

# Student Perception about the Use of Biometrics Technologies in an Academic Environment of Abdul Wali Khan University Mardan Pakistan

Fazal Hadi<sup>a</sup>, Ahmad Ullah<sup>b</sup>, Muhammad Haris<sup>c</sup>, Yasir Shah<sup>d</sup>

<sup>a b c d</sup> Abdul Wali Khan University Pakistan,

<sup>a</sup> Email: shahge9710@gmail.com

<sup>b</sup> Email: ahmadullahkhan249@gmail.com

<sup>c</sup> Email: csmharis@gmail.com

<sup>d</sup> Email: yasirshahbcs@gmail.com

## Abstract:

Security has been a critical issue always in life. In general allowing access of authorize people or to block unauthorized people to specific domain is known as security. Biometric are tools used for identification purposes. This survey is about the student perception of biometric technologies particularly "voice recognition, hand geometry, iris recognition, face recognition" and its suitability in an academic environment and the privacy concerns that arise from using these technologies. Because privacy is also one of most important concern for humanism. In this paper we compare and analyze different biometric techniques on the basis of cost, merits, accuracy and their shortcomings. Furthermore this survey provides the role of government in establishing laws and standards for such technologies that are briefly discussed. Moreover the public trust has a keen importance in implementing such technologies.

**Keywords:** Biometrics tools; Privacy; Security;

## Introduction :

Biometrics is considered as an advance tool for solution of recognition and authentication problems in the different fields of life. For example in the physical and computer security of immigration and custom department. It can be defined as "one or more unique physiological human characteristics" [1]. The shape of a body, finger prints, structure of the face, iris patterns and even odor recognition. Different behavior characters' can also be recycled like voice style and typing. This technology is unlike the existing methods of passwords and cards and it can never be forgotten [2] or lost copy [3] is the great promise of it [4]. Biometrics is increasing potential for the post

9/11. Biometrics methods are fast, reliable, accurate, in addition to the growing needs for security. This technology recently to day activities due to the application of high-profile entertainment, media and the public began to enter the consciousness. We know that when new solutions are discovered so there arise some side effects. The study of conditions that affect the use of biometrics for identification was conducted [4]. The automatic recognition of a person on the base of his or her physiological or behavioral characteristics refers to Biometrics. It contains iris, fingerprint, facial and retinal reliable security. Expensive collection of most secure verification and personal identification solutions are based on these technologies. Based on biometric techniques, in recent years to recognize people as the most promising option emerged, in its place of authenticating individuals and granting them access In setting forth the physical and virtual i-e smart cards, passwords, tokens, plastic cards, pins, keys and access to the domain based on these methods to determine and / or to determine the identity of an individual's physical and / or behavioral check features. Identification numbers and Personal Passwords are difficult to remember [5]; it can be pinched or predicted. Keys, codes, Cards, can be misplaced, forgotten, Voyeur or recurrence. Magnetic cards can become degraded and unreadable However, the qualities of biological individual cannot be misplaced, forgotten, stolen or forged. Includes tools of proof of identity based on biological features like the iris and fingerprints, engineering finger, hand structures, and the veins of the hand, palm, and face, retina of the eye, ear, sound and behavioral characteristics like walking, The autograph and the subtleties of the keys face looks recognition to offer many advantages compared with other vital roads, and some of them are listed below: In short all of those techniques need certain volunteer work by the consumer, any

user desires to put his hand on the hand and the reaming to take fingerprints or hand structures detect and contain to site in a fixed position in opposite of the detecting device for iris or determine the finger prints. On the other hand, it can be a negative is face recognition without taking any unambiguous inaction or involvement on the part of the consumer since the facial imageries can be obtained since distant by camera distance. It is useful mostly for the purposes of security and scrutiny. Moreover, access to information in general is anxious with other problems. Biometrics practices that trust on the fingers and hands can turn out to be useless in the case of skin flesh damage in some way (any bruises or fractured). Retinal and Iris credentials require costly apparatus and there are a lot very delicate to any movement of the body. Voice appreciation is vulnerable to noise present in background in communal places audio and volatility especially on the phone line or tape recording. Autographs can be changed or copied. But, facial pictures that would be found easily with two fixed cameras low-cost [2].

### 1. Literature Review.

Different researchers have worked on biometrics like the perception of the teachers and students about biometrics by Wafi AlBalawi in 2004. He concluded the following points: (i) "There is an actual privacy anxiety amongst teachers and students about putting into practice biometric tools; (ii) Religious anxieties were not a matter on behalf of the research members" [6]. His Research proposes that a public consciousness movement follow attention of biometric equipment execution. In 2010 Thamer Alhussain and Steve Drew worked on "employees' Perceptions of Biometric technology adoption in e-Government". An outcome of his learning specifies "an important arithmetical, traditional cavity among the hi-tech alertness of Staffs and the favored verification explanations sponsored by organization. An absence of reliance in tools, it's prospective for abuse and administration reasons return the executives' essential to think through their farm duties for tapering these breaches". He recommends that orientation Process and awareness almost biometrics must proceeds place earlier the introduction of technology is in any organization [7]. "Exploration of factors affecting adoption of biometric technology by five-star Egyptian hotel employees" by Ahmed Moustafa Abdelbary in University of Iowa State in 2011 .The outcome of his research encourages the hotel management to plan for training programs before the implementation of biometrics. The training

should focus on the benefits and value-added which seemed to be a major driver and factor mentioned by the participants as a possible motivator for adoption or use for a device. His research suggests that a close collaboration between universities in Egypt and the U.S. could improve access to data and employees to gather information and allow better understanding [8]. In this paper we have tried to identify those biometrics technologies that are acceptable and suitable for use in academic environments.

### 2. Research Method

Questionnaire was conducted to provide more comprehensive analysis and collecting of large amount of data in a standardized way in limited time [1] [2]. More than 500 hundred students of Abdul wali khan University Mardan KPK Pakistan, of varying educational backgrounds and demographics almost 40 percent female and 60 percent male students participated. Questions were related to the use of biometrics technology in the academic environment and the ratio of these technologies. Furthermore general merits and demerits were studied and analyzed. We have performed a pilot study prior to actual distribution of the questionnaire to advance the questions and define its content weight, assess clarity, readability, and time for completion. The people of the test study were a collection of graduate pupils and teachers of Abdul wali khan university mardan. We picked a suitable group of pupils and tutors to contribute in the experimental study; twenty students and five tutors contributed in the pilot revision. We deliberated diverse norms when we took the contestants; for example, contestants' familiarity, race and their sexual category.

### Analysis and Discussions.

In this section we will analyze discuss the results we have obtained from our questionnaire.

**2.1. Question no 1:**

What is your gender in the following options?

The graph shows the number of participants on the basis of gender. The percentages of males were 70 percent while the rest 30 percent were females of total participants. The no of female students is low because the female education is less compare to male students.

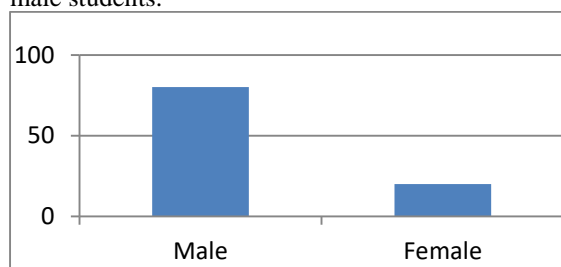


Fig.1 Ratio of male and female participants in servay **4.2 Question no 2:**

Do you know about the biometrics technologies?

More than 80 percent of the students were belonging to the computer science department so they were aware of biometrics technologies and about 20 percent of the students were belonging to other departments having not enough knowledge about these technologies. The following graph shows the number of selected options.

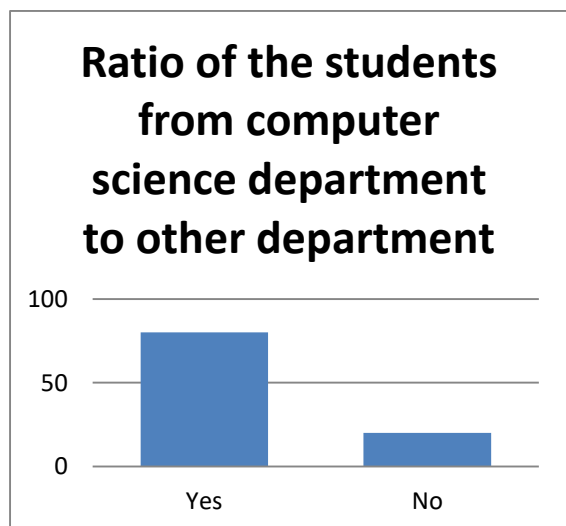


Fig. 2 Ratio of students from computer science to other departments

**4.3 Question no 3:**

Which of the following biometric technologies you prefer for using in an academic environment?

- (i) Iris recognition (ii) face recognition (iii) voice recognition (iv) Hand geometry

About 70 percent students prefer face recognition technologies in an academic environment as opposed to other biometric technologies such as iris scan 10 percent, hand geometry 10 percent and voice recognition 10 percent.

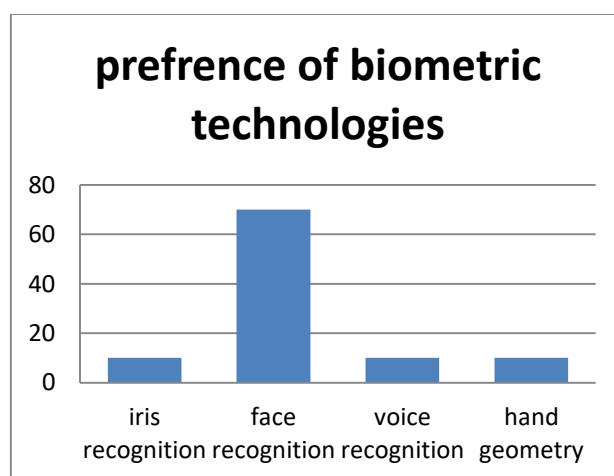


Fig. 3 priority ratio of different biometrics technology

Some of the reasons why students prefer using face recognition as compared to other available biometric technologies.

**4.3.1 The shortcomings of other biometrics W.R.T**

**Facial recognition:**

Facial recognition technology is very cheap as to the remaining biometric technologies. It has a low error rate of 1 in the 100. It is user friendly technology [3].The shortcomings of Voice recognition are “Recording of Human voice is possible so it would be utilized by an illegal person, party easily. It has a low rate of accuracy i.e. if a person has an illness like cold can change his voice, which causes the identification difficult or impossible [4]. May hacked with prerecorded voice messages. Several words have similar sound.

For example two, to, too. It's have huge cost [5]. Iris recognition technology have the demerits like: A lot of memory for storing the data is required. So it cost becomes large. Iris input devices could be fooled simply by a high class picture of an iris in its place of the actual object. There is a large impact of uncommon lights and brilliance from diverse reflective sorts of planes on the accuracy of iris scanning devices. Different disease i-e diabetes or little other severe illness can create variations in Iris scans [4]. The performance of finger prints can be affected by the dirtiness or dryness of the skin of a finger with the passage of time. It is not suitable for youngsters, for the reason that their fingerprints varies quickly. Picture taken at "500 dots / inch (dpi). Perseverance is 8 bit/pixel. Image of 500 dpi of a fingerprint taken at 8 bits/pixel needs a huge space in memory, 240 Kbytes roughly, Compression mandatory (a factor of 10 around)" [4]. Hand geometry is also an example of biometrics technology still it has some limitations like: it is also Very expensive and has extensive size. It is not valid for special individuals, because they are unable to put their hands on the scanner correctly [6].

#### **4.3.2 Comparison with other technologies:**

May be the Facial recognition would not be the best effective and reliable, among the different biometric techniques. But, one of the important advantages is that "it does not have need of collaboration of the experiment substance to work". Appropriately planned systems set up in "multiplexes, airports, and other civic places can classify entities amongst the gathering, lacking passers-by even being alert of the system". Further most biometrics like "voice, iris, and fingerprints recognition" is not able to carry out this type of huge recognition. On the other hand, there are some queries have been elevated on the facial recognition software efficiency in case security i-e of railways and airports [7].

