

Biometrics: Challenges And Opportunities

Er. Pawan Kumar*, **Er. Subham Gandhi****, **Er. Chander Prakash*****

***/**SBMN Engg College, Asthal Bohar, Rohtak, *** Govt Polytechnic Manesar, Gurgaon**

Abstract:- Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience.

This paper is an attempt to analyze biometrics various types of challenges associated with the technology in near future with core focus on application area.

I. INTRODUCTION

BIOMETRICS:- The need to authenticate ourselves to machine is ever increasing in today's society and is necessary to close the air gap between man and machine to secure our transaction and network [1]. The increase perception of the data and information as near equivalent of currency, in conjunction with the opportunities for the access provided by the internet is paradigm shift with significant repercussion for authentication [2]. Password, pins and tokens have no problems that call into question their suitability for their modern applications, particularly high security application such as access to online financial Accounts. Biometrics offer a strong authentication technology. More than a century ago Alphonse Bertillon first conceived and then industriously practiced the idea of using body measurement for identifying criminal [3]. In 1893 U.K. accepted that no two individual have the same finger prints which led to the development of first automatic finger

prints identification system (AFIS) in the 1960s. Due to the popularity of the AFIS fancy biometric systems shown in Hollywood science fi films and the intuitive appeal of biometric as the crime deterring security tool, biometric systems are successfully deployed in the market over the last couple of decades [4]. Benefits that biometrics provide compared to old authentication method are increased security, convenience, and Accountability which results in fraud detection and is deterrence in biometric technologies is essentially pattern recognition systems. Electronic or optical sensors such as camera and scanning device capture image, recording or measurements of a person's characteristic.

The computer hardware and software extract, encode, store and compare these characteristics result is very rapid biometric decision making that occurs in real-time in

most cases biometric technology have been used in wide area of applications that passports, national id card, refugee and asylum program and welfare fraud identification systems. Only biometrics can recognize as you as you. Biometric has been emerging as an essential component of any effective person identification solution because biometric identifier cannot be shared misplaced, and they intrinsically represent the individuals identity.

USE OF BIOMETRIC TO PROVIDE SECURITY:

An example

Most border security process identity travels by the travel documents such as passport and visas. Biometric on the other hand focuses more on the characteristics that can more securely bind a person's identify to travel document. Such document are more reliable cannot be forgotten and are less easily lost, stolen or gussed. Two process are keys to achieving this bindings. The first is enrollment; the process of establishing document ownership by using unique individual characteristic to create a secure credential. This ties the person's identity to the traveled documents. The identity claimed by the traveler is based on documents such as a birth certificate, passport or other government- issued documents. This enrollment process is required to capture a biometric sample, extract and encode the sample as a biometric template and store the data in a data base to facilitate the second process- identification and verification.

Identification or one-to-many recognition- determines a person's identity by performing matches against multiple biometric templates. Positive biometric identification answers the "who is this person?"

Verification or one-to-one matching or authentication is the process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification answers the question, "am I who I claim to be?"

USE OF FINGRE PRINTS MATCHING TO ACHIVE SECURITY:

It needs to follow certain steps to achieve security via a finger prints

ENROLLMENT: when a would be visitor applies for a passport in home country, his Finger prints must be scanned and its biometric template embedded in the passport.

For ex...the Motorola live scan station, using a proven print track technology, provides

Complete finger printing capabilities in an inkles environment and ideal for machine readable passport.

Features are extracted from the impression made by the distinct ridges

On the figure tips .The finger print image is then scanned, in hands and converted into a

Template enhancement reduces “noise”-caused by dirt, cuts, spares, scars, creases or dry

, wet or worn finger prints-enhances ridge definition. Algorithms extract minutiae; points relating to breaks in the ridges finger prints. Other algorithm extracts ridge patterns

Compilation: The same finger print imbedded in the passport is also entered into the finger print databases of every participating country.

Search/match: During the application process, the biometric automated finger print identification (AFIS) compares then applicant’s finger print against all finger prints in the data bases. If AFIS scores a hit that shows the applicant on a watch list, the application is denied.

