ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Comparative Study of Different Biometric Features

Kalyani Mali[1], Samayita Bhattacharya[2]

Department of Computer Science & Engineering, University of Kalyani, Kalyani, West Bengal, India[1,2]

Abstract: Biometrics is one of the biggest tendencies in human identification. Nowadays, biometrics is widely being used in many real life applications like security, forensic, and other identification and recognition purposes. Biometrics also successfully managed to generate a curiosity amongst many. Here we have discussed different biometric features and their usage along with the comparisons of different biometrics features. The fingerprint is the most widely used biometric, where as recently iris started to get a high importance too. Multimodal biometrics can improve the performance and reliability of biometric authentication even further.

Keywords: Fingerprint, DNA, Iris, Retina, Face, Signature, Voice, Gait, Hand Geometry.

INTRODUCTION

In the ever-changing world of global data communications, and fast-paced software development, security is becoming more and more of an issue. No system can ever be completely secure, all one can do is make it increasingly difficult for someone to compromise the system. The more secure the system is, the more intrusive the security becomes. One needs to decide where in this balancing act the system will still be usable and secure for the purposes. Here we have discussed different Biometric tools and related security issues.

Identity is to establish the identity of a person, or to ascertain the origin, nature or definitive characteristics of a particular person. To uniquely identify a person different types of information can be used with other sources. This concept is ancient, and has become much more important as information technology and the Internet have made it easier to collect identifiable documents. To identify a person, the recent trend is to use biometric. Different biometric features can distinctively identify a person unless there are identical twins. In case of identical twins many biometrics fail to distinguish them as separate person, but fingerprint still can distinguish. In recent technology more than one biometric feature is also being used in a combination to have more robust indentifying system. Several research projects have shown that multimodal biometrics (e.g. fingerprints and voiceprints combined) can improve the performance and reliability of biometric authentication.

1. BIOMETRIC

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. Currently Biometrics is one of the biggest tendencies in human identification.

Biometrics is claimed to be better than current and established authentication methods, such as Personal identification numbers (PINs), Passwords, Smart cards. Key advantages of using a biometric feature are: availability (always), uniqueness (to each person), not transferable (to other parties), not forgettable, not subject to theft, not guessable.

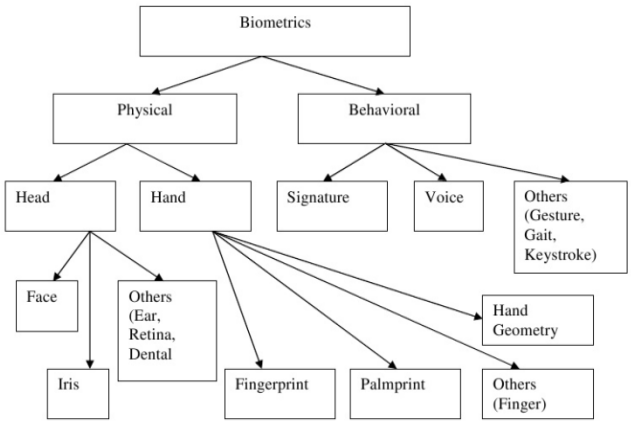


Figure 1: Various Biometrics

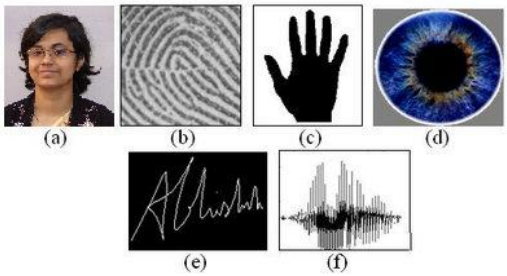


Figure 2: Few Biometric characteristics that are commonly used: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) signature, (f) voice.

1.1. DNA

Due to recent improvements in laboratory analysis and reduction in costs, many agencies are relying on deoxyribonucleic acid (DNA) as a form of identification. DNA is a chemical structure that forms chromosomes. A gene is piece of a chromosome that dictates a particular trait. That chemical structure can be identified through

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

laboratory analysis. DNA does not change over times, however, two people can have the same DNA (Identical twins)

DNA identification processes require a lengthy time period. In addition, some consider DNA collection to be personally invasive.

