Encyclopedia of Information Ethics and Security

Marian Quigley
Monash University, Australia

INFORMATION SCIENCE REFERENCE
Hershey · New York

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Assistant Managing Editor: Diane Huskinson
Copy Editor: Maria Boyer
Typesetter: Sara Reed
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-pub.com
Web site: http://www.igi-pub.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of information ethics and security / Marian Quigley, Editor.
p. cm.
Topics address a wide range of life areas affected by computer technology, including: education, the workplace, health, privacy, intellectual property, identity, computer crime, cyber terrorism, equity and access, banking, shopping, publishing, legal and political issues, censorship, artificial intelligence, the environment, communication.
Summary: "This book is an original, comprehensive reference source on ethical and security issues relating to the latest technologies. It covers a wide range of themes, including topics such as computer crime, information warfare, privacy, surveillance, intellectual property and education. It is a useful tool for students, academics, and professionals"--Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-59140-987-8 (hardcover) -- ISBN 978-1-59140-988-5 (ebook)
1. Information technology--Social aspects--Encyclopedias. 2. Information technology--Moral and ethical aspects--Encyclopedias. 3. Computer crimes--Encyclopedias. 4. Computer security--Encyclopedias. 5. Information networks--Security measures--Encyclopedias. I. Quigley, Marian.
HM851.E555 2007
174'.900403--dc22
2007007277

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Identity Verification using Resting State Brain Signals

Ramaswamy Palaniappan
University of Essex, UK

Lalit M. Patnaik
Indian Institute of Science, India

INTRODUCTION

In the last several decades, computers or automated technologies have been utilized to verify the identity of humans using biometrics (i.e., physical and behavioral characteristics) (Wayman, Jain, Maltoni, & Maio, 2004), as it often surpasses the conventional automatic identity verification measures like passwords and personal identification numbers (PINs) by offering positive human identification. For example, the use of a PIN actually denotes the automatic identification of the PIN, not necessarily identification of the person who has provided it. The same applies with cards and tokens, which could be presented by anyone who successfully steals the card or token. PINs and passwords also have the problem of being compromised by 'shoulder surfing' and people picking the obvious choices. Even the recently proposed graphical passwords share similar problems.

The fingerprint-based biometrics has seen the most extensive deployment (Maltoni, Maio, Jain, & Prabhakar, 2003). Nevertheless, the field of biometrics remains exciting and actively researched after the continuing threats of transaction forgery and security breaches in e-commerce and electronic banking. Further, it is also very useful in other areas such as access to restricted places (control gates) or resources (computer log-in, automated teller machines, digital multimedia data access). As such, other biometrics like signatures (Jonghyon, Chulhan, & Jaihie, 2005), face (Chellappa, Wilson, & Sirohey, 1995), palmprint (Duta, Jain, & Mardia, 2002), hand geometry (Sanchez-Reillo, Sanchez-Avila, & Gonzalez-Marcos, 2000), iris (Wildes, 1997), and voice (Roberts, Ephraim, & Sabrin, 2005) have been proposed as an alternative or to augment the fingerprint technology. More recently, the field of biometrics has seen the emergence of newer biometrics techniques like keyboard dynamics (Bechtel, Serpen, & Brown, 2001), ear force fields (Hurley, Nixon, & Carter, 2005), heart signals (Biel, Pettersson, Philipson, & Wide, 2001), odor (Korotkaya, 2003), and brain signals (Paranjape, Mahovsky, Benedicenti, & Koles, 2001; Poulos, Rangoussi, Chrissikopoulos, & Evangelou, 1999a, 1999b; Palaniappan, 2004).

There are only a small number of reported studies on using brain signals as biometrics, which can further be classified as electroencephalogram (EEG) based or Visual Evoked Potential (VEP) based. The advantage of using EEG- or VEP-based biometrics compared to other biometrics is its distinctiveness—that is, it is difficult to be duplicated by someone else, therefore not easily forged or stolen. The storage is not a problem as the feature vector is of a small size compared to other image-based biometrics.

BACKGROUND

A brief description on some of the previous studies on brain signal biometrics follows. Paranjape et al. (2001) examined the use of autoregressive (AR) coefficients with discriminant analysis that gave classification of about 80% for 349 EEG patterns from 40 subjects. Poulos et al. (1999a) used Learning Vector Quantizer[1] network to classify AR parameters of alpha rhythm EEG, where classification performance of 72-84% were obtained from four subjects with 255 EEG patterns. In another study, Poulos et al. (1999b) utilized this same EEG data and feature extraction method but used computational geometry to classify the unknown EEGs, which gave an average classification of 95%.

