Multimodal Biometrics: An Enhanced Authentication Technique

Mohamed Basheer K. P., PhD
Assistant Professor
Department of Computer Science,
SS College, Areacode, Malappuram-Dt, Kerala

Haulath K.
Assistant Professor
Department of Computer Science,
EMEA College, Kondotty. Malappuram-Dt, Kerala

ABSTRACT
Biometrics refers to identify an individual, based on human' physiological or behavioral characteristics. Many unimodal biometric systems exist, but often has limitations due to sensitivity to noise, data quality, spoofy attack etc. Multimodal biometric system evaluates some of the problem by providing multiple biometric features of same identity. This system helps to achieve an increased performance that may not be possible by using single biometric indicator.

Keywords
Traditional method, Biometrics, Unimodal system, Multimodal biometrics, Biometrics traits

1. INTRODUCTION
Any human characteristics which may be used for biometric authentication and identification. The automatic identification or identity verification of living human individuals based on behavioural or physiological characteristics. Biometric are used for authentication and unique identification of data or system security. The traditional techniques for authentication and identification are username, bank card, password, pin code respectively. There are lot of limitation in the traditional method. Biometric system provides strong authentication and identification method over traditional method. Biometric system provides very good strong measurement of authentication. In recent years' biometrics has become an increasingly feasible solution for reduced cost, reduced size, increased accuracy, increased ease of use in an authentication mechanism. The biometric system can't be lost or others can't able to guess it like password pin etc. one of the main advantage associated with biometric technology is high individual identification accuracy.

The following figure shows the categories of Behavioural and physiological characteristics.

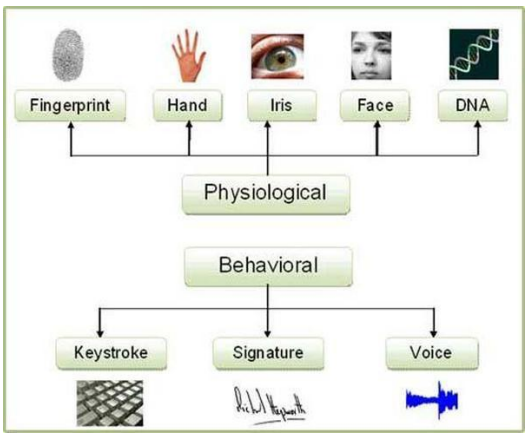

Figure 1: Categories of Biometrics.

If one physiological characteristic is considered for recognition, then they are termed as unimodal recognition systems. When multiple or a combination of personnel biometrics are considered then they are termed as multimodal biometric recognition systems. The aim of this paper is to recommend the literature survey on various multimodal biometric recognition. Other sections of this paper are categorized as follows. Section 2 discusses mode of Biometrics. Section 3 discuss multimodal biometric identification. Section 4 discuss advantage of multimodal identification over unimodal. Conclusion of the paper is discussed in section 5. Section 6 list the references.

2. MODES OF BIOMETRICS
2.1. Fingerprints
The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available, users no longer need to type passwords– instead, and only a touch provides instant access.

Fingerprint systems can also be used in identification mode (3). Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names. Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century fingerprints have been extensively used for identification of criminals by the various forensic departments around the world. Due to its criminal connotations, some people feel uncomfortable in providing their fingerprints for identification in civilian applications.

However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence, and compact solid state fingerprint sensors can be embedded in various systems (e.g., cellular phones), fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in. The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. Fingerprints also have a number of disadvantages as compared to other biometrics.

Figure 2a: finger tip

Figure 2b: finger print matching mechanism

2.2 Iris Recognition

This recognition method uses the iris of the eye which is the coloured area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

Figure 3: iris sample

2.3. Face Recognition

The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modelling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non- intrusive, hands-free, and continuous and accepted by most users.

2.4. Voice Recognition

Voice recognition has a history dating back some four decades, where the output of several analogue filters were averaged over time for matching. Voice recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioural patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice templates (the latter called "voiceprints") has earned speaker recognition its classification as a "behavioural biometric. "Voice recognition systems employ three styles of spoken input: text-dependent, text-prompted and text independent.

Figure 4: face recognition system.

Most voice verification applications use text- dependent input, which involves selection and enrolment of one or more voice passwords. Text- prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints include hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Performance degradation can result from changes in behavioural attributes of the voice and from enrolment using one telephone and verification on another telephone. Voice changes due to aging also need to be addressed by recognition systems. Many companies market voice recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometric is seen as non-invasive. The technology needs little additional hardware by using existing microphones and voice-transmission technology allowing recognition over long distances via ordinary telephones (wired or wireless).

