Securing Healthcare Data Using Biometric Authentication

Sharmin Jahan[1], Mozammel Chowdhury[2](✉), Rafiqul Islam[2], and Junaid Chaudhry[3]

[1] Department of Biochemistry and Molecular Biology,
Jahangirnagar University, Dhaka, Bangladesh
sharmin.biochemist@yahoo.com

[2] School of Computing & Mathematics, Charles Sturt University,
Bathurst, Australia
{mochowdhury,mislam}@csu.edu.au

[3] Security Research Institute, Edith Cowan University,
Joondalup, WA 6027, Australia
j.chaudhry@ecu.edu.au

Abstract. Preservation of privacy and security of healthcare data is very important in the electronic healthcare domain. Unauthorized access or attacks by hackers can breach or damage sensitive data of patients' health records that may lead to disclosure of patient's privacy or may slowdown the system. Hence, it is very crucial to provide and enforce privacy and security of clinical data using a secure authentication system. Biometric-based access control over healthcare data can provide the necessary security and privacy. In recent years, biometric technologies have gained traction in health care applications. This paper proposes a biometric authentication scheme to preserve privacy and security in healthcare systems. In this work, we have employed biometric fingerprint as a trait for user authentication and monitoring access to the healthcare systems.

Keywords: Privacy preservation · Security · Clinical data · EHR

1 Introduction

With the advancement of sophisticated information and communication technology (ICT), both patients and healthcare professionals can access, store and share clinical information electronically in an efficient and easier manner [1]. The emergence of ICT enabled electronic healthcare systems are very compelling for the health industry due to the many advantages. Electronic healthcare systems such as eHealth or tele-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. Recent advances in Electronic Health Record (EHR) technology have significantly increased the amount of clinical data consisting of medical documents and patient health records, that are electronically available and accessible [2].

X. Lin et al. (Eds.): SecureComm 2017 Workshops, LNICST 239, pp. 123–132, 2018.
https://doi.org/10.1007/978-3-319-78816-6_10

Despite many benefits, electronic healthcare systems still face a number of privacy and security challenges [3]. Due to the sensitive nature of medical information and healthcare records, issues of integrity, security, privacy, and confidentiality are significant concerns in this domain. Since medical information is usually associated to individuals, privacy and security must be effectively addressed and ensured to protect patient's health data. This is explicitly stated by the privacy regulations [4–6] to protect the electronic health data that the healthcare institutions maintain about their patients. HIPAA [4] standards for electronic health care information in the USA, address the physical security and confidentiality of patient identifiable electronic health care records. Security and privacy risks involved with archiving and retrieving patient records in the healthcare systems has increased the need for a reliable user authentication scheme to the protection and privacy of medical records in the healthcare domain.

Over the recent years, biometric technologies, such as fingerprint, iris recognition and hand geometry, have gained traction in electronic healthcare applications. Biometrics technology is capable to mitigate the security problems in the electronic healthcare systems by providing reliable and secure user authentication compared to the traditional approaches. Traditional authentication approaches based on user signatures, password, PINs, tokens and access cards are not appropriate in the electronic healthcare systems due to the possibility of being lost, stolen, forgotten, manipulated or misplaced. In general, traditional authentication methods are not based on inherent individual attributes [7]. On the other hand, biometrics is a security mechanism that assigns a unique identity to an individual according to some physiological (fingerprint or face) or behavioral characteristics (voice or gait) [8]. Therefore, biometrics based approaches are more reliable and capable than traditional authentication methods 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 [9]. 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 electronic healthcare systems, healthcare organizations are moving from traditional approaches to the utilization of biometrics technology.

In this paper, we present a biometrics framework based on fingerprint with the potential to extend current data privacy protection and identity verification systems in the context of electronic healthcare systems. In addition, this paper highlights the applications of biometrics in addressing some of the security and privacy challenges in electronic healthcare systems. The remainder of the paper is organized as follows. Section 2 presents an overview of biometrics technology and its applications currently available for healthcare security. In Sect. 3, a description of the proposed approach is provided. We outline the main results and discussions in Sect. 4. Finally, conclusions are documented in Sect. 5.

