

Securing Electronic Health Systems Using Enhanced Transform Domain Image Watermarking Technique

Abdulsalam Y. S, Olaniyi O. M., Ahmed A

Computer Engineering Department,
Federal University of Technology
Minna, Nigeria.

abdulsalam.pg611937@st.futminna.edu.ng, mikail.olaniyi; aliyu.ahmed @futminna.edu.ng

ABSTRACT

Abstract: The implementation of Electronic Health Records (EHR) in Telemedicine application has significant effects in the area of medical negligence liability. Exploring issues such as confidentiality, authentication and integrity raise several concerns as regards to the responsibilities service provider need to harbor following (EHR) implementation. A critical factor in storing and transmitting patient's information is to properly authenticate the integrity of patient's digital data. In these processes, the need to preserve the confidentiality of patient's is highly paramount. In most cases, an alternative is to embed all records in the intended image itself. Different schemes adopted in literatures seem to have effect on the diagnostic content. For instance, the Least Significant Bits (LSB) plane can be manipulated, due to its poor robustness and imperceptibility. This paper presents an enhancement to watermarking scheme in transform domain, with the use of Linde-Buzo-Gray (LBG) algorithm and Huffman compression technique. The objective of image compression is to reduce the redundancy of the image, transmit data securely and minimizing data size when transmitting data through communication links. The LBG algorithm further enhances the security of medical data in transit through simultaneous data compression and encryption prior to data concealment with discrete wavelet transform domain image watermarking technique. Analysis of the developed technique performance evaluation shows Peak to Signal ratio greater than 40dB and Structural Similarity ratio of 0.999. Therefore, the performance evaluation of the developed technique using these metrics revealed its adequacy to provide adequate confidentiality security pillar of medical data on transit in Electronic Health Systems.

Keywords: Watermarking, Electronic Health Record (EHR), Security, Confidentiality.

CISDI Journal Reference Format

Abdulsalam Y. S, Olaniyi O. M., Ahmed A (2017): Securing Electronic Health Systems Using Enhanced Transform Domain Image Watermarking Technique. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 2. Pp 103-118 Available online at www.cisdijournal.org

1. INTRODUCTION

In developing nations, the underserved population battles to benefit modern healthcare amenities. There is constantly lopsided number of children and elderly individuals with chronic ailments. Information and Data Communication Technologies has had a gigantic effect on this underserved populace by empowering access to healthcare services through telemedicine. Several application of telemedicine activities have attempted to interface the rural populace with medical facilities. Telemedicine has now made easy the way at which patients are been treated, examined and monitored, with patient and doctor located at diverse residence. Aside the concerns about information safety and privacy, the dissemination of Health Information Technology (HIT) and especially, EHR has several drawbacks which can lead to ethical complexities. Personal information stored in the Electronic Health Record (EHR) is precisely meant to be accessible by authorized personnel's only. The requisite for efficient and effective transfer of patient's medical data is one of the determining factor for huge amount of investment in e-health. Telemedicine application capable of transferring medical information between health practitioners at different locations, and connecting health personnel's has been found to be cost effective and time saving (Miller & Tucker, 2014).

The transition of medical information to digital format enables data transfer occur virtually in real-time. Angst (2009) commented on retaining patient's confidentiality in the era of digitization, and noted that patient healthcare information needs to be effectively secured in a networked environment. Providing security entails avoiding illegitimate access to health information by unauthorized personnel's, and at the same time safeguarding against unauthorized modifications of users' medical information (Al-Mawee, 2012). Security of therapeutic data is derived from established legislative rules which gives rights to patient and imposes privacy ethics on health professionals. These three mandatory privacy ethics are: confidentiality, integrity and availability as shown in Figure 1.

