Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometric System and Its Challenges

Meenakshi Kangra[1], Dr. Chander Kant[2]
[1]Research Scholar, [2]Asst. Professor
Department of Computer Science and Applications, K.U.,
Kurukshetra, Haryana, India

Abstract—The biometric community enjoys an active research field that has automated the reliable personal recognition schemes to verify and identify a user using his/her physiological and/or behavioral characteristics. Biometric detection with pattern recognition architecture can be used in various applications (computer systems, organisations, buildings, cellular phones, and ATM machines) to enhance security access. These automated recognition schemes are developed to ensure that the required services are accessed only by a legitimate user and no one else. In the absence of such recognition schemes, an authenticity may be vulnerable to an impostor. Biometrics, identification based on distinct personal modalities/characteristics has the potential to become key part of any identification system that defines about an individual rather than what he possess or remembers (e.g., an ID proof, a password). A biometric system based on such characteristics should be accurate, fast, robust and inexpensive. This paper gives brief outline about area of biometric & its system and also discusses about some of its advantages, disadvantages, and challenges in concern with privacy.

Keywords— Bio(life)-metric(measurement), identification, invasive, modalities, multimodal biometrics, non-invasive, recognition, verification.

I. INTRODUCTION

User authentication is extremely important wherever security is applicable and to authenticate any user mostly existing knowledge-based methods (e.g., pin, passwords) and token-based methods (e.g., smart cards, ID cards) are considered to be popular approaches. However, these methods are very complex as it has number of security flaws (misused, lost, stolen or shared). Biometric system authentication is very secure and convenient method as it doesn't require such things to remember. Nearly, all law enforcement agencies and forensics science agencies utilizes bios measurement to solve their cases or to recognize/identify criminals using available biometric technologies.

For identification/authentication, just link the digital identity of a person from his body's characteristics/modalities. From last thousands of years, face, voice, and gait like characteristics /modalities have been used by human beings to recognize each other and in same manner these characteristics /modalities can be used in biometric systems for recognition. However, each biometric modality to be recognisable must possess some properties/factors[1]:

- *Universality*: Everyone should contain the modalities.
- *Distinct*: No two persons should have the same modalities.
- *Permanent*: The modalities should be sufficiently invariant over a period of time.
- *Collectable*: The modalities can be measured quantitatively.
- *Performance*: Biometric modalities should have desired accuracy, recognition speed and should combat with the operational and environmental factors that may affect both the accuracy and speed.
- *Acceptable*: The modality is acceptable only if people are willing to use it in their daily lives.
- *Circumvention*: ease with which the system can be fooled.

A practical recognition system involves use of biometric and its selection depends on properties/factors discussed above and to be sufficiently robust with various existing frauds and attacks on system. However, reliable identification/authentication can be implemented using various existing modalities of a person such as fingerprints, face, DNA prints, odour, hand-geometry, palm-print[1]etc.

Biometric modalities can be used in various applications to resolve security issues and each modality has its concerned strengths and weaknesses. Practically no single biometric modality can effectively meet the requirements or we can say no single biometric is "optimal." From the results of years of research derived biometric modalities can be categorized as invasive and non-invasive.

(1) Invasive Modalities: Invasive modalities are those which require user involvement in process of verification and identification (eg.; putting fingers on sensor to get fingerprints).

(2) Non-Invasive: Non-invasive modalities are those which does not require user involvement while verifying and identifying (eg.; notifying voice or face). The categorization of different modalities can be diagrammed as below in Figure 1.

