ISSN: 2321-7782 (Online)
Volume 2, Issue 6, June 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Review on the Challenges Encountered in Biometric Based Authentication Techniques

Sheela Shankar[1]
Professor
Department of Electronics & Communication Engg
KLE Dr.M. S. S CET, Udyambag
Belgaum – India

Dr. V. R Udupi[2]
Department of Electronics & Communication Engg
Gogte Institute of Technology
Belgaum – India

Abstract: Authentication or uniquely identifying a person is a very crucial aspect and has vivid applications worldwide. The most robust being biometric, which has its own pros and cons inherent. Since they are hard to refute, effective utilization of these can effectively identify a person. Hence governing the negative issues is of paramount importance. This paper makes a survey of the challenges met in two biometric based approaches: face recognition and authentication via neuro-signals. It is found that the key challenges in the former are less complex when compared to the latter.

Keywords: Authentication techniques, biometric, face recognition, brainwave based authentication.

I. INTRODUCTION

Authentication techniques can be broadly classified into three classes [1]:

1) *Something-you-are:* deals with the bodily characteristics that are unique identification of a person. Such techniques are called biometric based and are discussed in detail, throughout the paper.

2) *Something-you-have*: can be objects or items to authenticate, for instance, ATM cards, passport, keys, etc.

3) *Something-you-know*: as the name implies, it is secret information known only to the user. Passwords and PIN numbers are better examples to substantiate this.

Currently authentication is mainly carried through user ids, passwords, PIN numbers, magstripe magnetic cards, etc. Though these techniques enjoy wide acceptance, they fall prey to few vulnerabilities. They can easily be disclosed or acquired by direct covert observation. They can also be shared, lost or can be forgotten owing to human nature. Maintaining same passwords for all the accounts can be easy to remember, but at the cost of security. Frequent amendments in passwords assure security to some extent, but pose difficulty in remembering them. Hence these methods upheld the issue of "repudiation" and are prejudicial. Although, secure encryption methods bestow a high degree of security to credit card based transactions to pass through the web; the technique fails to identify whether the right credit card owner is carrying out the transactions. Altogether, the use of the combination of mere user id's and passwords cannot be relied and alternative strategies are highly vital.

Biometric authentication, on the other hand, bequeath true user authentication. It is concerned with identifying a person based on his/her behavioral or physiological characteristics. This is of great help especially for illiterates. Behavioral biometric can be gait, speech, signature and keystroke analysis, whereas physiological biometric uses face, ear, finger-print, voice, finger geometry, palms, hand veins, hand geometry, iris matching and recently brain waves are used exclusively in this regard [2].

In this paper, we discuss in detail the problems related to two biometric based authentication techniques. We focus on face-recognition and brainwave based authentication. Section II deals with biometric systems in detail. Face recognition is explained in section IV. Brainwave based authentication is discussed in section IV. Concepts pertaining to challenges, design schema, and their

advantages over conventional methods are also briefed. Conclusion of the survey and the future scope of the above mentioned techniques are given in section V and VI, respectively.

II. BIOMETRIC SYSTEMS

A. General view:

Figure 1 represents the abstract working of a typical biometric system. A much detailed description can be found in [3,4]. The first phase consists of input acquisition and digitizing it. Examples include a fingerprint scanner, microphone, camera and an EEG device in case of finger-print, speech, face and brainwave based authentication, respectively. A/D convertors are embedded in this phase. Second phase deals with transforming the data from crude format to system desirable format. It includes removal of artifacts and later processing it by applying some kind of normalizations onto it. In the third phase, useful features are extracted from the digitized data. It is better known as identification of "landmarks" in the data. The fourth phase basically does away with fixed and well-known variations (often stored in a database) which are encountered frequently. Hence this phase is termed as "template generator". Finally the newly generated template is matched against the stored templates which are unique to a person. On successful match, the user is authenticated.

