Problems involved in analyzing complex and huge data volumes of digital evidence in digital investigations.[19] Digital evidence is explained as digital data which can be used to imply or deny a hypothesis about an incident. Digital evidence is on consistent increase encompassing technologies like computers, networks logs, mobile devices etc. In this paper different models and frameworks have been discussed that are currently being used in digital investigation. Paper highlights the issue concerning the analysis part of digital investigations, as it is upon the experience and technical expertise of the investigator which is mostly manual and relies on co-operative patterns. Semantic integration and representation of digital evidence is discussed in detail. Author

explains about the issues currently being faced in development of an evidence analysis, correlation and integration for digital investigation based on semantic technologies. [18]

2.5.14 Counter Terrorism

Different terms and definition have been explained for understanding of the concept of digital evidence and digital evidence gathering. Importance of digital evidence gathering in apprehending the cartels. Legal issues regarding the authenticity of the digital evidence have been explained. Main distinction of digital evidence gathering is also highlighted in this chapter. Resources required to gather digital evidence. Then the elements of the digital evidence gathering have been listed as well. Legal issues which are related to digital evidence gathering have been discussed in detail. At the end some good practice relating to digital evidence gathering are highlighted. This chapter explain the need and requirement of today's world changing technologies, more and more information is available in digital form nowadays to be stored and distributed by electronic means. This increase in electronic information requires many agencies to increase the use of digital evidence as a frequent or standard tool in their fight against cartels. The Anti-cartel Enforcement Manual is a work in progress currently to reflect the current status of digital evidence gathering at different tiers of Law Enforcement Agencies. In this manual especially in this chapter different terminologies have been explained like computer forensics, digital information, digital evidence, forensics itself, chain of custody of the evidence, chain of custody of evidence, data carriers, hash values, forensic image, live forensics and cloud computing. Then the importance of the digital evidence gathering is discussed as digital evidence collected in different jurisdictions such as raids, or inspections, or obtained through compelled discoveries, even at times not decisive by itself, has proven competition infringements. Now this digital evidence collected has become the most important and powerful tool to fight against cartels. Agencies have made collection of digital evidence as most important practice against cartels. Agencies are currently using digital evidence and are stating that some authorities are using it as a complement to other types of evidence. Furthermore digital evidence is also helping in different levels of investigation phases. Right now in USA more than 92% of the agencies have legal authority to collect digital evidence and more than 83% have used their powers. Some agencies have been given the authority to order necessary measures by themselves and some do require search warrants or court orders. Some agencies currently are using main distinctions in digital evidence gathering like raids, searches and inspections. While some are using both the compelled discoveries and as well as raids, searches and inspection as main practice. Resources required for the digital evidence gatherings are good staff, some recognizable position of digital evidence gathering in the organization, officers and forensic specialists, training of the staff and trainee and cooperation

with other public agencies. After that there are certain elements of the digital evidence gathering like tools both software and hardware. Then comes the chain of evidence / Authenticity of the digital evidence collected. Also the preservation of the digital evidence. Processing of the digital evidence. Analysis and storage of the evidence. After then the legal issues concerning the digital evidence gathered are required to be understood and completed in all respect. There are advantages and disadvantages both related to digital evidence gathering one disadvantage which is of unique importance that change in technology leads to change of equipment and procedures. [6]

The major focus is on evaluating the corroborative evidence. Author explains the corroborative evidence by giving an example about the questioned individual being present at the crime scene and a person testifying against him that he was present at the scene. Now this witness has less value in court of law. What happens that another individual testify against the questioned individual, than it is corroborating the effect of the first witness making its evidential value stronger. Corroborative evidence does not needs to be testimonial all the time. Author also explains about the circumstantial evidence as well, as in the case of I watching the time from my watch and asking another person about time on his watch, my saying about the time is corroborative by the other person if he says that it is the same time as of mine. Author brings about a specific point highlighting that the watch can be at the wrong time thereby making the corroborative evidence is fallible. Author proposes two methods for the audience to judge which is right. Each method has its pros and cons. Each method will contribute a lot to the evaluation of the corroborative evidence. [10]

Understanding of historical perspective of digital evidence is very important. Example of the Federal Bureau of Investigation has been discussed. Details about the development of the programs to examine computer evidence. Paper also explains about increase in the work load of addressing the demands of investigators and prosecutors in an effective, structured and programmatic manner. FBI has established Computer Analysis and Response Team (CART). Author highlights the problem that FBI was using the resources available within the organization to be used for examining the digital forensics. Now a days what is in practice is the evidence collected is sent to the laboratories where experts are analyzing the evidential value of the evidence. Author has referred to a survey which was conducted in 1995 the 48% of the agencies have the digital forensic capability. However 68% of the computer evidence which has been seized is forwarded to laboratories who are conducting the research. Paper also explains the transition of the working scientists from the group of technical working group (TWGs) to scientific working group (SWGs). [16]

Effective use of the biometric technology in Global war on terror (GWOT) has been explored and explained with regards to its application in Unmanned Arial Aircraft (UAV). Using biometric data like finger print, for rapid identification of high value target (HVT) in ground and Maritime Interdiction Operations (MIO). This study has been performed in a test bed environment to simulate a real live special operation environment in theatre (field). This paper provides a model for the identification of the biometric in tactical network environment. This paper also evaluated the time it took to send finger print data from field to central data base, with identification data results then sent it back to the field. The longest time frame was 70 minutes with low bandwidth satellite communication and shortest was 4 minutes for reach back to central data base and 2 minutes for local data base. [25]

Security after 11 September 2001 attacks on the US has become an important focal point. Many biometric techniques evolved after that. This paper aims at giving the introduction about the biometrics, smart cards and with the systems which are using cryptographic tools to communicate, secure and exchange biometric data from smart cards. After that about faking a finger print in the finger print sensing device. Then the approach for lightweight fingerprinting for smart cards will be explained. Security protocol involved in different applications. Then at the last technique NIST to be discussed as presented in the paper. Paper also present the antagonism involved between cryptography and biometrics as well. [32]

This study is of unique importance to this research work as it elaborates on the change of current Pakistani law, practice of the investigating agencies and use of modern technology to counter this menace of terrorism. Terrorism has shattered Pakistan in every aspect of todays modernized century. In past one and a half decade Pakistan has been in the forefront to fight the menace of the terrorism. Suggestions regarding the role of police to counter the terrorism in Pakistan have also been highlighted in the paper. This paper also highlights the main factor involved in the failure of working of Anti-Terrorist courts are, handing over of the terrorists to intelligence agencies for retention hampers the police procedure and the case stops, lack of cooperation and coordinated effort between different agencies working in Pakistan to counter terrorism, police has been given limited access to handle terrorist cases, delay of handing over of the individuals to police by different agencies working with in Pakistan, threats to lawyers, witness protection program, acquittal rate is very high, Lack of training and resources available to police to counter this threat etc.[31]

3 CHAPTER THREE: QUANTITATIVE AND QUALITATIVE ANALYSIS

3.1 Questionnaire

Questionnaire was made by listing the factor for variables i.e. Digital Evidence (Biometrics) and Investigation of terrorists from the literature. Questionnaire was divided in three parts.

1. In Part-I the information regarding respondent is asked which includes name, age, gender and experience in their own particular field.
2. In Part-II the questions regarding digital evidence (biometrics) have been asked to know the general understanding of the terminologies. Also to get the opinion of the respondents and factors about the use of biometric technology as digitized evidence.
3. In Part-III the questions regarding terrorist investigation have been asked. Use of biometric technology as digitized evidence, factors and legal issues involved in the use of biometric technology as digitized evidence during investigation of terrorists have been asked. These questions have been designed in a way to know the respondents opinion and their understanding of the issue.

Questionnaire underwent face validity and for content validity factors have been listed. Pilot study was conducted to further evaluate the content validity. After this, reliability analysis has been conducted to check the unrelated sub factors who are not contributing sufficiently to variables. Exploratory factor analysis have also been conducted to check the under lying construct validity of instrument. This was very important as to see whether it is collecting the data it is required to. Results of factor analysis were effective thereby making instrument valid. Data was collected on questionnaire in order to find out the opinion of using digital evidence (Biometrics) from people who are involved in investigating and apprehended terrorists/criminals on routine basis in different investigating agencies, intelligence departments, law enforcement agencies, police and army. Likert scale has been used for questionnaire. The scaling technique is used to get the opinion of the people about the use of digital evidence in form of biometrics during the investigation of terrorists/criminals etc. Pilot study was conducted to check the validity of the questionnaire on twenty sample (n=20). After that mean of variables have been computed. Co-relation of variable's mean was also checked which came out to be positive. Graphical representation of this relation is shown with the help of scatter plot, which is shown in Figure 28.

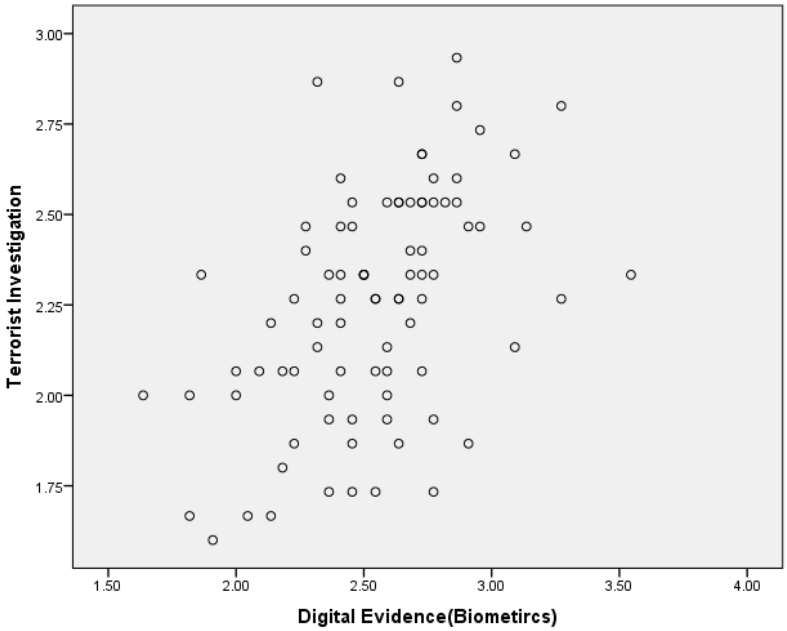

Figure 28 - Scatter plot showing positive correlation between variables

Also the Table - 1 shows that Pearson correlation is significant at 0.01 and the value of Pearson correlation came out to be .485.

Correlations

		DE	TCCT
DE	Pearson Correlation	1	.485**
	Sig. (2-tailed)		.000
	N	86	86
TCCT	Pearson Correlation	.485**	1
	Sig. (2-tailed)	.000	
	N	86	86

**. Correlation is significant at the 0.01 level (2-tailed).

Table 1 – Correlation of Variables

Reliability analysis of the variables is also carried out. Results of the Cronbach's alpha were found to be in permissible limits for both the variables. Values of Cronbach's Alpha for digital evidence (biometrics) and terrorist investigation are .691 and .612 respectively as shown in Table – 2 and 3.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.691	.694	22

Table 2 – Variable, Digital Evidence (Biometrics)

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.612	.651	15

Table 3 - Variable, terrorist's investigation

Exploratory factor analysis has also been carried out to further check the validity of questionnaire through SPSS. The values of determinant and KMO were also in permissible limits. Values of determinant and KMO for variable digital evidence (biometrics) are .001 and .566 and for variable terrorist investigation are .005 and .705 respectively. Values of KMO for both the variables are shown below in Table – 4 and 5.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.566
Bartlett's Test of Sphericity	Approx. Chi-Square	571.676
	df	231
	Sig.	.000

Table 4 – Value of KMO for variable Digital Evidence (Biometrics)

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.705
Bartlett's Test of Sphericity	Approx. Chi-Square	421.734
	df	105
	Sig.	.000

Table 5 - Value of KMO for terrorist investigation

3.1.1 Validity Threats

Validity threats are an important part of any research work. The results of research work can be improved to certain level due to validity threats as validity threats identifies those factors and issues which can affects the results of the research work.

In order to improve the research results, three types of validity threats have been carried out as mentioned by (Wohlin, et al. 2000) i.e. external validity, construct validity also checked by SPSS and conclusion validity. All three types of validity threats and their implication in the context of thesis research work have been discussed.

3.1.1.1 External Validity

According to Damm (2007) and Berander (2007) validity that makes sure that the results obtained from research work can be generalized to other domains or not is called external validity. According to Berander (2007) external validity is also known as generalizability.

According to Wohlin et al. (2000) external validity is'/.u used to determine the applicability of the research results to other domains.

Selection of wrong subjects from the population can cause a potential threat to external validity as results obtained from the wrong subjects cannot be generalized to whole population. In order to minimize the threats to external validity, interviewees have been selected based on having certain knowledge of investigation and apprehension, digital evidence and biometric technology. Interviewee were selected from different security departments, police, LEAs and intelligence agencies. As the study is performed to propose guidelines about the use of biometric technology to counter terrorism that's why interviewees with different expertise were selected in order to have their opinion on the subject.

3.1.1.2 Construct Validity

According to Wohlin, et al. (2000) and Bernader (2007) validity that shows the relationship between theory and observation is called construct validity. For example if experiment is the research methodology for a research work then according to construct validity, it is important that experiment results are generalized to the main idea behind the experiment (Wohlin, et al. 2000).

The main threat to the construct validity is called evaluation apprehension which is explained by Wohlin, et al. (2000). It is explained that there exists certain tendency among people that they like to look smart when there is some sort of evaluation while on the other hand there are people who are afraid of being evaluated (Wohlin, et al. 2000). Threat to construct validity has been eliminated by selecting interviewees based on their will and interest in the subject. Furthermore prior discussion, with the interviewees before interview, also helped to minimize the threats to construct validity. The threats to construct validity in the questionnaire part were eliminated by not mentioning the respondent's names.

According to Wohlin, et al. (2000) another threat to construct validity of the results is mono-operation bias which means that there is only one independent variable, case or subject involved in the research study. This threat to construct validity is eliminated by selecting thirty one interviewees for research study. Also the questionnaire respondents were selected from both sides i.e. citizens and Pakistani security forces (LEAs, Intelligence agencies, Police)

This threat has also been eliminated by carrying out exploratory factor analysis of the questionnaire to check the underlying construct validity of the questionnaire. Values of determinant > .00001 and KMO> .5 are greater than standards.

3.1.1.3 Conclusion Validity

According to Bernader Wohlin, et al. (2000) validity that guarantees that the results obtained from research work are reliable enough to lead researchers to the correct conclusion of the research work is called conclusion validity.

Questionnaire used for the interviews purpose can pose a possible potential threat to conclusion validity that's why a lot of work has been done to eliminate the potential threat caused by the questionnaire to the conclusion validity. The questionnaire was designed and sent to supervisor for feedback. After confirmation questions were finalized. Reliability analysis has been performed to check the values of Cronbach's alpha. All sub factors have been eliminated, which are not contributing sufficiently to variables. This threat has also been eliminated by carrying out exploratory factor analysis of the questionnaire to check the underlying construct validity of the questionnaire. Values of determinant > .00001 and KMO> .5 are greater than standards.

3.2 Questionnaire Findings

3.2.1 Respondents Details

A total of hundred (100) questionnaires were distributed out of which ninety one (91) questionnaires were collected back. After scrutiny of the questionnaire and considering the missing values in the results eighty six (86) questionnaires were included to find out the results. Out of these eighty six (86), sixty eight (68) respondents were male and eighteen (18) respondents were female. This questionnaire was distributed keeping in mind the sample population which is people from intelligence agencies, law enforcement agencies, police, security forces personel, lawyers and general public. They were of different age groups ranging from twenty (20) years to seventy (70) years. The Figure – 29 and 30 shown below gives the respondents gender and age.

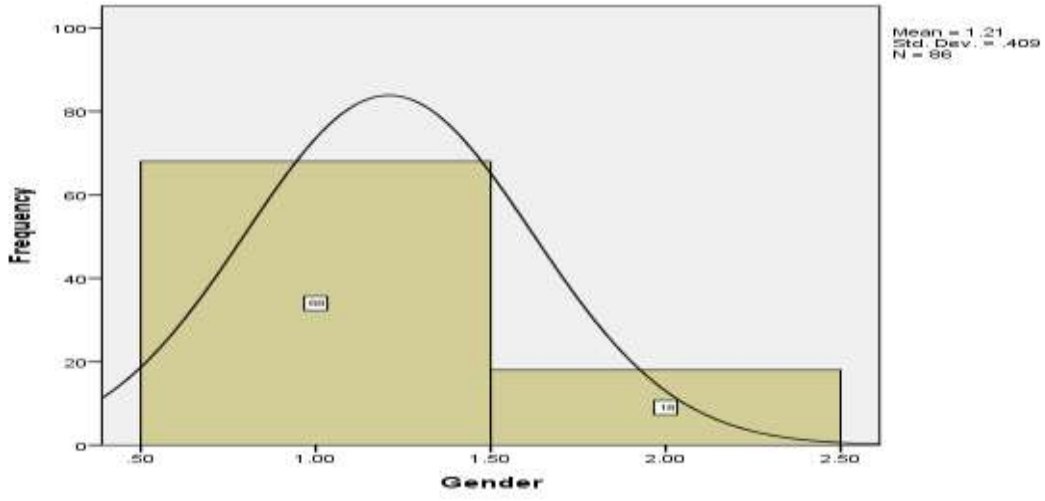

Figure 29 - Gender of respondents

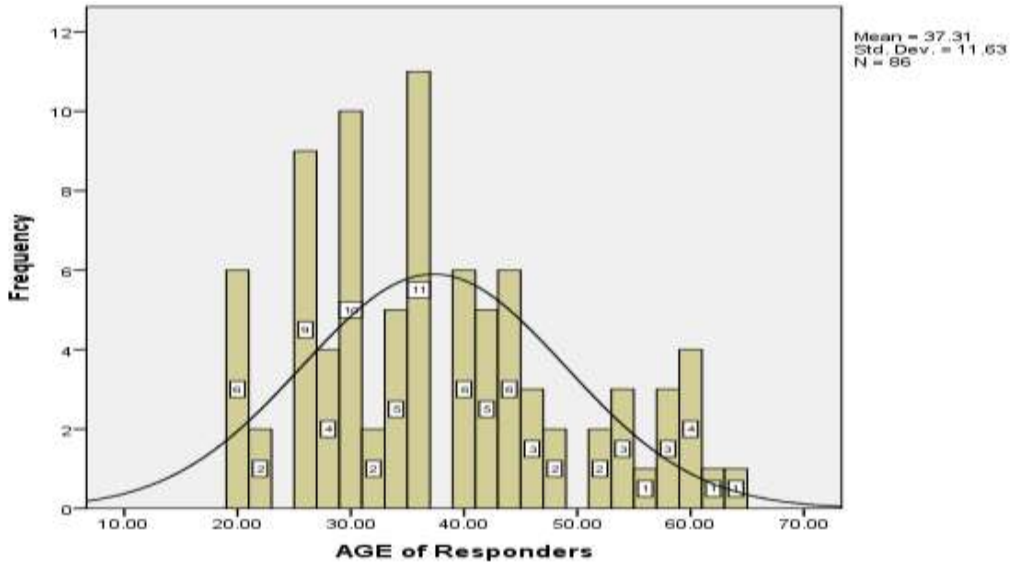

Figure 30 - Age of Respondents

3.2.2 Scaling Questions

Questionnaires are made on likert scale ranging from one (1) to five (5). One (1) being strongly agree , two (2) agree, three (3) neutral, four (4) disagree and five (5) strongly disagree.

3.2.2.1 Digital Evidence (Biometrics)

Question 1 & 2. The Figures – 31 and 32 are showing about the general understanding and know-how of terminologies which are under discussion. Mostly the respondents are aware of the terminologies i.e. digital evidence and biometrics. However there are certain people in the general public who are not aware of the terms. This is clearly shown by the figures. Seventy nine (79) 95.38% and eighty (80) 93.84% respondents out of eighty six are completely aware of the terms digital evidence and biometrics respectively. Three four (4) (6.14%) and (3) 4.52% respondents are unaware of the terminologies digital evidence and biometrics respectively.

