International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:1, 2016

Development of a Secured Telemedical System Using Biometric Feature

O. Iyare, A. H. Afolayan, O. T. Oluwadare, B. K. Alese

***Abstract*—**Access to advanced medical services has been one of the medical challenges faced by our present society especially in distant geographical locations which may be inaccessible. Then the need for telemedicine arises through which live videos of a doctor can be streamed to a patient located anywhere in the world at any time. Patients' medical records contain very sensitive information which should not be made accessible to unauthorized people in order to protect privacy, integrity and confidentiality. This research work focuses on a more robust security measure which is biometric (fingerprint) as a form of access control to data of patients by the medical specialist/practitioner.

***Keywords*—**Biometrics, telemedicine, privacy, patient information.

I. Introduction

THE history of modern telemedicine dated back to when the traditional telephone was invented, then medical advice was given by physicians over the telephone. Telemedicine is the description of supporting medical services through the use of telecommunications [1]. 'Tele' means distant, it originated from the ancient Greek. In other words, telemedicine is providing medical services over distance by using Information Technologies (IT) [1]. This system can be used in all phases of the primary health care process: from prevention and tele-diagnosis to treatment and tele-homecare. Besides, in countries where the ratio of doctor to patient is one-to-thousands, or health centers and hospitals are hundreds of miles from patient's homes, this system comes in handy as they allow timely access to quality health services like tele-monitoring, tele-diagnosis, and e-prescription at low costs thereby improving the quality of life of citizens and greater economic productivity.

Biometrics is derived from the Greek words "bio" (meaning life) and "metrics" (meaning to measure) [2]. Due to the notable advances in the field of computer processing over the few decades ago, automated biometric systems became readily available. Many of these new automated techniques are based on ideas that were originally conceived thousands of years ago. Biometrics refers to the identification of humans by their characteristics or traits. It is used in computer science as a form of identification and access control [2]. It is also used to identify individuals in groups that are under surveillance. A biometric system is a recognition system that identifies a person by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user [3]

Fingerprints are individual unique identifiers of any person. A fingerprint recognition system can be used for both verification and identification. In *verification*, the system compares an input fingerprint to the "enrolled" fingerprint of a specific user to determine if they are from the same finger (1:1 match). In *identification*, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:*N* match). Detecting *multiple enrollments*, in which the same person obtains multiple credentials such as passport under different names, requires the *negative identification* functionality of fingerprints.

New possibilities for health care service and delivery are rapidly been created, this is due largely to the recent advancements and increasing utilization of IT by the general population. These advancements in turn have led to the creation of a rich tapestry of telemedicine applications that the world is coming to use [4]. Access to patient information must be done discreetly and must comply with some corporate policies such as the rules stipulated in the health insurance portability and accountability act (HIPAA) conditions that must be met for "proper access". Granting any health professional full access to a patients' EHR (Electronic Health Records) may pose potential law violation and create privacy and security risks. A study analyzing whether or not different health professionals will comply with the information assurance policy of their respective health clinic reveals that as many as fifteen compliance factors are involved in such a decision [5]. Therefore, granting *full access* to any health professional is simply not wise. Instead, a limited and/or partial access is the solution. Granting partial or limited access to a patient's EHR outside of hospital grounds has been an area of interest, but it has been limited to close contact or carried on solutions. In this paper, the focus is on granting proper access to a patient's EHR remotely with the use of a biometric identification system (that is, Fingerprint).

II. Research Motivation

Rural areas find it difficult to get health care services especially from experts, referring patient from one location to the other without adequate initial consultation which has caused loss of lives and monetary resources among the rural dwellers [6].

Iyare O. is with the department of Computer Science, Federal University of Technology, Akure, Nigeria (phone: +2347033513174, e-mail: oiyare@futa.edu.ng).

Afolayan A. H., Oluwadare O. T., and Alese B. K. are with the department of Computer Science, Federal University of Technology, Akure (e-mail: ahafolayan@futa.edu.ng, Oluch4@gmail.com, bkalese@futa.edu.ng).

Telemedicine allows health care centers and hospitals to more efficiently provide services to a broader population, help protect and promote better health, enhance citizens' health status and minimize cost of service. As the transaction costs are coming down, telemedicine is likely to become widely acceptable [7].

Telemedicine can provide a powerful platform that could benefit the poorer citizens of developing countries (that is, overcome long established barriers, enabling people to access improved healthcare services faster, thus saving lives of people at first like a first-aid) by enhancing access to health education and health care through distance learning and telemedicine, IT can improve the quality of life for poor rural communities where there is no access to these medical facilities available in the urban areas [8].

Today, a new generation of technology solution is poised to help health care organizations in the area of database management (that is, data protection) which is susceptible to hackers and unauthorized users to have access to the information of patients. This research work will aid in the reduction of such scenarios from occurring frequently by using biometrics as a means of security measures in lieu of password provided by the doctor who holds the records of his/her Patients [9].

III. Research Methodology

Fig. 1 is the multimedia system architecture for telemedicine. The multimedia system architecture has three levels or stations of activities, namely: telemedicine capture station, telemedicine file server station and telemedicine view station.

The ***capture station*** consists of hardware and software that are to be used for digitizing and compressing video signals. It comprises of workstations equipped with video cameras and microphones and video capturing software (Window Media Encoder).

The ***telemedicine file server*** receives request from clients (the users) to send or receive data. The server is the distribution agent using multimedia server software to stream the media files.

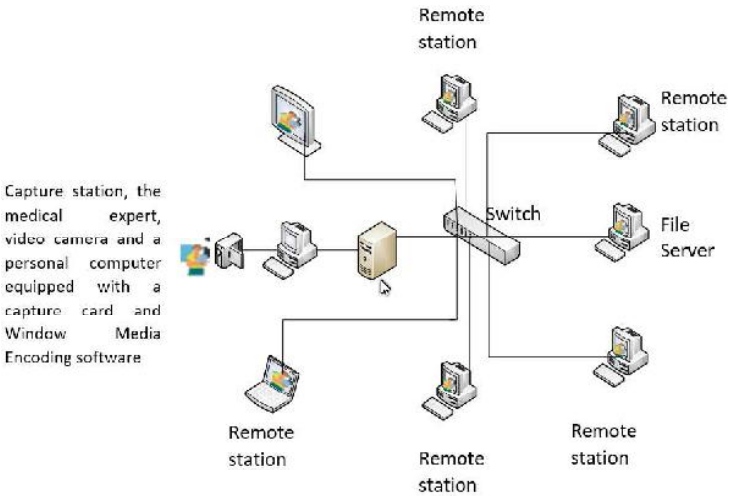

Fig. 1 Conceptual Diagram of the Levels of System

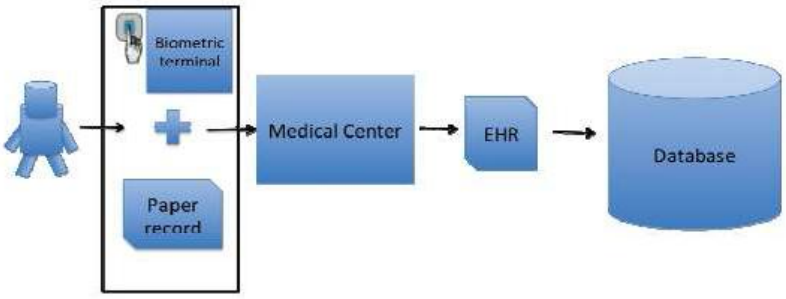

Fig. 2 System Preparatory Events [11]

The ***telemedicine view stations*** are where the proceedings of telemedicine are being viewed either live or on demand after they have been stored on the server. They decompress video streams and display the video on the video display unit. The telemedicine view station is composed of multimedia workstation equipped with video card, speakers, video player

software, and a projector for playing back the audio-video reception.

The architecture in Fig. 2 is defined as a unimodal biometric system that uses a singular biometric feature that is, Fingerprint [10]. Fig. 2 shows that the fingerprint should have been previously enrolled in the electronic health record database in order to find it in future queries.

A. Using the System

System components consist of both hardware and software elements. Hardware components include a fingerprint scanner, a mobile PC, and a hosting server computer. Fig. 3 depicts the system components architecture linked in functional sequence in order to demonstrate the sequence of events.

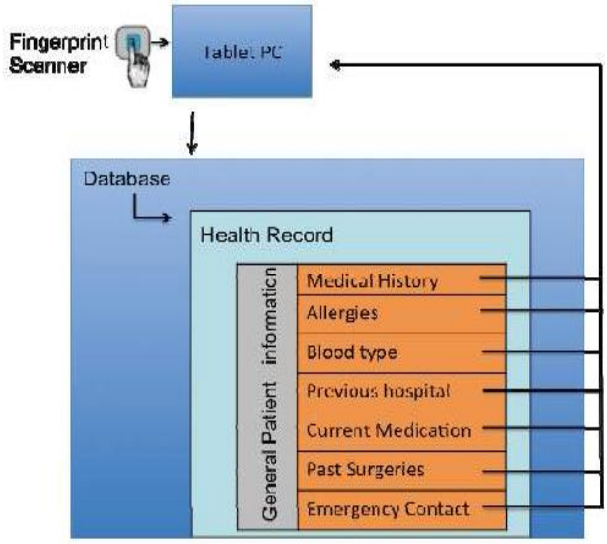

Fig. 3 Health record retrieval with privacy-preserved policies [11]

There are two hardware components, two software components, and a set of privacy-preservation policies in this system architecture. First, the medical expert or health assistant fingerprint image is being *enrolled* into the system database. Then, they select the *identify/verify command* from the system user interface. The fingerprint image is then sent as a SQL query to the central database through the biometric terminal's mobile broadband connection for *matching.* After this process, the result is either the set of privacy preserved values from a record or a not found message in order to grant or deny access respectively.

B. The Mathematical Model Approach

A fingerprint image is firstly enhanced before the features contained in it could be detected or extracted. A well enhanced image will provide a clear separation between the valid and spurious features. Spurious features are those false minutiae points that are created due to noise or artifacts and they are not actually part of the fingerprint. Thus, this aspect presents modified mathematical modeling approaches to fingerprint ridge segmentation and normalization which are essential parts of the enhancement process.

There are two regions that describe any fingerprint image; namely the foreground region and the background region. The foreground is region containing the ridges and valleys. As shown in Fig. 4, the ridges are the raised and dark regions of a fingerprint image. The low and white regions between the ridges are the valleys. The foreground regions are also known as the Region of Interest (RoI) since they contain the unique features that define the image. The background regions are mostly the outside regions where the noises introduced into the image during enrolment are mostly found.

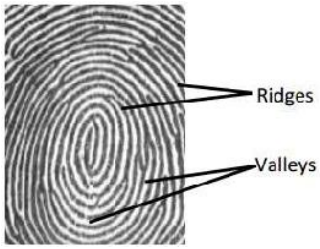

Fig. 4 Ridges and valleys on a fingerprint image

The foreground and the background regions of the image as shown in Fig. 5 are marked by the arrows. The essence of segmentation is to reduce the burden associated with image enhancement by ensuring that focus is only on the foreground regions while the background regions are ignored.

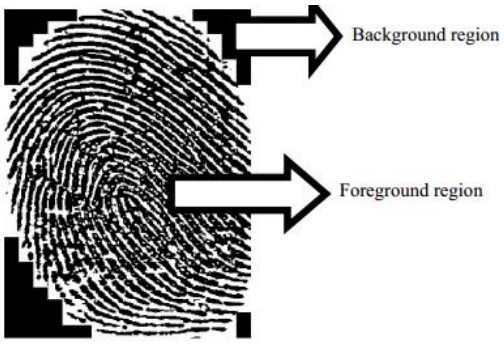

Fig. 5 A fingerprint image and its foreground and background regions

The background regions possess very low grey-level variance values while the foreground regions possess very high grey-level variance values. A modified version of the approach presented is used in this research for obtaining the grey-level variance values. The modified approach firstly divides the image into blocks of size S x S and then the variance, σ^2 (b) for each of the pixels in block b is obtained from:

$$a^2(b) = k\sum_{a=0}^{s-1}\sum_{b=0}^{s-1}\left[L(a+1,b+1) - N(b)\right]^2 \quad (1)$$

$$N(b) = k\sum_{i=0}^{s-1}\sum_{j=0}^{s-1}P(i+1,j+1) \quad (2)$$

$$k = \frac{1}{s^2} \tag{3}$$

L(u+1, v+1) and P(i+1, j+1) are the grey-level value for pixel (u+1, v+1) and (i+1, j+1) respectively in block b.

The purpose of normalization of the ridge structure of the segmented image is to standardize the level of variations in the image grey-level values. By normalization, the grey-level values are adjusted to certain range that is good enough for improved image contrast and brightness. The first of the tasks of image normalization implemented in and adopted for this research is the division of the segmented image into blocks of size S x S. The grey-level value for each pixel is then compared with the average grey-level value for the host block. For a pixel L(u,v) belonging to a block of average grey-level value of μ and variance V, the result of comparison produced a normalized grey-level value ϕ(u,v) defined by:

$$(u,v) = \begin{cases} \mu_0 + \sqrt{\dfrac{v_0\left(L(u,v)-\mu\right)^2}{v}} & if\ L(u,v) > \mu \\ \mu_0 - \sqrt{\dfrac{v_0\left(L(u,v)-\mu\right)^2}{v}} & otherwise \end{cases} \tag{4}$$

where μ_0 and V_0 are the assumed mean and variance respectively.

IV. Implementation

The software used in the development and building of the web based user interface are: WAMP Server version 2.0 (MySQL Database inclusive), Adobe Dreamweaver CS5 (HTML and PHP inclusive), Adobe Fireworks, Amara Flash Menu Builder and Photo Animation Slide Show, Windows Media Encoder running at file server and capture stations.

A. How to Access the Website from the Client Side

a. The client first connects to the network.
b. Open the browser and type the web address on the address bar as follows: http://192.168.13.1/ which is the IP address of the server.
c. The web page is being displayed on the client's browser.

The system begins at the homepage; it is the first page that will be displayed when the user launches the site on the URL address bar. This serves as the index to other pages linked to it. It contains brief information about telemedicine and also services provided (that is, links to get detailed information of other telemedicine services such as tele-treatment, tele-surgery, tele-nursing, tele-monitoring and so on).

The expert search page receives some basic medical information of a patient which is to be filled by a medical assistant or practitioner such as health assistant fullname, patient fullname, symptoms, nature of sickness, duration of sickness, medical area in which expertise might be needed, the name of hospital or health center that their service is requested also with some other relevant medical records or information. On receipt of the medical information as described above, the application locates the available medical expert in the location of the specialist hospital.

B. Hardware Requirements

a. Pentium IV processor or higher,
b. Minimum of 100MB Hard disk space,
c. Keyboard, Mouse and Monitor,
d. High Resolution Webcam.

C. Software Requirements

a. WAMP Server,
b. O/S Windows Server 2003, Window XP, Window Vista or Window 7,
c. Mozilla Firefox or any other compatible browser.

V. Conclusion

This work has successfully developed a secured telemedical system using a biometric feature that will further improve the access to quality health care, experts in medical services in respective of distance especially in the remote areas and increase security of patient records.

In the course of the work we used wireless systems with media encoder for the development of a web based video streaming application for telemedicine.

An expert search was also included to find medical experts that render their medical expertise remotely over the network through video streaming to the client system over the network. Finally, fingerprint scanning was also used to aid the password and username authorization, thus making it insusceptible to hackers.

References

[1] Bernard Fong, Fong A.C.M and C.K.Li (2011). A Telemedicine Technologies. A John Wiley production, ISBN 978-0-470-74569-4
[2] Rood E.P and Hornak L.A (2003). Are you who you say you are? World and I; August 2003, vol. 18 Issue 8, pp 142.
[3] Swati Bobde S. and Satange D. N. (2013): "Biometrics in Secure e-Transaction" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS): Volume 2, Issue 2, March – April.
[4] Wootton R, Jebamani LS, Dow SA. E-health and the Universitas 21 organization: 2. Telemedicine and underserved populations. Journal of Telemedicine and Telecare, 2005, 11(5):221–224.
[5] Cannoy S.D and Salam A.F (2010). A Framework for Health Care Information Assurance Policy and Compliance, Communications of the ACM, 53,3,126-131.
[6] Nakajima, I.; Sastrokusumo, U.; Mishra, S.K.; Komiya, R.; Malik, A.Z.; Tanuma, T. (2006) The Asia Pacific Telecommunity's Telemedicine Activities, IEEE Xplore.com website, 17-19, pp. 280 - 282, ISBN 0-7803-9704-5, doi:10.1109/HEALTH.2006.246471. August, 2006.
[7] Berman, Matthew, Fenaughty, Andrea (2005): "Health Economics" 14 (6): 559–573. doi:10.1002/hec.952. PMID 15497196. June, 2005.
[8] Conde Jose G., De-Suvranu Hall, Richard W., Johansen Edward, Meglan Dwight P., Grace C. Y. (2010). "Telemedicine and e-Health". Telemedicine and e- Health. February, 2010.
[9] Brewin. B (2008): Cyber criminals overseas steal U.S. electronic health records, http://www.nextgov.com/nextgov/ng_20080516_2203.php viewed on the 6th of April 2015.
[10] Sharma G.D (2011): The Challenge of Health for the Welfare State of India, Available at SSRN: http://ssrn.com/abstract=1852391 or http://dx.doi.org/10.2139/ssrn.1852391
[11] José R. Díaz-Palacios, Víctor J. Romo-Aledo, Amir H. Chinaei (2013): Biometric Access Control for e-Health Records in Pre-hospital Care. Proceedings of ACM 978-1-4503-1599-9/13/03.