An Introduction to Biometrics: The Power of Security

Selva Priya G[1], Anitha P[2], Vinothini C[3]

[1]PG Scholar, Department of CSE, Dr. N.G.P Institute of Technology
[2]Assistant Professor , Department of CSE, Dr. N.G.P Institute of Technology
[3]Assistant Professor, Department of CSE, Dr. N.G.P Institute of Technology

***Abstract*- Biometrics is the science of establishing security for person identification. It refers to the automatic recognition of a person based on his/her physiological or behavioral characteristics. It is possible to confirm or establish an individual's identity based on the traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness by using biometrics. Examples of such applications include secure access to laptops, buildings, cellular phones, computer systems and ATMs. In the absence of strong personal recognition schemes, these systems are vulnerable to an impostor. In this paper, a brief overview for biometrics will be presented.**

***Index terms Biometrics, security, identification, impostor*.**

I. INTRODUCTION

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [1]. A biometric system based on a physiological characteristics is generally more reliable than one which adopts behavioral characteristics, even if the latter may be more easy to combine within certain specific applications. Biometric system which perform in two modes: verification or identification. Identification which comparing the acquired biometric information against templates corresponding to all users in the database. In verification, it involves comparison with only those templates corresponding to the privilege identity. This suggests that identification and verification are two problems that should be deal with separately. A biometric system consists of four basic components:

- Sensor – It collects data and then converts the information to a digital format.
- Signal processing algorithms – It perform quality control activities and then develop the biometric template.
- Data Storage – It keeps information that new biometric templates will be compared to
- Matching algorithm – It compares the new biometric template to one or more templates in data storage
- Decision Process – It uses the results from matching component to make a system-level decision (either automated or human-assisted)

A. Physiological vs. Behavioral

When describing this biometric technology, it is essential to distinguish between physiological and behavioral human characteristic.

A physiological characteristic is relatively a stable human physical characteristic, such as a iris pattern, fingerprint, or blood vessel pattern on the back of the eye. This type of measurement is coherent and fixed without significant duress. Alternatively, a behavioral characteristic is a reflection of an individual psychological character, although physical peculiarity such as size and gender have a major inspiration. Some of the examples of behavioral peculiarity used to identify individuals include: Keystroke dynamics, and speech identification and/or verification [2].

B. Physical Biometrics

1. Fingerprint: Analyzing fingertip blueprint

2. Facial recognition/face location: Measuring facial physical appearance

3. Hand geometry: Measuring the of the hand outline

4. Iris scan: Analyzing highlight of colored ring of the eye

5. Retinal scan: Analyzing blood container in the eye

6. Vascular patterns: Analyzing vein blueprint

7. DNA: Analyzing genetic nature

8. Biometric data watermarking (which is really a method rather than a physical aspect) is used to store/hide biometric information [3].

C. Behavioral Biometrics

1. Speaker/voice recognition: Analyzing vocal deeds

2. Signature/handwriting: Analyzing signature active

3. Keystroke/patterning: Measuring the interval spacing of typed words

II. TYPES OF BIOMETRIC SYSTEMS

A. Unimodal biometric systems

There is a collection of problematic with biometric systems installed in real world applications which prove that biometrics is not fully solved problem.

Drawback of biometric systems using any distinct biometric characteristic [4]:

1) Noise in sensed data: Example is a fingerprint with a panic. Earsplitting data can also result from accumulation of dirt on a sensor or from ambient conditions.

2) Intra-class variations: Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during registration. This distinction is typically caused by a user who is incorrectly interacting with the sensor.

3) Distinctiveness: While a biometric trait is expected to vary significantly across persons, there may be large different class similarities in the feature sets used to represent these traits. This drawback restricts the intolerance provided by the biometric trait.

4) Non-universality: While every user is expected to possess the biometric trait being acquired, in reality it is possible that a group of users do not posses that particular biometric characteristic.

5) Spoof attacks: An individual may attempt to forge the biometric trait. This is predominantly straightforward when signature and voice are used as an identifier.

B. Multimodal biometric systems

Drawbacks of unimodal biometric systems can be overcome by using multimodal biometric systems [5]. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the combination of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are probable to be more consistent due to the presence of multiple, individual pieces of proof [6]. These systems are able to encounter the severe performance requirements imposed by various applications [7]. A multimodal system could be, for case in point, a mixture of face recognition, voice verification, fingerprint verification.