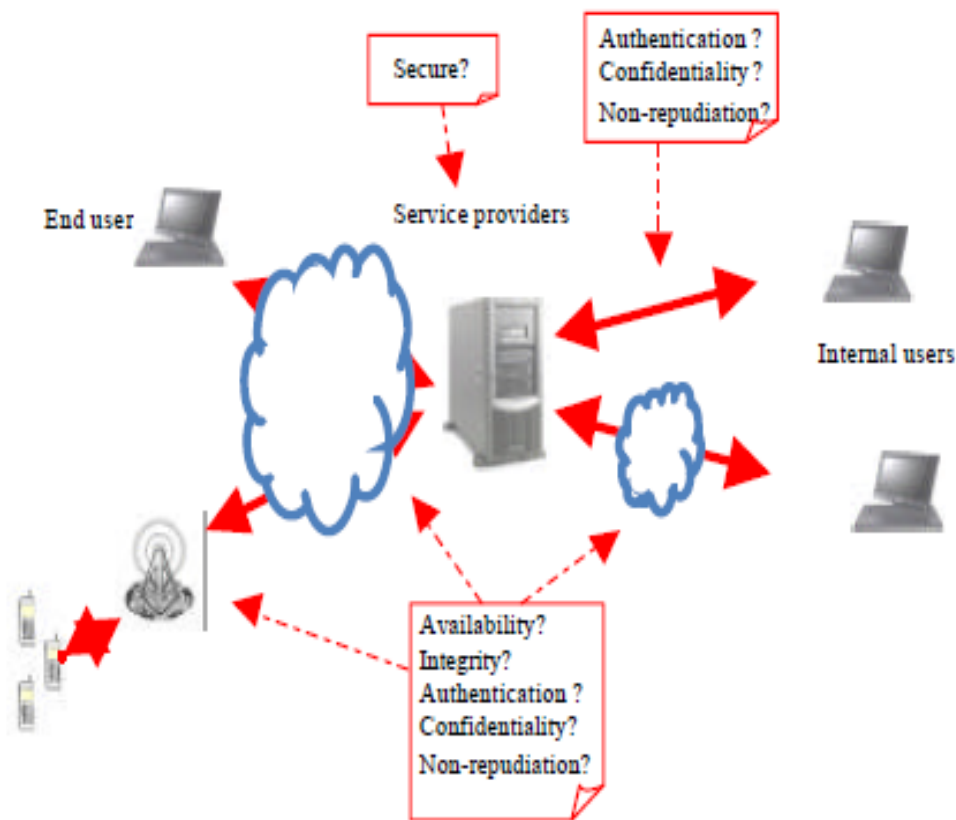


Figure 1: Telemedicine Security
Source (Zain & Clarke, 2005)

Addressing imminent security issues will successfully improve the availability and quality of therapeutic care by enabling distance health practitioner to treat, diagnose and assess patients in less-financially inaccessible locations. It can give productive intends to getting appropriate tertiary care counsel in underserved locations. By enhancing the security of restorative care, telemedicine can empower patients to look for treatment prior and hold fast better to their prescribed medicines, and enhance the personal satisfaction for patients with constant ailments, particularly for the elderly patient. Adoption and sustainability of EHR still carry heavy challenges in developing countries, mostly due to the fact that patients have less faith in unsecured technological networks (Mayoka *et al.*, (2012); Femi *et al.*, (2017)). Secured Primary Health Care (SPHC) delivery services would have a tremendous effect on the health of Nigerians. Many of the famous cost-effective health mediations to treat and prevent causes of morbidity and mortality in the nation and the progress towards health Millennium Development Goals (MDGs) can also be obtainable at this level of care. In addition, equity concerns draw attention to SPHC as the poor in Nigeria are more likely to seek care in SPHC facilities than the rich (FMOH & WB, 2005). Public contribution to major healthcare delivery has now been institutionalized in through the creation of Village Development Committees and District Development Committees and it has been shown that there are striking differences in their functioning in different states of Nigeria (Monica, 2014). Implementation of EHR will be of high benefit to individual and also to the masses, on the fact that EHR affords citizens an uninterrupted and effective way healthcare delivery (Femi *et al.*, 2017).

In this paper, we address the issue of confidentiality as regards to medical data in EHR system using transform domain watermarking technique, LBG algorithm for authentication and Huffman compression for data reduction as proposed in Abdulsalam *et al.*, (2017). The quantitative performance evaluation of the developed watermarking technique was carried out using MATLAB® image processing toolbox based on four performance evaluation metrics: Peak to Signal Noise Ratio (PSNR), Mean Squared Error (MSE) and Structural Similarity Index (SSIM). Further qualitative evaluation was achieved with Image Histogram visualization in MATLAB environment. The remainder of this paper is organized into four sections, section 2 presents review of related works, system methodology is provided in section 3, while discussion of results is presented in section 4. Conclusion and scope for future works is presented in section 5.

