International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 239-246
http://dx.doi.org/10.14257/ijsia.2015.9.4.22

Analysis of Multimodal Biometric Fusion Based Authentication Techniques for Network Security

R.Divya[#1] and V.Vijayalakshmi[#2]

[#1] *Research Scholar, Department of ECE, Pondicherry Engineering College, Puducherry*
[#2] *Assistant Professor, Department of ECE, Pondicherry Engineering College, Puducherry.*
[1]*div.1484@gmail.com;*[2]*vvijizai@pec.edu*

Abstract

Multibiometrics is the usage of more than one physiological or behavioral characteristic to identify an individual. Multibiometrics is advantageous over unibiometrics as it is resilience to spoofing and has low False Acceptance Rate (FAR). However Multibiometrics requires storage of multiple biometric templates for each user, which results in increased risk to user privacy and system security. This paper will discuss the concept off biometrics and biometric system, multimodal biometric fusion techniques, crypto-biometrics and an algorithm for session key generation for secure communication of data.

Keyword: *Biometrics, multibiometric fusion, cryptobiometrics, security.*

1. Introduction

Biometric systems operate under the premise that many of the physical or behavioral characteristics of humans are distinctive to an individual, and that they can be reliably acquired via appropriately designed sensors and represented in a numerical format that lends itself to automatic decision-making in the context of identity management. Thus, these systems may be viewed as pattern recognition engines that can be incorporated in diverse markets.

Traditional methods of establishing a person's identity include knowledge-based (*e.g.*, passwords) and token-based (*e.g.*, ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

2. Strength of Biometrics

Biometric identifiers are difficult to be lost or forgotten, difficult to be copied/shared, and require the person to be authenticated to be present at the time and point of authentication (a user cannot claim his password was stolen and misused). Instead of passwords, biometric systems could be used to protect the strong cryptographic keys. For a given biometric identifier, all users have a relatively equal security. There cannot be many users who have "easy to guess" biometrics that can be used to mount an attack against them.

3. Biometric System

In a biometric system, a physical trait needs to be recorded. The recording is referred to as an enrollment. This enrollment is based on the creation of a template. A template is the digital representation of a physical trait. The template is normally a long string of alphanumeric characters that describe, based on a biometric algorithm, characteristics or features of the physical trait. The basic block diagram of an biometric system is shown in Fig.1 The biometric algorithm can be viewed as the recipe for turning raw ingredients like a physical trait into a digital representation in the form of a template. The algorithm will also allow the matching of an enrolled template with a new template just created for verifying an identity, called a live template. When a stored template and a live template are compared, the system calculates how closely they match. If the match is close enough, a person will be verified. If the match is not close enough, a person will not be verified.

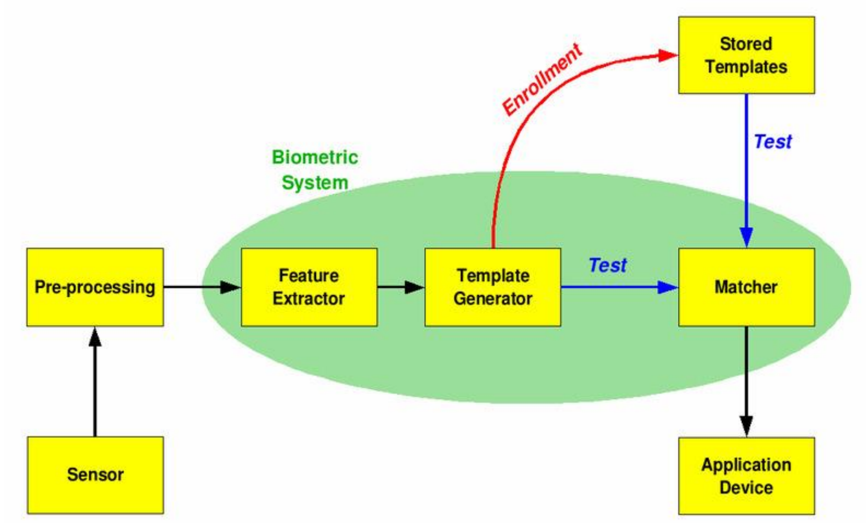

Figure 1. Block Diagram of Biometric System

Sensor: The sensor is an interface between the real world and the system. It is used to acquire all the necessary data, depending on the characteristic in consideration.

Pre-processing : This block is needed to enhance the input *(i.e.*, remove all the background noise and unnecessary artifacts during data collection) and also to use some kind of normalization, if needed.

Feature Extractor : This block is responsible to extract the necessary features from the pre-processed input in the correct
and in the optimal way.

