iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XI **Month of publication:** November 2019

DOI: http://doi.org/10.22214/ijraset.2019.11046

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XI, Nov 2019- Available at www.ijraset.com

User Authentication Model for Securing E-Health System using Fingerprint Biometrics

Lazarus Kwao[1], Wisdom Xornam Ativi[2], James Ben Hayfron-Acquah[3], Joseph Kobina Panford[4]
[1]*Ghana Baptist University College, Kumasi*
[2]*University of Education Winneba, Ghana*
[3, 4]*Department of Computer Science, KNUST, Kumasi, Ghana*

Abstract: ***The emergence of electronic health or eHealth has revolutionized the healthcare industry to offer better healthcare services at a low and affordable cost. However, it still suffers from security and privacy issues in handling health information. The privacy and security issues in eHealth domain are mainly centered around user authentication, data integrity, data confidentiality, and patient privacy protection. Biometrics technology has considerable opportunities to cope with the above security problems by providing reliable and secure user authentication. However, due to the sensitive nature of health data, the most important challenge lies toward the development of an efficient security model that can guarantee data privacy and reliability, verifying that only authorized personnel can access their corresponding health data. In this paper, we present a comprehensive overview of biometrics applications in eHealth and propose a robust and efficient scheme for user verification using fingerprint biometrics in order to enhance privacy and security in eHealth information systems. Moreover, additional issues like system complexity and processing time related to the use of biometrics should be taken into consideration. We therefore, emphasize to reduce the computation cost in biometric matching. In this work, we use local minutie features for user authentication and employ a fast stereo matching algorithm to compare the minutiae features of the test (probe) fingerprint with the minutiae features extracted from the gallery fingerprints (fingerprint database) in order to verify a person. Experimental results show that the proposed scheme leads to a compromise between the computation efficiency and the accuracy of the verification process. We believe that, our proposed scheme could be employed in real-time applications.***
Keywords: Biometrics; fingerprint verification; user authentication; access control; security and privacy; eHealth

I. INTRODUCTION

In recent years, eHealth has proved to be considered as one of the impulsive developments in the healthcare industry. Health information technology, especially electronic health records (eHR), has the potential to improve the quality and effectiveness of healthcare services [1–3]. eHR is the digitally stored health care information about an individual's lifetime with the purpose of supporting continuity of care, education, and research, and ensuring confidentiality always [4]. eHealth can be defined as the transfer of health resources and health care through electronic media [5]. The World Health Organization (WHO) defines eHealth as the combined use of electronic communication and information technology in the health sector [6]. eHealth has proved to be very compelling for the health industry to improve the quality of healthcare by making health information easily accessible, improving efficiency, and reducing the cost of health service delivery.

Despite the benefits of eHealth, it still faces a number of security challenges. eHealth security issues include the preservation of eHealth data confidentiality, data integrity, data availability, user authentication, and patient privacy protection [7]. Among the eHealth issues, data security and patient privacy stand out as the prime concerns that need to be addressed during implementation.

Preservation of the privacy and security in the eHealth systems involves securing eHealth applications and their communication components. The underlying issue that is particularly important in relation to the security requirements of eHealth is the user authentication and authorization. Authentication considers a significant element of security in the healthcare domain, aiming to verify a user's identity when a user wishes to request services from the cloud. Traditional authentication approaches such as user name, password, and access cards are not appropriate in the eHealth context due to the possibility of being lost, stolen, forgotten, or misplaced. In general, traditional authentication methods are not based on inherent individual attributes [8].

On the other hand, biometric technologies, such as fingerprint, iris recognition, and hand geometry, have gained traction in health care applications. 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) [9]. 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 [10]. 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 eHealth, healthcare organizations are moving from traditional approaches to the utilization of biometrics technology.

To mitigate the aforesaid eHealth issues, this paper seeks to embark on a review to highlight the applications of biometrics in addressing the eHealth security and privacy challenges. Our research focus is on biometrics applications in user authentication and access control over electronic health data. In this paper, we present a robust 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. The main contributions of this article include the following:

1) We propose a robust and efficient biometric scheme for user verification and access control in electronic healthcare system to ensure the security and privacy.

2) We use fingerprint biometric modality for user verification, since the fingerprint biometric occupies an important and a very special place in the field of health security due to its uniqueness and availability. User verification is performed by analyzing the minutie features of the fingerprint biometrics.

3) A fast stereo matching algorithm is used for match-ing the features of the test fingerprint with the features of the fingerprint database to verify the user, which is efficient in achieving a substantial accuracy with less computation time. We believe that, our proposed algorithm is suitable for real-time applications.

