A Survey of Biometrics Security Systems

Chien Le, chienqle@go.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download

Abstract:

In today's society, advances in technology have made life easier by providing us with higher levels of knowledge through the invention of different devices. However, each technological innovation harbors the potential of hidden threats to its users. One major threat is theft of private personal data and information. As digital data become more prevalent, users try to secure their information with highly encrypted passwords and ID cards. However, the misuse and theft of these security measures are also on the rise. T aking advantage of security flaws in ID cards result in cards being duplicated or counterfeited and being misused. This increasing battle with cyber security has led to the birth of biometric security systems. Outlining the main differences between the methods of biometric technology used to verify user identities will shed light on the advantages and disadvantages of personal data security systems.

Keyword:

Biometric, biometric security system, biometrics concerns, recognition methods, identification, access control, facial recognition, fingerprint reader, voice recognition, iris/retinal recognition, vein recognition, DNA recognition, privacy, safety.

Table of Contents:

1-Introduction to Biometrics and Biometrics Security System

A brief background of biometric and biometric security systems will provide a greater understanding of the concept of network security. Biometrics is defined as the unique (personal) physical/logical characteristics or traits of human body [Jain, 2004]. These characteristics and traits are used to identify each human. Any details of the human body which differs from one human to other will be used as unique biometric data to serve as that person's unique identification (ID), such as: retinal, iris, fingerprint, palm print and DNA. Biometric systems will collect and store this data in order to use it for verifying personal identity. The combination of biometric data systems and biometrics recognition/ identification technologies creates the biometric security systems. The biometric security system is a lock and capture mechanism to control access to specific data. In order to access the biometric security system, an individual will need to provide their unique characteristics or traits which will be matched to a database in the system. If there is a match, the locking system will provide access to the data for the user. The locking and capturing system will activate and record information of users who accessed the data. The relationship between the biometric and biometric security system is also known as the lock and key system. The biometrics security system is the lock and biometrics is the key to open that lock [Jain, 2006].

There are seven basic criteria for biometric security system: uniqueness, universality, permanence, collectability, performance, acceptability and circumvention [Schuckers, 2001]. As mentioned above, uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users. For instance, the DNA of each person is unique and it is impossible to replicate. Universality is the secondary criteria for the biometric security. This parameter indicates requirements for unique characteristics of each person in the world, which cannot be replicated. For example, retinal and iris are characteristics will satisfy this requirement. Thirdly, a permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will mostly be affected by the age of the user. Following the permanence parameter is the collectability. The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification. Then, performance is the next parameter for the system which outlines how well the security system works. The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable. Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of the verification process [Maestre, 2009].

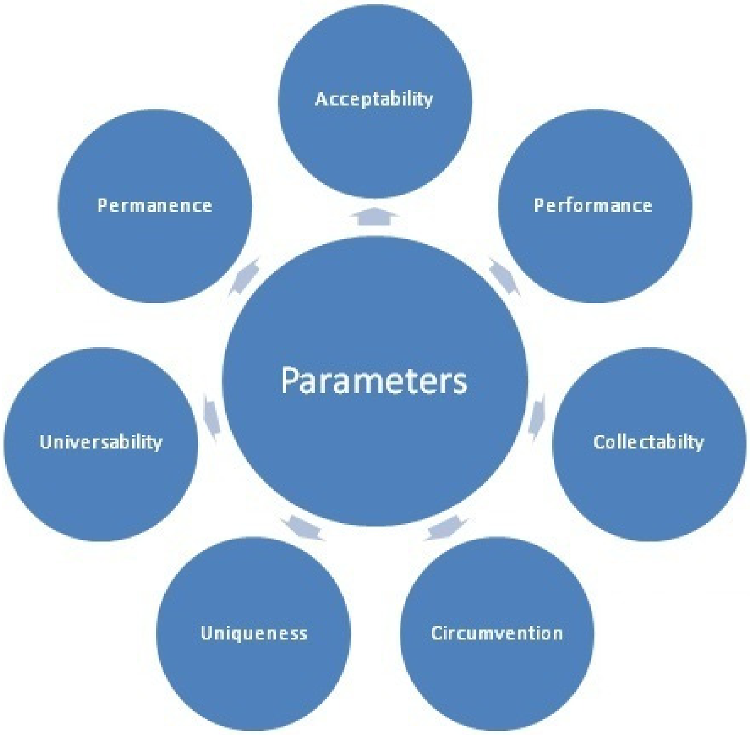


Figure - Basic Criteria for Biometrics Security System [Rahultech, 2010]

2-Application Fields for Biometrics Technology

Physical access control refers to the process that requires the physical characteristics. On the other hand, logical access control is the schemes, procedures and techniques which are used in the system. The difference between logical and physical access control is really small and it can be confused easily because physical access control is controlled by logical access control.