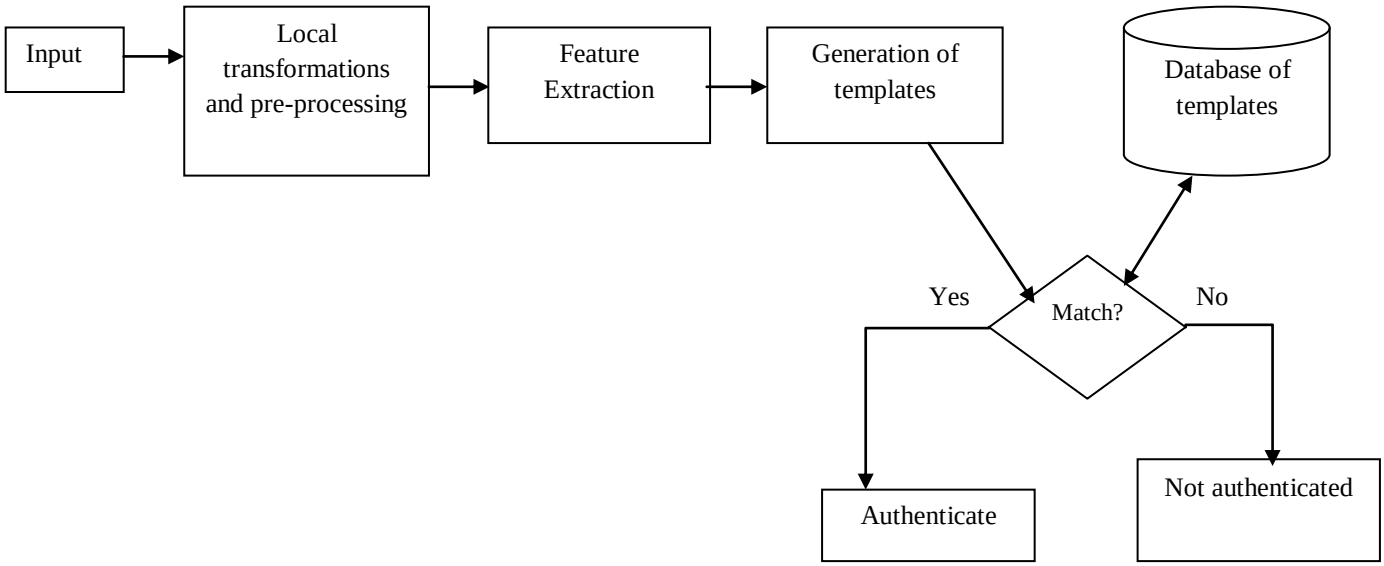

Figure 1 showing the block diagram of a typical biometric setup.

B. Basic aspects:

A biometric based system should satisfy the following criterion for mass- acceptance [5]:

1) Circumvention: The ease rendered by the system for its evading. 2) Stability: Non-changeability of the attributes with respect to time. 3) Acceptability: the system should be accepted by users and they must be well acquainted with it. 4) Uniqueness: The feature should be distinct between all users. 5) Universality: The feature should be present in every user required to run the system. 6) Collectability: Feature measurements should be less complex and feasible. 7) Performance: Time and space complexity should be better.

C. Limitations of existing approaches:

1) Iris verification: Sensitive to body motions, costly equipments required for data acquisition and parsing. The user is expected to stand in the fixed position in front of the camera. 2) Finger printing/hand geometry: The user is supposed to place his finger or hand on the sensor properly. Bruises or cracks on these body organs can cause hurdles. 3) Signature: may be subjected to forgery or modification. 4) Voice matching: Vulnerable to background noise (in case of public places).

The advantages and disadvantages of face recognition and brainwave based authentication system are discussed in the succeeding sections.

III. FACE RECOGNITION

A. General View:

Broadly speaking, face recognition is a non-intrusive form of identifying a given face image and matching it against a set of faces in the database, in order to validate a person [6]. Face recognition tasks can be grouped into three categories, namely open-universe face identification, closed-universe face identification and open-universe face verification [7]. The block diagram of the basic model of a face recognition system can be seen in Figure 2.