2. REVIEW OF RELATED WORKS

Various techniques exist for concealing data in different media. These strategies can either be spatial domain or transform domain. Spatial domain techniques like Least Significant Bit insertion, employs fundamental substitution techniques through encoding the mystery data by substituting insignificant parts of the cover with the secret message bits. The information can then be extracted if and only if the eavesdropper knows the positions where the secret bit has been inserted. When embedding in spatial domain, minor modifications are made in the implanting procedure which makes the sender accepts that further modifications cannot be made by malicious attackers, but this can only be true if there is no eavesdropper, and applying different compression techniques can easily damage the watermarks, simply by destroying the error bits.

Agarwal (2015) proposed an image watermarking technique using hybrid fuzzy architecture. The author was able to model the HVS in order for the extracted watermarks to yield a very high correlation coefficient. He further implemented fuzzy inference rule to determine the contrast, luminance, edge sensitivity and weight of watermarks. The model lacks robustness to very high attacks, but efficient and was able to overcome time complexity. Similarly, Yahya *et al.*, (2015) proposed a digital image watermarking technique using discrete wavelet transform. The authors implemented neural network training for pattern classification, the watermarks were later embedded after proper training of the algorithm. Three level wavelet decomposition was performed using haar filter and the discrete wavelet transform processes the watermark into four non overlapping sub bands. The technique achieved high correlation coefficients and an acceptable PSNR value. The final embedding was performed in the middle frequency coefficients of the sub bands and these possess a real limitation, due to the fact that, high concentration of the watermarks bits in the middle of the sub bands will reveal the frequency of the watermark.

Also, Santhoshi *et al.*, (2015) proposed a visible watermarking and image steganography technique by LSB extraction method. Least Significant Bit insertion was used to conceal the image in the non-region of interest using scale invariant feature transform. During extraction, the watermarks were successfully recovered with minimal error probability. Before embedding, the image was first converted into binary using the tradition LSB technique instead of fourier transform mechanism, which will in the end cause histogram distortion of the extracted watermarks. Though the PSNR value obtained was quite high and acceptable but the imperceptibility was quite low due to the LSB insertion mechanism. Kobayashi, Furuie, & Barreto (2009) enhanced therapeutic image security of medical images, by integrating stronger links provided during authentication of data in an image. In their research, Digital Imaging and Communications in Medicine (DICOM) images were implemented which further enhanced the security of the technique. Kannammal & Rani (2012) proposed sensitive watermarking algorithms for medical image confidentiality. Selective LSB bit plane were implemented and proper performance correlation metrics was analyzed. The algorithm was further analyzed using Independent Component Analysis and Wavelet Transform. With their limited scope, Zain, Baldwin, & Clarke (2014) proposed a reversible watermarking mechanism to further enhance the limitation to their work. The technique had better integrity and authenticity. In all of the above mentioned papers, data embedding was carried out in the ROI region which is easily detected by malicious attackers.

In the same vein, a novel way to deal with reversible information covering up in view of whole number wavelet change was proposed in Navas et al (2008). The calculation composes wavelet coefficients to produce wavelet squares, and applies a novel strategy to group these wavelet pieces in light of Human Visual System (HVS). The Electronic Patient Record (EPR) is embedded in light of the after effect of order. The parts of a picture which contains the noteworthy data for finding are called Region of Interest (ROI) and must be put away without bending. This idea is executed in the recently proposed strategy. It is efficient to embed information outside the Region of Interest (ROI) to give better insurance. Encryption of EHR was implemented to create better security. The proposed conspire likewise has huge limit with respect to information stockpiling, which is imperative for EHR storage and has higher estimation of Peak Signal to Noise Ratio.

A novel method to shade reversible information embedding based on wavelet transformation was presented in Navas *et al.*, (2008). The algorithm generated systematized wavelet transform coefficients blocks, and applied a novel technique to classify them, using Human Visual System (HVS). The EHR was inserted with the basis of the classification result. The region of the image which contained the noteworthy data (ROI) was maintained without any distortion. It was then desired to conceal the information outside the ROI in other to provide adequate protection. EHR encryption was then implemented to provide adequate security. The proposed technique also had huge data storage capability. Spatial domain methods like LSB substitution, spread spectrum, are trouble-free but not robust (Vallathan, *et al.*, 2016). The most significant portion in a medical image is known as Region of Interest (ROI). This portion becomes less robust when data embedding is done in spatial domain. However, different transform domains like Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are additionally robust to the same signal processing attack. This fact necessitates that the operations must be made in transform domain, so as to maintain its imperceptibility, robustness and capacity. LSB techniques provides embedded data prone to attacks with very little modification.