2.1-Physical access control

Physical access control covers identity authentication processes which require users to provide physical characteristics. It is used in high security locations such as: hospitals, police stations, and the military. The most common use for the physical access control application is the access devices which are applied at doors or computers. This application is confidential and important and is entrusted with a high level of security. The physical access control reduces the risk of human problems. It also covers the aspect of data loss in the system. The system helps to eliminate the process of identifying long and complex passcodes with different processes. Physical access control is not only effective and efficient but also safe, secure and profitable in the workplace [O'Neill, 2011].

2.2-Logical access control

Logical access control refers to a process of a scheme control over data files or computer programs. These contain personal or privacy information of many different users. Logical access control is used by militaries and governments to protect their important data with high security systems using biometric technology. The only difference between logical access control and physical access control is that the logical access control is used for computer networks and system access control. It helps to reduce the burden of long and complex password requirements for users. Moreover, it is more secure and effective in the way of protecting and maintaining privacy over data in the system. Furthermore, it also provides a great advantage by saving time and money [O'Neill, 2011].

3-Biometrics Solution

3.1-Facial Recognition Detector

The human face is one of the easiest characteristic which can be used in biometric security system to identify a user. Face recognition technology, is very popular and is used more widely because it does not require any kind of physical contact between the users and device. Cameras scan the user face and match it to a database for verification. Furthermore, it is easy to install and does not require any expensive hardware. Facial recognition technology is used widely in a variety of security systems such as physical access control or computer user accounts. However, it is still not as unique as its counterparts such as retinal, iris or DNA. Therefore, it is normally used with other characteristics in the system. On the other hand, time is the most negative affective factor with face recognition technology because as the user ages will change over time [Biometricsnewportal 2011].

Biometric face recognition systems will collect data from the users' face and store them in a database for future use. It will measure the overall structure, shape and proportion of features on the user's face such as: distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth and others expressions. Facial expression is also counted as one of the factors to change during a user's facial recognition process. Examples include, smiling, crying, and wrinkles on the face [Biometricsnewportal 2011].

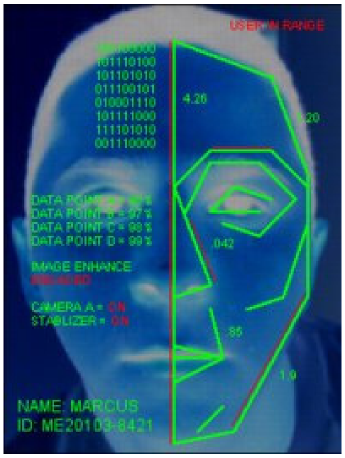


Figure - Example of face recognition scan [Vijayenthiran, 2008].

