The Promise of New Technologies in an Age of New Health Challenges
A.J. Maeder et al. (Eds.)

doi:10.3233/978-1-61499-712-2-42

Improving Patient Safety, Health Data Accuracy, and Remote Self-Management of Health Through the Establishment of a Biometric-Based Global UHID

Guy Hembroff
Michigan Technological University, Houghton, United States

Abstract. Healthcare systems globally continue to face challenges surrounding patient identification. Consequences of misidentification include incomplete and inaccurate electronic patient health records potentially jeopardizing patients' safety, a significant amount of cases of medical fraud because of inadequate identification mechanisms, and difficulties affiliated with the value of remote health self-management application data being aggregated accurately into the user's Electronic Health Record (EHR). We introduce a new technique of user identification in healthcare capable of establishing a global identifier. Our research has developed algorithms capable of establishing a Unique Health Identifier (UHID) based on the user's fingerprint biometric, with the utilization of facial-recognition as a secondary validation step before health records can be accessed. Biometric captures are completed using standard smartphones and Web cameras in a touchless method. We present a series of experiments to demonstrate the formation of an accurate, consistent, and scalable UHID. We hope our solution will aid in the reduction of complexities associated with user misidentification in healthcare resulting in lowering costs, enhancing population health monitoring, and improving patient-safety.

Keywords. algorithms, biometrics, health information and safety, telehealth, unique health identifier, national provider identifier

1. Introduction

In recent years we have witnessed healthcare's expansion of electronic medical records (EMRs) [1], electronic health records (EHRs) [2], and personal health records (PHRs) [3], providing an electronic means of access to an individual's health data, such as medical history, insurance information, and demographic data. Likewise, technology continues to advance in the areas of improved hardware, application development, and mobile platforms, such as mobile health applications, creating a potential ubiquitous computing environment for healthcare delivery and monitoring. This progress has led to a paradigm shift from what we have known as traditional healthcare, to a redefinition or an evolution of com-

puting in healthcare. Advancing computer-based healthcare delivery services will only prove beneficial if healthcare data is accurate, secure, and accessible across healthcare networks which query or populate the health-related information.

One of the largest health information technology issues surrounds the accuracy and efficiency of identifying a patient. A local system with a poorly maintained or 'dirty' patient Master Person Index (MPI) will contaminate all other systems in which it links, significantly increasing the inaccuracy of patient records, while simultaneously lowering a patient's safety and quality of care potential [4]. As remote self-management technological advances and telehealth opportunities expand, accurately identifying a patient remotely and aggregating their remote health data with existing clinical data from the EHR is critical when assessing health outcomes. While many countries have implemented National Provider Identifiers (NPI) for their respective populations, no country has developed a biometric solution for identification and health record linkage. As electronic records continue to expand for PHRs and computing in health becomes increasingly ubiquitous, the need to establish an efficient, accurate, and secure form of identification is critical.

According to the report *IDENTITY CRISIS: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System*, a unique patient identifier (UPI) would significantly improve patients' health record record linking, as matching capabilities of medical records to accurately identify a record being searched have a success rate of 85% to 92% [5]. Although the ASTM's International standards for identifiers E.1714 *Standard Guide for Properties of a Universal Healthcare Identifier* and E.2553 *Guide for Implementation of a Voluntary Universal Healthcare Identification System* provides guidelines of a UHID [6] [7], there exists no current standard for data elements used in algorithmic record matching. The development of a unique identifier would help establish and enforce a large-scale authorization of patient data, permitting collected data to be valuable in helping to improve health outcomes of a patient.

We introduce a new technique using our developed algorithms to establish a Unique Health Identifier (UHID) based on the user's fingerprint biometric, with the utilization of facial-recognition as a secondary validation step before health records can be accessed. Biometric captures can be completed using standard 8 megapixel minimum smartphones and Web cameras in a touchless method using our solution, permitting user identification of both patients and medical personnel to occur within a clinical environment or remotely, such as the user's home. A traditional username and password can be used as an alternative to the biometric UHID, however it contains a lower identification accuracy and security. We present a series of experiments to demonstrate the formation of an accurate, repeatable, and scalable UHID.