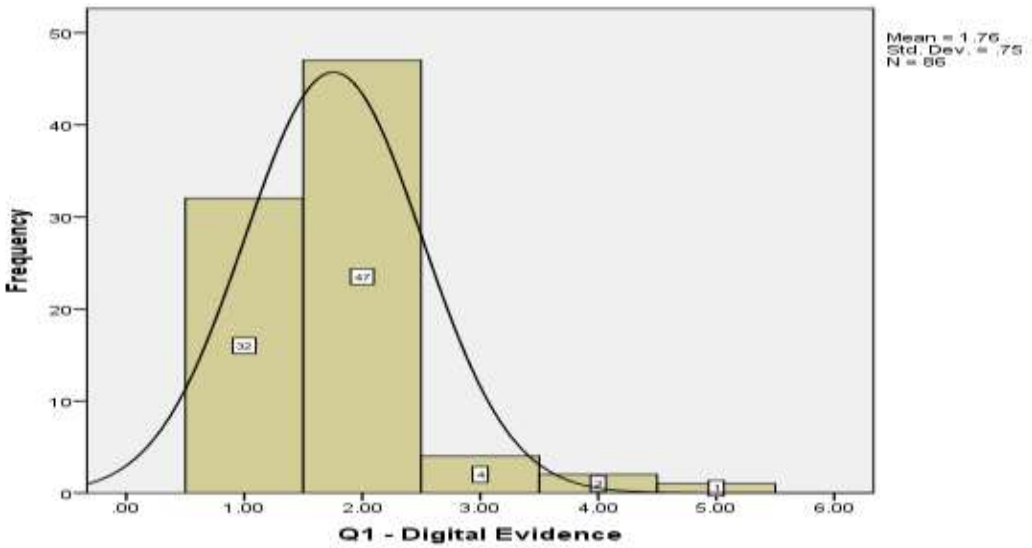

Figure 31 - Understanding about Digital Evidence

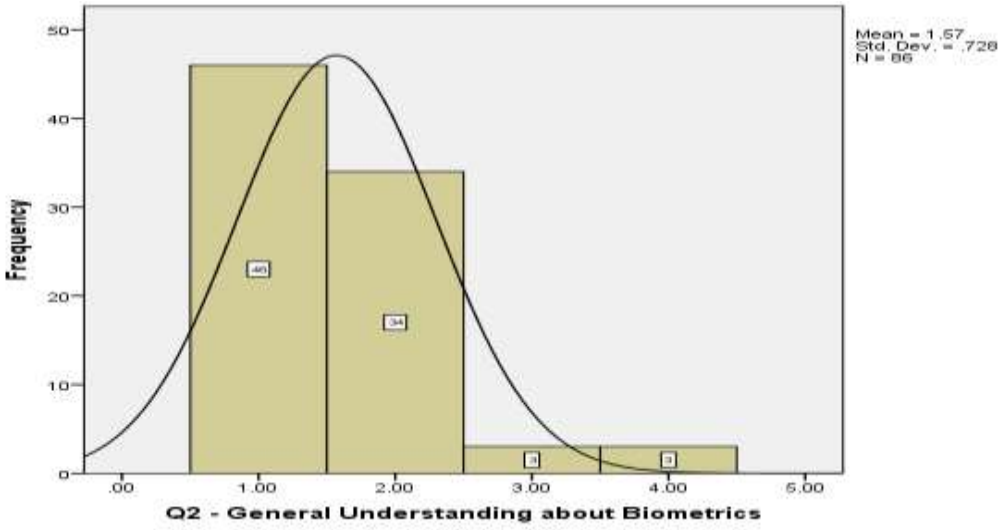

Figure 32 - Understanding about Biometrics

Question 3. The Figure - 33 shows that most of the respondents agree with the statement asked i.e. biometric forms part of digital evidence. Total of seventy three (73) 87.69% out of ninety one (91) have agreed with the statement. Seven (7) 9.23% didn't agree with the statement asked, and six (6) 3.07% have no idea about the use of biometrics as digital evidence.

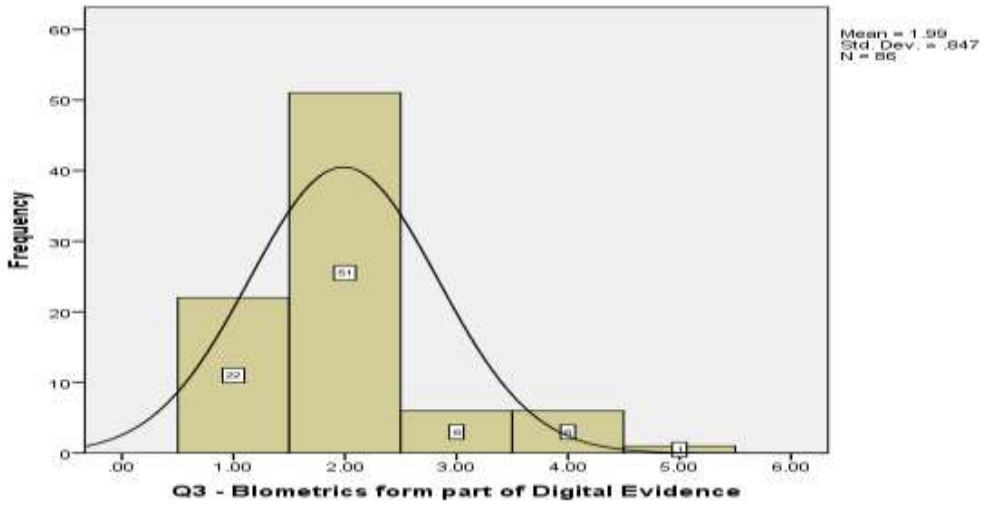

Figure 33 - Biometrics as Digitized Evidence

Question 4&5. The figure below shows the attitude of the respondents to the use of digital evidence in form of biometrics in apprehending the terrorists. Respondent have been asked questions separately distinguishing the digital evidence and biometrics as digitized evidence. The response shows that they have a strong believe about the use of biometrics as digitized evidence.

In question 4 respondent's response with regards to the used of digital evidence in proving terrorist guilty in court of law is shown in Figure - 34. Out of 86 respondents seventy five (75) 90.76% respondents are agreeing to the statement, eight (8) 4.61% don't know about digital

evidence and three (3) 4.61% don't agree that digital evidence can help in proving the terrorists guilty in court of Law.

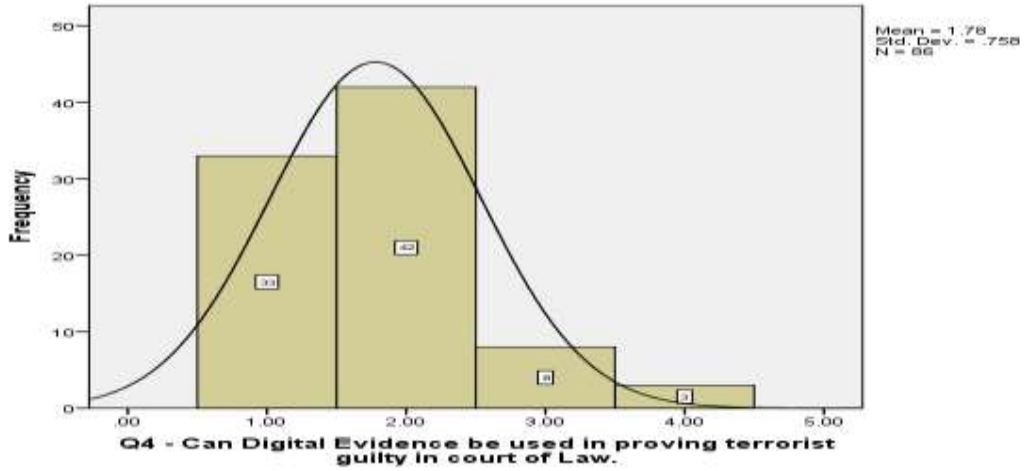

Figure 34 - Use of Digital Evidence in proving terrorist Guilty in court of Law

In question 5, the Figure - 35 shows the respondent's response towards the use of biometrics as digitized evidence. The response shows that there is a strong belief of the respondents that biometrics as digital evidence can be used in proving terrorist guilty in court of Law. Out of 86 respondents eighty (80) 95.38% are agreeing that it can be used whereas five (5) 3% are unaware of the use of biometrics as digital evidence and only one (1) 1.5% don't agree with the statement.

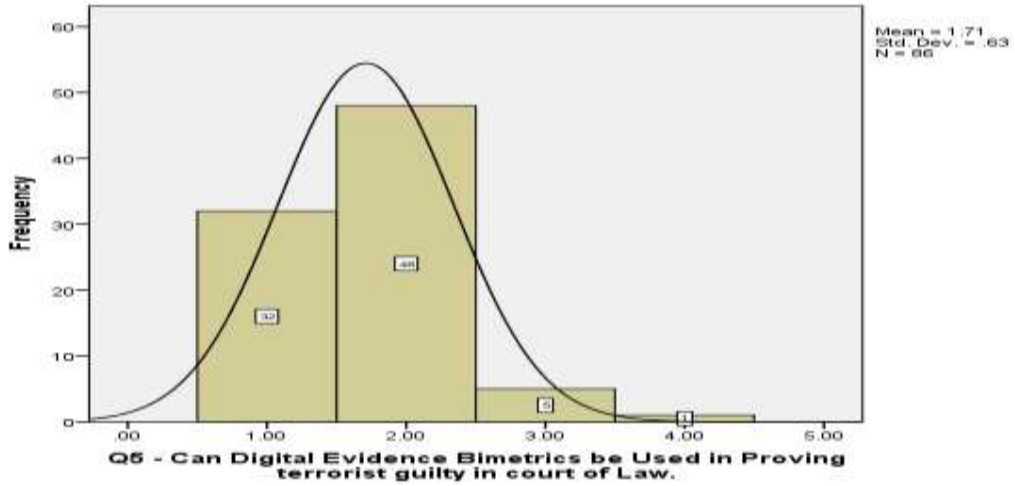

Figure 35 - Digital Evidence biometrics in proving Terrorist guilty in court of Law

Question 7. The Figure - 36 shows the respondents response about police that they collect sufficient evidence from the crime scene. A mixed response have been obtained as majority including the policemen and people from LEA's are agreeing that sufficient evidence is not collected from the crime scene against these terrorist/criminals. Out of 86 respondents thirty nine 39 (47%) are disagreeing that sufficient evidence is collected from the crime scene against these terrorist. Twenty four 24 (24%) out of 86 respondents don't even know that either the evidence is being collected or not. Twenty three 23 (27%) out of 86 respondents are agreeing that police collects evidence from the crime scene against these terrorists.

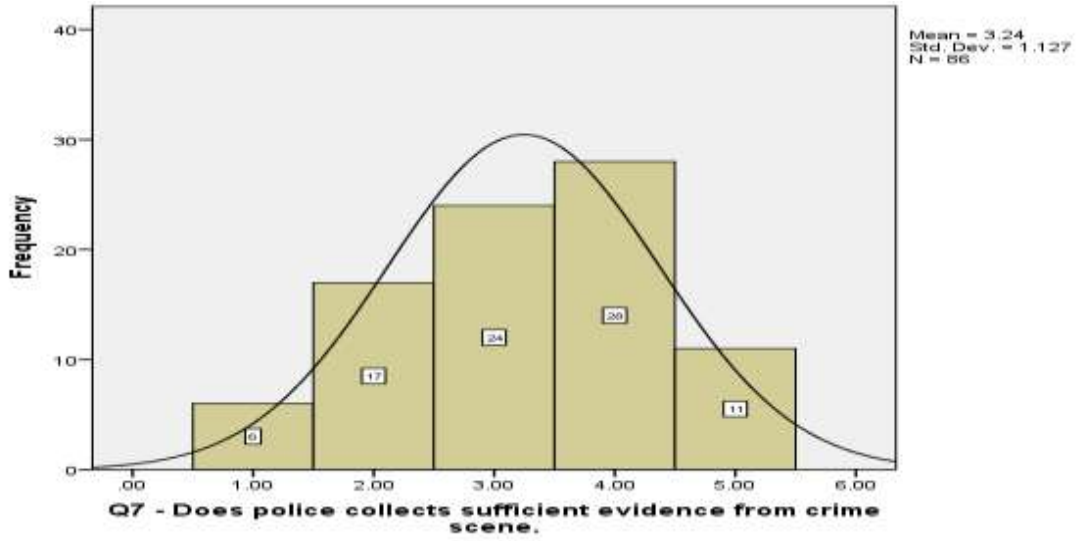

Figure 36 - Police Collection of Evidence

Question 8. The Figure - 37 shows the attitude of the respondents about the use of digital evidence against terrorists in court of Law. Out of 86 respondents thirty three 33 (43%) respondents believe that police does not uses digital evidence against terrorists in court of Law. Twenty three 23 (24%) respondent out of 86 don't know about the fact that either police is using digital evidence or not, they have a neutral approach. Thirty 30 (32%) are agreeing the yes police uses digital evidence against the terrorist in court of Law.

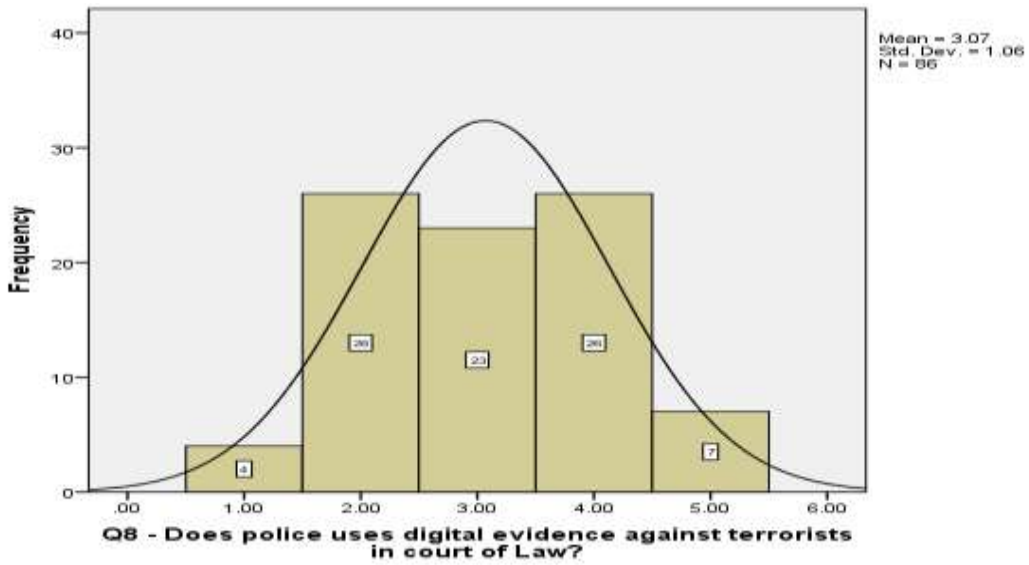

Figure 37 - Use of digital evidence by Police

Question 12. The Figure - 38 shows the respondents response when asked about i.e. Evidence collected by police from crime scene is sufficient to prove terrorists guilty in court of law. Forty nine 49 (58%) out of 86 respondents have disagreed with the statement showing that police do collect the evidence from the crime scene but it is not sufficient to prove terrorists guilty in court of law. Eighteen 18 (21%) out of 86 respondents are neutral about the statement asked. Nineteen 19 (20%) out of 86 believes that the police collects sufficient evidence from the crime scene which can prove terrorist guilty in court of law.

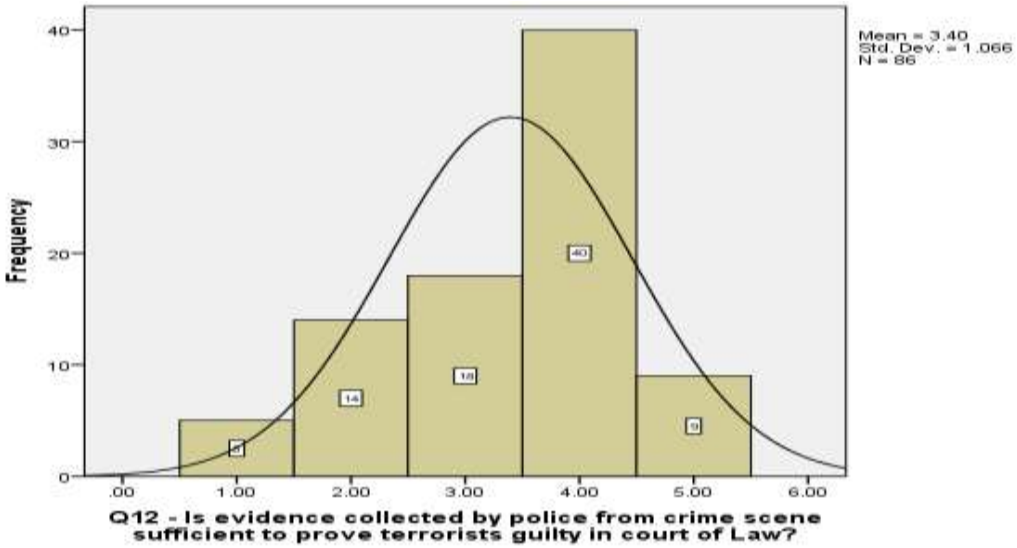

Figure 38 - Evidence collected is sufficient to prove terrorist guilty

Question 9. When the respondents were asked about the Law Enforcement Agencies that they collect evidence while apprehending terrorists from crime scene. The respondents have shown that yes they do as shown in Figure - 39. Fifty one 51 (58%) out of 86 have agreed that yes LEA collects evidence from the crime scene while apprehending the terrorists as shown in Figure - 40. Twenty three 23 (27%) have a neutral approach about collection of evidence by LEA while apprehending terrorists. Twelve 12 (15%) out of 86 have disagreed that no the evidence is not collected from the crime scene while the apprehension is taking place.

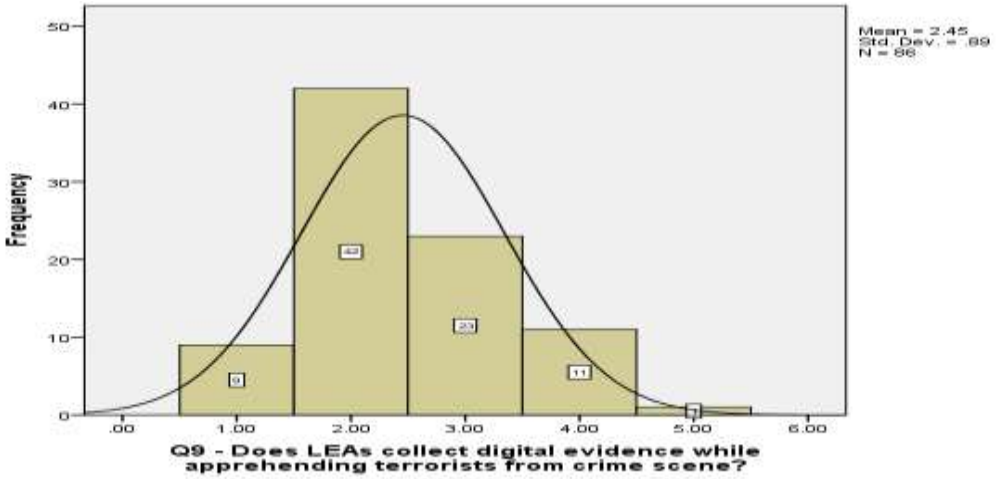

Figure 39 - Working of LEAs

Question 10. When the respondents were asked about the sufficient collection of the evidence from the crime scene by the LEAs, the responses are shown in Figure - 40. Thirty six 36 (38%) out of 86 respondents were agreeing to the statement that yes they do collect sufficient evidence from the crime scene. Twenty nine 29 (35%) out of 86 respondents were neutral about the statement and twenty one 21 (26%) out of 86 were disagreeing to the statement that no sufficient evidence is not collected from the crime scene by LEA's.

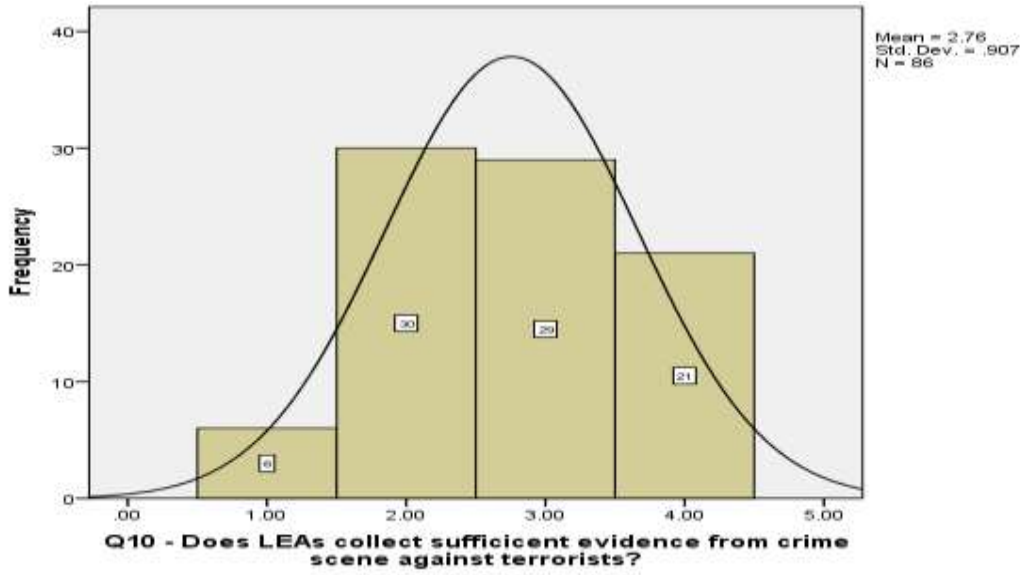

Figure 40 - Working of LEAs

Question 11. The respondents were asked about the use of digital evidence by LEAs against the terrorist in court of Law. The response is shown in the Figure - 41. Fifty nine 59 (69 %) out of 86 have agreed that yes LEAs can use digital evidence against terrorists in court of Law. Twenty 20 (21%) are neutral about the statement asked and seven 7 (9%) don't agree with the statement.