By simply applying signal processing attack techniques, a malicious attacker can easily destroy the embedded information entirely. Johnson & Katzenbeisser (2000) pointed out that, data embedding in the transform domain will prove to be more efficient and robust against attack. The effective robust watermarking techniques known have actually been found to be implemented in the transform domain. Transform domain techniques is capable of hiding messages in significant areas of the intending cover document which then provides efficiency against compression attacks and cropping as compared to the LSB insertion. Wavelet transformations could be applied on an entire image. Nevertheless, a trade-off exists in the amount and volume of data to be embedded to obtain high robustness and imperceptibility (Zain & Clarke, 2005). Most transform domain techniques are also independent of image formatting and efficient when using implementing lossy and lossless conversion formats. In this paper, a new digital message hiding technique is proposed, which utilizes watermarking in the transform domain, LBG Algorithm and Huffman Compression to properly secure patient information and at the same time maintaining patient's confidentiality, as compared to similar works in Kannammal & Rani (2012), Agarwal (2015), Yahya *et al.*, (2015) and Santhoshi *et al.*, 2015.

3. DESIGN METHODOLOGY

Confidentiality denotes non-exposure of data that represents a danger to the protection of patient's privacy. Privacy protection denotes the right to preserve certain information about oneself from others. The confidentiality of doctor to patient's relationship is regularly represented by medical morals as well as by law (Partala *et al.*, 2013). In this way, providing security to counter inappropriate confidentiality occurrences is a basic necessity for an effective and efficient health monitoring system. A summary of attacks common in EHR is shown in Table 1

Table 1: Summary of Confidentiality Attacks in EHR

Attack	Description	Active (A) / Passive (P)
Eavesdropping	Radio communication interference.	P
Location Tracking	Patients radio signal location	P
Condition Tracking	Tracking patient condition by outsiders.	P
Patient Impersonation	False claiming of patient private information.	A
Node Impersonation	Impersonation of nodes in a network	A
Side Channel Attack	Taking advantage and accruing sensitive information.	A/P
Traffic Analysis	Inferring and observing data flow.	P

Source (Partala, *et al.*, 2013)

3.1 Watermarking Technique in Information Hiding

The term watermarking first came to existence in 1993, when two watermarking strategies were proposed to conceal watermark information in pictures and images (Singh & Chadha, 2013). Watermarking technology guarantees security, copyright protection and data authentication of digital media (Zain & Clarke, 2005). Watermarking in another term is the signal embedding of secrete data (Watermark) in a digital or computerized media such as audio, video and image. The embedded data is later detected and extracted to uncover the genuine identity or property contained in the digital media. Watermarking can also be utilized for Broadcast Monitoring, Copyright Prevention, Data Hiding and Authentication.

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) (Abdulsalam *et al.*, (2017); Rathi, (2012)). It has now turned out to be a vital field of research in information hiding (Singh & Chadha, 2013).

3.2 Watermark Region Identification and Non Region Identification (ROI and NROI)

Every therapeutic image has basically two region identification, ROI and NROI. Diagnosis demands just ROI due to its sensitivity. As a result of this, little distortion in ROI would no longer be adequate for diagnosis, this gives reasons for why it should be well-preserved. The remaining region which is the NROI, is used to embed patient data. Utilizing edge detection strategies, it is possible to isolate ROI and NROI (Kumar & Kalpana, 2015). Several detection mechanisms exist, for instance, the Canny Edge, Marr-Hildreth detector and the 16 Gabor filter, implemented in separating ROI and NROI. In digital images, points are recognized by these techniques at which image brightness changes and used to separate these two region (Kumar, Kumar, & Chauhan, 2015). The frequency domain techniques are all implemented on MATLAB. Figure 4 shows a rain images ROI and NROI using the 16 Gabor filter. White and black represents the ROI and NROI respectively.