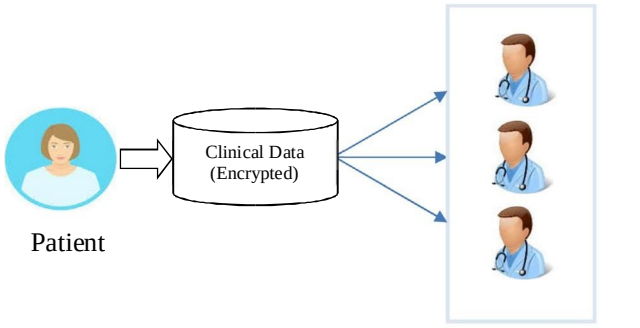


Figure 1. a patient-centric electronic healthcare model.

The remainder part of this paper is structured as follows: Section 2 presents an overview on biometrics technology for eHealth security. The related works on biometrics methods for eHealth security are described in Section 3. The detail architecture of the proposed biometric authentication scheme to control access to the eHealth records is demonstrated in Section 4. The stereo matching algorithm for fingerprint verification is described in Section 5. Experimental results are reported in Section 6, and finally, conclusions are documented in Section 7.

II. BIOMETRICS TECHNOLOGY IN EHEALTH

Biometrics technology serves to identify and authenticate individuals in eHealth systems. Biometrics technology can protect the privacy and confidentiality of medical records by means of authentication of both patients and healthcare providers [11]. Using biometrics, the patient is able to control access to their electronic medical data. The privacy and security of medical data is assured via biometric-based verification of authorized individuals, and care is improved through the real-time sharing of centralized medical data that facilitates medical decisions by doctors. To meet the guidelines of the HIPAA [12], both health professionals and patients must be given access to medical records. Considering the requirements of both patients and health professionals, biometric authentication is able to meet the privacy requirements. In the healthcare domain, biometric verification can be used at the following principal access control points of a patient-centric solution (shown in Figure 1) by the following ways:

A. Patient Verification on Login

The developer of a patient-centric health data repository must bear the responsibility to protect that data and assure its privacy, while providing necessary access to ensure that patients receive proper care. For patient processing, this can be achieved with biometric solutions that meet the following requirements:

1) Patients can specify the providers with whom their health data should be shared, including the revocation of access.

2) To protect the ability to grant and revoke access to healthcare data, patients must be able to verify themselves biometrically upon login to the centralized data repository. Therefore, a hacker could not gain access to a patient's healthcare data.

B. Patient Verification upon Appointment Arrival

In addition to data access, patient identity verification upon arrival for a doctor appointment has numerous benefits. The most notable benefits include:

1) Patients privacy is protected and improved, eliminating sign-in sheets that list the patient name, doctor's name, and insurance information.

2) With biometric check-in, receptionists are proactively informed of a patient's arrival, actions can be automatically triggered based on the patient's arrival, and 'waiting room time' can be minimized.

C. Provider Verification on Login

A patient-centric solution must meet the following requirements for providers:

1) Providers can only access records for patients who have granted the provider explicit access.

2) Like patients, providers can use biometrics to pro-tect their account (and associated data access privileges) against hacking.

III. RELATED WORKS

Biometrics technology has been employed by many health professionals for securing electronic health records (eHRs) [13–15]. Researchers have recently studied to employ new types of biometric traits for identification such as, heart rate variability (HRV) [16], interpulse interval (IPI) [17], features of electrocardiogram (ECG) [18], and photoplethysmogram (PPG) [19]. They have proposed approaches using HRV or IPIs as biometric characteristics to generate identity for authentication and encryption [15,16,20,21]. Several data encryption schemes have been proposed based on ECG [18,22,23], PPG [19] and multiple physiological signals [24]. Clancy et al. [25] suggested that fingerprint can be used to generate keys for cryptosystems in eHealth platforms.

Iris recognition technology is employed in the Australian Methadone program 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. One can envision similar uses of biometrics to automate and control distribution of vaccines during epidemics [26].

In the 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 [27].

In Africa, 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 where a nationwide eHealth infrastructure is being introduced, doctors will be able to digitally sign prescriptions using fingerprints [28].

IV. PROPOSED AUTHENTICATION SCHEME USING FINGERPRINT BIOMETRIC

This section demonstrates the proposed user authentication scheme using fingerprint biometric to control access to an electronic healthcare system. The motivation behind using fingerprint biometrics in this paper is that, it occupies an important and a very special place in the field of health security among all other biometric traits (e.g. palm, face, ear etc.) due to its several key features such as: unique to individuals availability invariant to age smaller in size reduced spatial resolution and uniform distribution of color. There are two tasks underlying in a fingerprint biometric scheme: (i) verification and (ii) identification of an individual based on his or her fingerprint features. In verification approach, it verifies the authenticity of one person by his or her 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. Figure 2 shows the architecture of the proposed user authentication scheme.