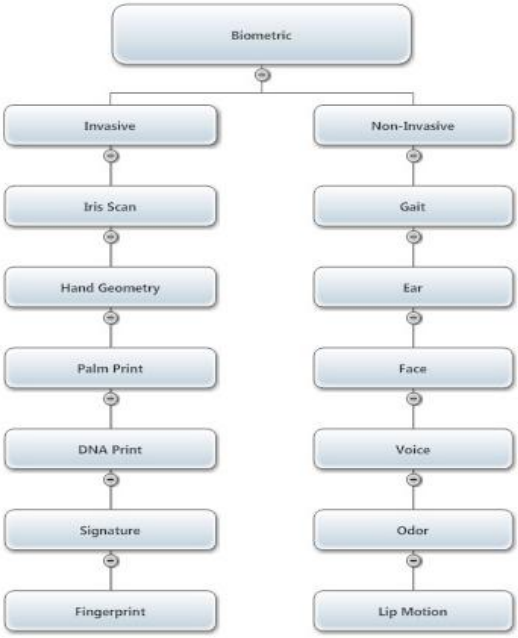

Figure1: Commonly Used Biometric Modalities

These modalities can be compared using some statistical data in relation with above discussed properties/factors as shown in Table 1.

Table 1: Showing Comparison Among Properties/Factors Of Biometric Modalities

Biometric-modalities	Universality	Persistence	Collectability	Performance	Acceptability	Circumvention
Face	Max	Min	Avg	Min	Max	Min
Finger Print	Avg	Max	Avg	Max	Avg	Max
Hand-geometry	Avg	Avg	Max	Avg	Avg	Avg
Iris	Max	Max	Avg	Max	Min	Max
Retinal Scan	Max	Avg	Min	Max	Min	Max
Signature	Min	Min	Max	Min	Max	Min
Voice	Avg	Min	Avg	Min	Max	Min

II. BIOMETRIC AUTHENTICATION SYSTEM

A biometric system [1, 2, 3, 4, 5, 6] an pervasive computing, based on signal detection mechanism which recognizes the biometric patterns via sensing biometric signals, processing those signals to extract a salient set of features known as feature vector and matching it against the feature sets residing in the database (templates), finally makes a decision about the identity of the person providing the input biometric signal. Apart from classical/traditional authentication methods, a process which ensures person authentication based on feature vectors fetched from human characteristics/modalities. Biometric system shown in Figure 2 is designed using the following main modules:

I. *Sensor module*, used for capturing the biometric data related to an individual pursuing for authentication. For eg. Palm sensor that images the ridge and valley structure of a user's palm.

II. *Feature extraction module*, which extracts the set of salient or needful features via processing the biometric data. For example, the matched position of pinna and landmark location of an ear.

III. *Matcher module*, in which comparison of extracted features (query template) is made against the stored (candidate) templates. For example, in the matching module of a fingerprint-based biometric system, the number of matching Minutiae between the input and the template fingerprint images is determined and a matching score is reported.

IV. *Decision module*, a part of matcher module capable of deciding whether the claimed identity is confirmed (verified/one-to-one) or a user's identity is established (identified/one-to-many) based on the matching score of modality.

V. *System database module*, which further stores the biometric templates of the enrolled users. The individuals enrolled into the biometric system through sensor interface during its enrolment phase and after that biometric modalities are first scanned by a biometric reader to produce a digital representation of the characteristic related to modality. Further, a quality check is performed ensuring reliable processing of samples being collected during successive stages of authentication system. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a *template*.