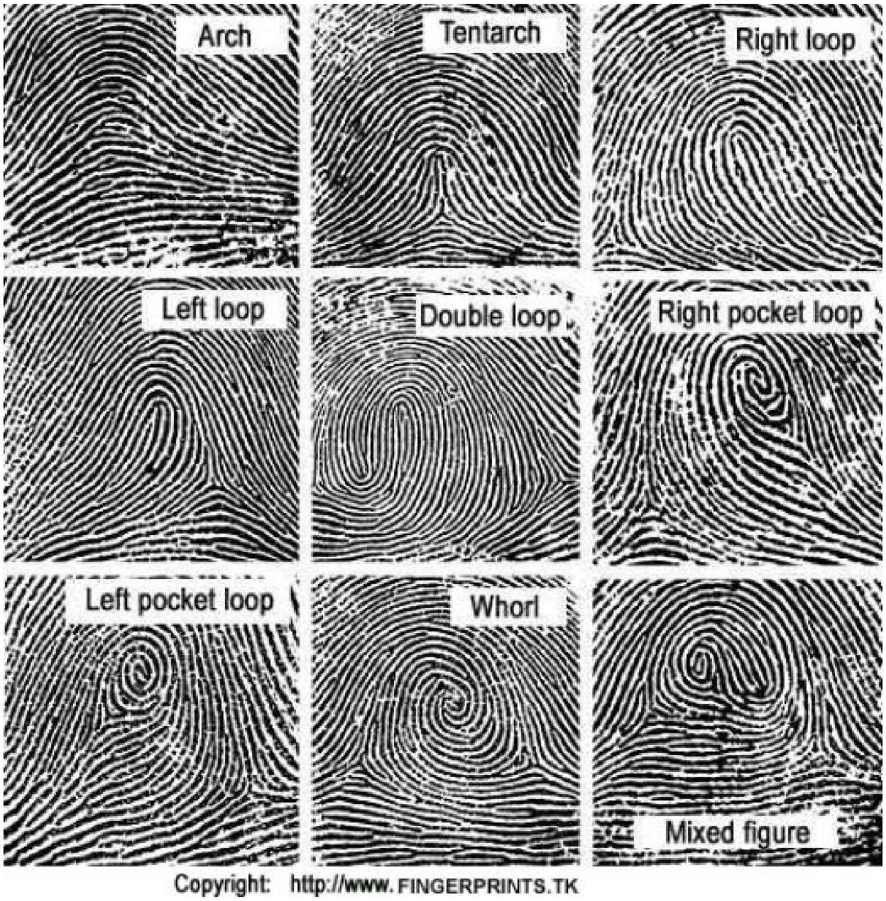
3.2-Fingerprint reader

Our fingerprint is made of a number of ridges and valley on the surface of finger that are unique to each human. "Ridges are the upper skin layer segments of the finger and valleys are the lower segments" [Biometricsnewportal 2011]. The ridges form two minutiae points: ridge endings-where the ridges end, and ridge bifurcations-where the ridges split in two. The uniqueness of a fingerprint can be determined by the different patterns of ridges and furrows as well as the minutiae points. There are five basic patterns which make up the fingerprint: the arch such as tented and plain arch covers 5% of fingerprint; left and right loop covers 60% of fingerprints; whorl covers 34% of fingerprints and accidental whorls covers 1% of fingerprints [Health Department of New Mexico].

To capture the surface of the fingerprint for verification during the identification of users, new technologies are designed with tools such as: optical and ultrasound. There are two main algorithms which are used to recognize fingerprints: minutiae matching and pattern matching.

- Minutiae matching will compare the details of the extract minutiae to identify the difference between one users fingerprint as compared to others. When users register with the system, they will record images of minutiae location and direction on finger surface. When users use fingerprint recognition system to verify their identification, a minutiae image is brought out and compared with the one which provided at the time of access. [Biometricsnewportal 2011].
- Pattern matching will compare all the surfaces of the finger instead of one particular point. It will concentrate more in thickness, curvature and density of finger's surface. The image of the fingers surface for this method will contain the area around a minutiae point, areas with low curvature radius or areas with unusual combinations of ridges [Biometricsnewportal 2011].

There are several benefits of using fingerprint recognition systems. This system is easy to use and install. It requires cheap equipment which generally has low power consumption. However, there are some disadvantages in this system. If the surface of the finger gets damaged and/or has one or more marks on it, identification becomes increasingly hard. Furthermore, the system requires the users' finger surface to have a point of minutiae or pattern in order to have matching images. This will be a limitation factor for the security of the algorithm. Fingerprint security system is used widely in different applications such as: cell phones, laptops, USB flash drives and others devices. It is also used in judicial systems in order to record users' information and verify one person's identity [Biometricsnewportal 2011].



Copyright: http://www.FINGERPRINTS.TK

Figure - Fingerprint types [Lazaroff, 2004].

3.3-Voice Recognition

There are two main factors which makes a person's voice unique. Firstly, it is the physiological component which is known as the voice tract. Secondly, it is a behavioral component which is known as the voice accent. By combining both of these factors, it is almost impossible to imitate another person's voice exactly. Taking advantages of these characteristics, biometrics technology created voice recognition systems in order to verify each person's identification using only their voice. Mainly, voice recognition will focus on the vocal tract because it is a unique characteristic of a physiological trait. It works perfectly in physical access control for users [O'Neill, 2011].