2. The Proposed Solution

Our solution, which we have named, Unique Medical Biometric Recognition Enforcement of Legitimate and Large-scale Authentication or UMBRELLA, provides a potential solution for large-scale architectures and ubiquitous computing

environments, including home-health and remote health self-management. The individual research areas, which are the pillars of the proposed architecture, can be divided into four distinct areas, shown in Figure 1.

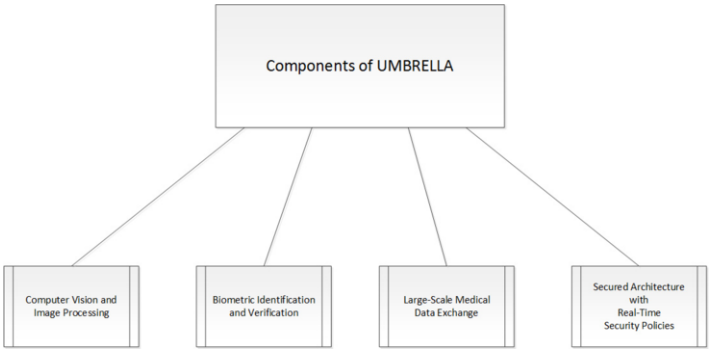

Figure 1. Components of the UMBRELLA Architecture.

3. Biometric Capture and Image Preprocessing

A key component of our solution is to accurately capture the user's fingerprints and facial features during the initial enrollment or when an enrolled user attempts to access the system. To avoid issues associated with touch fingerprint sensors, such as hygienic problems [8] and uneven finger pressure on a touch-based scanner leading to the problem of duality between fingerprint terminations and bifurcations [9], we introduce a touchless method using cameras in common devices such as Web cameras and smartphones. This provides a potential solution which does not depend on proprietary hardware, costly equipment, or single-use machinery.

3.1. Fingerprints Capture

Our developed application captures both the user's fingerprints and facial features using an overlay to the camera preview class written in Java code. The approach to capturing the user's fingers is structured, leading to consistent finger distances and fingerprint visibility. The user places their four fingertips, excluding the thumb, into the respective finger position markers, where all four fingerprints are captured simultaneously. Capturing the left and right hand results in a total possible of eight fingerprints captured. An illustration of the overlay capturing the fingers of a user's left-hand is shown in Figure 2.

3.2. Fingerprint Image Preprocessing

The fingerprint image preprocessing phase is a critical component to ensure accuracy of our system by preparing fingerprint images for minutiae extraction. Unlike past research, our solution captures four fingers of a hand simultaneously, using a variety of backgrounds and lighting conditions.

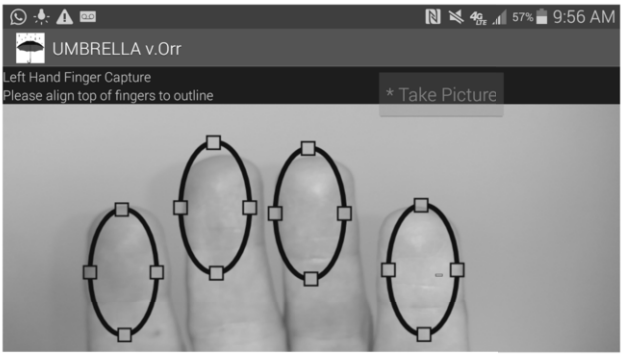

Figure 2. Fingerprint Capture - Left Hand

Our proposed algorithm is separated into three distinct parts. First the *Image Acquisition* phase, which captures images from the proposed application to perform local normalisation and RGB separation. Secondly, is the *Segmentation* phase, which conducts edge detection on the fingers before binary masking and cropping of the fingerprint region of interest is applied. Finally, the *Enhancement* phase is implemented. In this phase additional filters such as anisotropic diffusion, adaptive histogram equalization, ridge filtering, binarization, and thinning are conducted.

