Multi-Factor Biometrics: An Overview

Jones Sipho-J Matse

24 November 2014

Contents

Abstract

In today's technological and data intensive world security and privacy have become important issues. Consequently the growth in importance has driven the growth of security and access management technologies. The development uni-factor biometric systems have created a means of identifying or verifying individuals. However, the use of multi-factor biometric systems allows for greater accuracy and reliability in user authentication. In this paper, we discuss multi-factor biometric systems, the different levels of fusion, their advantages, privacy and security issues associated with biometrics.

1 Introduction

There are many issues regarding security and access control. We are always looking for ways to improve the security and access control systems in place. The common forms of authentication such as passwords and ID cards aren't entirely reliable. However, biometrics offer a solution to the increasing threat of unauthorized access to systems and data. Biometrics use physiological and behavioral characteristics to authenticate a person's identity. The advantage of using biometric data is that it is fairly difficult to duplicate or steal. Moreover, the use of multi-factor biometrics employs redundancy at one or steps of the authentication process to ensure greater accuracy and efficiency. This new system allows for compensation for any challenges or issues, which may occur in uni-modal system. As a result, the level of accuracy and reliability is greatly increased due to the existence of multiple "proofs". In addition, there are several methods that can be used to consolidate the systems redundant information; these are referred to as the levels of fusion. This paper concludes that multi-factor biometrics authentication systems are effective tools for security and access control.

1.1 Characteristics of Biometrics

For a physical and/or behavioral feature of the human body to be considered a biometric it must exhibit the following characteristics [11]:

- Universality: Each person accessing the biometric application should possess 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 have 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.

2 Types of Multi-Factor Biometric Systems

Multi-factor biometric systems aim to improve successful recognition rates by introducing redundancy at one or more of the steps in the recognition process. There are five general categories of multi-factor biometric systems [6]:

- Multi-Sample: This is when the system collects multiple images of the same biometric, and then processes them. For example, collecting several facial images from one video session.These systems have the advantage of minimizing sensor equipment costs. Multiple samples allow a higher chance of good quality images with a minimal amount of noise to be used [8]. On the other hand, collecting multiple samples may require multiple sensors which increases costs. Alternatively, it may take time to capture multiple samples and the increase the level of user cooperation which is undesirable.

- Multi-Instance: This system collects multiple instances of the same biometric feature such as samples of each fingerprint or capturing images of both irises. An alternative would be to capture a sample of the same biometric trait with controlled variations during the capture process. For example, facial recognition of a smiling person, and the same person with a neutral expression.

- Multi-sensor: A multi-sensor system is used to capture the same biometric feature with multiple sensors to help address a shortcomings of a specific sensors and obtain a 'cross-sensor consensus'. However, this approach leads to an increase in cost of the system's implementation.

- Multi-Algorithm: This system uses multiple algorithms on the same biometric sample being processed. The results from the algorithm are then compared to

produce a verification result of increased accuracy. This system has the advantage of working on the same sample/samples to curb algorithmic biases. Supportively, this type of system is also cost efficient in relation to sensors. This is an attractive approach in the development of applications and research because it results in lower overall costs [8].

- Multi-modal: This system takes into account more than one biometric feature, or modality in the recognition process. For example, using fingerprints as well as face recognition. The modalities can be considered independent when the outcome of one modality will not predict the outcome of the other [8]. In contrast, modalities are collaborative when they can influence the outcomes of each other however this is a less researched field.

  The ideal multi-modal system would have independent modalities, which are simultaneously captured with the same sensor at high qualities.

These are the five general types of systems, however, it is not uncommon to find combinations of two or more of these system types.

3 Levels of Fusion

Biometric systems go through a series of processes to determine the outcome during verification. There are four general processes within a system: (1) capturing raw data at the signal/sample level of a biometric trait; (2) performing feature extraction which processes the raw data into a compact representation (feature set) of the trait; (3) The process of comparing the extracted features with the data samples that are stored in the database at enrollment and; (4) the decision process which uses the matching scores to determine an identity or validate a claimed identity [8].

