A Survey of Multimodal Biometrics

Mini Singh Ahuja[1], Sumit Chabbra[2]

[1]*Dept of computer science and Engg*
GNDU Regional Campus
Gurdaspur (India)
[2]*Dept of computer science and Applications*
Khalsa College for Women
Amritsar (India)
[1]minianhadh@yahoo.co.in
[2]sumitchhabra_12@yahoo.com

Abstract – Biometric technologies are used to analyse human characteristics for security purposes. The most common physical biometrics patterns analyzed for security purposes are the fingerprint, hand, eye, face and voice. The advantages of using biometrics to verify a person's identity over using passwords or token have been broadly presented in many research papers. However recent research has revealed that biometric technologies can be defeated with low –tech and cheap materials. This provides a new challenge when people are encouraged to use biometrics as a means to enhance network security. In this paper we have discussed multimodal biometrics to increase the security level. With the fusion of multiple biometrics we can minimize the system error rates.

1 INTRODUCTION

Biometric refers to automatic system that uses measurable physiological characteristics or behavior traits to recognize the identity or verify/authenticate the claimed identity of an individual. The advantage to a biometric is that it doesn't change or lose. Many body parts, personal characteristics and imaging methods have been used for biometric systems such as fingers, hands, feet, eyes, ears teeth, veins voices, signatures, typing styles and gaits. Each biometric has its own strength and limitations and accordingly each biometric is used in identification (authentication) applications. It is not difficult to steal a biometric, create a copy and use the fake trait to attack biometric systems. This a serious issue as the people these days are using biometric as a means to enhance network security. Different technologies have been developed to defeat the spoofing attack. As biometrics is not secret they cannot be protected like passwords. People leave their biometrics everywhere without being aware that their biometric information can easily be captured, copied or forged. Another challenge to a biometric system is the speed i.e. the system must make an accurate decision in real time.

2 ATTACKS ON BIOMETRIC SYSTEMS

Even though biometric systems offer several advantages over traditional token (e.g. key) or knowledge (e.g. password) based authentication schemes. They are still vulnerable to attacks. These attacks can be grouped into eight classes.

Class I: Spoof attack: In this type of attack a fake biometric e.g. (finger made from silicon, face mask, lens including iris texture) can be presented to a sensor.

Class II: The second class of attack is called *replay attack.* In it an interspected biometric data is submitted to the feature extractor by passing the sensor. To detect the replay attack, the authenticator as to ensure that the data is captured through the sensor and has not been injected. But sensor noise and input variations make hurdle in this detection so the best method is either to build a time stamp or using challenge and response mechanism to address the replay attack.

Class III: Substitution attack: In the third type of attack the feature exactor module is replaced by a Trojan horse program that functions according to its designer specifications. Then the attacker gets an access to storage either locally or globally. He can overwrite the legitimate users template with his /her own -in essence stealing their identity

Class IV: In the fourth type of attack a genuine feature values are replaced with values (synthetic or real) selected by the attacker or an imposter

Class V: In this type of attack the matcher is replaced with a Trojan horse program. This class of attack is called *Trojan horse Attack.*

*Class VI***:** This type of attack occurs on the *template database.* The template database can be added, modified or removed. The templates can also be stolen which can be most dangerous.

Class VII: Transmission attack: A man in the middle attack is possible while the data is transmitted from one component to another. The attacker can manipulate the input data stream, send a fake template as an enrolled user, inject an artificial matching score or even generate a forged response.

Class VIII: Lastly the matured result (accept or reject) can be overridden by the attacker.

