Developing a Secure Distributed Electronic Health System Using Information Hiding Techniques

*Abdulsalam, Y.S., [1]Olaniyi, O.M., [1]Ahmed, A. & [2]Olaniyan, O.M.
*[1]Federal University of Technology Minna
[2]Federal University, Oye-Ekiti
E-mail: *abdulsalam.pg611937@st.futminna.edu.ng
Phone: +2348064157640

Abstract

In general, urban hospitals offer specialized healthcare services, while rural hospitals have limited services and normally offer only basic hospital facilities. Therefore, people in rural areas have to travel relatively long distances to urban hospitals for specialized healthcare services. Ever since healthcare information systems have been implemented, the importance of their security cannot be overemphasized, particularly in the brilliance of the fact that healthcare information systems are deemed to comprise extremely sensitive data. The idea of storing healthcare data in electronic form raises concerns about patient privacy and information security. A secure distributed system is design to mitigate any threats in a portion of the system that will endanger data confidentiality, integrity and availability. This enhancement on distributed systems enables isolation of elements so that an intrusion only offers physical access to a part of the system; averts computer break-in by malicious users, and possible attempts by registered users to exceed or abuse their privileges. This paper provides an insight on securing data in electronic health system using secure distributed computing through steganography and watermarking algorithms for information hiding. The successful design and development of the secure electronic health system will assist healthcare professionals to ensure trust and enhance work productivity for improved medical healthcare delivery in developing countries like Nigeria

Keywords: Confidentiality, Electronic Health System, Authentication, Security, Distributed System

iSTEAMS Conference Proceedings Paper Citation Format
Abdulsalam, Y.S., Olaniyi, O.M., Ahmed, A. & Olaniyan, O.M. (2017): Developing A Secure Distributed Electronic Health System Using Information Hiding Techniques. Proceedings of the 8th iSTEAMS Multidisciplinary Conference, Caleb University, Lagos, Nigeria. Pp 569-578

1. BACKGROUND OF THE STUDY

Telemedicine, which is the use of technology to deliver healthcare services from distance has been demonstrated as an effective way of overcoming certain barriers to healthcare, particularly for communities located in rural and remote areas [1]. In addition, telemedicine can ease the gaps in providing crucial care for those who are underserved, principally because of a shortage of sub-specialty providers. Therefore attempt to introduce computerized healthcare information systems should be able to guarantee adequate protection of the confidentiality and integrity of patient information [2]. The aim of which is not to replace face-to-face medicine, but more usually to improve people’s health in certain well defined situations [3].

Telemedicine mainly uses video conferencing equipment [4], which is an interactive technology that enables patient and health consultants at distant cites to establish a face to face session. In other to create a secured connection, effective security must be established between sessions. This involves combination of physical security, technical security, data integrity, availability of medical records, and most importantly data confidentiality between the practitioner and the patient. Managing health information through communication channels carries the risk that may adversely affect quality of care if such communication channels are not effectively secured. The integrity of the clinical workflow supported by the medical records must also be maintained.

Security considerations play an increasingly important role for distributed computing[5], and dependable distributed systems for open networks can no longer be designed without taking malicious attacks into account. High speed networks are used to integrate advanced visualization devices and workstations [6].There are many techniques that are available for protection of digital data, such as encryption, authentication and time stamping through digital signatures [7]. Also there exists another method that improved the safety of digital data by merging a low level signal directly into the digital data. This low level signal known as watermark can distinctly identify the ownership and provides the security to the digital data which can easily be extracted. In this paper, we provide an insight towards the application of information hiding techniques to the design and development of secure and scalable geographically dispersed electronic-health system as anticipated in [8].
The remaining section of the paper is organized as follows: Section II provides the review of related works, section III discusses brief underlying concepts of information hiding technique in medical domain and the research direction is discussed IV. Section V concludes and opens gaps for future research endeavours respectively.