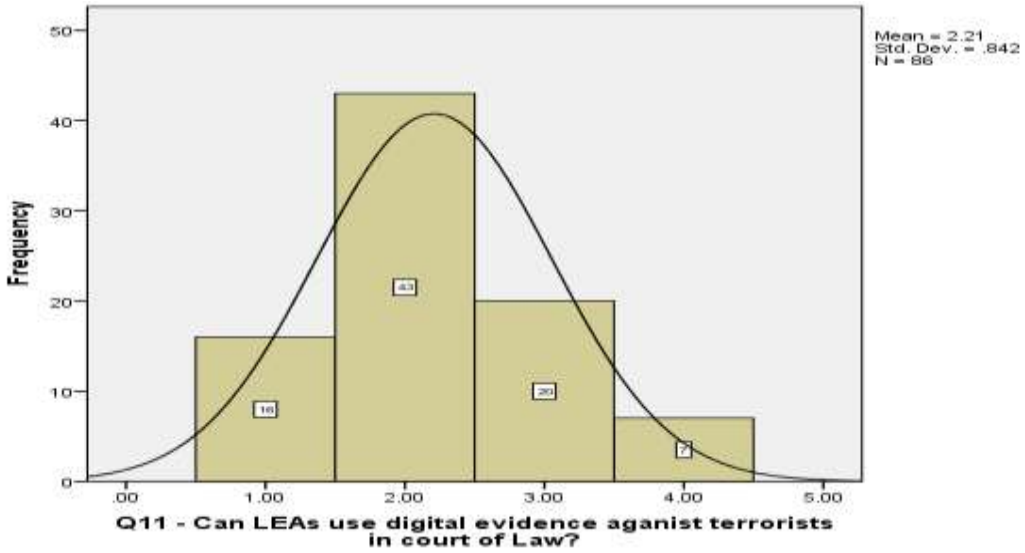

Figure 41 - Working of LEAs

Question 13. The Figure - 42 shows that majority of the respondents are disagreeing with the fact that LEAs are collecting sufficient evidence from the crime scene which can prove terrorist guilty in court of law. Some of them have no idea about the subject and some are agreeing that yes LEAs are collecting sufficient evidence from the crime scene. The respondent who are disagreeing are forty one 41 (47%) out of 86, while twenty two 22 (26%) who are agreeing and the respondents who have neutral stance, simply said they don't know are twenty three 23 (26%).

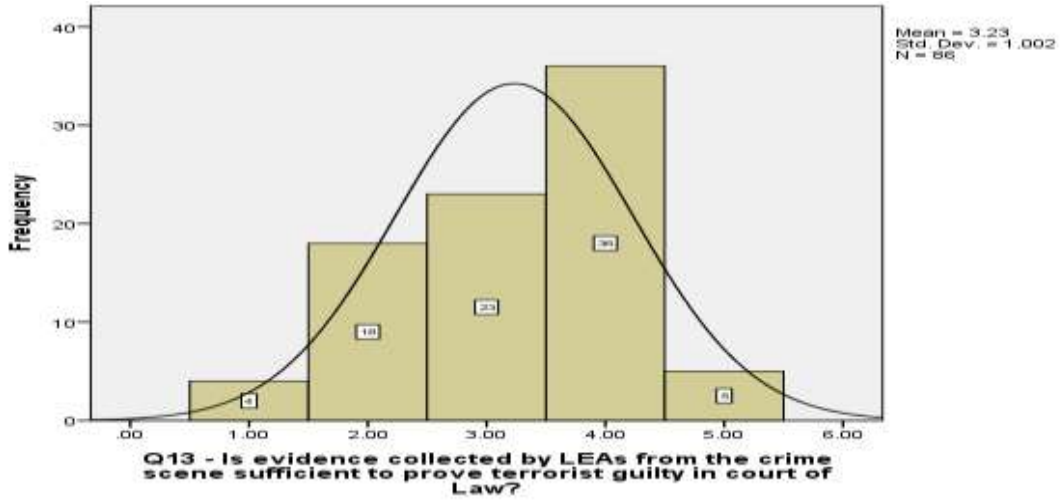

Figure 42 - Working of LEAs

Question 14. The Figure - 43 below shows the opinion of the respondents when they were asked about collection of digital evidence from the crime scene by intelligence departments while they apprehend the terrorists. Majority of the respondents who are working in the field of apprehension and collection of evidence from the crime scene are agreeing, some respondents don't know about this at all and have neutral opinion about the question asked. Forty seven 47 (55%) out of 86 have agreed that intelligence agencies do collect the digital evidence from the crime scene while apprehending the terrorists. Twenty three 23 (29%) have absolutely no idea about the question asked. Sixteen 16 (15%) out of 86 have disagreed to the question asked.

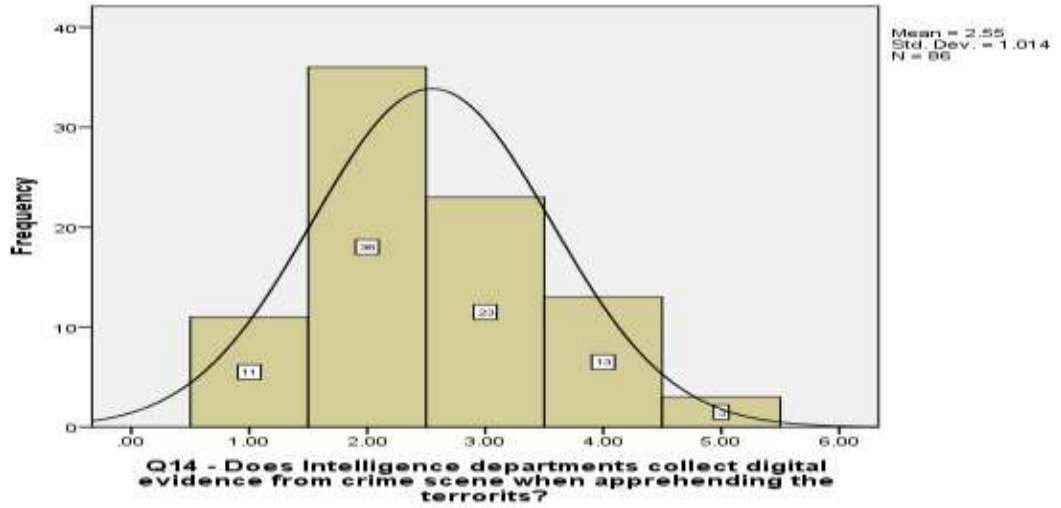

Figure 43 - Working of Intelligence Agencies

Question 15. When the respondents were asked about the information sharing of digital evidence collected from the crime scene between different LEAs, intelligence and security agencies the response achieved is shown below in the Figure - 44. Majority have disagreed to the statement asked. Some have no idea about the issue of information sharing and a quite few agreed as well that the information sharing about the digital evidence collected is present. Forty one 41 (47%) out of 86 have disagreed about the question asked, twenty five 25 (27%) out 86

have absolutely no idea as to what is being asked. And twenty 20 (24%) out of 86 are agreeing that yes information sharing about the digital evidence between different security departments is present.

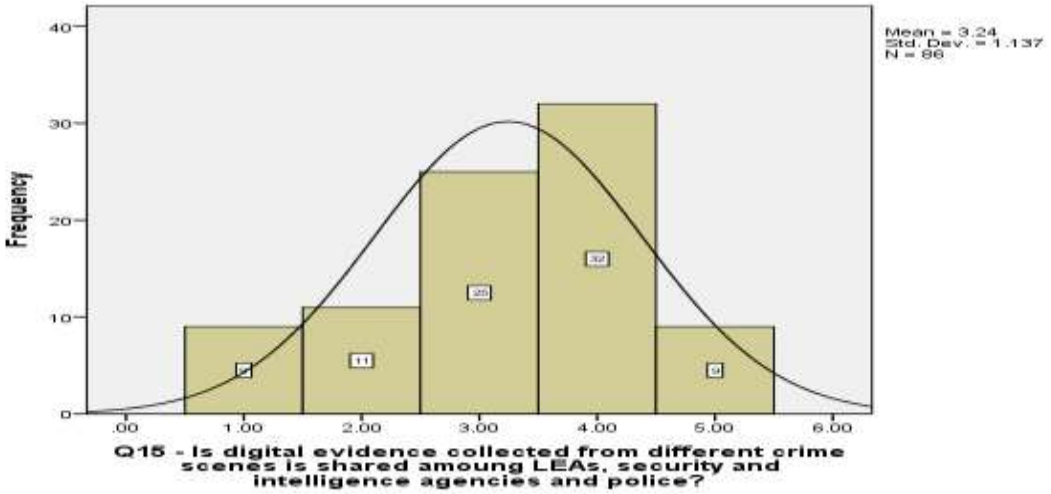

Figure 44 - Information Sharing

Question 16. The Figure - 45 below shows that out of 86 respondents 73 (90 %) have agreed that information sharing about digital evidence collected from the crime scene should be present between different LEAs, security and intelligence agenies and police. Whereas 9 (9.2%) respondents out of 86 have neutral stance towards the question asked. 4 () respodents have disagreed with the questionned asked.

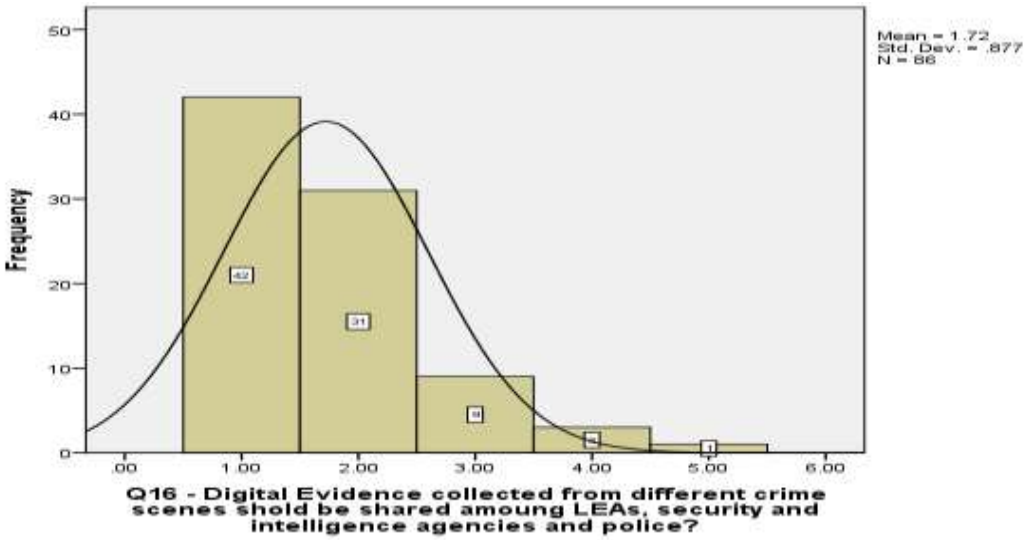

Figure 45 - Information Sharing

Question 17. The Figure - 46 shows opinion of the respondents about preserving the sanctity of the crime scene by cordoning it off, majority have agreed that it should be cordoned off in order to collect sufficient evidence from crime scene. 81 (95%) respondents out of 86 have agreed to it and 4 (3%) respondents out 65 have shown neutral approach towards it. Only 1 (1.5%) out 65 respondent has disagreed to it.

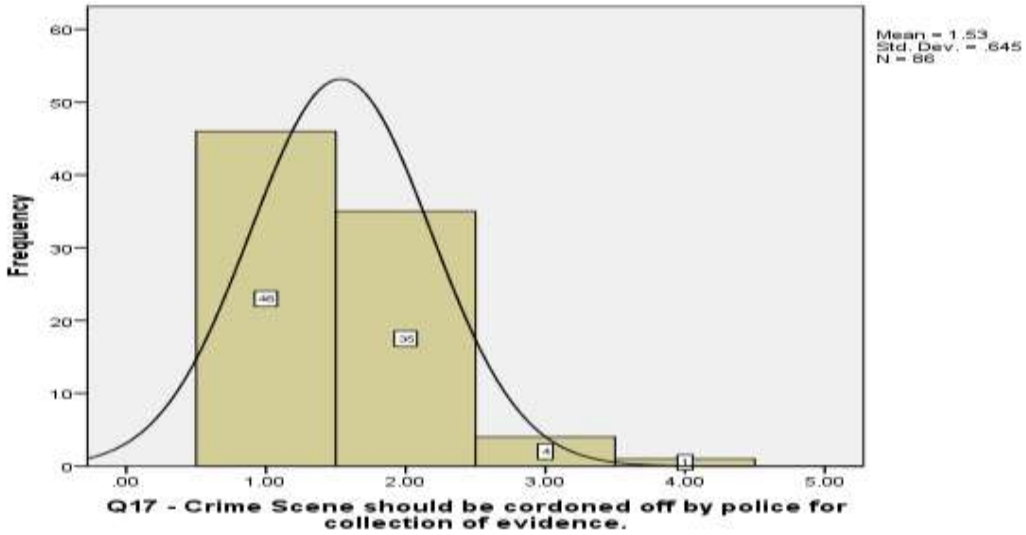

Figure 46 - Cordoning off of Crime Scene

Question 18. The Figure - 47 explains how respondents have shown their opinion about question asked that is police currently cordoning off the crime scene for the collection of the evidence. Out of 86 respondents 42 (48.8%) respondents are disagreeing with the fact that the police is cordoning off the crime scene for collection of the evidence. 30 (34.8%) respondents out of 86 are unaware of the question asked. 14 (16.27%) respondents out of 86 are agreeing that yes police is cordoning off the crime scene.

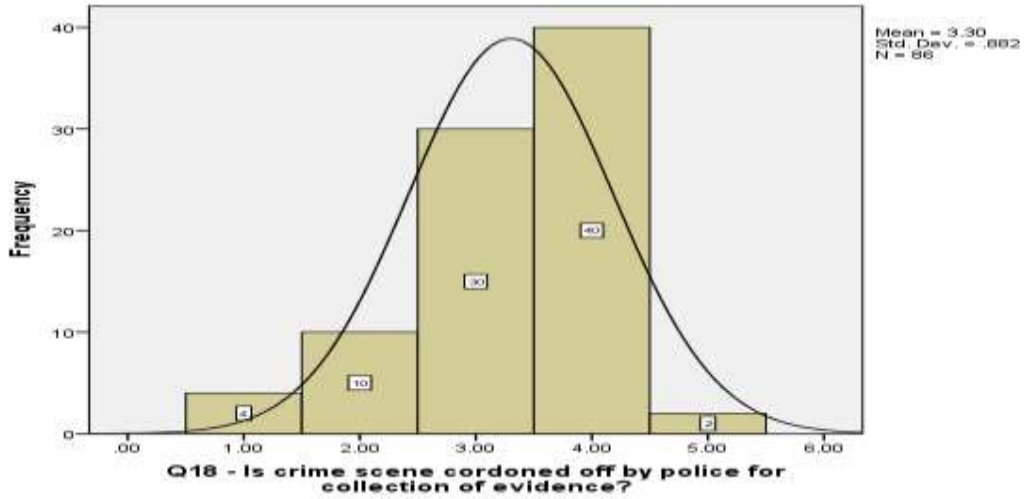

Figure 47 - Cordoning off of Crime Scene

Question 20. When respondents were asked about that it is the lack of digital evidence (biometrics) collected from the crime scene which is hampering in the process of persecution of terrorists. Majority of the respondents have agreed to it. 60 (72%) respondents out of 86 have agreed, 17 (18%) out of 86 are absolutely blank about question asked and are neutral about the opinion and 9 (9.2%) out of 86 have disagreed about it and replied that there are some other factors as well as shown in Figure – 48.

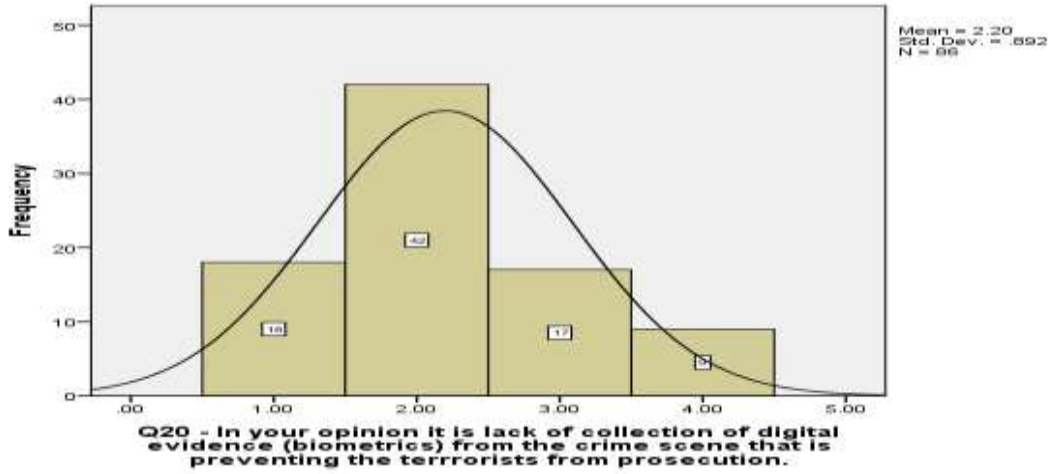

Figure 48 - Lack of Digital Evidence

Question 21. The Figure – 49 shown below explains the opinion of the respondents when they were asked that it is lack of providing digital evidence (biometrics) in courts which prevents the terrorists from being prosecuted. 54 (62.7%) out of 86 respondents are agreeing that yes it is the problem that digital evidence (biometrics) is not provided in courts which is preventing the terrorists from prosecution. 22 (25.58%) out of 86 respondents have absolutely no idea about the question asked and 10 (11.62%) out of 86 have disagreed and highlighted that it is not only the digital evidence (biometrics) which is preventing the terrorists from prosecution, there are many other factors as well.

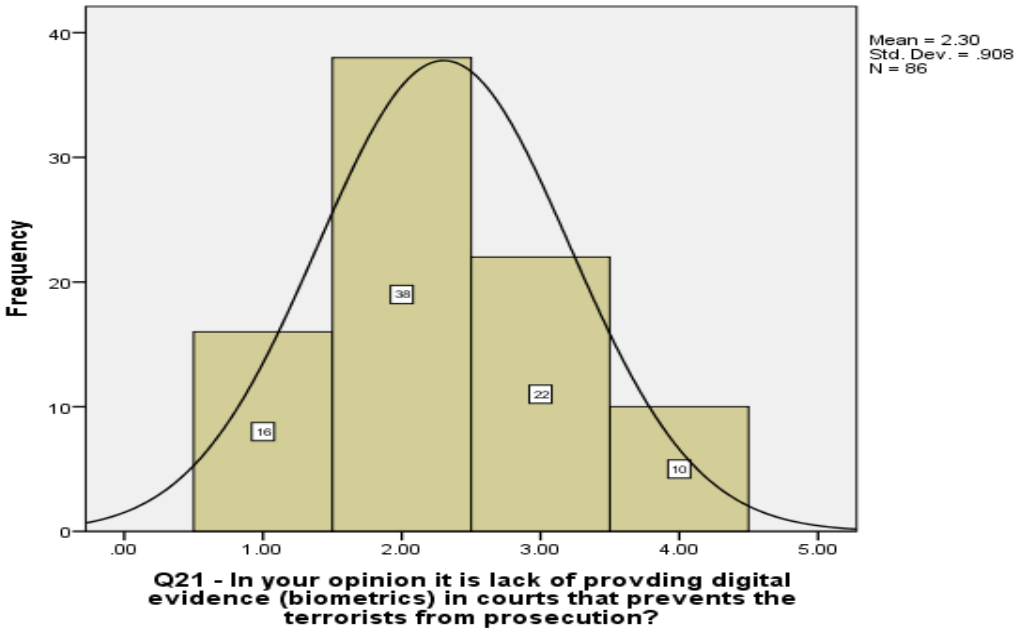

Figure 49 - Lack of Digital Evidence

3.2.2.2 Terrorist cases Investigation

Question 23.The Figure - 50 below explains the general understanding of the sample population about the term terrorism. 82 (93.84%) out of 86 respondents have agreed that they clearly know about the term terrorism. 4 (6.15%) out of 86 where not clear about the meaning of the term.