Fusion is the combination of redundant information to produce a single output [6]. All the general biometric system processes described above could produce redundant information for the system. In regards to the types of multi-factor biometric systems, potentially, a large amount of redundant information is being generated. We employ a fusion technique to process the redundant information into a single output. The are five categories of fusion techniques [11]:

- Signal-Level: Multiple high quality samples are gathered from a single biometric trait. The high quality samples are then combined for the recognition process. This is done individually for each modality. This happens at the sample capture stage.For the fusion to be executed successfully, it requires the compatibility

calibration of the different sensors and a data registration step before the fusion can be performed.

- Feature-Level: The matching features of each biometric sample is extracted and fused with the other features into a single biometric feature if they are compatible with each other. These features are usually fused through concatenation. However, fusing features can create dimensionality issues. As a result, a feature selection or feature transformation step may be applied. In addition, the same extraction algorithm may be used or a different algorithm can be used on each sample or modality. This is done in the sample analysis stage.

- Score-Level: The inputted samples are compared to the enrolled samples stored in the database to produces a match score. The match scores are obtained independently and are then fused. However, the match score will need to be normalized due to difference in match score ranges. Match score fusion is a relatively easy combination process. This level of fusion is more commonly used with a multi-algorithm systems or multi-sample systems where multiple match scores are produced from each individual sample.

- Decision-Level: The biometric samples are processed to obtain a Boolean outcome to determine if each comparison is a match. The fusion occurs from the Boolean outcomes to make the decision of a valid or invalid sample scan. Many of the approaches used in this level involve the AND or OR rule, majority voting, weighted majority, Bayesian decision, and/or the Dempster-Shafer theory of evidence. Since the decision level is a high level abstraction of the data its use in multimodal biometric systems is less preferred for fusion.