Experimental tests were conducted using the Goodness Index to evaluate the preprocessing algorithm. Results displayed a consistent average improvement of .31 in the image quality of the fingerprint after the algorithm was applied. False Non Match Rate (FNMR) and False Match Rate (FMR) were also calculated based from the minutiae mapping score within a given threshold. Results confirmed the images' quality and minutiae matching accuracy with a FNMR of 0.00 and a FMR of 0.016. With validation of the image preprocessing method, fingerprint images are prepared for the UHID process.

4. Development of the UHID

The establishment of a UHID for patients offers a paradigm shift from traditional identification measures used in healthcare and many other sectors of industry. It protects patient safety, reduces duplicate patient health records, and helps diminish healthcare costs associated with healthcare fraud, insurance fraud and correcting inaccuracies of health records due to patient misidentification. Likewise, the establishment of a biometric-based UHID allows authorized medical personnel to access patient health data without the requirement of usernames and passwords, however these forms of traditional identification can be utilized if needed. Through a medical personnel's unique identification, records are enforceable using the fingerprint biometric identification of the patient, where it is

validated through facial recognition, enhancing the security of patient identifiable information (PII).

At the time of this writing, only Krawczyk et al. has proposed a solution to secure electronic medical records using biometric authentication [10]. Their research, fused the biometrics of online signature and voice recognition to determine a user's authentication to their respective electronic medical record. This solution was based on a one-to-one matching environment and did not investigate the design of a UHID, nor did it take into account a large-scale architecture searching for multiple records within a one-to-many network.

4.1. Unique Identifier Parameters within the Medical Field

The discussion of creating a UHID has been debated extensively within recent years. As a result of the potential advantages sought from an established UHID, the American Society of Testing & Materials (ASTM) published a Standard Guide for Properties of a Universal Health Identifier in 2006, with re-approval confirmed in 2013 [11]. The ASTM's E1714-07 standards document stipulates thirty-one recommended criteria measures for an established UHID.

The ASTM document does not contain any text regarding protocols, examples, or linkage to a biometric UHID. The document only stipulates the technology used, must be scalable for the world population and its foreseeable future. Therefore, the document contains a loosely-coupled formation of guidelines and parameters in establishing and maintaining a UHID system. However, the premise of the ASTM's UHID standard brings about a common-sense logic in helping to structure one's approach in the development of a UHID system. We demonstrate our solution's design of an identification system in healthcare and its formation of a UHID to satisfy and comply with the suggested parameters brought forth by the E1714-07 document.

4.2. Triangulation

Fingerprint triangulation has proven to be a reliable method of establishing consistency within fingerprint analysis as it provides immunity against noise and distortion [12]. Experiments from Fengling Han et al. proved that minutiae points closest to the fingerprint's core are relatively stable, while points further from the core tend to produce more uncertainty [13]. Angles within the triangles are invariant under translation, rotation and scale, which was validated by work conducted by Bhanu and Tan [14][15].

Our solution develops an algorithm to capture the most stable minutiae points within each finger's already captured image. It then strategically creates a fictitious triangle to begin the process of marking key minutiae points, however our design differs from research conducted by Han et al. and others by several instances. First, the algorithm developed in our solution to create an existing UHID from the user's fingerprints is constructed to make certain no minutiae points are used more than two times in the selection of the lines of the fictitious triangle. Extensive testing concluded possible failures in forming the triangle and therefore calculating a unique identifier when the same minutiae point is used more

than twice. Secondly, the proposed solution performs a check to ensure no other minutiae points are in close proximity before a point is chosen. Due to possible saturation consisting of multiple minutiae points clustered together in a common space within the fingerprint, it becomes difficult for an algorithm to choose the same minutiae point each time when creating a fictitious triangle. The solution proposed chooses minutiae points based on stability and close proximity to other minutiae points, helping to ensure the same points are chosen each time. Third, the solution presented concatenates each finger's identification output sequentially by indexing each finger position, enabling a greater degree of uniqueness and scalability. Finally, no other solutions discuss methods of securing the UHID. The solution presented within UMBRELLA uses encryption of the UHID, adhering to the ASTM's traits of being *secure* and *disidentifiable.*

