2012 International Conference on Information and Knowledge Management (ICIKM 2012)
IPCSIT vol.45 (2012) © (2012) IACSIT Press, Singapore

A Novel Multimodal Biometric Fusion Technique for Security

B. Shanthini[1], S. Swamynathan[2]

[1] Research Scholar, Anna University, Chennai, India
[2] Associate Professor, Anna University, Chennai, India

[1]bshanthini@gmail.com, [2]swamyns@annauniv.edu

Abstract. As organizations search for more secure authentication methods for user access, e-commerce, and other high security applications, biometric system, which is a pattern recognition system that recognizes a person by determining the authenticity of a specific biological and/or behavioral traits possessed by that person, is gaining increasing attention. In this paper, we discuss a new mode of fusion of multimodal biometrics in which the number of security services provided by our system increases as the need for security increases and is mainly used in hierarchy-based high security MANETs say military scenario. Also we have discussed about the different multimodal techniques and algorithms proposed by various authors, the mode of fusing the multi modalities and the purpose of multimodal fusion etc.

Keywords: Multimodal Biometrics, Modes of Fusion, Security Services.

1. Introduction

1.1. Biometric System

There are three general ways to identify a person to a computer system, based on what you know, what you have, or who you are. “What you know” approaches such as passwords and PINs have less reliability because they can be lost, stolen, or guessed. “What you have” technologies such as RFID cards and e-tokens also can be stolen. Biometrics belong to the “who you are” class and can be subdivided into behavioral and physiological approaches. Behavioral biometric include signature recognition, voice recognition, keystroke dynamics, and gait analysis. Physiological biometric include fingerprints, iris, retina scans, hand, finger, face, ear geometry, hand vein, nail bed recognition, DNA and palm prints. As biometrics can't be borrowed, stolen, forgotten, and forging is practically impossible, it has been presented as a natural identity tool that offers greater security and convenience than traditional methods of personal recognition. Biometric system is an enabling technology with the potential to make our society safer, reduce fraud, and lead to user convenience by providing the functionalities [1] like verification, identification, screening and enrolment.

1.2. Issues and Challenges

Ratha *et al.* [2] identified different attacks that can be launched against the biometric system and these attacks are intended to either thwart the security afforded by the system or to affect the normal functioning of the system. The various causes of biometric system vulnerability are summarized by Anil K Jain et al. [3]. The failure modes of a biometric system can be categorized into two classes: intrinsic failure caused by Zero-effort attacks and failure due to an adversary attack.

Intrinsic failure is the security lapse due to an incorrect decision made by the biometric system. A biometric verification system can make two types of errors in decision making, namely false accept and false reject. A genuine user may be falsely rejected by the biometric system due to the large differences in the user’s stored template and query biometric feature sets. False accepts are usually caused by inter-user similarity that is lack of individuality or uniqueness in the biometric trait which can lead to large similarity between feature sets of different users.

Adversary attacks refer to the possibility that a determined impostor would be able to masquerade as an enrolled user by using a physical or a digital artifact of a legitimate user. These adversary attacks are categorized into three main classes:

i. Administration Attack: This insider attack refers to all vulnerabilities introduced due to improper administration of the biometric system.

ii. Non-secure infrastructure: An adversary can manipulate the biometric infrastructure like hardware, software and the communication channels between the various modules that can lead to security breaches.

iii. Biometric overt ness: It is possible for an adversary to covertly acquire the biometric characteristics of a genuine user and use them.

While a biometric system can enhance user convenience and support security, it is also susceptible to various threats like circumvention, repudiation, covert acquisition, collusion, coercion, denial of service and intrusion as discussed by Umut Uludag et al. in [4]. Also there are other algorithms like brute-force attack and hill climbing attack to attack the biometric systems and are explained in [5]. Limitations in a Unimodal Biometric System are summarized by Anil et. al. [6, 7] those operate on any single biometric characteristic. They include noise in sensed data, intra-class variations, distinctiveness, non-universality and spoof attacks.