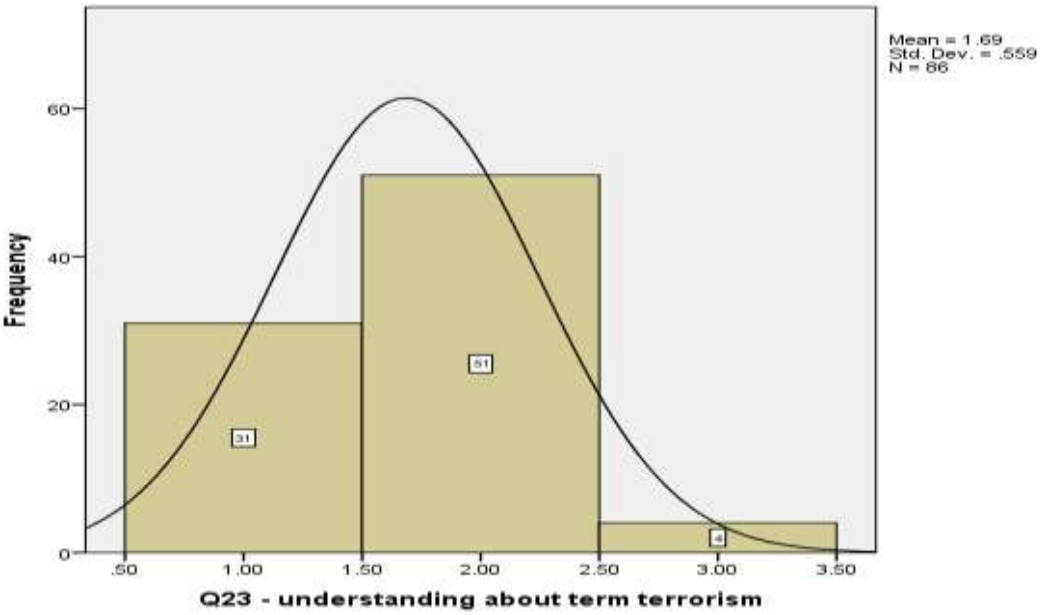

Figure 50 - Understanding about Terrorism

Question 24. The Figure - 51 below explains the general understanding of the sample population about the term counter-terrorism. 76 (90.70%) out of 86 respondents have agreed that they clearly know about the term counter-terrorism. 10 (9.23%) out of 86 where not clear about the meaning of the term.

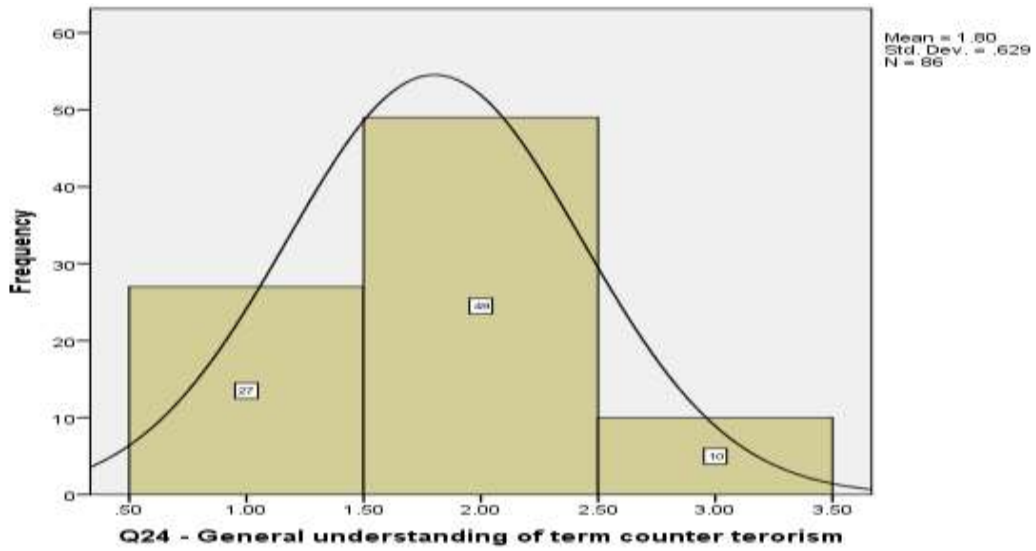

Figure 51 - Understanding of Term Counter Terrorism

Question 25. Respondents were asked that if they know about terrorist cases being run in Pakistani courts, most of them knew about it. Yet there is quite a large number of sample which has given a neutral stance about the question, they were not knowing about the terrorists cases being run in Pakistani courts. 40 (44.61%) out of 86 respondents were very clear that yes terrorist cases are being run in Pakistani courts. 29 (32.3%) out of 86 respondents were absolutely unaware of the process of terrorist cases being run in Pakistani courts. 17 (23%) out

of 86 respondents even denied that there is no such thing as terrorists cases in Pakistani courts as shown in Figure - 52.

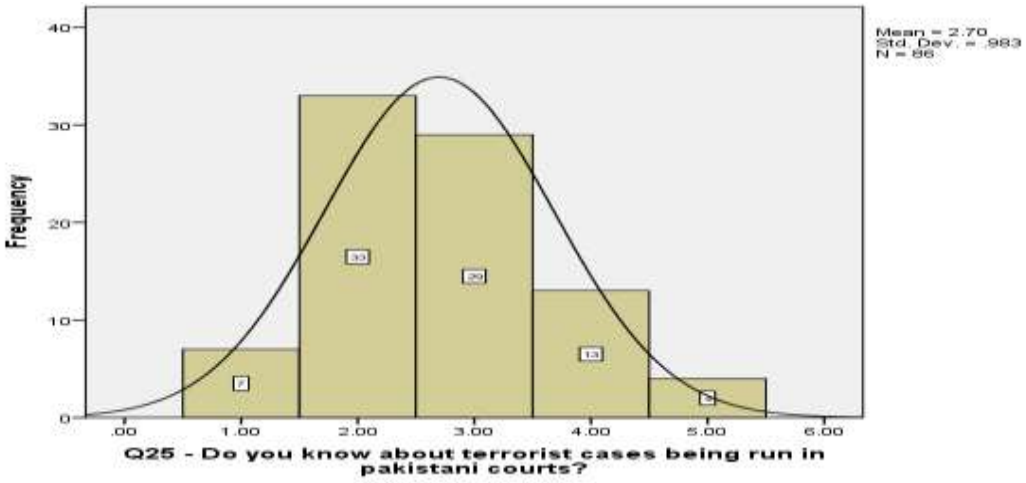

Figure 52 - Knowledge About terrorist Cassese in Pakistan

Question 26. The Figure - 53 below explain the response of the responders when they were asked about credibility of the terrorist cases being run in Pakistani courts. Majority of the people were unconfident about the question and have shown a neutral approach about it. Some have disagreed that credibility if the terrorists cases run in Pakistani courts is doubtful. Yet some have agreed that cases which are being run in Pakistani courts are credible. 34 (38.4%) out 86 were unaware of the issues and have given a neutral perception about the issue. 26 (27.6%) out of 86 have agreed that the cases of terrorist which are being run in Pakistani courts are credible, 26 (33.84%) out of 86 have disagreed about the credibility of the terrorist cases being run in Pakistani courts.

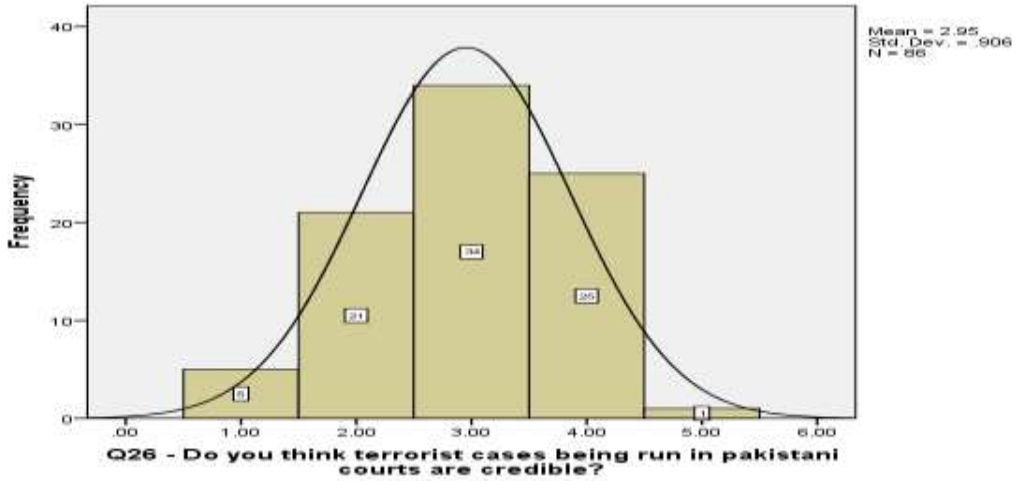

Figure 53 - Credibility of Terrorist Cases

Question 27. The Figure - 54 below shows the responder's response when they were asked about the use of digital evidence (biometrics) in terrorists cases which are currently being run in Pakistani courts. 35 (43%) out of 86 were not knowing about the statement asked. 29 (36.9%)

out of 86 have disagreed to the statement. 22 (20%) out of 86 have agreed that yes digital evidence (biometrics) is in use in Pakistani courts for terrorists cases.

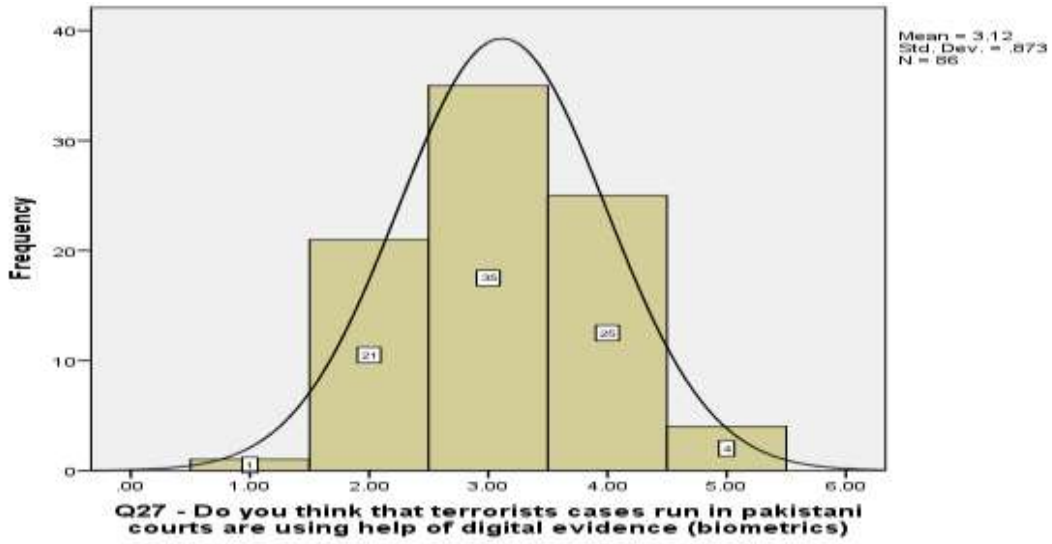

Figure 54 - Use of Digital Evidence (biometrics) in terrorist cases

Question 28. The Figure - 55 below shows the response to the statement, "Does digital evidence (biometrics) helps in investigation of terrorists against their crimes in court of Law?" 67 (80%) out of 86 responders have agreed that use of digital evidence (biometrics) will help in investigation of terrorists against their crimes in court of law. 13 (10%) out of 86 responders were neutral about the statement asked. 6 (9.2%) out of 86 respondents have disagreed with the statement.

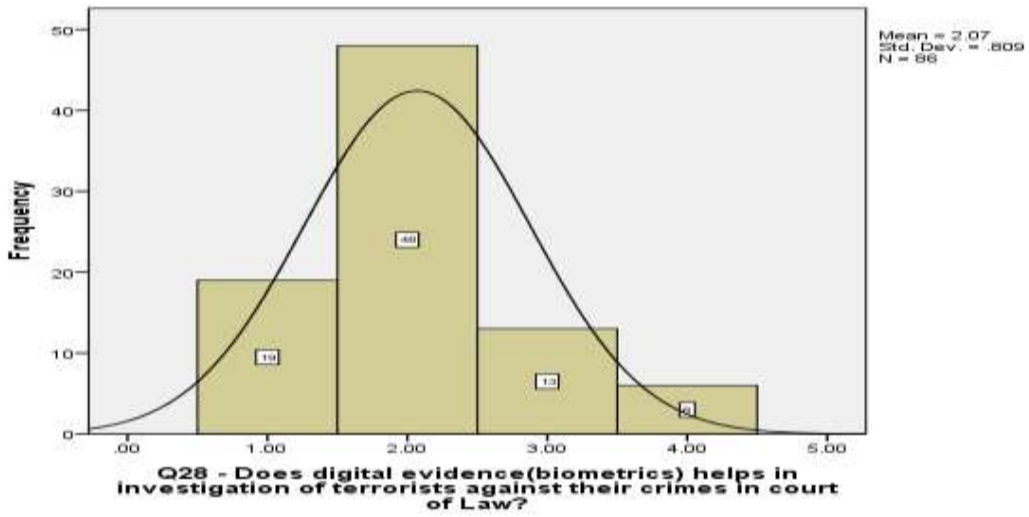

Figure 55 - Help of Digital Evidence (biometrics) in Terrorist Investigation

Question 29. The Figure - 56 below shows the response of the responders when they were asked this statement, "Do you think that currently investigation of terrorist's cases in Pakistan is successful?" Mostly have disagreed to the statement asked. Some have shown neutral approach towards the statement asked and very few have agreed to it. 47 (55%) out of 86 have

disagreed with the statement. 30 (36.9%) out of 86 have shown neutral stance towards the statement asked. 9 (7.6%) out of 86 have agreed with the statement.

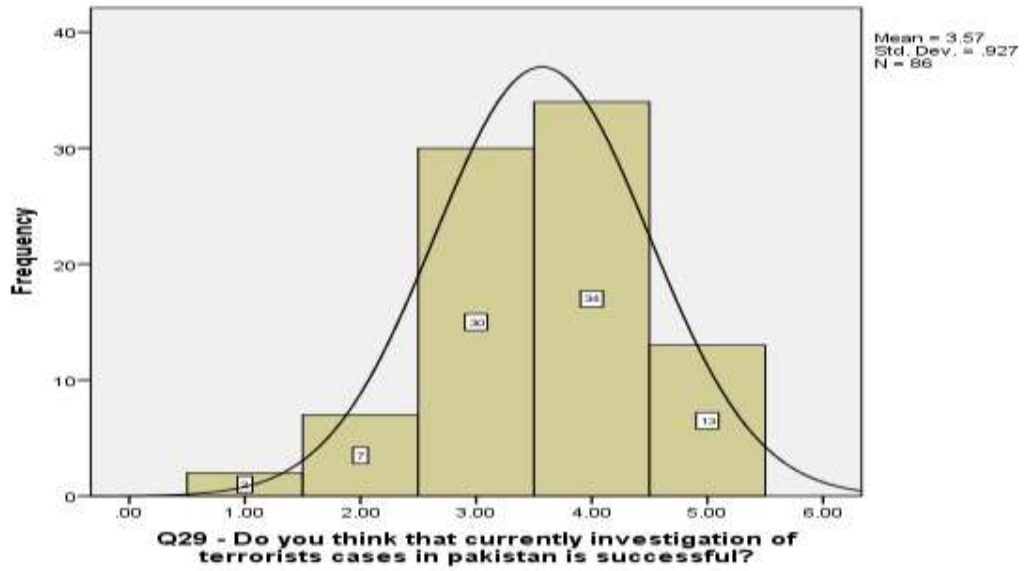

Figure 56 - Investigation of Terrorist cases is Successful

Question 30. The Figure – 57 below shows the respondent's response to the question asked which is, do you think that currently the investigation of terrorists cases in Pakistan is not successful. 59 (66%) out of 86 have agreed to the question asked and 22 (26.15%) out of 86 have shown neutral stance towards the issue whereas 5 (7.6%) out of 86 have disagreed with the question asked.

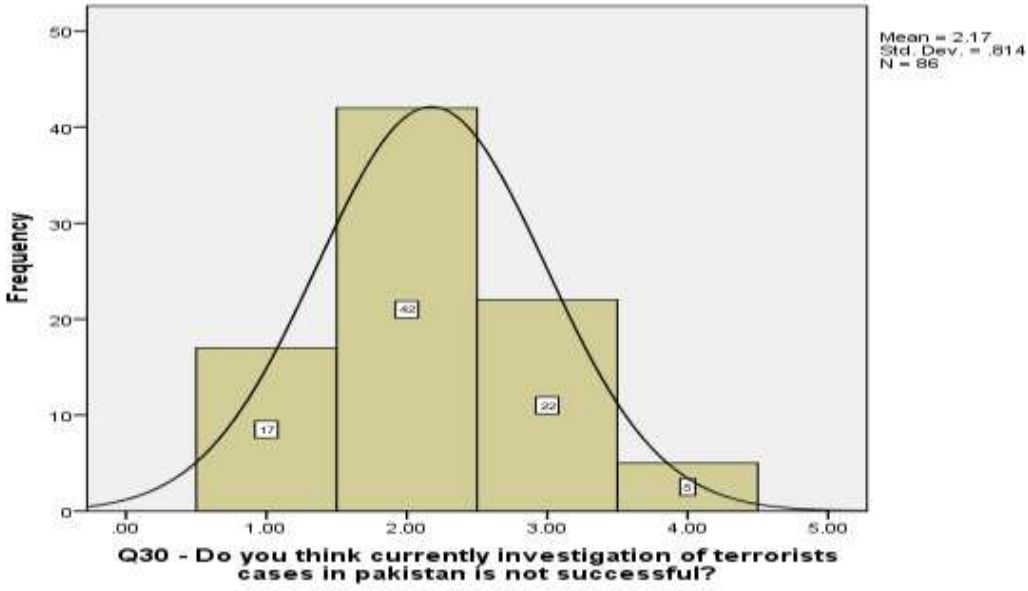

Figure 57 - Investigation of Terrorist cases is not successful

Question 31. The Figure -58 below shows the responder's response about the question asked which is, "Do you think that investigation can be improved against terrorists by using digital evidence (biometrics)?" 78 (90.69%) out of 86 have agreed to the question asked. 7 (8.13%)

out of 86 respondent shave absolutely no idea about the question asked. 1(1.1%) out of 86 has disagreed with the question.

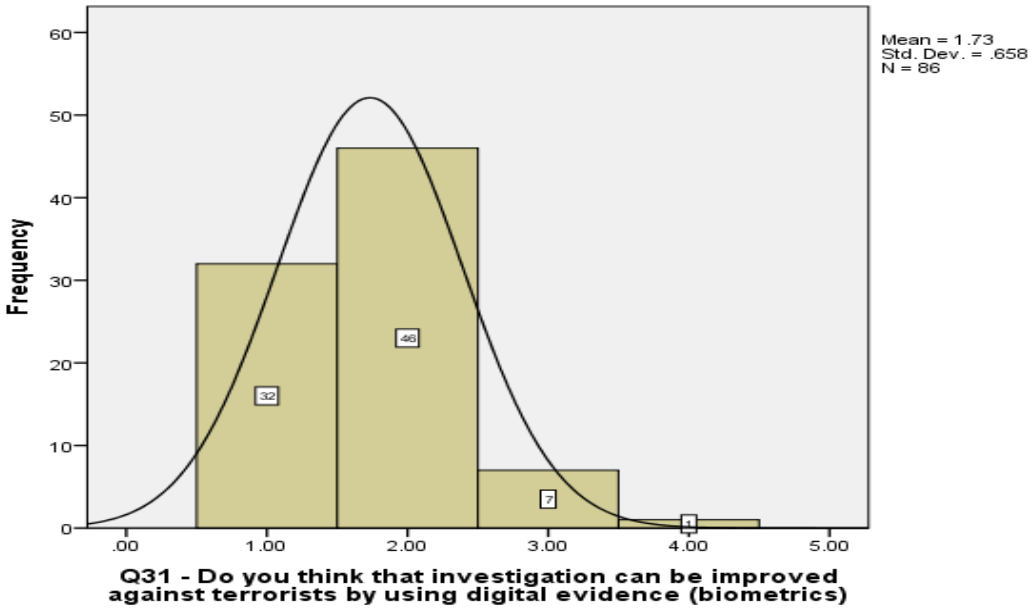

Figure 58 - Improvement in Investigation by using digital evidence biometrics

Question 33. The Figure - 59 below shows the responses of the responders about the question asked. 67 (76.9%) out of 86 have agreed to the question asked, that the delay in the trials of terrorist cases in Pakistan is because of lack of any suitable Law. 19 (20%) out of 86 are unaware of this and have given a neutral approach to the question's response. 3 (3%) out of 86 have disagreed with question asked.

