Integrating Palmprint and Voice Biometric for Identity Identification

Carlos Cabrera, Magno R. Guillen, Malek Adjouadi
Florida International University, Center for Advance Technology and Education, Miami, Fl, USA

ABSTRACT

In today's world it is quite common for anyone to find and use any form of biometric authentication. However, most systems use unimodal biometrics, which only requires the user to submit one form of trait. However, these systems carry several limitations and are proven to show signs of one or more weakness. In this esteem, it is welcome the implementation of multimodal biometrics systems that combine palmprint and voice recognition to overcome the limitations directly related to unimodal systems. Multimodal biometric systems merge information gathered, in this paper a case study using voice and palmprint was analyzed to improve the performance metrics by reducing the false acceptance rate (FAR) and false rejection rate (FRR).

Keywords: Biometrics, Multibiometrics, Security, Palmprint, Voice.

1. INTRODUCTION

Throught its history, the human race has been using biometric charateristics such as voice, facial recognition, gait, etc. to identify each other since the beginning of time. Recent advancement in both hardware and software elicit the development of mechanisms to fulfill the need in the entire world for tighten security. The field of biometrics has becomed regonized has an emerging field of study in the academic/research community. Biometric authentication is based on distinctive and quantifiable elements such as physical, biological or behavioral characteristics that are unique and distinctive of each individual (Chin, et al. 2009).

In the biometric field, the most common systems use a unimodal approach, which in essence only uses one biometric trait from a person, to perform the authentication process. However, the vast majority of unimodal systems have been demonstrated to reveal one too many limitations or weaknesses. Unimodal biometric systems undergo limitations such has the lack of ability to recognize deformed data, distorted signal by environmental noise, not to mention the changeability of an individual's physical appearance and behavior over a period of time. Moreover, the changeability of an individual basically can be classified into two major categories: a) Natural - The normal changes due to aging or b). Cosmetics – The removal or change of any form of biometrical trait by surgical procedure. In this perspective, multimodal biometrics systems are able to resolve some of these limitations by fusing biometric information from multiple biometrical sources.

Human interaction/acceptance with biometrical systems is also of a great concern, since it remains as the greatest obstacle to overcome (Deriche 2008).For years, users have been guarded in regards when submitting any form of biometrical trait. Disregarding ignorance, stigmatism or religious beliefs. Users are apprehensive to two issues: a) Computer Security – where are these traits stored and are they secure, and b) Purpose – what are these traits going to be used for or shared with what agency. Users may rest assured that governments and security agencies do their best in safeguard these traits. However, on one hand one can be apprehensive to provide biometrical traits and on the other hand the same individual can be anxious in submitting a first biometric trait at an early age, in some circumstances as early as 16 years old. This happens when we obtain, for the first time, our drivers license; since a facial image (frontal picture) must be taken, we have just submitted our first facial biometric trait and such will

be stored in the government database for eternity. In retrospective, it is possible to classify human interaction with biometric system in the following two categories:

a) Active or Overt[1]: in cases when the user is active and voluntarily submitting any form of trait. For instance fingerprint, palmprint, iris and retinal traits or b) Passive or Covert[2]: when the user is not aware or is not conscious of a sample being taking, hence the word Covert. Examples of these traits are voice, face and gait.

Global industry for some time now, has taken a huge interest in the biometric field (Group 2010). With the everlasting necessity to protect and safeguard information, industry has engaged with academic and research institutions in the goal to standardized biometric formats and traits. Moreover, revenues in this field are increasing year after year as shown in Figure 1.

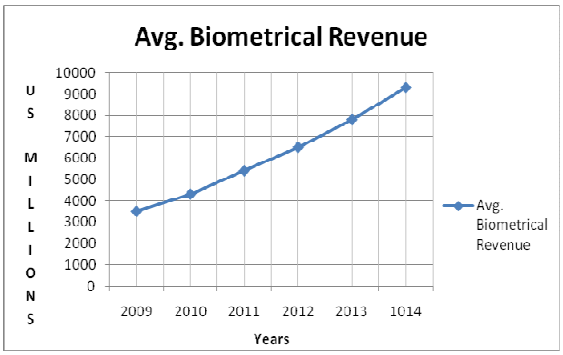

Figure 1: Average Biometrical Revenue as Provided by Biometric Group

2. Proposed Biometric System

A complete biometric system is composed of both hardware and software, each with a unique purpose.
Hardware elements collect the biometric sample while software elements manipulate the traits in order to render a final decision. Figure 2 depicts the proposed multimodal authentication system which consists of four levels as explained as follows:

Level 1: A hardware level that collects the biometric traits, both palmprint and voice.
Level 2: A hardware level that filters both traits independently and uniquely. The purpose is to "filter" elements such has: environmental noise, distortion and image resolution.
Level 3: A software level. This level is unique. First, it is the only level or stage where we find two inputs, one from each trait. Second, it should be held at the highest regard, since it is in this stage where the algorithm that manipulates these two biometric traits takes place. Level 4: A software level that is based on the information handed down from level 3. This algorithm makes a final decision of authenticating providing a binary output of yes or no.

From a security point of view, there are three general ways to authenticate an identity[3]:

1. Something you know
2. Something you have
3. Something you are

As far as the first way, "something you know", it can be stated that it is the most generally used. It is related to anything you need to remember. i.e. a password, PIN[4], pass phrases, etc. The second way, "something you have", refers to a token (Reid 2003). These tokens are classified as: a) Static and b) Dynamic. In static, we store any form

[1] Open to view
[2] Not openly viewed
[3] In most security books this is referred to as, "The Three Pillars of Authentication".
[4] Password Identification Number

of unique identification, for example a smart card or the express card (transducer[5]) in your vehicle that identifies you every time you take the express pass toll on a highway. On the other hand, dynamic tokens are used to create a onetime authentication code. This authentication is completed directly from the dynamic token and the computers security system, many times without user intervention. "Something you are" is the only method used in biometric recognition systems. Biometric systems perform two mayor tasks, a) Identifications and b) Authentication. Identification is a one-to-many matching scheme, because it matches the new obtained trait against each trait stored in the database. Authentication, is a one-to-one matching query, since it queries the database using the newly obtain trait against the one being claimed. This type of authentication is used for physical access control, you present a trait and if it is a match to the trait already present in the database, then access is granted if not, access is denied.

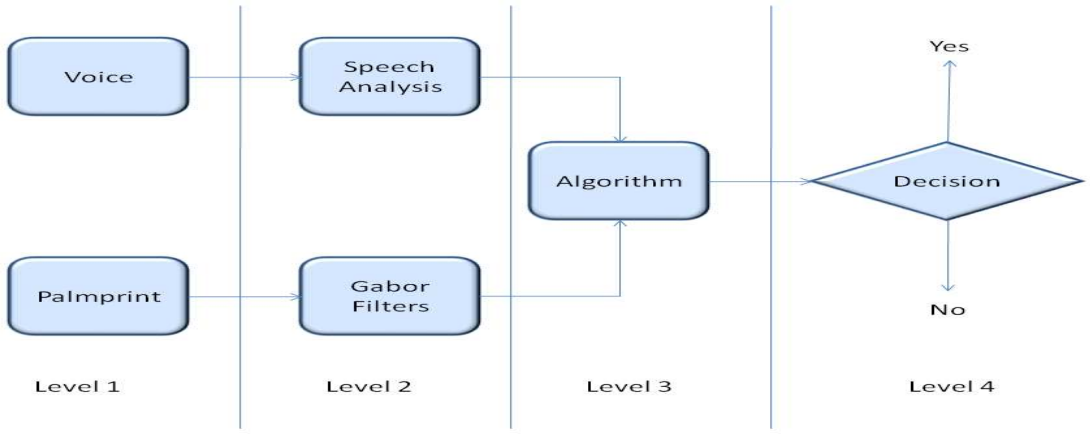

Figure 2: Proposed Multimodal Biometric Authentication System.

Authentication algorithms are of the upmost importance to define the optimal way to manipulate and query the acquired traits. Biometric databases are said to be dynamic, which means that the amount of data stored only gets bigger, and since data (traits) are never erased, therefore how they are stored (manipulated) and queried (searched) is of vital importance.

3. Multibiometric System

As stated earlier, unimodal biometric systems have their limitations, while multibiometrics compensate for such limitations by using two or more biometrical traits. These systems provide more reliability since users are asked to provide more than one biometrical trait, by doing this; the system makes it more difficult for an impostor to provide multiple traits. Multibiometrics systems provide an enhancement in performance and matching precision since they procure minimization of the FAR and FRR.