2 Biometrics Technology in Electronic Healthcare

Biometrics technology serves to identify and authenticate individuals in many security applications based on the physiological, chemical, or behavioral attributes of the individual [10] replacing current password, PIN or token based systems. Like many other application domain, its relevance is increasing in healthcare systems. Using biometrics, the patient, and only the patient, is able to control access to their electronic medical data. With biometric-driven patient control, medical records are no longer held exclusively by providers, but instead shared with authorised providers on an as-needed basis, under the direction of the patient. The privacy and security of medical data is assured via biometric-based verification of authorised individuals, and care is improved through the real-time sharing of centralised medical data that facilitates medical decisions by doctors. Biometrics technology in the healthcare domain can be capable to:

- combat fraud and abuse in health care entitlements programmes;
- protect and help in the management of confidential medical records;
- identify patients; and
- secure medical facilities and equipment.

Biometrics technology can protect the privacy and confidentiality of medical records by means of authentication of both patients and healthcare providers. It can emulate the current well accepted system whereby a patient authenticates herself when seeking treatment or visiting a doctor's office for consultation. A typical scenario consists of a patient telling his or her name to a receptionist and then signing a release form. In order to meet the guidelines of the HIPAA regulations, both health professionals and patients must be given access to medical records. Taking into account the requirements of both patients and health professionals, biometric authentication is able to meet the privacy requirements.

Biometric-based applications are chiefly intended to solve two main categories of problems: solutions that secure against nefarious individuals via intelligence background checks or law enforcement database checks (1:N searches); and solutions that protect a transaction and its associated data by verifying the identity of the individual performing the transaction (1:1 verifications). Healthcare biometric solutions fit in the second category, a type of commercial transaction that requires a 1:1 verification. In the healthcare domain, biometric verification can be used at the following principal access control points of a patient-centric solution:

- Patient verification on login
- Patient verification upon appointment arrival
- Provider verification on login.

Several organizations have employed biometrics for securing their electronic medical records (EMRs) that use modalities such as the fingerprint and iris [11–13]. Researchers have recently studied to employ new types of biometric traits for identification such as, heart rate variability (HRV) [14], interpulse interval (IPI) [15], features of electrocardiogram (ECG) [16] and photoplethysmogram (PPG) [17]. They have proposed approaches using HRV or IPIs as biometric characteristics to generate identity for authentication and encryption [13, 14, 18, 19]. Several data encryption schemes have been proposed based on ECG [16, 20, 21], PPG [17] and multiple physiological signals [22]. Clancy et al. [23] suggested that fingerprint can be used to generate keys for cryptosystems in electronic healthcare platform.

In Europe, the use of biometrics in the health area is still scarce. Presently most applications are restricted to access control and limited to fingerprints and iris scans, but several pilot projects have been initiated to widen the scope. Danish Biometrics, for example, is developing a biometric recognition solution for secure log-on procedures for doctors and nurses at the Copenhagen Hospital. In Germany, where a nationwide eHealth infrastructure is being introduced, doctors will be able to digitally sign prescriptions using fingerprints. In an Italian health care location, a biometric system controls the access to the surgical rooms [24]. In Texas, USA, a biometric and smart card-based program to address recipient and provider fraud in the Medicaid system has been in operation since 2004. The Medicaid Integrity Pilot, or MIP, was initially designed to evaluate the performance and acceptance of fingerprint and smart card technologies for recipient authentication at the point of service [25].

The Australian Methadone program uses iris recognition technology in support of the treatment of citizens addicted to heroin. The Methadone program registers patients in an iris recognition system to detect duplicate enrolees and to enable authentication for clients unable coherently or consistently to claim an identity. Personal information including biometric data, name, permitted dosage, last dosage, and next scheduled dosage are included in the database. A similar pilot program for the controlled distribution of methadone has been deployed in the Netherlands using fingerprint technology and smart cards. One can envision similar uses of biometrics to automate and control distribution of vaccines during epidemics [26].