Voice recognition systems are easy to install and it requires a minimal amount of equipment. This equipment includes microphones, telephone and/or even PC microphones. However, there are still some factors which can affect the quality of the system. Firstly, performance of users when they record their voice to database is important. For that reason, users are asked to repeat a short passphrase or a sequence of numbers and/or sentences so that the system can analyze the users' voice more accurately. On the other hand, unauthorized users can record authorized users' voices and run it through the verification process in order to get user access control to system. To prevent the risk of unauthorized access via recording devices, voice recognition systems will ask users to repeat random phases which are provided by the system during verification state [O'Neill, 2011].

3.4-Iris Scanner & Recognition

The human iris is a thin circular structure in the eyes which is responsible for controlling the diameter and size of the pupils. It also controls the amount of light which is allowed through to retinal in order to protect the eye's retina. Iris color is also a variable different to each person depending upon their genes. Iris color will decide eye color for each individual. There are several colors for iris such as: brown (most popular color for the iris), green, blue, grey, hazel (the combination of brown, green and gold), violet, pink (in really rare cases). The iris also has its own patterns from eye to eye and person to person, this will make up to uniqueness for each individual [Biometricsnewportal 2011].

Iris recognition systems will scan the iris in different ways. It will analyze over 200 points of the iris including: rings, furrows, freckles, the corona and others characteristics. After recording data from each individual, it will save the information in a database for future use in comparing it every time a user want to access to the system [Biometricsnewportal 2011].

Iris recognition security systems are considered as one of the most accurate security system nowadays. It is unique and easy to identify a user. Even though the system requires installation equipment and expensive fees, it is still the easiest and fastest method to identify a user. There should be no physical contact between the user and the system during the verification process. During the verification process, if the users are wearing accessories such as glasses and contact lenses, the system will work as normal because it does not change any characteristics of the user's iris. Theoretically, even if users have eye surgery, it will have no effect on the iris characteristics of that individual [Biometricsnewportal 2011].

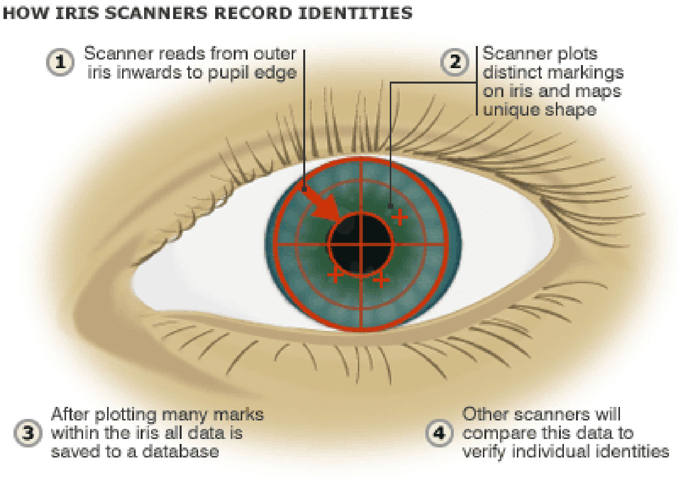

HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Figure - How Iris Scanners Record Identities [BBC].

3.5-Veins Recognition

One of the recent biometric technologies invented is the vein recognition system. Veins are blood vessels that carry blood to the heart. Each person's veins have unique physical and behavioral traits. Taking advantage of this, biometrics uses unique characteristics of the veins as a method to identify the user. Vein recognition systems mainly focus on the veins in the users hands. Each finger on human hand has veins which connect directly with the heart and it has its own physical traits [O'Neill, 2011].

Compared to the other biometric systems, the user's veins are located inside the human body. Therefore, the recognition system will capture images of the vein patterns inside of users' fingers by applying light transmission to each finger. For more details, the method works by passing near-infrared light through fingers, this way a camera can record vein patterns [O'Neill, 2011].

Vein recognition systems are getting more attention from experts because it has many other functions which other biometrics technologies do not have. It has a higher level of security which can protect information or access control much better. The level of accuracy used in vein recognition systems is very impressive and reliable by the comparison of the recorded database to that of the current data. Furthermore, it also has a low cost on installation and equipment. Time which is taken to verify each individual is shorter than other methods (average is 1/2 second) [O'Neill, 2011].