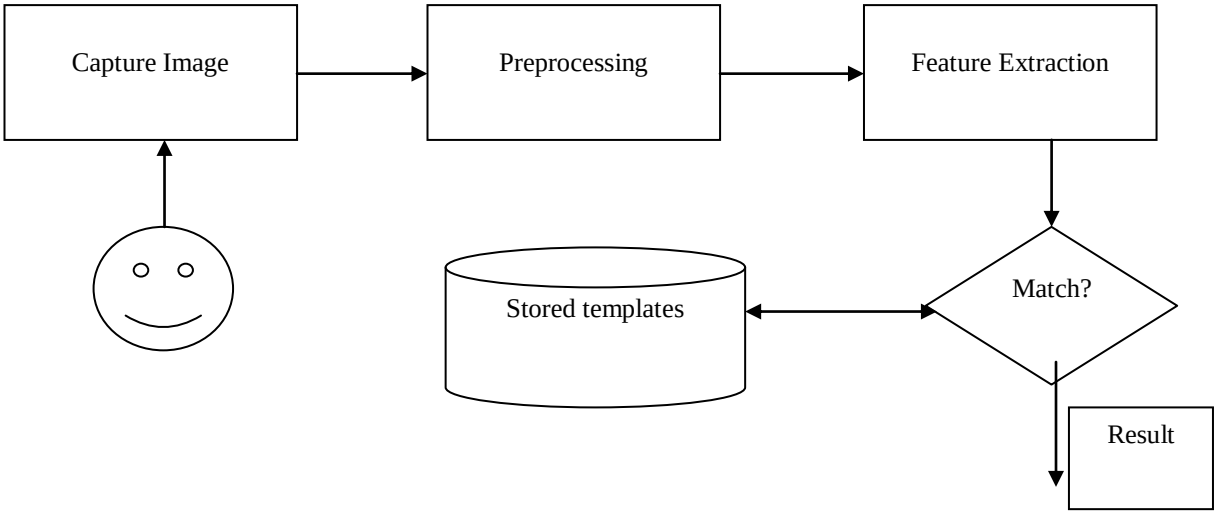

Figure 2. Abstract model of face recognition system.

B. Authentication Methodology:

Selection of face recognition techniques depends on the type of application under consideration. Few applications demand static images (taken by the camera) while others demand videos, especially in surveillance domains.

There are basically two major schemes for developing face recognition practices:

1) Build efficient techniques which can either lessen or completely excavate the artifacts generated in images. 2) Enhancing the universality and capability of the existing algorithms, so as to withstand the alterations. Techniques like artificial neural networks [9], principal component analysis (PCA), modular PCA, Fisher discriminant analysis, etc., are used widely.

C. Advantages of face recognition over conventional means of biometric authentication:

Most of the existing biometric techniques lead to accumulation of impurities and germs on the sensor devices and thereby their transmission onto the users is a common scenario. Face recognition does not suffer from this liability since the camera is placed at a distance and is not in contact of the user.

D. Challenges met:

1) The automation of face detection gets affected by a variety of considerations like partial occlusions of face, head orientation and variations in lighting, illumination, etc.

2) Differences based purely on the face: Is basically of two types: Interpersonal and intrapersonal. Variations in faces due to gender, race among different people are interpersonal factors. The intrapersonal factors which yield variations are goggles, facial hair, expressions, cosmetics, changes occurring owing to health and age, etc.

3) Managing pose when the face image is captured for testing [8].

E. Areas of applications:

Face recognition can be employed for both identification and verification of an individual. They find tremendous applications in ATMs, seaports, airports, security in computer networks [10]; identity verification in passports, ecommerce, driver license, forensics, missing children, reconstruction of the face of the witness [11]; surveillance in CCTVs; recognition of expression, gender classification, assessment of behavior, etc. They can be used in stress and exhaustion detection in drivers [12] and thus alarm him to drive carefully.