Template Generator : The template is typically a vector of numbers or an image with particular properties, and is generally a synthesis of the relevant characteristics extracted from the source.

Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee. If an enrollment is performed, the template is typically stored in a central database. If a matching is being performed, the obtained template is passed to a matcher that compares it with other relevant templates in the database and estimates the distance between them using any specific algorithm (*e.g.*, the Hamming Distance metric) and returns the result.

4.1. Performance Metrics for Biometric Systems

The different performance metrics for evaluating the biometric system are as follows

False Acceptance Rate (FAR) : The FAR is defined as the probability that a user making a false claim about his/her identity will be verified as that false identity. The importance of the FAR is the strength of the matching algorithm. The stronger the algorithm, the less likely that a false authentication will happen.

FRR (False Rejection Rate): The FRR is defined as the probability that a user making a true claim about his/her identity will be rejected as him/herself. The strength of the FRR is the robustness of the algorithm. The more accurate the matching algorithm, the less likely a false rejection will happen.

Crossover Error Rate (CER): The rate at which both the accept and reject errors are equal. A lower value for the CER is desired for a biometric system in order to be considered more accurate as well as convenient for its users.

Failure to Enroll Rate (FER): The rate at which attempts to create a template from an input is not successful. This is most commonly caused by low quality inputs that are insufficiently distinctive biometric samples or from a system design that makes it difficult to provide consistent biometric data.

Failure to Capture Rate (FCR): Applicable for automated systems, the probability that the system fails to detect a biometric input when presented correctly.

Template Capacity: The number of unique users that can be represented by its contents

Tradeoff: Larger the FER, lower the FAR and FRR; and vice-versa.

The graphical representation of relationship between FRR, FAR and CER is shown in Fig.2.

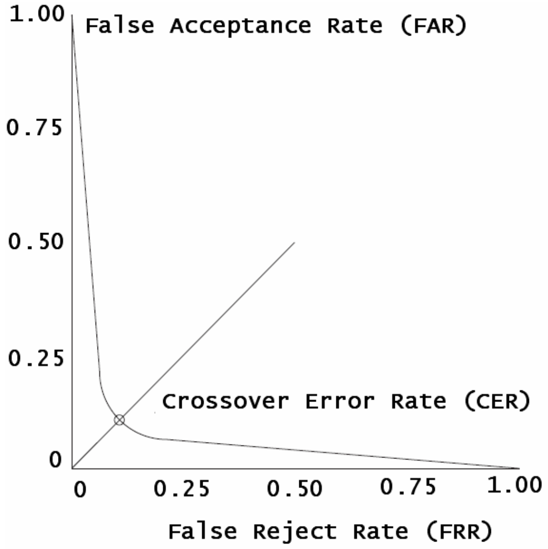

Figure 2. Typical Relationship between FRR, FAR and CER

4.2. Biometric System Evaluation

The biometric system can be evaluated with the help of these factors

Universality: Can everyone provide the considered biometric.

Uniqueness: How well the biometric separates individually from another.

Permanence : Stability along life time.

Collectability : Ease of capture for measurement.

Performance : Accuracy, speed, and robustness of technology used.

Acceptability : Degree of approval of a technology by end user.

Circumvention : How hard to fool the system.

4.3. Different Biometric Traits

The biometric trait can be classified into two different categories as

- Physical / Physiological Biometrics
- Behavioural Biometrics

The traits that comes by birth with the individual like finger print, face, iris, retinal pattern, ear, voice, hand, DNA, vein, tongue etc. can be classified as Physical / Physiological Biometrics and the traits that can be developed as the grows up like signature, keystroke, gait etc.can be classified as Behavioural Biometrics.

5. Multi-Biometric Systems

While every user is expected to possess the biometric identifier being acquired, in reality, it is possible for a subset of the users to be not able to provide a particular biometric. An impostor may attempt to spoof the biometric identifier of a legitimate enrolled user in order to circumvent the system. So multimodal biometric system is an advantage when compared to unimodal system. A Multi-biometric system could address the problem of non-universality, since multiple biometric identifiers would ensure sufficient population coverage. Provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric identifiers of a legitimate user. Ensure a "live" user is present at the point of data acquisition by asking the user to present a random subset of the multiple biometric identifiers. Overall, multi-biometric systems could facilitate a challenge-response kind of authentication.