A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the assimilation of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are probable to be more consistent due to the presence of multiple, individual pieces of proof. These systems are able to encounter the severe performance requirements imposed by various applications.

A multimodal system could be, for case in point, a mixture of face recognition, voice verification, fingerprint verification and smart-card or any other combination of biometrics. This superior structure takes benefit of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric.

III. A COMPARISON OF VARIOUS BIOMETRICS

There are several human distinguishable traits that fit the definition of biometrics. In order to be used for distinguish a person, the human feature needs to be distinctive and no matter to change. Fingerprints, for example, have been used for over one hundred years and, therefore, are commonly well acknowledged as a recognition technology. Other technologies such as hand geometry, speaker and iris recognition, face are also commonly accepted. A biometric that would require giving a blood sample for frequent personal verification would probably not be very well prevalent. Performance considerations are significant. No biometrics can warrant one hundred percent correctness. A short-term beginning of the commonly used biometrics is given below:

DNA: Deoxyribo Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA blueprint. It is, however, recently used above all in the context of forensic applications for person identification. [8] Three misgivings bound the utility of this biometrics for other applications:

(i) Contamination and sensitivity

(ii) Automatic real-time recognition issues

(iii) Privacy issues

Ear: It has been suggested that the shape of the ear and the structure of the cartilegenous tissue of the pinna are characteristic. The ear recognition methods are based on matching the distance of salient points on the pinna from a landmark site on the ear. The structure of an ear are not anticipated to be very distinctive in establishing the identity of an individual. [8]

Face Recognition: Different technologies can be used for face recognition. One method consists on observing an image of the face using an inexpensive camera (visible spectrum). This method classically models key characteristics from the central portion of a facial image

extracting these features from the captured image(s) that do not change over time while avoiding superficial features such as facial appearance or hair. Major charity event of facial recognition are that it is non-intrusive, hands-free, provides for continuous authentication and is accepted by majority users. Acceptance sample sizes(e.g., 5 face samples) may range from 1 KB-2KB/sample). Smaller template sizes are also used (e.g., less than 100 bytes). [9]

Fingerprints: Fingerprints are essential. By 1998, fingerprint recognition products reported for 78% of the total sales of biometric skill. These products look at the abrasion ranges that cover the fingertips and organize patterns, such as branches and end points of the ridges. Some also look at the apertures in the skin of the ridges. Fingerprint recognition gadget for desktop and laptop access are widely available from many different vendors at a low cost. [10] The relatively small size allows the sensor to be integrated in other devices (e.g., mice, keyboards). This biometric technology uses the pattern of friction ridges and valleys on an person's fingertips. These outline are considered distinctive to a specific person. The same fingers of equal twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A representative enrollment identifier may include two finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the trials of fingerprint expertise is individuals that have poorly defined (or tenuous) ridges in their fingerprints. [9]

Gait: Gait is the peculiar way one walks and is a complex spatial-temporal biometric. Gait is not supposed to be very typical, but is amply discriminatory to allow verification in some low-security applications. posture is a behavioral biometric and may not wait invariant, unusually over a long period of time, due to vicissitudes in body weight, chief grievances involving joints or brain, or due to intoxication.[11]

Hand and Finger Geometry: Hand recognition has been available for over twenty years. To realize personal certification, a system may measure physical characteristics of the fingers or the hand such as length, width, thickness and outward area of the hand. These procedures of personal certification are well established. [9] Some systems require a very small biometric sample (e.g., 9 bytes). Hand geometry can frequently be found in physical access control for commercial and residential purposes, for time and turnout systems, and for common personal certification applications. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. [11]

Iris: As far as is known, every human iris is measurably distinctive. It is fairly easy to detect in a video picture, does not wear out, and is secluded from the external environment by the cornea (which in turn has its own cleaning mechanism). The iris blueprint contains a large amount of casualness and emerge to have many times the number of degrees of freedom of a fingerprint. It is molded between the third and eighth month of gestation, and (like the fingerprint pattern) is phenotypic in that there appears to be limited genetic influence; the mechanisms that form it appear to be tumultuous. So the blueprint are different even for identical twins (and for the two eyes of a single individual), and they materialize to be stable throughout life. [8]

Retinal Scanning: This method of personal authentication uses the vascular patterns of the retina of the eye. [9] In healthy individuals, the vascular pattern in the retina does not change over the course of an person's life. The blueprint are scanned using a low-intensity (e.g., near-infrared) light source. It need the user to look into a device and focus on a given point. The image acquisition involves coordination of the subject, entails contact with the eye fragments. [10]

