Biometrics Applications in e-Health Security: A Preliminary Survey

Ebenezer Okoh[1] and Ali Ismail Awad[1,2]

[1]Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology, Luleå, Sweden
[2]Faculty of Engineering, Al Azhar University, Qena, Egypt
{ebeoko-2@student.ltu.se}, {ali.awad@ltu.se}

Abstract. Driven by the desires of healthcare authorities to offer better healthcare services at a low cost, electronic Health (e-Health) has revolutionized the healthcare industry. However, while e-Health comes with numerous advantages that improve health services, it still suffers from security and privacy issues in handling health information. E-Health security issues are mainly centered around user authentication, data integrity, data confidentiality, and patient privacy protection. Biometrics technology addresses the above security problems by providing reliable and secure user authentication compared to the traditional approaches. This study explores the security and privacy issues in e-Health, and offers a comprehensive overview of biometrics technology applications in addressing the e-Health security challenges. The paper concludes that biometrics technology has considerable opportunities for application in e-Health due to its ability to provide reliable security solutions. Although, additional issues like system complexity, processing time, and patient privacy related to the use of biometrics should be taken into consideration.

1 Introduction

The emergence of electronic health (e-Health) has proved to be very compelling for the health industry due to the many benefits it affords the industry. E-Health improves the quality of healthcare by making Patients Health Information (PHI) easily accessible, improving efficiency, and reducing the cost of health service delivery. Patients rarely get to spend much time with their physicians face-to-face. In spite of the benefits of e-Health, it still faces a number of security challenges that need to be addressed. E-Health data security and patient privacy stand out as top issues that health organizations implementing e-Health still grapple with, and to which they need solutions [1]. E-Health security requirements revolve around the basic principles of information security. E-Health security issues include the preservation of e-Health data confidentiality, data integrity, data availability, user authentication, and patient privacy protection [2].

Maintaining data security and user privacy in e-Health is therefore paramount. In order to ensure e-Health security from a technical point of view, it involves

securing e-Health applications and their communication components. The underlying issue that is particularly important in relation to the security requirements of e-Health is the user authentication and authorization. In this context, achieving reliable user authentication forms the basis for all other measures to be achieved. Traditional authentication approaches such as user name, password, and access cards are not appropriate in the e-Health context due to the possibility of being lost, stolen, forgotten, or misplaced. In general, traditional authentication methods are not based on inherent individual attributes [3].

Biometrics is a fundamental security mechanism that assigns a unique identity to an individual according to some physiological (fingerprint or face) or behavioral characteristics (voice or signature) [4]. Therefore, biometrics is more reliable and capable than traditional authentication approaches of distinguishing between an authorized person and an imposter. Biometric traits cannot be lost or forgotten; they are difficult to duplicate, share, or distribute. Moreover, it requires the presence of the person being authenticated; it is difficult to forge, and unlikely for a user to repudiate [5]. Biometrics offers a sense of security and convenience both to patients and physicians alike. In order to stay ahead of the emerging security threats posed by e-Health, healthcare organizations are moving from traditional approaches to the utilization of biometrics technology.

This paper explores the security and privacy issues in e-Health as they continue to remain challenges for the healthcare industry. In addition, it seeks to embark on a review to highlight the applications of biometrics in addressing some of the e-Health security and privacy challenges. The research focus is on biometrics applications in user authentication and health data encryption. We believe that this study will provide a good foundation for further research in the area of healthcare data security and patient privacy protection.

The remainder part of this paper is structured as follows: Section 2 presents background on biometrics technology. Preliminary information about e-Health and its current security challenges is covered in Section 3. A detailed exploration of biometrics applications in e-Health security, and how they address e-Health security issues, is placed in Section 4. Section 5 presents a discussion on the current biometrics deployments in e-Health domain, and a discussion of future research directions. Finally, conclusions are documented in Section 6.

2 Biometrics Technology

Biometrics is the science of establishing the identity of an individual based on the physiological, chemical, or behavioral attributes of the individual [6]. In order to identify individuals based on their biometric traits, biometric systems need to go through two major phases, namely an enrollment phase and a recognition phase [7], [8]. Alternatively, biometric systems are regarded as pattern recognition systems consisting of four phases: sensor, feature extractor, database, and matcher [7]. Although, biometric systems support both identification (recognition) and verification (authentication) modes of operation, the appropriate mode is decided according the target application. Biometric identification refers to identifying an

individual from a database of users based on his or her distinguishing biometric trait (unimodal) or traits (multimodal) [3]. However, verification mode ensures the authenticity of the identity claimed by an individual.