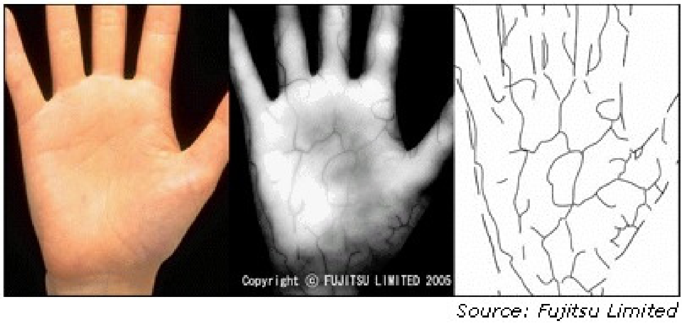


Figure - One example of vein scanning [Khan, 2006].

3.6-DNA Biometrics System

One of biometrics technology which is used in security systems recently is DNA biometrics. It is impossible to fake this characteristic because each person's DNA is unique. Each person's DNA contains some trait from his/her parents. Each cell in the human body contains a copy of this DNA. DNA profiling will decide the amount of VNTR (variable number tandem repeat) which repeats at a number of distinctive loci. These amounts of VNTR will make up an individual's DNA profile [Biometricsnewportal 2011].

In order to collect DNA from each person, the system needs time and goes through several complex steps. Firstly, it needs to collect the DNA from a physical sample of each user such as blood, saliva, hair, semen, tissue and others. Then, it needs to break down the samples into small fragments which contain VNTR. Next, the size of each DNA fragment will be measured and sorted before it is compared to different samples [Maestre, 2009].

DNA biometrics technology is highly unique and the chance of two individuals having the exact same DNA profile is extremely impossible, but this technology is still new and is hardly applied in public. It also requires lots of expensive equipment in order to break down the DNA successfully and analyze the unique features of DNA and create a DNA profile. Furthermore, the system will need to get physical samples (hair, blood, etc.) from users to collect their DNA data. Another factor that makes this system highly unused is time. The system requires long periods of time to go through all the processes of creating a DNA profile for each individual and verifying each individual's individual DNA profile. Due to these limitations and barriers, DNA biometrics is not used nearly as much as facial, iris, vein or voice recognition biometric systems. In near future, there will be solutions for these problems and we can actually apply this unique and better biometrics technology in our daily life [Biometricsnewportal 2011].

3.7-2D Barcode Scanner

2-D barcode biometrics technology is a 2-dimesional method of presenting digital security information which is provided by the biometrics technologies system. 2-D barcode is normally applied during the identification of items rather than users. However, its application is still used to verify the identification of users. By combining 2-D barcode and biometrics data, it will create a better security level which can be accessed easily and faster. By using this method, security levels of system cannot be easily penetrated by the unauthorized users. It provides a more effective and efficient security system [Wikipedia - data metrics].

Applications for 2-D barcode biometrics technology have been used for a certain time but it is not popular because users have not seen the benefit in identifying users. It can be used for scanning the identity of user's driver license, passport, ID cards, voter cards, etc.). 2-D barcode biometrics is also used in e-commerce purchasing and shipping processes in order to make sure items are delivered to the correct buyer [Wikipedia - data metrics].

2-D barcode has the same features with other biometrics technologies. It is installed with a sensor to read physical traits from items or individuals. Furthermore, 2-D barcode systems will print 2-D barcodes on the documents which contain the person's biometrics information. This step is provided in order to enhance the security capability [Wikipedia - data metrics].

2-D barcode biometrics technology is applied in various ways and it is becoming more useful and popular. A 2-D scanner can be a light-weight device which can be carried around. It is also easy to install with low costs on installation and equipment. It is also more flexible than other methods and the result of verification is much faster.

4-Middleware / software of biometrics security

Middleware and software for biometrics security system provides the link between services and instructions through the use of multiple processes. The middleware helps the biometrics devices and the database run effectively across the network. Middleware and software also connects biometrics devices and the computers together, while working compatibly with each other on the network. Furthermore, the software and middleware used by the biometrics systems form an integral part to the efficiency and effectiveness of the whole biometrics security system. It gives the system the flexibility to bind all the applications which are located at the database/server to any biometrics devices at the verification location [O'Neill, 2011].

5-Advantages and Disadvantages of Biometrics Security System

5.1-Advantages

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 [Tistarelli, 2009].

Secondly, 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 [Tistarelli, 2009].

Lastly, 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) [Tistarelli, 2009].