In another previous study (Palaniappan, 2004), VEP-based biometrics were proposed. This method was based on using energy of gamma band VEP potentials recorded from 61 channels while the subjects perceived common pictures. Perception of the picture stimulus

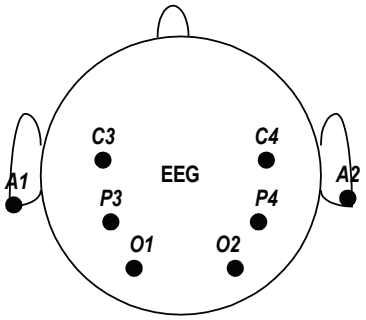
evokes recognition and memory, which involves gamma oscillations, which were distinct between the subjects, thereby being suitable for biometrics.

All these previous studies that used brain signals as biometrics concentrated on identification of a user from a pool of users. In this study, the focus is on verification of a user's claimed identity rather than identification. Further novelty of the proposed methods lies in the use of a two-stage verification procedure that gives good accuracy. It is also easier for the user as it requires only brain signals recorded during resting state, which do not require any degree of mental effort as compared to the requirement of focusing on the recognition of a picture stimulus as in the study in Palaniappan (2004). In addition, the proposed method requires only six channels, as compared to 61 channels as in Palaniappan (2004).

A system to verify the identity will either accept the user claiming a given identity or reject his or her claim. The user is called a client in the former case and an impostor in the latter case. There are two types of errors in this system: false match error (FME) or false non-match error (FNME). The former is the error made by the system when wrongly accepting an impostor, while the latter is the error made when wrongly rejecting the client.

A realistic application scenario for this sort of biometrics would be targeted at small groups of people, where the security would be an utmost important issue—for example, access to classified confidential documents or entry to restricted areas. Fingerprints could be easily forged, and most of the other biometrics like palmprint, face, and iris share the same problem of easy forgery. But it is not easy to duplicate the thought processes in the brain. However, it should be noted that this discussion applies to fraud in the samples, not fraud in the other parts of the system (extracted features, decision, etc.), which has the possibility of fraud for any biometrics.

Figure 1. Electrode placement



EXPERIMENTAL STUDY

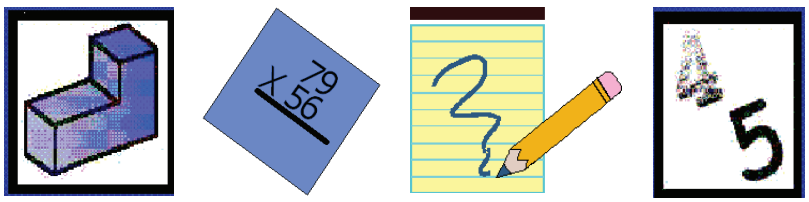
Data

EEG data from five subjects were used in this study. The subjects were seated in an industrial acoustics company sound-controlled booth with dim lighting and a noiseless fan (for ventilation). An Electro-Cap elastic electrode cap was used to record EEG signals from positions C3, C4, P3, P4, O1, and O2 (shown in Figure 1), defined by the 10-20 system of electrode placement. The impedances of all electrodes were kept below 5 KΩ. Measurements were made with reference to electrically linked mastoids, A1 and A2. The electrodes were connected through a bank of amplifiers (Grass7P511), whose band-pass analogue filters were set at 0.1 to 100 Hz. The data were sampled at 250 Hz with a Lab Master 12-bit A/D converter mounted on a computer. Before each recording session, the system was calibrated with a known voltage.

In this study, EEG signals were recorded from subjects while performing four different mental activities (shown illustratively in Figure 2), without vocalizing or making any other physical movements. These mental activities were:

a. **Mathematical multiplication activity:** The subjects were given nontrivial multiplication problems. The activities were non-repeating and designed so that an immediate answer was not apparent.
b. **Geometric figure rotation activity:** The subjects were given 30 seconds to study a particular three-dimensional block object, after which the drawing was removed and the subjects were asked to visualize the object being rotated about an axis.
c. **Mental letter composing activity:** The subjects were asked to mentally compose a letter to a friend or a relative without vocalizing. Since the activity was repeated several times, the subjects were told to continue with the letter from where they left off.
d. **Visual counting activity:** The subjects were asked to imagine a blackboard and to visualize

Figure 2. The four active mental activities performed by the subjects in the study: (a) rotation of a figure, (b) mathematical multiplication, (c) mental letter composing, and (d) visual counting. The other mental activity was resting. Note that the subjects imagined these activities without performing any form of action.



(a) (b) (c) (d)

numbers being written on the board sequentially, with the previous number being erased before the next number was written. They were also told to resume counting from the previous activity rather than starting over each time.

In addition, EEG signals were also recorded during a resting state where the subjects were asked to relax and think of nothing in particular. Signals were recorded for 10 seconds during each activity, and each activity was repeated for 10 sessions.

Signal Conditioning

The EEG signal for each mental activity was segmented into 20 segments with length 0.5 seconds. The sampling rate was 250 Hz, so each EEG segment was 125 data points (samples) in length. Since there were 20 EEG segments for a session; there were a total of 200 EEG segments (with six channels) from a subject. When a particular subject was in consideration for identity verification, 200 segments were treated as client data while the other 800 segments were treated as impostor data.

Each of the EEG segments was re-referenced to common average using:

$$z[n] = x[n] - \frac{1}{6}\sum_{i=1}^{6} x_i[n] \qquad (1)$$

where *x[n]* is the original signal, while *z[n]* is the new re-referenced signal. This would be useful in reducing the intra-subject variance of the EEG signals.

Feature Extraction

The EEG segments were filtered into three bands using Elliptic filter. These bands were alpha (8-13 Hz), beta (14-20 Hz), and gamma (21-50 Hz). Though only alpha and beta bands have been commonly used, we included gamma band due to its relationship with mental processes, which was shown in the study by Palaniappan, Raveendran, and Omatu (2002). Forward and reverse operations were performed to ensure no phase distortion. The stop-band width of the filter was 1 Hz beyond the pass-band width on both sides. The filter orders were chosen to give a minimum of 20 dB attenuation in the stop-bands and a maximum of 0.5 dB ripple in the pass-bands.

The filtered EEG segments were subjected to feature extraction using autoregressive (AR) modeling. A real valued, zero mean, stationary, AR process of order p is given by

$$z(n) = -\sum_{k=1}^{p} a_k z(n-k) + e(n) \qquad (2)$$

where p is the model order, *z(n)* is the re-referenced signal at the sampled point n, a_k are the real valued AR coefficients, and *e(n)* represents the error term independent of past samples.

In this article, Burg's method (Shiavi, 1999) was used to estimate the AR coefficients. It is more accurate than other AR coefficient estimators like Levinson-Durbin as it uses more data points simultaneously by minimizing not only a forward error but also a backward error. In computing AR coefficients, order six was used because it as used in another previous study by Palaniappan, Raveendran, Nishida, and Saiwaki (2002) for mental activity classification. Therefore,

six AR coefficients were obtained for each channel, giving a total of 36 features for each EEG segment for a mental activity. As there were three spectral bands, the size of the feature vector was 108.

Two-Stage Verification

For each subject, the 1,000 feature vectors (each with length 108) were split into:

- train patterns using 50 randomly selected client feature vectors
- validation patterns using 50 randomly selected client feature vectors (with no overlap to train patterns)
- test patterns using 100 remaining client feature vectors and all 800 impostor feature vectors

For different subjects, the allocations of the client and impostor feature vectors were different, where the particular subject's feature vectors were client feature vectors, while the rest of the subjects' feature vectors were impostor feature vectors. The Manhanttan[2] (city block) distances D were computed between 50 validation patterns and 50 training patterns. Manhanttan distance is simply the sums of lengths of the line segment in each dimension. For example, Manhanttan distance between two dimensional points P1 (x1,y1) and P2 (x2,y2) is |x1-x2| + |y1-y2|. Next, $D_{\min}$ and $D_{\max}$, the minimum and maximum of these D validation-training distances for each validation pattern were computed. Thresholds Th_1 and Th_2 were obtained using:

$$Th_1 = \min(D_{\min}) \text{ and } Th_2 = \max(D_{\max}) \qquad (3)$$

The Th_1 would be useful in reducing FME—that is, reducing the error of wrongly accepting impostors as clients—while Th_2 would be useful in reducing FNME—that is, reducing the error of wrongly rejecting the clients as impostors. D_{min} was used to ensure that only the extremely similar patterns close to the clients are accepted. This would filter out nearly all the impostors and perhaps some of the clients. So Th_2 would be useful in ensuring that the clients rejected using Th_1 were detected as clients, hence the use of D_{max}.

In the first verification stage, the maximum Manhanttan distances Dt_{max} of each of the 800 test patterns from the 50 training patterns were computed. The threshold Th_1 was used to determine whether each pattern was client or impostor, using the rule that the test pattern belonged to the client category if $Dt_{max}<Th_1$. Else, the test pattern was detected as from the impostor category. The focus of this verification level was to reduce FME only. No doubt, the FNME would be very high, but the second stage verification would solve this problem.

The second verification stage was used only for those test patterns that were detected as impostors. The minimum Manhanttan distances Dt_{min} of each of the test patterns (detected earlier as impostors) from the 50 training patterns were computed. The threshold Th_2 was used to determine whether the test patterns detected as impostors from first stage verification were really clients or impostors. Client was detected if $Dt_{min}<Th_2$. Else, it was impostor. The focus of this level was to reduce FNME.

Finally, FNME and FME were computed using:

*FNME=(no. of client patterns incorrectly detected as impostor patterns/100)*100%*

*FME=(no. of impostors patterns incorrectly detected as client patterns/800)*100%*

(4)

It should be noted here that there was no overlap between the test, validation, or training patterns. This was to ensure that accurate FNME and FME would be reflected. Figure 3 shows a simplified block diagram of the proposed approach.

Figure 3. Block diagram of the proposed approach

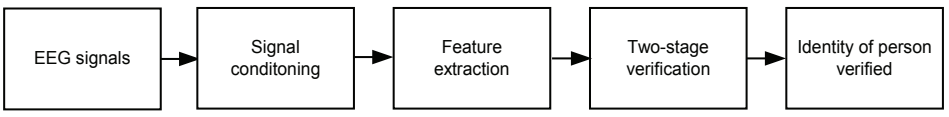


Table 1. Results of the experimental study

	Matching Error (%)											
Subject	S1		S2		S3		S4		S5		Average	
Activity	FNM	FM	FNM	FM	FNM	FM	FNM	FM	FNM	FM	FNM	FM
Resting	0	0	0	0	0	0	0	0	0	0	0	0
Count	0	0	0	0	4	0	0	0	0	0	0.8	0
Letter	0	0	0	0	0	0	0	0	0	0	0	0
Maths	16	0	0	0	8	0	14	0	1	0	7.8	0
Rotation	11	0	0	0	0	0	0	0	0	0	2.2	0
Minimum Error	0	0	0	0	0	0	0	0	0	0	0	0

Results

Table 1 shows the results of the experimental study. The FME and FNME values for each subject are shown. The low error values show the validity of the two-stage verification procedure using EEG signals. When comparing all the five subjects using the averaged FME and FNME values, the best mental activities were resting and letter composing. These activities gave good verification accuracy. Since resting activity is much easier to be performed by the subjects, it would be more suitable as compared to letter composing activity. The mental activity that gave the worst accuracy was mathematical multiplication activity.

FUTURE TRENDS

Although the proposed approach is still far from being suitable for an immediate industrial application, our aim was to draw attention of the international research community to the significant potential of brain electrical activity as a biometric.

For future work, we plan to investigate the stability of EEG signals over time and on extending the work to include more subjects. Further, a reduced feature set will also be studied, for example, use of a single channel (electrode) which will greatly simplify the EEG signal capture. It would also be worthwhile to study the use of this biometric in a multimodal environment—that is, to investigate if this biometric could be used in conjunction with other existing biometrics to increase the accuracy.

As this area is closely related to Brain-Computer Interface (BCI) designs for the use of paralyzed individuals, improvements in BCI would probably see similar improvements in this *brain biometrics*.

CONCLUSION

In the proposed approach, EEG data were recorded from five subjects while they were performing some simple mental activities. These EEG signals were subjected through several steps of signal conditioning, feature extraction, and decision making. In the signal conditioning step, the EEG signals were filtered into different spectral bands and re-referenced to common average, while in the feature extraction stage, AR coefficients were computed to be used as discriminative features. In the decision-making step, a novel two-stage verification procedure was used that gave good accuracy.

Though EEG data from six electrodes were used here instead of one to increase the inter-subject differences, it is still far less than 61 used in the earlier study for identification (Palaniappan, 2004). The good results obtained in this study indicate that it is possible to verify the identities of users by the use of resting state EEG signals alone. This pilot study has shown the potential of using EEG for biometric verification systems, especially for high-security environments as they are resistant to fraud.

Applications for this system include where fingerprints and other identity measures like passwords could be easily forged. It could also be used as a modality within a multimodal biometrics environment. The advantage of using such brain electrical activity as biometrics is its fraud resistance, that is the recorded brain response is difficult to be duplicated by someone else, and is hence unlikely to be forged or stolen. This

modality has the additional advantage of confidentiality ('shoulder surfing' is impossible) as brain activity is not easily seen.

The 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 and that the fraud resistance significantly outweighs this difficulty especially for high security applications.

ACKNOWLEDGMENT

The authors would like to acknowledge the assistance of Dr. C. Anderson of Colorado State University, USA, for giving permission to use the EEG data. We also thank the Department of Biotechnology, Government of India for supporting a portion of the work.

REFERENCES

Bechtel, J., Serpen, G., & Brown, M. (2001). Passphrase authentication based on typing style through an ART 2 neural network. *International Journal of Computational Intelligence and Applications, 2*(2), 131-152.

Biel, L., Pettersson, O., Philipson, L., & Wide, P. (2001). ECG analysis: A new approach in human identification. *IEEE Transactions on Instrument and Measurement, 50*(3), 808-812.

Chellappa, R., Wilson, C.L., & Sirohey, S. (1995). Human and machine recognition of faces: A survey. *Proceedings of IEEE, 83*(5), 705-740.

Duta, N., Jain, A.K., & Mardia, K.V. (2002). Matching of palmprint. *Pattern Recognition Letters, 23*(4), 477-485.

Hurley, D., Nixon, M., & Carter, J. (2005). Force field feature extraction for ear biometrics. *Computer Vision and Image Understanding, 98*(3), 491-512.

Jonghyon, Y., Chulhan, L., & Jaihie, K. (2005). Online signature verification using temporal shift estimated by the phase of Gabor filter. *IEEE Transactions on Signal Processing, 53*(2-2), 776-783.

Korotkaya, Z. (2003). *Biometric person authentication: Odor.* Retrieved June 12, 2006, from http://www.it.lut.fi/kurssit/03-04/010970000/seminars/korotkaya.pdf

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

Palaniappan, R. (2004). Method of identifying individuals using VEP signals and neural network. *IEEE Proceedings—Science, Measurement and Technology, 151*(1), 16-20.

Palaniappan, R., Raveendran, P., & Omatu, S. (2002). VEP optimal channel selection using genetic algorithm for neural network classification of alcoholics. *IEEE Transactions on Neural Networks, 13*(2), 486-491.

Palaniappan, R., Raveendran, P., Nishida, S., & Saiwaki, N. (2002). A new brain-computer interface design using fuzzy ARTMAP. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 10*(3), 140-148.

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

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

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

Roberts, W.J.J., Ephraim, Y., & Sabrin, H.W. (2005). Speaker classification using composite hypothesis testing and list decoding. *IEEE Transactions on Speech and Audio Processing, 13*(2), 211-219.

Shiavi, R. (1999). *Introduction to applied statistical signal analysis* (2nd ed.). London: Academic Press.

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 22*(10), 1168-1171.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (Eds.). (2004). *Biometric systems: Technology, design and performance evaluation*. New York: Springer-Verlag.

Wildes, R.P. (1997). Iris recognition: An emerging biometric technology. *Proceedings of IEEE, 85*(9), 1348-1363.

KEY TERMS

Autoregressive (AR): A type of modeling commonly employed for EEG signals.

Alpha, Beta, Gamma: Some commonly used spectral bands.

Biometric: A quantitative measure of physical and behavioral characteristics of humans, normally used for identification/verification of the identity of the user.

Client: The actual user claiming the identity.

Electroencephalogram (EEG): Electrical potentials (in micro Volts range) caused by brain activity and obtained from the scalp using electrodes.

False Matching Error (FME): Also known as false accept error; the error of the system when it wrongly accepts impostors as clients.

False Non-Matching Error (FNME): Also known as false reject error; the error of system when it wrongly rejects the clients as impostors.

Impostor: The user claiming to be another user.

Verification: Also known as authentication; the procedure to verify the claimed identity of the user.

Visual Evoked Potential (VEP): A type of EEG/brain signal that is evoked when the subject perceives a visual stimulus.

ENDNOTES

1 In the article, it is referred as Learning Vector Quantizer, though the common name is Learning Vector Quantization.

2 Alternatively, Euclidean distance could also be used.