South African government launched a pilot fingerprint identification program for government employees in response to growing health care concerns due mainly to the HIV/AIDS epidemic. In the past, individuals tended to steal identification cards to receive health care benefits, and many enrolled under multiple identities to receive additional, or replicate, services. The system was designed to detect multiple users at enrolment and to verify a user's identity when they seek services. The system allows patients and medical providers to interact with various settings of care, including hospitals and pharmacies, to prevent fraud and to manage the administration of health care benefits. This system can also track health histories to monitor the overall costs associated with disease treatment [25].

3 Proposed Biometric Authentication System

This section demonstrates the architecture of the proposed biometric authentication system to control access to an electronic healthcare system. A fingerprint biometric scheme can either verify or identify of an individual based on his or her fingerprint as trait. In verification approach, it verifies the authenticity of one person by his fingerprint. In identification approach, it establishes the person's identity among those enrolled in a database. Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. Among all other biometric traits, fingerprint biometrics occupies an important and a very special place in the field of health security due to its uniqueness and availability. The diagram of a proposed biometric system is shown in Fig. 1.

3.1 Fingerprint Acquisition

The first stage of the fingerprint authentication process is to capture a digital image of the fingerprint pattern using a sensor. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezo resistive, ultrasonic, piezoelectric [27].

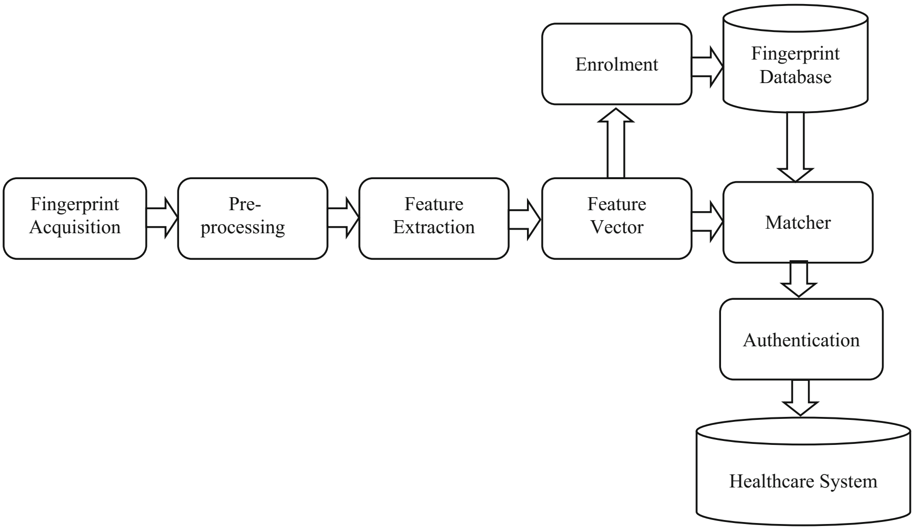


Fig. 1. Architecture of the proposed biometric authentication scheme for electronic healthcare.

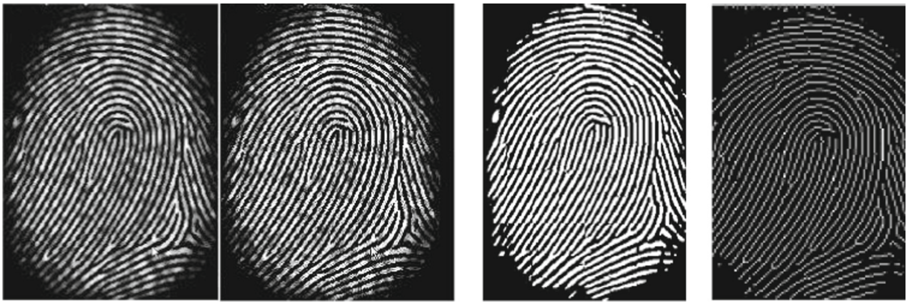
3.2 Pre-processing

Pre-processing is required to enhance the quality of an image by filtering and removing unnecessary noises because the captured images may be of poor quality. This process removes the noises in the images and enhance them for better features extraction. For image filtering we employ a fuzzy filtering technique [28] (Fig. 2).