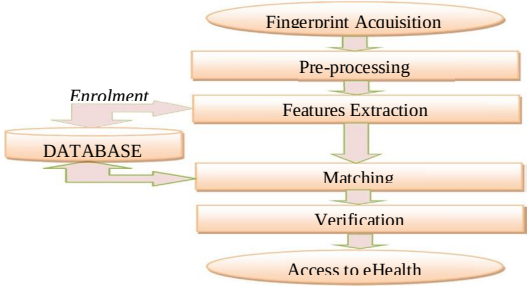


Figure 2. proposed user verification scheme eHealth system using fingerprint biometric.

A. *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 for capturing fingerprint images including optical, capacitive, RF, thermal, piezo resistive, ultrasonic, piezoelectric [29]. The captured fingerprint image is then normalized with a size of 140 × 160.

B. *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 [30]. The filtered image was then binarized and thinned to make it more appropriate for feature extraction. Thinning is a morphological operation that is used to remove selected foreground pixels from binary images. It is used to eliminate the redundant pixels of ridges till the ridges are just one-pixel wide. Thinning is normally only applied to binary images, and produces another binary image as output. It is the final step prior to feature extraction.

C. *Features Extraction*

Based on the features used, fingerprint verification methods can be classified into two categories: minutiae or texture based. The minutiae-based fingerprint verification systems have shown high accuracy [31]. The texture-based methods use the entire fingerprint image or local texture around minutiae points [32]. 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). Figure 3 shows the minutiae features of a fingerprint image. The ridge ending is the spot where a ridge end. A bifurcation is the spot where a ridge splits into two ridges. Spots are those fingerprint ridges that are significantly shorter than other ridges [33]. Minutia keypoints are searched over an enhanced, binarized, and thinned version of the input fingerprint image. The local orientation for each minutia keypoint is obtained from the estimated orientation field. The feature points are normalized to [0, 255]. To extract the minutiae set, the open FVS library is used [34].

D. *Matching and Verification*

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 a stereo matching algorithm [35] to compare the minutiae features extracted from the test fingerprints with features of database fingerprints to verify a person. The main idea of the algorithm is that the similarity (called the matching score) between any pair of the fingerprint templates is calculated, and then the order of the comparison with the input image is decided according to the matching scores.

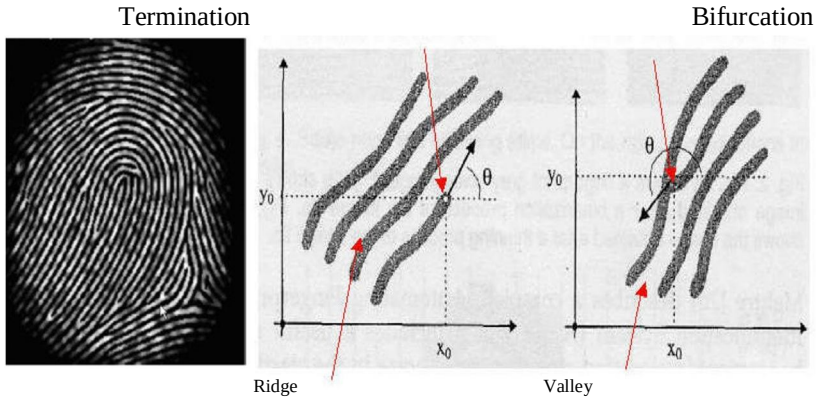


Figure 3. a fingerprint image and its minutia features [33].

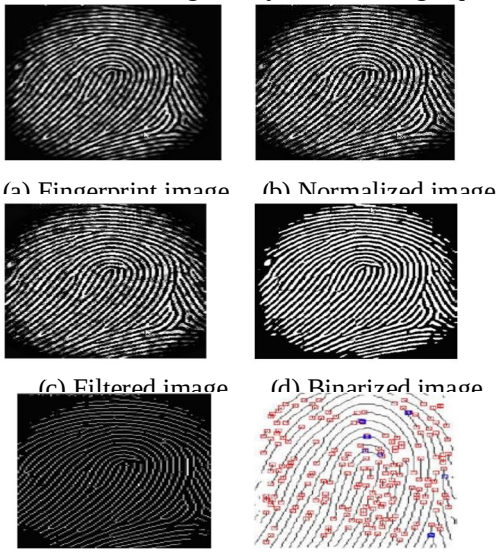
Table 1. description of fVC 2002 databases.