1.3. Techniques to Counter the Attacks

Several techniques have been suggested to protect biometric system from revealing important biometric information in the literature. To prevent the Hill-Climbing Attack, Andy Adler [5] has suggested the use of coarsely quantized match scores by the matcher. However, he demonstrated that it is still possible to estimate the unknown enrolled image. Soutar et al. [8] developed an innovative process called Biometric Encryption which combines the biometric image with a digital key to create a secure block of data, known as a Bioscrypt. Ferri et al. [9] proposed an algorithm to embed dynamic signature features into face images present on ID cards. These features are transformed into a binary stream after compression. During verification, the signature features hidden in the face image are recovered and compared against the signature obtained on-line.

Jain and Uludag [10] suggested different methods to hide biometric data in host images. In Spatial Domain either pixel values in the image channel are changed or based on Steganography the facial information is hidden inside the fingerprint images. In Spectral Domain watermark signal is added to the host image in a transform domain. Radha et al. [2] explained an Image-based challenge/response method in which a transaction is initiated at the user terminal. First, the server generates a pseudorandom challenge and the client system passes the challenge to the intelligent sensor. Now, the sensor acquires a new signal and computes the response to the challenge that is based on the newly acquired signal. The changing challenges ensure that the image was acquired after the challenge was issued.

Arslan Brromme [11] devised Biometric Signatures which is defined as a binary coded representation of biometric characteristics for distributed computing systems. He also classified the Biosignatures into six types namely Monomodal Biosignature, Multimodal Biosignature, Monomodal Biometric Template, Multimodal Biometric Template, Monomodal Biometric Multi Template and Multimodal Biometric Multi Template. Uludag et al. [12] convert fingerprint templates (minutiae data) into point lists in 2D space, which implicitly hide a given secret. The list does not reveal the template data, since it is augmented with chaff points to increase security. The template data is identified only when matching minutiae data from an input fingerprint is available.

Some hybrid techniques are widely used in recent years to overcome the limitations of uni-modal biometrics. Several techniques have been already explained in the literature to overcome the attacks against the biometric security system. Some of the limitations imposed by uni-modal biometric systems can be overcome by using multiple biometric modalities.

2. Multimodal Biometric Systems

2.1. Operational modes of multimodal biometric systems:

A multimodal biometric system can operate in three different modes [7]. In the ***serial mode*** of operation, the output of one biometric trait is used to narrow down the number of possible identities before the next trait is used. In a ***parallel mode*** of operation information from multiple traits is used simultaneously to perform recognition. In the ***hierarchical scheme***, individual classifiers are combined in a treelike structure.

2.2. Integration scenarios of multimodal biometrics [7]:

Multimodal biometric systems are designed to operate in one of the 5 integration scenarios as below.

i. Multiple sensors: the information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.

ii. Multiple biometric: multiple biometric characteristics such as fingerprint and face are combined. These systems will contain more than one sensor with each sensor sensing a different biometric characteristic.

iii. Multiple units of the same biometrics: fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.

iv. Multiple snapshots of the same biometrics: more than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.

v. Multiple representations and matching algorithms for the same biometrics: this involves combining different approaches to feature extraction and matching of the biometric characteristic.

2.3. Levels of fusion in multimodal biometric systems:

When combining two or more biometric systems in a multimodal biometric system, the information present can be consolidated at various levels as explained below:

i. Fusion of features of the multimodal biometric. The data obtained from each biometric modality is used to compute a feature vector. The vectors from 2 or more biometric are concatenated into a single new vector. Arun Ross et. al. [13] presented a technique to perform fusion at the feature level by considering two biometric modalities - face and hand geometry. The fused feature vector can be obtained by augmenting the normalized feature vectors and performing feature selection on the concatenated vector. The normalized vectors are computed by applying a transformation to the individual feature values in order to ensure that the feature values across the two modalities are compatible. Krishneshwari et. al. [14] proposed to fuse palm print image with finger print image and extract feature in the frequency domain using Discrete Cosine Transform. In this study Bi-orthogonal wavelet decomposition is done on the images to be fused. During fusion the minimum approximation of both the images are used. Since image fusion requires both the images to be of the same size, the images are resized before fusion.

ii. Fusion of multimodal biometric matching scores. Each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Terrence Sim et. al [15] presented the theory, architecture, implementation, and performance of a multimodal biometrics verification system that continuously verifies the presence of a logged-in user. They showed that continuous verification imposes additional requirements on multimodal fusion when compared to conventional verification systems. They combined face and fingerprint modalities at the score level. Dong-Ju Kim et. al. [16] proposed a new multimodal authentication system which combines teeth images and voice. The individual matching scores obtained from the teeth image and voice are combined using a weighted-summation operation, and the fused-score is utilized to classify an unknown user into acceptance or rejection.