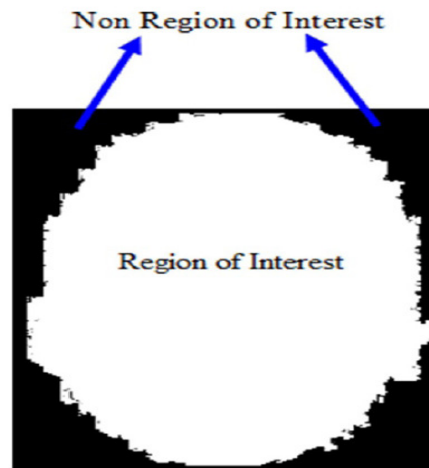


Figure 4: ROI and NROI
 Source (Kumar & Kalpana, 2015)

3.3 Developed Transform Domain Watermarking Algorithm.

Watermarking consists of three separate modules, watermark embedding, detection and the extraction module. Many applications of digital watermarking exist, which ranges from certification, protection, distribution and anti-counterfeit of digital data. Embedding in no region of interest sub bands creates high correlation and undistorted frequency distribution. Our medical image embedding and extraction procedure follows:

Embedding Procedure

Begin

Input:

An $M \times N$ host-image and a watermark.

Output:

Cover image

1. Divide host image into n blocks
2. Apply LBG algorithm to host image
3. Transform the entire host image into frequency domain by the DWT coefficients
4. Extract every data from watermark stream to be embedded.
5. Obtain generated random numbers which points to one n block of original image
6. Embed extracted the 8-bit watermarking data into the 8 lower band coefficients in the block pointed by previous step.
7. Repeat step 2 to 4 till watermark runs out.

Embedding Algorithm

Input:

An $M \times N$ host-image and a watermark.

Output:

Cover image

Divide host image into n blocks

for columns = 1: 8: 1024

 previousDct = 0;

 for rows = 1: 8: 1024

Apply LBG Algorithm

[M, N] = size(x);

[M2, P] = size(y);

if(M ~= M2),

 error('Matrix dimensions do not match.')

end

acquire Huffman table of secreta

Runlength coding

```

count = 0;
p=2;
runLenCoding = 0;
for i = 2:1:length(subZigzagArray)
    if subZigzagArray(i) ~=0
        runLenCoding(p) = count;
        p = p+1;
        runLenCoding(p) = subZigzagArray(i);
        p = p+1;
        count = 0;
    else
        count = count +1;
    end
end
runLenCoding(1) = firstDwt;
    
```

sequentially extract every 8 bit stream

```

[p,q] = size(redchan);
Embedd extracted bit
R = [rll];
G = [gll];
B = [bll];
routput = idwt2(rca,rch,rcv,rcd,'haar');
goutput = idwt2(gca,gch,gcv,gcd,'haar');
boutput = idwt2(bca,bch,bcv,bcd,'haar');
    
```

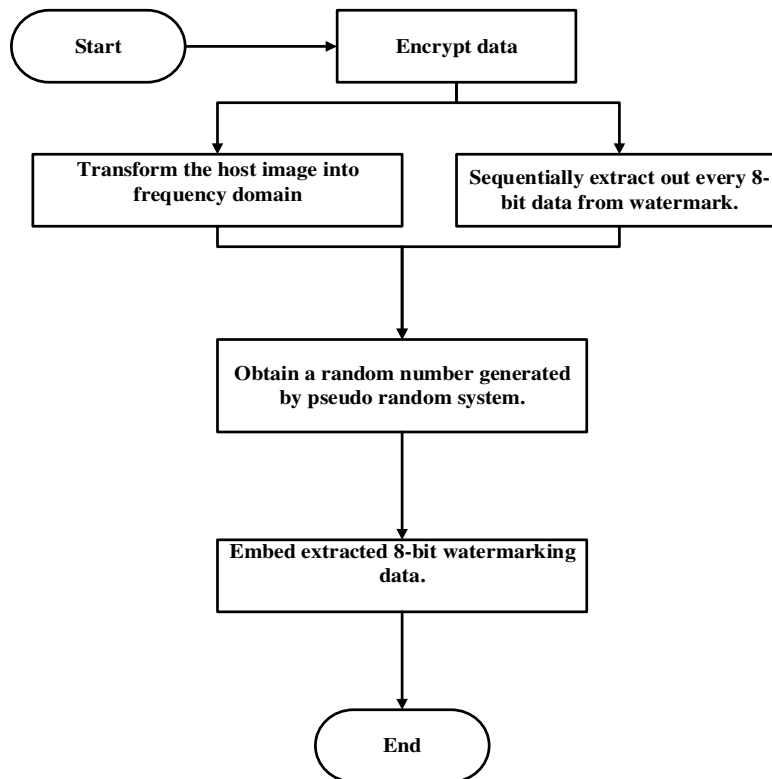


Figure 5. Flow Chat of the embedding algorithm

Extraction Procedure

Begin

Input:

An M×N Cover-image.

Output:

Host image and watermarked image.

1. Transform watermarked image by DWT.
2. Apply Run length encoder
3. Use set of generated random numbers applied in embedding process.
4. Apply generated random number to pinpoint the precise location of DWT block.
5. Extract watermark information from every DWT block by inverse embedding
6. Rearrange the 8-bit data into watermark image

Extracting Algorithm

Input:

An M×N Cover-image.

Output:

Host image and watermarked image.

Transform watermarked image to frequency domain

`redchanImg= img(:,:,1);`

`redchanImgWaterMarked= imgWaterMarked(:,:,1);`

Run length encoder

Runlength coding

`count = 0;`

`p=2;`

`runLenCoding = 0;`

Use set of generated numbers applied in the embedding process

Apply same random number

Extract watermark from DWT block by applying inverse transform

`greenchanImg= img(:,:,2);`

`greenchanImgWaterMarked= imgWaterMarked(:,:,2);`

`bluechanImg= img(:,:,3);`

`bluechanImgWaterMarked= imgWaterMarked(:,:,3);`

`Red = [rll];`

`RedW = [irl];`

`Green = [gll];`

`GreenW = [igl];`

`Blue = [bl];`

`BlueW = [ibl];`

Rearrange data into watermark

`rx = (RedW-(k*Red))/alpha;`

`gx = (GreenW-(k*Green))/alpha;`

`bx = (BlueW-(k*Blue))/alpha;`

`recoveredWaterMark = (rx+gx+bx);`

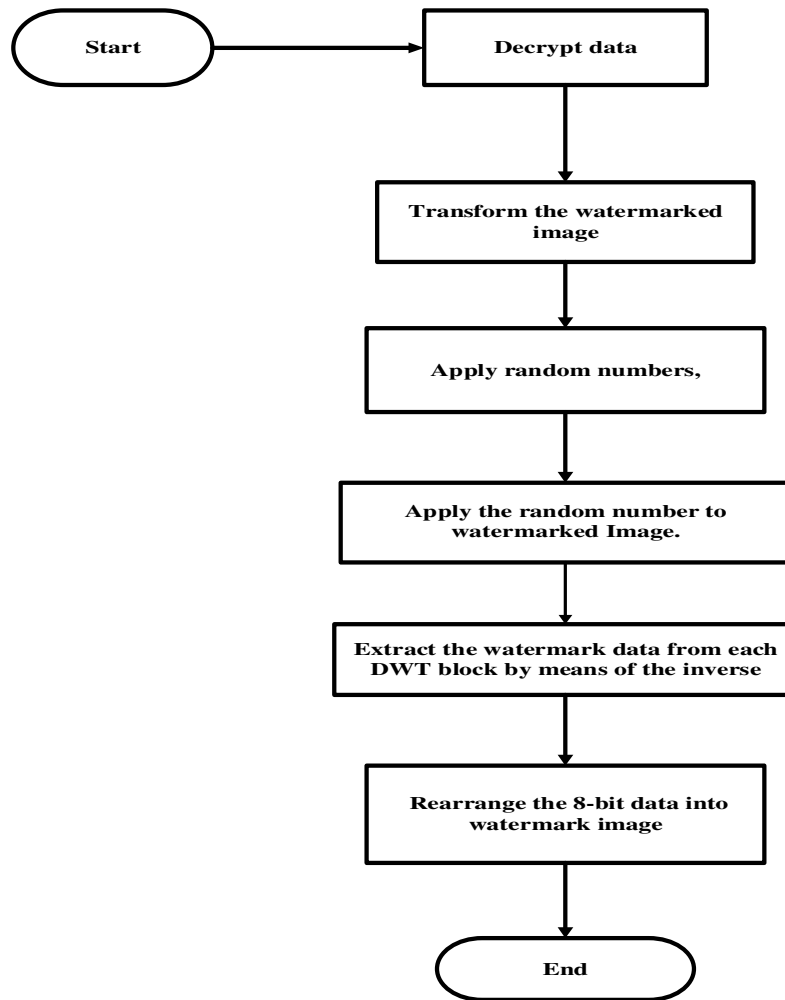


Figure 6. Flow Chat of the extraction algorithm

Generally, watermarking methods are meant to keep the capacity, imperceptibility and robustness of an image reasonably very high. Authentication, integrity and confidentiality are the most important issues concerned with Electronic Health Record (EHR) data exchange through open channels and all these requirements can be fulfilled using suitable watermarks (Abdulsalam *et al.*, 2017).