Statement Of Problem

One of the main worries circling the globe today is how to provide efficient and effective quality health services. Conventionally, part of the constraints in making these efficient quality health services possible is the fact that patients and consultants must be physically present in the same location. Modern development in information technology have been able to rise the number of possible ways health care can be delivered to reduce this constraints, but the issue of patient confidentiality and the security of information remains paramount. Personal information stored in the Electronic Health Record (EHR) is precisely meant to be stored and only accessible to authorized personnel's. The requisite for efficient and effective transfer of patient's information is the key driver for huge investment in e-health.

Objective

The main objective of this study is to develop a secure distributed electronic health system using information hiding techniques, incorporated with image cystography and watermarking algorithm using discrete wavelet transform, Huffman compression and LBG algorithms for medical confidentiality

2. REVIEW OF RELATED WORKS

A number of related works exist in literature in the application of data hiding techniques to secure distributed e-health system for provision of medical data privacy, diagnosis and prevention of diseases at near and remote locations. In [9], a reversible watermarking technique aimed at medical record protection and biometric recognition system was proposed. The goal of this technique was to design a system that can better store sensitive information and protect data privacy. The technique used the integer wavelength transform to successfully create embedding space in high frequency sub-bands. The technique developed in [9]lacks simplicity and robustness against common image processing operations such as compression, filtering and additive noise.

Similar cryptographic data hiding technique was proposed in [10]. The proposed stego-based-crypto technique was designed around the combination of RSA Cryptographic algorithm and lifting wavelet transform Stenographic algorithm. The RSA algorithm was used to increase the security of the system. The technique employed two methods of embedding; embedding either in the low frequency sub-band of the lifting wavelet transform or embedding in all sub-bands of the lifting wavelet transform. Both methods of embedding obtained high imperceptibility improvement. The technique was highly designed with maximum image precision and a combination of hybrid hiding information technique but a little flaw arises in the number of embedded message character. Consequently authors in [8] synergistically applied Advanced Encryption Standard cryptographic technique in secure distributed system for medical data confidentiality which uses web real time communication for clinical teleconsultation and simplified multi-tier electronic health system. The results of the system performance evaluation showed that the developed system could assist healthcare professionals in developing countries to improve security, efficiency, trust, enhance work productivity and increase the operational speed of medical health delivery. However, attempt in[8], lacks advanced security techniques for automatic identification and enrolment of patient data in EHR and improved confidentiality and integrity of patient data.

Similar work was proposed by [11]which described the development and implementation of a public state-wide telemedicine network in the Brazilian's State of Santa Catarina. They implemented the Santa Catarina State Telemedicine Network as a public health telemedicine concept integrating large scale routine examination processing together with the regulatory process and associated decision making procedures. All access was performed via SSL connection and encryption keys for all hospitals must be issued and certified by the ICP-SC, Santa Catarina State Public Key Index Examination. Time stamping and Data Integrity for documents stored at the server, including images, second opinions and complementary data was issued a cryptographic hash which receives a reliable timestamp. The telemedicine network solved the solution of urgent medical services but did not put high security implementation into consideration in that the documents are signed without proper digital signatures, images are not properly encrypted, the cryptographic key lengths were too short and can easily be cracked. Authors in [11] only concentrated in providing immediate healthcare without proper security design considerations for future intrusions.

The development of a technique on neural cryptography with secure electronic medical records in telemedicine system was proposed in [4]. The synchronized time of an attacker is increased by three transfer functions in the hidden unit using Hebbian learning rule, left-dynamic unit using Anti-Hebbian learning rule. The output layer used different transfer functions, which reduced the feedback mechanism. The compressed electronic medical record (CEMR) was password-protected from combination of lower layers and upper layers' spy units' vector which increases the security of CEMR. The CEMR was encrypted and decrypted using 256 bits secrete key. The major limitation to this technique is the key length and sizes which consumes more power, CPU resources and also waste time in the cipher text transformation process. A novel approach to blind reversible data hiding based on integer wavelet transform was proposed in [12]. The algorithm organizes wavelet coefficients to generate wavelet blocks, and applies a novel method to classify these wavelet blocks based on Human Visual System (HVS). The Electronic Patient Record (EPR) is inserted based on the result of classification. The portions of an image which contains the significant information for diagnosis are called Region of Interest (ROI) and must be stored without distortion. This concept is implemented in the newly proposed method. It is desirable to embed data outside ROI to give better protection. Encryption of EPR is done to provide additional security. The proposed scheme also has large capacity for data storage, which is important for hiding EPR and has higher value of Peak Signal to Noise Ratio.