Database	Sensor type	Image size	Set A (fingers × images)	Set B (fingers × images)	Resolution (dpi)
dB1	optical	388 × 374	100 × 8	10 × 8	500
dB2	optical	296 × 560	100 × 8	10 × 8	569
dB3	Capacitive	300 × 300	100 × 8	10 × 8	500
dB4	synthetic	288 × 384	100 × 8	10 × 8	500

V. STEREO ALGORITHM FOR FINGERPRINT MATCHING

The stereo algorithm compares two fingerprint images (test and gallery database) and computes the degree of similarity between the test image and the gallery image and identifies the user's fingerprint that produces the best matching score. Prior to stereo matching, we need to rectify the fingerprint images for their alignment. The test and gallery images are rectified and the similarity score is computed by computing the stereo matching cost (similarity score) of every row of the rectified images. The rectification allows the use of epipolar geometry environment where the epipolar lines are horizontal i.e. parallel to the lines of the image sequences. In epipolar geometry, any point lying on an epipolar line in the reference image (i.e. test image) corresponds to a point lying on the same epipolar line in the target image (i.e. gallery image). After rectification of the two fingerprint images, the matched points have necessarily the same coordinate in the both images. Therefore, in case of searching for corresponding points in two fingerprint images, it is only necessary to search in the same epipolar line, reducing a 2D search space to 1D. In order to achieve rectification, we adopt the algorithm proposed by Fusiello et al. [36].

To determine the correspondences between two images, we match the windows of pixels on the same epipolar lines in the reference (test) and target (gallery) image. In our method, we assume that the pixels surrounded by a window possess approximately equal disparity. Thus, the matching cost C for a key point (x, y) in the test image is estimated by taking a window of pixels centered at (x, y) in the test image, and placing a similar window of pixels centered at $(x + d, y)$ in the gallery image and computing the difference between these two windows using a fuzzy correlation measure given by the following Equation (1).



(a) Fingerprint image (b) Normalized image

(c) Filtered image (d) Binarized image

(e) Thinned image (f) Extracted Minutiae

Figure 4. experimental results for pre-processing steps in the proposed scheme. Here, d is a searching range over the same epipolar line in the gallery image.

$$C(x,y,d) = \frac{\sum_{x,y\in W} F(x,y)\left|I_p(x,y) \times I_G(x+d,y)\right|}{\sqrt{\sum_{x,y\in W} F(x,y) I_p^2(x,y) \times \sum_{x,y\in W} F(x,y) I_G^2(x+d,y)}} \quad (1)$$

where $I_P(x, y)$ and $I_G(x, y)$ are the intensities of the minutia points at position (x, y) in the probe (test) and gallery images, respectively; and W is a square window. $F(x, y)$ is the fuzzy measure corresponding to the pixel at position (x, y), has Gaussian distribution which is proportional to fuzzy membership function:

$$F(x,y) = \exp\left(-\frac{\left|I_P(x,y) - I_G(x+d,y)\right|^2}{2\sigma^2}\right) \qquad (2)$$

where, σ is the standard deviation of all pixels within the window.
The matching cost $C(x, y)$ for every minutia points (x, y) can be computed by the winner-take all strategy such that,

$$C(x,y) = \arg\max C(x,y,d) \qquad (3)$$

In order to authenticate a user, the matching is performed between the fingerprint probe image and the enrolled gallery pattern. A number of iterations is accomplished for matching the probe image with the stored gallery images and thus we obtain different window costs. We pick the best matching scores and estimate a normalized matching cost for every pair of the probe and the gallery fingerprint images, using the following equation:

$$C(I_P, I_G) = \frac{\sum_{i=1}^{n} C(I_{P,i}, I_{G,i})}{\sum_{i=1}^{n} |I_{P,i}| + |I_{G,i}|} \qquad (4)$$

where C is the normalized matching cost for the image pair: the probe and a gallery fingerprint image. Thus, we compute normalized costs for all pair of images by comparing the probe with all gallery images. We then identify the gallery fingerprint image that provides best similarity score given by,

$$S = \max\{C_n(I_P, I_G)\} \qquad (5)$$

where, C_n refers to the normalized cost of nth image pair (the probe and the gallery image), $n = 1 \ldots N$; and N denotes the total number of images considered in the gallery. The best match is considered for identification when, $S > T$. Here, T is a predetermined threshold and is set to 0.7 by empirical evaluation.