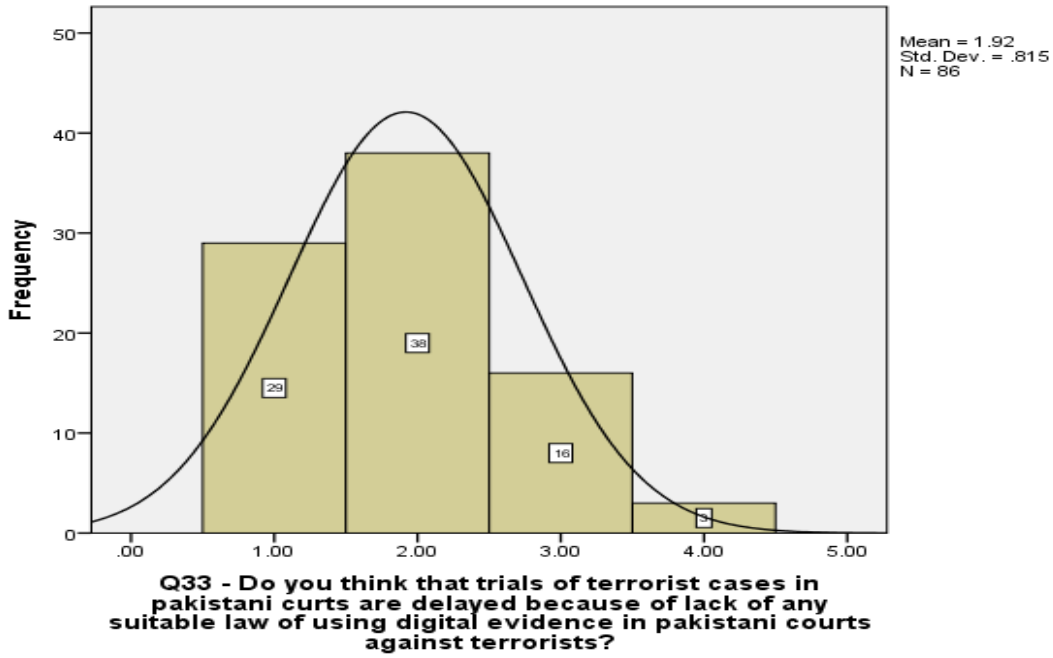

Figure 59 - Lack of Digital Evidence in Trials

Question 34. When respondents were asked about the trial of terrorist cases in Pakistani courts are delayed because of poor management of the chain of custody of the evidence, Figure -60 shows that, 69 (86%) out of 86 have agreed to the question asked. 12 (12.3%) out of 86 have absolutely no idea as to what is happening in the Pakistani courts. Only 2 (1.5%) out 86 has disagreed to it.

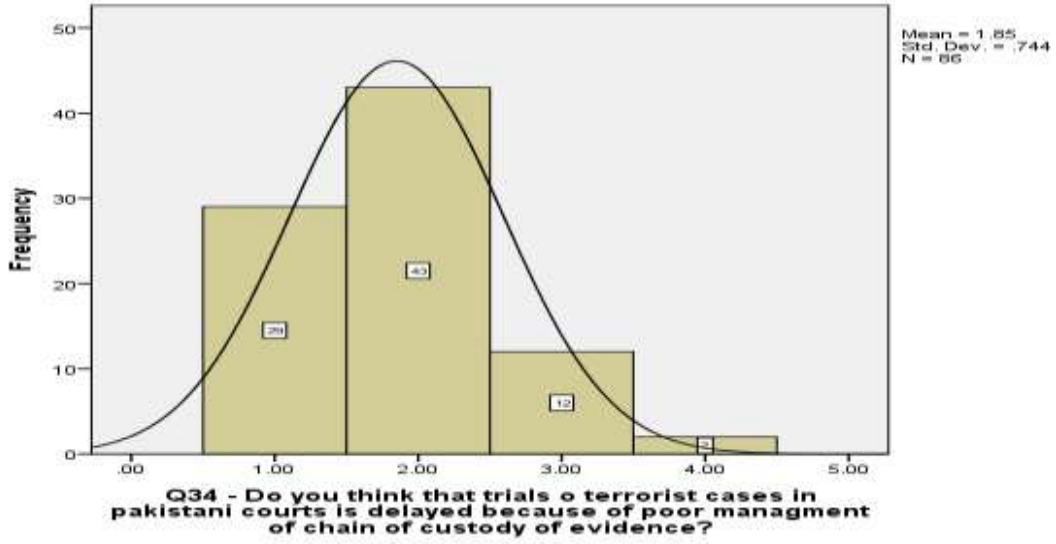

Figure 60 - Poor Management of Chain of custody of Evidence

Question 35. Respondent's response was noted against the question asked. "Do you think investigation of terrorist cases in Pakistan is delayed because of contamination of the crime scene?" 67 (78%) out of 86 have agreed to the question asked. 14 (13.8%) out of 86 have absolutely no idea about the question and they have shown a neutral stance towards It. 5 (6.15%) out of 86 have disagreed to the question asked as shown in Figure - 61.

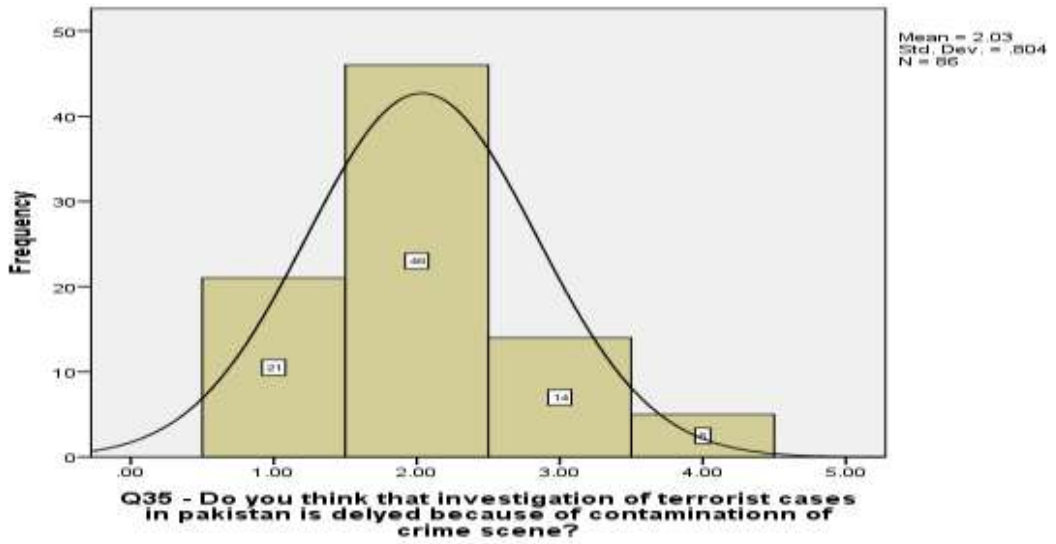

Figure 61 - Contamination of Crime Scene

3.3 Interview Findings

3.3.1 Brief Summary

Interviews were conducted in order to answer research question three (3). The third step in answering the research question was to know in person what all are the problems and legal issues associated with the use of biometrics as digitized evidence by interviewing individuals who are actively performing the duties of investigating and apprehending the terrorists/criminal.. In this regard, interviews have been conducted on only those individuals who are involved in the process of apprehension and investigation. Unstructured interviews have been conducted and the empirical findings are analyzed in tool NVIVO. In NVIVO systematically open coding technique is used to identify all emerging and relevant themes. These themes are present in form of nodes in NVIVO. After that axial coding is carried out to further categorize the themes and defined the relationship between different themes. After doing so selective coding technique is used. After selective coding, all the themes and defined relationships which are identifying the problem areas and legal issues being faced by the persons have been extracted out in form of models, which will answer research question three. These models are showing the main problems and legal issues currently being faced.

3.3.2 Model 1

The Figure – 62 shows the working of the courts. Two types of courts are related to the topic under discussion civil courts are the courts which were earlier hearing the terrorist cases. The working of civil courts was not very effective so they were relinquished from their duties. Antiterrorist courts were made to solve the terrorist cases in Pakistan. Now both the courts are working separately. They are meant to work separately and follow their independent rules and regulations. But in reality civil courts and antiterrorist courts are having symmetrical relation between them. This is because the judges and lawyers who are conducting the trials are working in both civil courts and anti-terrorists courts. They are not specific to courts.

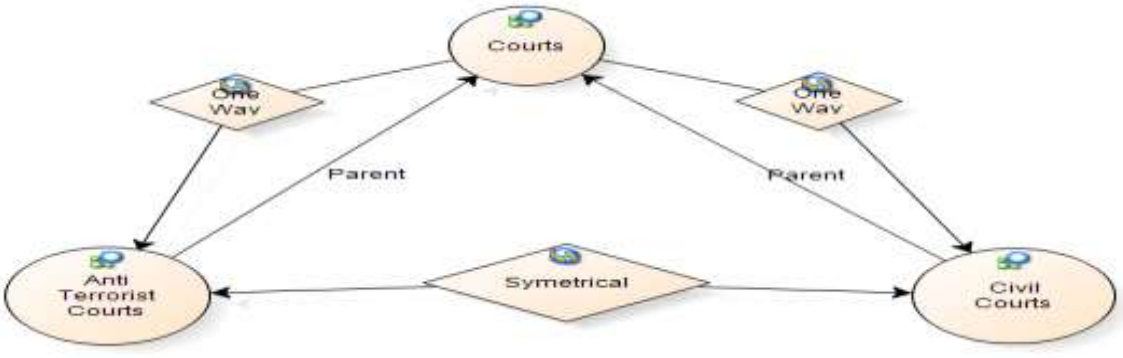

Figure 62 - Working of Civil and Anti-terrorist Courts

3.3.3 Model 2

The Figure - 64 shows the problems which are currently faced by the Anti- terrorist courts. When interviewed various lawyers and police men, different associated and symmetrical problems are highlighted. Political influence, financial aspects involved in the process of trials, threats to different lawyer and police men by terrorists are main problems. Legal issue like ban of death sentence, collection of evidence which is linked with the crime scene will be explained in figure 63 and lack of witness protection program are also hurdle in the process.

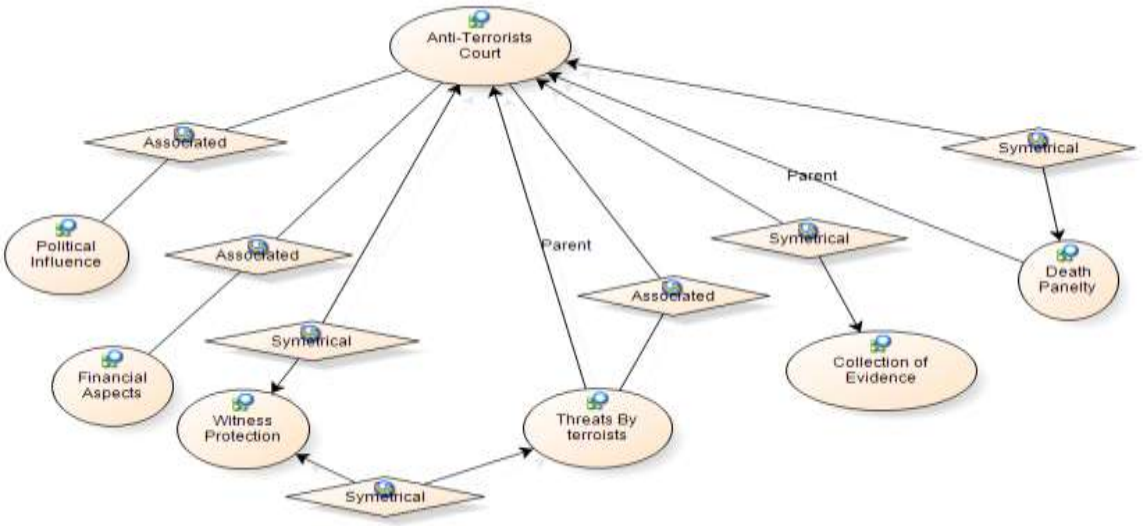

Figure 63 - Problems Associated with working of Anti-terrorist Courts

3.3.4 Model 3

This Figure – 64 explains that lack of witness protection program is associated to the working of the anti-terrorist courts (ATC). It is the absence of the Witness protection program that is causing legal problems in the working of the ATC. Lack of Witness protection program is exploited in advantage to terrorist which is there one of the tactics.

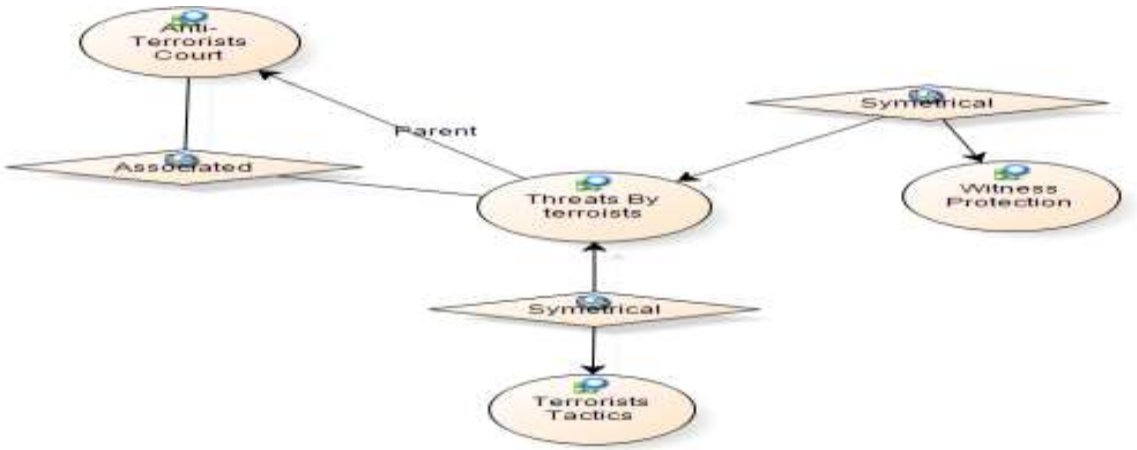

Figure 64 - Threats by terrorists is tactics used

3.3.5 Model4

The Figure - 65 shows the problems which are present at the crime scene. Two processes which are related to crime scene i.e. collection of evidence and contamination of crime scene are symmetrical with each other. Meaning thereby if the crime scene is contaminated the process of collection of evidence is hampered and is incomplete which becomes the legal issues at later stages of the trial.

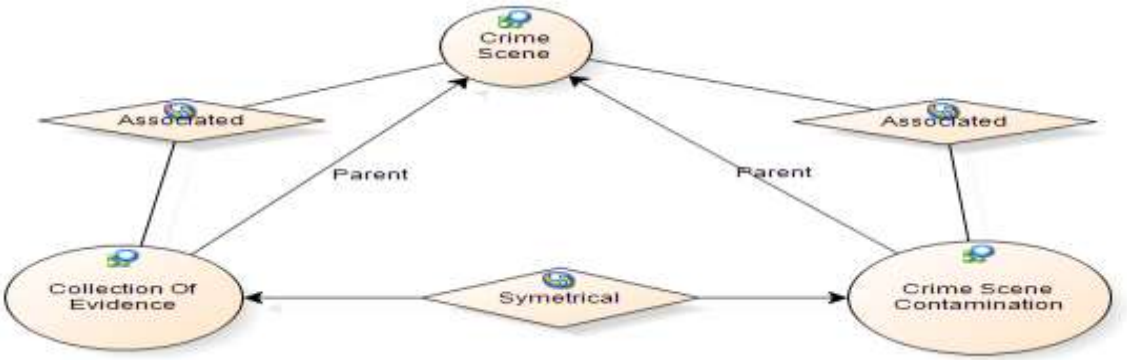

Figure 65 - Problems Associated with the Crime scene

3.3.6 Model5

The Figure – 66 explains the problems and legal issues linked with the Crime scene Contamination. Problems like Provision of the emergency services, general public gathering at the crime scene, self-respect of the bosses who visits the crime scene if any, assertiveness of the police at the crime scene and conflict of interest of different agencies who comes to the crime scene are symmetrical problems. Meaning that they are linked and directly affect the crime scene sanctity. Problems like understanding of the sensitivity of the issue, awareness of the terrorism and its implications at crime scene, political influence are associated with the crime scene contamination.

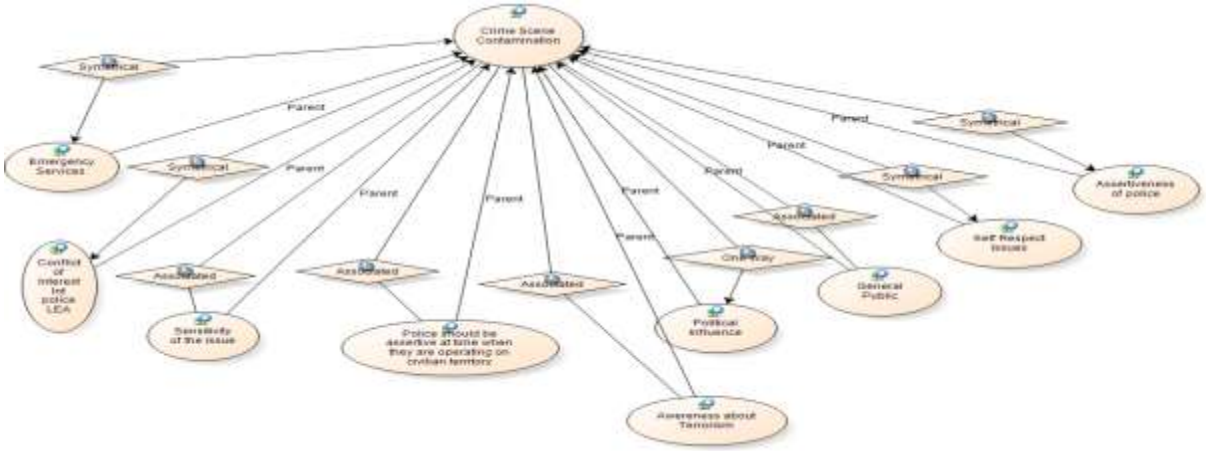

Figure 66 - Problems associated with Crime scene contamination

3.3.7 Model6

The Figure - 67 shows that the collection of evidence has major problems associated with it. Collection of evidence is directly linked to the training of the individuals who are collecting the evidence. On this issue unfortunately there is acute lack of training imparted to the police personel who will have to perform the duty of collection of evidence on priority. Lack of equipment and resources in form of material as well as financial are not available to the departments concerned. Also some intangible tangible problems highlighted in the interviews are lack of sincerity with the work and shurk work.

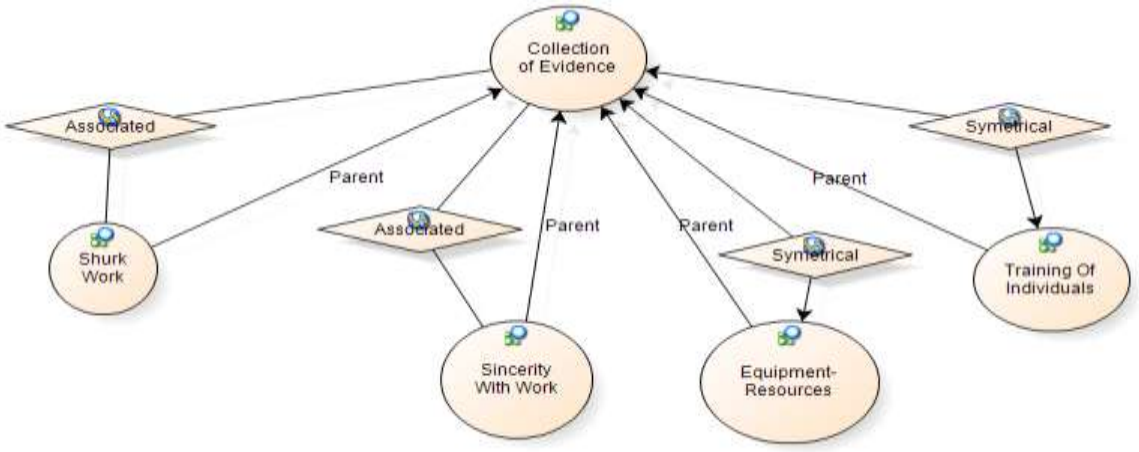

Figure 67 - Problems being faced during the collection of evidence

3.3.8 Model7

The Figure - 68 shows that the collection of evidence form part of legal issues like after the processing of evidence and chain of custody of evidence.