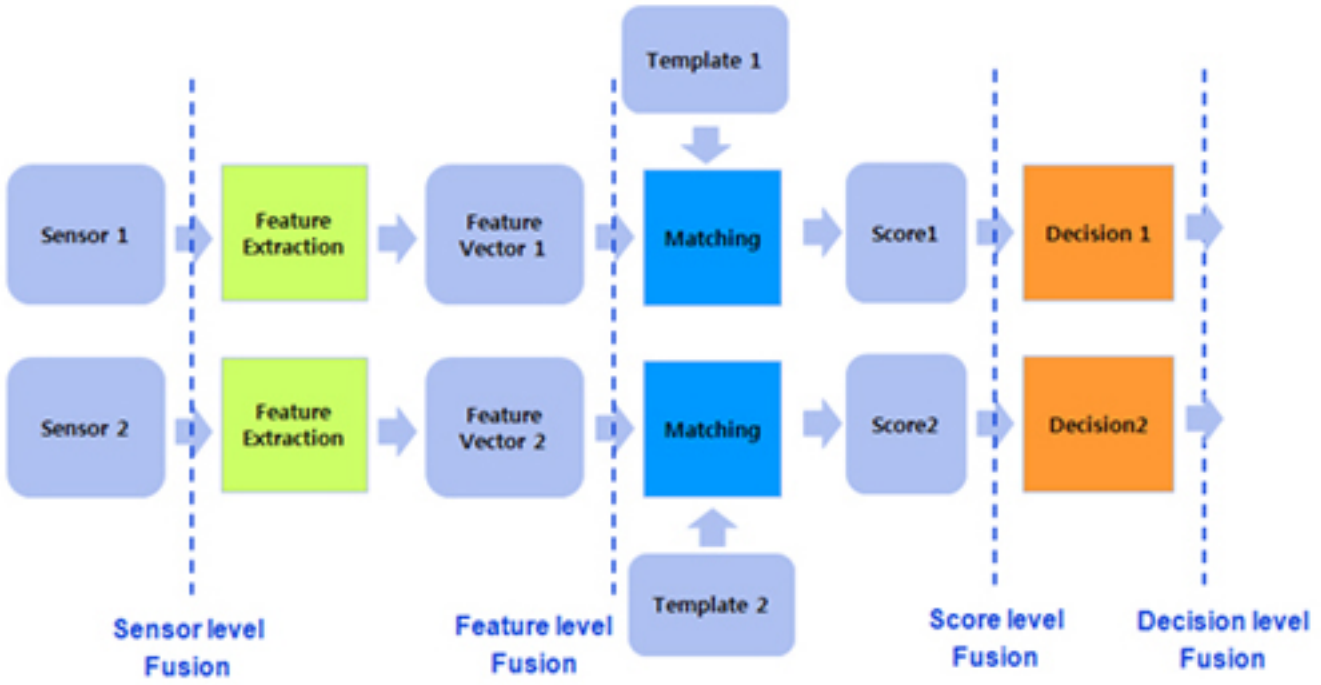

Figure 1: Example of recognition process and where different fusion levels take place.

The amount of information available to perform the fusion process is decreased at each level. Raw data provides the largest amount of data to process for fusion [11]. However, in some multimodal systems, raw data of feature sets may not be available or compatible for fusion. These cases tend to have better fusion capabilities later on in the verification process, usually from the score level up to the decision level.

Score-fusion and feature level fusion are the more common approaches in fusion techniques .The different levels of fusion have advantages however, incorporating fusion techniques early in the recognition process is said to be potentially more efficient than using the fusion process later in the recognition process. On the other hand, score-level fusion is said to be more efficient implementation in relation to the trade-off between the potential performance gain and ease of implementation [1].

4 Advantages of Multi-Factor Biometric Systems

The idea behind multi-factor biometrics is to increase the accuracy and reliability of the biometric authentication process. The advantages depend on the type of multi-factor system in place. However, an advantage of all multi-factor systems is that the probability of the system incorrectly identifying or verifying an unauthorized user (False Accept Rate) is lowered. Similarly, the probability of the system failing to identify or verify an authorized user (False Reject Rate) during verification is lowered

as well [7]. Intra-class variation is when the user interacts with the system incorrectly; this produces inaccurate or incompatible data from the sensor and leads to higher false rejection rates [11]. User interaction with the system cannot be completely controlled so incorrect interaction with the system is bound to occur however multi-factor systems can reduces the effects of the user.

In contrast, people are known to attempt to trick the system and gain access or authorization. These attempts are known as *spoofing*. By introducing multiple biometrics it limits the possibility of successful identity spoofing attempts [5].

Population coverage, also referred to as universality, is described as the number of people able to use the system. Single biometric systems may exclude users with certain disabilities from using the system. However, with multi-factor biometrics population coverage is increased by allowing disabled users to enroll with their valid biometric features [11].

In addition, by employing a multi-factor system, the inability of the sensor to capture good quality data or from the sensor collecting data which does not correspond with samples currently stored in the database due to a users change in biometrics will only partially affect the outcome of the users authentication. This is specifically advantageous to multi-sample, multi-instance, multi-sensor, and multi-modal systems [11].

Intra-class similarities is when two or more people share similar physical traits in a biometric feature, which can lead to false acceptance rates to increase. Multi-factor biometric systems reduce the probability of this scenario [11].

There are three modes of operation which a multi-factor biometric system can employ such as serial mode, parallel mode or hierarchical mode. Serial mode allows the system to collect one trait at a time. This could be used for systems which cannot collect all the biometric data it needs simultaneously. The one trait can be used to narrow down the identities before the next modality or sample is used or potentially make a decision on the identity of a user [8]. Both cases can reduce the recognition time. In parallel mode, information from multiple modalities are used to make a decision. In the hierarchical mode, the biometric traits are combined in a structure similar to decision-trees. This mode is relevant when there are a large number of traits/samples to analyze.