VI. RESULTS AND DISCUSSION

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 algorithms have been implemented using MATLAB and Visual C++.
The performance of the proposed fingerprint biometric verification scheme has been evaluated on FVC2002 fingerprint data-set [37]. The data-set has four databases:

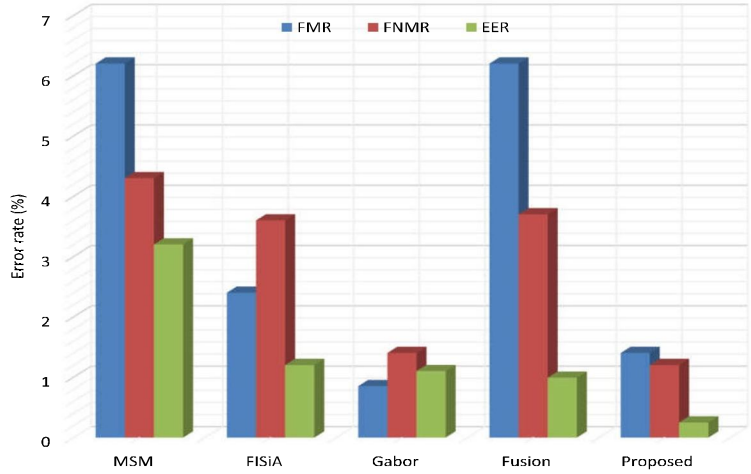


Figure 5. performance comparison of fingerprint matching techniques using dB1 data-set.

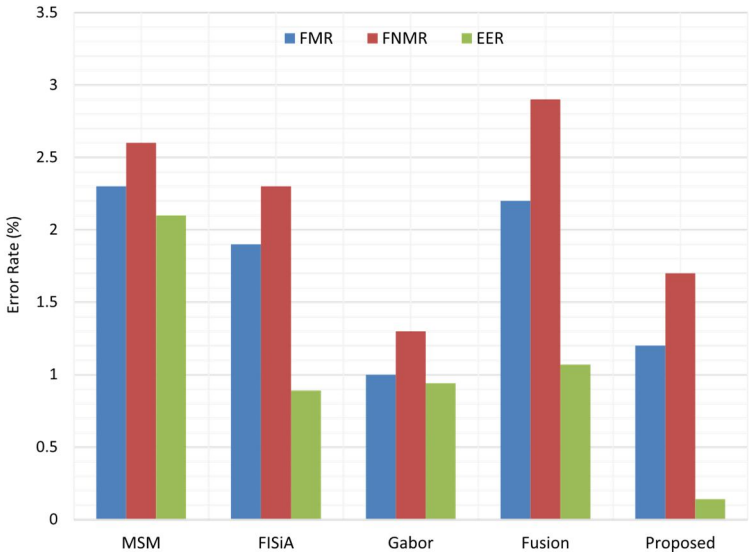


Figure 6. performance comparison of fingerprint matching techniques using dB2 data-set.

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. The features of these databases are summarized in Table 1.

Figure 4 shows the pre-processing results in our proposed scheme. To verify the performance of the proposed algorithm, we compare the accuracy of our method with other similar and recent fingerprint matching algorithms including: MSM [38], FISiA [39], Gabor [40], and Fusion [41]. To justify the performance of the approaches, we evaluate three statistical measures: False Match Rate (FMR), False Non-Match Rate (F NMR), and Equal Error Rate (EER). EER is the rate at which both FMR and F NMR are equal. EER determines the threshold values for FMR and F NMR of the biometric system. 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 accuracy results for FMR, F NMR, and EER with different fingerprint databases are reported in Figures 5–8.

From the experimental results, we can find that the error rate for identification is reduced by the proposed method. Experimental results reveal that the proposed method is superior to other similar techniques in case of all fingerprint databases. It is found that the performances for FVC 2002 DB1, DB3, and DB4 databases are lower than those for FVC 2002 DB2 database. A comparison for average processing time of different matching techniques is reported in Table 2. Results show that in case of all datasets our proposed algorithm requires less computation cost in fingerprint matching.