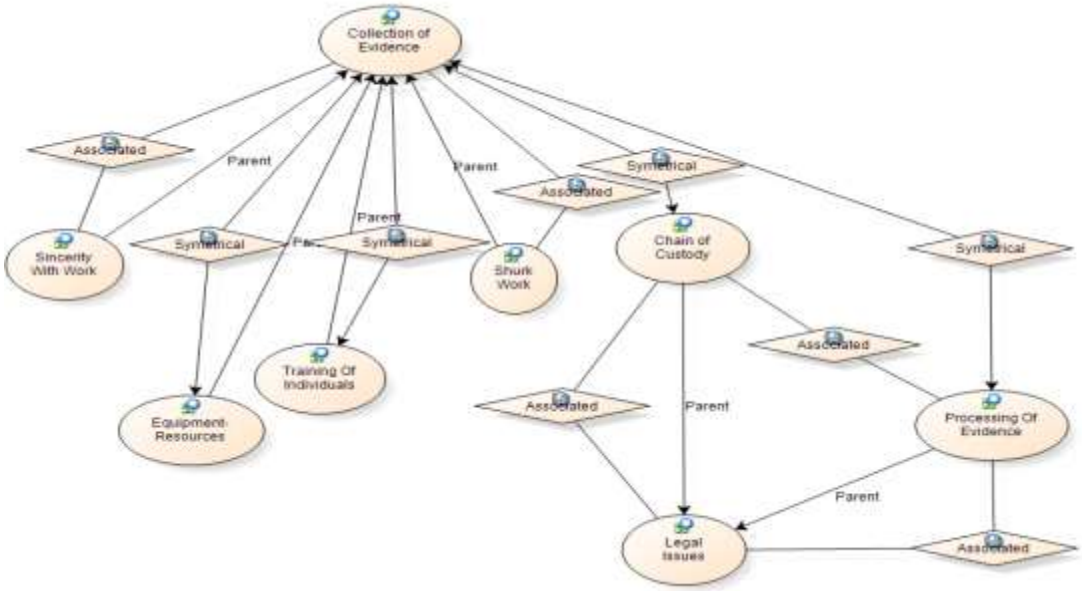

Figure 68 - Legal Issues linked with the collection of evidence

3.3.9 Model8

The Figure - 69 explains numerous problems associated with the legal issues involved in the trials of terrorists. The symmetrical issues like ban on death penalty and crime scene which have been explained earlier, are hampering the successful prosecution of the terrorists. Lack of processing of evidence, missing links in the paper work about chain of custody of evidence, third degree investigation merely because of the lack of evidence, lack of witness protection program are associated problems which must be addressed in order to have successful investigation and further trial of terrorists. Mistrust between different agencies, financial aspects in the legal working of the entire hierarchical procedure and lack of any central storage of data are also hampering the legal working. Also during the interviews presence of no suitable law is highlighted by many interviewees as the current law does not support the specific cases of the terrorists apprehended and investigated. Also evidence collected in form of biometrics against the terrorists/criminal is not accepted in the court of Law, there is requirement for the amendment of legal process for these terrorists. This model is linked with model 1 as well. The judges and lawyers who are fighting the cases of terrorists must be separated from the civil courts.

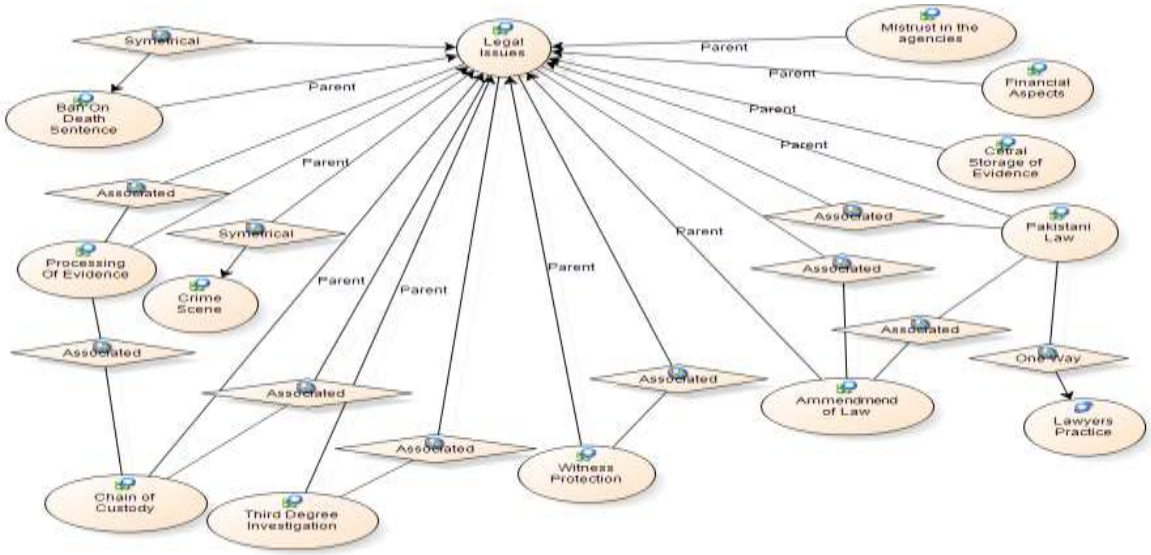

Figure 69 - Legal Issues involved in Investigation of terrorists

3.3.10 Model9

In Figure - 70 the working and important factors which are influencing the terrorist cases investigation are discussed. The investigation which are carried out are third degree. Chain of custody of evidence problem is associated with the investigation as the persons apprehended by police are taken by the intelligence agencies. Same crime scene but different departments present for the collection of evidence. Chain of custody is difficult to maintain. Involvement of Security forces. Use of biometrics as digitized evidence can be very helpful during the

investigation and apprehension of the terrorists. Which in most of the cases is not present, collected and contaminated. Threats given to investigation officers. Political influence asserted during the investigation of the terrorist. Conflict of interest between different agencies, LEAs and police department in apprehending and investigating terrorists. Problems at crime scene and collection of evidence are also associated with terrorist cases investigation.

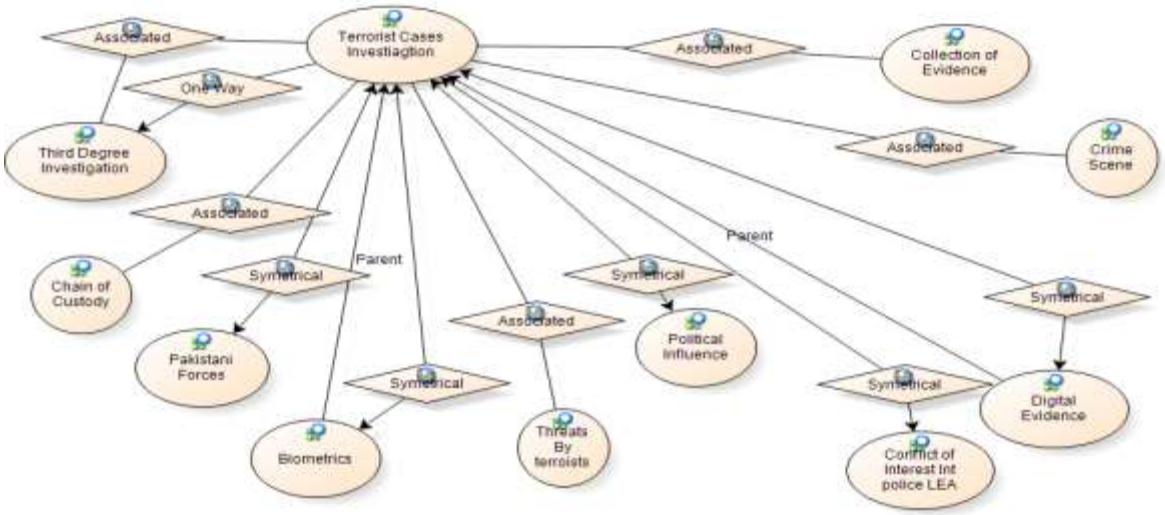

Figure 70 - Problems in terrorist's cases investigation

3.3.11 Model10

This model explains the convergent effort by Pakistan security force working to counter terrorism. The Figure - 71 explains that the army, LEAs police and intelligence agencies are working independently. During the interviews this theme originated that every department is working separately in its own regime while addressing to this national menace, the effort exerted must be convergent. However police and intelligence departments have something in common which is also frequently observed that the investigation officer is common.

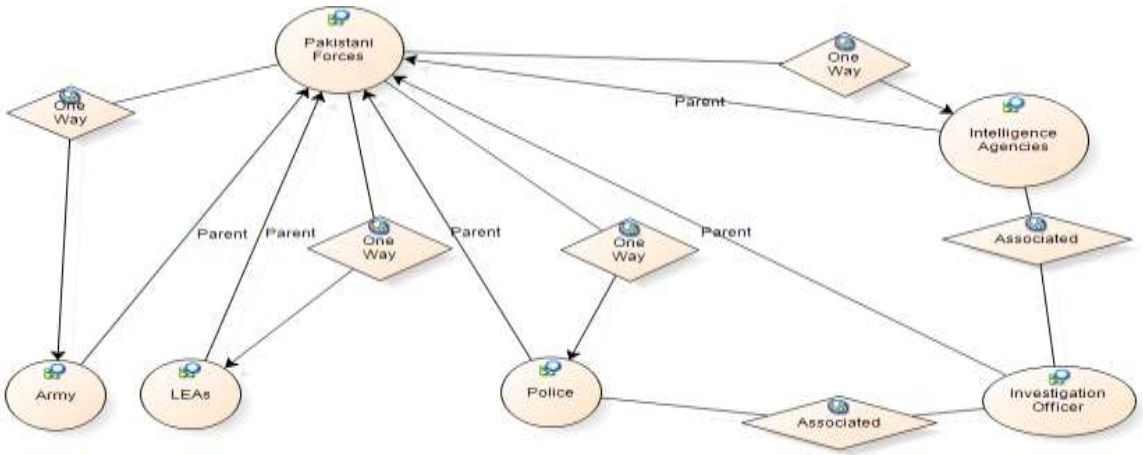

Figure 71 - Pakistani Security forces working

3.3.12 Model 11

The Figure - 72 below shows the linkage of the investigation officer with the crime scene. The importance of linkage is off very grave nature. Right completion of this step will lead to completion of legal formalities, which will further lead to successful investigation of the terrorists.

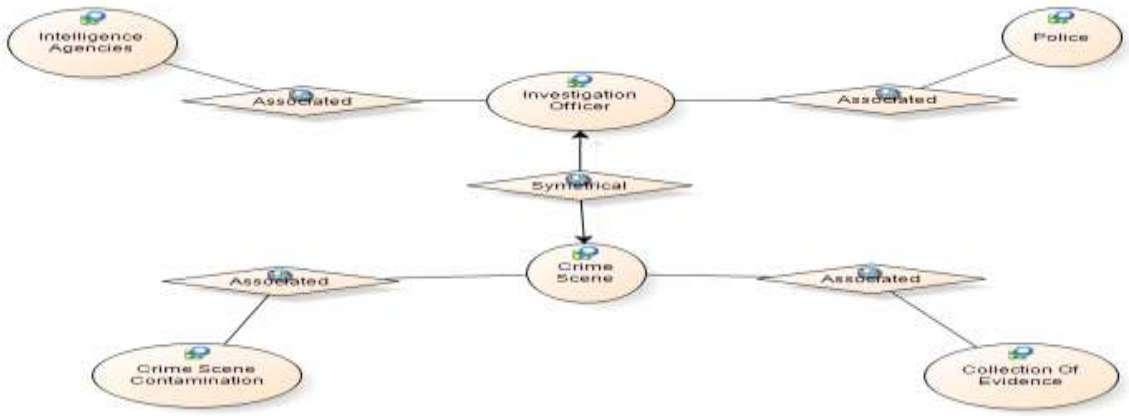

Figure 72 - Linkage of IO and Crime scene

3.3.13 Model 12

The model below explains that how the lack of any suitable law is related to terrorist cases investigation. As per the interviews, Figure – 73 showing a model which is clearly showing that how need for amendment in law is linked with the problems in the terrorist cases investigation, legal issued being faced by different departments and Investigation officers (IO), ban on death sentence, use of biometrics as digitized evidence against the terrorists.

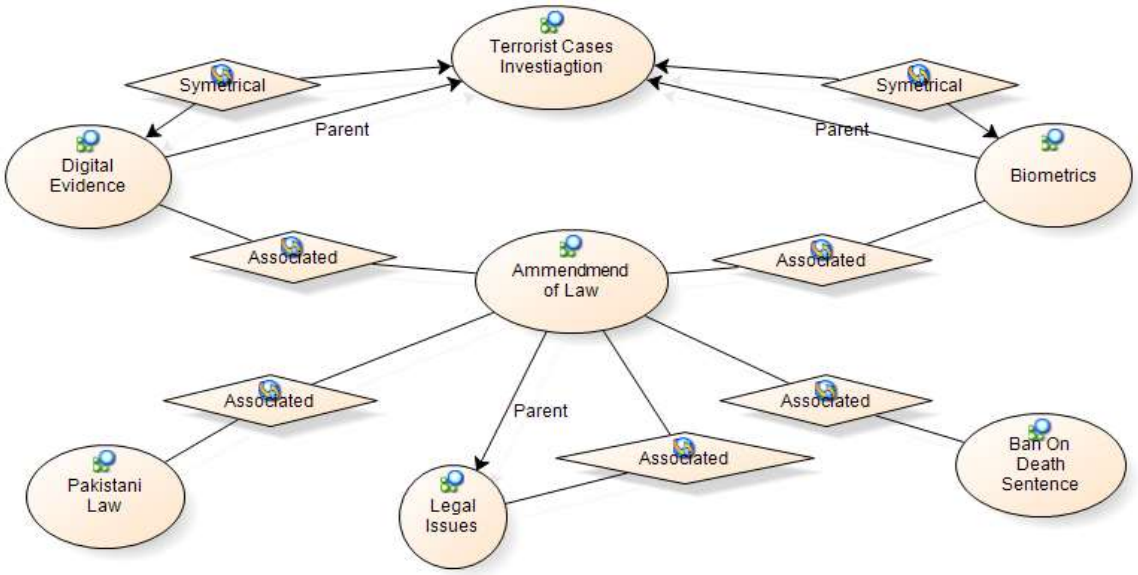

Figure 73 - Need for amendment in Law

3.3.14 Model 13

The Figure - 74 shows that the ban on death sentence is symmetrical to the legal issue. Which is also causing hurdle in the process invoke?

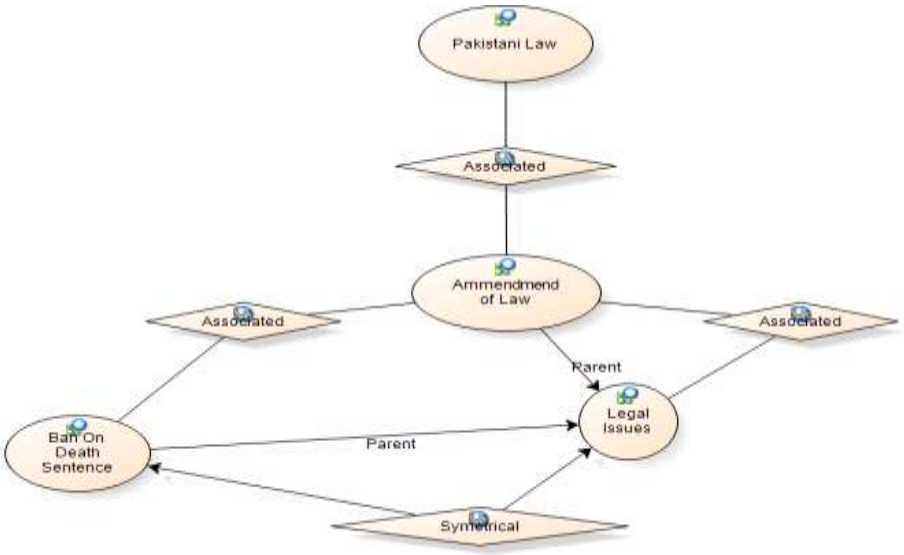

Figure 74 - Ban on Death is symmetrical to Legal Issues

4 CHAPTER FOUR: RESULTS AND ANALYSIS

This part constitutes the analysis of both the quantitative and qualitative findings. The analysis is drawn as per the research questions. Firstly the quantitative findings will be analyzed to answer the research questions one, two and a part of research question three. Secondly the qualitative findings will be analyzed to answer the third research question. In qualitative part the main factors and legal issues which are being highlighted from the interviews will analyzed.

4.1 Quantitative analysis (As per research Question)

As the questionnaire main aim was to analyze the people's perception i.e. Intelligence departments, security forces, LEAs personals, policemen, lawyers and general public about the use of biometric technology as digitized evidence during the investigation process. That's why the questions are classified and grouped into two matrices i.e. Digital Evidence (Biometrics) and Terrorist Investigation as shown in Table 1. The questionnaire has two types of questions scaling question on a likert scale and at the last one qualitative questions asking about, to highlight factors other than discussed in the questionnaire.

S/N	Criteria	Questions
1	Digital Evidence (Biometrics)	1-22
2	Investigation of Terrorists	23-37
3	Qualitative Question	38

Table 6 - Showing the question relation

4.1.1 Digital Evidence (Biometrics)

Questionnaire's question from 1 to 22 had the purpose to see and identify the people's opinion when it comes to use of biometric technology as digitized evidence.

Question 1, 2 and 3 were asked to know about the people understanding about the term biometrics. Most of the respondents were adequately conversant with these terms and were completely aware of that the biometric technology can be used as digitized evidence.

Question 4 and 5 were asked to ascertain the use of biometric technology as digitized evidence to prove terrorists guilty in court of law. Mostly the respondents were off the opinion that yes biometric technology can be used as digitized evidence in court of law to prove terrorist guilty in court of law.

Question 7 was asked to know the actual state of what is happening in the field, mostly the respondents from the police were also agreeing that sufficient evidence is not collected from the crime scene. Respondents from the general public were generally unaware of what is happening at crime scene with regards to the collection of the evidence. Also the lawyer agreed that sufficient evidence is not collected from crime scene against terrorists as they face difficulties during the trials in courts.

Question 8 was asked to get an insight of the working of police. Police does uses the digital evidence against the criminals but when it comes to the terrorists cases the police is reluctant. Majority of the respondents didn't agreed that police uses digital evidence against terrorists in court of law. Also most of the respondents have no idea about the working of the police against the terrorists. Some respondents have agreed that police uses digital evidence against terrorists in court of law.

Question 12 was asked to differentiate that weather the evidence collected from the crime is sufficient or just a formality. As per the results the evidence collected from the crime scene is not sufficient which can be helpful in proving terrorist guilty in court of law. Mostly the respondents did not agree with the statement. Some respondents were unaware of the question asked hardly few have agreed that sufficient evidence is collected from the crime scene to be incorporated into the trial system against terrorists.

Question 9 was asked to see how the respondents have responded when asked about collection of evidence from the crime scene by LEA's. Mostly respondents have agreed that yes they collect digital evidence while apprehending the terrorists from crime scene. Some have them are unaware of the working of the LEAs. Very few have disagreed with the question asked and referred that LEAs are not collecting evidence while apprehending the terrorists from the crime scene.

Question 10 was asked to differentiate that weather the evidence collected by LEAs from the crime is sufficient or just a formality. Even the LEA personel are not knowing about the collection of evidence from the crime scene. Equal proportion of the respondents have agreed that yes they do collect and quite a few disagreed as well.

Question 11 was asked from the respondents to know about their perception about the use of evidence collected by LEA against terrorist in court of Law. Majority has agreed that yes they can use evidence collected from the crime scene against terrorist in court of law. Very few have disagreed with the question asked. Some of the respondents were unaware that LEA can use digital evidence in court of Law against terrorists.

Question 13 asked is to know about the evidence so collected by LEA from the crime scene is sufficient or not. Majority has disagreed with it, saying that the evidence collected is not sufficient to prove terrorist guilty in court of law. Some have agreed that yes the evidence collected by LEA is sufficient to prove terrorist guilty in court of Law.

Question 14 was asked to know the working efficiency of the intelligence agencies. Question asked was responded by the respondents that intelligence agencies collect evidence while apprehending the terrorists. Very few have disagreed with the statement and quite a few don't know about the question asked.

Question 15 was asked to highlight the factors which can contribute positively towards successful use of the evidence collected by different department against these terrorists. Question asked was known in reality about the sharing of digital evidence collected from the crime scene. Very few have agreed that information is being shared between different departments. Some respondents are unaware of the question asked.

Question 16 was asked to get the opinion of the respondents about the possible prospects of information sharing of digital evidence. Mostly the respondents have agreed that information sharing about digital evidence must be present between different departments. This opinion was a unanimous approach of all the respondents that information about the evidence collected must be shared between departments for convergent effort against these terrorists. Very few have some unawareness about the question asked.

Question 17 was asked to identify another factor which can contribute towards the evidence collection from the crime scene. The question asked was to know people's perception that crime scene should be cordoned off before the collection of the evidence. Almost everybody agreed that for sufficient collection of the evidence from the crime scene it is important to cordon off the crime scene.

Question 18 was reciprocal of the question 17, it is asked to know that in reality the crime scene is cordoned off or not for the collection of evidence by police. It is quite clear from the response that the crime scene is not cordoned off for the collection of the evidence by police. That is why there is no sufficient evidence against these terrorists, to prove them guilty in court of law. Same quite a few people are unaware of question asked.