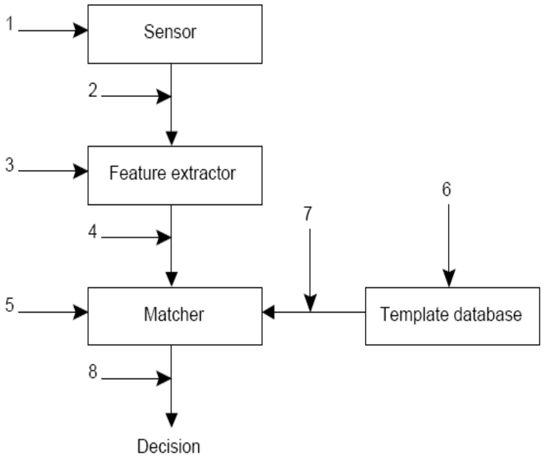

Fig 1: Location of attacks in Biometric System

3 MULTIMODAL BIOMETRIC SYSTEMS

Biometric systems used in real world applications are unimodal. They rely on the evidence of a single source of information for authentication. These systems have to deal with variety of problems such as:

Noise in the sensed data. (e.g., due to repeated use of fingerprint sensor)

Intra-class variation: User who is incorrectly acting with the sensor typically causes these variations.

Inter-class similarities: In a Biometric System where there are large no of users, there may be inter–class overlap in the feature space of multiple users.

Non-Universality: The Biometric System might not be able to acquire a meaningful Biometric data from a subset of users.

Spoof Attack: This attack occurs when signature or voice are used in Biometric System.

Not all but some of the limitations of the unimodal can be overcome by including multiple source of information for identification**.** These types of system are called as *Multimodal Biometric Systems***.** These systems are more reliable due to the presence of multiple, independent biometrics. They also have better performance, as it would be difficult for an imposter to spoof multiple biometric traits of a genuine user simultaneously. Moreover, they provide a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition. Some common multimodal biometrics are: face and finger print, face and iris, iris and finger print etc.

4 LITERATURE SURVEY

The research on multi modal biometrics started in late 90's. Face is most common biometric which is used alone or in combination with other biometrics. In 1998, a bimodal approach was proposed by Hong and Jain [5] for a PCA based face and a minutiae-based fingerprint identification system with a fusion method at the decision level. In 2000, Frischholz and Dieckmann [7] developed a commercial multimodal approach, BioID. Lip motion and face images were extracted from a video sequence and the voice from an audio signal for verifying the person. Fierrez-Aguilar and Ortega-Garcia (2003) [4] proposed a multimodal approach using face and minutiae-based fingerprint verification system, and an online signature verification system. Ross and Jain (2003) [2] combined face, fingerprint and hand geometry at the matching score level. Kumar et al. (2003) presented multimodal personal verification system using hand images by combining hand geometry and palm image at the feature level and match score level. Fusion at the match score level had good performance as compared to unimodal biometric. In 2004, Toh et al. [9] developed a multimodal biometric system using hand geometry, fingerprint, and voice at match-score-level fusion. Shahin et al. (2008) [11] used hand veins, hand geometry and fingerprint to provide high security. Chandran et al. (2009) [8] combined iris and fingerprint to improve the performance. Chin et al. (2009) [13] integrated palm print and fingerprint at feature level. Kang and Park (2009) [14] presented multimodal finger veins recognition using score level fusing for finger geometry and finger veins. Poinsot et al. (2009) [10] presented palm and face multimodal biometrics for small sample size problems. They used Gabor filter to extract features of palm and face images. Tayal et al. (2009) [12] presented multimodal iris and speech authentication system using decision theory.

5 LEVELS OF FUSION

The information of the multimodal system can be fused at any of the four modules.

Fusion at the sensor level: in this the raw data from different sensors are fused. In it we can either use samples of same biometric trait obtained from multiple compatible sensors or multiple instances of same biometric trait obtained using a single sensor. In it the data is fused at very early stage so it has a lot of information as compared to other fusion levels. Very less work has been done in this area.

Fusion at the Feature Extraction Level: The data or the feature set originating from multiple sensors or sources are fused together. Features extracted from each sensor form a feature vector. These features vectors are then concatenated to form a single new vector. In feature level fusion we can use same feature extraction algorithm or different feature extraction algorithm on different modalities whose features has to be fused. The feature level fusion is challenging because relationship between features is not known and structurally incompatible features are common and the curse of dimensionality. Because of these difficulties, only limited work is reported on feature level fusion of multimodal biometric system.

