Different Modalities in Biometric Detection

Mukesh Rinwa[1], **Bharat Borkar**[2]

[1]Department of Information Technology, Pune University, AVCOE Sangamner-422605, Ahemadnagar Dist., India

[2] Department of Information Technology, Pune University, AVCOE Sangamner-422605, Ahemadnagar Dist., India

Abstract: ***Many organizations are using different kinds of automated person's identifications systems which improve the user's needs, satisfaction, and efficiency to secure critical resource. In this paper we are giving the information on the recent developments in person's identification using Biometric technology method. By using this technology we are to ensure to identify a person weather he/she is real person or a fake person. The objective is to increase the security of biometric reorganization frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner. In this paper we are giving information about different modalities such as fingerprint, face recognition, and iris to study against the different types of vulnerabilities attacks.***

Keywords: Biometric recognization, liveness detection, image quality assessment, attacks, security

1. Introduction

In Recent years, automated person identification is highly researched because for protected access to computer, buildings, mobile phones, ATM'S and video surveillance. Person identification is the process of associating an identity to an individual. Person identification techniques are broadly classified into three types such as knowledge based approach, token based approach, and biometric based approach [1]. *A knowledge-based approach* depends on something an individual knows to make a personal identification, like a password or a personal identification number (PIN). *Token-based approaches* are based on something an individual have to make a personal identification like a passport, driver's license, ID card, credit card, or keys. *Biometric based systems* use physiological or behavioral features of an individual for identification [1], [2]. Knowledge based and Token based approaches have several disadvantages like password forgotten, or password was stolen by hackers or unauthorized person, Tokens may be forgotten, lost, stolen, or misplaced. Whereas, in Biometric based systems it cannot be forged or stolen [3], [4]. You don't want to replace password based access control to avoid having to reset forgotten password and be bothered about the integrity of your system? You don't want to like to rest secure in comfort that your healthcare system does not merely on your social security number as proof of your identity for granting access to your medical records? Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Although warning, many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have enhance the need for methods to prove that someone is truly who he/she claims to be.

Biometric such as Face recognition, iris, and fingerprint technology may solve this problem since a face is definitely connected to its owner expect in the case of identical twins. It's nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card. The term "Biometric" comes from the Greek words bios (life) and metric (measure) [2].

(1) General: Biometric is the science of measuring the physical properties of living beings.
(2) ISO/IEC: Biometrics is the automated recognition of individuals based on their behavioral and physiological characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

1. Finger-scan
2. Facial Recognition
3. Iris-scan
4. Retina-scan
5. Hand-scan

Behavioral biometrics (based on measurements and data derived from an action) include:

1. Voice-scan
2. Signature-scan
3. Keystroke-scan

A "biometric system" refers to the integrated hardware and software used to conduct biometric identification or verification.

A simple biometric system has four important components:

(i) Sensor module which gets the biometric data of an individual [7] for example, a fingerprint sensor that captures fingerprint impressions of a user, & camera for face recognization
(ii) Feature extraction module in which the captured data is processed to extract feature scores or values. For example, the position and orientation of minutiae points (ridges position and orientations) in a fingerprint image would be extracted in the feature extraction module of a fingerprint system.
(iii) Matching module in which the feature values are compared against those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score. (iv)Decision-making module in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module. The biometric

identification method consists of three operations; they are firstly capture biometric sample of the person and make a digital representation of the sample, then extract distinctive features from the digital representation using feature extractor, and finally compare the extracted feature set against the template set in the database[7].

2. Biometric Biometric

2.1 Sample Features

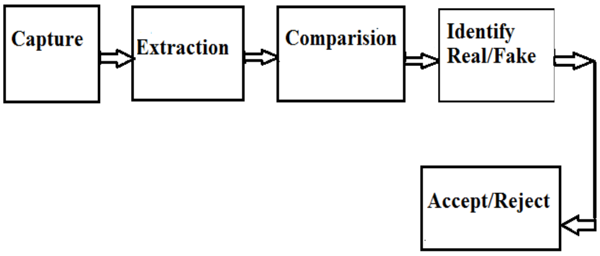

Figure 1: Typical components of Biometric Recognization System

The vulnerability attacks can be broadly divided into two main groups:

Direct attacks: The attacks at the sensor level are referred to as direct attacks [5][6]. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to copy the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. This type of attacks is performed in the analogy domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems.