The same scanning procedure is followed when a passport holder reaches other country. his finger print scanned again and a scan system is first make sure that his finger print matches the one imbedded in the passport. If not he is stopped. At the same time a compression of that finger print of its AFIS database is also made this entire process takes just moments an credit goes to innovations such as faster match processors enhanced matching algorithms and the significantly expended capability to store ,search and retrieve the right information at the right time.



Leading Biometric Technologies

The leading biometric technologies for security applications include finger prints, face, voice, hand, iris, signature, retina, keystroke etc. All biometric technologies offer promise- some today and some in the future. A matrix of factors-accuracy, ease of use, and stability, vendor and technology experience in the filled track record and acceptance – combined to make some specific biometric applications more widely deployed. Each have their strengths and weakness and are each well-suited for particular application.

Finger prints

Finger print identification has two basic premises: The basic characteristics of finger prints do not change over time and each person’s finger prints are unique. It has been estimated that the number of possible finger print patterns is

10^{48} .this makes duplicates nearly impossible .fingerprint identification has been used in law enforcement for more than a century and has become the de facto international standard for positively identifying individuals. The FBI has been using fingerprint identification since 1928.

Today fingerprint recognition is one of the best known and most widely used biometric technologies. Formulation of finger prints (graphical flow – like ridges) depends on the initial conditions of the embryonic development and they are believed to be unique to each person (and each finger). Optical silicon and ultra sound are the leading methods to acquire fingerprint image of sufficient quality to create finger scan templates. Finger prints mature and proven core technologies capable of high levels of accuracy and can be deployed in the range of environments. The ability to enroll multiple fingers can increase the system accuracy and flexibility. The performance of this system can deteriorate over time and it has a stigma of criminality associated with it (if association with forensic application).

Facial Scan

Facial scan technology utilizes distinctive features of the human face in order to verify or identify individual. This technology identifies people by the sections of the Faces that are less susceptible to alteration- the upper outlines of the eyes sockets, the around the cheekbones and the sides of the mouth. Facial recognition is one of the newer biometric technologies, with systems only recently showing the accuracy necessary for commercial application. Two dimensional face recognition suffers from problems where non frontal images are often not identified or misidentified by the software. Newer 3d facial recognition is showing significant improvements over its predecessor and products should be in the marketplace within the next year.

The face is the only biometric used in a viable recognition technology that is able to operate without the subject’s cooperation. Because facial images can be captured from video cameras, facial recognition is only biometric that – in conjunction with closed circuit television (CCTV) - can be used for surveillance to spot suspected criminals or terrorist whose facial characteristics have been captured and stored in a data base on a template. Facial recognition technology can also be used to compare static images, such as digitized passport photographs, which makes it an ideal biometric to achieve desired security.

There are four types of facial recognitions:-

- Type 1: Photo ID recognition: The computer will compare (match or deny) a stored original image to the picture image identification document .(most accurate)
- Type2: High restriction live image: The person places his chin on a certain spot while his picture is taken .This picture is then compared to the stored image.
- Type3: Low restriction live image: The person is asked to stand in a marked area and look forward.

- Type4: No restriction: The person walks through a security area and his image is captured and compared to the original image.(least accurate).

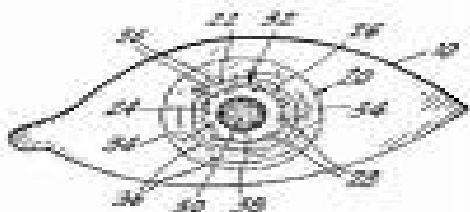
The accuracy of facial recognition is not as reliable as finger print; they are ubiquitous in the world of identity documents .a facial in mage is usually amendatory field on these types of document and can be particularly useful when used with another biometric-for example, a passport the combines a facial image with a finger print .