5 Challenges

One of the difficulties in implementing a multi-factor biometric system is selecting the source biometrics to use for the application. Consequently, depending on the biometric data being gathered the cost of the implantation may increase due to sensor costs [11]. These systems can potentially suffer from computational demands as well. On the

other hand, the traits being considered can have a higher performance increase than other combinations [8].

Similarly, depending on the biometric data being gathered the level of invasiveness may increase. In addition, another issue would be considering cultural and gender dimensions, this falls under a biometrics system's universality [11].

The processing architecture of a multi-factor biometric needs to be decided. There is a choice to process the information in sequence or in parallel. This becomes a challenge due to the different types of biometric information being processed. In addition, the processing architecture will also depend on the type of application and how it will be used. Moreover, deciding which level to employ the fusion step becomes a challenge due to effect on performance of the system. Similarly, the cost of developing the system can be influenced by the level of fusion employed. Finding an optimal combination of biometric sources and fusion level is a challenge due to the relatively large number of combinations and techniques available.

Deciding on which level the biometric traits should be fused, furthermore, deciding on the methodology adapted to integrate the information is difficult because there are implementation trade offs between level of invasiveness, cost, computational performance and recognition accuracy [8].

6 Security and Privacy

6.1 Security

Biometric authentication systems can be implemented to perform matching on the client or on the server. The two different matching locations possess individual security issues.

Server matching implementations ideally should be secure and decentralized for security purposes. Usually, the servers store large quantities of information in repositories. The information being stored is a collection of enrolled biometric data of a large population of people. The repositories usually hold important personal information. The issue of having a centralized database of personal information is that it allows for more points of direct access to sensitive information [10]. If these repositories are not properly secured, they are vulnerable to external or internal attacks where information within the database is used outside its intended purpose. For example, an attack may involve altering information in the repository. This is especially true for systems which have implemented a *backdoor* for administrative purposes [3]. However, the backdoor can be exploited to give the hacker easy access to the information. Similarly, for those who may not have biometric information for one or more biometric traits having an exception case allows for another method to exploit the system.

Local matching on the client is a simpler and cheaper to implement. However, it has its own security drawbacks such as replay attacks, non-repudiation, and cryptanalysis. One proposed method to improve local biometric information is to generate a biometric-key using biometric features and a biometric specific key-generator. The challenge lies in developing an algorithm that will produce the same key with varying extracted features produced from the same biometric trait.

6.2 Privacy

Privacy is defined as the ability for a person to live free of all manner of intrusions, remain autonomous and be able to have full control of access to personal information [2]. However, due to the increase in cases of identity fraud and the need to secure various sources of private information many security systems and structures have been constructed to prevent misuse of sensitive information.

Some people believe that collecting biometric information is unethical as it is one of that last pure forms of privacy that a human has. Many people seem to be uncertain as to what their biometric information will be used for once obtained [4].The number one issue of using biometric data as a means of authentication is that biometric data is essentially permanent. If the database of all the biometric enrolled entries were to be compromised the user would be unable to change their biometrics as easily as it would be to change their password.

A biometric system could simply allow users to access a system by matching their biometric trait to those in a sample database that doesn't explicitly specify the user's name. On the other hand, identity recognition has several issues surrounding it. Some biometrics can be seen as culturally unacceptable and others may have negative connotations associated with it due to it prevalence in criminal investigations [2]. There are also reasons to object to biometric systems on the grounds of religious beliefs. In addition, there are issues related to hygiene from biometric sensors that require contact.

There are three systematic privacy concerns: unintended functional scope, unintended application scope, and covert recognition [10]:

1. First, unintended functional scope refers to where a collection of biometric information is gathered and collectors are able to extract additional information by studying patterns in the samples. The most likely case would be inferring medical disorders from the biometric samples which could lead to systematic discrimination against segments of the population.