1.2. Iris

Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high resolution images of the irises of an individual's eyes.

Iris recognition uses camera technology, with subtle infrared illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

Iris recognition efficacy is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. Because of its speed of comparison, iris recognition is the only biometric technology well-suited for one-to-many identification. A key advantage of iris recognition is its stability, or template longevity, a single enrollment can last a lifetime. There are few advantages of using iris as biometric identification: It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labour. The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation.

Even genetically identical individuals have completely independent iris textures, whereas DNA (genetic "fingerprinting") is not unique for the about 0.2% of the human population who have a genetically identical twin. An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years. But Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition. Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters. As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates [3]. As with other identification infrastructure (ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

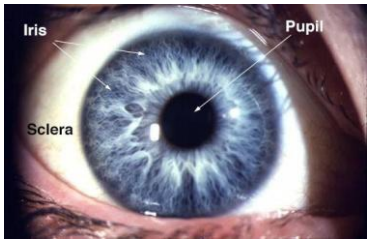


Figure 3: Iris Sample

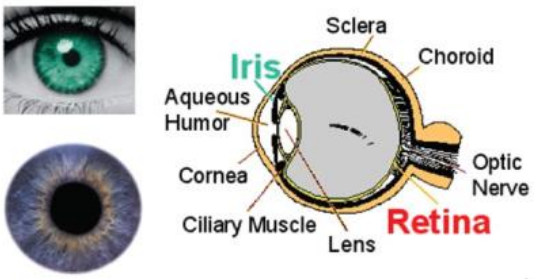


Figure 4: Difference of Iris & Retina

1.3. Retina

A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them. The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric [7]. Advocates of retinal scanning have concluded that it is so accurate that its error rate is estimated to be only one in a million.

Retinal scan is used to map the unique patterns of a person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Because retinal blood

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

vessels are more absorbent of this light than the rest of the eye, the amount of reflection varies during the scan. The pattern of variations is converted to computer code and stored in a database. Retinal scanners are typically used for authentication and identification purposes. Advantages of using Retinal scan include low occurrence of false positives, extremely low (almost 0%) false negative rates, highly reliable because no two people have the same retinal pattern, speedy results: Identity of the subject is verified very quickly [8]. Disadvantages include measurement accuracy can be affected by a disease such as cataracts, measurement accuracy can also be affected by severe astigmatism, canning procedure is perceived by some as invasive, not very user friendly, subject being scanned must be close to the camera optics, high equipment costs [8][9].

1.4. Face

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems. Face recognition can be considered to be same as photograph recognition, so it lacks in many areas. Even the automated system for face recognition has lacking as photographs are highly affected by camera angle, brightness, etc. And also the face of the person changes over the time, unlike fingerprint which remains same throughout the life span of a person. Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems [1]. Other conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low resolution images [2]. Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective. For instance: few countries now allow only neutral facial expressions in passport photos. An emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space [2]. Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent [1] [2].

Figure 5: Change of face of same person over time

1.5. Voice

Speaker recognition is the computing task of validating a user's claimed identity using characteristics extracted from their voices. Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their co-operation. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc. In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match. Feeding the wrong voice cannot always be avoided in voice recognition as well as the voice capturing machine should be near to the user.

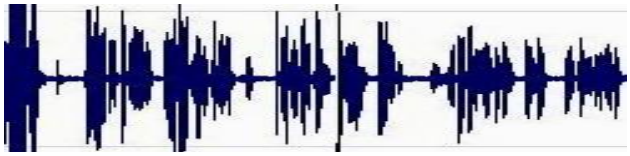


Figure 6: Sample voice clip as shown in sound editor

1.6 Signature

A signature is a handwritten (and sometimes stylized) depiction of someone's name, nickname, (or even a simple "X") that a person writes on documents as a proof of identity and intent. The role of a signature is not solely to provide evidence of the identity of the contracting party, but rather to additionally provide evidence of deliberation and informed consent. Signatures can be easily falsified. With advanced signature capturing devices, signature recognition correctly became easier and more efficient.