Signature Verification: The way a person signs her name is known to be a characteristic of that person. Monogram of some people vary materially: even successive impressions of their signature are substantially different. [17] It is based on measuring energetic signature features such as velocity, gravity and direction used when a person signs a standard, recorded pattern (e.g., autograph). One spotlight for this method has been e-business applications. [9]

Voice Recognition: Voice recognition or speaker recognition is the problem of identifying a speaker from a short utterance. [8] This biometric technology uses the acoustic features of speech that have been found to differ between person. These acoustic methods reflect both framework (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). [9] A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as contextual blast. Speaker recognition is most suitable in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel. [10]

IV. COMPARISON BETWEEN VARIOUS BIOMETRICS

Biometrics	Advantages	Disadvantages
Facial recognition	It does not require any co-operation of the test subject to do any work. This performs massive identification which usually other biometric system can't perform [13]	Face recognition isn't perfect and face challenges to perform under certain conditions. Not much effective for low resolution images [13].
Iris	High accuracy and High recognition process speed [13]. Scalability along with the speed is significantly advantageous [14].	Iris scanners tend to be more expensive in comparison with additional biometrics [12]. Iris recognition is vulnerable to inadequate image quality.
Finger print	A fingerprint pattern has individually distinctive composition and characteristic remains the same with time [13]. It is easy to use along with the high verification process speed and accuracy [12].	Cuts, marks transform fingerprints which often has negatively effect on performance [13]. Finger prints aren't private. The finger prints are for life time and there is no way to get back to a secure situation [15].
Finger Vein	Vein patterns need only low image resolution. The level of accuracy from vein recognition systems is quite outstanding.	Expensive: The actual technologies seriously aren't cheap enough for bulk deployment. Larger Size: The existence of CC camera makes the system larger than a fingerprint scanner.
Voice recognition	This technique helps those people who have difficulty of using their hands. It does not require any training for users.	May hacked with prerecorded voice messages. Possesses primary amount of time for adjustment with each user's voice

V. CONCLUSION

This paper presents a shorter introduction on numerous biometric techniques undertaking the comparison examination regarding widely used biometric identifiers and also the identification strategies. As this is a new technology for most of the peoples since it has simply been implemented in public areas for short time period. It provides benefits that may improve our lives in such a way by increasing security and efficiency, decreasing scams and reducing password administrator cost. Despite the fact the biometrics security systems still have many issues like data privacy, physical privacy, and spiritual arguments.

VI. FUTURE WORK

Biometrics technology is used in a number of ways and in different fields of our daily lives. In future we mainly focus on facial expression recognition technology. Using this technology, we can easily identify a person in a crowd and by so we can verify their identity. We can furthermore make use of this technology to detect previously identified terrorists, criminals or scammers in society. It may help us to reduce the criminal offense in the world. But as we can see from the above given comparison between different biometrics, it is clear that face recognition faces a challenging problem in the field of accuracy, efficiency, speed cost and security. So we need to work upon it to make

it more effective.

REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42.
[2] Arpita Gopal, Chandrani Singh, e-World : Emerging Trends in Information Technology, Excel Publication, New Delhi (2009).
[3] John Woodward, Nicholas M. Orlans, Peter T. Higgins, Biometrics, Tata McGraw Hill.
[4]A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.
[5] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?," in Proc. AutoID'99, Summit, NJ, October 1999, pp. 59-64.
[6] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good for combining classifiers?," in Proc. Int. Conf. Pattern Recognition (ICPR), Vol. 2, Barcelona, Spain, 2001, pp. 168-171.
[7] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," IEEE Trans. Pattern Analysis Machine Intell., Vol. 20, pp. 1295-1307, December 1998.
[8] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
[9] Fernando L. Podio: "Personal Authentication Through Biometric Technologies".
[10] Ross Anderson's: "Chapter 13th Biometrics of Security Engineering".
[11] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
[12] Anil K. Jain, Arun Ross and Salil Prabhakar (2004), "An Introduction to Biometric Recognition.".
[13] Alina Klokova, "Comparison of Various Biometric Methods".
[14] Joseph N. Pato and Lynette I. Millett, Editors; Whither Biometrics Committee; National Research Council (2010), "Biometric Recognition: Challenges and Opportunities".
[15] David Weiss (2009), "Fingerprint Biome.