Biometric Recognition: A Literature Review

C.B. Tatepamulwar[#], V.P. Pawar[#], H.S. Fadewarr[#3]

[#]*School of Computational Sciences,*
Swami Ramanand Teerth Marathwada University
Nanded(Maharashtra), India
[3]fadewar_hsf@yahoo.com

Abstract - Biometric as the science of recognizing an individual based on his or her physical or behavioral traits, it is beginning to gain acceptance as a legitimate method for determining an individual identity. Biometric have now been deployed in various commercial, civilian, and national security applications. Biometric described various biometric techniques and the need to be addressed form making biometric technology an effective tool for providing information security. This research paper is focus on how literatures review of the biometric applications that they are useful in HCI.

Keywords - Biometrics, digital rights management, receiver operating characteristics.

I. *INTRODUCTION*

Biometrics refers to certain physiological or behavioral characteristic that is uniquely associated to a person. This trait is highly distinctive and can be utilized for distinguishing different individuals.

Physiological biometrics refers to a person's physical attribute, such as fingerprint, face, and iris. It is well known for its permanence and high uniqueness that promote high recognition accuracy. Unfortunately, it is not likely to be revoked if compromised (unable to change fingerprint pattern) [4], may possibly suffer low public acceptance due to invasiveness (iris scanning), and could be unlikely practical in large-scale deployment due to implementation cost (DNA analysis).

The way people do things such as speaking (voice), writing (signature), typing (keystroke dynamics), and walking style (gait recognition) are known as behavioral biometrics. Behavioral biometrics has the edge over its physiological counterpart on the ability to work in stealth mode verification. As such, minimal interaction is required during authentication process reduces invasiveness and thus promotes user acceptability. In addition, in the event if one's behavioral attribute is compromised, it is likely to be replaced (changing to a new password, thus, new keystroke print or new written signature) [5]. While these merits may be encouraging, they are normally inferior to physiological biometrics in terms of variability (voice changes along with aging factor) and may consequently influence verification accuracy computer. interaction (HCI) is a multidisciplinary field concerned with the application of computer science, psychology, cognitive science, ergonomics and many other disciplines[1]. It is the study of how people interact with computer and to what extent computers are or not developed for successful interaction with human beings

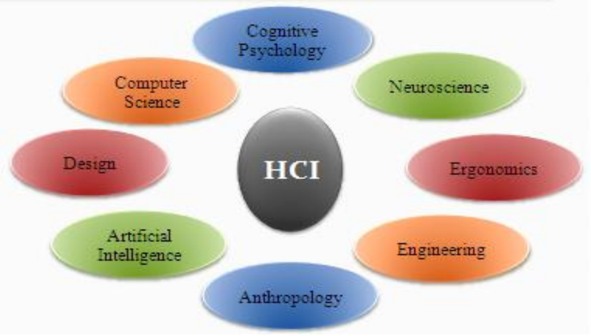

Fig : Multidisciplinary Research in HCI.

Human-computer interaction is becoming an active and important research area. Adequate feedback like speech, facial expression and body gestures are essential modalities of such interaction since these components satisfy certain communication expectations in human-human interaction. Furthermore, the human face constitutes a source of informative social signs which allow good communication expectation response[2].

II. *TYPE OF BIOMETRICS*

They involve two categories: physiological biometrics and behavioral biometrics.[7]

A. *Physiological Biometrics*

The **Figure 1** shows this category the recognition is based upon physical characteristics. (e.g., face, fingerprint, hand, iris, DNA).

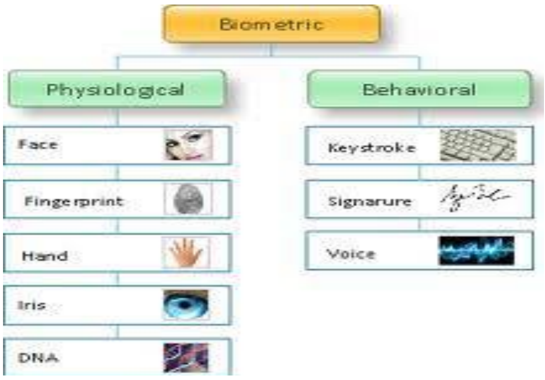

Fig.1. Biometric characteristic

1. *Fingerprint*

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons [4].

2. *Face Recognition*

Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either *(i)* the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or *(ii)* the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order that a facial recognition system works well in practice, it should automatically *(i)* detect whether a face is present in the acquired image; *(ii)* locate the face if there is one; and *(iii)* recognize the face from a general viewpoint (i.e., from any pose)[4].

3. *Iris Recognition*

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective [4].

4. *Speech Recognition*

Speech recognition or Automatic Speech Recognition (ASR) system is converts the acoustic signal (audio) to a machine readable format. ASR recognizes the words & these words are worked as input for a particular application, it may be worked as command or for document preparation. Now a day there is glamour of designing an intelligent machine that can recognize the spoken word & understand its meaning & capture corresponding actions. One of the most difficult aspects of performing research in speech recognition by machine is its interdisciplinary. The early studies focus on monolithic approach to individual problems [8].