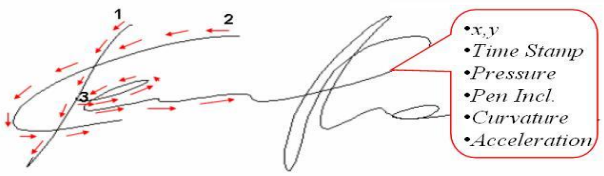


Figure 7: Signature Features

1.7. Palm Print

A palm print refers to an image acquired of the palm region of the hand. It can be either an online image (i.e. taken by a scanner, or CCD) or offline image where the image is taken with ink and paper [5].The palm itself consists of principal lines, wrinkles (secondary lines) and ridges. It differs to a fingerprint in that it also contains other information such as texture, indents and marks which can be used when comparing one palm to another. Palm prints can be used for criminal, forensic or commercial applications. The main disadvantage of palm print is that the print changes with time depending on the type of work the person is doing for a long duration of time.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

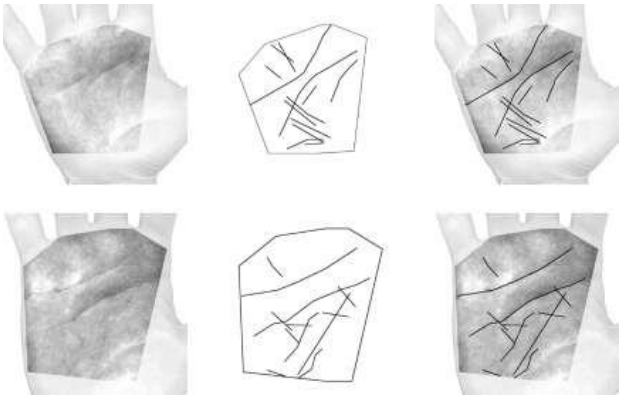


Figure 8: Palm-print and Palm-print Features

1.8. 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 behavioural 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 connecting directly with the heart and it has its own physical traits.

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.

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 A Survey of Biometrics Security Systems http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/index.html 5 of 10 shorter than other methods (average is 1/2 second) [6].

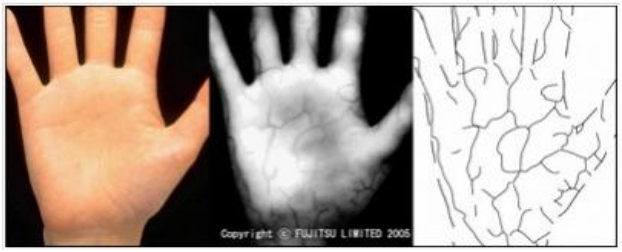


Figure 9: One example of vein scanning

1.9. Ear

The human ear is a new feature in biometrics that has several merits over the more common face, fingerprint and iris.

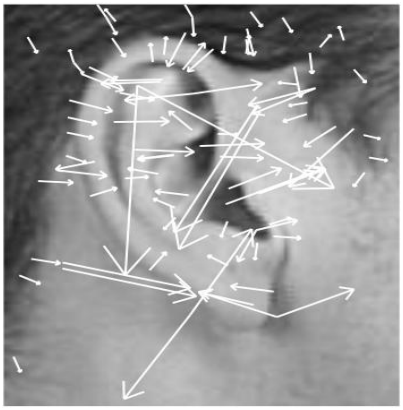


Figure 10: Ear Features

Unlike the fingerprint and iris, it can be easily captured from a distance without a fully cooperative subject, although sometimes it may be hidden with hair, scarf and jewellery. Also, unlike a face, the ear is a relatively stable structure that does not change much with the age and facial expressions.

1.10. Gesture

A gesture is a form of non-verbal communication in which visible bodily actions communicate particular messages, either in place of speech or together and in parallel with words. Gestures include movement of the hands, face, or other parts of the body. Gestures differ from physical non-verbal communication that does not communicate specific messages, such as purely expressive display or displays of joint attention. Gestures let individuals to communicate a variety of feelings and thoughts, from contempt and hostility to approval and affection, often together with body language in addition to words when they speak. Gestures have been studied for centuries from different viewpoints. Gesture recognition is a topic in computer science and language technology with the goal of interpreting human gestures via mathematical algorithms. Gestures can originate from any bodily motion or state but commonly originate from the face or hand. Recent focuses include emotion recognition from the face and hand gesture recognition. Many approaches have been made using cameras and computer vision algorithms to interpret sign language. However, the identification and recognition of posture, gait and human behaviours is also the subject of gesture recognition techniques. Gesture recognition can be seen as a way for machines to begin to understand human body language and building a stronger bridge between machines and humans than primitive text user interfaces which still limit the majority of input to keyboard and mouse.