5. UMBRELLA's UHID

As a method of enforcing consistency and stability to achieve correctness in every digit of a UHID, UMBRELLA has focused on providing an algorithm using the methods of triangulation. The algorithm, and its associated User Interface (UI), was written in Java using Neurotechnology's Verifinger software developer kit (SDK). Verifinger was chosen due to its accurate matching capabilities between fingerprint samples and templates, along with its wide use within the academic research environment [16], [17] [18], [19]. Please note, the maximum number of fingers from a user is eight, while the algorithm used to define the unique and repeatable attributes from each of the user's individual fingerprints is nine. Therefore, each of the eight fingers contain nine unique attributes or digits. An explanation of this process is provided below.

To begin the process of establishing a UHID, five minutiae points with the closest proximity to the core, cores, or delta are selected, using each captured fingerprint's processed image. The distance between each selected minutiae point is calculated and the longest three lines between each selected minutiae point is determined. After the completion of locating the longest three lines between selected minutiae points, a fictitious triangle can be formed by calculating the coordinates of where the three lines intersect. Figure 3 illustrates the triangulation of the longest three calculated lines on one of the fingerprint images used within the research test images. With the triangle formed, the algorithm uses geometric properties of the triangle to establish the longest side of the triangle, known as the maximal side or x_1. Also, the angle between the angles of the two vertices of this line is labeled as the medial angle (αmed) and the other angle as the minimal angle (αmin).

The calculation of angles within the fictitious triangle of the fingerprint is the final step before being able to map the user's fingerprint to a unique identifier. As there are three sides, a total of six minutiae are present to end the lines of the triangle. Therefore, the process begins by marking each minutiae as a 1 if it is bifurcation or a 0 if it is an end. Digits 1-6 of each fingerprint's identifier would be a binary series of data populating the first six fields.

Fingerprint digits 7-9 are used to further extend the identifier within each fingerprint and assist in accounting for any discrepancies due to deformations,

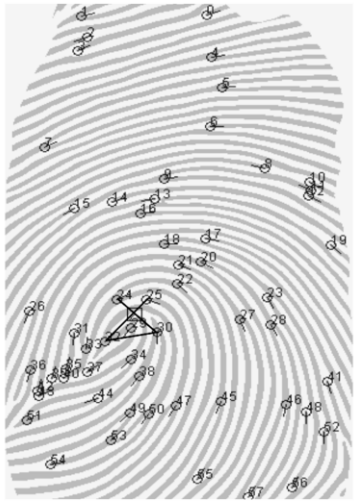

Figure 3. Triangulation of Selected Minutiae Points with Longest Three Lines

unforeseen shadowing or additional blurriness of the image resulting in change. Han et al. calculated a variance from their test results to determine average values of x_1, αmed, and αmin. Based on their findings of these values and their respective variations, a transformation was calculated to ensure the quantity each all three values would remain consistent during multiple captures of the same finger, producing the same values. Therefore, digits 7, 8 and 9 were based on previous error-tolerant transformation work by Han [13] and advanced through our research to produce more accurate results. Additionally, our proposed solution uses hexadecimal values instead of the 0-9 numbering system, providing a greater degree of uniqueness and scalability of a user's UHID through the use of 16 possible values instead of 10. Therefore, a total of nine alphanumeric digits are derived from each fingerprint image. While previous work cited the generation of an identifier by a single fingerprint, the proposed solution extends a UHID by combining each of the user's fingerprint image value output into single health identification attribute.

5.1. Concatenation

The current solution permits a total of eight fingers to be captured, or four fingers per hand. Each fingerprint is configured to generate nine digits, representative to the uniqueness of the minutiae within that respective fingerprint, and totaling a possible thirty-six digits from one hand or seventy-two digits from each. Using concatenation, fingerprint identification values can be presented together as a single UHID. This is possible due to the placement labeling of each finger position during the capture and image processing method. Images are aligned according to hand and finger position, producing a concatenated UHID.