Matcher Score Level: Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. The scores obtained from different matchers are not homogeneous, score normalization technique is followed to map the scores obtained from different matchers on to a same range. These scores contain the richest information about the input. Also it is quite easy to combine the scores of different biometrics so lot of work has been done in this field.

Fusion at the Decision Level: The final outputs of the multiple classifiers are combined. A majority vote scheme can be used to make final decision. Decision level fusion includes very abstract level of information so they are less preferred in designing multimodal biometric systems.

Biometric systems that integrate information at the early stages are more effective than those in which integration is done in later stages. So fusion at the feature level is expected to give better recognition results but it is difficult to integrate at this level because feature sets of the various systems may not be compatible. More over all commercial Biometric systems don't provide access to the feature sets, which they use in their products. Fusion at the matcher score level is usually preferred because it is relatively easy to access and combine the scores presented by different modalities.

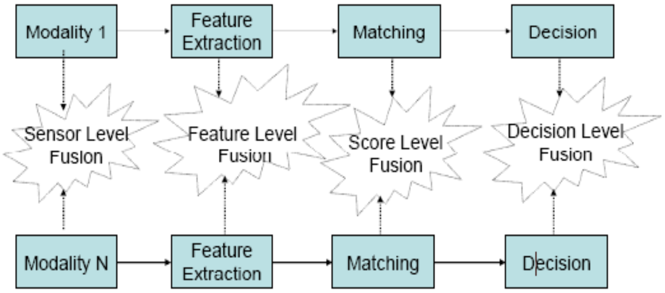

Fig 2: Fusion at different levels

6 TYPES OF MULTIMODAL SYSTEMS

Depending on the traits, sensors and feature sets many different types of multimodal systems are there:

Single biometric trait, multiple sensors: Multiple sensors are used to record the same biometric characteristic. The raw data taken from different sensors can then be combined at the feature level or matcher score level to improve the performance of the system.

Multiple biometrics: Multiple biometric traits such as fingerprints and face can be combined. Different sensors are used for each biometric characteristic. The interdependency of the traits ensures a significant improvement in the performance of the system. A commercial product BioID [7] uses voice, lip motion and face of a user to verify identity.

Multiple units, single biometric traits: Two or more fingers of a single user can be used as a biometric trait. It is inexpensive way of improving system performance, as it doesn't require multiple sensors or incorporating additional feature extraction or matching modules. Iris can also be included in this category.

Multiple snapshots of single biometric: In this more than one instance of the same biometric is used for the recognition. For e.g. multiple impressions of the same finger or multiple samples of the voice.

Multiple matching algorithms for the same biometric: In it different methods can be applied to feature extraction and matching of the biometric characteristic.

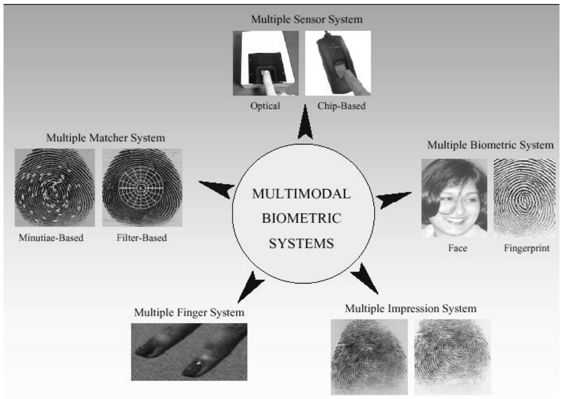

Fig 3: Types of Multimodal Systems

7 MODES OF OPERATION

A multimodal biometric system can work in three modes:

Serial mode: In the serial mode the output of one biometric characteristic is used to reduce the no of possible identities before the next characteristic is used. So multiple source of information is not collected simultaneously.