1.11. Gait

Gait is the pattern of movement of the limbs of animals, including humans, during locomotion over a solid substrate. Most animals use a variety of gaits. Human gait is the way locomotion is achieved using limbs. Human gait is defined as bipedal, biphasic forward propulsion of centre of gravity of human body, in which there is

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

alternate sinuous movements of different segments of the body with least expenditure of energy. Different gaits are characterized by differences in limb movement patterns, overall velocity, forces, kinetic and potential energy cycles, and changes in the contact with the surface (ground, floor, etc.). There are gender differences in human gait: females walk with lesser step width and more pelvic movement. Gait analysis generally takes gender into consideration.

1.12. Hand Geometry

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.

Viable hand geometry devices have been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It remains popular; common applications include access control and time-and-attendance operations. Since hand geometry is not thought to be as unique as fingerprints or irises, fingerprinting and iris recognition remain the preferred technology for high-security applications. Hand geometry is very reliable when combined with other forms of identification, such as personal identification numbers. In large populations, hand geometry is not suitable for so-called one-to-many applications, in which a user is identified from his biometric without any other identification.

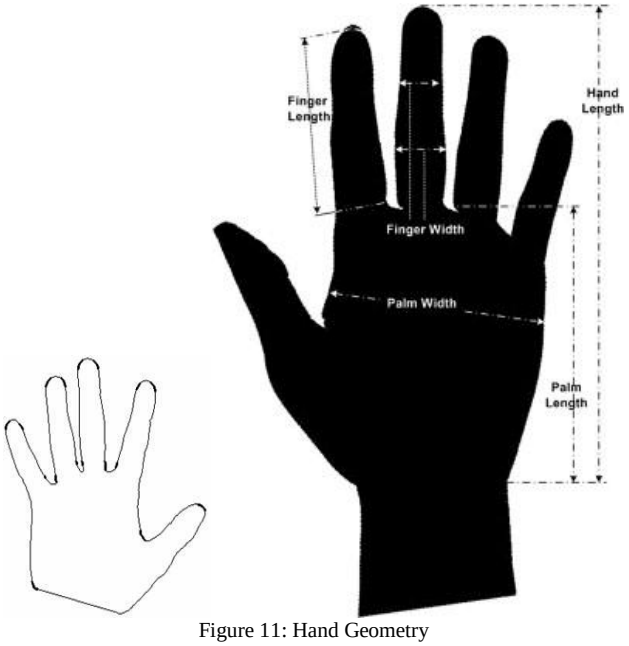


Figure 11: Hand Geometry

1.13. Odour

An odour or fragrance is caused by one or more volatilized chemical compounds, generally at a very low concentration, that humans or other animals perceive by the sense of olfaction. The ability to identify odours varies among people and decreases with age. Studies show there are sex differences in odour discrimination; women usually outperform males. Humans can detect individuals that are blood-related kin (mothers and children but not husbands and wives) from olfaction. In humans, the formation of body odours is mainly caused by skin glands excretions and bacterial activity. Body odour is present both in animals and humans and its intensity can be influenced by many factors (behavioural patterns, survival strategies). Body odour has a strong genetic basis both in animals and humans, but it can be also strongly influenced by various diseases and psychological conditions, making a unique identification more difficult.

1.14. Dental Orientation

Every individual is supposed to have a unique dental orientation. But using dental pattern for identifying a person cannot be of much success as there is a change of dental pattern of a child and when that person is grown up. Also removing a damaged tooth is a common practice in human, making identification difficult.