In this paper, we propose to design, develop and evaluate techniques to secure automated data transactions between RFID tags and Readers to enhance existing secure tele-clinical system to EPR as compared to the work proposed in [8]. Integration of countermeasure for Confidentiality, Integrity and Availability of threats and health message services for patient care management services as opposed to the implemented technique in [11] and most importantly the number of embedded character in the stego-document. The proposed technique shall make use of appropriate Watermarking and Stenographic techniques to ensure secure and seamless data transactions among geographically dispersed electronic-health system facilities for secure data confidentiality. Data availability in the technique shall enshrine appropriate packet scheduling algorithm for mitigation against possible denial of data service from erring malicious parties within the channel of remote data communication.

3. METHODOLOGY

3.1 Software Design Approach

The design applies Incremental Software Modelling and Agile Approach for the development of the tele diagnostic system. The incremental model combines the features of parallel and linear process flows in generating deliverable increments of the software in a way that will be similar to the increments generated through an evolutionary process flow as shown in Figure 1. This process flow mostly provides a series of different releases called increments otherwise also known as *"updates"*, this updates progressively provides efficient functionality for clients, as each increment is generated. This technique was adopted for the software design so as to reduce the work downtime and upload, rather than starting the entire coding from scratch, also, this model employs further reusability of the interface in other to enhance the entire process.