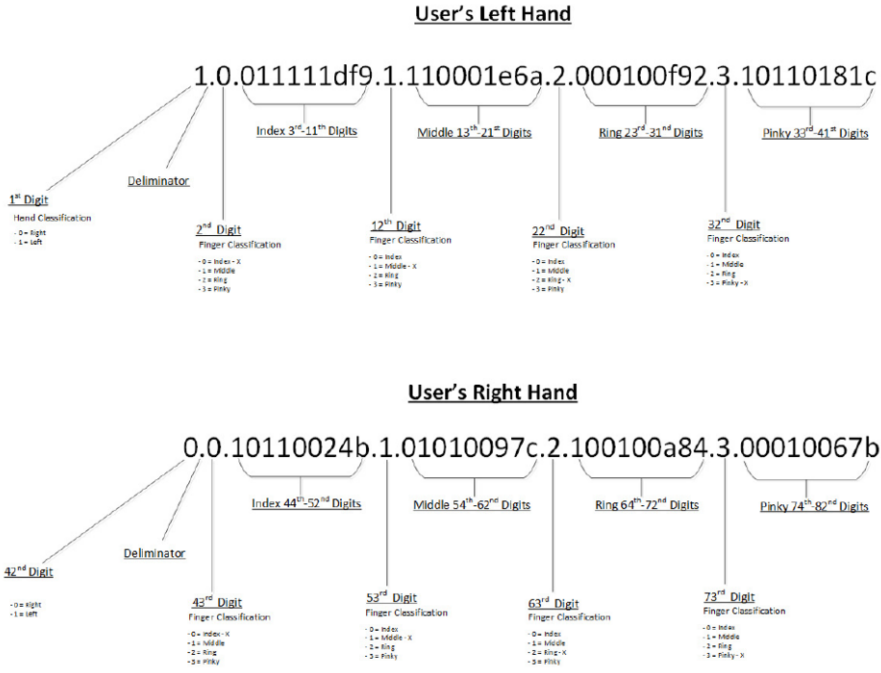

Figure 4. UMBRELLA's UHID Digit Classification

Figure 4 displays UMBRELLA's methodology of concatenating the four fingerprints from both the left and right hand. The concatenated UHID has a total of eighty-two digits, seventy-two stemming from the eight fingerprint images' identification output and an additional ten digits used for classification of hand and finger position. A delimiter is used to separate the classification of hand, finger position, and each fingerprint identification values from each other.

An accurate concatenation process offers several enhancements to user identification. First, it improves the uniqueness attribute of the UHID. Increasing the amount of digits of the identifier, subsequently will increase the variance between UHIDs, helping to provide a truly unique and scalable identifier. Secondly, an extended UHID identification value, which will become encrypted, increases the difficulty of capturing a user's identification number and using it for malicious purposes, such as medication fraud. Finally, the concatenation of a user's fingerprints helps in achieving a potential global UHID facilitating accurate user identification and health record exchange on a large-scale platform.

To secure the UHID, we encrypt it upon its initial creation, along with its use anytime within the system using the Advanced Encryption Standard (AES)

256-bit encryption seen in Figure 5.

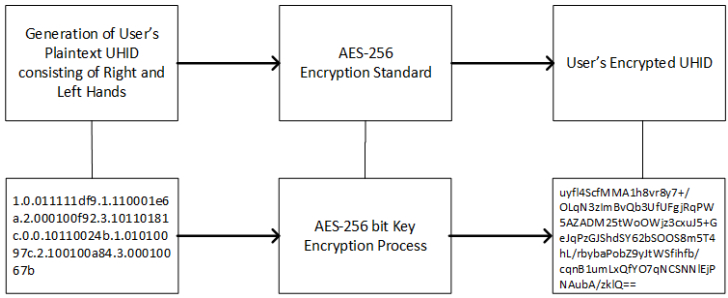

Figure 5. UHID Encryption of User's Concatenated Fingerprints

6. UHID Experimental Results

To perform experiments in developing a repeatable UHID, images captured from the four impressions of each hand for test participants were processed within our image preprocessing algorithm and used within our tests for a total of 420 images. An additional four impressions of each users' hands were taken and processed, permitting them to be used as a comparison in our verification process, creating another 420 images or a total of 840 images used within performance evaluation.