*Parallel mode***:** In it the information from multiple characteristics is taken together to perform recognition.

Hierarchical mode: In it individual classifiers are combined in a tree like structure. This mode is well suited where we have large no of classifiers.

8 DESIGN ISSUES IN MULTIBIOMETRICS

- Choice and number of biometric indicators
- Fusion Level:
  -Representation (incompatibility & unavailability of features)
  -Matching score (preferred; normalize matching scores)
- Decision (too rigid; majority vote)
- Fusion methodology
- Learning weights of individual biometric for each user
- Cost versus performance trade-off
- Verification vs. Identification system

9 APPLICATIONS OF MULTIMODAL BIOMETRICS

The defense and the intelligence communities require high level security systems. Border management, interface for criminal and civil applications, and first responder verification are the major areas which use the Multimodal Biometrics. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Multi modal biometrics can provide best solutions to all the areas where high level security systems are needed.

10 CONCLUSIONS

Biometric technology adds a new layer of security by ensuring secure identification and authentication. But biometric authentication systems like any other technology are also vulnerable to attacks such as transmission, replay and spoofing. There are many proposed methodologies that are used to defeat them. Multimodal biometric system is a major approach to defeat spoofing attacks. Various fusion levels and scenarios of multimodal systems are discussed.

REFERENCES:

[1] L. Hong, A. Jain & S. Pankanti, *Can Multibiometrics Improve performance*, Proceedings of AutoID 99, pp. 59-64, 1999.
[2] A. Ross & A. K. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.
[3] Ross.A. A, Nandakumar.K, Jain.A.K. Handbook of Multibiometrics. Springer-Verlag, 2006.
[4]J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez Rodriguez, ―A comparative evaluation of fusion strategies for multimodal biometric verification,‖in Proc. 4th Int, Conf,Audio-video-based Biometric PersonAuthentication , J. Kittler and M. Nixon, Eds., 2003 vol. LNCS 2688, pp. 830–837
[5] L. Hong and A. K. Jain, ―Integrating faces and fingerprints for personal identification,‖ IEEE Trans. Pattern Anal. Mach. Intell. , vol. 20, no. 12, pp. 1295– 1307, Dec. 1998
[6] A. Kumar, D. C. M. Wong, H. C.Shen1, and A. K. Jain, ― Personal verification using palmprint and hand geometry biometric,‖in Proc. 4th Int. Conf. Audio- Video-Based Biometric Person Authentication , J. Kittler and M Nixon, Eds., 2003 vol. LNCS 2688, pp 668–678
[7R. Frischholz and U. Dieckmann, ―BiolD: A multimodal biometric identification system,‖ Computer,vol.33,no.2, pp.64-68,Feb,2000
[8] Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.
[9]K. A. Toh, X. D. Jiang, and W. Y. Yau, ―Exploiting global and local decisions for multi-modal biometrics verification,‖ IEEE Trans. Signal Process. , vol. 52, no. 10, pp. 3059–3072, Oct. 2004
[10] Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International Multi-Conference on Computing in the Global Information Technology.
[11] Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIBEC'08.
[12]Tayal A, Balasubramaniam R, Kumar A, Bhattacharjee A, Saggi M (2009). A Multimodal Biometric Authentication System Using Decision Theory, Iris and Speach Recognition, 2nd International Workshop on Nonlinear Dynamics and Synchronization.
[13] Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.
[14] Kang BJ, Park K (2009). Multimodal Biometric Authentication Based on the Fusion of Finger Veins and Finger Geometry, Optical Eng., 48.
[15] J.Daughman, ―Combining multiple biometric,‖ Avaliable online at www.cl.ca.ac.uk/users/igd1000/combine.html, 2002.
[16] Anil K. Jain , Ruud Bolle and Sharath Pankanti "Biometric Personal Identification in Networked Society".
[17]" Global Security. Emerging Technologies
URL: http://www.globalsecurity.org/security/systems/emerging.htm