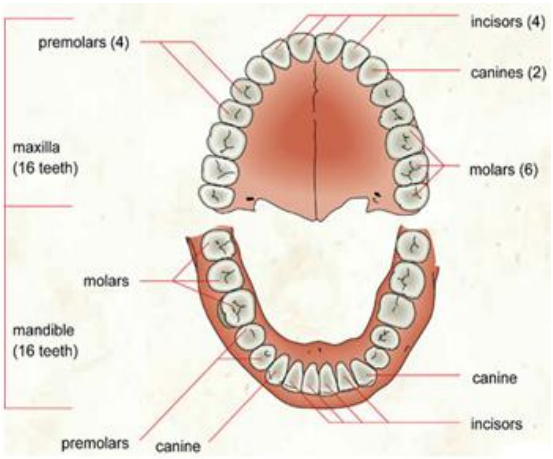


Figure 12: Dental Arch of an Adult

1.15. Facial Thermograms

Thermograms of face can be used to identify a person. Temperatures vary from red (hottest) through yellow, green and blue to mauve (coldest). Thermal skin imaging may be used for security access or, if used in conjunction with a police database, to identify known criminals. The infrared cameras used in such systems can work at distances of over 150 metres. Smiling female identical twins are seen with thermograms of their heads. The thermograms show the facial heat patterns produced by blood flowing through blood vessels below the skin's surface. The patterns are unique even in these identical twins, allowing them to be accurately identified.

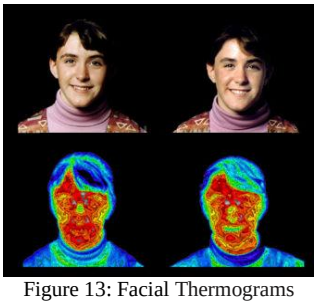


Figure 13: Facial Thermograms

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

1.16. Fingerprints

Fingerprints are the graphical flow-like ridges present on human fingers. Finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier. Fingerprint-based personal identification has been used for a very long time [10]. Owning to their distinctiveness and stability, fingerprints are the most widely used biometric features.

Most importantly, even the twins don't share same fingerprints. the environment in the uterus affects the phenotypic development of all parts of the twin fetuses. Thus, despite an identical DNA structure of the two fetuses, fingerprints become different.

Figure 14: Fingertip

Figure 15: Fingerprint Matching Mechanism

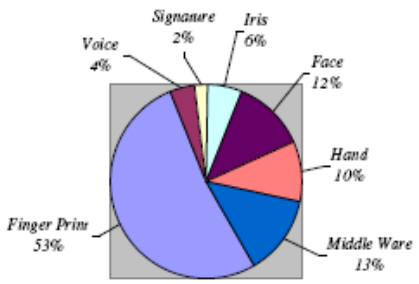


Figure 16: Biometric Market Report (International Biometric Group) estimated the revenue of various biometrics in the year 2002

2. Identical Twins, DNA & Fingerprints

Identical twins generate a lot of curiosity. Parents of multiples have probably not given a great deal of thought to their children's' fingerprint patterns, but the general public has spent a lot of time wondering about this topic.

Identical twins have fingerprints that can be readily distinguished on close examination. However, the prints do have striking similarities. In fact, before the arrival of modern genetic testing, similarity of fingerprints was often used to determine whether twins were identical or fraternal.

The last decade of forensic science has been dominated by genetic analysis. Lawyers now focus on DNA testing to prove the guilt or innocence of those accused of crimes, pushing traditional techniques such as fingerprint analysis into the background. Ironically, however, fingerprint analysis could be used to solve a key conundrum of genetic analysis — how do we tell about identical twins?

Identical -- or monozygotic -- twins form when a single fertilized egg splits in two after conception. Because they form from a single zygote, the two individuals will have the same genetic makeup. Their DNA is virtually indistinguishable.

Yet the parents of twins can usually tell them apart by subtle visual cues, and, while their fingerprints are generally similar, they are not identical.

Fingerprints are not an entirely genetic characteristic. Scientists love to use this topic as an example of the old "nature vs. nurture" debate. Fingerprinting, along with other physical characteristics, is an example of a phenotype -- meaning that it is determined by the interaction of an individual's genes and the developmental environment in the uterus.

The ultimate shape of fingerprints are believed to be influenced by environmental factors during pregnancy, like nutrition, blood pressure, position in the womb and the growth rate of the fingers at the end of the first trimester. Thus, you will find similar patterns of whorls and ridges in the fingerprints of identical twins. But there will also be differences -- just as there are differences between the fingers on any individual's hands.