The average time to transform a single fingerprint into a portion of the UHID was 3.11 seconds, and totaling 24.88 seconds for all eight fingerprints and the concatenated user's UHID. To test, each of the user's eight fingerprints, consisting of four impressions for each finger were calculated. The remaining four impressions consisting of a separate capture process were used to validate the algorithm's consistency and repeatable UHID. Per Finger UHID Match is calculated by the following equation:

$$PerFingerUHIDMatch = \frac{UHIDMatch}{TotalUsers} \tag{1}$$

Results from our experiments are shown in Table 1. One finger from a user within our participant group did not match it's original UHID, the left-hand pinky. Upon investigation, although the algorithm was able to correctly choose the appropriate minutiae positioning as in the original template for the user, the third digit was incorrectly labeled as a *termination*, when it was actually a *bifurcation*. Due to the user's angle of their pinky finger's position with heaving shadowing in natural light, the single minutiae point classification was too difficult to determine for our algorithm. Although the facial recognition would have properly denied an incorrect user during the secondary biometric verification phase, we plan to continue in improving our algorithm even further to ensure a greater level of accuracy and consistency.

Table 1. UMBRELLA captured images' UHID match results

Finger Position Per Hand	Digits 1-6	Digits 7-9
Left Hand - Index	1.00	1.00
Left Hand - Middle	1.00	1.00
Left Hand - Ring	1.00	1.00
Left Hand - Pinky	0.93	1.00
Right Hand - Index	1.00	1.00
Right Hand - Middle	1.00	1.00
Right Hand - Ring	1.00	1.00
Right Hand - Pinky	1.00	1.00

We also conducted UHID on images from the Fingerprint Verification Competition (FVC) 2004 fingerprint database. The FVC 2004 database, consisted of eight impressions of a user's single finger. Using four impressions for each user to establish a UHID based on a single finger, the remaining four impressions of each finger was used to establish a separate UHID. The two UHIDs for each user were compared. Table 2 displays the results. One individual's, user 7, single finger UHID doesn't not match on digits 1-6. After further analysis of the image, we determined the issue was attributed to the very poor quality of the user's fingerprint involving the area around the fingerprint's core. As a result, the algorithm is not able to determine the distinction between several of the minutiae points clustered together and falsely chooses the incorrect minutiae.

Table 2. FVC 2004 database UHID match results

FVC 2004 Database	Digits 1-6 Matched	Digits 7-9 Matched
User 1	Yes	Yes
User 2	Yes	Yes
User 3	Yes	Yes
User 4	Yes	Yes
User 5	Yes	Yes
User 6	Yes	Yes
User 7	Yes	Yes
User 8	No	Yes
User 9	Yes	Yes

7. Conclusion

We have introduced a new technique of user identification in healthcare in a design which is scalable, promotes interoperability on a large-scale architecture, and secure. The proposed architecture offers a potential solution capable of patient identification, health data exchange and security. Our research has developed algorithms capable of establishing a UHID based on the user's fingerprint biometric, with the utilization of facial-recognition as a validation step before health records can be accessed. The design is flexible and does not require the current NPI's to be replaced. Rather, a user's UHID may be cross-mapped to their existing NPI, therefore not requiring existing records to be remapped to a new health identifier.

Experiments conducted show promising results. Both UMBRELLA captured images and fingerprint images from the FVC's 2004 Database show a high accuracy. Using a standard deviation of 9% digits 7-9 matched perfectly in both tests. While the facial biometric would have detected a non authorized user trying to access a record for the two failed cases, there remains continued development in the UHID algorithm to further improve its accuracy and consistency. We anticipate this solution to aid in the reduction of complexities associated with user misidentification in health care resulting in lowering costs, enhancing population health monitoring, and improving patient-safety.