The requirements of biometrics deployment demand certain traits be used. Each biometric identifier has its own strength and weakness, and the choice of a certain biometric identifier is based on the systems needs [5]. Every biometric trait must fulfill, in different degrees, the following properties [7], [9]: universality (every person must possess the trait); uniqueness (the trait should be sufficiently distinct between persons); permanence (the trait should be invariant over time); measurability (the possibility of measuring the trait quantitatively); performance (achievable recognition accuracy); acceptability (the willingness of people to accept the system); and circumvention (the ability of the biometric system to defend against any system hacking operation). Table 1 shows a comparison of different biometric identifiers based on the aforementioned selection criteria. The the final score indicates the overall evaluation of the identifier.

In general, a similarity match score is used to measure the similarity between two feature sets from same or different biometric traits. A higher matching score provides a strong indication that the two biometric features originate from the same person. In practice, there are two basic techniques for measuring the accuracy of a biometric system; False Non- Match Rate (FNMR) and False Match Rate (FMR). These are also considered to be the two major errors made by a biometric system. FNMR refers to the probability that two samples of the same biometric trait from the same user are falsely declared as a non-match. Thus, the biometric system mistakenly rejects a genuine individual as an imposter. FMR refers to the probability that two samples from different biometric traits are mistakenly recognized as a match, and hence, the biometric system mistakenly accepts an imposter as a genuine individual [7].

There are other types of failures encountered by any biometric system. These are Failure to Capture (FTC), Failure to Acquire (FTA), and Failure to Enroll (FTE). FTA represents the proportion of times a biometric device fails to capture a sample when biometric characteristics are presented to it. FTE represents the proportion of users that cannot be successfully enrolled in a biometric system

Table 1. A comparison between different biometric identifiers: 1 = High, 0.5 = Medium, and 0 = Low. The table is adapted from [4], [5], [9].

	Universality	Uniqueness	Performance	Acceptability	Circumvention	Score
Fingerprint	0.5	1.0	1.0	0.5	1.0	**4.0**
Face image	1.0	0.0	0.0	1.0	0.0	2.0
Iris pattern	1.0	1.0	1.0	0.0	1.0	**4.0**
DNA	1.0	1.0	1.0	0.0	0.0	**3.0**
EEG	1.0	0.0	0.0	0.0	0.0	1.0
Signature	0.0	0.0	0.0	1.0	0.0	1.0
Voice	0.5	0.0	0.0	1.0	0.0	1.5
Gait	0.5	0.0	0.0	1.0	0.5	2.0

[6]. There is a tradeoff between biometric systems FMR and FNMR which could be plotted on a Receiver Operating Characteristics (ROC) curve or Detection Error Tradeoff (DET) curve [3]. The ROC curve gives a measure of the system accuracy in a test environment [3]. The performance of a biometric system could also be determined by the Equal Error Rate (EER) of the system. The EER refers to the point in a DET curve where the FMR equals the FNMR. A lower value of EER indicates a better biometric system performance [6], [7].

3 Electronic Health (e-Health)

Recent advances in the field of telemedicine around the twentieth century paved the way for e-Health. Following that came developments in computerization, digitization of data, and digital networks which led to a multiplicity of e-Health applications [10]. Currently, e-Health comprises a whole range of services or systems at the edge of healthcare and information technology such as: telemedicine, which is defined as a remote healthcare delivery system using telecommunication and information technology; Electronic Health Records (EHR), which include electronic health information about a patient or individual; consumer health informatics, which is use of medical informatics to analyze consumer needs for information; health knowledge management, which aims to capture, describe, organize, share, and effectively use healthcare knowledge; medical decision support systems, which are interactive expert systems that assist health professionals with decision-making tasks; and mobile health (mHealth), which uses mobile devices for different applications in healthcare [10]. The underlying factor in all of these technologies is the digitization of data. In that regard, the term (e-Health) suggests digital health information in contrast to a paper-based system.