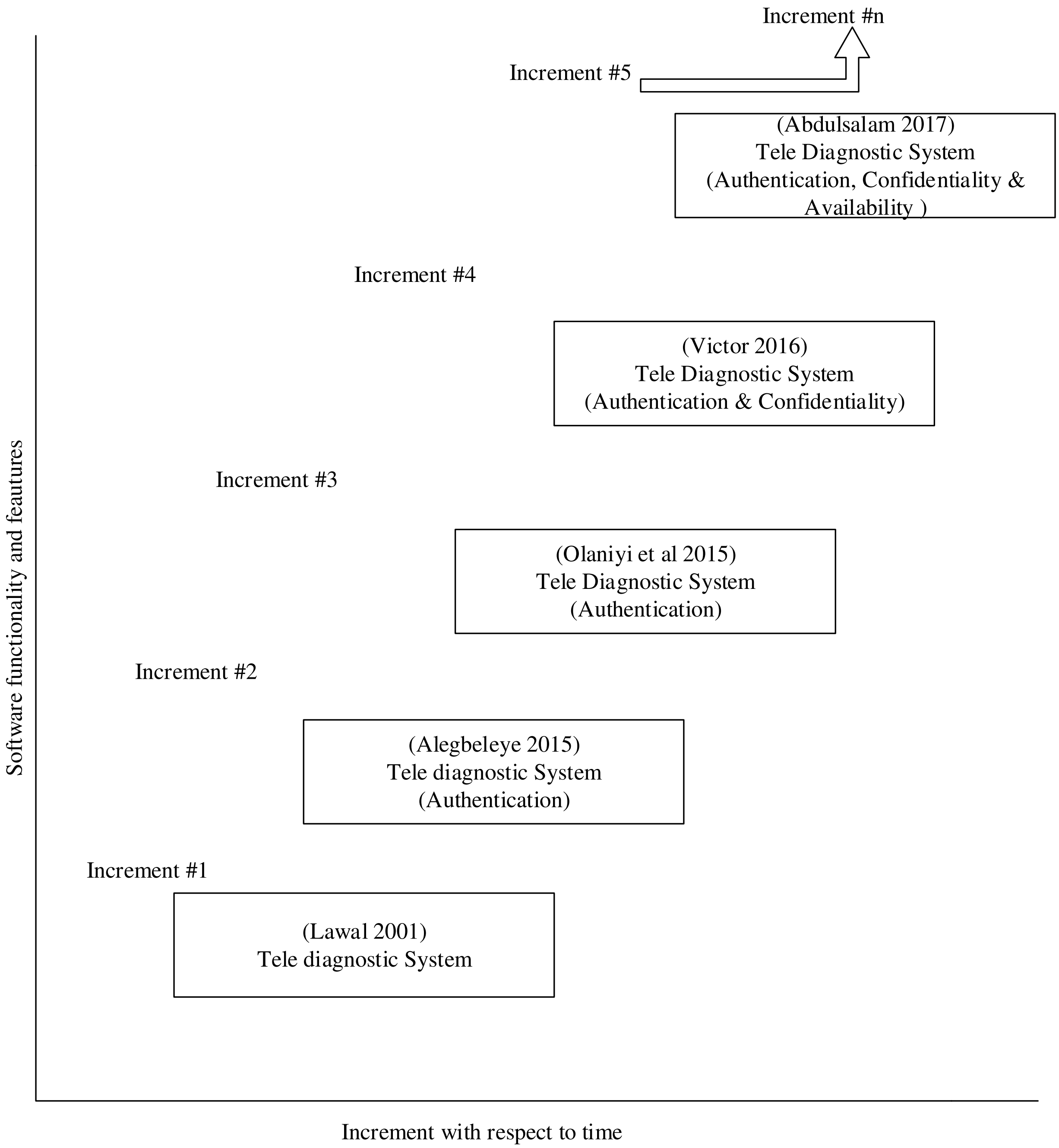

Figure 1: The Incremental Model [13-16]

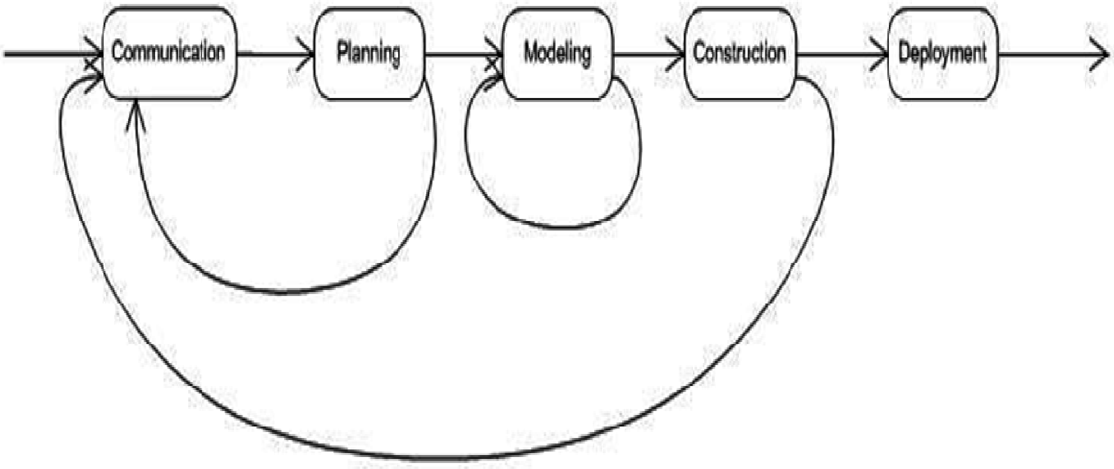

Figure 2. Process flow diagram

The Agile Approach mainly, promotes an orderly project supervision and management, which goes a long way in encouraging the adaptation, inspection, teamwork, accountability and self-organization. Also, it helps in focusing on individual communications over tools and processes, the functionality of the software over intensive documentation, client's cooperation over contract negotiation, and ability to respond to changes over following a plan. In the entire software design approach of creating the software, the generic process framework for software engineering was carried out as shown in Figure 2. These include communication, planning, modeling, construction, and deployment.