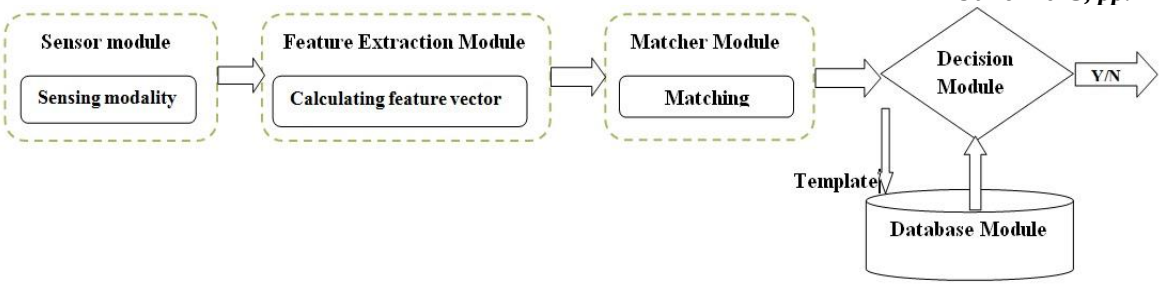

Figure 2: Biometric Recognition System

A. Biometric system functions

A biometric system functions (represented in Figure [3(a), 3(b)]) can be defined as (1) Enrolment phase, in which user enrol its modality through sensors and further system generates a template via processing it. (2) Recognition phase again "to know" about the identity and can be performed as (a) *Verification* phase/positive claim, a claim of identity is submitted together (already enrolled in the system) with the captured biometric data and performs one-to-one comparison. (b) Identification phase/negative claim, captured biometric data is submitted (not enrolled in the system) without any claim of identity and performs one-to-many comparisons.

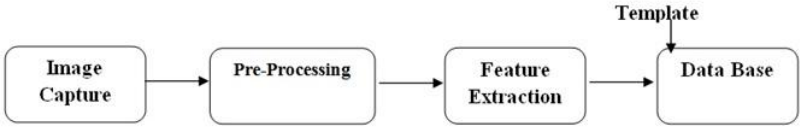

Figure 3(a): Enrolment

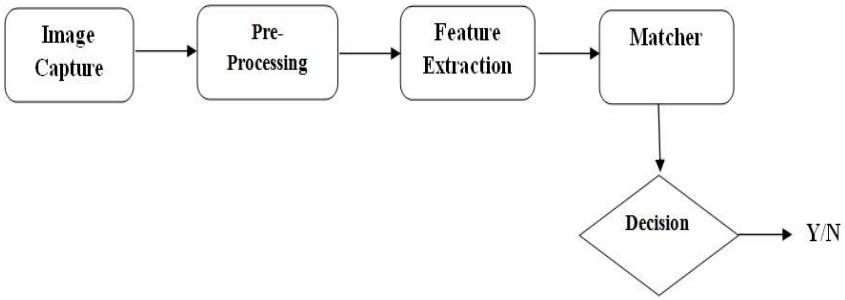

Figure 3(b): Recognition

B. Biometric System Technologies and Challenges

Below Table 2 represents technologies [7] for above discussed modalities and incorporates challenges faced during statistical measurement of an biometric authentication process.

Table 2: Technologies & Challenges

Technologies	Concerned Challenges
Face Recognition	1) Illumination problem 2) Collusion problem (hat, scrap, sun glasses) 3) Varying pose during capture
Finger Print Recognition	1) Wet and wrinkled 2) Cuts on fingers
Hand-geometry Recognition	1) Dimensional issues of hardware 2) Wet and wrinkled
Iris Recognition	1) Collusion problem(contact lenses) 2) Illumination problem 3) Positioning of eye
Retinal Recognition	1) Collusion problem(contact lenses) 2) Illumination problem 3) Positioning of eye
Signature Recognition	1) Reliability 2) Accuracy
Voice Recognition	1) Requirement of memory space 2) Influence Factors(emotions or sick) 3) Wrong pronunciation

C. Performance Issues

There are several types of errors [8] exists, as a result which affects the accuracy and performance of the biometric system:

1. **Failure to capture error (FCE):** This defines the inability of the used input device to capture the biometric information hence a device and also a human dependent error.
2. **Failure to enrol error (FEE):** This defines the inability of the biometric system to extract the template information after a successful device capture. This error is an algorithmic type error associated to the step of processing and extraction of templates from the input device.
3. **False match error/False Acceptance error (FME/FAR):** The failure of the algorithm when distribution between legitimate user and impostor is not genuine i.e. impostor gets treatment of genuine one during comparison between two templates. This type of error occurs during matching algorithm and also depends on device and human factors at the time of biometric trait capture.
4. **False non-match error/False Rejection error (FNME/FRR):** The failure of the algorithm when genuine user declared as an impostor during comparison between two templates. This type of error occurs during matching of templates and depends on template extraction, device and human factors at the time of biometric modality/trait capture.
5. **Equal Error rate:** The rate at which both FRR and FAR in Figure 4 are equal distinguish about the distributions (genuine and imposter).