Indirect attacks: This attack includes attacks might be carried out using a Trojan horse that bypasses the feature extractor, and the matcher respectively. Attack in the system database is manipulated (a template is changed, added or deleted) in order to gain access to the application. The remaining points of attack are thought to exploit possible weak points in the communication channels of the system, extracting, adding or changing information from them. In opposition to direct attacks, in this case the intruder needs to have some information about the inner working of the recognition system and, in most cases, physical access to some of the application components (Feature extractor, matcher, database...etc.) is required.

2.2 Liveness Assessment

Liveness assessment is given much attention by the researchers which use different physiological properties to distinguish between the real and the fake trait [5]. For Liveliness Tests Possible solutions being explored:

- Measure temperature
- Measure current flow (inject a small voltage across the fingerprint)
- Use IR Led sensors to look for blood veins [7][8].

Liveness detection method is broadly classified into two types:

(i) Hardware-based liveness detection techniques which adds some specific device to the sensor in order to detect particular properties of a living trait For example blood pressure, fingerprint sweat, or specific reflection properties of the eye.
(ii) Software-based liveness detection techniques here once the sample is captured with a standard sensor a fake trait is detected [5].

However, there is the merits & drawbacks of the above mentioned liveness detection methods, hardware based detection method is more expensive than the software based method Hardware based schemes having higher fake detection rate capability as compared to the software based techniques. Software based techniques protect the system against the reconstructed or synthetic samples which are injecting into the communication channel between the sensor and the feature extractor [9][10].

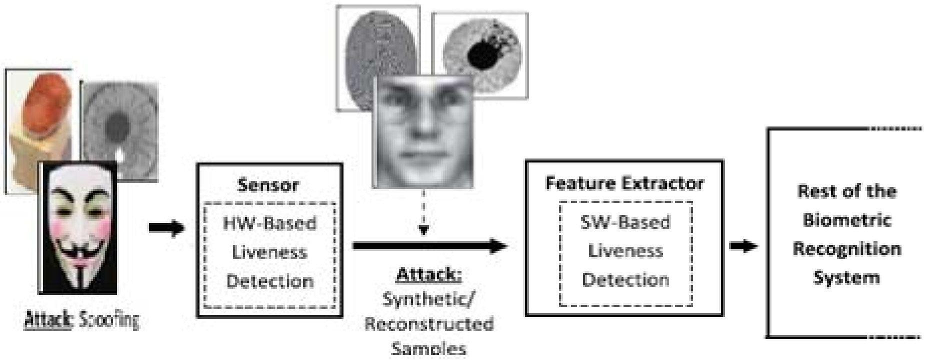
Attack: Spoofing
Sensor
HW-Based Liveness Detection
Attack: Synthetic/ Reconstructed Samples
Feature Extractor
SW-Based Liveness Detection
Rest of the Biometric Recognition System

Figure 2: shows types of attacks potentially detected by hardware-based and software-based liveness detection techniques [5]

Liveness Detection which is an antispoofing method which ensures only the biometric from a live, certified person is submitted for enrollment, verification and identification [11].

"It is found that a fake image captured in an attack will have different quality ratio than a real sample acquired in the normal operation [5]". Expected image quality differences between real and fake image samples may include color and

luminance levels, local artifacts, degree of sharpness, amount of information found in both type of images called entropy, structural distortions or natural appearance.

2.3 Security

Several elements of a biometric system can be vulnerable against different types of attacks if not implemented in a sufficiently secure way. Some elements that can be attacked or broken in an attack of the system are:

(i) Sensor:
The sensor needs to be accurate enough to distinguish between the Users i.e. a fake user and a real user and detect spoof attempts.

(ii) Feature Extractor:
Knowledge of the feature extractor algorithm can be used for detection.

(iii) Database:
Admission to the biometric templates may be broken by non-authorized users.

(iv) Matcher:
Any access to modifying the matching score can be critical.