2. The second, unintentional applications scope, refers to a biometric system having additional uses such as uncovering a persons legal aliases. In addition, the different applications where users have their biometrics enrolled can indicate behav-

ioral patterns of the users by linking the biometrics and the types of applications. Large organizations and governments may use this to gain power over individuals. For example, if a biometric system were to be put in place and linked to other databases with the users personal information it would allow the system to track the user. This allows corporations to track consumers, and the government to track its population.

3. The final systematic concern is covert recognition, this is where a persons information or sample is taken unknowingly from the individual. This allows the culprit to access that users information with relatively low risk. On the other hand, those who wish to stay anonymous in particular situations are denied their privacy because of the use of biometric recognition. These issues will remain until standards are put in place for the use of biometrics. Consequently, people are less likely to share their biometrics in centralized systems and untrustworthy applications that may share data with other applications.

7 Software Project

The goal of my supporting software was to build a multi-factor biometric access control application for android. I am implementing a multi-sample system which takes in fingerprint images as biometric input. I chose to use a multi-sample system as the initial approach for this project because I felt it was one of the simpler approaches.

The application would have an enrollment feature that would process the colored image into a black and white image. The second step would be to store images on the phones internal storage space as its database for the templates. To access their phone the user would take a picture of the finger that would match the previously enrolled finger as an input. That image would also be processed into a black and white image.

I am working under the assumption that the user will be consistent in the size, orientation and position on camera of the image that they take when trying to access the phone. So I am using a simple XOR function and counting the mismatches.

In future implementations of this project I would consider having a multi-instance system in place. Further improvements, would be to implement a more robust algorithm for image matching. Currently, the application's purpose is only to unlock the phone but I would like it to be used as an alternative for accessing other applications which require passwords.

8 Conclusion

The use of multi-factor biometrics provides a great advance in capabilities of access assurance when compared to uni-factor biometric systems. The advantages of each type of multi-factor system and its supporting fusion process should be considered well when developing applications to ensure the system runs as efficiently and as accurately as desired. One the other hand, biometric systems have security and privacy issues associated with them. Determining, how to overcome these issues is one of the larger problems of implementing biometric authentication systems.

References

[1] N. Morizet and J. Gilles, *A New Adaptive Combination Approach to Score Level Fusion for Face and Iris Biometrics Combining Wavelets and Statistical Moments,* in Proceedings of the 4th International Symposium on Advances in Visual Computing, Part II, Berlin, Heidelberg, 2008, pp. 661-671.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, *Biometric Recognition: Security and Privacy Concerns*, IEEE Security and Privacy, vol. 1, no. 2, pp. 33-42, Mar. 2003.

[3] Wayne Penny, *Biometrics: A Double Edged Sword - Security and Privacy,* GSEC Certification Practical - Version 1.3.

[4] J. Roberts and S. Patel, *Biometrics: Does Convenience Outweigh Privacy?*, Convenient or Invasive, p. 62.

[5] Y. Wang, T. Tan, and A. K. Jain, *Combining face and iris biometrics for identity verification*, 2003, pp. 805-813.

[6] R. Connaughton, K. W. Bowyer, and P. J. Flynn, *Fusion of Face and Iris Biometrics*, in Handbook of Iris Recognition, Springer, 2013, pp. 219-237.

[7] L. Hong and A. Jain, *Integrating Faces and Fingerprints for Personal Identification,* IEEE transactions on pattern analysis and machine intelligence, vol. 20, pp. 1295?1307, 1998.

[8] A. Ross and A. Jain, *Multimodal biometrics: An overview* na, 2004.

[9] A. Mishra, *Multimodal Biometrics it is: Need. .*

[10] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, *Privacy Preserving Multi-factor Authentication with Biometrics*, in Proceedings of the Second ACM Workshop on Digital Identity Management, New York, NY, USA, 2006, pp. 63-72.

[11] G. H. Kumar and M. Imran, *Research Avenues in Multimodal Biometrics.*

[12] Suprema - All about Biometrics and Security, *Levels of Fusion. Digital image.*, Web. 9 Dec. 2014.