4.4.1. Levels of Fusion in Multi-Biometric Systems

The various fusion levels for a multi-biometric system is summarized in this section. They are as follows

- Sensor-Level Fusion
- Feature-Level Fusion
- Match Score-Level Fusion
- Decision-Level Fusion

Sensor-Level Fusion: The raw data obtained from multiple sensors (one for each biometric identifier) can be processed and integrated to generate new data from which features can be extracted.

Feature-Level Fusion: The feature sets extracted from each biometric identifier sources can be fused to create a new feature set to represent the individual. The block diagram of feature level fusion multi-biometric system is shown in Fig.3.

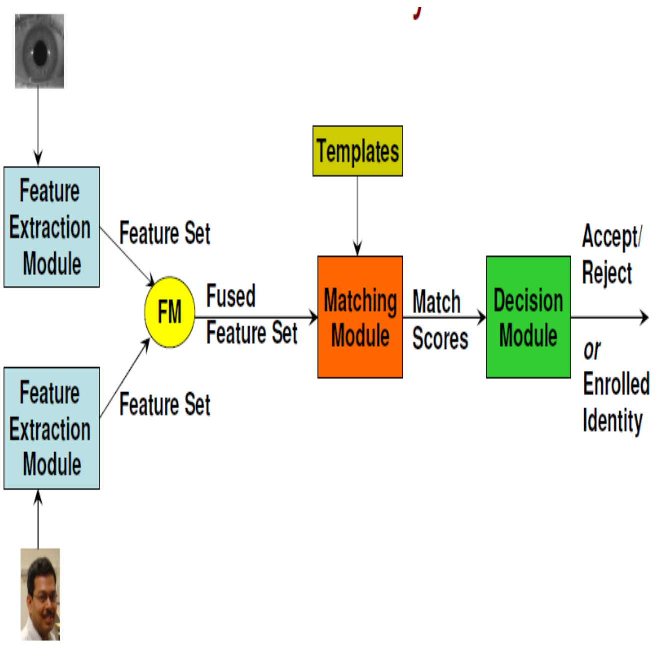

Figure 3. Block Representation of Feature Level Fusion

Match Score-Level Fusion: The match scores obtained from each biometric classifier are normalized and the normalized scores are summed to obtain a new match score used to make the final decision. The block diagram of score level fusion multi-biometric system is shown in Fig.4.

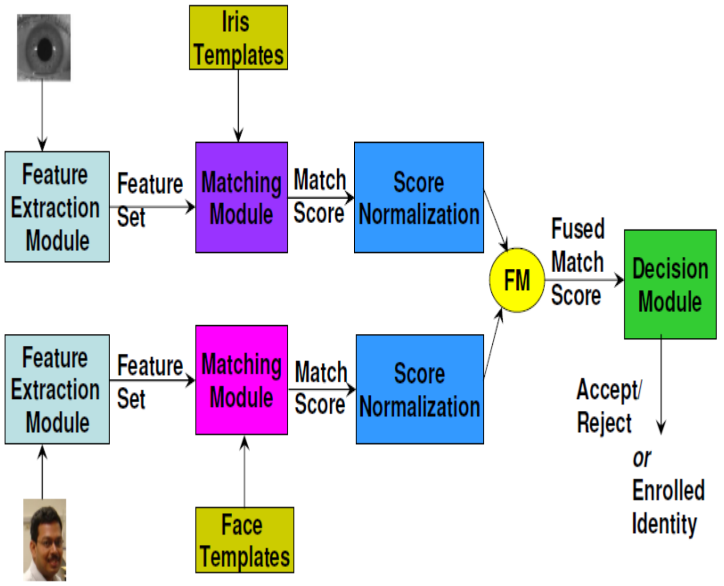

Figure 4. Block Representation of Score Level Fusion

Decision-Level Fusion: The decisions (Accept/ Reject) made at each biometric system based on the individual scores are then combined (usually a majority voting approach) to arrive at a final decision. The block diagram of decision level fusion multi-biometric system is shown in Fig.5.