In the case of fingerprints, the genes determine the general characteristics of the patterns that are used for fingerprint classification. As the skin on the fingertip differentiates, it expresses these general characteristics. However, as a surface tissue, it is also in contact with the amniotic fluid in the uterus. The fingertips are also in contact with other parts of the fetus and the uterus, and their position in relation to uterus and the fetal body changes as the fetus moves on its own and in response to positional changes of the mother. Thus the microenvironment of the growing cells on the fingertip is in flux, and is always slightly different from hand to hand and finger to finger. It is this microenvironment that determines the fine detail of the fingerprint structure. While the differences in the microenvironment between fingers are small and subtle, their effect is amplified by the differentiating cells and produces the macroscopic differences that enable the fingerprints of twins to be differentiated.

More generally, the environment in the uterus affects the phenotypic development of all parts of the twin fetuses. Thus, despite an identical DNA structure of the two

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

fetuses, a very careful examination of other physical characteristics will show that twins are systematically different, although those differences may be too subtle to detect without careful measurement. This process of differential development continues throughout life. As twins age, they diverge more and more, and in middle and old age will look more like non-identical twins.

If you compare palm prints and fingerprints of the Dionne quintuplets (born in 1934, they were the first quints of which all five survived), you find that the broad-brush pattern of lines, whorls, loops, etc., as well as what researchers call "ridge count," were quite similar for the whole crew. Nonetheless each kid had unique prints due to differences in detail. "There is as yet no evidence that the arrangement of the minutiae (ending ridges, bifurcating ridges, etc.) is in any way genetically influenced," writes fingerprint expert James Cowger. Presumably these minor but crucial differences arise from random local events during fetal development. One genius has computed that the chances of duplicating even a portion of a fingerprint are 1 in 100 quintillion (one followed by 20 zeros). Multiply that by the totality of each finger times ten fingers to get the real picture. Fingerprints suggest we are not simply the prisoners of our genes. On the contrary, much of our physical makeup seems to be improvised.

3. Advantages of a Biometric System

The advantages of biometrics are the person is the key so you need never remember your card or key again. Each body part is unique and Biometrics uses your unique identity to enable a purchase activate something or unlock something. Biometrics encompasses Voice, Vein, Eye, Fingerprint, Facial recognition and more.

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. For e.g. minimize the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access'
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

4. Disadvantages of a Biometric System

Biometric identification systems have many disadvantages. Police have at times misused biometric information. Fingerprint readers are used to limit access to computers, but they are no more reliable than turnkey locks. Of course, people are free to do what they will with their own biometric information, but such systems can be abused. One disadvantage is that a determined pirate can steal the biometric information if it's stored on a computer. There are many other drawbacks to these systems.
Criminals have been known to remove fingers to open biometric locks, Biometrics requires a lot of data to be kept on a person, these systems are not always reliable as human beings change over time if you are ill; eyes puffy, voice hoarse or your fingers are rough from laboring for example it may be more difficult for the machinery to identify you accurately. Every time you use Biometrics you are being tracked by a database bringing up a range of privacy issues. The final disadvantage is the expense and technical complexity of such systems.

And if the system is strict enough, in case of emergency too it may not give access permission (or in case of data loss due to accidental reasons). Like for example there is fire caught in office and the door is not opening due to loss of data stored due to fire, and the gates are all biometric operated, then how will the people inside survive!

Other Important Factors:

- The fingerprints of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication.
- It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time.
- For people affected with diabetes, the eyes get affected resulting in differences.
- Biometrics is an expensive security solution.

5. Comparison between Different Biometrics Used

The following table compares some of the biometric systems used lately, from the point of view of accuracy, cost, and devices required and social acceptability. We can see that fingerprint has a good balance about everything from the bellow tables.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Biometric identifier	universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	H	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Odor	L	L	L	M	L	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1: Comparison of various biometric

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Table 2: Comparison of various biometric

CONCLUSION

Biometrics is more secured and safer than a simple password. Biometrics is a technology that will either greatly benefit or burden us in the near future. With a boost in security and surveillance in the past few years, the only step that we can take is to implement biometrics into our everyday lives. Whether we do this by simply putting our fingerprints on our drivers license's (as some states have already done, including California), or making DNA sampling a common task in peoples everyday lives.

Warren and Brandeis, for instance, stated in 1890 that our privacy is ever so slowly being dissolved. This was brought to their attention after an uninvited guest had taken a photograph at a private wedding.

