Biometric Paradigm Using Visual Evoked Potential

Cota Navin Gupta
University of Essex, UK

Ramaswamy Palaniappan
University of Essex, UK

INTRODUCTION

Recognizing humans based upon one's intrinsic physical or behavioral traits has been gaining acceptance and is termed as biometrics. It involves either confirmation or denial of the identity that the user is claiming. It is especially important in ensuring security for access to highly restricted areas (for example: accessing classified documents, control gates and defence related applications). This chapter will discuss the use of brain signals at an application level exploiting the evoked potential approach for biometrics.

BAKGROUND

The most primitive and widely used authentication method to establish a person's identity is the textual password and usage of personal identification number (PIN) which are motivated by the facts of popularity due to low cost and user familiarity.

However these schemes have obvious shortcomings in the form of dictionary attack, shoulder surfing and people picking up obvious known words which can be easily cracked. Dictionary attacks can be prevented by using human-in-loop verifications (Pinkas & Sander, 2002) and encrypted key exchange methods (Bellovin & Merritt, 1992), but operating system vulnerabilities and access control failures may lead to disclosure of password databases. The use of PIN actually denotes the automatic identification of the PIN, not necessarily identification of the person who has provided it. The same applies with card and tokens, which could be presented by anyone who successfully steals the card or token. The system and information is definitely vulnerable during the period before a user's card or token is revoked. Even the recently proposed graphical password which is motivated by the fact that people have a remarkable memory for pictures seem to share similar problems along with the shortcomings of guessing attacks (Thorpe & Van Orschot, 2004) and reduced effective password space. The ominous presence of mobile phone cameras, digital cameras, and wireless video cameras brings in a new threat in the form of "recorded shoulder surfing" for high security applications.

Hence biometric technology based on measurable physiological and/or behavioral characteristics (e.g., fingerprints, Roddy & Stosz, 1996, the iris, Daugman, 2004, and voice recognition, Monrose, Reiter, Li & Wetzel, 2001) is often considered to surpass conventional automatic identity measures like passwords and PIN by offering positive human identification.

Fingerprint biometric systems have found its way in many public person identity databases (Maltoni, Maio, Jain & Prabhakar, 2003), but they do not seem suitable for high security environments. Recent articles and studies (BBC, 2007a; Matsumoto, Matsumoto, Yamada & Hoshino, 2002) show that common household articles (e.g., gelatine) can be used to make artificial fingers and prints to bypass the security systems. Also development of scars and cuts can result in erroneous fingerprint matching results thus increasing false rejects. Voice recognition as a biometric seems to suffer from several limitations. Different people can have similar voices and it may also change over time because of health, emotional state and age. Face recognition has been used as a biometric system but issues like the family resemblance, occurrence of identical twins (one in every 10,000) seem to question the reliability. A recent article shows that face recognition systems can be bypassed by using still and video images of a person (BBC, 2007b). Also it is inherently unreliable where high security is needed because there is not nearly enough randomness in the visual appearance of people's faces and also small variations in pose angle, illumination geometry, and facial expression have disastrous effects on the authentication algorithm accuracy (BBC, 2007b).

Another issue facing many of the biometric systems is the factor that biometric data (e.g., fingerprints or iris scans) have information which is valid and unchangeable for lifetime of the user and is irreplaceable if stolen. However it is a known fact that no biometric is expected to effectively meet the requirements for all applications. The choice of a specific biometric completely depends on the requirements of the application domain.

The above discussion on the existing biometric technologies definitely highlights the shortcomings for high security

environments and reiterates the need for an authentication system which has the following characteristics (Thorpe, Van Oorschot & Somayaji, 2005):

- ***a.*** *Changeability*: The ability to replace authentication information.
- ***b.*** *Privacy (theft protection)*: A biometric which is fraud resistant and does not use a template for lifetime.
- ***c.*** *Shoulder surfing*: System should be immune to all forms of shoulder surfing.
- ***d.*** *Universality*: Every person should have the considered characteristics.
- ***e.*** *Permanence (stability)*: Characteristic should be invariant and stable over a period of time.