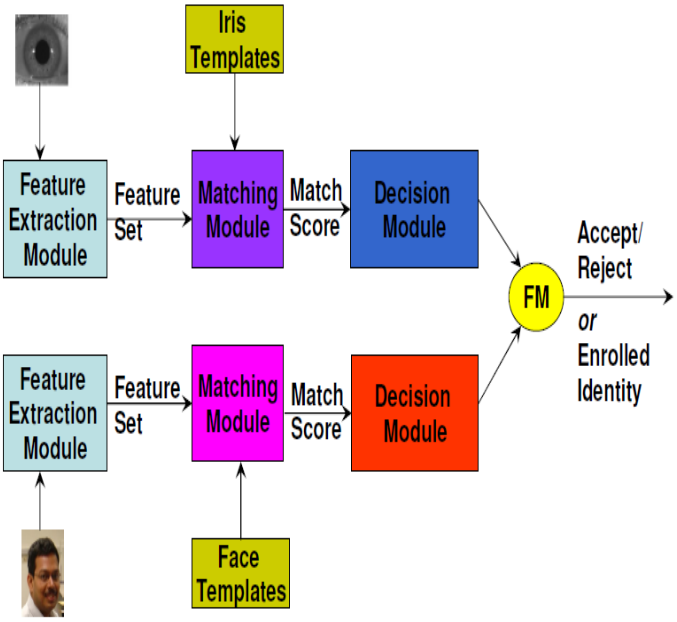

Figure 5. Block Representation of Decision Level Fusion

6. Biometric for Network Security

Combining Biometrics with Cryptography for secure data communication takes place with the help of two steps as

- Biometric-Key Release
- Biometric-Key Binding

Biometric-Key Release: A legitimate user (say ‘Alice’) wishes to access certain digital content. She offers her biometric sample to the system. If the biometric matcher successfully matches Alice’s input biometric sample with her enrolled biometric template, then a cryptographic key can be released. The cryptographic key is used to decrypt the content and Alice is allowed to access the content. If an illegitimate user attempts to access the same digital content posing as Alice, his biometric match with the biometric template of Alice will fail and Alice’s cryptographic key will not be released by the system.

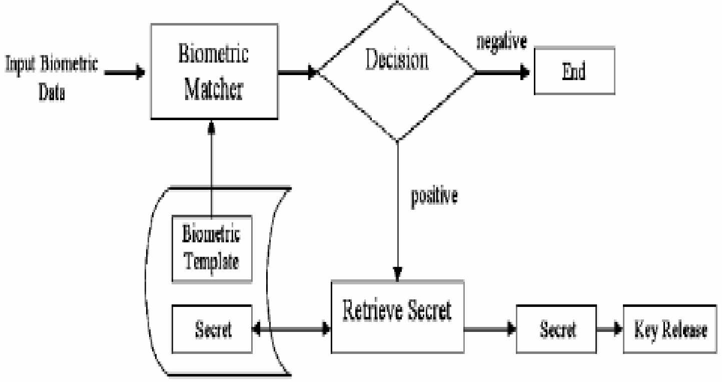

Figure 6. Biometric-Key Release

Biometric-Key Binding: The idea is to store only a hash of the biometric template (instead of the actual template) in the database, similar to the concept of cancellable biometric. If the hash function chosen is a one-way hash function, it may not be possible to use the hash value of the biometric template to extract the original biometric sample. So, even if the template hash database is stolen, it would not be a problem. In addition, a trusted and secret bit-replacement algorithm can be used to hide the cryptographic key within the user's biometric template itself rather than storing it separately. A simple bit-replacement algorithm could be to replace the least significant bits of the pixels values/features of the biometric template with the cryptographic key. Since the biometric matching and key extraction are integrated, it may not be possible for an attacker to compromise the biometric authentication system with a Trojan horse and expect the cryptographic key to be released. However, if the biometric smart card is stolen, the person who has the Smart card would be still able to extract the cryptographic key.

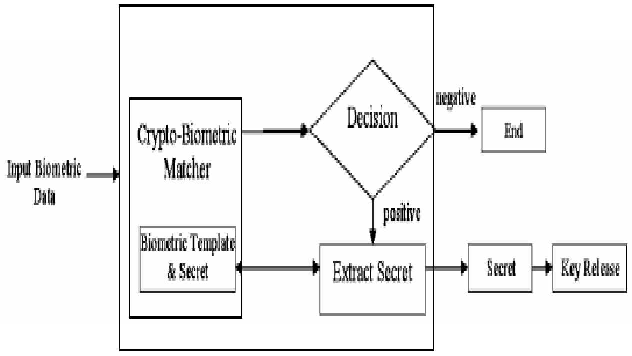

Figure 6. Biometric-Key Binding

6.1 Biometrics based Session-key Generation and Sharing Protocol

In this Biometrics based session-key generation and sharing protocol the enrollment is securely carried out off-line and cancelable template is generated using the biometric data of the user and it is stored in the database at the server. The cancelable template from biometric data is θ_{canc} The shuffling of the enrollment biometric data is done by θ_{ref} + shuffling key K_{sh}. The shuffling key K_{sh} is either stored on a smart card or can be generated from a password. The algorithm for generating session key is as follows

When a client desires to securely communicate with the server, following steps are carried out:
The client sends authentication request to the server.
The server sends acknowledgement to the client.
Shuffled test biometric data θ'_{canc} by client
1. Fresh biometric data θtest of the user is captured .
2. Shuffled using the shuffling key K_{sh}
3. $\theta'_{canc} = \theta_{test} + K_{sh}$

User ID of the user is sent to the server not the biometric
Locked code θ_{lock} is created by server
1. The server generates a random key K_r
2. Stored cancelable template θ_{canc}.
3. $\theta_{lock} = E(K_r, \theta_{ref})$ where E( ) indicates the encoding function.