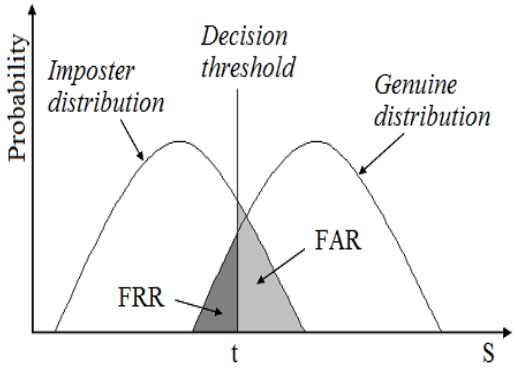

Figure 4: System Error Rates [9]

From Figure 4, it is assumed that;
t-> threshold value, S-> measured value;
If
measured value(S)>threshold value (t);
then
distribution is genuine (i.e. legitimate user);
else
distribution is imposter;

But the fact is that chosen threshold should be optimum otherwise increased threshold decreases the chances of verification (of even genuine person).

D. Factors causing errors in biometric system

Before the system performs recognition with the use of available sensitive sensors, the very first step is to capture the enrolled user template which we termed as query template [2,5] and then authentication system recognise the identity by matching the recorded query template against the stored template which is also termed as candidate template of large database. During this scenario, sometimes obtained results are not up to the expectations and leads to an error. Errors are generated due to some unavoidable factors raised to traits/modalities that affect the system performance. Following are some common factors [11] affecting the biometric system.

(1) *Human factor*: Human participation is essential during capturing the query template (eg., For fingerprint capture, fingers must be placed on sensor surface) and accuracy of recognition depends on the user. Here the factor arises as some changes may occur in physiological or behavioral characteristic of user modality (eg., Cuts and bruises on finger, imperfect positioning of finger).

(2) *Device factor*: Apart from human part, sensors used during recognition also plays a critical role in recognition, reason being due to environmental conditions(temperature and humidity) and technological properties of devices, quality of the captured biometric template may get affected.

(3) *Algorithm Factor*: The main components of a typical biometric algorithm are (a) Enrolling component, is responsible for analyzing the record, extracting its features and convert them into final biometric (candidate) template for storing in database. (b) Evaluation component, matches the two templates and generates the score for two templates. (c) Decision Component, finally decides an output for the templates using the score of the templates. Hence decision dependency on matching algorithm and failure while making decision arising the sources to error.

III. APPLICATION AREA RELATED TO BIOMETRIC

(1) *Commercial applications* rely on knowledge based mechanism such as one has to maintain (PIN, Passwords and Patterns etc.). Examples are: network login, internet access, e-commerce, banking, access control and file managements.
(2) *Government applications* rely on token based mechanism such as any ID proofs. Examples are: passport administration, national ID proofs, state ID proofs, social security.
(3) *Forensics applications* rely on human expert mechanism to match captured features. Examples are: police investigation, corpse and terrorist identification, missing children and parenthood determination.

IV. CHOICE OF BIOMETRIC

Biometric is playing a major role being deployed in many application areas and enhancing the security far better than the traditional methods. However, no single biometric modality is applicable and satisfiable for all applications. Hence the question arises which biometric is to be choosen? The answer to the question is from the Table[1] showing the comparison among modalities, that defines the statistics of various properties/factors. Each application has its own requirements which is necessary to be fulfilled (accuracy, performance and speed etc). For example when application demands high performance then the concerned factor/property (performance) needs to be considered and maximum value of property/factor determines the choice. Below Figure 5 represents the assumed statistics of factor/property(performance) related to biometric modalities.