iii. Fusion of decisions taken for multimodal biometric. Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme can be used to make the final decision. Multiple biometrics are fused at the decision level to support a system that can meet more challenging and varying accuracy requirements as well as address user needs such as ease of use and universality better than a single biometric system or static multimodal biometric system. The decision fusion rules are adapted to meet the varying system needs by particle swarm optimization in paper [17] is an evolutionary algorithm. This paper focuses on the details of the new sensor management algorithm and demonstrates its effectiveness. Krzysztof Kryszczuk et. al. [18] presented a methodology of reliability estimation in the multimodal biometric verification scenario which has shown to be an efficient and accurate way of predicting and correcting erroneous classification decisions in multimodal systems.

iv. Fusion of security services provided by multimodal biometric. Each biometric modality is used for providing different security services. As the security level increases accordingly the no. of security services provided by the system is also increases. For example, one biometric can be used for security, another for authentication and other for authorization etc. The Multimodal Biometric-based Authentication Combined Security System [19-20] provided authentication using face / voice biometrics and security using fingerprint biometrics. In these systems, for authentication, Eigen face or voice signal of the sender is attached to the data to be transferred. Second, to enhance security, the data and the Eigen face of the sender or voice signal are encrypted by using the key which is extracted from the fingerprint biometric of the receiver. The Privacy Protected Multimodal Biometric-based Secured Authentication System proposed in [21] authenticates the sender by using face biometric and the data transferred between the users are encrypted by the fingerprint based key generated from the receiver's fingerprint biometric. For authorization of the receiver the voice biometric is used.

By this way different security services say authentication, data security and integrity are provided by our multimodal biometric based secured authentication systems. Table 1 compares the different modes of multimodal biometric fusion done by various authors and the security services provided by these systems.

3. Case Study of our Fusion Techniques

From the references given [13-18] we can understand that these security systems concentrates only on one security service, either authentication or access control etc. Our fusion technique focuses on fusing the security services provided by multimodal biometric. As shown in figure 1, as the security level increases the number of security services provided by biometric modalities also increases. For example, [19] uses face modality for authentication and fingerprint for data security, [20] uses voice signals for authentication, and fingerprint for data security and [21] uses face for authenticating the sender, fingerprint for data security and voice signal for authorizing the receiver. Our fusion techniques are explained in figure 2, where Level 1 uses only one biometrics for securing the data, Level 2 uses two modalities say face and fingerprint for authentication and data security and Level 3 uses 3 modalities say face for authentication, fingerprint for security and voice for authorizing the receiver.