#### **4.3.3 Face recognition technologies are famous among students due to:**

The most natural biological characteristics recognition technology is Face recognition

agreeing to the perceptive rule of humans [8]; the algorithm of fingerprint is ten times easy than face algorithm. Face appreciation is contained by the next merits associated to fingerprint. "Dual Sensor" is an Industrial Leading Face identification Algorithm, enough other facts than fingerprint [9]. FAR<0.0001%. Several up and around to "1400 consumers fewer than 1 second". Letdown to join and gain frequency is "less than 0.0001%", fingerprint equipment will have difficulties on behalf of acceptance "with desquamation, wet, cold, elder, about 5% individuals cannot become join up with fingerprint technology. Photo taken by camera is able to track can Incident from security point [10], no evidence are present in fingerprint technology for tracking such incidents". Contactless verifications for the eventual aseptic [11] after the understanding of how face scanning biometrics operates, any one should surprise almost in what way one of these biometric members of staff time clocks could give advantage to enterprise. A list of the top profits any one can like when they put in a facial time attending and tracing system. A great benefit of the use of biometric schemes face [12] that in the enterprise is boss will not have any anxiety about cheating time. Difficult for stamping companion to happen, because everybody that have gone through biometric scanning devices in time to face. Boss will always enjoy better facial biometrics system security. Boss can not only keep record of staffs through biometric time tracking presence, however, every visitor to the system can track across the region also added. Anyone who does not exist in the scheme cannot be granted right to use. Numerous firms, such as the fact is that the biometric scanning system is the mechanism. No one will have to fear about someone for monitoring the system seven days a week and 24 hours a day. Biometric facial integrated easy-to-program systems in your system in your computer companies as well. Usually it would operate with the programs in your existing place. Now a day's Facial biometrics technologies got a high success rate, specifically with the advent of 3D facial scanning technology. Cheating the system is particularly difficult, that's why anyone can feel safe knowing that biometrics' computer security scheme and you should be successful in track time

and presence with provided that superior security [10] [13]. Some of the students give their comments that face recognition is cheap and can process large number of images in little amount of time. And the error rate is also acceptable in this type of environments.

**4.4 Question no 4:**

Are Biometric technologies violating the laws of privacy?

(1)Yes (2) no (3) may be.

Most of the students (80 percent) select “yes” .some (15 percent) selects “no” only 5 percent select the “may be” option. The graph shows the number of selected options.

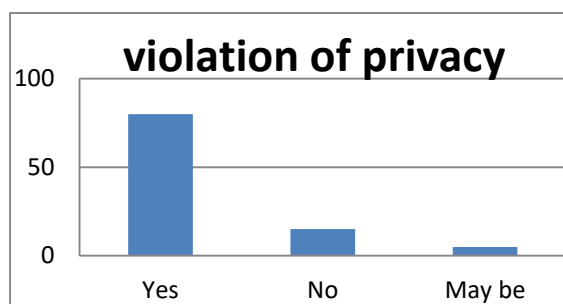


Fig. 4 violation of privacy

**4.4.1 Privacy problems:**

Organizations of Civic rights and privacy supporters like the Electronic frontier foundation and the American civil liberties union says about the worry that “using of surveillance technologies privacy is being compromised, few are worried that it may lead to a “society totally under surveillance,” by which the government and other higher ruling classes having the ability to trace all citizens activities any time. Criticizing the lawful exercise of citizen rights in office like government policies and corporate practices, knowledge has been continuing for its prevention”. Some of the privileges granted to the center authorities for access, maintain and control of economic and political apparatus are misused, they should restrict the general changes. Facial recognition cannot be utilized only to recognize a person; however it also uncovers additional private data related with a person. Such as other pictures containing the personal, “social networking profiles, blog posts, Internet activities, tourism arrangements, etc.” All through facial scrub features by you. Furthermore, people have partial capability to sidestep or prevent face identification tracing if they cover their own

faces. This basically varies the dynamic of daily privacy by allowing any “seller, administration agencies, or arbitrary foreigner can collect the identities and related personal data of any person captured by the face recognition system secretly”. Web sites Social media i-e twitter, Face book have a huge amount of pictures of general public, marked with names. This signifies a databank which might be possibly used (or ill-treated) by administrations for the purposes of facial recognition. A hearing was held in July 2012 before the subcommittee on technologies, privacy and the laws on the judiciary of the committee, united states senate for addressing the problem and issues surrounding that how a facial biometrics technology means for civil liberties and privacy” [14] [15].