Figure 5:sample voice clip as shown in sound editor

2.5. Hand and Finger Geometry

These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

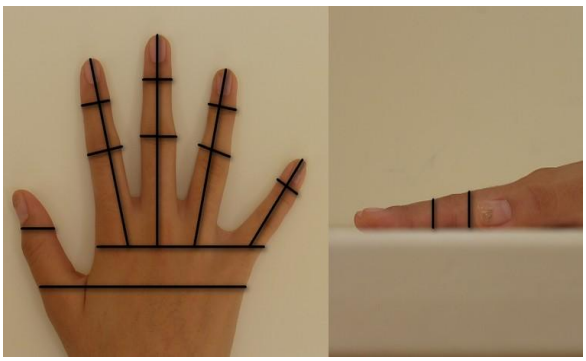

Figure 6: Geometry of a hand

2.6. Signature Verification

This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e- business applications and other applications where signature is an accepted method of personal authentication.

Figure 7: Signature scanning

3. MULTIMODAL SYSTEMS

Multi-modal biometrics is the system that is capable of using more than one physiological or behavioural characteristic for enrolment, verification, and identification. Human identification based on multi-modal biometrics is becoming an emerging trend, and one of the most important reasons to combine different modalities is to improve recognition accuracy. There are additional reasons to combine two or more biometrics such as the fact that different biometric modalities might be more appropriate for unique deployment scenarios or when security is of vital importance to protect sensitive data.

Multi-modal biometric systems take input from single or multiple biometric devices for measurement of two or more different biometric characteristics. For example, a multi-modal system combining fingerprint and iris characteristics for biometric recognition would be considered a multi- modal system regardless of whether fingerprint and iris images were captured by different or the same biometric devices. It is not a requirement that the various measures be mathematically combined in any way because biometric traits remain independent from each other, which results in higher accuracy when identifying a person .

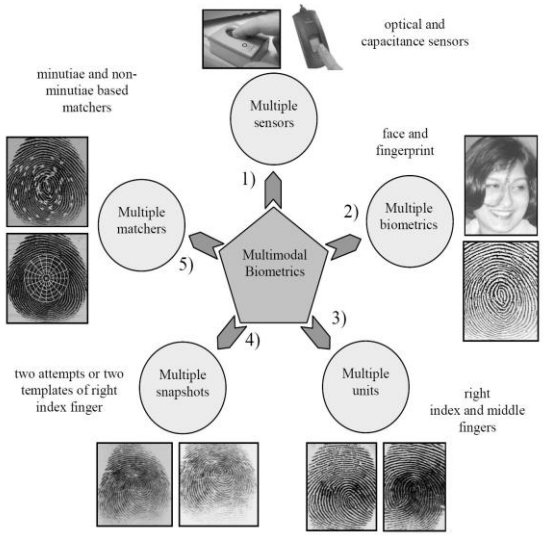

Figure 8: Scenarios in a multimodal biometric system

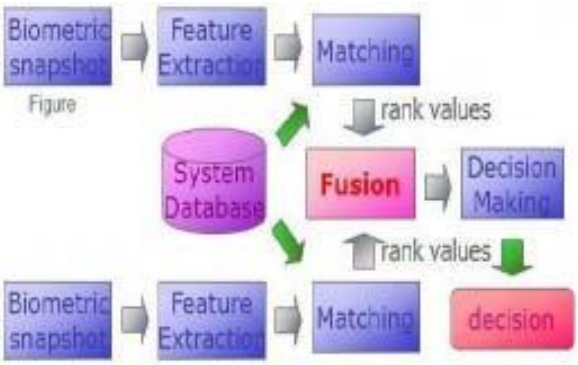

Figure 9: Flow of multimodal system

4. LIMITATIONS OF UNIMODAL TRAITS

4.1. Noise in sensed data

The sensed data might be noisy or distorted. A fingerprint with a scar or a voice altered by cold are examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavourable ambient conditions (e.g., poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

4.2. Intra-class variations

The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrolment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified (e.g., by changing sensors—the sensor inter- operability problem) during the verification phase. As another example, the varying psychological makeup of an individual might result in vastly different behavioural traits at various time instances.

4.3. Inter-class similarities

While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait.

4.4. Non-universality

While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users not to possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges, thus, there is a failure to enrol (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors.

4.5. Spoof attacks:

An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioural traits such as signature and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/ fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

5. ADVANTAGES OF MULTIMODAL BIOMETRICS

5.1. Accuracy

Multi-modal biometric uses multiple modalities to identify a person which ensures higher accuracy.