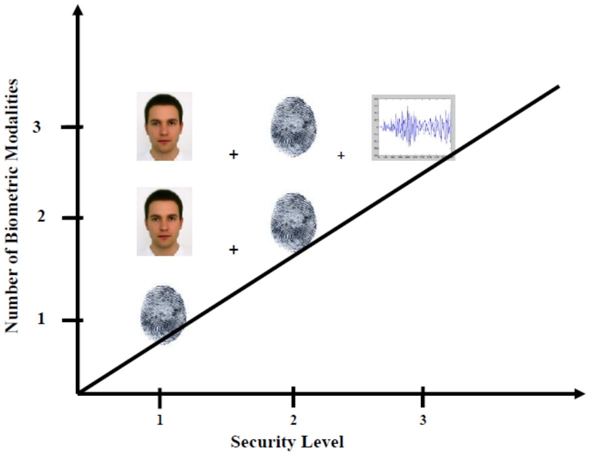

Fig.1. Fusion Techniques to increasing security levels

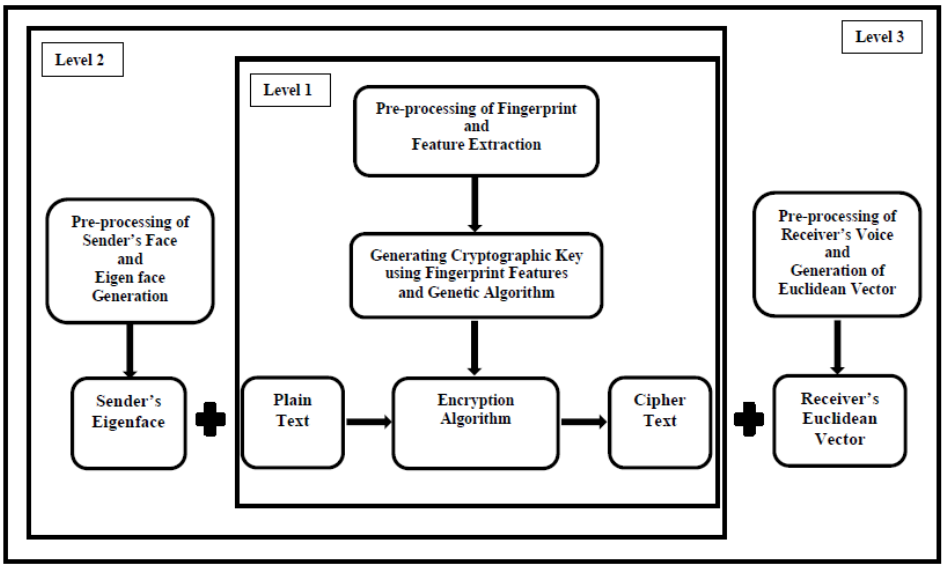
Level 3
Level 2
Level 1
Pre-processing of Fingerprint and Feature Extraction
Generating Cryptographic Key using Fingerprint Features and Genetic Algorithm
Pre-processing of Sender's Face and Eigen face Generation
Pre-processing of Receiver's Voice and Generation of Euclidean Vector
Sender's Eigenface
Plain Text
Encryption Algorithm
Cipher Text
Receiver's Euclidean Vector

Fig.2. Our Fusion Techniques

Table 1. Security parameters for various techniques and Key size and Timing Measurements for various algorithms

Fusion Tech.	Security Parameters						Key size Time Complexity Parameters					
	Security–Encryption	Authentication	Revocability	Practicality	Liveness	Authorization	Key Size	Time for Key Gen. (ms)	Time for Enc. (ms)	Time for Dec. (ms)	Time for Auth. (ms)	Time for Autho. (ms)
GBBSSM	Yes	No	Yes	Yes	Yes	No	64	0,06	0.04	0.03	-	
SSMGBB	Yes	No	Yes	Yes	Yes	No	64	0,06	0.04	0.04	-	-
SASMBM	Yes	Yes	Yes	Yes	Yes	No	64	0.08	0.04	0.02	0.045	-
SASMVFB	Yes	Yes	Yes	Yes	Yes	No	64	0.08	0.04	0.02	0.022	-
PMBSAS	Yes	Yes	Yes	Yes	Yes	Yes	64	0.08	0.04	0.02	0.064	0.051

A brief comparison of security related parameters and time taken for key generation, encryption and decryption for various techniques of our biometric-based security systems like GBBSSM[22], SSMGBB[23], SASMBM[19], SASMVFB [20] and PMBSAS [21] are given by table 1. The graph shown in figure 3 is generated by using the timing measurements given in table 1.

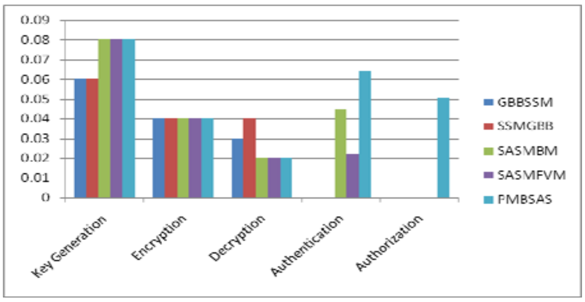

Fig.3. Timing measurements for various techniques

4. Conclusion

Biometrics systems are expected to add a new level of security and reliable user authentication to all sorts of applications. Due to the evidence of growing public awareness and interest in the use of biometrics, these systems will propagate into the core information infrastructure of the near future. In this paper, we have summarized various attacks and vulnerabilities in a biometric system and discussed different techniques to counter these threats. Multimodal biometric systems can be the best solution for the problems arised by the uni-modal system which integrate information at various levels. Besides improving matching performance, they also address the problem of non-universality and spoofing. From these discussions we conclude that the major challenge in designing a biometric security scheme should satisfy the important properties like Diversity, Revocability, Security and Performance. Since a single approach may not be sufficient to meet all the application requirements, hybrid schemes that make use of the different approaches must be developed.