3.4 Performance Evaluation Metrics for Image Analysis

The Mean Square Error (MSE) signifies the collective error between output and original image. The lesser value of the squared error, the lesser the quality distortion, this can be calculated using Equation (1).

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

Where: C_{ij} denotes the significance of the pixel in input image, S_{ij} signifies the rate of pixel in output image, M and N are rows and columns respectively in the input image. The Peak Signal to Noise Ratio (PSNR) computes peak signal to noise ratio between two images, in decibels. This ratio is often used as a quality measurement between the original and output image. A high PSNR value depicts an image of high quality This can be calculated with Equation 2.

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

These two performance metrics are inversely proportional to each other. The value of PSNR increases when two images are close to each other whereas the value of MSE decreases when the two images are similar to each other. Using PSNR, images of values above **30db** are said to be of high quality.

The Structural Similarity Index Metric (SSIM) estimates the visual impact of shift in Image luminance, changes in photograph contrast which are collectively identified as structural changes in images (Olaniyi *et al.*, 2014). For two images x and y of common size $N * M$, SSIM is given in Equation 3 as:

$$SSIM(x, y) = \frac{[(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)]}{[(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_1)]} \quad (3)$$

Where:

μ_x is the average of x , μ_y is the average of y , σ_x^2 is the variance of x , σ_y^2 is the variance of y , σ_{xy} is the covariance of x and y ,

$C_1 = (k_1L)^2$ and $C_2 = (k_2L)^2$ are two variables to stabilize the division with weak denominator. L is the dynamic range of the pixel-values and $k_1 = 0.01$ and $k_2 = 0.03$ by default. As equation (3) approaches 1, the greater the degree of fidelity of the compressed image is close to the original image (Aibinu *et al.*, 2008). The dynamic range of equation (3) is given in Equation (4).

$$SSIM = [-1, +1] \quad (4)$$

The best value 1 is achieved if and only if the two images are similar and -1 if the two images are highly structurally un-similar (Olaniyi *et al.*, 2014).

4 Results and Discussion

The developed wavelet image watermarking scheme in Section 3.3 was quantitatively evaluated using metrics such as PSNR, MSE and SSIM. Further qualitative evaluation was done using Human Visual System (HVS) with image histogram visualization.

Experiments were carried-out using colored CT scanned images of sizes 512*512 embedded in a host image. Medical reports such as medical X-rays were embedded into a flower color image, which created the cover image. The recovered watermarks were in grey scale formats which added robustness, allowing proper recovery of the watermarks at lower correlation between original watermark and the extracted one. Perceptual quality of watermarked therapeutic image was evaluated using MSE and PSNR between watermarked and cover image as shown in Tables 2 and 3 respectively. Extracted watermark at the receiver's end was also evaluated by determining its correlation with original watermark.

Table 4 – 6 shows the original CT scanned images and the recovered watermarked images, by applying the developed watermarking algorithm in distributed LL sub band DWT coefficients. Extracted watermarks alongside the host watermarks are also shown. As observed during experimental analysis, the performance of the watermarking algorithm solely lies on the magnitude of watermark. As a result of this, serious deviation occurs in the histogram image, as represented in Figure 7 to Figure 11. So, the algorithm uses image sizes of 512*512. As the watermark size increases the performance evaluation of the PSNR reduces.

The metrics result presented in Tables 2 and 3 respectively shows that all PSNR value are greater than **50db** which depicts a high quality when using the Human Visual System (HVS). Tables 4, 5 and 6 shows the HVS comparison between host image, watermark, watermarked image and cover image. After adequately extracting different host images, the HVS shows nearly no difference when looking with the human eye. The Mean Square Error (MSE) as also evaluated in Tables 2 and 3 shows the collective squared mean error amongst different cover images. The algorithm provides a cover image of which calculated MSE value were observed to have a negligible difference that lie between 0.0235 to 0.0879.

The Structural Similarity Index (SSIM) results also shown in Tables 2 and 3 proves that the image similarity index is highly negligible and at an acceptable level, due to the fact that the value obtained is close to +1. Figure 7 – 11 shows the histogram realization of the host and cover images in red, blue and green channels, after embedding medical images respectively. For instance, Figure 7 shows the histograms of host images in Table 5. The histogram realization in Figure 7 when compared to Figure 8, indicates a little change in histogram deviation due to the result of the watermarked bit streams, because the watermark bit streams are of different sizes and correlation.

