IARS' International Research Journal
p-ISSN 2202-2821 e-ISSN 1839-6518 (Australian ISSN Agency)

Vol. 06 No. 02 2016
82800602201603

Biometric Identification Criminal, Terrorist, and Individual Identification System It's a New Wine & Taste

Adnan Majeed
Researcher , Beacon House National University, Lahore, Pakistan

***ABSTRACT** –Biometric system used for security purpose. Mostly the biometric system used for individual identification e.g. to scan finger, eye, iris, voice, signature, DNA, and Hand geometry. The main purpose of installing biometric system to minimize crimes and terrorist attack. The methodology of the paper to collect primary data from research, interviews, and human observation case studies. The objective of this research paper to control human theft, and terrorist activity in Pakistan.*

Key words: Biometrics System; Criminal Identification; Terrorist Identification; Facial Recognition; Finger Identification.

I. Introduction

Biometric systems are used to verify and identify human. It analyzes which person has its own unique identity. Basically, biometric systems are used for security purposes, the main objective of biometric system to achieve goal of transparent identity. Biometrics measure individual's unique physical or behavioral characteristics to recognize authenticate their identity. Common physical biometrics system includes fingerprints, hand or palm geometry, and retina, iris, or facial characteristics, enrollment and authentication.

Behavioral characters include DNA recognition, Palm Print recognition, signature, voice, (which also has a physical component), keystroke pattern and gait, of this class of biometrics, technologies for signature and voice are the most developed. The main purpose of biometric to verify and identify users. Identification has a tendency to be more difficult of the two uses because a system must search a database of enrolled users to find a match. Biometric systems ensure to depend in part of what the system is protecting and what it is trying to protect alongside. In France biometric system are used for crime detection and protection. It minimizes the terrorist attack, open weapon attack, misbehavior attack, cyber crime attack, bomb blast attack. Biometric system is basically a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person process. Depending on the application situation. A biometric system typically operates in one of two modes.

Biometrics offer greater security and ease than traditional methods of personal recognition. In some applications biometric can replace or supplement the existing technology. In others, it is the only feasible approach. Biometric contain sensitive information about the people. The biometric system that is considered in this paper is a verification system. Biometric system makes two types of errors e.g. false match or false accept. Mistaking biometric measurements from two different people to be from the same person. Biometric system also used for attendance system in different organization and institution. The paper is organized as follows section II describe Classification of Biometric System Section III describe literature review, section IV describe purpose and objective and section V describe methodology and section VI describe experiment and results.

II. Classification

A. Components of a typical Biometric System

A typical biometric authentication system consists of five modules/components

Sensor module: It is used to capture user's raw biometric data. An example is camera used to take a picture of human face.

Feature extraction module: It is used to process the acquired biometric data to extract a set of features. For example, features on the surface of a face, such as the contour of the eye sockets, nose, and chin can be extracted.

Matcher module: It is used to compute matching scores of comparing the extracted features against the stored ones.

System database module: It is used to store the biometric templates of features the enrolled users.

Decision-making module: It is used to either determine the user's identity or confirm the users claimed identity [1].

B. Fingerprint

Biometric fingerprint identification is most popular method for person identification. Fingerprint has been widely used in business transaction. Fingerprints consist of a regular texture pattern composed of ridges and valleys. These ridges are characterized by several landmarks points, recognized as minutiae, which are typically in the form of ridge endings and ridge bifurcations. The spatial distribution of these details points is maintain to be unique to each finer, it is the collection of minutia points in a fingerprint that is primarily employed for matching two fingerprints. Since all government agencies and institution used automatic fingerprint identification system. Materialization of low cost and compact fingerprint readers has made fingerprint modality a preferred choice in many civil and commercial applications [2].

Figure 1: Biometric finger identification

C. IRIS

The iris pattern is taken by a special grey scale camera in the distance of 10- 40 cm of camera. One time the grey scale picture of the eye is obtained then the program tries to locate the iris within the picture. Iris recognition is a computerized system of biometric identification that makes use of mathematical path recognition method. Iris images get under infrared illumination consist of complex texture pattern with numerous individual attributes, e.g. stripes, pits, & furrows, which permit for highly reliable personal identification. The visual texture of iris is formed in the work of fetal development & becomes stable in first years itself. Iris recognition is also widely used; it is feasible in huge scale. Each iris is different for twins like finger print. It is difficult to alter iris pattern & it is simple to detect the artificial iris. The main advantages of iris recognition are high accuracy & verification times takes less than seconds. The disadvantage of this recognition are cost is high, much movement of head & use of color contact lens. Conversely, high sensor cost, along with comparatively huge failure to enroll (FTE) rate reported in some studies, & lack of legacy iris databases may limit its usage in some large-scale government applications [3].