**4.5 Question no 5:**

It is necessary for Government to define laws/acts related to use of biometrics technologies in public place /govt organization?.

(1)Agree (2) Strongly Agree (3) Disagree (4) strongly disagree.

The graph of this question is given below:

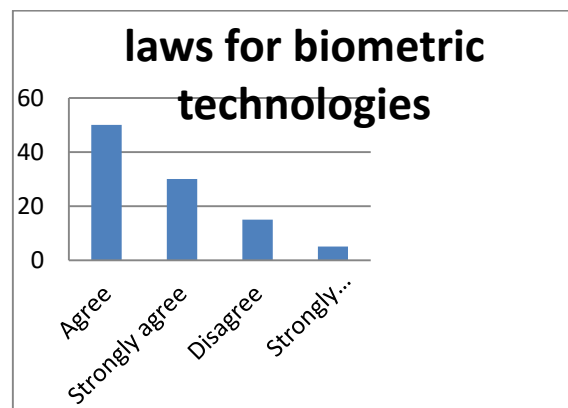


Fig. 5 Establishment of Laws

Most of the students (50 percent) were agree, about 30 percent were strongly agree,15 percent were disagree and 5 percent were strongly disagree with this statement .because they knew the ethical concerns of using these technologies like privacy etc. Mostly students feel that government have the title role to play in the usage of biometrics tools [16] since it allows the key charge for the ensuring of the citizens privacy & security. Some feel that administration should make the standards for using these technologies; some people think that it might

support development and research financially. This survey was conducted in Pakistan so when we search government laws for the usage of these technologies there are no clear laws because these technologies are not used in large numbers. So we are comparing the US laws like “**The Privacy Act of Protection and Freedom of Information**” which protects the individual privacy right [17]. And the presidential directive for the usage of biometrics as follows:

#### **4.5.1 National Security Presidential Directive and Homeland Security Presidential Directives;**

A frame work is established by this directive for ensuring of executive agencies and developments of federal authorities use compatible mutual procedures and methods in the collection, use, storage, sharing and analysis of biometrics related contextual and biographic data of the people in a legal and suitable method. Although taking care of their data privacy and remaining lawful rights comes under the law of USA” [18]. There are some of the standards for biometrics like **ISO/IEC Biometric Standards** related to privacy.

#### **ISO/IEC TR 24741:2007**

These standards are the unite of a huge set formed under the supervision of the main International authorities i-e Joint Technical Committee, International Electro technical Commission, international Organization for Standardization [19]. The aim of such a huge collection of criterions is for the support of biometric technologies standardization, relating to humans furthermore to support compatibility and exchange of data between authorities, systems, and applications [14]. The collection of standards is possibly the utmost inclusive to era; more than 40 standards are issued and further are being printed. The sponsor of ISO/IEC JTC 1 SC 37 is Canada, “Harmonized Biometric Vocabulary and Definitions which is the unit of ISO/IEC TR 24741:2007 [19] categories are also sponsored by Canada. It should also be noted that in the United States, furthermore the American National Standards Institute (ANSI) in USA also sponsor to the category of Biometric Testing and Reporting i-e ISO/IEC JTC 1 SC 37”. NIST works narrowly with ANSI and NIST mutually works for the development of biometrics standards, provided that preferred real-world professionals.

#### **4.6 Question no 6:**

What is your preference while using Biometrics in public places/Govt organization?

#### (1) Security (2) privacy

Most of the students prefer the security while using these technologies. There are some factors like terrorism and other security threats in that area where we have conducted this survey. Therefore, they prefer to use biometrics for security any way to violate the privacy laws. Because these areas are greatly affected by the war against the terrorism. I want to discuss the recent terrorist attacks in Khyber pukhtunkhwa Pakistan. “In 13 February 2015 three suicide bombers attacked on shia’s worship place (Imambargah) in phase-5 Hayatabad in Peshawar the capital city of KPK in which 22 people were killed and 50 were injured. In 16 December 2014 a school named “Army Public School (APS)” was attacked by terrorists and they killed 3 soldiers of Pakistan Army, principal of the school, more than 135 students and 10 teachers of that school were killed. In this regard, the government decided to start the punishment of hanging to death in the country. This punishment was stopped unofficially by Asif ali zardari the president of Pakistan in 2008. After starting execution on the moratorium, 24 people which were in prisons have been hanged to death. It also includes two prisoners who had no relation with terrorists. More than 65 prisoners in which 15 terrorists, 4 security forces and 36 civilians have been killed in connection with terrorists’ related violence till February 2015 according to a report of “(SATP) terrorism portal of south Asia”. Furthermore in 2014, 156 lives are lost including 103 general public, 41 security forces soldiers and 12 terrorists. The government of KPK has recorded the life loss more than 617 containing 108 security forces soldiers, 406 civilians and 104 militants since 2010 to 2012. The sum of life loss in 2013 was 936 recorded i-e 162 terrorists, 172 security soldiers and 406 of public people. Other major violence parameters like suicides, explosions and major incidents rate remained less in 2014. 49 major violence incidents which involve 5 to 7 or more deaths results of 435 lives lost are accounted by KPK province in 2014. In addition no of attacks were 65 causing 694 lives lost, compared to 22 attacks of suicide led to 635 injuries and 350 deaths in the year of 2013. Moreover nine attacks were registered causing 250 injuries and 196 deaths in 2014 [20]. The graph shows the numbers of selected options:

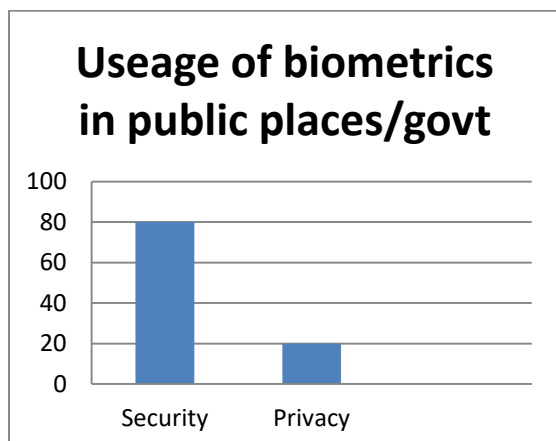


Fig. 6 usage ratio in organizations.

So many students (80 percent) add their comments that the security is the critical issue so these technologies should be used for it no matter if they violate the privacy rights of some one. But still some students (20 percent) stated as “the privacy is the basic right of an individual so it should be protected under the government laws and rules” According to the patriot act 2001 the federal law enforcement agencies have the power to access your personal information or violate your privacy right without any court order. This act is so controversial but it for the sake of the protection of US from the terrorist attacks it is still implemented in USA. So in this type of situation any way if some one’s right is violated.

## 5. MERITS AND DEMERITS OF BIOMETRICS TECHNOLOGIES;

Greatest benefit of biometric technologies is to enhance security, tracked by accurateness, and additional profits i-e irreplaceable characteristic which cannot be shared, misplaced or copied, paperwork can be reduced conveniently by this way. However the costs of implementation are one of the supreme shortcomings.

## 6. CONCLUSION

When new technologies are introduced, they bring some problems as well. The outcome of our study indicates “that few people don’t want to adopt biometric techniques due to the impact of safety and personal privacy. However they are completely aware of its benefits. Moreover these technologies involve the biographic features of individuals so

business communities and government should take care of public trust. Security concerns are arising day-to-day so the needs of biometrics become compulsory. Educational institutions, private corporates and government all of them are responsible for the refining and encouraging the use of these technologies through education, dissemination, knowledge, reliability and established standards.

## References

- [1] "questionnaire," 3 9 2015. [Online]. Available: <http://www.evalued.bcu.ac.uk/tutorial/4a.html>.
- [2] "questionnaire-info," 4 9 2015. [Online]. Available: [www.icbl.hw.ac.uk/ltidi/cookbook/info\\_questionnaires](http://www.icbl.hw.ac.uk/ltidi/cookbook/info_questionnaires).
- [3] Mohammed Javed, Bhaskar Gupta, "Performance Comparison of Various Face Detection Techniques," *International Journal of Scientific Research Engineering & Technology*, pp. 019-0027, 2013.
- [4] "disatvantages of biometrics," 12 05 2015. [Online]. Available: [www.sciencepublication.org](http://www.sciencepublication.org).
- [5] rupinder saini, narinder rana rayat, "comprision of various biometrics methods," *international journal of advances in science and technology*, 2014.
- [6] "disadvantages of biometric technologies," 12 07 2015. [Online]. Available: <http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies>.
- [7] "facial recognitionsystem advantages and disadvantages," 17 05 2015. [Online]. Available: [http://en.wikipedia.org/wiki/Facial\\_recognition\\_system\\_Advantages\\_and\\_disadvantages](http://en.wikipedia.org/wiki/Facial_recognition_system_Advantages_and_disadvantages).
- [8] Urvashi Bakshi, Rohit Singhal, "A SURVEY ON FACE DETECTION METHODS AND FEATURE EXTRACTION TECHNIQUES OF FACE RECOGNITION," *International Journal of Emerging Trends & Technology in Computer Science*, 2014.
- [9] Rajkiran Kaur, Rachna Rajput,, "Face recognition and its various techniques: a review," *International Journal of Science Engineering and Technology Research*, 2014.
- [10] Riddhi Patel, Shruti B. Yagnik, "A Literature Survey on Face Recognition Techniques," *international journal of computer trends and technology*, 2013.
- [11] "features of facial recognition," 15 3 2015. [Online]. Available: <http://www.hanvon.com/en/products/FaceID/downloads/FAQ.html>.
- [12] Jyoti S. Bedre ,Shubhangi Sapkal,, " Comparative Study of Face Recognition Techniques: A Review", *Emerging Trends in Computer Science and Information Technology*, *international journal of computer application*, 2012.
- [13] Jigar M. Pandya, Devang Rathod, Jigna J. Jadav., "A Survey of Face Recognition approach," *International Journal of Engineering Research and Applications*, pp. 632-635, 2013.
- [14] "missourians amended the missouri constition," 1 5 2015. [Online]. Available: <http://www.aclu-mo.org/legislation/2014-privacy-bills/vote-yes-on-amendment-9/>.
- [15] "civil liberties," 5 8 2015. [Online]. Available: [http://www.Brainyquote.com/quotes/keywords/civil\\_liberties.html](http://www.Brainyquote.com/quotes/keywords/civil_liberties.html)



- [16] "Identifying Legal Concerns in the Biometric Context," *journal of international commercial law and technology*, 2008.
- [17] "freedom of information and privacy protection of privacy act," 30 10 2009. [Online]. Available: <http://foip.alberta.ca>.
- [18] "national security presidential directive homeland security presidential directive," 12 5 2015. [Online]. Available: <http://www.TheWhiteHouse.com> .
- [19] "information technology biometrics tutorial ISO/IECTR24741," 12 6 2015. [Online]. Available: [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=38851](http://www.iso.org/iso/catalogue_detail.htm?csnumber=38851).
- [20] "recent attacks in pakistan, khyber pakhtunkhwa assessment-2015," 2 6 2015. [Online]. Available: <http://www.satp.org/satporgtp/countries/pakistan/nwfp/index.html> .
- [21] James, T., Pirim, T., Boswell, K., Reithel, B., Barkhi,, "Determining the intention to use biometric devices : an application & extension of the technology acceptance model," *Journal of organizational and end user computing*, pp. 1-25, 2006.
- [22] rabia jafri,hamid r.arabnia, "A survey of face recognition techniques," *journal of information processing systems*, 2009.
- [23] vivian chu,gayathri rajendran, "use of biometrics," *techcast article series*, 2009.
- [24] w. albalawi, "students and instructors attitudes toward using biometric techonology as an identification method in online courses," college of human resources and education at west virginia university, 2004.
- [25] thamer alhussain griffith,steve drew, "Employees' Perceptions of Biometric technology adoption in e-Government: an exploratory study in the kingdom of Saudi Arabia," *international journal of E-adoption*, pp. 59-71, 2010.
- [26] adelbary,ahmed moustafa, "exploration of factors affecting adoption of biometric technology by five-star egyptain hotel employees," 2011.