3.2 Application of Information Hiding Techniques in Secure Electronic Health Record

Medical image data hiding has strict constraints such as high imperceptibility, high capacity and high robustness. Achieving these three requirements simultaneously is highly cumbersome. These constraints are accomplished through data hiding, watermarking and steganography, which are suitable for telemedicine applications. None of these techniques is completely 100% reliable in all aspects of security protection. Electronic Patient Record (EPR) data hiding for telemedicine demand its information hidden and easily reversible so as to maintain integrity, confidentiality and availability of medical records. The next two sections propose an approach to hiding and recovering data, based on integer wavelet transform.

3.2.1 Image Wavelet Steganography

Steganography has been used immensely in various fields to maintain the confidentiality and integrity of messages transferred via the internet [17]. The need to hide messages has increased with the increase of fraudulent activities in the cyber space. A number of optimized and advanced steganography schemes have been invented by researchers to mitigate the number of such cybercrimes. Different optimization techniques like Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Genetic Algorithm (GA) and also hybrid optimization techniques like PSO-GA, PSO-ACO, GA-ACO) have been implemented by researchers so as to maintain the emphasis in a steganography implementation. In the sense that the deformity caused to the cover file due to the addition of secrete bit should be undetectable and the stego-document should have enough potential to stand an attack. There will be no loss of data during transmission and the message can be received correctly on the receiver's end. Steganography refers to the art and science of hiding secret information in some other media [18]. The information to be hidden is called the secret message and the medium in which the information is hidden is called the cover document. The cover document containing hidden message is called stego-document. The algorithms employed for hiding the message in the cover medium at the sender end and extracting the hidden message from the stego-document at the receiver end is called stego-system.

Number of EPR characters that can be embedded successfully is given by equation (1) and it is a function of three factors: the threshold value, the size of secrete medical image and lastly the bit depth of the medical image.

$$NOC = \frac{NM}{k}[k - (\log_{251} 2^{b})] \qquad 1$$

Stego images are created by hiding the share images into cover images; the criterion for the visual quality of the stego image is calculated using the Peak Signal to Noise Ratio (PSNR).

$$PSNR = 10 \log_{10} \frac{((2^{b} - 1)^{2})}{MSE} \quad dB \qquad 2$$

Where

$MSE \text{ is the mean square error between } C \text{ and } S \text{ image}$

$$MSE = \frac{1}{4MN} \sum_{i=1}^{2M} \sum_{j=1}^{2N} (C_{ij} - S_{ij})^{2} \qquad 3$$

$k = threshold\ value,$
$M \times N = size\ of\ secrete\ medical\ image,$
$b = bit\ depth\ of\ the\ medical\ image,$
$C\ and\ S = Cover\ and\ Stego\ image\ respectively.$

3.2.2 Wavelet Image Watermarking

Medical image watermarking is one of the important applications of watermarking. Medical image authentication systems cannot only authenticate medical images but would also be able to secretly communicate auxiliary information through watermarking technique. Only the authorized clinicians would thus be able to modify the content of medical image. The medical images can be transferred securely by embedding watermarks in Region of Non Interest (RONI) allowing verification of the legitimate changes at the receiving end without affecting Region of Interest (ROI) [7]. Segmentation plays an important role in medical image processing for separating the ROI from medical image.

Wavelet-based watermarking technique has ability to provide excellent multi-resolution analysis, space-frequency localization and superior HVS modelling. Discrete Wavelet Transform (DWT) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple “scale” wavelet decomposition. This allows the use of higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL, and HH). This domain also offers added benefits like increased robustness, tolerance to various compression algorithms and filtering.

In spread-spectrum communications, one transmits a narrowband signal over a much larger bandwidth, such that the detectability of signal energy present in any single frequency is impossible. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into a single output with high signal-to-noise ratio (SNR). However, to destroy such a watermark would require a noise of high amplitude to be added to all frequency bins and also, spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: that is, the location of the watermark is not obvious. A sample of an image going through security process in wavelet watermarking is shown in Figure 5, the depicted image is unnoticeable and can hardly be suspected of any embedded schemes.