D. FACE

Face acknowledgment may be a nonintrusive procedure, and facial pictures range unit without a doubt the principal basic biometric trademark utilized by people to shape a private acknowledgment. The uses of personality check shift from a static, controlled "mug-shot" confirmation to a dynamic, uncontrolled face recognizable proof amid an untidy foundation (e.g., air terminal). 1) the situation and form of facial attributes like the eyes, eyebrows, nose, lips and chin, and their abstraction relationships, 2) the (global) analysis of the face image that represents a face as a weighted combination of variety of canonical faces. While the verification performance of the face recognition systems that are commercially on the market is affordable, they impose variety of restrictions on however the facial images are obtained, generally requiring a set and simple background or special enlightenment [4].

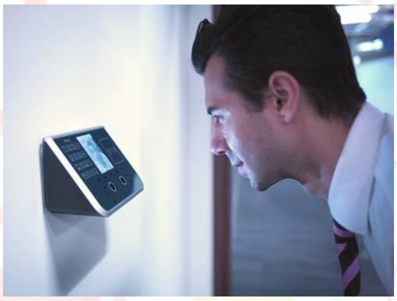

Figure 2: Face Recognition System

E. PALM GEOMETRY

The palmprint and hand geometry unadulterated arithmetic pictures may be separated from a hand picture in an exceptionally single shot at indistinguishable time. Distinctive multibiometrics frameworks (e.g., face and unique mark, voice and face and so forth.), a client doesn't have to hold up under the impairment of going through numerous sensors. Moreover, the extortion identified with imagine hand, close by geometry based for the most part check framework, may be satisfied with the mix of palmprint components. Each obtained pictures should be adjusted in a favored course in order to catch the same components for coordinating. The picture thresholding operation is utilized to acquire a twofold hand-shape picture. The edge quality is more than once figured utilizing Otsu's strategy. The hand geometry frameworks have huge physical size and can't be effortlessly installed in existing security frameworks [5].

F. RETINA

The retinal vasculature is to a great degree rich in structure. It is said to be most secure biometric framework. It is hard to change or altered in light of the fact that there exists retinal vasculature. The picture increasing done by a man to look into an eye-piece and center to discover particular spot in visual field [6].

G. ENROLLMENT & AUTHENTICATION

A client is added to the biometric framework. A persuaded number of biometric presentation of a demanding client are acquire, preprocessed, changed into elements, and post prepared, then used to prepare a client model and adjust (retrain) the world model if important. The client demonstrate alongside impostor presentations may be utilized to acquire an edge for that client. The new model is then put away, alongside the limit for that client if necessary. The case to a client's character causes the exhibited biometric.

Information to be analyzed against the guaranteed client's model. Along these lines, the biometric information is acquire, preprocessed, misshaped into components, and postprocessed, before being coordinated with the guaranteed client's model and the subsequent score being contrasted and the put away limit ascertain for the keep up client or general edge esteem [7].

H. DNA Recognition

The DNA is an acronym for deoxyribonucleic corrosive which is available in core of each cell in human body and in this manner an exceedingly stable biometric identifier that speaks to physiological trademark. The DNA structure of each human is one of a kind, with the exception of from indistinguishable twins, and is made out of qualities that focus physical attributes (like eye or hair shading). Human DNA tests can be gained from a wide mixture of sources; from hair, finger nails, salivation and blood tests. Recognizable proof in light of DNA obliges first segregating from source/tests, intensifying it to make numerous duplicates of target succession, trailed by sequencing that creates an exceptional DNA profile. The DNA coordinating is truly famous for measurable and law authorization applications. In any case, it obliges solid specimens and isn't possible progressively. At present, not every one of the progressions in DNA coordinating are computerized and hence results can be skewed if the procedure is not directed appropriately or the DNA tests themselves get defiled. In outline, the DNA coordinating procedure is costly, tedious and along these lines not yet suitable for expansive scale biometrics applications for non military personnel utilization [8].

Figure 3: DNA identification using Finger

I. Palm Print Recognition

The picture of a singular's palm comprises of volar grating edges and flexion fold. Inert palmprint distinguishing proof is of developing significance in logical applications since around half-hour of the inactive prints upraised from wrongdoing scenes (from knifes, firearms, guiding wheels) square measure of palms rather than fingers. Verging on like fingerprints, inert palmprint frameworks use insignificance and wrinkles for coordinating. While authorization and legal sciences offices have always gathered fingerprints, its singularly as of late that colossal palmprint databases are getting realistic [8].

J. SIGNATURE

Signature verification methodology in varied fields like government, legal and industrial transactions. Signature is an activity biometric that alteration over an amount of your time. Signature of some individuals varies substantially: even sequent impressions of their signature appearance totally different. Further professional falsifier might ready to reproduce signature that freaks the system [9].

K. VOICE

Voice may be a combination of physiological and activity biometrics. The options of associate individual's voice are based on the form and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are utilized in the synthesis of the sound. These physiological attributes of human discourse are invariant for a private, however the movement piece of the discourse of an individual changes after some time because of age, therapeutic conditions, (for example, a normal chilly), and soul, and so on. Voice is moreover not horrendously unmistakable and may not be worthy for huge scale ID. A content region voice acknowledgment framework depends on the announcement of a set preset expression. A content autonomous voice acknowledgment framework recognizes the speaker independent of what she talks. A content free framework is harder to style than a content region framework yet offers extra security against extortion. A problem of voice-based acknowledgment is that discourse choices are touchy to mixed bag of things like foundation sign [4].

L. GAIT

Gait recognition could be a specific mode of biometric remaining to its capability to mark someone at distance. Gait is explained to the approach of the person walking. The step recognition framework use standard camera in any conditions and create calculations to extract the outline of the individual just in the event that he is moving. Accordingly the framework will track the individual after some time. Be that as it may, the algorithmic principle isn't terribly careful for this attribute is stricken by a few conditions like the kind of materials or shoes the singular's porting, the strolling surface or the wellbeing. of these measurements are adequate in distinctive surroundings and none of them is great. However the principal right ones are iris and unique mark strategies. Because of the genuine actuality iris response is unreasonable and it needs boost interest, unique mark is one amongst the most develop insights and suitable for a few applications [10].

M. KEYSTROKE

Keystroke dynamics may be a methodology of corroboratory the identity of associate degree individual by their writing rhythm which might address trained typists moreover because the amateur two-finger employee. Systems will verify the user at the log-on stage or they will regularly monitor the Biometric Systems thirty two employee. These systems ought to be low cost to put in as all that is needed may be a software system package.

III. Literature Review

A. Criminal Investigation and Identification System

Now a day's utmost people's android operating system phones to keep with this, author projected the android application for police furthermore as for peoples. If just in case somebody has not good phones author develop net portal for them. By synchronizing police aspect and public aspect android application they get simple thanks to scale back the crime in society and this method positively facilitates them to form a criminal offense free society. The foremost unimaginable risk for the department of local government is investigation crimes with the present technologies, as a result of they still use standard manual processes to handle crimes that do with the utilization of advanced technologies.

This system facilitates police to spot the criminal by accessing the info of criminal from anywhere; by recognizing his/her thumb impression. Additionally, police broadcast the news if one thing happened wrong within the explicit space and that they wish people's cooperation to handle true. The CI2S additionally facilitate public to register their complaints by victimization app running on their phones. They additionally post there suggestion. Get updated with crime news denote by the police. Not with standing they're not glad with investigation standing of case they're filed they directly contact to the pinnacle officer [11].

Figure 4: Biometric system help police to identify criminal

B. Video Surveillance

Cyrus shahbi (2014) Video system capture human, pose, object, behavior and it's also capture face and detect crime mostly the purpose of video surveillance system to provide crime detail, in the form video, CCTV camera capture video and sent to the database server. Combining image/video data with its corresponding time and location can provide an effective way to index and search videos, especially when a database handles an extensive amount of data in a scalable system. There have been significant researches on organizing and browsing photos according to location and time [12].

C. Online signature for identify document

General purpose pen tablet device should be used as they are widely available and the price is fairly low. A pen contain sensor for sensing the online data and it is connected with the internet. Feedback should be provided either in the form of an immediate LCD response or a simple sheet of paper. The writing area should be controlled by a box, which will fix both maximum size and orientation of the signature. Features are extracted with the Gaussian filtration algorithm method. Euclidean distance measure online signature verification [13].

D. Fingerprint Identification

Barua et al. (2010) defines the Fingerprint identification is one of the most popular and reliable personal biometric identification methods. This paper describes an on-line fingerprint identification system consisting of image acquisition, edge detection, thinning, feature extractor and classifier. The pre-processing part includes steps to acquire binaries and skeleton zed ridges, which are needed for feature point extraction. Feature points (minutia) such as endpoints, bifurcations, and core point are then extracted, followed by false minutia elimination. Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The goal of this project is to develop a complete system for fingerprint identification [14].

E. Ear Based Biometric Recognition

According to Shritosh Kumar (2015), he proposed an Ear Based Biometric Recognition using Gabor Mean Feature Extraction. He suggests Ear Biometric used in Criminal cases, investigation, and security purpose. Gabor filter have a problem of high dimension and high redundancy. Sampling filter is a problem of not reducing features optimum way. In the proposed Gabor feature extraction technique the Gabor features are filtered using proposed mean filter and obtained optimum features for ear biometric dataset. He suggests Ear biometric recognition is one of most biometric identification in which the criminal and terrorist identified [15].

Figure 5: Sample image from AMI Database.

F. Criminal Identification Using Fingerprint and Footprints

Fingerprints and criminal histories of individuals are currently submitted to the database voluntarily by local, state, and federal police agencies. The database currently is home to more than 70 million files in the criminal master file along with more than 31 million civil records [3]. In 2010, the database processed more than 61 million submissions. With all of these records, a typical comprehensive search takes about 27 minutes and a civil search takes about an hour and twelve minutes. Searches for similar prints can now take as little as ten minutes, a process that once took weeks [9]. The use of fingerprints has now expanded far beyond the identification of a corpse and the matching of an unknown print at a crime scene to a suspect [16].

Figure 6: Example of Finger print.

G. Hiring Individual

Private companies, along with most federal and state governmental agencies, use fingerprints in a number of capacities. Most commonly, they are used to help assist in the hiring of individuals and determining if a candidate is well suited for a position within a company. As part of the application and interview process, an increasing number of companies are asking applicants to be fingerprinted as part of a comprehensive background check before hiring [3]. Fingerprints are then sent to an AFIS database, typically the FBI, to be compared to all other prints in the system. This allows a company to know if an applicant has been fingerprinted and entered into the system for any reason, including military service and arrest in connection to a crime. These background checks can often be a deciding factor in whether or not an applicant gets hired. This practice was once only common to governmental hiring, including within the military, police, and other security related positions [16].

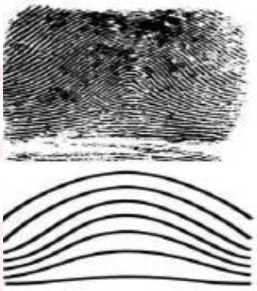

Figure 7: Whorl pattern

H. Biometric Forensics Applications

Given the egregious nature of crimes committed by perpetrators depicted in forensic sketches – including murder, terrorism, sexual assault, and armed robbery – failing to quickly capture them can have severe consequences. Improving forensic sketch recognition would greatly increase public safety. Under the broad umbrella of biometric recognition, another standard has risen for distinguishing suspects utilizing scientific portrayals. A portrayal can be changed over to an advanced picture and afterward consequently coordinated against mugshots and other face pictures in a database – for instance, drivers' permit photographs – to focus a match. This computerized methodology, empowered by advancement in Computer vision and machine learning calculations, can offer a profitable asset to powers looking to precisely and rapidly catch criminal [17].

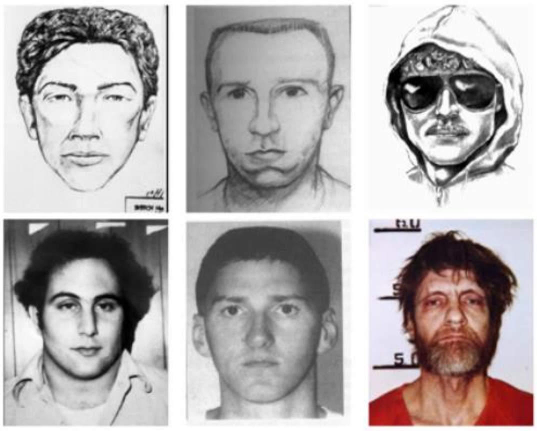

Figure 8: Example of Facial Recognition Using Forensics

I. Cybercrime Attack

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details. Phishing often directs users to enter details in a fake website who's URL, look and feel are almost identical to the legitimate one. Even when using SSL with strong cryptography for server authentication it is practically difficult to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploit the poor usability of current web security systems [18].

J. ATM Security Using Fingerprint Biometric Identification

Amurthy and Redddy developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. Bank United was the first bank in the United States to implement iris recognition at Automated Teller Machines (ATMs) in 1999 [19].

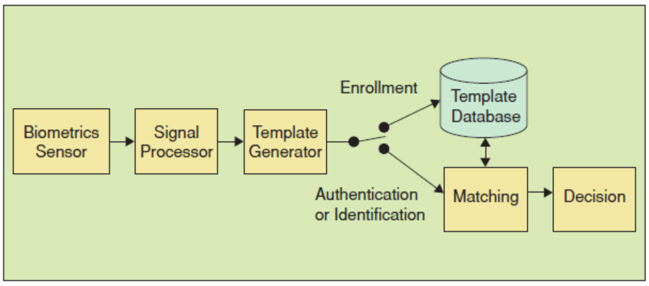

Figure 9: A Generic Biometric System

K. Medical Diagnosis

Jitendra Choudhary (2012) suggest biometric system also used in medical diagnosis e.g. Tongue, color of face and beat of heart and other aspects of our body can also be used as biometrics features or medical diagnosis. Traditional biometric system also used to check level of blood, sugar, and disease in the body. Medical biometric detector widely used in this field to diagnosed disease [10].

L. Face Recognition Technology

A face recognition system is a function of computer technology for repeatedly identifying a person from digital camera or video source. It is the most common testing system of biometric identification; there are two types of face recognition technology e.g. Facial Matric and Eigen Faces. The Eigen Face method is based on group faces according to the degree of it with a fixed set of 100 to 150 eigen faces. The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern demonstrates how distinctive components of a face are singled out. It must be assessed and scored. There will be an example to assess symmetry, if there is any style of facial hair, where the hairline is, or assess the extent of the nose or mouth. Other eigen countenances have designs that are less easy to recognize, and the picture of the eigen face may look almost no like a face. This procedure is truth be told like the police system for making a representation, however the picture preparing is robotized and in view of a genuine picture [20].

M. Biometric ID Card

Finger is scan through biometric identification system and it is based on person to person this is old trend of biometric identification, modern biometric identification in which IRIS, RETINA, Face is used for biometric Id card identification. Information is fetched and stored in National database of the federal government organization. Every person has their own record and it is verified with their own biometric system.

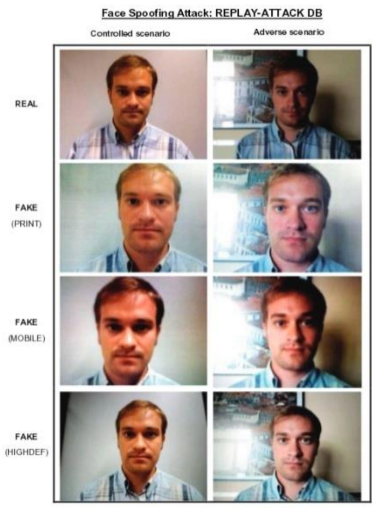

Figure 10: Face Spoofing Attack

N. Biometric Passport/VISA

After the terrorist attacks of 11 September 2001, security concerns played an even more important role in border protection, passport fraud, and forgery for many nations. One way to enhance passport security is to include biometrics the International Civil Aviation Organization has proposed using the face as the primary biometric with fingerprint or iris as an optional secondary measurement [3]. Plans for the new biometric international ID (once in a while known as BioPass or ePassport) ordinarily incorporate an implanted Radio Frequency Identification (RFID) chip conveying the same information that is imprinted on the information page and additionally the travel permit holder's biometric identifiers. While these applications ought to be alter safe, Lukas Grunwald, an advisor with a German security organization, as of late showed the cloning of a biometric identification. The security subtle element Is installed in travel permit and its connection with database framework and it is known as ePassport [21].

O. Biometric Mobile SIM

Mobile device is widely used for communication purpose. Mobile devices used worldwide not only for communication purpose but also for personal affair, relationship, meeting, business, transaction purposes.

Online Mobile banking deeply involved. Tao et al. [9] have developed a biometric system using a user's mobile camera which takes 2D face image to ensure the existence of user. This authentication system consists of 5 modules: face detection, face registration, illumination social control, face authentication and knowledge fusion. The mobile camera initial takes a sequence of pictures for the user so processes them at the mobile's processor. Face detection then species the situation of face within the self-taken photos. Face recognition methodology is that the one within which an individual's face is captured employing a mobile's camera then this face is employed to evidence this human to the mobile. The face recognition authentication makes use one of two ways: 1) shape and location of facial properties such as the eyes, nose, lips and their spatial relationships, or 2) the overall face image [22].

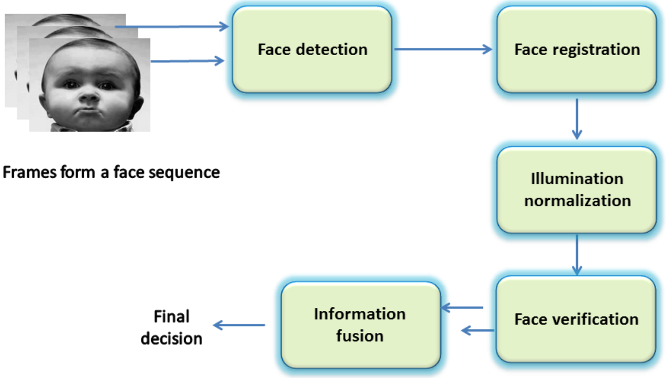

Figure 11: Face recognition system

P. University Attandace System

O. Shoewu(2012) proposed biometric university attendance system in which the system detect fingerprint of the student and stores in a database. The fingerprints matches with the recorded database and the biometric system respond with the recorded feature. Almost 94% accuracy is happened with biometric authentication attendance system [29].

IV. III. Purpose and Objective

A. Identification and Verification

Occasionally confirmation and identification infer as similar terms but they have two separate meanings. Identification occurs when an individual’s characteristic is being selected from a group of stored images. Identification is the way the human brain performs most day to day identifications. For example, if a person encounters a familiar individual, the brain processes the information by comparing what the person is seeing to what is stored in memory.

