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

Figure 1. Donchin's stimulus matrix viewed by the subject (Donchin et al, 2000)

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	space

performing a mental count of one of the stimuli. In response to mentally counting the appearance of the rare stimulus, a typical potential is evoked in the brain. At any given moment the user selects (say a color or symbol) that the user wishes to communicate, and maintains a mental count of the number of times it is intensified. In response to this counting, a potential is elicited in the brain each time the color or symbol is flashed and the response is known as a P300 wave (Sutton et al, 1965). The P300 based Donchin paradigm (Farwell and Donchin, 1988) enabled communication of the alphabets and few symbols using the P300 component of the VEP. The 26 characters and symbols were displayed on the computer as shown below in Figure 1. The subject focuses successively on the character that the subject wishes to communicate. The computer detects the character focused by the subject because of the alternate repeated flashing of the columns and rows. When a column or row containing the chosen character is flashed, a P300 is evoked and would be detected by the computer.

A preliminary study on "Inblock" and "Outofblock" P300 oddball experiment

In this preliminary study, we wished to investigate the effects of presenting the oddball stimulus in "Inblock" and "Outofblock" fashion (as illustrated in Figure 2). The Donchin's paradigm (Donchin et al., 2000) is based on the Outofblock' fashion but here we show that the Inblock fashion would be more suitable to evoke P300 using the oddball paradigm for biometric applications.

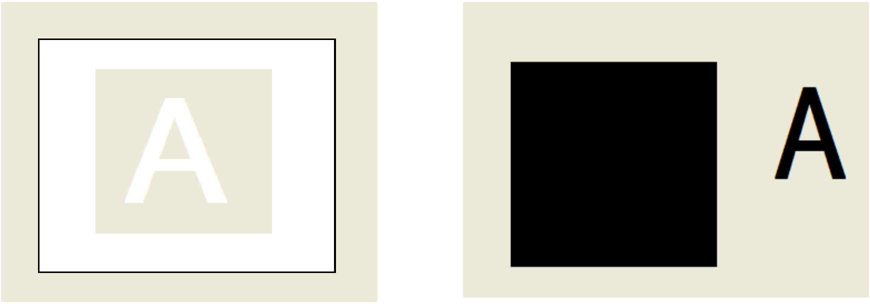
We recorded EEG data from a male subject aged 27 with no known neurological disorders. A very simple form of visual stimulus presentation was used here where the subject was asked to concentrate on the letter "A". The letter Awas flashed 30% of the time while the square block was flashed for the rest 70% of the time. It is assumed that the infrequent stimuli (i.e., when the subject concentrates on the letter A) will evoke a P300 component.

The flashes were intensified for 100 ms, with an interstimulus interval (ISI) of 300 ms. During the ISI, there would be no intensifications. The ISI is defined as the end of the intensification to the start of the next intensification. The period of 300 ms was chosen after some preliminary simulations.

The sampling frequency was 256 Hz and EEG data was recorded from 64 channels using Bio-semi system. EEG data was recorded for every intensification (i.e., flash of the "block" or letter A). First, averages of left and right mastoid channels were used to re-reference the data. To extract P300 component, each EEG signal was low pass filtered to 8 Hz using a fourth order Elliptic Infinite Impulse Response filter (with forward and reverse filtering to avoid phase distortion) and then normalised to zero mean and standard deviation of one. The cut-off frequency of 8 Hz was chosen after some preliminary simulations.

Next, P300 amplitude was computed as the most positive peak in the range of 300-600 ms (or 77-154 sampling points) after stimulus onset. The above trials for the Inblock