Iris-Scan

This technology utilizes the distinctive features of the human iris [9]. Developed in 1992, iris recognition is based on the distinctly visible characteristic of the eye's iris, the coloured ring surrounding the pupil-A very rich source of biometric data, with approximately 266 distinctive characteristics. Iris recognition technology uses about 173 of these distinctive characteristics. Iris recognition is one of the most accurate of all biometric technologies with very little overlap between acceptance and rejection curves. The high price of this technology still limits its application to very high security requirements

Iris recognition systems uses a small, high quality camera that provides necessary infrared illumination to capture a black & white, high resolution image of the iris .the technology that defines the boundaries of the iris ,establish a coordinate system over the iris and defines the zones for analysis within the coordinate system. Software components consist of the image processing and matching engines & database.

Some people resist technologies that scan the eye. But iris recognition requires no body contact and is more user-friendly than retina recognition systems in that no light source is shone into the eye and close proximity to the scanner is not required .images of the iris acquired for iris recognition reveal no information about a person's health.



Voice-Scan

Voice-scan technology focuses on voices differences resulting from the shape of vocal tracts and learned speaking habits. The shape of the vocal tract determines, to large degree, how a voice sounds [10]. Voice-scan technology is text-dependent the system can't verify a speaker speaking random snippets of text. A user's spoken phrase is converted from analog to digital format and transmitted to a local for central PC for template generation, storage and matching.

Voice-scan can be effectively layered with speech recognition and verbal passwords but the large size of template limits the number of potential application. Because voice recognition operates best when there's no background noise, it still has a error rate of five percent. As compared to other biometric technologies, it is potentially more susceptible to replay attacks.

Hand Geometry

Hand-scan technology utilizes the distinctive aspects of the hand; for example the height and the width of the back of the hand and fingers. Hand-scan is more application-specific solution than most biometric technologies, used exclusively for physical access and attendance applications. All components of a hand-scan system reside within a standalone device. Hand-scan system can be used in conjunction with cards that store user IDs for templates retrieval. Hand-scan development can be locally or centrally managed. Based on a relatively stable physiological characteristics, this technology is reliable, established and generally perceived as none intrusive. The ergonomic design limits uses by certain population and the form factor limits the scope of potential application [1].[2]

Retina Scan

One distinctive characteristic of the retina , the surface on the back of the eye, that process light entering through the pupil is used here [2].it is relatively new technology, developed in the 1980s and is one of the least deployed also. based on a relatively stable physiological characteristic , this technology is used exclusively for physical access application and in application requiring exceptional or high degree of security .retina scan and iris scan differs substantially .they measure different physiological features and also the software and hardware required for the too are quite dissimilar. Retina scan systems are self contained, with acquisition hardware as well as templates processing components within a dedicated device. Due to user discomfort it has limited application.

Signature recognition

Signature are a behavioral biometric and there are two approaches to signature verification [11].Static (geometric/shape features of the signature are used for authentication) and dynamic (shape features plus dynamic features like acceleration, velocity and trajectory profiles of the signature are used for authentication). Signature recognition is a biometric technology that has been worked on for some years and the dynamic recognition of relative pen speeds and pressures has significantly improved the accuracy. This technology is also now at a price that is well within the budget of many organizations

The real hurdle with this technology is differentiating between the consistent parts of the signature and the behavioral parts of the signature that vary with each signing. And individual's signature is never entirely the same every

time it is signed and can vary substantially over an individual's lifetime. There are also the problems of dealing with foreign languages and people with writing difficulties.

Keystroke Recognition

Assesses the user's typing style, determining dwell time (how long each key is depressed), flight time (how long to move between keys) and such other characteristics as typical typing error. However, keystroke recognition is an internal security technology-say, for providing computer access within an organization-and is not applicable to border security.

DNA (De-Oxy-Ribo Nucleic Acid) Identification

DNA is the ultimate unique code for one's individuality – except for the fact that identical twins have the identical DNA pattern. Currently it is used mostly in the forensic applications for identification [12]. Three issues limit the utility of this biometrics for other applications [1]: (i) Contamination and sensitivity (it is easy to steal a piece of DNA from an unsuspecting subject to be subsequently abused for an ulterior purpose); (ii) Automatic real-time identification issues (the present technology for genetic matching is not geared for online unobtrusive identifications); (iii) Privacy issues (information about susceptibilities of a person to certain diseases could be gained from the DNA pattern).