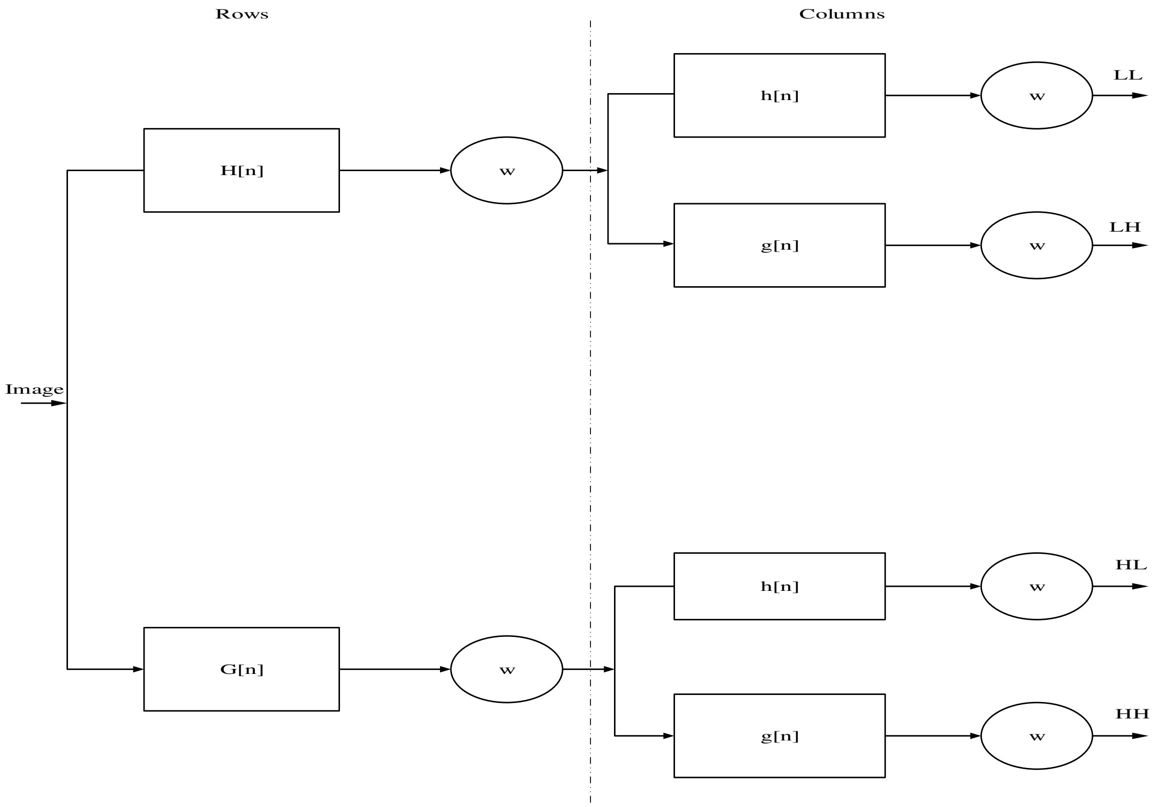

Figure 4: Filter Bank Structure used in wavelength decomposition of a message[7].

$$H[n] = \sum_{k} h_k \, e^{-jkn} \qquad 4$$

$$G[n] = \sum_{k} g_k \, e^{-jkn} \qquad 5$$

where

$h[n] = higher\ pass\ filter$

$g[n] = low\ pass\ filter$

$W = wavelet\ function$

The energy of the approximation and detailed images obtained can be calculated using equation (6).

$$e_k = \frac{1}{N_k M_k} \sum_{i} \sum_{j} |C_k(i,j)| \qquad 6$$

where

$k = approximation\ at\ each\ of\ the\ decomposition\ levels$

$C_k = cooficient\ of\ the\ sub\ band\ images$

$M_k N_k = corresponding\ dimensions$

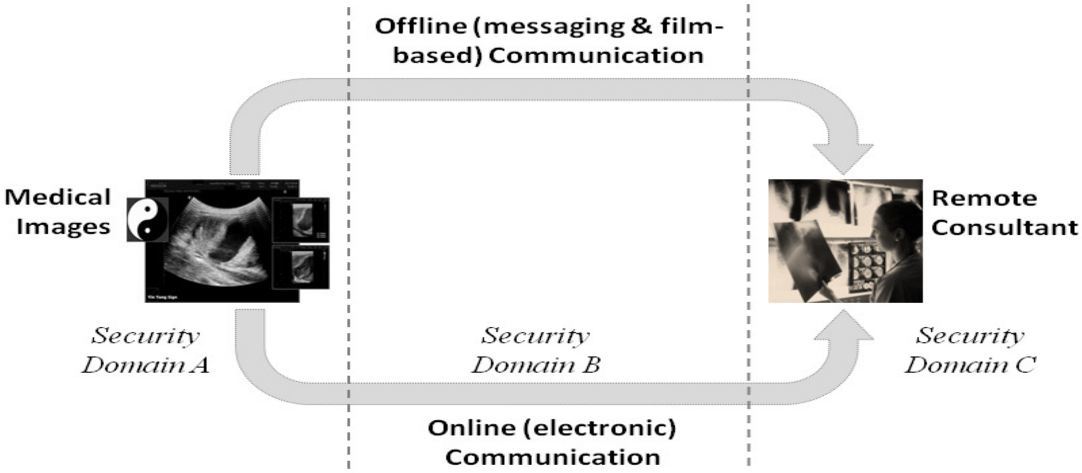

Figure 5.; Watermarking Security Process[12]

To embed the medical image shown in figure 3, the steps are.

1. Original medical image is transformed using integer wavelet transform.
2. Selection of two adjacent pixels in a row as a single block in the horizontal and vertical sub bands of level 1.
3. Identifying the highest pixel value from the block and division of the value by 2.
4. If block smallest pixel value is greater than the value obtained in step 3, block is selected for data embedding.
5. Then the first nibble of the data to be embedded is compared with the difference of the pixel values in the selected block.
6. If the first nibble of the data and difference of the pixel values are not the same then adjust the pixel value to make them equal.
7. Therefore, data is embedded in the HL and LH sub bands in level 1 excluding ROI.
8. Apply the inverse integer wavelet transform to obtain the embedded image.

The following steps are used in Data and Image Recovery

1. Transformation of the embedded image using integer wavelet transforms.
2. Repeat steps 2 and 3 of the data embedding process.
3. If block smallest pixel value is greater than the value obtained in step 2, then block contains the embedded data.
4. Obtain the difference of the pixel values in the selected block. This gives the embedded data.
5. Apply the inverse integer wavelet transform to recover the original image.

Generally, watermarking methods are meant to keep the capacity, imperceptibility and robustness of an image reasonably very high because authentication, integration and confidentiality are the most important issues concerned with EPR (Electronic Patient Record) data exchange through open channels and all these requirements can be fulfilled using suitable watermarks.

4. OUR RESEARCH DIRECTION

Based on the understanding presented in section 4, our research direction in this work is to design and develop a novel technique to address the problem of fundamental security issues of authentication, confidentiality and availability of secure distributed electronic health system in geographically dispersed health infrastructures. The secure system shall be designed around dispersed health infrastructures of Federal University of Technology Minna, Nigeria test bed. The University comprises of two campuses and a way to integrate e-health security into both campuses is shown in figure 4. Appropriate secure system requirement, design and development shall be carried out to provide results to solve authentication, confidentiality and availability. In order to eliminate security issues and provide seamless teleconsultation.