Figure 5: Choice Of Biometric

Hence, now it is easy to determine from Figure 5, which biometric can be an choice, as it can be found that value is maximum for invasive modalities (fingerprint, iris, retina). Further choice can be cleared from user's perspective, which will be best for its application.

V. BIOMETRIC SYSTEM TECHNICAL CHALLENGES

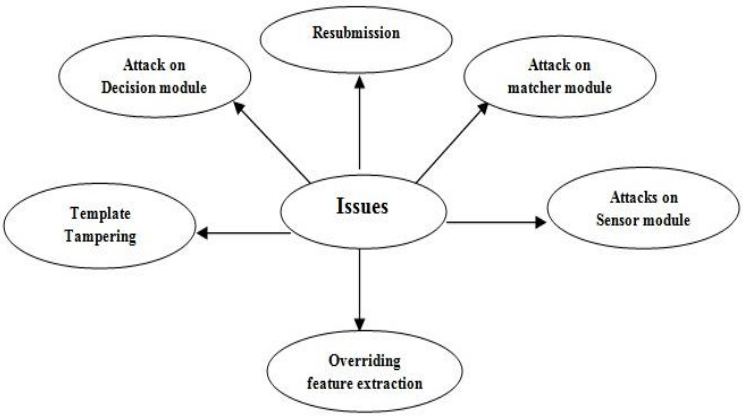

Figure 6: Technical Challenges

VI. BIOMETRIC ADVANTAGES AND DISADVANTAGES

Biometric system technology meant for user authentication in computer system or many other areas is growing and expanding and has associated some advantages and disadvantages with it, described below in Table 3.

Table 3: Advantages v/s Disadvantages

Advantages	Disadvantages
Confidence in decision making/Identified or Verified user	Authentication time delay
Template security/Increased security	User acceptance required
Reduced flaws related to traditional methods	Misuse via producing fake biometrics
Reliable, Efficient and economical	Required system accuracy

VII. MULTIMODAL BIOMETRIC SYSTEM

Multimodal biometric system integrates the results of recognition from two or more patterns and these results are based on extracted features from biometric technologies or signals generated from input and extracted via matching with stored templates. Multimodal biometric systems may be viewed as further enhancements in security and also act as collective measures to errors such as imposter acceptance and genuine rejection. A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one biometric as your verification tool. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions [1, 2, 5].

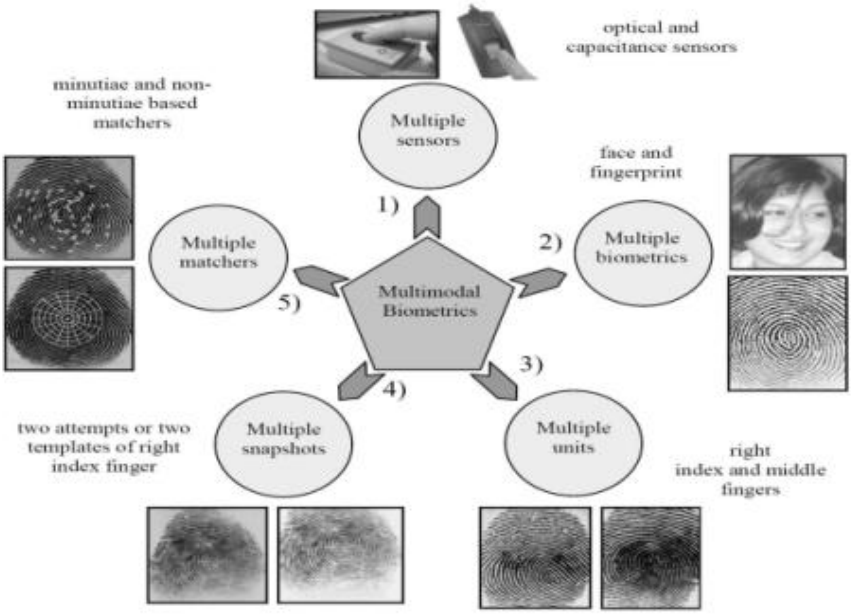

Figure 7: Multimodal Biometric System [9]

