ICT in Telemedicine: Conquering Privacy and Security Issues In Health Care Services

R. F. Olanrewaju[1], Nor'ashikin Bte. Ali[2], Othman Khalifa[1], Azizah Abd Manaf[3]
[1]Department of Electrical & Computer Engineering, Faculty of Engineering,
International Islamic University Malaysia
Kuala Lumpur Malaysia
[2]College Of Information Technology, Universiti Tenaga Nasional Malaysia.
[3] Advanced Informatics School (UTM AIS)
UTM International Campus, Kuala Lumpur, Malaysia.
[1]frashidah@yahoo.com

Abstract – **Advancement in telecommunication combined with improved information technology infrastructures has opened up new dimensions in e-health environment. Such technologies make readily available to access, store, manipulate and replicate medical information and images. These technologies help reduced the time and effort in diagnoses and treatment at lower cost. However, protection and authentication of such medical information and images are now becoming increasingly important in the telemedicine environment, where images are readily distributed over electronic networks. Intruders/hackers may gain access to confidential information and possibly alter or even delete such vital records. The ultimate success of telemedicine demands an effective technology as well as privacy and security of records. This paper explores recently identified privacy and security issues that affect telemedicine. We feature threats on security and authentication of medical records, and propose digital watermarking as a technology to curb authentication issues in telemedicine.**

Keywords: Authentication; ICT; Privacy and Security, Telemedicine; Telehealth.

I. INTRODUCTION

Protection of personally identifiable information whether health information, banking records, employment history or credit score, must be ensured. With the advent of telehealth, e-health and/or telemedicine; a system were application of wireless communications is used in connecting healthcare professionals and patients through ubiquitous and cloud computing over electronic networks, authentication, integrity and confidentiality of patient's data are often pointed out as key factors to be considered.

Newer information technology and telecommunication products offered to patients and healthcare professionals alike are capable of transmitting vital signals, such as key blood test results for diabetics and blood pressure data. The technology has grown to advanced imaging technologies and gamma cameras with higher data requirements that can be used to transfer data and images such as CT Scanners, MRIs, PET-CT, C-Arms, Mammography, X-Rays, Bone Densitometers, Radiographic and urology systems [1].

Telecommunication technologies and information systems are being integrated and adopted in medical field to store patient information in digital format that allows adequate medical assistance delivered to the patient in distinct places and scenarios, called Electronic Patient Records (EPR) [2]. Such records are used in conjunction with sensor networks for remote patient monitoring, consulting, training and diagnoses to form a telemedicine system.

In many health care organizations, management of telemedicine technology has been *ad hoc* [3]. Ineffective management of privacy and security issues in telemedicine may compromise the overall success of the health system. During file-sharing over the network, intruders may gain access to confidential information and possible alter, steal or even delete patient records. This has led to wrong diagnosis and wrong decision taken on patients, some of which may be life threatening cases. Consequently, it cost some hospitals billions of law suits.

A stolen record is even worse because it can lead to Medical Identity Theft (MIDT). MIDT is a specific type of identity theft that occurs when a person uses someone else's personal health identifiable information, such as insurance information, Social Security Number, health care file, or medical records, without the individual's knowledge or consent to obtain medical goods or services, or to submit false claims for medical services [4]. A typical example of MIDT is an electronic health record of the United States which was stolen in 2004 and was found on a computer server in Malaysia. It is controlled by cyber criminals.

The stolen files included names of health care providers, security numbers, birthdates and addresses of the patients. Criminals may create false billings, which can bring in millions of dollars from stolen health records. The discovery of the stolen records has revealed the vulnerability of electronic medical records, and can cause more damage than the loss of money to false billings. When cyber criminals alter a patient's medical records, the results could be potentially deadly [5].

MIDT is becoming one of the fastest growing crimes in the USA today [6], with sophisticated and organised hacking groups stealing patient identities; MIDT used to illegally obtain medical services, prescription drugs, as well as the bank accounts or credit card**.** Furthermore, due to sharing of Electronic Medical Records (EMR) among business partners and other entities, thus exacerbates the situation. Recent incidents of MIDT is when a hacker from Eastern Europe illegally accessed Utah Department

of Technology Services (DTS) servers containing patients' Social Security numbers and data on children's health plans due to a weak password. The breach involved 780,000 individuals both Medicaid patients as well as recipients of Children's Health Insurance Plan stolen from the server [7]. Cyber attacks on patients' EMR and health information systems (HIS) can lead to severe consequences like patient identity disclosure, embarrassment, privacy violation and in the worst case, integrity violation resulting in a patient's death [8].

In a recent case, March 2012, Blue Cross Blue Shield of Tennessee (BCBST) agreed to pay U.S. Department of Health and Human Services (HHS) $1.5 million for inadequate security measures which allowed 57 unencrypted hard drives containing private health information to be stolen from its facility [9]. These challenges prompted significant research in developing efficient methods to protect and authenticate digital medical images and information in order to prevent forgery and impersonation.

Various measures have been employed to prevent, deter, detect and correct damages caused in telemedicine due to privacy and security threats. One such deterrent measure was the creation and enactment of the Health Insurance Portability and Accountability act (HIPAA) in 1996. The aim of HIPAA was to improve the Medicare program and the efficiency and effectiveness of the health care system. This is done by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information [10].

A similar regulatory body is the creation of Agency for Healthcare Research & Quality (AHRQ), which is a United States of America Federal agency under Health & Human Services working to improve the quality, effectiveness and safety of health care. AHRQ gathers information in surveys, funds research projects, and provides evidence-based practice guidelines for health care practitioners. The AHRQ's Consumer Assessment of Healthcare Providers and Systems (CAHPS) program provides a national benchmarking (health care standards) database [11].

Apart from such regulatory measures, several technological and financial measures have also been taken to reduce the impact of security and privacy breaches on telemedicine networks [8]. One of the oldest and common tools available forms of data protection is by means of encryption. Encryption protects contents particularly during transmission of data from sender to receiver. However, once it reaches a recipient and is decrypted, the protection ends and the data can be copied and redistributed without further complications [12, 13]. This is because the object loses its protection once it is decrypted. Consequently, mishandling of sensitive information cannot be prevented effectively by this traditional means. Figure 1 shows how an image is illegally copied after decryption.

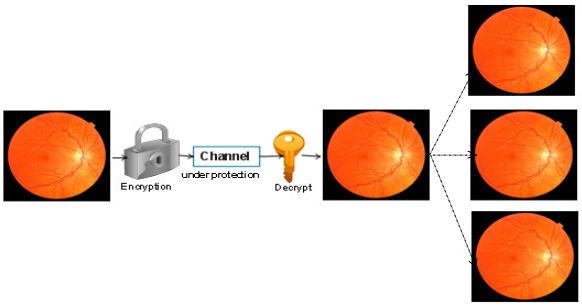

Figure 1: Loss of protection after decrypting digital image [29]

The study in [14] confirms that using encryption is insufficient to protect the confidentiality of patient telemetry.

II. OVERVIEW OF TELEMEDICINE

More than 52 million deaths in 1996 worldwide, about 40 million occurred in the developing world due to lack of medical facilities. More than 600 million people worldwide have chronic diseases with treatments costing $500 billion per year in 2010 and these costs will increase by 37% until 2020 [15]. Poor countries had four times more deaths than rich countries. One of the ways to curb this problem is by relevant development and implementation of telehealth services supported by ICT.

Telemedicine is the use of modern telecommunications and information technologies for the provision of clinical care to individuals at a distance and the transmission of information to provide that care [16]. E-health/telehealth is an emerging field in the intersection of medical informatics, public health and business, enhanced through the Internet and related technologies, to improve health care locally, regionally, and worldwide by using information and communication technology [17]. In this sense, telehealth and e-health is equivalent to the broad use of the term telemedicine, Therefore, telehealth, telemedicine or e-health terms will be used interchangeably.

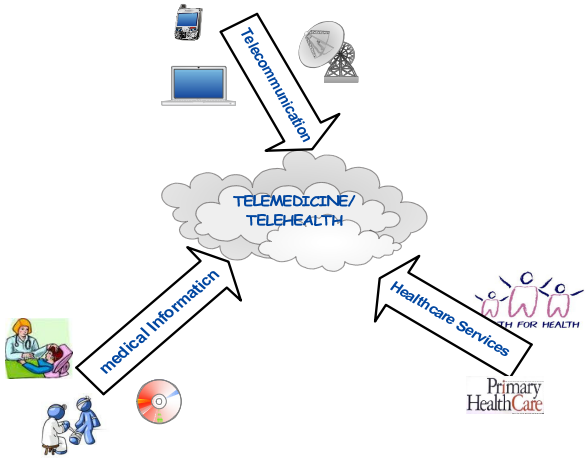

Figure 2: Components of telemedicine

Telemedicine is possible due to the current trends in information and communication technology. Such as cloud computing and ubiquitous computing, where small computers are embedded in almost everyday objects around us using both mobile devices as well as wireless connections for recording, storage and delivery medical data. Medical personnel can use these facilities to remotely provide consultation to patients or even cooperate with colleagues. Information technology has become an important enabling factor in implementing telehealth.

In the developed world, telehealth has become standard medical practice [18]. There has been a rapidly growing interest in telemedicine and telehealth as a means to ease the pressure of health care on national budgets. Distant health care was successfully applied in several pilot studies, such as the telementoring of laparoscopy procedure in [19], where a remote surgeon located in a control room supervised an inexperienced surgeon. Another project is the International MedioNet of China (IMNC) network initiative that connects 300 hospitals (3,000 specialists) to remote patients through telephone lines and the internet [20]. Newer projects includes telemedicine and trauma referrals in Plastic Surgery [21], telemedical applications in psychiatry [22], surgical robotics [23] post-hospital care, epidemiology, cardiology [24-25] etc. Most of the branches of medicine, are now implemented in telemedicine such as consulting, operation, mentoring, diagnostics and monitoring.

III. SECURITY AND PRIVACY ISSUES IN TELEMEDICINE

As an individual, he/she have right to privacy, that is, having control over personal information such as name, social security number, medical diagnoses, shopping habits, work history and credit score. Therefore the right to privacy is the ability to limit who has this information, how the information is kept and what can be done with it. For this reason, Electronic Patient Record (EPR), EPR on a network requires a systematic content validation to provide quality control such as correctness and reliability of the source. In telemedicine, file sharing may create new security and customer privacy issues. There are numerous potential risks to privacy in any health care activity that requires the exchange of patient information between organizations or individuals.

The potential for protected health information to be exposed when organizations or individuals cooperate in a telehealth/telemedicine interaction may be greater than face-to-face interactions, particularly when telehealth activities are not integrated into an organization's usual practice patterns [26]. The security of medical images, derived from strict ethics and legislative rules, gives rights to the patient and duties to the health professionals. This imposes three mandatory characteristics: confidentiality, reliability and availability [27]. Table 1 shows the security services and their application in telemedicine.

Other security issues include data access, and storage; this is because eavesdropping and skimming are possible when the sensor data is transmitted wirelessly. Yet another issue is data mining. When mining on human data, there are unique privacy and security constraints that limit what collection, distribution, and analysis can be done, in which some of this large amount of medical data is not stored electronically and cannot be mined. While the type of data mining done on this information has security and privacy concerns, the heterogeneity of the databases and the scattering of the data throughout the medical care facilities also contributed to the security issue [28]. Furthermore, the lack of standardized regulatory framework, that is, different states have different laws.

Table 1: Security and their applications to telemedicine.

Security Services	Description
Availability	It is a timely access to data. Patient information and images needed should be readily available even when there are unpredicted power outages or hardware/software failure [8]. Availability also involves ensuring that data are prevented from disasters such as natural disaster, machine faults, etc. which may cause unavailability of data.
Confidentiality	Prevention of medical data and images from disclosure, that is, information is only accessed by authorized individuals.
Integrity	It is the ability of an image and information of a patient to be used by authorized personnel.

IV. THREATS/ATTACKS ON SECURITY AND PRIVACY

Attacks on security are described based on the function of the computer system as provision of information. Normally, communication is represented as a flow of information from a source to a destination. However, with a security threat [27], it can take a new form such as shown in Figure 3. Since telemedicine involves the use of the Internet to connect patient and the health care givers, it makes it vulnerable to attacks and most of the network attacks are possible on telemedicine data. The attacks can be grouped into two broad categories of active and passive attacks, as shown in Figure 4.

Active attacks involve attackers engaging in modification, interruption or fabrication of patient images and information such as replay or retransmission to produce an unauthorized effect, modification of message as well as masquerade (pretends to be some other entity and denial of service). Passive attacks are mainly where the attacker merely eavesdrops and monitors a system performing its tasks or collects information. This includes interception of information, though not alteration or addition of information. Traffic analysis of information involves observing message patterns service to valid users and releasing of the message content which may be carrying sensitive or confidential data.

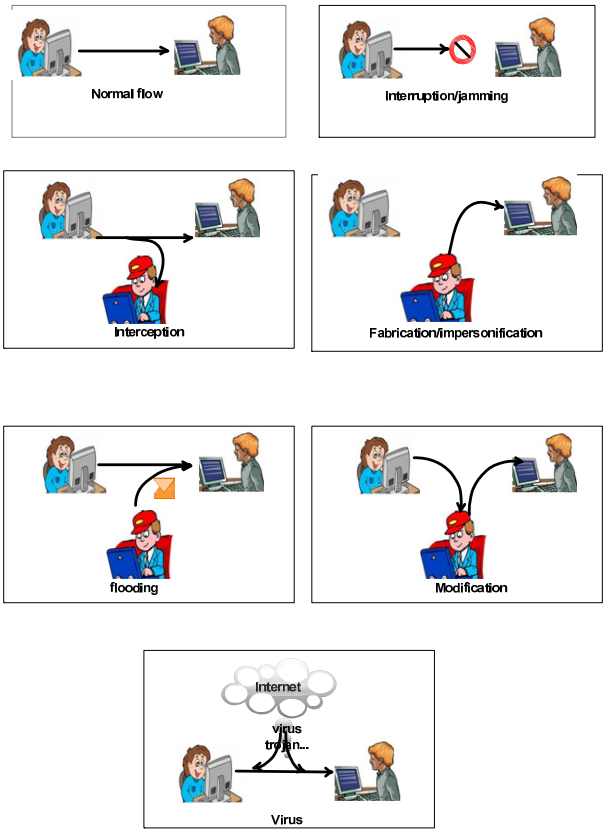

Figure 3: Flow of Security attacks/threat.

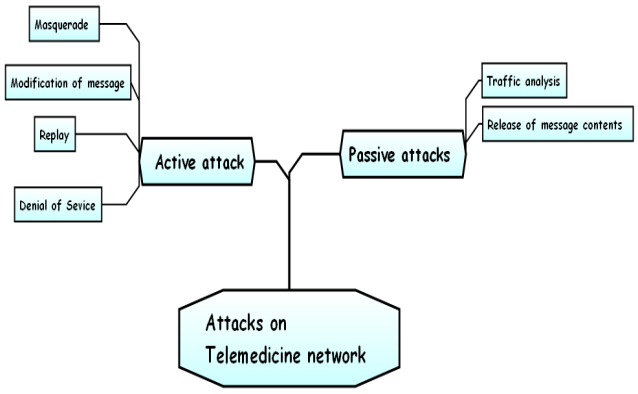

Figure 4: Types of attacks on telemedicine data.

V. DIGITAL WATERMARKING AS A MEANS FOR CURBING PRIVACY AND SECURITY ISSUES

Watermarking, in contrast to encryption, has been used for centuries to prove the authenticity of bank notes, postage stamps and documents [29]. Digital Watermarking is a tool use to fight against digital piracy, to authenticate and verify the integrity of digital media. Though watermarking does not prevent copying, but depending on the application, it helps both health care giver and patient to differentiate what content is authentic and what is counterfeit**.** Digital Watermarking is also used in monitoring and tracking illegal copies of digital media, filtering, communicating copyright messages and deterring alteration of multimedia content [30-31].

Medical images such as fundus and mammograms contain diagnostic information which can be used for early detection of retinopathy, breast cancer diseases/breast abnormality respectively. Protection and authentication of such images are now becoming increasingly important in telemedicine environment. For medical images such as mammograms, it should be ensured that embedding a watermark does not interfere with the diagnostic information in the mammogram [32].

Digital watermarking has become a matter of more concern over the past few years and preferable to other traditional methods of protecting data integrity and authentication of information resources. This is due to digital watermark's crucial features such as; imperceptibility, inseparability of the content from the watermark, and its intrinsic ability to undergo the same transformation experienced by the host signal. This preference has been established to provide improved security [33].

Digital watermarking addresses issues related to intellectual property, image authentication, copyright protection, device control, tamper detection, data monitoring/tracking, labelling and ownership or license identification. In digital watermarking, the object being communicated is the cover or host signal and the watermark provides additional information about the cover. It can be used to hide plain text, serial numbers, images or encoded information which makes it useful in various applications [29].

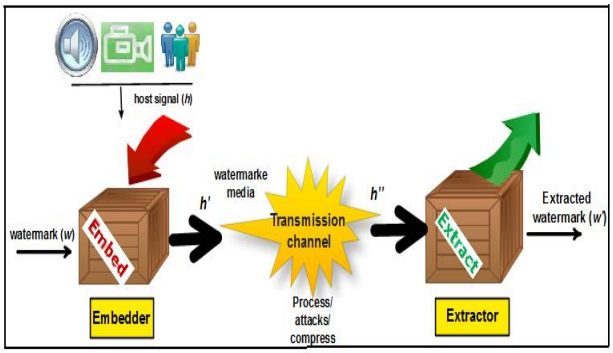

Figure 5: Generic Digital watermarking scheme with embedding and extracting block [29].

A typical digital watermarking system consists of two generic building blocks; the watermark embedding block and extractor block also known as watermark recovery block. The embedding block inserts the watermark information in the data while the recovery block extracts the watermarked information as shown in Figure 5. Another requirement of a watermarking system is robustness of the algorithm against attacks. Robust watermarks are designed to survive common distortion and resist deliberate/malicious attacks [34].

Several methods have been suggested for watermarking medical images [35-38], both in spatial and transform domains. Authors in [39] demonstrated the transmission

and storage of medical data with images in noisy environment using error control coding techniques. A different scheme by [36] focused on security of medical image sharing among clinicians based on Shamir's secret sharing scheme which prevents unintentional disclosure of medical information to unauthorized personnel.

A system presented in [40] for authenticating mammogram images focuses on the effect of adding the watermark below the perceptual threshold scheme to increase security, confidentiality and integrity of medical images to transmit them via the internet by combining two watermarking techniques. A new blind method for embedding and detecting mammogram image using CVNN in transform domain was developed in [41]. The method focuses on imperceptibility and detectability of tampered images used for authentication. Most of the above methods are used in limited organizations thus, it is extremely important to assess the viability of incorporating appropriate watermarking technique in telemedicine to prevent potential damages.

VI. CONCLUSIONS

Telemedicine is an enabling technology that provides cheap and effective healthcare with interconnected sensor networks making it an ideal for remote patient monitoring. Currently, telemedicine is becoming a viable alternative that supplements conventional face-to-face health care service because of availability of ICT. The number of unnecessary admission and emergency visits to the hospital is reduced; at the same time, early intervention is facilitated.

However, privacy and security issues continue to plague telemedicine projects, especially due to the extensive use of information and communication technologies like wireless networks. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses health information security and privacy issues. Digital Watermarking has the potential to redress privacy-security problems that have plagued telemedicine. In this paper we discussed the privacy and security issues that arise when using telemedicine. We explored some of the existing solutions and found that Digital Watermarking is a means of data protection with minimal security and privacy risks.

REFERENCES

[1] F. E. Ferrante, *Maintaining Security And Privacy Of Patient Information.* Paper Presented At 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2006. EMBS '06. (2006, Aug. 30 2006-Sept. 3 2006).

[2] S. S. Furuie, M. S. Rebelo, R. A. Moreno, M. Santos, N. Bertozzo, G. H. M. B. Motta, et al., Managing Medical Images and Clinical Information: Incor's Experience. *, IEEE Transactions On Information Technology In Biomedicine, 11*(1), 17-24, 2007.

[3] O. R. L. Sheng, P. J. H. Hu, W. Chih-Ping, & Pai-Chun, M. Organizational Management of Telemedicine Technology: Conquering Time and Space Boundaries In Health Care Services. *IEEE Transactions On Engineering Management, 46*(3), 265-278, 1999.

[4] ONC, Office of the National Coordinator for Health Information Technology (2009), *ONC Commissioned Medical Identity Theft Assessment,* Accessed May, 2012 At http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__medical_identity_theft/1177

[5] B. Brewin, Cyber Criminals Overseas steal U.S. electronic health records, *NEXTGOV*, 2008. retrived May 2012 at: http://www.nextgov.com/nextgov/ng_20080516_2203.php

[6] I. Armstrong, Medical ID Fraud Booming, *SC Magazine,* 2012. retrieved May, 2012; http://www.scmagazine.com.au/news/299209 medical-id-fraud-booming.aspx

[7] B. T. Horowit, Utah Health Care Data Breach Exposed About 780,000 Patient Files, *Health Care IT News,* 2012. Retrieved May 2012 at: http://www.eweek.com/c/a/Health-Care-IT/Utah-Health-Care-Data-Breach-Exposed-About-780000-Patient-Files-189084/

[8] S. Das and A. Mukhopadhyay, Security and Privacy Challenges In Telemedicine, *Research Front*, CSI Communications, pp 20-23, 2011.

[9] Health and Human Services, OCR's Strict HIPPA's Enforcement Trend Continues, *Health Law Monitor,* 2012. Accessed April 2012. http://healthlawmonitor.jacksonkelly.com/

[10] HIPPA, Health Insurance Portability And Accountability Act , HIPPA, 2012) Accessed May 2012, At http://omhc.com/content/media/hipaa_glossary.pdf

[11] W. Lockwood, What Are Health Care Regulatory Agencies? Retrived April, 2012. http://www.ehow.com/about_5187634_health-care-regulatory-agencies_.html

[12] C. Busch, F. Graf,, S. Wolthusen, and A. Zeidler, *A System For Intellectual Property Protection. Fraunhofer Institute,* 2000.

[13] R.F. Olanrewaju, O.O. Khalifa A. Abdalla and A.A Aburas, Damageless Digital Watermarking Using Complex-Valued Artificial Neural Network, *Journal of Information & Communication Technology,* Vol 9, pp.111-137, 2010, ISSN 1675-414X.

[14] M. Salajegheh, Molina, A., & Fu, K. Home Telemedicine: Encryption Is Not Enough. *Journal Of Medical Devices, 3*, 2009.

[15] Continua Health, Personal Telehealth Overview, 2010. Accessed April 2012, Online At http://www.continuaalliance.org/connected-health-vision.html

[16] J. M. Fitzmaurice, *Telehealth Research And Evaluation: Implications For Decision Makers*, 1998.

[17] G. Eysenbach, What Is e-Health? *Journal of Medical Internet Research, 3*(2), 2001.

[18] E. Supriyanto, *A Suitable Telehealth Model For Developing Countries.* Paper Presented At The 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2011.

[19] R. Moore, J. Adams, A. Partin, S. Docimo, & L. Kavoussi, Telementoring of Laparoscopic Procedures. *Surgical Endoscopy, 10*(2), 107-110, 1996.

[20] Z Wang. and H. Gu, A Review of Telemedicine in China". Online *Journal of Space Communication*. Issue No. 14. 2009.

[21] A. J. Diver, H. Lewis, and D. J. Gordon, Telemedicine And Trauma Referrals—A Plastic Surgery Pilot Project. *The Ulster Medical Journal, 78*(2), 113, 2009.

[22] S. Norman, (2006). The Use Of Telemedicine In Psychiatry. *Journal Of Psychiatric And Mental Health Nursing, 13*(6), 771-777.

[23] B. R. Lee,, Cadeddu, J. A., Stoianovici, D., & Kavoussi, L. R. Telemedicine And Surgical Robotics: Urologic Applications. *Reviews In Urology, 1*(2), 104, 1999.

[24] R. Gomes,, Rossi, R., Lima, S., Carmo, P., Ferreira, R., Menezes, I., et al. Pediatric Cardiology And Telemedicine: Seven Years' Experience Of Cooperation With Remote Hospitals. *Journal Of Cardiology 29*(2), 181, 2010.

[25] J. M. Simpson, The Role Of Telemedicine In A Fetal Cardiology Service. *Archives Of Disease In Childhood-Fetal And Neonatal Edition, 96*(6), pp. 392-393, 2011.

[26] Center for Telehealth, Assessing Telehealth Operational and Technology Security Risks to Privacy, 2003. Accessed May 2012, http://hsc.unm.edu/som/telehealth/docs/AssessingPrivacyRisk.pdf

[27] J. Zain, and M. Clarke, *Security In Telemedicine: Issues In Watermarking Medical Images*, 2005.

[28] M. Meingast, T. Roosta, and S. Sastry, *Security And Privacy Issues With Health Care Information Technology*, 2006

[29] R. F. Olanrewaju, Development of An Intelligent Digital Watermarking Algorithm Via Safe Region", Unpublished PhD thesis, International Islamic University Malaysia, 2011.

[30] M. Hirakawa, anf J. Iijima, *A Study On Integrated Mobile Service Using Digital Watermark For Various Information Carriers*. 10th International Conference on Mobile Business, ICMB, pp.283-291, 2011.

[31] R. F. Olanrewaju, O. Khalifa, A. Abdulla, and A. M. Z. Khedher, *Detection Of Alterations In Watermarked Medical Images Using Fast Fourier Transform And Complex-Valued Neural Network.* Paper Presented At The 4th International Conference On.Mechatronics (ICOM), 17-19 May 2011.

[32] K. Engan,, Gulsrud, T. O., & Josefsen, K. R. *Watermarking Of Digital Mammograms Without Interfering With Automatic Detection of Microcalcifications*. 2003.

[33] R. F. Olanrewaju, A. A. Aburas, and O.O. Khalifa and A. Abdalla State-of-The-Art Application of Artificial Neural Network In Digital Watermarking And The Way Forward. Paper Presented At The *International Conference on Computing & Informatics (ICOCI 09),* Kuala Lumpur Malaysia. Malaysia, 2009.

[34] I. Cox, *Digital Watermarking And Steganography*: Morgan Kaufmann, 2008.

[35] J. Nayak,, P. Subbanna Bhat, U.R. Acharya & M. Sathish Kumar, Efficient Storage and Transmission of Digital Fundus Images with Patient Information using Reversible Watermarking Technique And Error Control codes. *Journal of medical systems*, 33(3): 163-171, 2009.

[36] M. Ulutas, G. Ulutas, & V.V. Nabiyev, Medical Image Security and EPR Hiding Using Shamir's Secret Sharing Scheme. Journal of Systems and Software., 341-353, 2010

[37] U. Niranjan, Simultaneous storage of medical images in the spatial and frequency domain: Acomparative study. *BioMedical Engineering OnLine*, 3: 17, 2004.

[38] A. Wakatani, " Digital watermarking for ROI medical images by using compressed signature image", Proc. of the 35th Annual Hawaii IEEE Int. Conf. on System Sciences, pp.2043-2048, 2002.

[39] J. Nayak, P. Subbanna Bhat, M. Sathish Kumar, R. Acharya Reliable and Robust Transmission and Storage of Medical Images With Patient Information, *International Conference on Signal Processing and Communications*, SPCOM '04. 2004.

[40] A. Maeder, J. Dowling, A. Nguyen, E. Brunton & P. Nguyen, Assuring Authenticity of Digital Mammograms by Image Watermarking. *Digital Mammography*, 204-211, 2010.

[41] Olanrewaju, R. F. Khalifa, O. O., Abdalla A., Aburas, A. A. A. M Zeki, Forgery Detection In Medical Images Using Complex Valued Neural Network (CVNN). *Australian Journal Of Basic And Applied Sciences* 5(7): 1251-1264, 2011.