5.2. Security

Multi-modal biometric systems increase the level of security by eliminating any chance of spoofing. It is unlikely that a person would be able to spoof multiple types of biometric traits at once.

5.3. Liveness Detection

Multi-modal biometric systems ask end users to submit multiple biometric traits randomly which ensures strong liveness detection to protect from spoofing or hackers.

5.4. Universality

A multi-modal biometric system is universal in nature, even if a person is unable to provide a form of biometric due to disability or illness, the system can take other form of biometric for authentication.

5.5. Cost-effective

Multi-modal biometric systems are cost effective by providing higher levels of security to lessen the risk of breaches or criminal attacks.

6. CONCLUSION

Multi-modal biometric systems have performed well in addressing the problems of unimodal systems by combining information from different sources and improve the systems performance, the use of multiple biometric traits for recognizing persons, known as multimodal biometrics, has been shown to enhance precision and population coverage, while decreasing vulnerability to spoofing. Several studies prove the advantages of multimodal biometrics.

7. REFERENCES

[1]. N Gopal, Dr R Selvkumar-Multimodal Biometric System – An Overview International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 7- March 2016.

[2]. Kalyani CH, Various Biometric Identification Techniques: A Review. journal of Biometrics and Biostatistics.

[3]. Ratha.N et al. "Adaptive flow orientation based feature extraction in fingerprint images Pattern Recognition", Vol.11, Issue 28 (1995), pp. 1657–1672.

[4]. Mini Singh Ahuja, Sumit Chabbra A survey of Multimodal Biometrics. International journal of Computer Science and its Applications.

[5]. A. Ross and A . K. Jain, *"Multimodal biometrics: an overview,"* Proc.European Signal Processing Conference, pp. 1221–1224, Vienna, Austria, Sept 2004.

[6]. *Arun Ross and Anil K. Jain* Multimodal Biometrics: An Overview

[7]. T.Sabhanayagam , Dr. V. Prasanna Venkatesan and Dr. K. Senthamaraikannan· A Comprehensive Survey on Various Biometric Systems. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2276-2297 © Research India Publications.

[8]. J.Wayman , A Jain, D. Maltoni, D.Maio, Biometric systems , Technology ,Degign Performance evaluation, Springer 2005.

[9]. A.K.Jain, A.Ross and S.Prabhakar, "An introduction to biometric recognition ", IEEE Trans. On Circuits and Systems for Video Technology, vol 14, pp. 4-20, Jan 2004. [10]. Bounkong, S., Toch, B., Saad, D. and Lowe, D. (2003) ICA for watermarking digital images, Journal of Machine Learning Research, Pp. 1471-1498.

[11]. A.Ross , K.Nandakumar, and A.K.Jain, Handbook of Multibiometrics. Springer, 2006.

[12]. A.Ross and A.K. Jain, "Information fusion in biometrics", Pattern Recognition Letters, vol. 24, pp. 2115-2125, Sep 2003.

[13]. M. Indovina, U. Uludag, R.Snelick, A. Mink and A.Jain, "Multimodal Biometric Authentication methods: A COTS Approach".

[14]. R.M.Bolle, S.Pankati and N.K.Ratha, "Evaluation Techniques for Biometrics-Based Authentication Systems (FRR), "Proc. 15th Int'1 Conf.Pattern Recognition, vol 2, pp. 831-837, Sept.2000.

[15]. Teddy Ko,"Multimodal Biometric Identification for large user population using fringer print, face and iris recognition

", Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05), 2005.

[16]. N.Ratha, J.Connell, and R.Bolle,"Enhancing security and Privacy in biometrics-based Authentication Systems", IBM Systems Journal, vol-40, no-3, pp614-634, 2001.

[17]. R.W.Frischholz and U.Dieckmann,"Bioid: A Multimodal Biometric Identification System," IEEE Computer, vol-33,no-2, pp. 64-68, 2000.

[18]. Monrose, F.,Rubin,A.D.,"Keystroke Dyanamics as a Biometric for Authentication" Future Generation computer systems, vol-16, no-4(2000) 351-359.

[19]. A.K.Jain and A.Ross, "Learning User-Specific Parameters in a Multibiometric System",Proc. IEEE Int'1 conf. Image Processing , PP. 57-60, Sept. 2002.

[20]. A.K.Jain, K.Nandakumar, A.Ross, "Score normalization in multimodal biometric systems", Pattern Recognition, 2005.

[21]. Vetrro and N.Memon, "Biometric system security", tutorial presented at second International Conference on Biometrics, Seoul, South Korea, August 2007.