E-Health is an emerging field of medical informatics that refers to the organization and delivery of health services and information using the internet and related technologies [11]. In a broader sense, e-Health involves the application of information and communication technologies in healthcare. It involves all digital health-related information, encompassing products, systems, and services. The term health does not solely refer to medicine, disease, or healthcare but also comprises public health and healthcare.

The adoption of e-Health services achieves different goals including: increased efficiency in healthcare, enhanced quality care, evidence-based medicine, empowerment of consumers and patients by broadening the knowledge base of medicine, encouragement of new relationships between patients and health professionals, education of physicians and consumers, enabling information exchange and communication, extending the scope of healthcare; posing new ethical issues, and promoting equity in healthcare [11]. In concise terms, it promotes health information sharing, ensures effective healthcare, and empowers health consumers to manage their own health. It seeks to transform the healthcare system from a "provider-driven" model to a "patient-centric" paradigm [12].

Several studies that have been undertaken in the field of e-Health have demonstrated system architecture in order to represent a proposed e-Health

system [12], [13], [14]. Several of these studies present a three-level system architecture of e-Health. For instance, in [12], the authors present an e-Health architecture consisting of three layers. The first layer consists of devices that help collect real-time data from patients. The second layer consists of the internet or interconnected devices that help transport the collected data from patients to third-party database servers or healthcare service providers. The third level is made up of intelligent systems to help in making health decisions. Similarly, in [13], the authors present a network layer architecture for an e-Health system.

3.1 Security Challenges in e-Health

There are, however, concerns about the security and privacy of patient health information. Privacy is considered one of the fundamental issues in e-Health. The electronic nature of health information introduces certain vulnerabilities that increase the possibility of security breaches occurring. E-health information can exist in three states: storage, transmission, and processing [15]. The threats associated with the different states are: threats to data confidentiality or privacy, threats to data integrity, threats to user authenticity, threats to availability, threats to storage, and threats to data transmission [15].

The confidentiality of patient data becomes a concern as healthcare professionals continue to transmit or share patient health information by relying on internet-based technologies. The privacy of the patient is always affected should such confidential information be disclosed. Effective access control is crucial in order to protect sensitive patient health information from unauthorized access. Established conventional authentication methods are known to have inherent vulnerabilities. Passwords, which can easily be compromised, thus making health data only as secure as the password is not a reliable security scheme. Password-based smart cards are a good example of that case.

In wireless healthcare, that is wireless sensor networks (WSN), it is essential to ensure secure communication among biosensors in order to protect the vital physiological data collected from patients. Communication within such an environment requires there to be confidentiality, integrity and authenticity of the data being communicated between the patient and the physician or medical center. Encryption helps to secure the transmitted data. However, there are some key factors that need to be considered such as encryption method, key generation, and key distribution, as the biosensors are resource constrained [16].

4 Biometrics in e-Health

Biometrics is increasingly gaining recognition within the healthcare environment as pressure increases on healthcare providers to reduce fraud, to provide secure access to medical records and facilities, to reduce costs, and to facilitate easier access to medical records [17]. The adoption of biometrics in healthcare goes along with the adoption of Electronic Health Record (EHR) systems as EHR makes the use of biometrics more efficient and effective [18]. As a consequence of