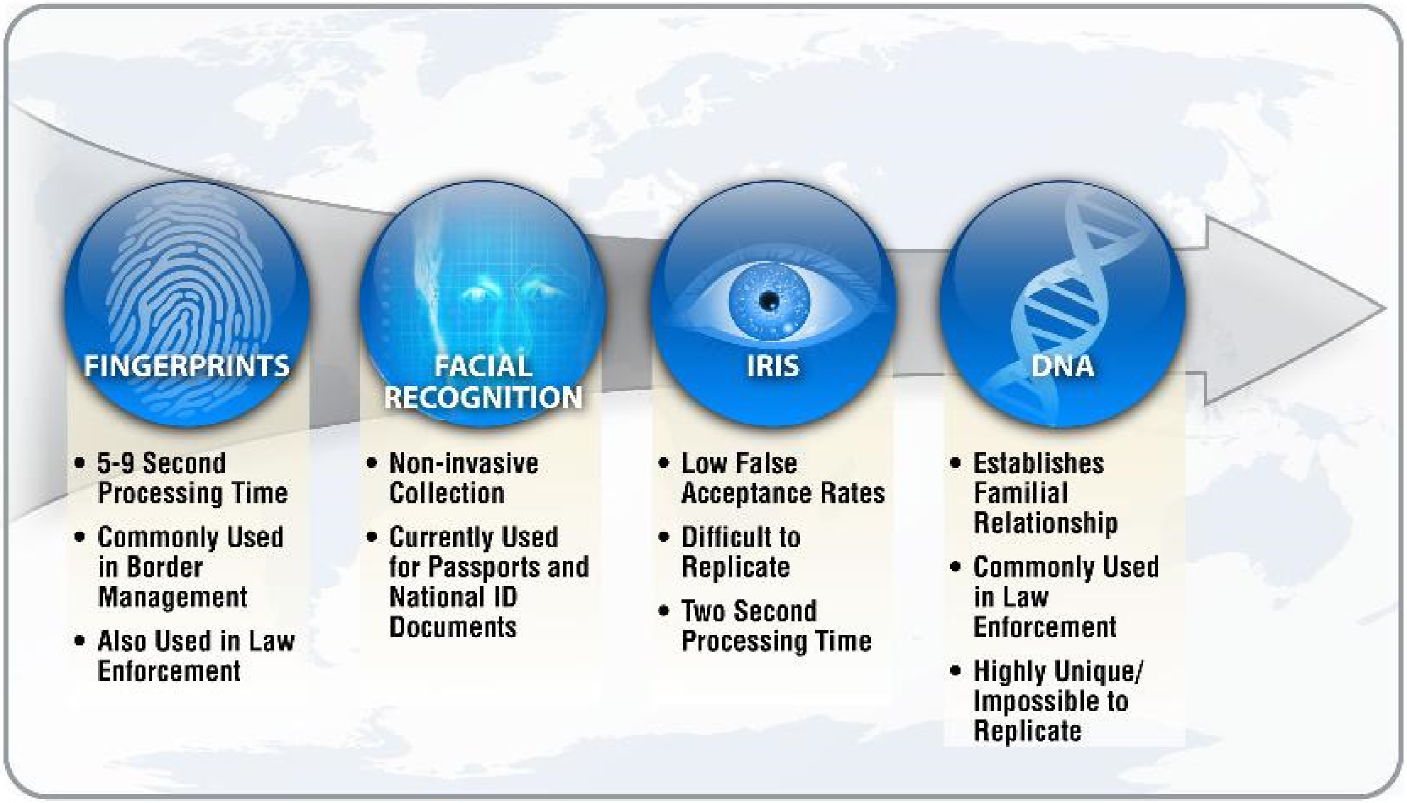

FINGERPRINTS
• 5-9 Second Processing Time
• Commonly Used in Border Management
• Also Used in Law Enforcement
FACIAL RECOGNITION
• Non-invasive Collection
• Currently Used for Passports and National ID Documents
IRIS
• Low False Acceptance Rates
• Difficult to Replicate
• Two Second Processing Time
DNA
• Establishes Familial Relationship
• Commonly Used in Law Enforcement
• Highly Unique/ Impossible to Replicate

Figure - Advantages of biometrics security system [Arc Aspicio, 2009].

5.2-Disadvantages

Even though, there are many advantages of biometrics security system, it still has many flaws in its system. Each biometrics application method has weaknesses 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 [PBworks 2006].

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 [PBworks 2006]. Finally, lots of people are still concerned about biometrics technology in different aspects such as: security, adaptability to rate of change in life, scalbility, accuracy, privacy and others.

6-Biometrics Future View

6.1-Biometrics techonolgy affects to our life

As we can see from different products from various companies, biometrics technology has major effects on our lives. Biometrics technology provides us with great number of new inventions which improves both the quality and the longevity of our lives. Nowadays, biometrics technology is considered one of the best protection methods of user information, data, etc. Basically, biometrics technology method will collect and measure data of human physiology and behavior. There are several ways to collect and measure data of users such as: scanning the unique characteristics of the person (retinal, finger-print, facial expression, etc.) or analyzing the unique behavior of human (signature, keyboard typing styles, etc.). The main purpose of biometric system is to identify and verify a person's identity. Biometrics technology is more convenient than other protection technologies of identity authentication. For example, ID card (student IDs in school) is one of the examples to authenticate a user's identity. If you forget your ID card at home then you will not be able to access to school building. In this case, biometrics system will be more efficient and useful because chances that you forgot your eyes or fingers at home are very unlikely. With biometrics security system, we just need to verify our identity by the unique characteristics that are always with us reducing the chances of losing ID cards and other identifying accessories. Furthermore, ID cards can be duplicated increasing the risk of unauthorized users gaining access to import data. With our own unique characteristics and behaviors, it will be harder to change or make copies.

Biometrics security system has bigger applications in our lives and in recent years, scientists have developed higher stages of identifying a user's identity. Our main application is facial recognition technology. With this technology, we can recognize any person in a crowded group; therefore, we can verify their identification. We can also use this method of biometrics technology to detect previously identified criminals and terrorists in society. This will help us to reduce the crime rate in the world.

Biometrics technology is applied in a variety of ways and different fields of practice. For example, we can see that it is applied in hospitals to verify the identity of patients and to protect their privacy. Furthermore, biometrics technology has been used at airports to verify the identity of people. By using this technology, it helps governments keep track of people going in and out of country. It also helps to identify criminals and terrorists. Other example of this technology which is applied in our daily lives is voice recognition; voice recognition systems are applied in homes to verify identities of authorized users. This technology is not only used for security sections, but it also can be applied in the other aspects of life. It has been used in businesses such as e-commerce and shipping sections. Biometrics technology such as 2-D barcode makes our life a lot easier with much faster item identification. With this technology, it will make sure packages are sent to correct recipients. 2-D barcode biometrics technology also applied for items. For example, it is applied to items in supermarkets and stores with detailed information of that item.

6.2-Biometrics technology concerns

There are many concerns for biometrics technology over its advantages and disadvantages. Many experts have been looking into this aspect of new technology to try and find out the value of biometrics technology. There are three main concerns about this new-born technology including: information privacy, physical privacy and religion objections.

Information privacy: there are threats (function creep and tracking capabilities of biometrics system) that are concerns affecting the privacy of information of users [Woodward, 2001].

- Function creep: is the process of over collecting unnecessary data which can be used by the system. It can occur with or without the knowledge of data-provider and collector. Many experts believe that function creep cannot be avoided. It depends on how and when function creep occurs and it can either result in the rightful or unrightful act. "For instance, using social security number to search for a parent who is delinquent with child support payments may be seen as desirable. On the other hand, having a person's digitized state Department of Motor Vehicles (DMV) photo-graph sold to a commercial firm to create a national photo ID database might be considered unacceptable (Davies, 1994, pp. 61-62)"

- Tracking capabilities: the biometrics system has large amounts of databases which contain personal details and information of the public and private sectors raising many questions of maintaining each individual's anonymity. Many people are concerned that authorized people who got control over biometrics systems will be able to track individuals without their knowledge. One of example of this concern is facial recognition software and systems. With this technology, the system can recognize and verify each individual wherever they go which might be seen as an invasion of privacy [Woodward, 2001].

Physical Privacy: by affecting of information privacy, the physical privacy also gets some attention from users. These concerns include the stigma associated with some biometrics, the possibility of actual harm to the participants by the technology and the concern that the devices used to obtain or read the biometrics data may be not clean as expected [Woodward, 2001].

Religious Objections: this aspect of concern for biometrics security system is not expected to be wide-spread. However, its problem will decide if the biometrics system can be applied in public or not. One example for this concern is 2-D barcode. There are certain religious groups that believe barcodes on users is "the Mark of the Beast" and can a number of evils. For religious objections, governments must take this problem seriously and find the solutions for the biometrics technology in order to spread its use [Woodward, 2001].

6.3-Biometrics applies in network security

The biggest problem for network security is the authentication system. For most systems, they mainly use and rely on passwords which is a combination of letters, characters and/or numbers. However, passwords need to be renewed within a certain period of time to maintain a high level of security. Moreover, it might be copied and used by unauthorized users. To fix that problem, biometrics security system can be applied. The most use of biometrics security system in network is the logical access control method. It will verify person's identification for secure workstation logon or network logon to get access control to the system [Reid, 2011].

7-Summary

In conclusion, biometrics technology is a new technology for most of us because it has only been implemented in public for short period of time. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

9-References

- [Lai. 2011] Lifeng Lai, Sui Wai Ho and H. Vicent Poor "Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case" EEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011
- [Jain, 2004] Jain, A.K.;Ross, A.;Prabhakar, S.;"An introduction to biometric recognition", Volume: 14 Issue: 1 Issue Date: Jan. 2004, on page(s): 4 - 20
- [Jain, 2006]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
- [Maestre, 2009] Sandra Maestre, Sean Nichols "DNA Biometrics", 2009
- [Reid, 2011] Paul Reid, "Biometrics for network security", Pearson Education Inc., 2004, ISBN 0131015494
- [Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001
- [Tistarelli, 2009] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743
- [Cransor, 2005] Lorrie Faith Cranor, Simson Garfinkel, "Security and usability: designing secure systems that people can use", O'Reilly Media, Inc., 2005, ISBN 0596008279
- [Mosdorf, 2006] Khalid Saeed-Jerzy Pejas-Romuald Mosdorf, "Biometrics, Computer Security, Systems and Artificial Intelligent Applications", S pringer-Verlag Berlin Heidelberg 2006, ISBN 0387362320
- [Woodward, 2001]John D. Woodward (Jr.), United States. Army, Arroyo Center "What concerns do biometrics raise and how do they differ from concerns about other identification methods?" Army biometric applications: identifying and addressing sociocultural concerns, 2001
- [Health Department of New Mexico] New Mexico, Department of Health "Fingerprint Techniques Manual what.pmd" http://dhi.health.state.nm.us/elibrary/cchspmanual/fingerprint_manual.pdf
- [Biometricsnewportal 2011] "Biometrics new portal" UK 2011http://www.biometricnewsportal.com/
- [O'Neill, 2011] Peter O'Neill; Anne O'Neill; Shaun Winters; Lucy Kwiaton "Biometrics security system", 2011 http://www.findbiometrics.com

- [QuestBiometrics, 2005] "Biometrics Access Control", 2005 http://www.questbiometrics.com/biometric-access-control.html
- [Wikipedia - data metrics] http://en.wikipedia.org/wiki/Data_Matrix
- [PBworks 2006] PBworks, "Advantages and Disadvantages of technologies", 2006 http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies
- [Vijayenthiran, 2008] Vijayenthiran "BMW using face recognition to personalize cars" 2008 http://www.motorauthority.com/news/1024835_bmw-using-face-recognition-to-personalize-cars
- [Rahultech, 2010] Rahultech "IT trends-latest/recent trends in information technology" 2010 http://rtmnuittrends.blogspot.com/2010/09/biometrics.html
- [Arc Aspicio, 2009] Arc Aspicio "DNA: The last biometric" 2009 http://www.arcaspicio.com/insights/2009/3/19/dna-the-last-biometric.html
- [Lazaroff, 2004] Mr. Lazaroff & Mr. Rollison "Classification of Fingerprints" 2004 http://shs.westport.k12.ct.us/forensics/04-fingerprints/classification.htm
- [Khan, 2006] Imran Khan "Vein Pattern Recognition - Biometrics Underneath the Skin" 2006 http://www.frost.com/prod/servlet/market-insight-top.pag?docid=86268767
- [BBC] BBC "Biometrics Technology" http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn3page1.stm

8-Acronyms

- **DNA :** Deoxyribonucleic acid [Deoxyribo (D) nucleic (N) acid (A)]
- **USB :** Universal Serial Bus
- **PC :** Personal computer
- **VNTR :** Variable number tandem repeat
- **2D barcode :** 2-dimension barcode
- **ID :** Identification
- **DMV :** Department of Motor Vehicles

Last Modified on: November 28, 2011
This and other papers on latest advances in network security are available on line at http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page