Figure 2. Visual stimulus for Donchin's paradigm: (a) Inblock and (b) OutofBlock



(a) Inblock stimulus

(b) OutofBlock stimulus

Figure 3. Averaged EEG signal for Inblock case

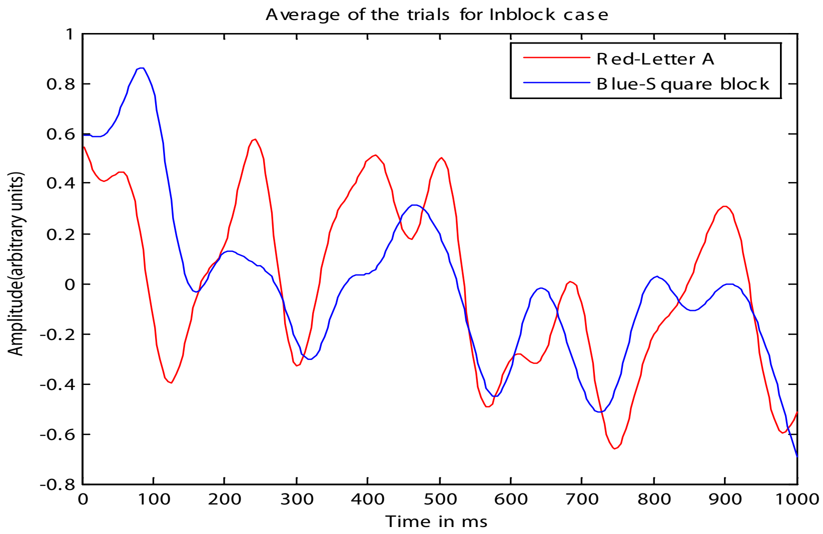
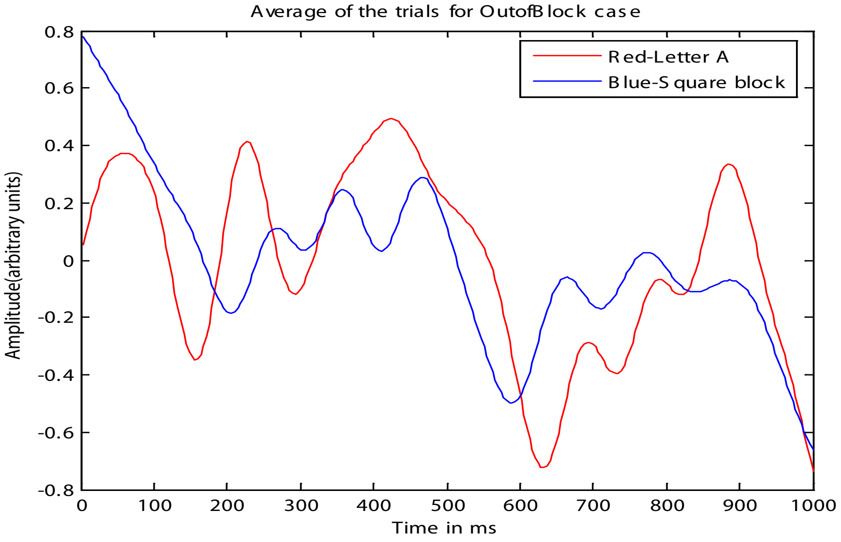


Figure 4. Averaged EEG signal for Outofblock case



and OutofBlock cases were averaged to reduce noise and are as shown below in Figures 3 and 4 where red indicates the EEG data when the letter A was flashed which has the P300 component (because the subject concentrated on the letter) and blue when the square block was flashed. The analysis was done for the channel Cz which is known to have maximal P300 component.

It could be seen that the signal component for the target letter A case has higher amplitude in the region of 300-600 ms rather than the square block. This is in line with the results expected from oddball paradigm. But the more important observation is the fact that the P300 peak is more easily distinguishable using the Inblock rather than Outofblock fashion. Therefore, in future experiments, we could use Inblock type of fashion for evoking P300 components using oddball paradigm.

Color "Blocks" Visual Stimuli

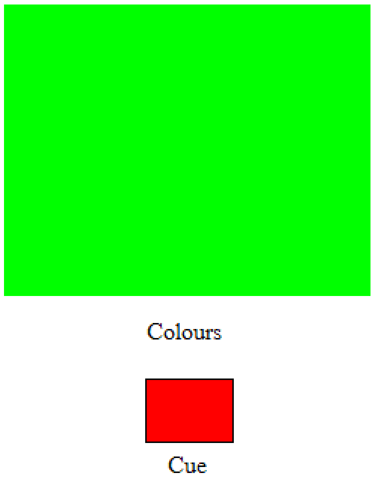
To make the concept of using brain biometrics universal across all boundaries (i.e., to avoid language differences), we are currently investigating the possibility of using colors (or universal symbols) instead of English alphabets as in Donchin's paradigm.

This proposed system, which is still in early stages of research, will authenticate users using their brain signals in response to a sequence of on-screen color stimuli as well as audio signals. So at any time, the system's focus for the biometric application is to differentiate the colors on screen rather than the individuals. The EEG data will be recorded when the subject perceives different color flashes on white background within a single square block (i.e., Inblock case). The basic colors: black, red, green and blue were decided because of the contrasting difference which will easily evoke the P300 potential. The cue on which the subject has to concentrate will also be presented below this block as shown in the Figure 5.