3.3 Features Extraction

Based on the features used, fingerprint verification methods can be classified into two categories: minutiae based or texture based. The minutiae based fingerprint verification systems have shown high accuracy [29]. The texture based methods use the entire fingerprint image or local texture around minutiae points [30]. In this paper, we employ the minutie features for fingerprint identification.

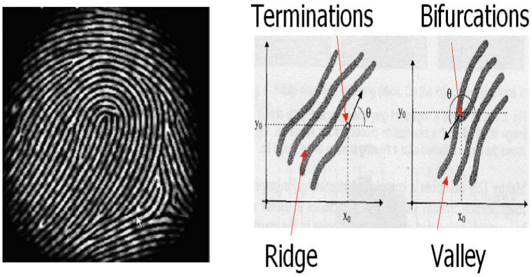
Minutiae are some specific points in a fingerprint, these are the small details in a fingerprint that are most important for fingerprint recognition. There are three major types of minutiae features: the ridge ending, the bifurcation, and the dot (also called short ridge) (Fig. 3). The ridge ending is the spot where a ridge ends. A bifurcation is



(a) Original image (b) Filtered image (c) Binarized image (d) Thinned image

Fig. 2. Pre-processing steps in fingerprint identification.

the spot where a ridge splits into two ridges. Spots are those fingerprint ridges that are significantly shorter than other ridges [31]. Minutia keypoints are searched over a enhanced, binarized and thinned version of the input fingerprint image. The local orientation for each minutia keypoint is obtained from the estimated orientation field. To extract the minutiae set, the open FVS library is used [32].



(a) A fingerprint (b) Minutia

Fig. 3. A fingerprint image and its minutia.

3.4 Matching

A fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Most fingerprint-matching algorithms adopt one of four approaches: image correlation, phase matching, skeleton matching, and minutiae matching. Minutiae-based representation is commonly used, primarily because minutiae-based fingerprint matching is more reliable and acceptable by the forensic experts and other security professional and its representation is storage efficient.

In this paper, we employ the Matching Score Matrix (MSM) algorithm [33] to compare the minutiae features extracted from the test fingerprints with features of database fingerprints to verify a person. The Matching Score Matrix algorithm is able to reduce the number of matching comparisons in linear search. The main idea of the algorithm is that the similarity (called the matching score) between any pair of the finger templates is calculated in advance, and then the order of the comparison with the input image is decided according to the matching scores.

4 Experimental Evaluation

In this section, we evaluate the performance of our proposed approach and compare with other similar techniques reported in this work. To demonstrate the effectiveness of our algorithm, we perform experiment using several standard fingerprint datasets. Experiments are carried out on a computer with 2.8 GHz Intel Core i7 processor. The algorithm has been implemented using Visual C++.

4.1 Datasets

The performance of the proposed fingerprint biometric verification scheme has been evaluated on FVC2002 fingerprint databases [33]. FVC2002 project has four different databases: DB1, DB2, DB3 and DB4. Each database has 110 fingers with 8 impressions per finger (110 × 8 = 880 fingerprints in all); The fingers are split into set A (100 fingers − evaluation set) and set B (10 fingers − training set). During a session, fingers were alternatively dried and moistened. Some characteristics of these two databases are summarized in Table 1.

Table 1. Description of FVC 2002 databases.