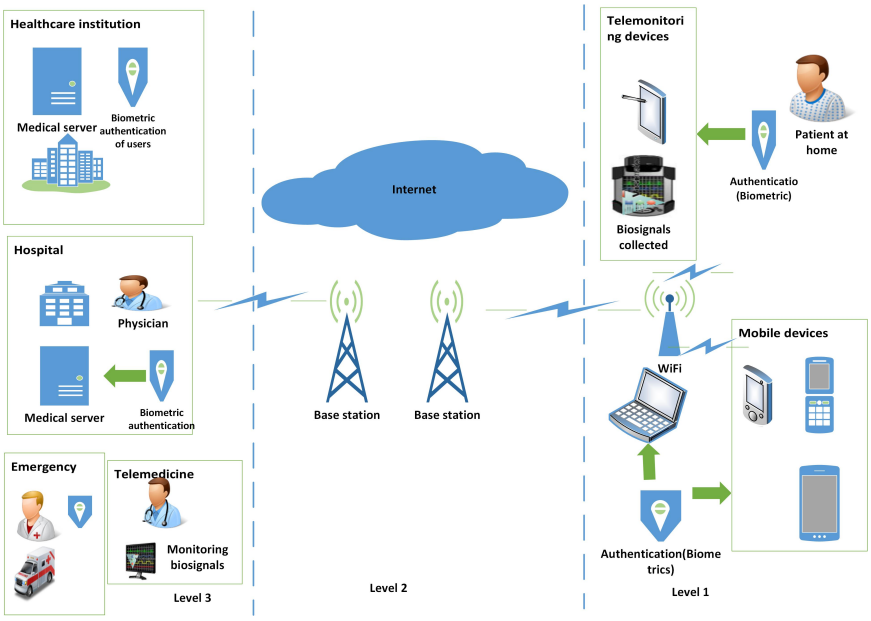

Fig. 1. System architecture of e-Health leveraging on biometric technology.

the adoption of EHR, it is now easy for health professionals to view or tamper with patient records [19]. A secure authentication system in the form of biometric technologies, traits, or identifiers has been adopted by most healthcare organizations to meet the challenges for protecting patient privacy [19].

The current nature of biometrics technology adopted within the healthcare industry is based on physiological characteristics and multi-modal biometric systems, most of which are concerned with one-time verification [20]. Traditional biometric traits include fingerprints and iris patterns, which are considered to be static [21]. However, in recent times other potential biometric modalities have been studied within the healthcare industry based on biosignals [20]. The signal attributes of these modalities are time-varying, and thus dynamic. Within the medical setting, these biometric modalities, i.e. biosignals, are accessible and readily available as they have already been assessed as part of patient follow-up.

The biometric data of a patient or physician is used for authentication in order to access healthcare information. It provides a convenient authentication mechanism that removes the need to memorize long or complex passwords or PINs. As such, it is ideal for elderly people, especially those with mental disorders, and unconscious patients. In Fig. 1 level 1 is made up of all devices that form a network that helps to collect and transmit data from patients, or to gain access to health information by a consumer. The devices include medical sensors, mobile phones, and computers. Level 2 represents the main communication infrastructure that connects level 1 to level 3. Level 3 consists of those

elements that deal with healthcare provision, the storage of health information, and telemedicine. In levels 1 and 3, patient or physician biometric data is used to provide authentication in order to gain access to health information.

Biosignals are ideal for a continuous biometric process, as they do not interfere with the regular tasks performed by the user [20]. Some of the biosignals that have received a lot of attention in terms of research are: electrocardiogram (ECG), electroencephalography (EEG), and photoplethysmography (PPG). An ECG is a diagnostic tool that measures and records the electrical activity of the heart in detail [22]. An EEG is a signal that represents the sum of the electrical activity of the functioning human brain [23]. PPG is a simple and low-cost optical technique that can be used to detect blood volume changes in the microvascular bed of tissue [24].

Other studies on ensuring e-Health security through the use of biometrics have been carried out in terms of authentication, data integrity, data confidentiality, and data authenticity. Data integrity, confidentiality, and authenticity may be achieved through biometric encryption. In a wireless Body Sensor Networks (BSN), sensors rely on biometric encryption for secure communication. BSNs consist of interconnected devices or sensors implanted in or worn on the human body in order to share information and resources. BSNs help provide healthcare services such as medical monitoring, memory enhancement, control of home appliances, medical data access, and communication in emergencies [32].

Through encryption, access to sensitive information is restricted, and thus protecting health information. An important aspect of biometrics cryptography is the use of biometrics to generate cryptographic keys. Biometrics are also used to generate authentication keys for data transmission in wireless communication [29]. The dynamic biometric traits are good for generating keys as a result of their randomness and time variance [29]. Several studies have proposed the use of dynamic biometric features such as ECG [25], [26], [27], [28], [29], and PPG [31] to generate keys for biometrics cryptosystems.

Specifically, in [29] the authors propose a biometric-based solution that combines encryption and authentication for wireless communication in BSNs. Similarly, the authors of [26] propose a biometric-based approach to ensuring secure communication in BSNs by employing biometrics to generate keys. The authors use physiological features such as ECG or PPG to generate cryptographic keys communicated within the network, thereby ensuring security. Usually, proposed methods extract features such as Interpulse Interval (IPI) from ECG or PPG in the time domain or in the frequency domain using Fast Fourier Transform (FFT). In order to provide a strong cryptosystems, the quality of the generated keys must be taken into consideration.