The subject will be instructed to focus on colors that randomly flash on screen. The objective would be to form a color coded pass code generated by thought alone, which could be used to authenticate the identity of a person. For example, a passcode could be RED, BLACK, BLUE, GREEN (sequence is important as it determines the passcode). Each color would flash in random order until all colors have flashed; this is known as randomized block intensification. Each randomised block intensification of four colors will be considered as a trial. Currently, we are investigating various other novel visual stimulus paradigms (for example, using picture instead of colors) to decide the suitable stimulus for biometric applications.

This may be extended to various scenarios like words, graphical images or music to form a sequence in the form of a password. The advantage of using such brain electrical activity as biometric is its fraud resistance, that is the brain response cannot be duplicated by someone else, and is hence unlikely to be forged or stolen. The only disadvantage of the system lies in the cumbersome data collection procedure but improvements in data collection procedures (such as dry electrodes, instead of wet) will reduce the unwieldiness. However the fraud resistance significantly outweighs this difficulty especially for high security applications.

Figure 5. Color visual stimulus under investigation for brain biometrics



FUTURE TREND

The field of crossmodal perception refers to different sensory modalities (say audio and visual) and is being increasingly studied to gain better understanding of the long-term properties of the brain. Matched sensory inputs (such as the sight and sound of a cat) enhance our perception. Studies have shown that performance improvements can be achieved on low-level visual perceptual tasks with practice but is difficult as well as slow and requires many days of training (Adini, Sagi & Tsodyks, 2002; Poggio, Fahle & Edelman, 1992). In the study by Seitz et al (2006), a multisensory audiovisual training procedure facilitated faster visual learning than unisensory visual training. In this biometric application, the remembrance of password may be considered as a recall from episodic memory, which is a subset of declarative memory because it is related to storage of facts and can be discussed or declared. Declarative memory is subject to forgetting, but if accessed frequently they can last indefinitely (Tulving & Schacter, 1990). Since it is known that matched sensory inputs enhance our perception, it would be worthwhile to investigate and compare evoking the declarative memory (i.e. password) by one of the three protocols: visual stimulus, audio stimulus and visual combined with audio stimuli.

CONCLUSION

Although much work has been done in the past decade using brain signals for clinical analysis, the application of brain signals for biometric purpose is relatively new. It is also known that in a P300-based biometric system, the communication speed of characters is dependent on the number of trials. We are working on developing new framework at an algorithm level which we foresee will use less number of trials (Gupta & Palaniappan, 2007). It is anticipated that much of the work in future will concentrate on developing a really robust and user-friendly system where the number of trials used will be minimum (i.e., to obtain a higher bit rate). It is envisaged that the future work and technological advancements will move this concept from research into a practical working system. No doubt, one of the main constraints is the long set-up time. However, with steady research progress in signal processing, we should be able to use only a few channels that will still give accurate authentication. Then, a simple headband with electrodes attached could be used instead and set-up time would only be on the order of seconds.

Concluding, a biometric authentication system using brain's electrical response patterns using the evoked potential approach has the potential to satisfy all of the requirements for a high security scenario and should be seriously considered as one of the emerging biometric paradigms.

REFERENCES

Adini, Y., Sagi, D., & Tsodyks, M. (2002). Context-enabled learning in the human visual system. *Nature, 415*, 790–793.

BBC (2007a). Retrieved June 17, 2008 http://news.bbc.co.uk/2/hi/science/nature/1991517.stm

BBC (2007b). Retrieved June 17, 2008 http://news.bbc.co.uk/1/hi/sci/tech/2016788.stm.

Bellovin, S. & Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 72–84O.

Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 21–30.

Donchin, E., Spencer, K. M., & Wijesinghe, R. (2000). The mental prosthesis: Assessing the speed of a P300-based brain-computer interface. *IEEE Transactions on Rehabilitation Engineering, 8*(2), 174–179.

Farwell, L. A. & Donchin, E. (1988). Talking off the top of your head: A mental prosthesis utilizing event-related brain potentials. *Electroencephalography and Clinical Neurophysiology, 70*(6), 510–523.

Gupta, C. N. & Palaniappan, R. (2007). Enhanced detection of visual evoked potentials in brain-computer interface using genetic algorithm and cyclostationary analysis. [Special Issue] *Journal of Computational Intelligence and Neuroscience*, DOI: 10.1155/28692.

