Chapter 1

PCG-Based Biometrics

Takhellambam Gautam Meitei
NERIST, India

Sinam Ajitkumar Singh
NERIST, India

Swanirbhar Majumder
Tripura University, India

ABSTRACT

These days the wide usage of data has opened security vulnerabilities everywhere. This has led to research in the biometrics area for improving security. Presently with wide development of technology different forms of biometrics are being used in various applications. Thus, fingerprint and face are no longer the only ones being used in this field. The authors have concentrated on PCG as a biometric in this chapter. A very few sources are available in this area deeming it to be nascent. Recent proposals were examined, and it was observed that PCG reduces the risks of vulnerability faced by other biometric system. A simple biometric system would consist of steps like preprocessing, segmentation, feature extraction, and comparison or matching phase. In this chapter, some pre-processing steps as implemented by various authors using wavelets and other feature extraction techniques, implemented for the PCG biometric system by various researchers, are reviewed. Later, in the matching phase, Euclidean distance, GMM, FSR, VQ method are examined.

INTRODUCTION

Latest advancements in technologies have driven us for the need of a secure identification of a particular person for security purposes. Various frauds and cybercrimes have led us to look out for a secure identification purpose. Previously people used passwords (something uniquely known only to us) or a token (proving we own something unique to identify ourselves). The chances of a password or a token getting stolen or shared are high, so Biometrics was introduced to reduce the vulnerabilities.

DOI: 10.4018/978-1-5225-5152-2.ch001
Biometrics plays an important role in securing our identity. It can be understood as a process or the ability of a system to identify a particular person based on some unique biological features or patterns such as fingerprints, facial recognition, DNAs, voice, eye-iris and retina, palm prints, signatures, etc. The data obtained are compared to a previously stored reference data or templates, and determines if the newly generated data could have been generated by the same person. So, a biometric authentication comprises of two phases, Enrollment phase and Authentication phase. In enrollment phase, as shown below in figure 1(a), a set of databases is created by capturing the patterns or features that provides information about each individual. In the authentication phase, the newly captured feature searches the template for a match. Biometric authentication runs in two modes, depending upon the application used, i.e., identification and verification modes.

1. **Identification Mode:** It takes in information about the unique traits of a user, i.e. it captures the biometric information and searches the whole database for a match, to the captured information. Here, the classification module is trained previously with various sets of extracted features. The features of the input data from the user is then compared with the extracted features stored while training. The general block diagram of identification mode is shown below, Figure 1(b). After classification, the biometric system decides as to whose features does the input sample matches to.

2. **Verification Mode:** This is similar to the identification mode, except for the classifier used. The identification mode classifier uses a 1:N classifier, while the classifier used here is 1:1 classifier. i.e. it is basically a yes or no decision. The system compares the captured data with previously stored information about the same individual and authenticates the particular individual. The block diagram for verification mode is shown below, Figure 1(c).

Pre-processing steps are employed here to minimize noise, making it ready for a better segmentation of the PCG signal, which will provide clear features in the feature extraction process. The extracted features will be stored in a database in the enrollment phase. During authentication, after the pre-processing steps, the feature extraction stage gives the unique information of an individual and finally in the classification stage, the data is compared to the previously stored information in the template, as shown in the block diagrams in Figure 1.

The biometrics mentioned above is without any doubt better than the methods used previously (passwords and tokens), but they all share a common problem of being duplicated. For example, the authors in (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002) proved that fingerprints can be duplicated. About 65-100% accuracy rate was achieved by using gummy fingers on 11 different commercial fingerprint systems. Facial recognition has also been studied to be easy to spoof using 3D printed face models. Voice can be recorded without the consent of the person. Signatures can be copied and duplicated, in fact, there are professional people who can copy and provide exact signatures. DNAs are easy to acquire. With all the advancement in technologies, there is always someone or something that will provide a weakness over a system. So, we look for an alternative, where the problems faced above are minimum. PCG (Phonocardiogram) is one of the emerging techniques that uses the heart sound and has a particular set of features, that can help overcome or reduce the problems faced above. The first use of heart sound as a biometric was introduced by (Beritelli & Serrano, 2007).
Related Content

A Comprehensive Literature Review on Construction Project Risk Analysis
[www.igi-global.com/article/a-comprehensive-literature-review-on-construction-project-risk-analysis/165969?camid=4v1a](www.igi-global.com/article/a-comprehensive-literature-review-on-construction-project-risk-analysis/165969?camid=4v1a)

Spam Classification Based on E-Mail Path Analysis
[www.igi-global.com/article/spam-classification-based-mail-path/2481?camid=4v1a](www.igi-global.com/article/spam-classification-based-mail-path/2481?camid=4v1a)

Risk Factors to Retrieve Anomaly Intrusion Information and Profile User Behavior
[www.igi-global.com/chapter/risk-factors-retrieve-anomaly-intrusion/23229?camid=4v1a](www.igi-global.com/chapter/risk-factors-retrieve-anomaly-intrusion/23229?camid=4v1a)

Trustworthy Web Services: An Experience-Based Model for Trustworthiness Evaluation
[www.igi-global.com/article/trustworthy-web-services/2453?camid=4v1a](www.igi-global.com/article/trustworthy-web-services/2453?camid=4v1a)