Question 20 clearly shows one of the important factor which is hampering the process of persecution of terrorists, the question asked is, and it is lack of collection of digital evidence (biometrics) from the crime scene that is preventing the terrorist from the prosecution. The

response clearly showed that almost everybody agreed that it is lack of collection of digitized biometric evidence collected from the crime scene that is preventing the terrorists from persecution. A few respondents were disagreeing with the statement.

Question 21 was asked to know that if collected evidence is currently being given or produced in court of law against these terrorists, the response clearly shows that it is not being produced in court of law. Most of the respondents agreed that yes it is the lack of producing the collected evidence in court of law which prevents the terrorists from prosecution. There are some respondents how have no idea about the question asked. However some respondents have said that there are other factors which are also hampering the prosecution of the terrorists, lack of producing digital evidence (biometrics) in court of law is the most important of all.

4.1.2 Terrorist Cases Investigation

Questionnaire's question from 22 to 37 had the purpose to see and identify the people's opinion when it comes to use of biometrics as digitized evidence in terrorist's cases investigations.

Question 23 & 24 have been asked to know the peoples general understanding of the terminologies terrorism and counter terrorism. The responses shows that mostly the meanings of the terms is adequately understood by the people concerned in the field. Very few are those who don't know about the terminologies asked.

Question 25 shows the responses when asked about the knowledge of terrorist's cases being run in Pakistani courts. Quite a few people were aware of the fact that the terrorist cases are being run in Pakistani courts. Majority are unaware of this information. These responses are taken from the people who are apprehending and investigating terrorists on daily basis.

Question 26 shows the response of the people when asked about the credibility if the terrorist cases which are currently being run in Pakistani courts. Mostly the respondents are unaware of the fact that terrorist cases are being run in Pakistani courts. Majority have disagreed to the statement asked. And some have agreed as well.

Question 27 aims at identifying the ground reality about the use of biometric technology as digitized evidence during the terrorist's cases in Pakistani courts. The responses clearly shows that majority of the people were disagreeing to the statement and likewise quite a number of people are unaware of this fact. Now the reason why these people are disagreeing to the statement asked, because the collection of the evidence is barely to a minimum level at the crime scene. Sufficient evidence is not collected from the crime scene that is why the terrorist cases are not using the help of digitized evidence in form of biometrics which can help in

successful investigating and court trial of the terrorist cases in Pakistan. Minimal number of people are agreeing about the use of biometrics digital evidence in terrorist cases.

Question 28 was asked to now the people perception about, that either the use of digital evidence (biometrics) can help in terrorists investigations or not. The response clearly shows that almost everybody agreed that by using the digital evidence (biometrics) the investigation of the terrorist can be improved.

Question 29 & 30 are actually reciprocating each other, clearly showing the responses of the people who are actually working in the field of investigating and apprehending these terrorists. That investigation of these terrorist is currently unsuccessful, there are many reasons to it which can be seen in earlier asked questions. Which are lack of collection of evidence from the crime scene, lack of sufficient evidence collected from the crime scene against these terrorist, lack of providing the evidence in court against these terrorists etc.

Question 31 was asked to know from the people about how investigation of the terrorists can be improved. Almost all of them agreed to the statement asked that investigation can be improved with the use of digital evidence (biometrics). A few people were unaware of the question asked. Only one has disagreed to the statement.

Question 33 was asked to highlight the important factor and legal issue which is currently being faced by people of investigating authorities and is hampering the use of digital evidence biometrics against these terrorist. Question asked was to get the opinion of the people, that trials of terrorist cases in Pakistani courts is delayed because of lack of any suitable law for using digital evidence biometrics in Pakistani courts against terrorists. All the respondent shave agreed to the statement a very few are those who are completely ignorant about the question's importance which is asked.

Question 34 also brings out an important factor which is contributing towards the unsuccessful investigation of the terrorist in Pakistan. The question asked shows the response of the people when asked about the reason of delay of terrorist's cases in Pakistani courts is poor management of the chain of custody of the evidence. Mostly the people have agreed to the statement, this is because the evidence collected is not centrally stored. Evidence collected is separately collected by different departments as well.

Question 35 also brings out an important legal issue regarding the contamination of the crime scene which is causing the slowdown of the process of investigation and terrorist trials at Pakistani court of law. When people were asked about whether the contamination of the crime

scene is effecting or causing unnecessary delays in investigation of the terrorist. Mostly the respondents have agreed to the statement that yes one of the reasons for the delays in the investigation of terrorist is contamination of the crime scene. Very few were unaware of the question asked and some even disagreed as well.

4.2 Qualitative analysis (As per Research Question)

Qualitative analysis is performed to answer the research question three. Research question three constitutes to understand and know in person the main problems and legal issues being faced in the use of biometrics as digitized evidence. Also the factors and legal issues which have been analyzed in the quantitative analysis are also considered during the qualitative data analysis. As in qualitative the focus is on more refine and more detailed insight of the problems and legal issues involved. NVIVO tools has been used to identify different themes and relate them to generate models which will show inter linked relation between different factors and legal issues.

4.2.1 Model 1

The first model generated was to show the working of the Pakistani courts. As per the discussion from the interviewees Anti-terrorist courts (ATC) are working for only terrorist cases and the civil courts for the civilian cases. In true sense these courts should work independently, as the model is showing that the both these courts are linked with each other, this is because the judges and lawyer are the same which are working in these courts. So principally the same practice as in civil courts are being followed in ATC as well. The working of the ATC should be different than the civil courts.

4.2.2 Model 2

As per the interviews conducted, there are many associated and linked problem with the working of the ATC. Mostly the interviewees said presence of political influence hampers the working in the terrorist's cases. The involvement of influential people in the terrorist cases leads to delays and at times the setting free of the terrorists. Also the involvement of finance in the terrorist cases altogether changes the true dynamics of the terrorist cases in Pakistan. Witness protection program is a legal issue which is being faced by the judges, lawyers and policemen in the working of the ATCs. Now the lack of witness protection program is directly linked with the terrorist threats to the witnesses, judges, lawyers and even to policemen as well. Also there is another important factor like collection of evidence from the crime scene which symmetrical to the working of the ATCs. Legal issues like ban of death sentenced is major hurdle which is causing the huge hurdle in the working of the ATCs. All the death sentences

decisions to these terrorist are being held up in the ATCs because of the ban on death penalty by president of Pakistan.

4.2.3 Model 3

This model simply shows that how these terrorist are exploiting the non-availability of the witness protection program. They have made it as their tactics and part of practice to threat the witness, judges, lawyers who are involved in the cases of terrorists. This is causing unnecessary and unwanted delays in the legal proceedings of these terrorists' cases.

4.2.4 Model 4

When the interviewees were asked about problems associated with the crime scene. According to them the crime scene has generally two main problems. One is the collection of the evidence from the crime scene. Secondly is the contamination of the crime scene. These two problem are also highlighted in the quantitative analysis part as well. Collection of evidence and crime scene contamination are inter-linked with each other. Collection of evidence is symmetrical to the crime scene contamination. If the crime scene is contaminated the collection of evidence becomes a problem and vice versa.

4.2.5 Model 5

When the interviewees were asked about the crime scene contamination they explained many factors and legal issues which are present at the crime scene. They also explained that these factors are contributing very negatively in the working of terrorist cases. Problems like provision of the emergency services at the crime scene contaminates the crime scene a lot. As their presence to the site is very necessary for the evacuation of the injured people and giving first aid to the injured. They must have to be regulated to some standoff distance from the main crime scene for the evacuation of injured and dead bodies. Secondly when asked about how different departments are working at the crime scene, unanimous theme of conflict of interest came up. All departments are working separately. Police comes and collects the data which they find from the crime scene, intelligence agencies comes and do their collection at the crime scene, LEAs come and they collect remaining evidence from the crime scene and in this way the complete evidence is divided into bits and pieces. In this entire process the crime scene gets contaminated a lot. Problems like self-respect of the bosses who wants to see and visit the crime scene out of curiosity, presence of general public on the crime scene, non-awareness of the sensitivity of the crime scene that how important is to keep the crime scene free from the people to avoid any contamination, presence of political influence contaminates the crime scene like in case of assassination of Benazir Bhutto. Also the assertiveness of police at the

crime scene is mostly not present which leads to entry of unwanted and undesired people on the crime scene.

4.2.6 Model 6 & 7

This models explains the people's response to the problems which are related to the collection of the evidence. According to the response of the interviewee the collection of evidence from the crime scene is directly linked to the training of the people who are meant to collect the evidence. Secondly, equipment and resources must be available for the collection of evidence from the crime scene. Also collection of the evidence is linked to some intangible tangibles like shirking work and sincerity with the work as well. Collection of evidence from the crime scene and chain of custody of the evidence collected both are associated to legal problems in the investigation and further prosecutions of the terrorists.

4.2.7 Model 8

As per the requirement of the research question 3 the comprehensive list of all the legal issues associated with the investigation of the terrorists are extracted out of the interviewee's opinion. Firstly according to interviewees the ban on the death sentence is causing main hurdle in the successful prosecution and investigation of the terrorist. Terrorists under investigation take advantage of this by simply denying the allegations which goes into their benefits and leads the investigators to resort on third degree investigation. The processing and chain of custody of the evidence also causes problems in the investigation of terrorist. As the evidence collected is already in bit and pieces. Lack of witness protection program, which indirectly is going in the benefit of the terrorist. Involvement of the finance at different tires of terrorist's case investigation and prosecution. To avoid any problems regarding evidence, there is lack of central storage of evidence against these criminals which is causing problems in the processing and maintain the chain of custody of the evidence. Also there is no law favorable to the use of biometrics as digitized evidence in court of law.

4.2.8 Model 9

This model explained the factors and problems which are present in the investigation the terrorist. Firstly and most importantly the investigation which are carried out against terrorists are third degree, when asked why, all the investigating officers replied that because of non-availability of the evidence we have to resort to third degree. We know that the suspect is involved in the criminal and anti-state activities but we don't have proof in form of evidence. Also the threat given by the terrorist is also posing some problems in investigation process. Political influence in the investigation of the terrorist. Lack of acceptability of the biometric evidence in our law against these terrorist. When these terrorist are apprehended from the crime

scene, there is a lot of biometric evidence present at the crime scene but collected evidence does not help in the investigation as it is not accepted in the court of law. Crime scene problems are also linked to the investigation of the terrorist. Conflict of interest between different investigating departments also leads to unsuccessful investigation of the terrorist. This is because the leads which a suspects gives during the investigation are mostly in form of other terrorist confirmation, now to apprehend the lead given by the suspect under investigation is already under captivity by other departments which are at times reluctant to share the information regarding the lead given. Problems of collection of evidence are also linked with the terrorist investigation. Pakistani forces which includes all the LEAs, police department, intelligence agencies and Pakistan army are also linked to the investigation of the terrorist, it will be explained in the other model.

4.2.9 Model 10 & 11

According to the model generated it was observes that all the departments which are fighting against the terrorist are following a divergent approach to address this one national mance. Army working independently, LEAs working independently, police working at its own and intelligence agencies as well. That is why the complete picture of what is happening id not being made in clarity. Model 11 shows the relationship of the Investigation officer (IO) to the crime scene. It is very clear from the earlier models as well that everything is interlinked between all the main factors and legal issues.

4.2.10 Model 12

This model shows the interlinkage of terrorist cases investigation with the different main problems and legal issues. Digital evidence and biometric evidence must be incorporated in the amendment of law. Ban on death sentence is also linked with the amendment in law. Amendment in law is a legal issue which must be addressed to have effective results in investigation of terrorist and their prosecution.

5 CHAPTER FIVE: CONCLUSION

The main contents of this chapter are research questions, conclusions and recommended guidelines.

5.1 Research Questions

In this section the research questions are checked that if they are answered or not.

Research Question 1. ***Can how biometric technology can be used as digital evidence***.

This question is answered from the literature review, which is performed to provide meaningful information about the biometric technology to the intended readers (see section 1.8 – 1.10.11).

Research Question 2. ***Can Digital Evidence (Biometrics) be used in apprehension and investigation of terrorists to counter terrorism in Pakistan?***

This question has been answered from literature review as well as from the questionnaire. Literature study is performed to identify various factors which are contributing positively and negatively towards the use of biometric technology in apprehension and investigation of the terrorists to counter terrorism. (See Section 2 – 2.4.3). Questionnaire was also used to get the input from the individuals who are actually performing the job of apprehension and investigation of terrorist. Use of digital evidence (biometrics) can be used very effectively against the terrorist during the apprehensions and investigation (See Section 3.1).

Research Question 3. ***What are the main problems and legal issues faced by the persons who are apprehending and investigating terrorists/criminals cases by using digital evidence (Biometrics) in Pakistan?***

This question has been answered from literature review. Questionnaire was used to have people's concerns about the problems and the legal issue which are present in the process of using digital evidence (biometrics) in apprehension and investigation of terrorist cases in Pakistan (See Section 3.1). Also the interviews have been conducted to further refine and get a deeper insight about problems and legal issues faced by the people. (See Section 3.2 – 3.2.14)

5.2 Conclusions

Biometric technology is used to for the ease of working of different state departments to counter the threat of terrorist in terrorism struck countries. Its wide implementation can be seen cross border monitoring at the airports, central biometric registration of the masses in different parts of the world. Its application in investigation and apprehension of terrorist will be of very helpful as biometric technology has many benefits in identifying individuals on basis of their

behavioral and physiological attributes. In context to this study the problems and legal issued faced by the people who are performing actively the duties of the apprehending and investigating the terrorist on routine basis are highlighted. In order to do this extensive literature has been studied, data collection by questionnaire has been carried out and interviews of the people who are performing the duties in the field. Main factors and legal problems which are faced by the people are analyzed and discussed.

It was observed that problems and legal issues are mostly because of the lack of evidence and in particular biometric evidence which can help in identifying and verifying the suspects. This problem is further linked with crime scene preservation, collection of evidence, processing of evidence in context to maintaining its chain of custody, contamination of the crime scene, technical expertise of the people who are collecting the evidence, resources and equipment available in the process of collection and processing of evidence, lack of central storage of data bank for cross referring of data, lack of information sharing between different department about evidence, provision of evidence collected from the crime scene during the investigation, acceptability of the digital evidence in form of biometrics during the trials in court of law.

Also on basis of data collected it has been observed that mostly the people are unaware of the sensitivity of the issue and use of biometric in investigation and apprehension as digitized evidence. However it has also been found from the data that people are facing problems in investigating and apprehending terrorist with the current evidence which is being collected and have a strong will to use biometric based digital evidence which is more reliable and effective.

5.3 Recommended Guidelines

Following guidelines have been proposed for effective use of biometrics as digitized evidence to counter terrorism in Pakistan. These guidelines have been extracted out from literature, questionnaire and interviews which have been conducted. Knowing the issue (See Section 1.11 and 1.12) and advantages of biometric technology in apprehension and investigation of terrorists is completely understood.

1. **Understanding and Clarity in Use of Biometric Technology.**

   It has been observed from results that mostly people are well aware conceptually about the terminologies. But still there is quite a number of people who are actually unaware of the use of biometric technology as digitized evidence in investigation. It will be of great and immense importance to demonstrate the operation of biometric technology to the concerned people. Special video and audio sessions to be arranged at intra-department level to give the idea of the working of biometric technology.

2. **Training of the individuals.**

    a. **Collection of Evidence**

    It is observed that the people from the police, intelligence departments, LEAs and security forces are not collecting sufficient evidence from the crime scene. This makes the investigation process difficult. To counter this people must be trained quarterly or semi-annually to refresh the details. Also people must also be trained on international courses to further refine the process of collection of evidence.

3. **Information sharing about the evidence and crime scene for convergent effort.**

    It has been observed that currently information sharing between different state departments is not a precedence, however every department is working to counter terrorism. Also people have shown concerns to share information to work effective yet people have shown great willingness to share information in between departments to have a convergent effort. Because of lack of information sharing different terrorist are under investigation but because of relevant precursors of information their investigation is pending and unsuccessful. To address this issue certain cases can be selected at departmental level to start work with and information can be shared so that these cases can be further evaluated with those who are not shared.

4. **Crime scene preservation and contamination for collection of digitized evidence in form of biometrics.**

    It has been observed that the crime scene gets contaminated, which is a hurdle in process of data collection. It has also been observed that there are many reasons as to why this contamination occurs, which includes general public as they are coming in and out of the crime scene without any relevance. Provision of emergency services which have to come in for evacuation of causalities. No cordoning off of the crime scene for collection of evidence as people concerned have agreed that if the crime scene is cordoned off properly the evidence can be collected and which can lead to successful investigation of terrorist. It would be of great importance that the media can used in this regard to teach the masses of Pakistan about the sanctity of the crime scene and importance of preservation. Which will directly leading to counter terrorism in Pakistan. Also the cordon of the crime scene must be established in order to avoid contamination of the crime scene. Emergency services must be kept out and away from the crime scene and causalities must be brought out of the instead of emergency services going into the

crime scene. Also these type of acts leads to evolve new threats by terrorists once these incidents are shown on the television.

5. **Biometrics technology should be made as pivot for investigation**

It has been observed from the responses that the use of biometric technology as digitized evidence can help in investigation process of terrorist, as of currently it is not being used in the investigation because of crime scene preservation issues. That is why the agencies are resorting to third degree investigation techniques which is mostly not very effective and successful technique. Also people concerned have shown great interest and willingness towards the effectiveness and usage of biometric based evidences. It can be achieved if the data collected is without contamination and is shared among different departments for investigating terrorists.

6. **Significance and working of Anti-terrorist courts (ATC) in use of biometric evidence and investigation**

It has been observed from the data that the lawyers and judges who are performing the duties in the ATCs are actually the ones who were working in the civil courts earlier. Their training and practice is as per civilian murderers who are convicted in court of law. In current law the benefit of doubt is given to the alleged person. In case of terrorists the evidence is already very less and at time its present and not collected because of so many reasons like expertise and resources, crime scene contamination, at times political influence as well, also some intangible factors like awareness of terrorism, lack of sincerity with the work and shurk work. The benefit is taken and given to the terrorist who tends to get the sympathizers as well. In order to counter this mance these terrorists should not be treated as normal murderer but instead they should be taken on as war combatants. For these war combatants the judges and lawyers should be trained separately and these terrorists must be dealt by strict laws whereby any small biometric evidence would be considered as sufficient evidence to prove them guilty in court of law.

7. **Curbing of monetary and political aspects involved in the process of investigation**

It is observed that in many cases of terrorist's investigation the monetary aspect has its involvement throughout the process of chain of custody of evidence and its processing in legal matters like provision of evidence in courts for trials. Also during the investigation of the terrorist. In order to have an efficient and strong system of evidence processing and management of its chain of custody, strict disciplinary actions must be

taken against the personel who are found to have any sort of involvement in monetary aspects. Also should be discharged from services as well.

Also the involvement of political dignitaries is affecting the process of investigation and is leading as main cause of mistrust between government and security departments. Policy reforms should be made which should base on making the investigation process free from political influence.

8. Lack of witness protection program

Witness protection program is also contributing a lot in the process of investigation of terrorists**.** It is observed in the data that because of lack of any witness protection program there are incidents in which witnesses have left the cases of terrorists for witness ship. Also life threats have been given to people who are investigating the terrorists. Also in case of lawyers who are defending or convicting the terrorists also gets threats, in both the cases what happens is that the benefit goes in favor of terrorists as people have surrendered the jobs and have shown unwilling to serve in their required fields. In order to take advantage of the people's expertise who are doing these duties it is very important that witness protection should be formulated, which can give protection to witnesses and people who are working to counter terrorism.

9. Provision of central storage of data collected as evidence

As people were observed having problems working with evidence. This is because evidence collected from crime scene is not shared with any other department. So at times when biometric based evidence is required to further investigate the terrorist it is either not available or not collected from the crime scene. To smooth line the problem of evidence a central storage facility at provincial level must be established and funded by government and different stakeholders.

10. Provision for amendment of law.

It has been observed that in most of the terrorist cases where biometric evidence is sufficient the death ban currently prevailing in Pakistani justice system is hampering their death sentence. Also as per the opinion of the people who have been interviewed and data has been collected on questionnaire that if the law is amended to accommodate fully the biometric evidence, it would be quite helpful to investigate these terrorists and will lead to successful investigation. In order to have a strong and reliable system of investigation the amendment in law must be incorporated in present law to facilitate and achieve better results.

5.4 Future Work

In context to this thesis work, various guidelines have been proposed which are based on understanding of the issue. It is believed that each guideline can be explored to further pin point the root causes of the problem that why these terrorist are being set free once they have been apprehended and investigated by our state departments.

6 END NOTES

[1] Timothy. V, B. K, Matthew. G., *OpenVL: Empowering investigators and first-responders in the digital forensics process*, Digital Investigation, S45 – S53, 2014.