5. CONCLUSION

Providing an enhanced security environment for the deployment of Electronic Health Record (EHR) is of great concern, because the most likely scenario for the expansion of telemedicine services to rural countries will be through networks using Internet technology. Considerable measures are taken for those who do not adhere to good security and privacy practices. Therefore, a formal approach to managing the use and disclosure of personal health information should be in the best interests of patients, individual researchers, organizations and society. The technique of the anticipated secure tele-health system shall protect the confidentiality of patient's medical information from those who are not allowed access to such information. Also making it possible for neither the clinicians nor consultants to have information about highly reputable individuals prior to consultation. At this stage, the research is open to suggestions and criticisms. In future, the adoption of hybrid schemes with more efficient encryption mechanism will prove to be more effective in securing patient's information.

REFERENCES

1. Vo, A., R. Farr, and B. Raimer. *Benefits of Telemedicine in Remote Communities & Use of Mobile and Wireless Platforms in Healthcare* in *Telemedcine and Center for TeleHealth Research and Policy* 2012.
2. Smith, E. and J. Eloff, *Security in health-care information systems—current trends.* International journal of medical informatics, 1999. **54**(1): p. 39-54.
3. Craig, J. and V. Patterson, *Introduction to the practice of telemedicine.* Journal of Telemedicine and Telecare, 2005. **11**: p. 7.
4. Prabakaran, N., P. Saravanan, and P. Vivekanandan, *A new technique on neural cryptography with securing of electronic medical records in telemedicine system.* International Journal of Soft Computing, 2008. **3**(5): p. 390-396.
5. Deswarte, Y., L. Blain, and J.-C. Fabre. *Intrusion tolerance in distributed computing systems*. in *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*. 1991: IEEE.
6. Foster, I., et al., *A computational framework for telemedicine.* Future Generation Computer Systems, 1998. **14**(1): p. 109-123.
7. Rathi, S.C., *Medical Image Authentication through Watermarking Preserving ROI*, in *Department of Computer Engineering andInformation Technology*. 2012, College of Engineering, Pune: Pune.
8. Olaniyi, O.M., Foloronsho T.A., Omotosho A & Alegbeleyye I,. *Securing Digitized Campus Clinical Healthcare Delivery System*. in *1st International Conference on Applied Information Technology* 2015. Nigeria.
9. Guo, X.C., *Methodologies in digital watermarking: Robust and reversible watermarking techniques for authentication, security and privacy protection*. 2008, Citeseer.
10. Brifcani, A.M.A. and W.M.A. Brifcani, *Stego-Based-Crypto Technique for High Security Applications.* International Journal of Computer Theory and Engineering, 2010. **2**(6): p. 835.
11. Maia, R.S., A. von Wangenheim, and L.F. de Souza Nobre. *A Statewide Telemedicine Network for Public Health in Brazil*. in *CBMS*. 2006.
12. Navas, K., S.A. Thampy, and M. Sasikumar, *EPR hiding in medical images for telemedicine.* International Journal of Biomedical Sciences, 2008. **3**(1).
13. Victor, O.O., *Development of Secure Clinic Tele-Diagnostic System Using Enhanced Tiny Encrypted Radio Frequency Identification and Image Steganographic Technique* 2016, Federal University of Technology Minna.
14. Lawal, A.L., *Development of an Electronic Health System for Campus Use.*, in *Computer Engiuneering*. 2013, Federal University of Technology Minna, Niger State.
15. Alegbeleye, I.I., *Design and Development of Secure Tele Clinical Diagnostic System (A Case Study of Federal Uniiversity of Technology Minna Health Centre)* 2015, Federal University of Technology Minna, Niger State.
16. Olaniyi, O.M., Folorunsho, T. A., Omotosho, A., & Alegbeleye, I. *Securing Digitized Campus Clinical Healthcare Delivery System.* Paper presented at the 1st International Conference on Applied Information Technology Nigeria 2015b.
17. Guha, S. and D.K. Sarmah, *Current Status: Comparative Analysis Of Optimization Techniques Used In Steganography Schemes* International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 2015. **2**(12): p. 5.
18. Shikha and V.K. Dutt, *Steganography: The Art of Hiding Text in Image using Matlab* International Journal of Advanced Research in Computer Science and Software Engineering, 2014. **4**(9): p. 7.