Chapter XXXIX
Bio-Cyber Machine Gun:
A New Mode of Authentication Access Using Visual Evoked Potentials

Andrews Samraj
Multimedia University, Malaysia

ABSTRACT

The bio-cyber machine gun (BCMG) is a defensive tool used to protect misuse of authentication, access control, and aid cryptography and information hiding by means of password shooting. BCMG is developed to be a ray of hope for the disabled community who live in the dark expanses of life, by providing all possible technical support to the disabled by increasing their ability by means of creating innovative software and hardware that helps them to live independently in a stress free environment and to enjoy the desired choice, control and freedom as others. The brain wave P300 component is used for this purpose. This chapter describes that how the P300 components are created, identified, extracted, and classified for the use in the BCMG.

INTRODUCTION

The *bio-cyber nachine gun* (BCMG) is a defensive tool used to protect misuse of *authentication*, and access control. It also aids cryptography and information hiding by means of biological password shooting. Use of biometrics as a tool for authentication is a popular means nowadays (Pankanti, 2001). Among various types of *biometrics* like fingerprints, palm prints, iris recognition, face recognition, voice recognition, and others using bio-signals for authentication purposes is novel and unique. The need for this tool amidst various existing authentication protection methods is to have an easy, cost effective, and reliable way. The conventional password, pin number, smart card, barcodes or biometric fingerprints, palm prints, iris pattern, and face recognition are only used for a specific purpose of authentication or access control on a one time basis. The amount of information we can pass through these methods is also very limited. The ever-growing demand for integration of services and higher level security needs, calls for an efficient and reliable

system, which can do multiple tasks in a highly secured way. This kind of sensitive and complex system can be made effective and robust, but at the same time be simple to implement, when we use them from a very close mode like biometrics of a person. This has to be carried out exclusive of the major drawbacks of biometrics. More over this may be the only possible authentication and access control method for patients, the elderly, and the disabled who may not be able to adapt to conventional methods.

BACKGROUND

Biometrics is a technique which uses the unique features of the human body as an identification tool to recognize a person. The biometrics function works on a simple principle that everyone in the world is unique, and this inherent uniqueness can be used for identity verification. The face is a good example of what helps to identify each individual. Along with the face, height, skin, voice, and hair styles are also useful. Similarly the centuries old method of using fingerprints to identify people is still being used as a signature as well as in forensic science (Pankanti, 2001). The major disadvantage of using biometrics is that it is extremely sensitive. The biometric components are complex starting from access, deployment, and securing them for further use. It is prone to misuse if stolen and needs complex retrieval methods and expensive devises. In addition it involves ethical issues. Cancelable biometrics solves this problem to a certain extent (Vaughan, Wolpaw, & Donchin, 1996) and it still needs to be improved in terms of flexibility and reliance. The proposed method of using bio-signals for this purpose solves the problem innovatively and simply. The human body generates many kinds of signals known as, in general, bio-signals, which include signals from the heart beat (ECG), from the brain (EEG) and others. Using EEG signals for communication is an emerging technology in the rehabilitation field (Vaughan et al., 1996). Most of the bio-signals are independent from human activities and they are automatic, so these signals cannot be composed to a fixed rhythm by others. On the other hand, some of the signals generated by muscle activities can be controlled by the person and can be made rhythmical. But the generation of these signals are not secured and protected. The *visual evoked potential* (VEP) signals for this purpose are found to be feasible and appropriate for sensitive multipurpose security systems since it is securely produced and can be made rhythmic.

The VEP that is generated using an oddball paradigm that gives a visual stimulus (Andrews, Palaniappan, & Kamel, 2005) normally buried in the ongoing background EEG. We can divert the function of the oddball paradigm and the signals produced can be made rhythmic to symbolize a particular meaning. It is faster than the mental prosthesis method (Donchin, Spencer, & Wijesinghe, 2000) used to generate brain activity signals. A conventional light machine gun (LMG) can fire at the rate of 300 to 500 rounds per minute in its rapid-fire mode (R) using a belt supply. We use this model of rapid-fire mode to randomly activate the paradigm to evoke the VEP from brain to coin the currently required password at any moment. So we could call this a brain computer machine gun.

METHODS AND BENEFITS

This BCMG tool that we designed for this purpose uses two major components, one is the signal capture unit and the second is an interface unit. Using the first unit the raw EEG recordings are taken from the scalp as shown in Figure 3. These signals are always contaminated with noise and artifacts which will be eliminated by filtering (Andrews, Kamel, & Palaniappan, 2005; Kriss, 1993).

The state of the art, cutting edge technology that BCMG utilizes is the simplest physiological behavior activity of viewing the paradigm that evokes brain potentials. Using the electrodes fixed on the parietal area of the scalp (Kriss, 1993) EEG signals for one second immediately after the visual stimulus is recorded. Using the interface unit, these recordings are band pass filtered to remove artifacts (Andrews et al., 2005; Kriss, 1993), using a low pass filter with the