The main advantages of multibiometrics systems are (Chin et al., 2009):

1. Larger samples traits can be submitted. By submitting your palm print the system has a larger surface area where to obtain information from, compared to the area of the finger print.
2. Multibiometrics systems make it more difficult for an imposter to pose as another individual.
3. Multibiometrics systems are robust, since they can continue to work even lacking one or more biometrical traits.
4. Multibiometrics address issues such as noise, distortion, image resolution, etc.

[5] The term commonly implies use as a sensor/detector

3.1 Voice biometric

The technology used today in voice biometric has been available since the 1960's when Texas Instrument introduced it (Chirillo and Blaul, 2003). Of all forms of biometrics, voice has lead in research in recent years. Moreover, it conveys also one of the greatest challenges, which is to capture a voice sample and be able to complete the authentication process with the presence of noise, distortion, etc. One of the major drawbacks to this system is how to account for the variations in voice during the sampling. Variations in one's voice could be due to the following reasons: illness, fatigue, pitch, surgery involving tampering with the vocal cord, or any combinations of them.

3.2 Palmprint biometrics

This paper introduces a more complex form of use of palmprint biometrics by manipulating the palmprint image.[6] We start from the principal fact that the surface area of the palm is large, therefore instead of using it has an entire image, we treat the palmprint as a matrix of size M x M holding M^2 cells as shown in Figure 3. On taking this approach we have a number of M^2 cell much smaller in size, thus each cell contains the necessary unique information in order to authenticate the user. One of the advantages of this approach is that if one cell is corrupted, for any reason, we still can authenticate the user. Given:

$$M^2\text{-}1, M^2\text{-}2, M^2\text{-}3\ldots\ldots M^2\text{-}n = \sum_{n=0}^{M^2-n}(M^2 - n)$$

where n would be the number of cells used in such case that the cell data is corrupted.

This reasoning provides us with the number of cells available to use in the matrix palmprint.. Moreover, other advantages of this method, is bandwidth saving, since the amount of bandwidth necessary decreases given that the size of each cell, given by $[M^2\text{-}(M^2\text{-}1)]/M^2$, compared to the total size of the palmprint trait is to a great extent much less and by default query response is increase. For instance, if a palmprint is defined as a matrix of 3x3 cells, then each cell is 1/9 of the total matrix. Also, if the image has a resolution of 250KB then each cell would only be 250KB/9 = 27KB in size.

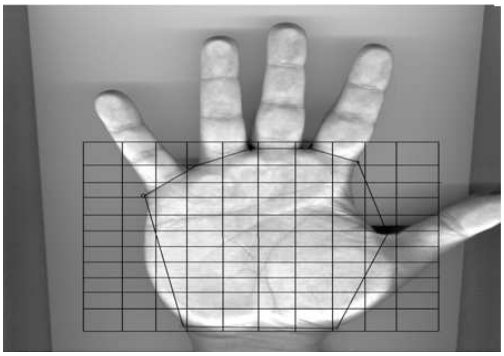

Figure 3: Palmprint Matrix

4. Conclusion

We presented in this paper a comparison between unimodal and multimodal biometrics, with focus on palmprint and voice biometrics. We then proposed a new design for a multimodal authentication system which should reduce the amount of false positive and false rejection rates, key to any biometric system. We are also conscientious that although much has been progressed more research is need, since the need for information, network, computer and personal security increases exponentially every year.

5. Acknowledgment

The author would like to acknowledge the support of Dr. Malek Adjouadi, Director of the Center for Advance Technology and Education, (CATE) at Florida International University, Miami, Florida for the support provided to carry and continue to carry this research.

6. Future Work

The breakthrough we have achieved is just the beginning; we are currently working developing the algorithms to simulate the new system stated. We will extract the statistical results to determine how the system response in worst case scenarios.

References

Chin, Y., T. Ong, et al. (2009). Integrating Palmprint and Fingerprint for Identity Verification. Third International Conference on Network and System Security.

Chirillo, J. and S. Blaul (2003). Implementing biometric security, Hungry Minds, Incorporated.

Deriche, M. (2008). "Trends and Challenges in Mono and Multi Biometrics." Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on: 1-9.

Group, I. B. (2010). " www.biometricgroup.com." Retrieved 2/14/2010, 2009.

Reid, P. (2003). Biometrics and network security, Prentice Hall PTR Upper Saddle River, NJ, USA.

Authorization and Disclaimer