Gait Recognition

Gait is the peculiar way one walks and is a complex spatio-temporal behavioral biometrics. Gait is not supposed to be unique to each individual, still this characteristics allows identity authentication [13]. The characteristics gait of a human walk has been well researched in biometrics community to detect abnormality in lower extremity joints; the use of gait identification purposes is very recent. Typically, gait features are derived from an analysis of video-sequence footage of a walking person [14] and consist of characterization of several different movements of each articulate joint. Still in early developmental stage, right now this technology is plagued by accuracy problems.

Thermograms

Human body radiates heat and the pattern of heat radiation is a characteristic of each individual body [15]. An infrared sensor could acquire an image indicating the heat emanating from different parts of the body. These images are called thermograms. The method of acquisition of the thermal image unobtrusively is akin to the capture of a regular (visible spectrum) photograph of the person. Any part of the body could be used for identification. The absolute values of the heat radiation are dependent upon many extraneous factors and are not completely invariant to the identity of an individual; the raw measurement of heat radiations need to be normalized, e.g. with respect to heat radiating from a landmark feature of the body. The technology can distinguish between identical twins also and claim to provide enabling

technology for identifying people under the influence of drugs, (the radiation pattern contains signature of each narcotic drug) [16]. In uncontrolled environment heat emanating surfaces in the vicinity of the body, e.g. room heaters and vehicle exhaust pipes, may drastically affect the image acquisition phase, infrared facial thermograms seems to be acceptable since their acquisition is a non invasive sensing technique. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of thermograms.

Some other biometrics are nail-bed identification (vertical ridges beneath human finger nail), odor, subcutaneous hand-scan (tissues structure below surface of skin on the palm), and vein identification (vein pattern on the back of hand).

APPLICATIONS

Network / PC Login Security

Biometric Logon for PC and Networks is now well developed with a number of players in the market. Best of these in our view is the Identix technology which is integrated into Windows 2000 Active Directory and provides rapid verification at logon. The second player in this market is the Digital Persona system which is slightly behind the Identix system in its development but still provides a robust and affordable solution.

Web Page Security

For the most effective security for web pages, the Bio Web Server system is the leading market player. Integrated with a number of hardware options including Digital Persona, which we at Eye Net Watch reckon is the most reliable the system is easy to install and to integrate with web applications. This system has provided security for the admin system for Global Real Estate for the last 3 years.

Employee Recognition

There are many employee recognition systems available but Biometrics provides a cheaper alternative to most, very few people lose their fingers or eyes when compared with those who lose smartcards or forget passwords.

Time and Attendance Systems

Time and attendance has always been a problem in some industries. Biometrics can effectively eliminate problems with buddy clocking by ensuring that the employee in question is present.

Voting Solutions

The management of voters to ensure no one votes twice has been a notoriously difficult application; however recent developments in the technology have allowed governments to adopt a high degree of security to prevent such a problem

Concluding Remarks

Although successful in some niche markets, the biometric technologies have not yet delivered its promise of foolproof automatic identification. For example, almost a century after the fingerprints were observed to be unique, a 2004 fingerprint contest revealed that fingerprints matching have an equal error rate of 2%. If this system were to be deployed on an Airport of capacity ~ 200,000 passengers/day it would result in 4,000 false alarms and 4,000 false rejects everyday! While the error rate of the fingerprint system can be significantly reduced by using significantly reduced by using multiple fingers, the point we want to emphasize is that the

error rate is non zero. Similarly, even through the first paper on automatic face recognition appeared in early 1970'ss, the state of the art face recognition systems have been known to be fragile in the recent operational tests. Face recognition system have also been proven fragile. Iris scan technology has extremely low error rates, but it also displays signs of fragility in the recent pilot studies .In case of voice scan technology also some critical issues need to be addressed. If we can make biometric system more secure, robust and cost-effective, the result will be a widespread adoption of biometric system, resulting in broad economical and social impact.

REFERENCES:-

- [1]. Jain AK, Biometrics: personal identification in networked society, Kluwer Academic, dec 1998
- [2]. Biometrics technologies by prietee khanna.