There are different types of attacks in Biometric systems:

(i) Spoof attack:
Fingerprint can be obtained by copying the fingerprint which left on the object, such as glass. Based on gelatin, silicone, and play-doh materials attacker can develop a gummy finger. By using liveness detection technique we can easily identify the gummy finger [5] [12].

(ii) Replay Attack:
By taking the use of sniffer device for legitimate network management functions and for stealing information off a network. The data sent can be captured and replayed later. This method requires the sensor to be bypassed [12].

(iii) Transmission Attack:
If an unauthorized person accesses the transmission medium between the different components in the biometric systems we called them as the "man-in-middle attack". Enrolled user data can be stopped, manipulated or replaced, and even matching values can be manipulated with access to the transmission mediums [12].

(iv) Template Attack:
Template attack includes stealing, modifying, adding new ones, or deleting stored template. Template can be protected using encryption method.

3. Review on Biometric Systems

In this section we will be relating the various approaches that were used in person identification by using biometric systems. A biometric system is the specific physiological or behavioral features haunted by the user for identification and these features are distinctive, general and persistent. These Biometric systems include face recognition, fingerprint technology, iris recognition, hand geometry, and signature and speech recognition. We are mainly focusing and surveying on face recognition, fingerprint and iris technology in this paper.

a. Face Recognition

Face recognition is a biometric modalities used to determine the identity of the individual which uses the computer software.

Face recognition is mainly performed by two approaches i.e. Eigen based face recognition and 3D face recognition [13]. The Eigen face based recognition works by analyzing face images and computing Eigen faces which are faces composed of eigenvectors[13]. The comparison of Eigen faces is used to identify the presence of a face and its identity. The Eigen face technique is a easy, well-organized, and gives generally better results in controlled environment. Some of the demerits of Eigen faces are robustness to changes in lighting, distance and angle. 2D face recognition systems do not capture the actual size of the face, which is a basic problem. These demerits influence the technique's application with security camera because the front shot of the face and consistent lightning cannot be depend upon. 3D face recognition solves the problem of the 2D face recognition i.e. it is to be robust to the type of issues comes under 2D approach. 3D face recognition approach generates 3D model of faces. These systems are more accurate because they capture the actual shape of faces [13]. Skin texture analysis in combination with face recognition improves the accuracy by 20 to 25 percent. The acquisition of 3D data is one of the main problems for 3D systems.

b. Fingerprint technology

A fingerprint is the made of ridges and valleys on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by the prototype like valleys and ridges, as well as minutiae points which are local ridge characteristics that occurs at either a ridge bifurcation or ridge endings [15]. The recent studies shows that probability of two individuals fingerprint, having the same fingerprint is less than one in a billion. There are several fingerprint matching algorithms like minutiae based matching, correlation based matching, genetic algorithms based matching [15]. Among these algorithm, minutiae based matching is the best one. In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae i.e. ridges and valleys from these two scanned fingerprints. Extraction of minutiae features before matching fingerprint requires a series of processes containing position calculation, image segmentation, image enhancement, and ridge extraction and shinning, minutiae. Extraction and filtering. Correlation based matching uses 1:1 correlation between fingerprints. This method gives poor results in fingerprint recognition because correlation can't recognize elastic-distorted versions between two fingerprints of the same fingerprint. In neural network based approach the finger prints are classified by using HAVNET [16]. The number of output nodes of HAVNET was equal to number of enrolled fingerprints. The method was not able to distinguish fingerprints of similar shapes the genetic algorithm based methods try to identify the optimal global alignment between two fingerprints. This process is highly time consuming.

c. Iris recognition

Iris recognition systems make use of the uniqueness of the iris patterns to identify a person. This system uses high-quality camera to capture a black-and-white image, high-resolution image of the iris. Iris is the colored ring surrounding the pupil. Iris recognition consists of five operations; they are image acquisition, iris localization or segmentation, iris normalization and unwrapping, feature encoding, and matching algorithm [17]. In image acquisition step the systems takes a high-quality image of the iris, Iris localization takes place to detect the edge of the iris as well as that of the pupil; thus extracting the iris region, Normalization is used to transform the iris region to have fixed dimensions, and hence removing the dimensional inconsistencies between eye images, other inconsistencies include varying image distance, camera rotation, eye rotation within eye socket, tilting of the head, the normalized iris region is unwrapped into a rectangular region. The normalization process produces the iris region. The feature encoding is used to extract the most discriminating feature in the iris pattern so that a comparison between templates can be done. Finally a decision can be made in the matching step, for matching, the Hamming distance was chosen as a metric for recognition [18].