5. References

[1] Anil K. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Information Security,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing Security and Privacy in Biometric-based Authentication System”, IBM Systems Journal, Vol.40, No.3, pp.614-634, 2001.

[3] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, 2008.

[4] U. Uludag and A. K. Jain, “Attacks on Biometric Systems: A Case Study in Fingerprints,” in Proc. SPIE-EI Security, Steganography and Watermarking of Multimedia Contents VI, San Jose, CA, pp.622–633, 2004.

[5] Andy Adler, “Vulnerabilities in Biometric Encryption Systems,” Work Supported by NSERC Canada, 2004.

[6] Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition”, IEEE Transactions On Circuits And Systems for Video Technology, Vol. 14, No. 1, 2004.

[7] Anil K. Jain, Arun Ross and Sharath Pankanti, “Biometrics: A Tool for Information Security” IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006.

[8] C. Soutar, “Biometric system security,” White Paper, Bioscrypt, http://www.bioscrypt.com.

[9] L. C. Ferri, A. Mayerhofer, M. Frank, C. Vielhauer, and R. Steinmetz, “Biometric authentication for ID cards with hologram watermarks,” in Proc. SPIE, Security and Watermarking of Multimedia Contents IV, vol. 4675, pp. 629–640, 2002.

[10] A. K. Jain & Uludag, “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intel., vol.25, no.11, pp.1493–1498, 2003.

[11] Arslan Brromme, “A Classification of Biometric Signatures,” ICME 2003.

[12] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy vault for fingerprints,” Proc. Audio- and Videobased Biometric Person Authentication (AVBPA), 2005.

[13] Arun Ross and Rohin Govindarajan, "Feature Level Fusion in Biometric Systems", in proceedings of Biometric Consortium Conference (BCC), 2004.

[14] Krishneswari, K. and S. Arumugam, “Multimodal Biometrics using Feature Fusion”, Journal of Computer Science, Vol.8, Issue 3, pp. 431-435, 2012.

[15] Terrence Sin, Sheng Zhang, Rajkumar Janakirman and Sandeep Kumar, “Continuous Verification using Multimodal Biometrics”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.29, No.4, 2007.

[16] Dong-Ju Kim and Kwang-Seok Hong, “Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment”, IEEE Transactions on Consumer Electronics, Vol. 54, No. 4, 2008.

[17] Kalyan Veeramachaneni, Lisa Ann Osadciw, and Pramod K. Varshney, “An Adaptive Multimodal Biometric Management Algorithm”, IEEE Transactions on Systems, Man and Cybernetics—Part C: Applications And Reviews, Vol. 35, No. 3, 2005.

[18] Krzysztof Kryszczuk, Jonas Richiardi, Plamen Prodanov, and Andrzej Drygajlo, “Reliability-Based Decision Fusion in Multimodal Biometric Verification Systems”, EURASIP Journal on Adv. in Signal Processing Vol.2007, ID 86572, 2007.

[19] B. Shanthini and S. Swamynathan, “A Secure Authentication System using Multimodal Biometrics for High Security MANETs”, The 1st Int. Conf. on Advances in Computing and Information Technology, CCIS 198, pp. 290-307, 2011.

[20] B. Shanthini and S. Swamynathan, “A Secured Authentication System for MANETs using Voice and Fingerprint Biometrics”, European Journal of Scientific Research, vol. 59, no. 4, pp. 533-546, 2011.

[21] B. Shanthini and S.Swaminathan, “Privacy-protected Multimodal Biometric-based Secured Authentication System for Hierarchy-based High Security MANETs”, Journal of Communication Networks. (Communicated)

[22] B. Shanthini and S. Swamynathan, “Data Security in Mobile Ad Hoc Networks using Genetic Based Biometrics”, International Journal of Computer Science and Information Security,vol. 8, no. 6, pp.149-153, 2010.4195516abstract

[23] B. Shanthini and S. Swamynathan, “A Security System using Genetic Based Face Biometrics for MANETs“, Int. Conference on Intelligent Systems and Technology, CSE-124, 2011.