IV. BRAINWAVE BASED AUTHENTICATION

A. General View:

Brainwave based authentication is recently a new addition to the conventional authentication techniques. It involves the use of electrical activity in brain to confirm a person's identity. A more detailed description of the brainwaves and its applications are discussed in section B. Figure 3 depicts the abstract view of brainwave based authentication.

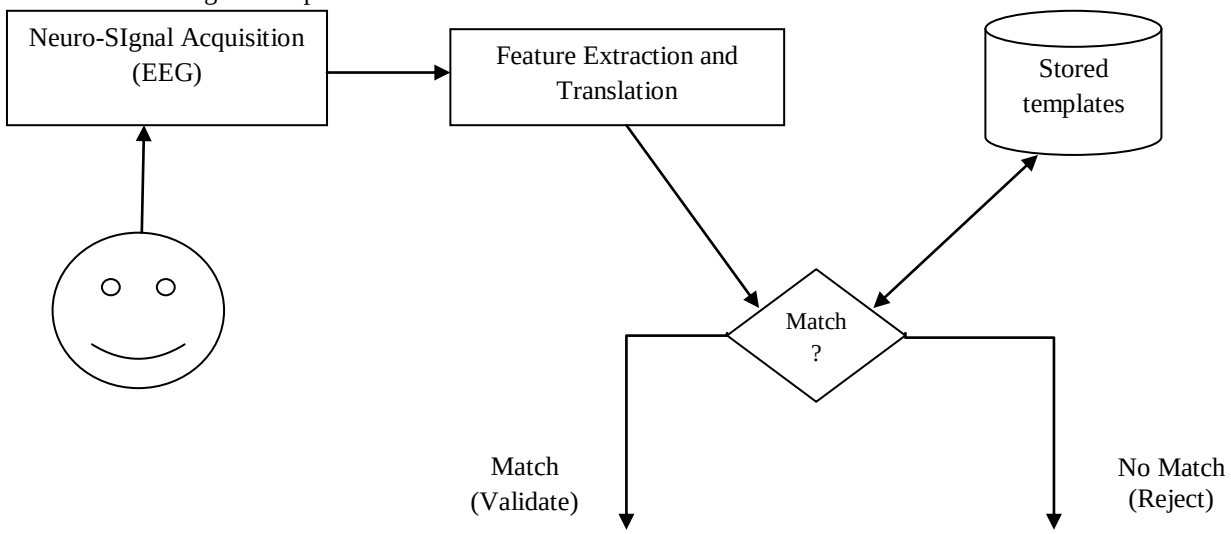

Figure 3. Block diagram of brainwave based authentication technique

B. Brain Computer Interface:

Human brain consists of millions of neurons, which forms a network and uses electric impulses to communicate. This electrical activity is analogous to various activities of human beings. The waveforms can be recorded using an Electroencephalography (EEG) device. Currently, this has reached par with medical applications and running computer applications is gaining wide acceptance. This methodology has emerged as Brain-Computer Interface technology [13, 14]. The areas of application ranges from medical to cognitive improvement, education and training, entertainment, gaming, user state monitoring, evaluation in neuro-marketing and neuro-ergonomics, etc. Major research is going on in using one's neuro–signals to uniquely identify him. It mainly comprises of a signal acquisition phase (facilitated by EEG device), signal processing (to extract data from the brain waves and translate them to machine understandable format) and the final phase deals with driving computer applications.

C. Authentication methodology:

Each physiological and mental activity of the brain is associated with brainwaves. So it's obvious to raise the question: authentication based on raw waveforms (pertaining to any activity) or based on a specific expected thought. The password here may be thinking of a specific number or character, picture, color, etc [15]. Auto Regressive parameters, Fast Fourier Transforms (to determine spectral power), Dynamic Time Warp algorithm [16] are widely used in EEG based authentication. Much detailed work can be found in [17-20].