The locked code θ_{lock} and $H(H(K_r))$ is sent to the client.
1. The client regenerates a trial value of the random key K'_r

$$K'_r = E\text{-}1(\theta'_{canc}, \theta_{lock})$$

2. K'_r is made as $H(H(K'_r))$

If $H(H(K_r)) = H(H(K'_r))$ – Server Authentic
then
$H(K'_r)$ is sent to server
Server compares $H(K'_r) = H(K_r)$, to check the authenticity of the client.
If $H(K'_r) = H(K_r)$ – user Authentic - both parties - same key K_r.
Server sends the signal to start secure communication using the key Kr.

The Client & server share the same key which is a concept of symmetric key cryptography. The key is temporary and it is destroyed at the end of the communication session. Next communication session, a new key Kr will be randomly generated. The data being transferred through the channel during the protocol are Request, user ID, locked code θlock, hash values H(H(Kr)) and H(K′r) . None of the data reveal the biometric information.

7. Conclusion

The proposed algorithm can be illustrated with the practical example application like online secure transaction. It contains two ends namely Server and client which performs full duplex communication between them. With the proposed session key generation protocol mutual authentication can be achieved. With the help of session key generation protocol better security and enhanced operation between server and client using multibiometrics can be achieved.

References

[1] M. R. Ogiela and U. Ogiela, "The use of mathematical linguistic methods in creating secret sharing threshold algorithms", Computers and Mathematics with Applications, vol. 60, no. 2, **(2010)**, pp. 267-271.

[2] M. Drahansky, "Biometric Cryptography Based on Fingerprints : Combination of Biometrics and Cryptography Using Information from Fingerprints", LAP LAMBERT Academic Publishing, **(2010)**.

[3] M. Upmanyu, A. M. Narnboodiri, K. Srinathan and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, **(2010)**, pp. 255-265.

[4] S. Kanade, D. P. Delacretaz and B. Dorizzi, "Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, **(2009)**.

[5] S. Argyropoulos, D. Tzovaras, D. Ioannidis and M. G. Strintzis, "A Channel Coding Approach for Human Authentication From Gait Sequences", IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, **(2009)**, pp. 428– 440.

[6] S. Kanade, D. P. Delacretaz and B. Dorizzi, "A Novel Crypto-Biometric Scheme for Establishing Secure Communication Sessions Between Two Clients", International Conference of the Biometrics Special Interest Group, **(2012)**.

[7] A. Nagar, K. Nandakumar and A. K. Jain, "Multibiometric Cryptosystems Based on Feature- Level Fusion", IEEE Transactions On Information Forensics And Security, vol. 7, no.1, **(2012)**, pp. 256-278.

[8] N. Poh and J. Kittler, "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures", IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 34, no. 1, **(2012)**, pp. 3-17.

[9] R. N. Rodrigues, L. L. Ling and V. Govindaraju, "Robustness of Multimodal Biometric Fusion Methods Against Spoof Attacks", Journal on Visual Language Computation, vol. 20, no. 3, **(2009)**, pp. 169–179.

[10] A. Nagar and A. K. Jain, "On the Security of Non-invertible Fingerprint Template Transforms", Proceedings of IEEE Workshop on Information Forensic sand Security, **(2009)**; London, U.K..

[11] T. Ignatenko and F. M. J. Willems, "Biometric Systems: Privacy and Secrecy Aspects", IEEE Transactions On Information Forensics And Security, vol. 4, no. 4, **(2009)**, pp. 956–973.

[12] W. Scheirer and T. Boult, "Bio-Cryptographic Protocols with Bipartite Bio-Tokens", Proceedings of Biometric Symposium, **(2008)**.

[13] A. B. J. Teoh, K. A. Toh and W. K. Yip, "Discretisation of Biophasor in Cancellable Biometrics", Proceedings of Second International Conference on Biometrics, **(2007)**; Seoul, South Korea.

[14] N. K. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, "Generating Cancelable Fingerprint Templates", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, **(2007)**, pp. 561–572.