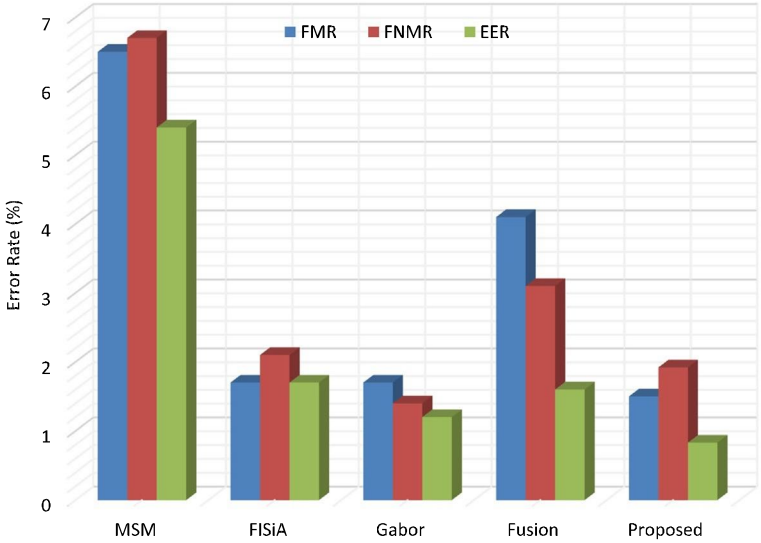


Figure 7. performance comparison of fingerprint matching techniques using dB3 data-set.

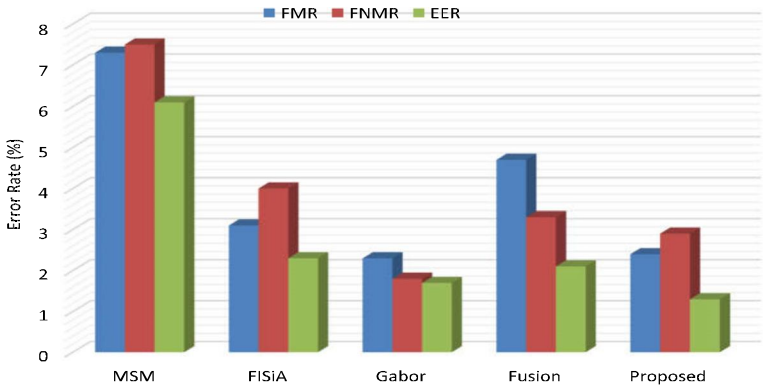


Figure 8. performance comparison of fingerprint matching techniques using dB4 data-set.

Table 2. average matching time comparisons for different methods on fVC 2002 databases.

Data-set	MSM (s)	FISiA (s)	Gabor (s)	Fusion (s)	Proposed (s)
dB1	3.6	1.8	2.3	5.2	0.42
dB2	4.8	2.5	3.1	4.8	0.61
dB3	6.4	3.2	5.4	6.4	1.27
dB4	7.3	4.1	5.9	7.1	1.31