D. Advantages over conventional methods:

1) Keys, ATM cards, and other hardware means of authentication can be lost but not the brain. It is present in every human (universality property). 2) Shoulder surfing or careful observation can help to determine the passwords typed. But it is highly impossible to visualize one's thought processes. Nevertheless, even if the user shares or writes down his/her thought, it is highly impractical for the intruder to reconstruct it in the same fashion as that of the user. This reduces the degree of 'identity theft', wherein the intruder steals the secret information of the user [21].

3) Physically handicap people cannot use retina scanning or fingerprinting, but brain functions as long as a person is alive. 4) High degree of intricacy (uniqueness property) of brain makes it difficult for the intruder to imitate other's brain (circumvention property).

E. Pitfalls:

1) Maintaining the same thought process every time for the fixed entity is at an increased level of complexity. 2) Brainwaves get basically altered with respect to increase in age. Therefore, the system should adapt itself to this change effectively (stability property) [22]. 3) There is a wide range of EEG devices available in the market. Sophisticated, high end devices are costly as well as non-portable. But they help in acquiring good quality waveforms. On the other hand, cheap devices do not facilitate this (collectability property). 4) The fear of leakage of mental processes in an individual is hampering its usage (acceptability property).

V. Conclusion

As a summary, the paper deals with the advantages of biometric based authentication techniques and the challenges innate in them. Among them, two robust techniques were discussed in detail. Face recognition, though a more challenging approach, is well established when compared to EEG based authentication. The latter consumes considerable amount of time of the user in wearing the device in conjunction to the processing time of the system; with respect to the former. Brainwave authentication requires rigorous research so as to work in real time systems and become widely acceptable.

VI. Future Scope

Biometric systems should be designed to handle all the vulnerabilities discussed in the paper to a maximum extent. Neuro-signals based authentication should be fast, robust and should gain the confidence of public by ensuring security against their mental data disclosure. Face recognition systems should deploy all the parameters in a single implementation, so as to do away with the existing shortcomings.

Acknowledgement

The authors are immensely grateful to the valuable suggestions and help provided by Prof. U. L. Naik, Department of Telecommunication Engineering, KLE Dr. M. S. S College of Engineering and Technology, Udyambag, Belgaum.

References

1. Merkow, M. & Breithaupt, J. 2006. Information Security: Principles and Practices.Pearson Prentice Hall.
2. A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Security," A. K. Jain, R. Bolle, and S. Pankanti, Eds.: Kluwer Academic Publishers, 1999.
3. B. Miller, Vital signs of identity, IEEE Spectrum 31 (2) (1994) 22–30
4. A.K. Jain, L. Hong, S. Pankanti, Biometrics identi5cation, Commun. ACM 43 (2) (2000) 91–98.
5. Jain, A. K., Ross, A., , & Prabhakar, S. 2004. An introduction to biometric recognition. IEEE Transactions On Circuits and Systems for Video Technology, 14, 4–20.
6. Rabia Jafri, Hamid R. Arabnia, "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol.5, No.2, June 2009. DOI : 10.3745/JIPS.2009.5.2.041
7. Enrique G. Ortiz, Brian C. Becker, "Face recognition for web-scale datasets", Comput. Vis. Image Understand. (2013), http://dx.doi.org/10.1016/j.cviu.2013.09.004, Elsevier.