Database	Sensor type	Image size	Set A (Testing) (fingers × images)	Set B (fingers × images)	Resolution
DB1	Optical sensor	388 × 374	100 × 8	10 × 8	500 dpi
DB2	Optical sensor	296 × 560	100 × 8	10 × 8	569 dpi
DB3	Capacitive sensor	300 × 300	100 × 8	10 × 8	500 dpi
DB4	Synthetic	288 × 384	100 × 8	10 × 8	About 500 dpi

4.2 Results

To justify the performance of the proposed scheme, we evaluate three statistical measures: False Match Rate (FMR), False Non-Match Rate (FNMR) and Equal Error Rate (EER). The FMR is the rate at which the system incorrectly matches or accepts imposter fingerprint inputs (also known as False Acceptance Rate or FAR). FNMR is the rate at which inputs of genuine fingerprint are incorrectly rejected by the system (also referred as False Rejection Rate or FRR). EER is the rate at which both FMR and FNMR are equal. EER determines the threshold values for FMR and FNMR of the biometric system. When the rates are equal (FMR = FNMR), the common value is referred to as the equal error rate. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the EER value, the higher the accuracy of the biometric system. The results for EER using different fingerprint databases are reported in Table 2. We compare the accuracy of our method with another standard method [35]. Our evaluation results confirm that the number of matching processes is reduced and the error rate for identification is reduced by the proposed method. From the experimental results, we can see that the proposed method is superior to the conventional minutiae-based one for all the databases. Even though the performances for FVC 2002 DB3 and DB4 are lower than those for FVC 2002 DB1 and DB2.

Table 2. EER comparisons of two matching methods on FVC databases.

Database	FISiA [35]	Proposed method
DB1	1.0%	0.26
DB2	0.89%	0.19
DB3	1.7%	0.87
DB4	2.3%	1.2

5 Conclusion

Biometrics can be incorporated in a wide-range of health care applications. Driven by the desires of healthcare authorities to offer better healthcare services at a low cost, electronic healthcare has revolutionized the healthcare industry. However, while electronic healthcare system comes with numerous advantages that improve health services, it still suffers from security and privacy issues in handling health information. eHealth 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 research offers a comprehensive biometrics authentication scheme in order to protect unauthorised access to the healthcare system and preserve its privacy and security.

References

1. Jahan, S., Chowdhury, M.M.H.: Assessment of present health status in Bangladesh and the applicability of e-health in healthcare services: a survey of patients' expectation toward e-health. World J. Comput. Appl. Technol. **2**(6), 121–124 (2014)
2. Martínez, S., Sánchez, D., Valls, A.: A semantic framework to protect the privacy of electronic health records with non-numerical attributes. J. Biomed. Inform. **46**, 294–303 (2013)
3. Fernández-Alemán, J.L., et al.: Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. **46**, 541–562 (2013)

4. HIPAA 1996: US Department of Health & Human Services. https://www.hhs.gov/sites/default/files/privacysummary.pdf
5. EU Directive 95. http://www.dataprotection.ie/docs/EU_Directive_95/46/EC_Chapter1/92.htm
6. The Department of Health, Australian Government. PCEHR: Personally Controlled Electronic Health Record System Operator: Annual Report 2012–2013
7. Chandra, A., Durand, R., Weaver, S.: The uses and potential of biometrics in health care: are consumers and providers ready for it? Int. J. Pharm. Healthc. Mark. **2**(1), 22–34 (2008)
8. Chowdhury, M., Islam, R., Gao, J.: Robust ear biometric recognition using neural network. In: IEEE Conference on Industrial Electronics & Applications, ICIEA 2017, Siem Reap, Cambodia (2017)
9. Zhang, D., Campbell, J.P., Maltoni, D., Bolle, R.M.: Special issue on biometric systems. IEEE Trans. Syst. Man Cybern. Part C **35**(3), 273–275 (2005)
10. Wayman, J.L., Jain, A.K., Maltoni, D., Maio, D.: Biometric Systems: Technology. Design and Performance Evaluation. Springer, London (2005). https://doi.org/10.1007/b138151
11. A4 Health Systems: A4 Health Systems Electronic Medical Record Solutions. http://www.a4healthsystems.com/
12. BCBSRI: Blue Cross Blue Shield of Rhode Island. https://www.bcbsri.com
13. University of South Alabama Health System. http://www.southalabama.edu/usahealthsystem/
14. Bao, S.D., Zhang, Y.T., Shen, L.F.: Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In: 27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEEEMBS 2005, pp. 2455–2458 (2005)
15. Poon, C.C.Y., Zhang, Y.-T., Bao, S.-D.: A novel biometrics method to secure wireless body area sensor networks for telemedicine and mhealth. IEEE Commun. Mag. **44**(4), 73–81 (2006)
16. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: ECG-based key agreement in body sensor networks. In: INFOCOM Workshops 2008, pp. 1–6. IEEE (2008)
17. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.: Plethysmogram-based secure inter-sensor communication in body area networks. In Military Communications Conference, MILCOM 2008, pp. 1–7. IEEE (2008)
18. Bao, S.D., Poon, C.C.Y., Shen, L.F., Zhang, Y.T.: Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Trans. Inf. Technol. Biomed. **12**(6), 772–779 (2008)
19. Bao, S.D., Shen, L.F., Zhang, Y.T.: A novel key distribution of body area networks for telemedicine. In: 2004 IEEE International Workshop on Biomedical Circuits and Systems, pp. 1–17–20a (2004)
20. Bui, F.M., Hatzinakos, D.: Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling. EURASIP J. Adv. Signal Process. **13**, 3142–3156 (2008)
21. Challa, N., Cam, H., Sikri, M.: Secure and efficient data transmission over body sensor and wireless networks. EURASIP J. Wirel. Commun. Netw. **3**, 707–710 (2008)
22. Cherukuri, S., Venkatasubramanian, K.K., Gupta, S.K.S.: BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: Proceedings of the 2003 International Conference on Parallel Processing Workshops, pp. 432–439 (2003)
23. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure smartcard-based fingerprint authentication. In: Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. ACM, Berkley (2003)

24. Biohealth Newsletter, vol. 5, December 2007. http://biohealth.gsf.de
25. Marohn, D.: Biometrics in healthcare. Biometr. Technol. Today **14**, 9–11 (2006)
26. DOH: Review of Methadone treatment in Australia. http://www.health.gov.au/internet/main/publishing.nsf/content/phd-illicit-review-of-methadone-treatment
27. Jain, A.K., Feng, J., Nandakum, K.: Fingerprint matching. IEEE Comput. Mag. **43**, 36–44 (2010)
28. Chowdhury, M., Gao, J., Islam, R.: Fuzzy logic based filtering for image de-noising. In: IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2016, Vancouver, Canada, pp. 2372–2376
29. Jain, A.K., Hong, L., Bolle, R.: On-line fingerprint verification. IEEE Trans. Pattern Anal. Mach. Intell. **19**, 302–314 (1997). ISSN 0162-8828
30. Chikkerur, S., Pankanti, S., Jea, A., Ratha, N., Bolle, R.: Fingerprint representation using localized texture features. In: Proceedings of ICPR 2006, August 2006, pp. 521–524. IEEE Computer Society, Hong Kong (2006). ISSN 1051-4651
31. Zhao, F., Tang, X.: Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. Pattern Recognit. **40**(4), 1270–1281 (2007)
32. FVS 2003: Fingerprint Verification System. http://fvs.sourceforge.net
33. Maeda, T., Matsushita, M., Sasakawa, K.: Identification algorithm using a matching score matrix. IEICE Trans. Inf. Syst. **1**(7), 819–824 (2001)
34. FVC 2002 Fingerprint Database. http://bias.csr.unibo.it/fvc2002/
35. Zhou, R., Zhong, D., Han, J.: Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching. Sensors **13**, 3142–3156 (2013). https://doi.org/10.3390/s130303142