References

[1] Xierali IM, Hsiao CJ, Puffer JC, Green LA, Rinaldo JC, Bazemore AW, Burke MT, Phillips RL. *The rise of electronic health record adoption among family physicians.* The Annals of Family Medicine. 2013 Jan 1;11(1):14-9.

[2] Berner ES, Detmer DE, Simborg D. *Will the wave finally break? A brief view of the adoption of electronic medical records in the United States.* Journal of the American Medical Informatics Association. 2005 Jan 1;12(1):3-7.

[3] Liu LS, Shih PC, Hayes GR. *Barriers to the adoption and use of personal health record systems.* In Proceedings of the 2011 iConference Feb 8 (pp. 363-370). ACM.

[4] Morris G, Farnum G, Afzal S, Robinson C, Greene J, Coughlin C. *Patient Identification and Matching Final Report.* Office of the National Coordinator for Health Information Technology, contract HHSP233201300029C, 2014 Feb 7.

[5] Hillestad R, Bigelow JH, Chaudhry B, Dreyer P, Greenberg MD, Meili RC, Ridgely MS, Rothenberg J, Taylor R. *Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the US Health Care System* (Santa Monica, CA: Rand, 2008).

[6] Hieb BR. *The case for a voluntary national healthcare identifier.* Journal of ASTM International. 2006 Jan 5;3(2):1-2.

[7] Hieb B. *A Cost Effective Approach to Create a Universal Healthcare Identifier System.* electronic Journal of Health Informatics. 2009 Aug 4;5(1):5.

[8] Hiew BY, Teoh AB, Yin OS. *A secure digital camera based fingerprint verification system.* Journal of Visual Communication and Image Representation. 2010 Apr 30;21(3):219-31

[9] Gue D. *The HIPAA security rule (NPRM): Overview.* HIPAAdvisory. Retrieved June. 2003;14:2004.

[10] Krawczyk S, Jain AK. *Securing electronic medical records using biometric authentication.* International Conference on Audio-and Video-Based Biometric Person Authentication 2005 Jul 20 (pp. 1110-1119). Springer Berlin Heidelberg.

[11] Leonard DC, Pons AP, Asfour SS. *Realization of a universal patient identifier for electronic medical records through biometric technology.* IEEE Transactions on Information Technology in Biomedicine. 2009 Jul;13(4):494-500.

[12] Germain RS, Califano A, Colville S. *Fingerprint matching using transformation parameter clustering*. IEEE Computational Science and Engineering. 1997 Oct 1;4(4):42-9.

[13] Han F, Hu J, He L, Wang Y. *Generation of reliable PINs from fingerprints*. In2007 IEEE International Conference on Communications 2007 Jun 24 (pp. 1191-1196). IEEE.

[14] Bhanu B, Tan X. *Fingerprint indexing based on novel features of minutiae triplets*. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2003 May;25(5):616-22.

[15] Bhanu B, Tan X. *Computational algorithms for fingerprint recognition*. Springer Science & Business Media; 2012 Dec 6.

[16] Mascher-Kampfer A, Stgner H, Uhl A. *Comparison of compression algorithms impact on fingerprint and face recognition accuracy*. InVisual Communications and Image Processing 2007 Jan 28 (pp. 650810-1).

[17] Perez-Diaz AJ, Arronte-Lopez IC. *Fingerprint Matching and Non-Matching Analysis for Different Tolerance Rotation Degrees in Commercial Matching Algorithms*. Journal of applied research and technology. 2010 Aug;8(2):186-98.

[18] Paulino AA, Jain AK, Feng J. *Latent fingerprint matching: Fusion of manually marked and derived minutiae*. In 2010 23rd SIBGRAPI Conference on Graphics, Patterns and Images 2010 Aug 30 (pp. 63-70). IEEE.

[19] Zhao Q, Jain AK. *On the utility of extended fingerprint features: A study on pores*. In 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops 2010 Jun 13 (pp. 9-16). IEEE.