[2] Brian D.C, Eugene H. Spafford., *An Event-Based Digital Forensics Investigation Framework*, *Center for Education and Research in Information Assurance and Security*, Purdue University, USA.

[3] Nick. B, *Establishing the Digital Chain of Evidence in Biometric systems(Dissertation)*, Morgantown, West Virginia, 2009.

[4] Nathan. J, *DNA Testing in criminal Justice: Background, Current Law, Grants, and Issues,* Congressional Research Service, 6 December 2012.

[5] Brain. C, *Defining Digital Forensics Examination and Analysis Tools Using abstraction Layers.* International Journal of Digital Evidence, *Volume 1, Issue 4, 2003.*

[6] Cartel, W, (2010). *Anti-Cartel Enforcement Manual*. (pp. 1-37). International Competition Network

[7] Aleksandra, B. *Biometric Authentication. Types of Biometrics Identifiers (Thesis),* University of Applied Sciences, 2012.

[8] Falak. Z, & Sajid .N., *Guidelines for the Deployment of Biometrics Technology in Blekinge Health care System with the Focus on Human Perception and Cost factor* (Thesis), Blekinge Institute of Technology, Sweden, January 2010.

[9] Nicole A. Spam., *Forensic Biometrics from Images and Video at the Federal Bureau of Investigation.*

[10] Douglas. W, *Evaluating Corroborative Evidence,* Department of Philosophy, *University of Winnipeg, Canada.*

[11] David. G, *Modeling Corroborative Evidence: Inference to the Best Explanation as Counter-Rebuttal, Department of Philosophy, Old Dominion University, Virginia, USA, 2014*.

[12] Shahzad. S., Oliver. Popov, Ibrahim. B., *Extended abstract digital forensics model with preservation and protection as umbrella principles,* Department of computer & electrical engineering and computer science, University of New Haven, West Haven, USA, 2014.

[13] Reith M, Carr C, Gunsch G. An Examination of Digital Forensic Models. *Int J Digit Evid*. 2002; 1(3):1–12.

[14] Robert. R., *A Ten Step Process for Forensic Readiness,* International Journal of Digital Evidence, Volume 2, Issue 3, winter 2004.

[15] Mark. R., Clint. C, & Gregg Gunsch. *An Examination of Digital Forensic Models, International Journal of Digital Evidence*, volume 1, Issue 3, fall 2002.

[16] Carrie, M., Whitcomb, *An Historical Perspective of Digital Evidence: A Forensic Scientist's View*. International Journal of Digital Evidence. Volume 1, Issue 1, spring 2002.

[17] Petter. C. B., Katrin. F., & Andre. A., *Practical use of approximate Hash Based Matching in Digital Investigations. Norwegian information security lab, Gjovik University College, Norway, 2014.*

[18] Spyridon. D., Irvin. H., and Oliver. Popov. *Semantic Representation and Integration of Digital Evidence. Department of Computer and system Science, Stockholm University, Sweden 2013.*

[19] B. D. Carrier and E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework," *Proceedings of the 4th Digital Forensic Research Workshop DFRWS*, pp. 1–12, 2004.

[20] T., Fladsrud. *Face Recognition in a border control Environment: Non Zero Effort Attack' Effect on False Acceptance Rate (Thesis).* Department of Computer Science and Media Technology, Gjovik University College, 2005.

[21] M. Eriksson., *Biometrics: Fingerprint based identity verification.* Department of Computing Science. UMEA University. 2001.

[22] J.A. Unar, Woo. C. Seng, Almas. Abbasi. *A review of Biometric Technology along with trends and propects. (Science Direct).2014. University of engineering and technology, Pakistan.*

[23] S.Yan, Z.Xukai, E.Y.Du, Biometrics-based authentication: anew approach, in: Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 2011, pp.1–6.

[24] M.Gudavalli A.V.Babu, S.V.Raju, D.S.Kumar. Multimodal biometrics— sources, architecture and fusion techniques: an overview in Proceedings of the 2012InternationalSymposiumonBiometricsandSecurityTechnologies (ISBAST), IEEE, March2012.pp.27–34).

[25] Marianna J. Verett., Performance and Usage of Biometrics in a Test Bed Environment for Tactical Purposes. Naval Postgraduate School, California. Dec 2006.

[26] Vilas H. Gaidhane, Yogesh V. Hote & Vijander Singh., *An Efficient Approach for Face Recognition based on Common Eigenvalues. Department of Electrical Engineering, Indian Institute of Technology (IIT), India. 2014.*

[27] Nathan D. Lewis, *Corneal Topography Measurements for Biometrics Application. University of Arizona. 2001.*

[28] Chiraz. B. Abdelkader., *Gait as a Biometric for Person Identification in Video. Department of Computer Science. 2001.*

[29] Dipl. Lng. Xuebing Zhou., *Privacy and security assessment of biometric Template Protection.* Geboren in Shenyang, China. 2001.

[30] Umut. U., *Secure Biometric System (Dissertation). Department of Computer Science & Engineering, Michigan State University. 2006.*

[31] Muhammad. M, and M. S. Arif., *Role of Investigation Agencies and Judiciary to warfare Terroism in Pakistan. University of Faisalabad, Pakistan. Volume 1, issue 1, January 2013.*

7 BIBLIOGRAPHY

http://www.cacianalyst.org/publications/analytical-articles/item/12720-pakistans-war-on-terror-up-to-and-beyond-2014.html

http://www.satp.org/satporgtp/countries/pakistan/database/casualties.html

http://www.cacianalyst.org/publications/analytical-articles/item/12720-pakistans-war-on-terror-up-to-and-beyond-2014.html

Paul Reynolds, quoting David Hannay, Former UK ambassador (14 September 2005). "UN staggers on road to reform". BBC News. Retrieved2010-01-11.

Nachman Ben-Yehuda, The Masada Myth: Scholar presents evidence that the heroes of the Jewish Great Revolt were not heroes at all.

Otto Scott, *The Secret Six: John Brown and the Abolitionist Movement* (Murphys, Calif.: Uncommon Books, 1979, 1983), 3.

Martin Goodman, *Rome and Jerusalem: The Clash of Ancient Civilisations* (2008:407) talks of *sicarii* practicing "terrorism within Jewish society"

Wayman, J.L., 2008. Biometrics in Identity Management Systems, *IEEE Security and Privacy*, vol.6, no.2, pp.30-37.

Mansfield, A. J., & Wayman, J. L., 2002. *Best Practices in Testing and Reporting Performance of Biometric Devices,* Version 2.01.

http://www.homeoffice.gov.uk/counter-terrorism/securing-2012-olympic-games/safeand secure-games/

Victim ology: Theories and Applications, Ann Wolbert Burgess, Albert R. Roberts, Cheryl Regehr, Jones & Bartlett Learning, 2009, p. 103

Fundamentals of Criminal Investigation (Sixth Edition). Charles E. O'Hara and Gregory L. O'Hara; 1994; ISBN 0-398-05889-X

"Forensics". TheFreeDictionary.com.

U.S. Department of Labor. Bureau of Labor Statistics. Occupational Employment `and Wages, May 2011. "19-4092 Forensic Science Technicians". http://www.bls.gov/oes/current/oes194092.htm

Dawn.com, Available at: http://www.dawn.com/news/1059862/hyderabad-police-not-trained-to-solve-terrorism-cases

Daily Times, Available at: http://www.dailytimes.com.pk/default.asp?page=2007%5C02%5C14%5Cstory_14-2-2007_pg7_8

Ozgul Faith, Erdem Zeki and Bowerman Chris, (2007), Prediction of Unsolved Terrorist attacks Using Group Detection Algorithms.

Spiegel ONLINE International, Available at: http://www.spiegel.de/international/germany/new-twist-in-unsolved-terror-case-dna-traces-link-ex-raf-terrorist-to-buback-murder-a-644191.html

Yue Liu. Scenario study of Biometric systems at Borders. Computer Law and Security Review, 27(2011); 36-44.

Karnan .M, Akila .M, Krishnaraj .N. Biometric personal authentication using keystroke dynamics: A review, Applied Soft Computing, Vol 11, Issue 2, March (2011), 1565-1573.
Kai Yang, Eliza Yingzi Du, Zhi Zhou, Consent Biometrics, Neurocomputing, Volume 100, 16 January 2013, Pages 153-162.

Shanker, Thom. 'To track militants, US has system that never forgets a face'. New York Times, 13 July 2011. Accessed Feb 2012. www.nytimes.com/2011/07/14/world/asia/14identity.html
Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport'. Currah, P, and Mulqueen, T. Social Research 78 (2): 557-606 (ASLIB). June 2011

Brent L., Smith. Kelly, R. and Damphousse, 2001, American Terrorism Study: Patterns of Behavior, Investigation and Prosecution of American Terrorists, Final Report, p 45.

O'Gorman, L., 2003. Comparing passwords, tokens, and biometrics for user authentication, *Proceedings of the IEEE*, vol.91, no.12, pp. 2021-2040.

Stanley, P., Jeberson, W., & Klinsega, V.V., 2009. Biometric Authentication: A Trustworthy Technology for Improved Authentication, In Future Network, 2009 *International Conference on,* pp. 171 – 175

Vielhauer, C., 2005. *Biometric User Authentication for IT Security: From Fundamentals to Handwriting*, 1edition, Springer, pp. 27.

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E., 2006. Privacy preserving multi-factor authentication with biometrics, In *Proceedings of the Second ACM Workshop on Digital Identity Management,* ACM, New York, NY, pp. 63-72.

Liu, S.; Silverman, M., 2001. A practical guide to biometric security technology, *IT Professional*, vol.3, no.1, pp.27-32, Jan/Feb 2001

Gregory, P. & Simon, M.A., 2008. *Biometrics for Dummies*, For Dummies.

Mansfield, A. J., & Wayman, J. L., 2002. *Best Practices in Testing and Reporting Performance of Biometric Devices,* Version 2.01.

Moskovitch, R. et al., 2009. Identity theft, computers and behavioral biometrics, *Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on*, vol., no., pp.155-160.

Nanavati, R.; Nanavati, S. & Thieme. M., 2002. *Biometrics Identify Verification in a Networked World,* John Wiley & Sons, INC. New York.

Mark Reith, Clint.C. & Gregg Gunsch,2002. An Examination of Digital Forensic Models, Vol 1, Issue 3.

Julian, A., 2002. *Biometrics: Advances Identity Verification the Complete Guide*, Springer, pp. 45.

Wohlin, C., Runeson, p., et al., 2000. *Experimentation in Software Engineering: An Introduction*, Kluwer Academic Publishers London, 2000 [e-book] Google books, Available at: Google Books, http://books.google.se/books?id=nG2UShV0wAEC&dq=Experimentation+in+Software+Engineering+an+Introduction&printsec=frontcover&source=bn&hl=sv&ei=1KIeS5yjHInCsAbs88CvCw&sa=X&oi=book_result&ct=result&resnum=5&ved=0CCUQ6AEwBA#v=onepage&q=&f=false [Accessed: Sep 3, 2009].

Deriche, M., 2008. Trends and Challenges in Mono and Multi Biometrics, *Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on*, vol., no., pp.1-9, 23-26.

Draper, S.C., Khisti, A., Martinian, E., Vetro, A., & Yedidia, J.S., 2007. Using Distributed Source Coding to Secure Fingerprint Biometrics, *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*, vol.2, no., pp.II-129-II-132.

Damm, L.O., 2007. *Early and Cost-Effective Software Fault Detection*, Ph.d Doctoral Dissertation. Sweden: Blekinge Institute of Technology.

Berander, P., 2007. *Evolving Prioritization for Software Product Management*, Ph.d Doctoral Dissertation. Sweden: Blekinge Institute of Technology.

Jain, A.K., Ross, A., & Prabhakar, S., 2004. An introduction to biometric recognition, *Circuits and Systems for Video Technology, IEEE Transactions on*, vol.14, no.1, pp. 4-20.

Jain, A.K., Ross, A., & Pankanti, S., 2006. Biometrics: a tool for information security, *Information Forensics and Security, IEEE Transactions on*, vol.1, no.2, pp. 125-143.

Moore, J., 2005. „Biometrics takes on physical access,“ *Federal Computer Week*, vol. 19, no. 5. pp. 16-20.

Biometrics: Newsportal.com, 2009. [Online]. Available at: http://www.biometricnewsportal.com/ [Accessed: Nov 14, 2009].

Jain, A.K., Pankanti, S., Prabhakar, S., Lin Hong, & Ross, A., 2004. Biometrics: a grand challenge, *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, vol.2, no., pp. 935-942.

Jain, A.K., Pankanti, S., Prabhakar, S., Lin Hong, & Ross, A., 2004. Biometrics: a grand challenge, *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, vol.2, no., pp. 935-942.

Jain, A., Hong, L., & Pankanti, S., 2000. Biometric identification, *Commun. ACM* vol. 43, no. 2, pp. 90-98.

Jain, A., Bolle, R., & Pankanti, S. 2002, „Introduction to Biometrics", *In Biometrics: Personal Identification in Networked Society*, *Kluwer Academic Publishers*.

Dawson, B., 2002. Machine vision online, Iris Scan, [electronic print]. Available at: http://www.machinevisiononline.org/public/articles/archivedetails.cfm?id=364 [Accessed: Nov 15, 2009].

Iridian technologies, 2009. „Biometric comparison Guide, " Available at: http://epic.org/privacy/surveillance/spotlight/1005/irid_guide.pdf [Accessed 11 Nov 2009]/

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. 2000, „Biometric identification through hand geometry measurements", *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol.22, no.10, pp. 1168-1171.

Salavati, S., 2006. Biometrics in practice The security technology of tomorrow's airports, B.S Project, School of Mathematics and System Engineering, Växjö University, Sweden.

Libin, P., 2005. ASSA ABLOY, *pros and cons of biometric* [electronic print]. Available at: http://www.assaabloyfuturelab.com/FutureLab/Templates/Page2Cols 294.aspx [Accessed: Sep. 23, 2009].

Biometrics: Newsportal.com, 2009. [Online]. Available at: http://www.biometricnewsportal.com/ [Accessed: Nov 14, 2009].

Bolle, R., Connell, J., Pankanti, S., Ratha, N., & Senior, A., 2003. *Guide to Biometrics*, Springer Verlag. [E-book] Google books. Available at: http://books.google.com/books?id=OubHQ9Czgr0C&dq=Guide+to+Biometrics&printsec=frontcover&source=bn&hl=en&ei=0XUZS7NC4WGsAb1gpWQBg&sa=X&oi=book_result&ct=result&resnum=4&ved=0CBgQ6AEwAw#v=onepage&q=&f=false [Accessed: Oct 02, 2009].

Campbell, J.P., Jr., 1997. Speaker recognition: a tutorial, *Proceedings of the IEEE,* vol.85, no.9, pp.1437-1462.

Nalwa, V.S., 1997. Automatic on-line signature verification, *Proceedings of the IEEE*, vol.85, no.2, pp.215-239.

Digital Signature | Keystroke Biometric, 2009. Find Biometrics: Global identity Management, [online]. Available at: http://www.findbiometrics.com/signature-keystroke/ [accessed: Nov 22, 2009].

Figure image of key stroke, 2009. [Electronic print]. Available: http://www.deepnetsecurity.com/products2/images/TypeSense1.gif [Accessed: Sep 28, 2009].

BenAbdelkader, C., Cutler, R. G., & Davis, L. S., 2004. Gait recognition using image self-similarity, *EURASIP J. Appl. Signal Process,* pp. 572-585.

DNA-Based Biometrics, [electronic print]. Available at: http://misbiometrics.wikidot.com/dna [Accessed: Sep. 27, 2009].

Creswell, J.W., 2002. *Research Design. Qualitative, Quantitative and Mixed Method Approaches*. Second Edition, Sage Publications.

Hazzan, O., Dubinsky, Y., Eidelman, L., Sakhnini, V., & Teif, M., 2006. Qualitative research in computer science education, *In Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education. SIGCSE '06. ACM,* New York, NY, pp. 408-412.

Seaman, C.B., 1999. Qualitative methods in empirical studies of software engineering, *Software Engineering, IEEE Transactions on,* vol.25, no.4, pp.557-572.

Rijgersberg, H., Top, J., & Meinders, M., 2009. Semantic Support for Quantitative Research Processes, *IEEE Intelligent Systems*, vol, 24, no. 1, pp. 37-46.

Hove, S.E., & Anda, B., 2005. Experiences from conducting semi-structured interviews In empirical software engineering research, *Software Metrics, 2005. 11th IEEE International Symposium*, vol., no., pp.10 pp.-23.

Preece, J., Rogers, Y., & Sharp, H., 2002. *Interaction Design: beyond Human-Computer Interaction*, New York: john Wiley & sons, pp. 14, 230, 390-398.

8 APPENDIX

8.1 Appendix A

Guideline to counter terrorism on basis of digital evidence (Biometrics) in Pakistan – Questionnaire

Note: **This questionnaire is related to research work which intends to find out the "*Guideline to counter terrorism on basis of digital evidence (Biometrics) in Pakistan*". The information shared will be solely used for research purpose and will be kept confidential.**

PART- 1

Name:
Age:
Gender:
Qualification:
Experience:
(In your own particular Field)

PART- 2

Digital Evidence (Biometrics) (Q1-Q22)

		Strongly Agree (1)	Agree (2)	Neither agree or Disagree (3)	Disagree (4)	Strongly Disagree (5)
1.	Digital evidence means: Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial?					
2.	Biometrics means: **Biometrics** refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes?					
3.	Do biometrics form part of digital evidence?					
4.	In your opinion, can digital evidence be used					

	in proving terrorist guilty in court of Law?					
5.	In your opinion, can digital evidence (Biometrics) be used in proving terrorists Guilty in court of Law?					
6.	Does Police collect digital evidence while apprehending terrorists for crime scene?					
7.	Does police collect sufficient evidence from the crime scene against terrorists?					
8.	Does police uses digital evidence against terrorist in court of Law					
		Strongly Agree (1)	**Agree (2)**	**Neither agree or Disagree (3)**	**Disagree (4)**	**Strongly Disagree (5)**
9.	Does LEAs collects digital evidence in apprehending terrorists for crime scene					
10.	Does LEAs collect sufficient evidence from the crime scene against terrorists					
11.	Can LEAs use digital evidence against terrorist in court of Law					
12.	Is evidence collected by Police from the crime scene sufficient to prove terrorist guilty in court of law?					
13.	Is evidence collected by LEAs from the crime scene sufficient to prove terrorist Guilty in court of law?					
14.	Does intelligence departments collect the digital evidence from the crime scene when apprehending the terrorists					
15.	In your opinion, what do you say that digital evidence collected by different LEAs is shared among all security agencies/ LEAs departments					

16.	In your opinion, what do you say that digital evidence collected by different LEAs should be shared among all security agencies/ LEAs departments					
17.	**In your opinion, crime scene should be cordoned off by police for collection of evidence**.					
18.	**In your opinion, is crime scene cordoned off by police for collection of evidence**					
19.	In your opinion, digital evidence collected from crime scene is sufficient against terrorists					
20.	In your opinion, what do you think that it is the lack of collection of digital evidence from crime scene that prevents the terrorists from prosecution?					
21.	In your opinion, what do you think that it is the lack of providing digital evidence in courts that prevents the terrorists from prosecution?					
22.	Do you think that evidence used against terrorists in the court of law is sufficient					

PART- 3

Terrorist cases Investigation & Counter Terrorism (Q23-Q37)

		Strongly Agree (1)	**Agree (2)**	**Neither agree or Disagree (3)**	**Disagree (4)**	**Strongly Disagree (5)**
23.	Do you understand the meaning of term Terrorism					
24.	Do you understand the meaning of counter terrorism					
25.	Do you know about terrorist's cases being run in Pakistani courts?					

26.	Do you think about terrorist's cases being run in Pakistani courts are credible?					
27.	Do you think that the terrorist cases run in Pakistani courts are using help of digital evidence					
28.	Does digital evidence helps in investigation of terrorists against their crimes in court of law					
29.	Do you think that currently investigation of terrorists cases in Pakistan is successful					
30.	Do you think that currently investigation of terrorist cases in Pakistan is not successful					
31.	Do you think that investigation can be improved against terrorist by using Digital evidence (Biometrics)					
		Strongly Agree (1)	**Agree (2)**	**Neither agree or Disagree (3)**	**Disagree (4)**	**Strongly Disagree (5)**
32.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because of lack of Digital Evidence?					
33.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because of lack of any suitable laws of using digital evidence in Pakistani courts against terrorists?					
34.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because of lack of poor management of chain of custody of Evidence?					
35.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because of contamination of digital evidence at the crime scene?					
36.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because					

	of lack of collection of Digital Evidence at crime scene?					
37.	Do you think that investigation of terrorist cases in Pakistani courts is delayed because of lack of Digital Evidence?					

38. In your opinion, is there any other factor/thing which is causing delay in prosecution the terrorist cases in Pakistani courts? Please List
    1.
    2.
    3.