Two features are used to determine the quality of the generated keys: randomness and distinctiveness [33]. Distinctiveness determines if the keys generated can distinguish between different people. Metrics used to evaluate distinctiveness are FAR, FRR, and Hamming Distance(HD). Randomness ensures that the distinctive keys are unpredictable. Randomness is evaluated by computing the entropy of the keys generated. Table 2 shows a comparison in terms of distinctiveness

Table 2. A comparison of research contributions that use biometric traits (static or dynamic) to generate keys for authentication and encryption.

Study	Data size	Biometric trait	Key length (bits)	Distinctiveness –	Method of Distinctiveness	Randomness –	Method of Randomness	Sampling rate (Hz)
[25]	84	ECG	128	Mean(HD)=64	HD	Mean Entropy> 0.99	Entropy	250
[26]	79	ECG	128	Mean(HD)=64	HD	Mean Entropy> 0.99	Entropy	250
[27]	11	ECG	-	FAR almost zero(0) when Threshold above 5; FRR almost zero(0) when Threshold <12	FAR/FRR	FAR almost zero(0) when time variance >125	Time variance	125
[28]	-	ECG	128	FAR almost zero(0) when Threshold above 5; FRR almost zero(0) when Threshold <15	FAR/FRR	–	Time variance	–
[29]	9	ECG and PPG	64 and 128	–	HD	0.662 - 1	Entropy	1000
[29]	20	Fingerprint	64 and 128	–	HD	0.928 – 1	Entropy	–
[30]	31	ECG	128	Average(HD)=64	HD	0.996 - 1	Entropy	125
[31]	10	PPG	128	FRR almost zero (0) when Polinormial order(v) <4; FAR almost zero (0) when Polinormial order >11	FAR/FRR	–	–	60

and randomness of research contributions explored in this study. In Table 2, the "data size" represents the number of subjects from which the biometric features were generated, the key length represents the length of the generated keys in bits, and the sampling rate refers to the frequency (the number of times per second the biosignals are sampled).

5 Discussion and Future Vision

Biometrics technology has proven to provide a sure way of addressing the above e-Health security issues. In this context, the technology is used to provide identity verification, as well as encryption during exchange or transmission of health information. The use of biometrics encryption provides a secure means of protecting health information from attacks such as eavesdropping, data modification, and replay. It is evident that biometrics afford the healthcare industry several promising opportunities. As technology continues to advance, so do security and privacy issues that continue to be a major concern in the industry. To this end, biometrics have been shown to be efficient and robust in tackling security and privacy challenges in e-Health.

On the other hand, biometrics is not a silver bullet in that it cannot provide complete and enough reliable solutions to all security problems [34]. In spite of the robustness of biometrics, it still suffers from several attacks due to the inherent weaknesses that exist in a biometric-based authentication systems. Attacks on biometric templates could lead to vulnerabilities including the replacement of templates by an imposter to gain access, the spoofing of templates by an adversary to gain access, and the replay of attacks. Biometrics templates, when compromised, are impossible to replace as they are permanently linked to an individual. Therefore, the cancelable biometrics concept should be considered.

The total processing time (identification or verification time) is a crucial issue in any biometric system [35]. Biometric-based systems include many subprocesses such as enhancement or noise removal, feature extraction, feature matching, and classification. Attention should be given to the system's time consumed, feature extraction operations, and the large database classification, should be considered [36], [37].

Data encryption has received a lot of attention in healthcare. This is due to the fact that e-Health is pushing the frontiers of healthcare from health institutions to the home (mobile health, telemedicine, etc.), leveraging wireless communication. In any cryptographic system, key generation is vital for secure communication. In this, biometrics is increasingly proving to be very efficient and effective in cryptosystems in encrypting and decrypting sensitive information. Dynamic biometric features such as ECG, PPG, and EEG are useful in generating keys for encryption due to their randomness and time-variance [29]. This has resulted a number of research proposals regarding these aspects.