To this day there are no specific articles in the constitution that protects ones privacy. Over the last hundred years the public has been desensitized to everyday events such as surveillance. Biometrics poses great benefits but also many drawbacks, one being that we may also become desensitized to its effects.

A world in which biometrics grow to become common could greatly benefit us. Instead of paying cash at a grocery store, you could simply have an iris scan, and the store will put it onto your account. There would be no reason to carry around wallets with credit cards and drivers license. Everything would be stored digitally on a nationwide network. Forget about remembering passwords and PIN numbers, your fingerprint will do.

Not only could everything be much easier and streamlined in a world of biometric technologies, but also identity theft would be a thing of the past.

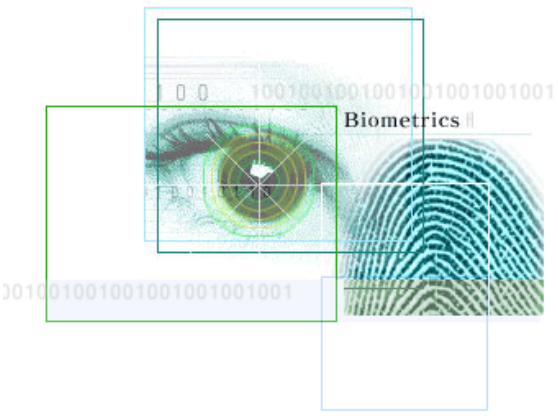
Everyone would be totally accountable for their own actions and their own actions alone. This could send crime rates to an all-time low. There appear to be countless benefits that biometrics can help us achieve. This world would truly be a remarkable one to live in, but many experts agree that it is a naive world.

Biometrics has many hurdles to get by in order to become as present and common as they are in the world described above. Problems that face biometric growth is the fact that the cost of identification devices are, presently, much too high and "people are hesitant to trust giving a 'piece of themselves' to a machine". Another problem is that biometrics has always been used in the case of criminals, and when we start using these identification technologies on innocent civilians, it gives the innocent civilians a presumption of guilt.

Perhaps the strongest argument against implementing biometrics into our everyday lives is that people would have to enter the information into machines, and people make mistakes. In a world where your name would be tied to nothing but your biometric fingerprint, a mix-up could be disastrous and place false guilt on someone.

Imagine the case of a disgruntled employee at a biometrics database agency. It can be better hoped that she doesn't hold a grudge against anyone because how hard would it be for her to link that person's name to the DNA of a convict.

Each one of the Technologies used in our days bring us a manner to restrict the access to a system, allowing the entrance only to those persons who know a specific code, own a card or have determined physic marks. The more complex is the system, the most difficult is to be attacked, although it will be more expensive and will require more software and hardware resources. When a new authentication system is implanted, it is essential a judgment between simplicity, price and efficiency, as well as social acceptability. From our study we can see that that the most adequate methodology is the fingerprint authentication.



ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

REFERENCES

1) Williams, Mark. "Better Face-Recognition Software". http://www.technologyreview.com/Infotech/18796/?a=f. 2008-06-02.
2) Bonsor, K. "How Facial Recognition Systems Work". http://computer.howstuffworks.com/facial-recognition.htm.
3) Zhaofeng He, Tieniu Tan, Zhenan Sun and Xianchao Qiu, "Towards Accurate and Fast Iris Segmentation for Iris Biometrics", In: IEEETransactions on Pattern Analysis and Machine Intelligence, 15 July 2008.
4) N. Poh and S. Bengio, "Database, Protocol and Tools for Evaluating Score-Level Fusion Algorithms in Biometric Authentications," PatternRecognition, vol. 39, no. 2, pp. 223-233, 2005.
5) Zhang, D. ''Palmprint Authentication'', Kluwer Academic Publishers.
6) Rankl, W.; W. Effing (1997). *Smart Card Handbook*. John Wiley & Sons. ISBN 0-471-96720-3.
7) Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.
8) Hill, Robert. "Retina Identification". Msu.Edu.
9) Roberts, Chris. "Biometrics" Retrieved on 2009-06-11.
10) A. Almansa and L. Cohen, "Fingerprint image matching by minimization of a thin-plate energy using a two-step algorithm with auxiliary variables," in Proc. IEEE 5thWorkshop Applications Computer Vision, Dec. 2000, pp. 35– 40.