Multimodal biometric systems overcomes the limitations of uni-modal biometric systems such as noise in sensed data**,** intra-class variations, distinctiveness, non universality, spoof attacks which further enhances the secure authentication, which get restricted due to the failure of single biometric trait. And hence, includes more than one trait to verify an individual. A multimodal biometric system uses multiple applications to capture different types of biometrics [11].

VIII. CONCLUSION

Biometric is our future through which we can combat our security issues related to verify only legitimate user, but it has its associated unique challenges. Biometric rejects the conventions associated with traditional/conventional knowledge-based and token-based methods that do not really provide positive recognition of an individual reason being they rely on surrogate representation of user. The scope of this review which was done as part of our literature review on biometric authentication system, to extend the use of biometric system up to maximum areas so that one can enjoy the secured access to the services be confined to authorized users. It is thus obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. This is not, however, to state that biometrics alone can deliver reliable personal recognition component. In fact, a sound system design will often entail incorporation of many biometric and non biometric components (building blocks) to provide reliable personal recognition [2,11]. With the continuation of this work, our future plan is to study and optimising biometric system using iris recognition.

REFERENCES

[1] 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.

[2] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition:Security and Privacy Concerns", IEEE Security & Privacy, MarcWApril2003, pp. 33-42.

[3] Ross, A. K. Jain, "Information fusion in biometrics", Pattern Recognition Letters 24 (2003) 21 15-2125, available at http://www.computerscienceweb.com/.

[4] Lifeng Lai, Sui Wai Ho and H. Vicent Poor "Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case" EEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011.

[5] Jain, A.K.;Ross, A.;Prabhakar, S.;"An introduction to biometric recognition", Volume: 14 Issue: 1 Issue Date: Jan. 2004, on page(s): 4 – 20.

[6] Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June2006, page(s): 125 – 143.

[7] P.J.Phillips and W.T. Scruggs, A.J.O'Toole, P.J. Flynn, K.W.Bowyer, C.L.Schott, and M.Sharpe, "FRVT 2006 and ICE 2006 Large-Scale Results, "NIST, Technical Report NISTIR 7408, March 2007.

[8] Anne O'Neill; Shaun Winters; Lucy Kwiaton "Biometrics security system", 2011 http://www.findbiometrics.com.

[9] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42.

[10] Biometric recognition: challenges and opportunities (2010) http://www.nap.edu/openbook.php?record _id=12720 & page=2.

[11] A. Adler, "Can images be regenerated from biometric templates?," in Biometrics Consortium Conference, (Arlington, VA), September 2003.

[12] Ross, J. Shah, and A. K. Jain, "Towards reconstructing fingerprints from Minutiae points," in *Proc. SPIE, Biometric Technology for Human Identification II*, vol. 5779, pp. 68–80, (Orlando, FL), March 2005.

[13] A.K. Jain and A. Kumar, "Biometric Recognition: An Overview", *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras (Eds.), pp. 49-79, Springer, 2012.

[14] A.K. Jain, A. Ross, and K. Nandakumar, "Introduction to Biometrics", Springer, 2011 (ISBN 978-0-387-77325-4).

[15] K. Niinuma, U. Park, A. K. Jain, "Soft Biometric Traits For Continuous User Authentication", *IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 4, pp. 771-780, 2010.

[16] Phillips et al. (2005) P.J. Phillips, P.J. Flynn, T. Scruggs, K.W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. "Overview of the face recognition grand challenge". In IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2005, pp. 947–954.

[17] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001.

[18] http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarIvanisovJain_BiometricRecognition_SensorCharacteristicsImageQuality.