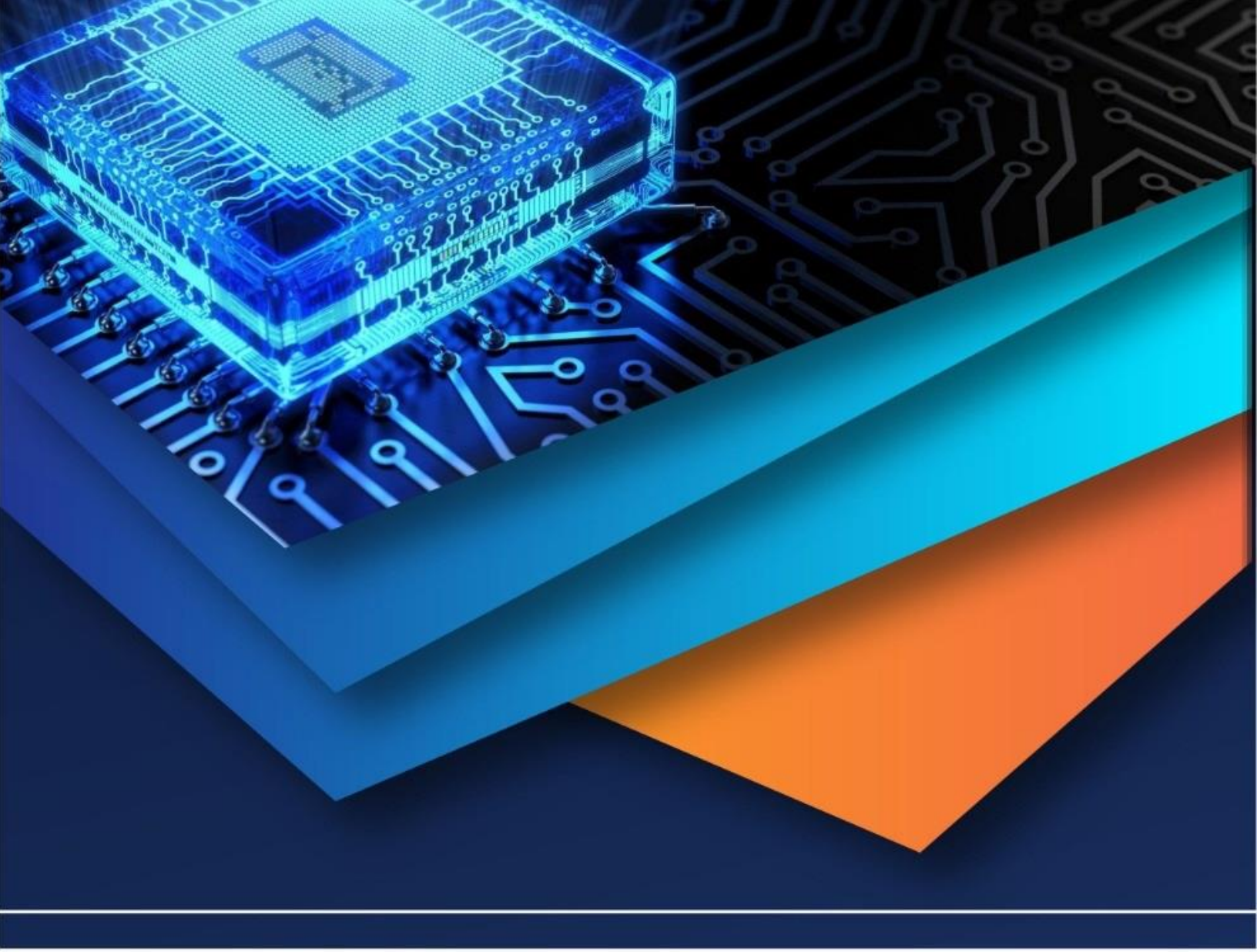
VII. CONCLUSION

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 unauthorized access to the healthcare information system and preserve its privacy and security. In this paper, we propose a robust and efficient scheme for user verification using fingerprint biometrics. We emphasize to reduce the computation cost in biometric matching. In this work, we use local minutiae features for user authentication and a fats stereo matching algorithm to compare the minutiae features of the test (probe) fingerprint with the minutiae features of the gallery fingerprints (enrolled fingerprint database) to verify a person. This leads to a trade-off between the computation efficiency and the accuracy of the verification process. We believe that our proposed scheme is suitable to employ in real-time applications. In future work, we wish to integrate multiple traits for authentication with a view to improve the recognition accuracy and security.

REFERENCES

[1] Ahmed IT. Continuous authentication using biometrics: data, models, and metrics. Hershey, PA: IGI Global; 2012.
[2] Chaudhry B, Wang J, Wu S, et al. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med. 2006;144:742–752.
[3] Blumenthal D, Glaser JP. Information technology comes to medicine. N Engl J Med. 2007;356:2527–2534.
[4] Gajanayake R, Iannella R, Sahama T. Privacy oriented access control for electronic health records. Electron J Health Inf. 2014;8(2):e15. Available from: www.eJHI.net
[5] J ahan S, Chowdhury MMH. 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. 2014;2(6):121–124. USA.
[6] Eysenbach G. What is e-health? J Med Internet Res. 2001;3:1–20.
[7] Martínez S, Sánchez D, Valls A. A semantic framework to protect the privacy of electronic health records with nonnumerical attributes. J Biomed Inf. 2013;46:294–303.
[8] Fernández-Alemán JL, Señor IC, Lozoya PÁ, et al. Security and privacy in electronic health records: a systematic literature review. J Biomed Inf. 2013;46:541–562.