4. Conclusion

This paper presents a literature survey on the various techniques involved in person identification. The survey emphasizes on biometric recognition system. Biometrics is reliable way for identification because it is based on behavioral or physiological characteristics of a person. We still need to improve the biometrics technology by using various techniques in future work.

References

[1] Sruthy Sebastian, “Literature Survey on Automated Person Identification Techniques” *IJCSMC, Vol. 2, Issue. 5, May 2013, pg.232 – 237*

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar. /Apr. 2003.

[3] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, Javier Ortega-Garcia “A high performance fingerprint liveness detection method based on quality related features”, ELSEVIER 8 December 2010 Biometric zz7Recognition Group - ATVS, EPS, Universidad Autonoma de Madrid, C/Francisco Tomas y Valiente, 11 - 28049 Madrid, Spain.

[4] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia,”Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection”, 2007, Biometrics Recognition Group - ATVS, Escuela Politecnica Superior Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente, 11Campus de Cantoblanco - 28049 Madrid, Spain.

[5] Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez, “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition”, IEEE Transactions on Image processing, VOL. 23, NO. 2, FEBRUARY 2014

[6] U.L.Sindhu, A.Asha, S.Suganya,M.Vinodha , “Face Recognition in Online Using Image Processing”, Karpagam Institute of Technology, International Journal of Communication and Computer Technologies Volume 02 – No.13 Issue: 02 March 2014

[7] Tormod Emsell Larsen, A book for ”Biometric Solutions for Personal Identification”, Norwegian University of Science and Technology Department of Telematics- may 2008. Page 1-10, 19-23.

[8] Dat Tien Nguyen, Young Ho Park, Kwang Yong Shin, Seung Yong Kwon, Hyeon Chang Lee, Kang Ryoung Park, “Fake finger-vein image detection based on Fourier and wavelet transforms”, 10-april 2013 Division of Electronics and Electrical Engineering, Dongguk University, 26, Pil-dong 3-ga, Jung-gu, Seoul 100-715, Republic of Korea.

[9] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, “Fingerprint image reconstruction from standard templates,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[10] S. Shah and A. Ross, “Generating synthetic irises by feature agglomeration,” in Proc. IEEE ICIP, Oct. 2006, pp. 317–320.

[11] International biometric group whitepaper, Liveness Detection in Biometric Systems, available at /www.ibgweb.com/reports/public/reports/liveness.html.

[12] Xiao Qinghan. Security issues in biometric authentication. In Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, pages 8-13, 2005.

[13] Matthew A. Turk, Alex P. Pentland, “Face recognition using Eigen faces”, Proc. IEEE Conference on Computer Vision and Pattern Recognition: 586–591. 1991.

[14] Mark Williams, "Better Face-Recognition Software," Technology Review, May 30, 2007

[15] Jain, A. Ross, S. Prabhakar, “Fingerprint matching using minutiae and texture features”, International Conference on Image Processing (ICIP), Thessaloniki, Greece, 2001, pp. 282–285.

[16] V.A. Sujan, M.P. Mulqueen, Fingerprint identification using space invariant transforms, Pattern Recog. Lett. 23 (2002) 609–619.

J. Daugman, “Recognizing persons by their Iris patterns,” in Biometrics: Personal Identification in a Networked Society, 1999, pp. 103–121.

[17] Padma Polash Paul, Md. Maruf Monwar,” Human Iris Recognition for Biometric Identification”, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.

Author Profile

Mukesh Rinwa received B.E degree in Information Science in 2008 from VTU. Has worked as a Software Tester in Dkash Technology, Pune. Currently he is doing M.E in Information Technology at AVCOE Sangamner from Pune University. Currently he is studying and doing research on Biometrics Systems.