**Personalized Mobile eHealth Services for Secure User Access Through a Multi Feature Biometric Framework**

Georgios C. Manikis, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece
Marios Spanakis, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece
Emmanouil G. Spanakis, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece

**ABSTRACT**

Humans have various features that differentiates one person from another which can be used to identify an individual for security purposes. These biometrics can authenticate or verify a person’s identity and can be sorted in two classes, physiological and behavioural. In this article, the authors present their results of experimentation on publicly available facial images and the efficiency of a prototype version of SpeechX Rays, a multi-modal biometric system that uses audio-visual characteristics for user authentication in eHealth platforms. Using the privacy and security mechanism provided, based on audio and video biometrics, medical personnel are able to be verified and subsequently identified for two different eHealth applications. These verified persons are then able to access control, identification, workforce management or patient record storage. In this work, the authors argue how a biometric identification system can greatly benefit healthcare, due to the increased accuracy of identification procedures.

**KEYWORDS**

Biometrics, Decision Threshold, DET, eHealth, Equal Error Rate (EER), mHealth, Personal Health Systems

**INTRODUCTION**

Biometric authentication is the process of verification of a person’s identity using a physical trait or a behavioural characteristic in order to accept the identity of the person and verify him/her as an authorized user (Jain et al., 2007; Li & Jain, 2009). From the technical perspective, biometric systems mainly rely on models derived from pattern recognition, where several characteristics from a person (e.g. voice, facial expression, fingerprint, etc.) are first transformed into a feature vector and then processed to deny or reject the verification and identification of a user. A major prerequisite in this process is the so-called training phase of the model composed of a pipeline in which: (i) captured biometric characteristics from specific users are stored in a database, and (ii) used for training the model based on that known content. Once training is performed accurately, the biometric system can be applied for verification and identification.

Verification process addresses biometric authentication of a specific user who claims an identity and desires to be recognized by the system (i.e. John Doe uses his magnetic ID card and his fingerprints, and requests access to building A). The system performs a one-to-one comparison between the biometrics of the user requesting access and his/ her corresponding characteristics retrieved from the
database. A pattern recognition model estimates the level of similarity or matching score between the characteristics and allows access, in case this similarity metric shows a value above a predefined level of security. User identification is a more computationally complex process in which the biometric system searches all the available information stored in the database when a user requests access without providing any credentials. The system is responsible for answering questions such as “who is this person?”, “is he-she enrolled in the database?” and conducts a one-to-many comparison to verify that the user is registered to the security protocol and has been granted access to the requested entrance. Biometric recognition systems extract the features from voice, face and compare them with templates stored in databases for verification of a person. If the system uses only a single trait it is characterized as a unimodal biometric system, whereas if two or more biometric traits are used to identify and authenticate a person, the system is called multi-modal (Larcher et al., 2012; Ross et al., 2006).

SpeechXRays biometric system is designed in order to develop and test in real-life environments a user recognition platform based on voice acoustics analysis and audio-visual identity verification (http://www.speechxrays.eu/). SpeechXRays provide a state-of-the-art, high accuracy and user-friendly solution allowing storage and analysis of biometric data for authentication. The system aims to apply in eHealth in order to authenticate users and provide different level of access to medical personnel, based on their rank in patient management (Spanakis et al., 2016; Chronaki et al., 2003; Kartakis et al., 2012). Security issues for eHealth system (Hristoskova et al., 2014; Spat et al., 2011) are usually centred on user authentication, data integrity, data confidentiality, and patient privacy protection. With SpeechXRays we aim to study how to address these by providing reliable and secure user authentication, compared to the traditional approaches. The eHealth pilot for SpeechXRays involves one hospital and all corresponding wards/clinics aiming to enrol >400 medical users. In the context of the pilot study, the medical personnel will use the SpeechXRays in order to be authenticated as users of a medical application (OAcare). The OAcare application is a dynamic web application developed for patients and clinicians for the management of osteoarthritis (OA) (Maniadi et al., 2015). Recently an evaluation survey and preliminary results regarding functionality, efficiency and user-friendly environment were presented along with the acceptance of using the biometric system proposed from SpeechXRays for user authentication (Spanakis et al., 2016). On the other hand, in order the biometric system to be applied in a clinical environment it is essential to evaluate its performance regarding successful authentication of the user. The aim of this work is to present a methodological multi-feature biometric framework based on machine learning and feature selection techniques, addressing the needs of SpeechXRays. The proposed approach is a prototype and for feasibility reasons, currently is dealing with multi-feature extractions of facial characteristics due to larger variability that is observed in voice analysis (Cociocoeanu et al., 2016a; Cociocoeanu et al., 2016b). The biometric system is flexible in terms of adjusted decision thresholds that must be defined and adapted, based on the level of security and confidentiality of the medical data that the user attempts to access.

BIOMETRIC SYSTEM ERRORS

A biometric verification system usually makes two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person, and (ii) mistaking two biometric measurements from the same person to be from two different persons (Jain et al., 2004).

Errors of the first type are measured using FMR (false match rate) or FAR (false acceptance rate), whereas FNMR (false non-match rate) or FRR (false rejection rate) are frequently used to quantify errors of the second type.

There is a trade-off between FMR and FNMR in every biometric system. In fact, both FMR and FNMR are functions of the system threshold $t$; if $t$ is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if $t$ is raised to make the system more secure, then FNMR increases accordingly. The threshold at which FMR is equal to FNMR is
Feasibility of Hospital-at-Home for Older Patients With an Acute Medical Illness
www.igi-global.com/article/feasibility-of-hospital-at-home-for-older-patients-with-an-acute-medical-illness/214994?camid=4v1a

Achieving E-Health Success: The Key Role for ANT
www.igi-global.com/chapter/achieving-e-health-success/192692?camid=4v1a

Implementing RFID Technology in Hospital Environments
www.igi-global.com/chapter/implementing-rfid-technology-hospital-environments/13003?camid=4v1a