[9] Chowdhury M, Islam R, Gao J. Robust ear biometric recognition using neural network. IEEE Conference on Industrial Electronics & Applications (ICIEA); Siem Reap, Cambodia; 2017.
[10] Ahmed IT. Continuous authentication using biometrics: data, models, and metrics. Hershey, PA: IGI Global; 2012.
[11] Zhang R, Liu L. Security models and requirements for healthcare application clouds. Proceedings of CLOUD'10. Washington, D.C., USA: IEEE; 2010. p. 268–275.
[12] HIPPA. 1996. US Department of Health & Human Services. Available from: https://www.hhs.gov/sites/ default/files/privacysummary.pdf
[13] A4 Health Systems. A4 health systems electronic medical record solutions. Available from: http://www. a4healthsystems.com/
[14] BCBSRI. Blue cross blue shield of Rhode Island. Available from: https://www.bcbsri.com
[15] U niversity of South Alabama Health System. Available from: http://www.southalabama.edu/usahealthsystem/
[16] B ao SD, Zhang YT, Shen LF. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. 27th Annual International Conference of the Engineering in Medicine and Biology Society, 2005. NX Amsterdam, The Netherlands: IEEEEMBS; 2005. p. 2455–2458.
[17] P oon CCY, Zhang Y-T, Bao S-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun Mag. 2006;44(4):73–81.
[18] Venkatasubramanian KK, Banerjee A, Gupta S. "ECGbased key agreement in body sensor networks." INFOCOM Workshops 2008. Hefei, China: IEEE; 2008;. p. 1–6.
[19] Venkatasubramanian KK, Banerjee A, Gupta S. Plethysmogrambased secure inter-sensor communication in body area networks. IEEE Military Communications Conference (MILCOM); Secaucus, NJ, USA; 2008. p. 1–7.
[20] Bao SD, Poon CCY, Shen LF, et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Trans Inf Technol Biomed. 2008;12(6):772–779.
[21] Bao SD, Shen LF, Zhang YT. A novel key distribution of body area networks for telemedicine. 2004 IEEE International Workshop on Biomedical Circuits and Systems; Fukuoka, Japan; 2004. p. 1–17–20a.
[22] Bui FM, Hatzinakos D. Biometric methods for secure communications in body sensor networks: resourceefficient key management and signal-level data scrambling. EURASIP J Adv Signal Proc. 2008;13:3142– 3156.
[23] C halla N, Cam H, Sikri M. Secure and efficient data transmission over body sensor and wireless networks. EURASIP J Wirel Commun Networking. 2008;3:707–710.
[24] Cherukuri S, Venkatasubramanian KK, Gupta SKS. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. Proceedings 2003 International Conference on Parallel Processing Workshops; Orlando, FL, USA; 2003. p. 432–439.
[25] Clancy TC, Kiyavash N, Lin DJ. Secure smartcardbased fingerprint authentication. Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. Berkley (CA): ACM; 2003.
[26] DOH. Review of methadone treatment in Australia. Available from: http://www.health.gov.au/internet/ main/publishing.nsf/content/phd-illicit-review-ofmethadone-treatment
[27] Biometrics in Healthcare. Biometric technology today; Alabama, United States; 2006 Sep. p. 9–11.
[28] Biohealth Newsletter. Vol. 5; 2007 Dec. Available from: http://biohealth.gsf.de
[29] Jain AK, Feng J, Nandakumar K. Fingerprint matching. IEEE Commun Mag. 2010;43:36–44.
[30] C howdhury M, Gao J, Islam R. Fuzzy logic based filtering for image de-noising. IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). Vancouver, Canada; 2016. p. 2372–2376.
[31] J ain AK, Hong L, Bolle R. On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 19; San Diego, CA, USA; 1997 Apr. p. 302–314, 0162–8828.
[32] Chikkerur S, Pankanti S, Jea A. Fingerprint representation using localized texture features. Proceedings of ICPR 2006. Hong Kong, China: IEEE Computer Society. 2006 Aug. p. 521–524, 1051–4651.
[33] Zhao F, Tang X. Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. Pattern Recognit. 2007;40(4):1270–1281.
[34] FVC. 2003. Fingerprint verification system. Available from: http://fvs.sourceforge.net
[35] Chowdhury M, Gao J, Islam R. Fast stereo matching with fuzzy correlation. IEEE Conference on Industrial Electronics & Applications (ICIEA). Hefei, China; 2016.
[36] F usiello A, Trucco E, Verri A. A compact algorithm for rectification of stereo pairs. Mach Vision Appl. 2000;12:16–22.
[37] FVC. 2002. Fingerprint database. Available from: http:// bias.csr.unibo.it/fvc2002/
[38] A wad AI, Baba K. Evaluation of a fingerprint identification algorithm with SIFT features. 2012 IIAI International Conference on Advanced Applied Informatics; Canberra ACT, Australia; 2012. p. 129–132.
[39] Z hou R, Zhong D, Han J. Fingerprint identification using SIFT-based minutia descriptors and improved all descriptor-pair matching. Sensors. 2013;13:3142–3156. doi:10.3390/s130303142.
[40] Liu L, Cao T. The research and design of an efficient verification system based on biometrics. International Conference on Computer Science and Electrical Engineering; Switzerland; 2012.
[41] Park U, Pankanti S, Jain AK Fingerprint verification using SIFT features. Proceeding of SPIE Defense and Security Symposium. Orlando, FL, USA; 2008 Mar 16; paper 6944–19.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY