ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

Authentication Progression through Multimodal Biometric System

Snehlata Barde, Sujata Khobragade, Rasmiprava Singh

Abstract— ***Automatic person identification is an important task in our day to day life. Traditional method of establishing a person's identity includes knowledge based like password or token base like id cards. These identities may be lost stolen or shared by any person .For these reasons they are not suitable for authentication and identity verification. Thus we provide a biometric authentication system which is more reliable as compared to the traditional security system and it will overcome all the limitations of traditional method. This paper discusses about the overture, reward of biometrics, challenges in the progress of biometrics and its task domain in the field of security.***

Keywords— **Biometric, Unimodal, Multimodal, Security, Spoofing Attack.**

I. INTRODUCTION

Identity management system is challenging task in providing authorized user with secure and easy access to information and services across a wide verity of networked system. A reliable identity management is a critical component in several applications that provide services to only legitimately enrolled users. Some of applications include physical access control to secure facility, access to computer networks, performing remote financial transactions etc. The primary task in an identity management system is determination of individual's identity. The traditional method of establishing a person's identity include knowledge based like password or token based like ID cards, but these representations of the identity can easily be lost, stolen or shared. Therefore they are not sufficient for identity verification. Establishing the identity of a person is becoming critical in our vastly interconnected society. Questions like "Is she really who she claims to be?", "Is this person authorized to use this facility?" or "Is he in the watch list posted by the government?" are routinely being posed in a variety of scenarios ranging from issuing a driver's license to gaining entry into a country. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication and mobility. Biometrics refers a technology to authenticate individuals by automated means that rely on anatomical or behavioral human characteristics. Biometric systems have the potential to do the people authentication with a high degree of assurance.

Biometrics, described as the science of recognizing an individual based on her physiological or behavioral traits e.g., face, fingerprint, hand geometry, iris, palm print, voice and handwritten signatures.

Diagram....traditional

Each biometric trait should pose attributes like Uniqueness, and hard to circumvent. Sadly, recent researches have shown that an attacker can lift and replicate the biometric traits, which later can be used to attack on biometric systems. As a result, multimodal biometric systems have been proposed to increase the recognition accuracy as well as security against attacks as compared to the unimodal biometric systems that make them up.

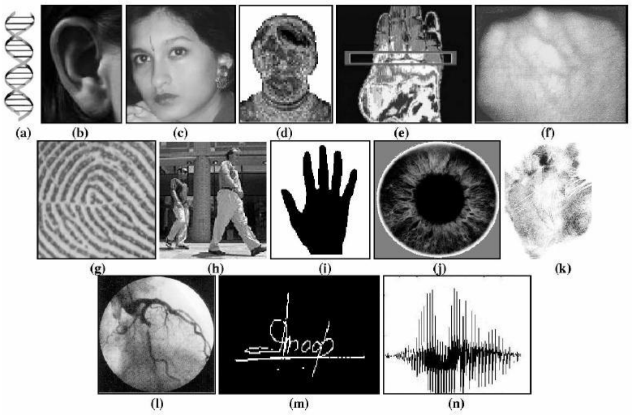

Fig 1. Diagram of Biometrics

A. Characteristics of Biometrics

Any physical and/or behavior characteristics of a human can be considered as a biometric if it exhibits following characteristics as explained by Jain et al., [1]:

- Universality: Each person accessing the biometric application should posses a valid biometric trait.
- Uniqueness: The given biometric trait should exhibits distinct features across individuals comprising the population.
- Permanence: The biometric characteristics should remain sufficient invariant over a period of time.
- Measurability: The biometric characteristics can be quantitatively measured i.e. acquiring and processing of biometric trait should not cause inconvenience to the individual.
- Performance: The biometric trait should the required accuracy imposed by the application.
- Acceptability: The chosen biometric trait must be accepted by a target population that will utilize the application.
- Circumvention: This indicates how easily the chosen biometric trait can fooled using artifacts.

B. Advantage:

Biometrics eliminates fraud, enhances security, cannot be easily transferred, forgotten, lost or copied.

C. Challenges in Biometric:

•Large number of classes
•Large Intra-class variability
•Small inter-class variability
•Noisy and distorted images
•Population coverage and scalability
•System performance (error rate, speed, cost)
•Attacks on the biometric system
•Individuality of biometric characteristics

Few examples of biometric traits are: Iris, Retinal scan, Face, Speaker/Voice, Fingerprint, Hand / Finger geometry, Signature, Keystroke dynamics, Gait etc. Most biometric systems deployed in real world applications are unimodal, i.e. including single trait or modality. These systems have to contend with a variety of problems:

a. Noise in sensed data: A fingerprint image with a scar or a voice sample altered by cold is examples of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system).

b. Intra-class variations: These variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication (e.g., optical versus solid-state fingerprint sensors).

c. Inter-class similarities: A biometric system comprises of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users. The number of distinguishable patterns in two of the most commonly used representations of hand geometry and face are only of the order of 105 and 103, respectively.

d. Non-universality: The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges.

e. Spoof attacks: This type of attack is especially relevant when behavioral traits such as signature or voice are used. However, physical traits such as fingerprints are also susceptible to spoof attacks.

D. Types of Biometrics

The biometric system can be classified into two different types:

1. **Unimodal Biometric System:** The unimodal biometric employs single biometric trait (either physical or behavior trait) to identify the user. Example: Biometric system based on Face or Palmprint or Voice or Gait etc.

2. **Multimodal Biometric System:** A biometric system that consolidates the information from multiple sources is known as multimodal biometric system. Example: Biometric system based on face and gait or face and speech, etc.

Multimodal Biometrics

The term "multimodal" is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. In orthogonal multimodal biometrics, different biometrics (like face and fingerprint) is involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing. In collaborative multimodal biometrics, the processing of one biometric is influenced by the result of another biometric. Multi-modal biometrics usage is being actively considered in applications involving Border Control, Physical Access Control, and PC/Network security [1-4].

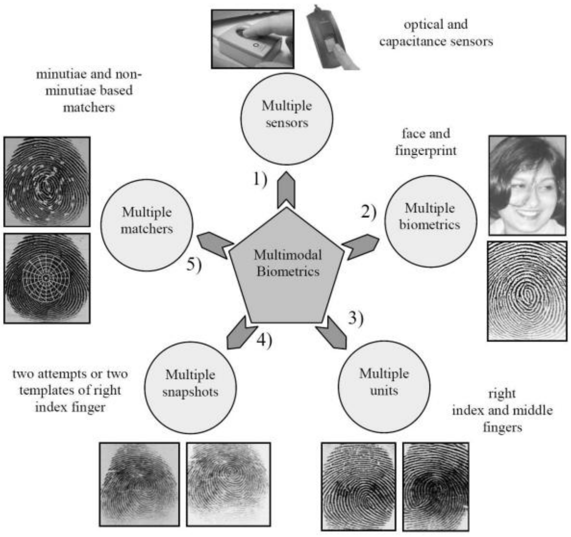

Fig 2. Diagram of Multimodal Biometrics

E. Need of Multimodal Biometrics

Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics.

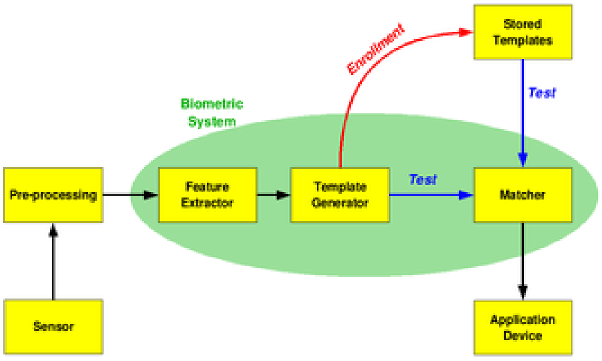

Fig 3. Basic modal of Biometrics

II. APPLICATIONS

The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification. Enterprise solutions require the oversight of people, processes and technologies. Network infrastructure has become essential to functions of business, government, and web based business models. Consequently securing access to these systems and ensuring one's identity is essential. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

III. CHALLENGES AND RESEARCH AREAS

Based on applications and facts presented in the previous sections, followings are the challenges in designing the multimodal systems. Successful pursuit of these biometric challenges will generate significant advances to improve safety and security in future missions. The sensors used for acquiring the data should show consistency in performance under variety of operational environment. Fundamental understanding of biometric technologies, operational requirements and privacy principles to enable beneficial public debate on where and how biometrics systems should be used, embed privacy functionality into every layer of architecture, protective solutions that meet operational needs, enhance public confidence in biometric technology and safeguard personal information.

Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is also the challenging area. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll. The multimodal biometric systems can be improved by enhancing matching algorithms, integration of multiple sensors, analysis of the scalability of biometric systems, followed by research on scalability improvements and quality measures to assist decision making in matching process. Open standards for biometric data interchange formats, file formats, applications interfaces, implementation agreements, testing methodology, adoption of standards based solutions, guidelines for auditing biometric systems and records and framework for integration of privacy principles are the possible research areas in the field.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[2] Chander Kant, Rajender Nath, "Reducing Process-Time for Fingerprint Identification System", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1- 9, 2009.

[3] A.K. Jain, A. Ross, "Multibiometric systems". Communications of the ACM, vol. 47, pp. 34-40, 2004.

[4] Phillips, P.J., P. Grother R.J. Michaels, D.M. Blackburn and E. Tabassi and J.M. Bone, "FRVT 2002: overview and summary", March 2003.

[5] Gokberk, B., A.A. Salah. and L. Akarun, "Rank-Based Decision Fusion for 3D Shape- Based Face Recognition," LNCS 3546: AVBPA, pp. 1019-1028, July 2005.

[6] Xu, C., Y. Wang, T. Tan and L. Quan, Automatic 3D face recognition combining global geometric features with local shape variation information," Auto. Face and Gesture Recog. pp. 308 -313, 2004.

[7] Chang, K. I., K. W. Bowyer, and P. J. Flynn, "An evaluation of multi-modal 2D+3D face biometrics," IEEE Trans. on PAMI 27 (4), pp. 619-624, April 2005.

[8] A. Ross, A.K. Jain, "Multimodal Biometrics: An Overview", 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp. 1221- 1224, 9/2004.

[9] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?". in Proceedings of International Conference on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain), pp. 168–171, 2000.

[10] L. Rukhin, I. Malioutov, "Fusion of biometric algorithms in the recognition problem". Pattern Recognition Letter, pp. 26, 679–684, 2005.

[11] Kittler, “On combining classifiers”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20 (3), pp. 226–239, 1998.

[12] P. Verlinde, G. Chollet, M. Acheroy, “Multimodal identity verification using expert fusion”. Information Fusion, vol. 1 (1), pp. 17-33, 2000.

[13] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, “Fusion strategies in multimodal biometric verification”. In Proceedings of International Conference on Multimedia and Expo (ICME ’03), vol.3 (6–9), pp. 5–8, 2003.

[14] J. Fierrez-Aguilar, “Kernel-based multimodal biometric verification using quality signals”. Biometric Technology for Human Identification, Proceedings of the SPIE, vol. 5404, pp. 544–554, 2004.

[15] B. Gutschoven, P. Verlinde, “Multimodal identity verification using support vector machines (SVM)”.Proceedings of the Third International Conference on Information Fusion, vol. 2, pp. 3–8, 2000.

[16] J. Bigun, et al., “Multimodal biometric authentication using quality signals in mobile communications”. Proceedings of IAPR International Conference on Image Analysis and Processing (ICIAP), IEEE CS Press, pp. 2–13, 2003.

Author Biography

Snehlata Barde, MCA, National and international journals in Image processing, Network.

Sujata Khobragade.MCA, NIT Raipur, International and national journal in network, mobile computing, image processing

Rasmiprava Singh, MTECH, NIT Raipur, international journal and national journal in manet,wireless communication, image processing.