A biometric system using brain's electrical response patterns with the evoked potential approach seems to have the potential to satisfy all of these requirements. Applications for this biometric system include high security systems (access to classified documents, defence applications) where fingerprints and other identity measures like passwords could be easily forged. It could also be used as a modality within a multimodal biometric environment. The advantage of using such brain electrical activity as biometric is its fraud resistance, that is someone else cannot duplicate the recorded brain response, and is hence unlikely to be forged or stolen. This modality has the additional advantage of confidentiality ("all forms of shoulder surfing' is impossible"), as brain activity is not easily seen. An added impetus for this sort of approach is the recent report in Newscientist (2007) about an initial study on the possibility of developing an electronic security system that will identify people by monitoring the brain activity.

BIOMETRIC SYSTEM USING BRAIN SIGNALS

In general, data for brain biometric system are collected using an electrode cap worn by the person (also known as subject). The electrodes are connected to the holder as shown and the brain signals are recorded in response to the activity on the computer screen. Electrode gel is used at the point of contact while fixing the electrodes to the electrode cap for improving conductance of brain potentials. There are also interfacing cables which interface the computer and the electroencephalogram (EEG) equipment to record the responses to the ongoing paradigm. The electrode configurations commonly used are the 32, 64, and 128. A number of trials of the same paradigm are usually performed during the course of the experiment and averaging taken to reduce artifacts (i.e., noise).

Given the risks with invasive implanted devices in brain and the associated ethical concerns, non invasive approaches (in particular those using EEG) seems to be more popular. EEG which is the recording of the brain's electrical activity is the de facto standard in diagnosis of brain related diseases, however recently there has been a spurt of activity in the studies on brain biometrics (Marcel and Millan, 2007; Palaniappan & Mandic, 2007; Palaniappan & Ravi, 2006; Palaniappan & Raveendran, 2002). Some early work on EEG based biometrics include the use of autoregressive (AR) models of various orders computed from EEG signals recorded from subjects with eyes open and eyes closed (Paranjape, Mahovsky, Benedicenti & Koles, 2001). A linear discriminant analysis was employed to classify the 40 subjects which gave an accuracy of 80 percent. Learning Vector Quantizer network (LVQ) was used to classify AR parameters from four subjects describing the alpha rhythm EEG feature, where the classification performance of 72-84 percent was obtained (Poulos, Rangoussi, Chrissikopoulos & Evangelou, 1999a). In a similar related study using the same data set but a different classification technique based on computational geometry gave a much improved average classification of 95% (Poulos, Rangoussi, Chrissikopoulos & Evangelou, 1999b).

More recently a statistical framework based on Gaussian mixture models and maximum a posteriori model adaptation (Marcel & Millan, 2007) was used for person authentication. The study also highlighted that certain mental tasks are more appropriate for authentication. However, many of these studies were conducted for a relatively small number of subjects.

BIOMETRIC SYSTEM USING THE EVOKED POTENTIAL APPROACH

Evoked potential is a type of EEG that is evoked in response to a stimulus, which could be visual, auditory or somatosensory. Visual evoked potential (VEP) is the evoked response to visual stimulus. In a recent study (Palaniappan & Mandic, 2007), multiple signal classification (MUSIC) algorithm was used to extract features in the gamma band of VEP based experiment study and gave enhanced person recognition of over 96% with 102 subjects. Other systems have exploited the P300 component of VEP as a medium of communication (Donchin, Spencer & Wijesinghe, 2000; Farwell & Donchin, 1988), which could be adapted from biometrics. P300 is an endogenous component of the VEP, which is most frequently elicited within the framework of an "oddball paradigm". P300 based systems are promising and motivating as they require no or very less training. It is known for its simplicity, ease of use and low error rates (Kaper, Meinicke, Grossekathoefer, Lingner & Ritter, 2004; Serby, Tov & Inbar, 2005,).

In the oddball experiment the subject is asked to distinguish between two stimuli, one common and one rare, by