B. Advantages of Biometric system

The first advantage of using this new technology is the uniqueness and it is also the main characteristic which allows biometrics technology to become more and more important in our lives. With uniqueness of biometrics technology, each individual's identification will be single most effective identification for that user. A chance of two users having the same identification in the biometrics security technology system is nearly zero. the highly secure way of identifying users makes this technology less prone for users to share access to highly sensitive data. For example, users can share their fingerprints, iris and so forth allowing other users access to secure information. Each trait used during identification is a single property of that user. In other words, it is extremely hard or impossible to make duplicate or share biometrics accessing data with other users. This makes it ever more secure allowing user information and data to be kept highly secure from unauthorized users.

This identification of users though biometrics cannot be lost, stolen or forgotten. This aspect of biometrics technology allows it to become more popular in its use. This method of identifying and giving access to user makes user identification a lot easier. Finally, most biometrics security systems are easy to install and it requires small amount of funding for equipment (except modern biometrics technology such as: DNA/retinal/iris recognition [23].

C. Disadvantages of Biometric system

Jain (2006) it still has many fault in its system. Each biometrics application method has disadvantage which can cause problems for its users. For example, if the biometrics security system uses fingerprints to identify its users and an accident causes a user to lose his/her finger then it can be a problem during the verification process. For voice recognition methods, illnesses such as strep throat can make it hard for authorized users to get access to their information. Another factor that can influence voice recognition systems is the continuous aging of its users. Noise in an environment where voice recognition is used to identify its users can also make it hard for users to be identified. For iris or retinal scanning applications, users may find it very intrusive. Users may also have the concern for the safety of their eyes during the iris or retinal scan. Furthermore, databases used to store user identification data will be very large which might form a potential threat. For scanning retinal/iris characteristics and storing large amount of database, biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive. Finally, lots of people are still concerned about biometrics technology in different aspects such as: security, adaptability to rate of change in life, scalability, accuracy, privacy and others [24].

D. Comparison between Face Recognition & Finger Recognition

Face recognition is such a challenging task for researcher and yet to be designed. Researcher have different background e.g. psychology, pattern recognition, neural networks , computer vision and computer graphics. In face recognition technique, Holistic matching methods, feature-based matching, and hybrid method used and tool are used for describe picture modules e.g. principal component analysis, eigen faces. Zhao et al. (1998) which use linear/Fisher discriminate analysis, De Carlo and Metaxas [2000], a system called PersonSpotter was described. This system is able to capture, track, and recognize a person walking toward or passing a stereo CCD camera [25].

Face recognition are the most common biometric technique used by humans to make a personal identification. Its most commonly used in person identification. Identification is based on face is one of the most active areas of research, with applications ranging from the stationary, controlled mug-shot verification to a dynamic unrestrained face recognition in a messy environment. Approaches to face recognition are typically based on location and shape of facial attributes, such as the eyes, eyebrows, nose, lips and chin shape and their spatial relationships. While in fingerprint re recognition human have used fingerprints for personal identification for centuries and the validity of fingerprint identification has been well-established. A fingerprint is the pattern of ridges and furrows on the surface of a fingertip, the formation of which is determined during the fetal period. They are so distinct that even fingerprints of identical twins are different as are the prints on each finger of the same person. The overall analysis of the face image and its break down into a number of canonical faces or a combination. Consequently, fingerprints are expected to lead the biometric applications in the near future, with multiple fingerprints providing sufficient information to allow for large-scale recognition involving millions of identities. One problem with fingerprint technology is its lack of acceptability by a typical user, because fingerprints have traditionally been associated with criminal investigations and police work. One more problem is that automatic fingerprint identification generally requires a large amount of computational resources. Finally, fingerprints of a small fraction of a population may be unsuitable for automatic identification because of genetic, aging, environmental, or occupational reasons. Summarize what is achieved to the study [26].

V. Methodology

For the investigation, the data was carried out from different researches, case study, analysis report and interviews was conducted from different author and professor. The primary data has been collected based on qualitative approach e.g. research paper , case studies and human observation. . The purpose of this research to highlight the causes of biometric identification using different techniques. There is a need in Pakistan to implements because in some sensitive area e.g. sensitive location where there is chance of crime.

The requirement of the research to highlight the problem in Pakistan city e.g. Peshawar, Swat, Quetta, and in FATA Pakistan, in some certain situation when terrorist attacked at public places and how is it possible to identify criminal and terrorist. Video surveillance technique and face recognition and finger recognition technology is the best choice to detect crime and criminal. The extensive research question has been collected from literature. The variable of interest has been collected from literature. The main finding of this research to implement biometric system to detect crime and arrest terrorist in Pakistan.

The requirement of the research to highlight the problem in Pakistan city e.g. Peshawar, Swat, Quetta, and in FATA Pakistan, in some certain situation when terrorist attacked at public places and how is it possible to identify criminal and terrorist. Video surveillance technique and face recognition and finger recognition technology is the best choice to detect crime and criminal. The extensive research question has been collected from literature. The variable of interest has been collected from literature. The main finding of this research to implement biometric system to detect crime and arrest terrorist in Pakistan.

VI. Experiments and Results

A. Experiment & Implementation

Biometric identification system has been implemented in Faisalabad Pakistan for criminal identification. They have been handed 50 mobile biometric scanners to help in crackdowns on insurgency and crime.

City Police Officer (CPO) Faisalabad Afzaal Kausar, who installs the biometric system at Kotwali police station on Thursday, said 10 devices would be placed at entry and exit points of the district. He said the biometric devices would help verify fingerprints and CNICs (Computerized National Identity Card) with the National Database and Registration Authority (NADRA). In May 2015, Sindh province revealed plans to launch a biometric database by June that will collect the fingerprints, photographs and personal crime histories of felons. The biometric data will be managed by the Criminal Record Office of Crime Investigation Agency, chief secretary Muhammad Siddique Memon announced this week at a meeting in the province's capital, Karachi. Developed through cooperation with the National Database Registration Authority, the system will allow every police station access to the record of every criminal [27].

B. Comparative Results

Table 1: Results of Fingerprint-Livedet09

	Comparative Results: Fingerprints-LivDet09								
	Biometrika			CrossMatch			Identix		
	FFR	FGR	HTER	FFR	FGR	HTER	FFR	FGR	HTER
IQA-Based	14.0	11.6	12.8	8.6	12.8	10.7	1.1	1.4	1.2
Best LiveDet09[10]	15.6	20.7	18.2	7.4	11.4	9.4	2.7	2.8	2.8
Marasco et al.[28] reported in	12.2	13.0	12.6	17.4	12.9	15.2	8.3	11.0	9.7
Moon et al [22] reported in [21]	20.8	25.0	23.0	27.4	19.6	23.5	74.7	1.6	38.2
Nikam et al. reported in [27]	14.3	42.3	28.3	19.0	18.4	18.7	23.7	37.0	30.3
Abhyankar et al [28] reported	24.2	39.2	31.7	39.7	31.5	31.5	48.4	46.0	47.2
Av. Exec (s)	0.169			0.231			0.368		

.

Table 2: Result of Face Replay Attack DB

	Results: Face Replay- Attack DB											
	Print			Mobile			Highdef			Grandtest		
Head	FFR	FGR	HTER	FFR	FGR	HTER	FFR	GRR	HTER	FFR	FGR	HTER
Fixed	13.6	5.0	9.3	1.9	3.7	2.8	15.6	10.5	13.1	19.6	11.3	15.4
All	11.5	5.3	8.4	2.8	4.1	3.5	8.4	9.9	9.1	13.7	11.7	12.7
	11.6	4.1	7.9	2.4	3.9	3.2	14.0	10.2	12.1	17.9	12.5	15.2
Av. Exec	0.148			1.150			1.147					

C. Discussion

Facial recognition and identifying suspects in the Boston Marathon bombing:

The investigation nearby the Boston Marathon bombings was an overlook opportunity for automated facial recognition to assist law enforcement in identifying suspects. After reviewing "photo, video, and other evidence" the FBI released images and videos of the two suspects. In addition to seeking identification help, the release of the images and videos was also in part to limit the damage being done to people wrongly targeted as suspects by news and social media. Shortly after the release, the two suspects were identified as brothers, Tamerlan Tsarnaev and Dzhokhar Tsarnaev, by their aunt who made a call to the FBI tip line "The feasibility of facial recognition is always determined by pose and illumination, so it works best when someone is looking straight at the camera and the illumination is right," Jim Albers, Senior Vice President of Government Operations for MorphoTrust USA said. "Therefore in surveillance situations where people are not drawn to look at the camera, you have difficulties in using facial recognition," [28].

Dr. Brian Martin, MorphoTrust USA's Director of Research, who specializes in facial recognition, says the algorithms developed over the last 15 years have been trained to match faces looking at the camera, and at times, require digital compensation. "When you have poor quality data, face recognition is better used as a tool to generate leads," Martin said. According to Paul Schuepp, CEO and President of Animetrics, a firm which specializes in face recognition and 2D-to-3D visualizations, Smartphone's have increasingly powerful on-board cameras and can often produce valuable images for facial analysis. "Cell phones are great because the cameras have very high resolution," Schuepp said. "The problem does get into the wide angle aspect ratio [of smartphone cameras] which can distort faces a little bit. If they are too close to the face, you see the wide angle effect."

"Pose is one thing and because of our technology, we can mitigate the pose, but to make the three-dimensional model of the face for accurate comparison, you need the information of the face that is useful," Schuepp said. "You really need to get upwards of 65 pixels between the eye centers, for enough resolution to give you a good statistical comparison." The biometric expert state that while there have been major successes in terms of biometrics solving major crimes such as facial recognition helping identify one of the 2013 Boston bombers that the two fields need to come closer to meet the challenge of solving crimes.

VII. Conclusion

This research paper concludes with the most advanced biometric technology e.g. face recognition and finger identification. The biometric technology helps the police crime branch to identify criminal and terrorist. Iris recognition is very complicated because there is a chance to effect badly. DNA recognition play a significant role in these days. Crimes and criminal activities increased day by day and in Pakistan there are largest cities e.g. Karachi, Peshawar and Quetta where there is crime occurred, there is a need to implement biometric scanner to scan criminal at the gateway of these cities.

VIII. References

[1]. Reham Amin et al. Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues Tarek Gabor July 2015.

[2]. Anil K. Jain, Ajay Kumar Biometrics of Next Generation: An Overview 'SECOND GENERATION BIOMETRICS' SPRINGER, 2010.

[3]. ARULALAN.V, BALAMURUGAN.G A Survey on Biometric Recognition Techniques International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

[4]. Anil K. Jain, An Introduction to Biometric Recognition IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.

[5]. Ajay Kumar1, David C. M. Wong1 Personal Verification using Palmprint and Hand Geometry Biometric Pattern Recognition and Image Processing Lab, 2006.

[6]. ARULALAN.V1, BALAMURUGAN A Survey on Biometric Recognition Techniques International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

[7]. Damien Dessimoz Multimodal Biometrics for Identity Documents Research Report PFS 341-08.05 (Version 2.0) June 2006.

[8]. Anil K. Jain, Ajay Kumar Biometrics of Next Generation: An Overview 'SECOND GENERATION BIOMETRICS' SPRINGER, 2010.

[9]. ARULALAN.V1, BALAMURUGAN A Survey on Biometric Recognition Techniques International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.

[10]. Jitendra Choudhary, Survey of Different Biometrics Techniques, International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol. 2, Issue. 5, Sep.-Oct. 2012 pp-3150-155.

[11]. Saurabh Zadikar1 et al. Criminal Investigation & Identification System (CI2S) IJCSMC, Vol. 4, Issue. 2, February 2015, pg.402 – 407

[12]. Cyrus Shahabi et al. Multi Source Event Detection and Collection System for Effective Surveillance of Criminal Activity. J Inf Process Syst, Vol.10, No.1, pp.1~22, March 2014.

[13]. C. S. Chua and R. Jarvis, "Point signatures: A new representation for 3D object recognition," International Journal of Computer Vision, vol. 271,pp. 63–85, 1997]

[14]. Barua K., Bhattacharya S., "Fingerprint Identification", Global Journal of Computer Science & Technology, Vol. 11 (Issue 1), (Apr 2011).

[15]. Shritosh Kumar, Vishal Shrivastav, Performance of Gabor Mean Feature Extraction Techniques for Ear Biometric Recognition. International Journal of Informative & Futuristic Research Vol 2, Issue 2, 2015.

[16]. Amandeep Singh Dhillon, Ashok Kumar Bathla, Approaches for Finding Correlation Between Fingerprints and Footprints of a Person, Journal of Information Sciences and Computing Technologies. Vol 1, Issue 1, December 2014.

[17]. Anil K. Jain* and Arun Ross, Bridging the Gap: From Biometrics to Forensics, Philosophical

Transactions of The Royal Society B, 2015.

[18]. M.Loganathan, Dr.E.Kirubakaran, A Study on Cyber Crimes and protection, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011 ISSN (Online): 1694-0814.

[19]. N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[20]. Debnath Bhattacharyya, Rahul Ranjan, Biometric Authentication: A Review , International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009.

[21]. Qinghan Xiao Defense Research, Biometrics—Technology, Application, Challenge, and Computational Intelligence Solutions, Technology Review, Defense Research and Dev Canada.

[22]. Qian, T., Raymond, V.: Biometric authentication system on mobile personal devices. Instrumentation And Measurement, IEEE Transactions on 59(4) (2010)763{773]

[23]. Tistarelli, 2009 Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743]

[24]. Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125 - 143

[25]. W. ZHAO, R. CHELLAPPA, Face Recognition: A Literature Survey, ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399–458.

[26]. Anil Jain, Lin Hong, and Sharath Pankanti, BIOMETRIC IDENTIFICATION,COMMUNICATIONS OF THE ACM February 2000/Vol. 43, No. 2

[27]. http://www.planetbiometrics.com/article-details/i/3235/desc/pakistan-police-handed-50-mobile-biometric-scanners/#sthash.YXJyB2kQ.dpuf]

[28]. Joshua C. Klontz, Anil K. Jain, A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects Technical Report MSU-CSE-13-4 May 22, 2013

[29]. O. Shoewu, Ph.D. and O.A. Idowu, B.Sc. Development of Attendance Management System using Biometrics, The Pacific Journal of Science and Technology – Volume 13. Number 1. May 2012 (Spring).

Association of Research Scholars
IARS
Transforming Research
Since 2011