Future research may take many promising directions. First of all, future research should explore the potential benefits and limitations associated with the use of biometrics in cryptosystems in e-Health, such as, for instance, the con-

straints encountered in the generation and distribution of keys in wireless communication networks, or the strengths and weaknesses of the various biometric traits in key generation. Secondly, future research should continue to investigate how to provide robust authentication mechanisms in e-Health applications or systems using biometrics without undermining user access. Furthermore, there is a high demand for research on the adoption of biometric identification and verification systems for elderly people. The factors that influence the adoption of specific forms of authentication mechanisms in e-Health, as well as the implications of authentication mechanisms on the entire e-Health system, are interesting future research directions.

6 Conclusions

This paper has explored various literatures to determine the impact of using e-Health on the healthcare industry in terms of the benefits it affords to the industry as well as the challenges it poses. Patient e-Health data security and patient privacy are of the utmost concern in the domain of e-Health. Traditional authentication mechanisms, such as passwords and access cards, are not appropriate for addressing the current e-Health security and privacy issues due to their susceptibility to be lost, duplicated, or forgotten. Biometrics technology has proven to effectively address e-Health security and privacy challenges. Various forms of biometrics technology have been proposed in e-Health applications or systems ranging from unimodal to multimodal biometrics, continuous and unobtrusive authentication approaches, and in wireless sensor networks to secure communication channels. In addition, unconventional biometrics biosignals such as electrocardiogram (ECG), photoplethysmography (PPG), and electroencephalography (EEG) open new horizons for biometrics technology deployments in e-Health domain. In spite of all the benefits of using biometrics in e-Health, additional issues such as processing time, patient privacy related to using biometric traits, and biometric database protection should be taken into consideration.

References

1. Sharma, S.K., Xu, H., Wickramasinghe, N., Ahmed, N.: Electronic healthcare: issues and challenges. International Journal of Electronic Healthcare 2(1), 50–65 (2006)
2. Katsikas, S., Lopez, J., Pernul, G.: The challenge for security and privacy services in distributed health settings. Studies in health technology and informatics 134, 113–125 (2007)
3. Jain, A., Hong, L., Pankanti, S.: Biometric identification. Communications of the ACM 43(2), 90–98 (2000)
4. Awad, A.I., Hassanien, A.E.: Impact of some biometric modalities on forensic science. In: Muda, A.K., Choo, Y.H., Abraham, A., N. Srihari, S. (eds.) Computational Intelligence in Digital Forensics: Forensic Investigation and Applications, Studies in Computational Intelligence, Vol. 555, pp. 47–62. Springer International Publishing (2014)

5. Jain, A., Ross, A., Pankanti, S.: Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security 1(2), 125–143 (2006)
6. Jain, A.K., Flynn, P.J., Ross, A.A.: Handbook of biometrics. Springer (2007)
7. Jain, A.K., Ross, A.A.A., Nandakumar, K.: Introduction to biometrics. Springer (2011)
8. Egawa, S., Awad, A.I., Baba, K.: Evaluation of acceleration algorithm for biometric identification. In: Benlamri, R. (ed.) Networked Digital Technologies, Communications in Computer and Information Science, Vol. 294, pp. 231–242. Springer Berlin Heidelberg (2012)
9. Jain, A.K., Bolle, R., Pankanti, S.: Biometrics: Personal Identification in Networked Society. Springer (1999)
10. Sadr, S.M.H.: Consideration the relationship between ICT and ehealth. Journal of Biology, Agriculture and Healthcare 2(8), 49–59 (2012)
11. Eysenbach, G.: What is e-health. Journal of Medical Internet Research 3(2) (2001)
12. Bai, G., Guo, Y.: A general architecture for developing a sustainable elderly care e-health system. In: 8th International Conference on Service Systems and Service Management (ICSSSM). pp. 1–6. IEEE (2011)
13. Ahmed, S., Raja, M.: Integration of wireless sensor network with medical service provider for ubiquitous e-healthcare. In: 9th International Conference on High Capacity Optical Networks and Enabling Technologies (HONET). pp. 120–126 (2012)
14. Mukherjee, S., Dolui, K., Datta, S.K.: Patient health management system using e-health monitoring architecture. In: IEEE International Advance Computing Conference (IACC). pp. 400–405. IEEE (2014)
15. Adibi, S., Agnew, G.B.: On the diversity of ehealth security systems and mechanisms. In: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Vol. 2008, pp. 1478–1481 (2007)
16. Cherukuri, S., Venkatasubramanian, K., Gupta, S.K.S.: Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: International Conference on Parallel Processing Workshops, 2003. pp. 432–439 (2003)
17. Marohn, D.: Biometrics in healthcare. Biometric Technology Today 14(9), 9–11 (2006)
18. Chandra, A., Durand, R., Weaver, S.: The uses and potential of biometrics in health care. International Journal of Pharmaceutical and Healthcare Marketing 2(1), 22–34 (2008)
19. Krawczyk, S., Jain, A.K.: Securing electronic medical records using biometric authentication. In: 5th international conference on Audio- and Video-Based Biometric Person Authentication, AVBPA'05. pp. 1110–1119. Springer-Verlag, Berlin, Heidelberg (2005)
20. Silva, H., Loureno, A., Fred, A., Filipe, J.: Clinical data privacy and customization via biometrics based on ECG signals. In: Holzinger, A., Simonic, K.M. (eds.) Information Quality in e-Health, Lecture Notes in Computer Science, Vol. 7058, pp. 121–132. Springer Berlin Heidelberg (2011)
21. Awad, A.I., Baba, K.: Evaluation of a fingerprint identification algorithm with SIFT features. In: the 3^{rd} 2012 IIAI International Conference on Advanced Applied Informatics. Fukuoka, Japan
22. Baig, M.M., Gholamhosseini, H., Connolly, M.J.: A comprehensive survey of wearable and wireless ECG monitoring systems for older adults. Medical & Biological Engineering & Computing 51(5), 485–495 (2013)

23. Paranjape, R., Mahovsky, J., Benedicenti, L., Koles', Z.: The electroencephalogram as a biometric. In: Canadian Conference on Electrical and Computer Engineering, 2001. Vol. 2, pp. 1363–1366. IEEE (2001)
24. Allen, J.: Photoplethysmography and its application in clinical physiological measurement. Physiological Measurement 28(3), R1–R39 (2007)
25. Zhang, G.H., Poon, C.C., Zhang, Y.T.: Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks. IEEE Transactions on Information Technology in Biomedicine 16(1), 176–182 (2012)
26. Zhang, G., Poon, C.C.Y., Zhang, Y.: A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health. In: 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). pp. 2034–2036 (2010)
27. Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., Chen, D.: OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In: Proceedings of IEEE INFOCOM. pp. 2274–2282. IEEE (2013)
28. Zhou, J., Cao, Z., Dong, X.: BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks. In: Proceedings of the 8th International Conference on Body Area Networks. pp. 488–494. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2013)
29. Zhang, G., Poon, C.C.Y., Zhang, Y.: A biometrics based security solution for encryption and authentication in tele-healthcare systems. In: 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies ISABEL, 2009. pp. 1–4 (2009)
30. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K., et al.: Ekg-based key agreement in body sensor networks. In: INFOCOM Workshops. pp. 1–6. IEEE (2008)
31. Venkatasubramanian, K., Banerjee, A., Gupta, S.K.S.: Plethysmogram-based secure inter-sensor communication in body area networks. In: IEEE Military Communications Conference, 2008. MILCOM 2008. pp. 1–7 (2008)
32. Darwish, A., Hassanien, A.E.: Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors 11(6), 5561–5595 (2011)
33. Poon, C.C.Y., Zhang, Y.T., Bao, S.D.: A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine 44(4), 73–81 (2006)
34. Modi, S.K.: Biometrics in identity management: Concepts to applications. Artech House (2011)
35. Awad, A.I., Baba, K.: Fingerprint singularity detection: a comparative study. In: Software Engineering and Computer Systems. Communications in Computer and Information Science, Vol. 179, pp. 122–132. Springer-Verlag (2011)
36. Awad, A.I., Baba, K.: Toward an efficient fingerprint classification. In: Biometrics - Unique and Diverse Applications in Nature, Science, and Technology, pp. 23–40. InTech (2011)
37. Awad, A.I., Baba, K.: Singular point detection for efficient fingerprint classification. International Journal on New Computer Architectures and Their Applications 2(1), 1–7 (2012)