5. *Gesture Recognition*

Gesture recognition can be seen as a way for computers to begin to understand human body language, thus building a richer bridge between machines and humans than primitive text user interfaces or even GUIs (graphical user interfaces), which still limit the majority of input to keyboard and mouse. Gesture recognition enables humans to interface with the machine (HMI) and interact naturally without any mechanical devices. Using the concept of gesture recognition, it is possible to point a finger at the computer screen so that the cursor will move accordingly. This could potentially make conventional input devices such as mouse, keyboards and even touch-screens redundant. Gesture recognition can be conducted with techniques from computer vision and image processing. The literature includes ongoing work in the computer vision field on capturing gestures or more general human pose and movements by cameras connected to a computer [6].

6. *Gait Recognition*

Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive [4].

7. *Handwriting Recognition*

Computer Recognition of handwritten cursive script has received relatively little attention, until recently, when compared to Optical Character Recognition (OCR), speech recognition, and other image or scene analysis areas. Interest began to grow significantly in the 1980s and 1990s [7].

8. *Palm Print Recognition*

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and as a result, palm prints are expected to be even more distinctive than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [5]. When using a high resolution palm print scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system [6].

9. *Ear Shape Recognition*

It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive.

The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual [4].

B. Behavioral Biometrics

The **Fig 1** shows behavioral biometrics is traits that is learned or acquired over time as differentiated from physical characteristics (e.g., keystroke, signature, voice).

1. Keystroke Recognition

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information [7].

2. Signature Recognition

Some dynamic signature recognition algorithms incorporate a learning function to account for the natural changes or drifts that occur in an individual's signature over time. The characteristics used for dynamic signature recognition are almost impossible to replicate. Unlike a graphical image of the signature, which can be replicated by a trained human forger, a computer manipulation, or a photocopy, dynamic characteristics are complex and unique to the hand writing style of the individual. Despite this major strength of dynamic signature recognition, the characteristics historically have a large intra-class variability (meaning that an individual's own signature may vary from collection to collection), often making dynamic signature recognition difficult. Recent research has reported that static writing samples can be successfully analyzed to overcome this issue

3. Voice Recognition

Voice Recognition is a technology which allows a user to use his/her voice as an input device. Voice recognition may be used to dictate text into the computer or to give commands to the computer (such as opening application programs, pulling down menus, or saving work). Older voice recognition applications require each word to be separated by a distinct space. This allows the machine to determine where one word begins and the next stops. These kinds of voice recognition applications are still used to navigate the computer's system, and operate applications such as web browsers or spread sheets. Newer voice recognition applications allow a user to dictate text fluently into the computer. These new applications can recognize speech at up to 160 words per minute. Applications that allow continuous speech are generally designed to recognize text and format it, rather then controlling the computer system itself. Voice recognition uses a neural net to "learn" to recognize your voice. As you speak, the voice recognition software remembers the way you say each word. This customization allows voice recognition, even though everyone speaks with varying accents and inflection[9].

In addition to learning how you pronounce words a voice recognition also uses grammatical context and frequency of use to predict the word you wish to input. These powerful statistical tools allow the software to cut down the massive language data base before you even speak the next word. While the accuracy of voice recognition has improved over the past few years some users still experience problems with accuracy either because of the way they speak or the nature of their voice[10].

III. CONCLSION

Biometrics refers to an automatic authentication of a person based on his physiological and/or behavioral characteristics. The usage of biometrics as a reliable means of authentication is currently gaining momentum, thou the industry is still evolving and emerging.

IV. REFERENCES

1. *Jin-Hyuk Hong, Eun-Kyung Yun, and Sung-Bae Cho, "A Review of Performance Evaluation for Biometrics Systems", International Journal of Image & Graphics, vol. 5, no.3 (July 2005), pp. 501-36.*
2. *Zhenan Sun, Tieniu Tan. [2009]. "Ordinal Measures for Iris Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 31, No. 12, pp. 2211 - 2226.*
3. *Hugo Proenca, Lui's A. Alexandr [2007]. "Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, SPECIAL ISSUE ON BIOMETRICS, VOL. 9, NO. 4, .pp. 607 – 612.*
4. *Anil k. Jain, fellow, IEEE, Arun Ross, member, IEEE," Biometrics : A Tool for information security" IEEE Transactions on information forensics and security. VOL.1.No.2.June 2006.*
5. *AES Encryption Information. http://www.bitzipper.com/aes-encryption.html.*
6. *Advanced encryption standard. tp://en.wikipedia.org/wiki/Advanced_encription_standerd*
7. *Biometrics and Biostatistics. http://www.omicsonline.org/jbmbshome.php*
8. *Biometrics for network security Paul Reid, 2004 by pearson education.*
9. *Alfredo c.lopez,,Ricado R. lobez "fingerprint rscognition".*
10. *Jammi Ashok, vaka shivashankar,"An overview of biometrics".(IJCSE)International journal an computer science and Engineering. VOL.02.no.07 ,2010.*