Kaper, M., Meinicke, P., Grossekathoefer, U., Lingner, T., & Ritter, H. (2004). BCI competition 2003-data set IIb: Support vector machines for the P300 speller paradigm. *IEEE Transactions on Biomedical Engineering, 51*(6), 1073–1076.

Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition.* Springer-Verlag.

Marcel, S. & Millan, J. (2007). Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 743-752.

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. In E.L. van Renesse (Ed.), *SPIE Optical Security and Counterfeit Deterrence Techniques, IV*(4677) 275–289.

Monrose, F., Reiter, M.K., Li, F.Q., & Wetzel, S. (2001). Cryptographic key generation from voice. In *Proceedings of the IEEE Conference on Security and Privacy* (pp. 202-213).

NewScientistTech (2007). Retrieved June 17, 2008, from http://www.newscientisttech.com/channel /tech/dn10963-brain-activity-provides-novel-biometric-key.html

Palaniappan, R. & Raveendran, P. (2002). Individual identification technique using visual evoked potential signals. *Electronics Letters, 138*(25), 1634-1635.

Palaniappan, R. & Ravi, K. V. R. (2006). Improving visual evoked potential feature classification for person recognition using PCA and normalization. *Pattern Recognition Letters, 27*(7), 726-733.

Palaniappan, R. & Mandic, D. P. (2007). Biometrics from brain electrical activity: A machine learning approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 738-742.

Paranjape, R. B., Mahovsky, J., Benedicenti, L., & Koles, Z. (2001). The electroencephalogram as a biometrics. *Proceedings of Canadian Conference on Electrical and Computer Engineering, 2*, 1363-1366.

Pinkas, B. & Sander, T. (2002). Securing passwords against dictionary attacks. In *Proceedings of 9th ACM Conference on Computer and Communications Security* (pp. 161–170).

Poggio, T., Fahle, M., & Edelman, S. (1992). Fast perceptual learning in visual hyperacuity. *Science, 256*, 1018–1021.

Poulos, M., Rangoussi, M., Chrissikopoulos,V., & Evangelou, A. (1999a). Person identification based on parametric processing of the EEG. *Proceedings of IEEE International Conference on Electronics, Circuits, and Systems, 1*, 283-286.

Poulos, M., Rangoussi, M., Chrissikopoulos, V., & Evangelou, A. (1999b). Parametric person identification from the EEG using computational geometry. *Proceedings of IEEE International Conference on Electronics, Circuits, and Systems, 2*, 1005-1008.

Roddy, A. R. & Stosz, J. D. (1996). Fingerprint features—Statistical analysis and system performance estimates. *Proceedings of the IEEE, 85*(9), 1390–1421.

Seitz, A. R., Kim, R., & Shams, L. (2006). Sound facilitates visual learning. *Current Biology, 16*(14), 1422-1427.

Serby, H., Tov, E. Y., & Inbar, G. F. (2005). An improved P300 brain computer interface. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 13*(1), 89-98.

Sutton, S., Braren, M., Zubin, J., & John, E. R. (1965). Information delivery and the sensory evoked potential. *Science, 155*, 1436–1439.

Thorpe, J. & Van Oorschot, P. C. (2004). Graphical dictionaries and the memorable space of graphical passwords. In *Proceedings of 13th USENIX Security Symposium*.

Thorpe, J., Van Oorschot, P. C., & Somayaji, A. (2005). Pass-thoughts: Authenticating with our minds. In *Proceedings of the New Security Paradigms Workshop*, Lake Arrowhead, California.

Tulving, E. & Schacter, D.L. (1990). Priming and human memory systems. *Science, 247*(4940), 301-306.

KEY TERMS

Authentication System: A system which securely identifies/authenticates users.

Biometrics: Recognising human beings using their intrinsic physical or behavioral traits.

Crossmodal Perception: Using more than on modality, say audio and video to analyze the perception skill or response from subjects.

Donchin Paradigm: It is an oddball paradigm that evokes P300 component and can be used by subjects to select alphabets or menus on screen.

Electroencephalogram (EEG): It is the neurophysiologic measurement of the electrical activity of the brain recorded from electrodes placed on the scalp.

Interstimulus Interval (ISI): *T*he time (interval) between the presentation of stimuli.

P300 Potential: A component in VEP which is evoked 300 ms after the presentation of the visual stimulus.

Visual Evoked Potential (VEP): A brain potential which is evoked on the presentation of a visual stimulus.

Visual Stimulus: A stimulus normally in the form of a picture or color shown on screen, which usually is used to evoke a VEP.