8. Xiaozheng Zhang, Yongsheng Gao, "Face recognition across pose: A review", Pattern Recognition 42 (2009) 2876 – 2896, Elsevier.doi: 10.1016/j.patcog.2009.04.017
9. Nathan Intrator, Daniel Reisfeld, Yehezkel Yeshurun, "Face recognition using a hybrid supervised/unsupervised neural network", Pattern Recognition Letters 17 (1996) 67-76, Elsevier.
10. H. Moon, "Biometrics Person Authentication Using Projection-Based Face Recognition System in Verification Scenario," in International Conference on Bioinformatics and its Applications. Hong Kong, China, 2004, pp.207-213.
11. C. G. Tredoux, Y. Rosenthal, L. d. Costa, and D. Nunez, "Face reconstruction using a configural, eigenface-based composite system," in 3rd Biennial Meeting of the Society for Applied Research in Memory and Cognition (SARMAC). Boulder, Colorado, USA, 1999.
12. Jaeik Jo, et al., "Detecting driver drowsiness using feature-level fusion and user-specific classification", Expert Systems with Applications 41 (2014) 1139–1152. Elsevier. Doi: 10.1016/j.eswa.2013.07.108
13. Jonathan R. Wolpaw, et.al., "Brain–Computer Interface Technology: A Review of the First International Meeting", IEEE TRANSACTIONS ON REHABILITATION ENGINEERING, VOL. 8, NO. 2, JUNE 2000.
14. GerwinSchalk, et.al., "BCI2000: A General-Purpose Brain-Computer", IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 51, NO. 6, JUNE 2004
15. Fladby, Kennet. "Brain wave based authentication." (2008).
16. Keogh, E. & Pazzani, M. 2001. Derivative dynamic time warping. First SIAM International Conference on Data Mining, (Chicago, IL, 2001).
17. Chrissikopoulos, V., Evangelou, A., Poulos, M., & Rangoussi, M. 1999. Person identification based on parametric processing of the eeg. Electronics, Circuits and Systems, 1999. Proceedings of ICECS '99. The 6th IEEE International Conference on, 1.
18. Alexandris, N., Poulos, M., & Rangoussi, M. 1999. Neural network based person identification using eeg features. Acoustics, Speech, and Signal Processing, 1999. ICASSP '99. Proceedings., 1999 IEEE International Conference on, 2.
19. Poulos, M., Rangoussi, M., Alexandris, N., & Evangelou, A. 2002. Person identification from the eeg using nonlinear signal classification. Methods of information in medicine., 41.
20. Chrissikopoulos, V., Evangelou, A., Poulos, M., & Rangoussi, M. 1999. Parametric person identification from the eeg using computational geometry. Electronics,Circuits and Systems, 1999. Proceedings of ICECS '99. The 6th IEEE International Conference on, 2.
21. Loibl, T. R. 2005. Identity theft, spyware and the law. In InfoSecCD '05: Proceedings of the 2nd annual conference on Information security curriculum development, 118–121, New York, NY, USA. ACM.
22. Vogel. 1970. The genetic basis of the normal human electroencephalogram (eeg). Humangenetik, 10, 91–114.

AUTHOR(S) PROFILE

Prof. Sheela Shankar has completed her Bachelor of Engineering in Electronics and Communication from BIET, Davangere, Karnataka. She has pursued her Masters in Electronics and Control Engineering from Birla Institute of Technology and Science, Pilani. Currently she is working as an associate professor in the department of Electronics and Communication Engineering, KLE Dr.M.S.Sheshgiri College of Engineering and Technology, Belgaum, Karnataka, India. Her areas of research includes image processing, communication engineering and control engineering.

Dr. V. R. Udupi did his bachelor's degree in Electronics and communication Engg. from Mysore University in 1984 and pursued his master's degree in Electronics Engineering with computer applications as specialization from Shivaji University, Kolhapur, Maharashtra state, in 1989. He has completed his doctoral degree in Electrical Engineering from Shivaji University, Kolhapur, Maharashtra state, in 2003. His field of interests includes signal processing, Image processing, cryptography, and knowledge based systems. Currently he is working as a professor in Electronic and communication department of Gogte institute of Technology, Belgaum, Karnataka state. He has 30 years of total teaching experience and currently he is guiding 05 research scholars and has guided 04 candidates for Ph.D. He has published more than 42 technical papers in national and international conferences and 08 articles in journals. He is a life member of ISOI, SSI, CSI, BMESI, and ISTE.