Table 2: Metrics evaluation of different cover images

Size of image M*N	Cover Image	PSNR	MSE	SSIM
512*512	Cover Image (flower 1)	65.7237	0.0235	0.9999
512*512	Cover Image (flower 2)	62.5849	0.0358	0.9999
512*512	Cover Image (ship)	60.1582	0.0879	0.9999

Table 3: Metrics evaluation of recovered watermarks

Size of image M*N	Recovered Watermark	PSNR	MSE	SSIM
512*512	Recovered (chest) Watermark	66.0102	0.0222	0.9999
512*512	Recovered (fingers) Watermark	68.0077	0.0200	0.9999
512*512	Recovered (wrist) Watermark	69.2493	0.0199	0.9999

Table 4: Human Visual System (HVS) Comparison of cover Image (flower 1) with corresponding cover images and watermarked images

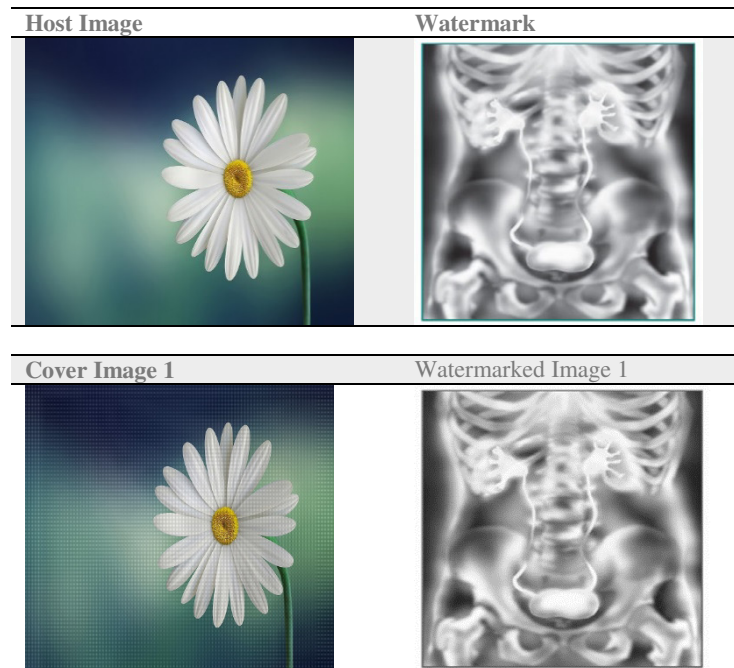


Table 5: Human Visual System (HVS) Comparison of cover Image (flower 2) with corresponding cover images and watermarked images

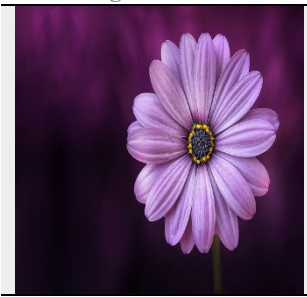
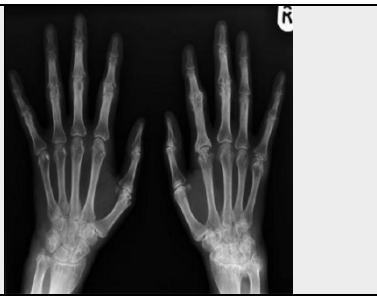
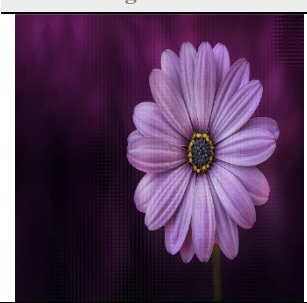
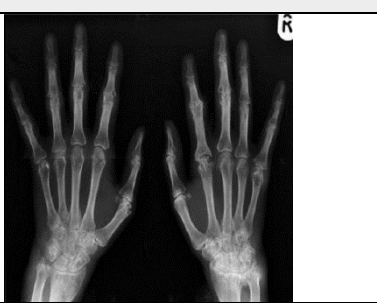




Host Image	Watermark
	
Cover Image 3	Watermarked 3
	

Table 6: Human Visual System (HVS) Comparison of cover Image (ship) with corresponding cover images and watermarked images

Host Image	Watermark
	
Cover Image 2	Watermarked Image 2
	

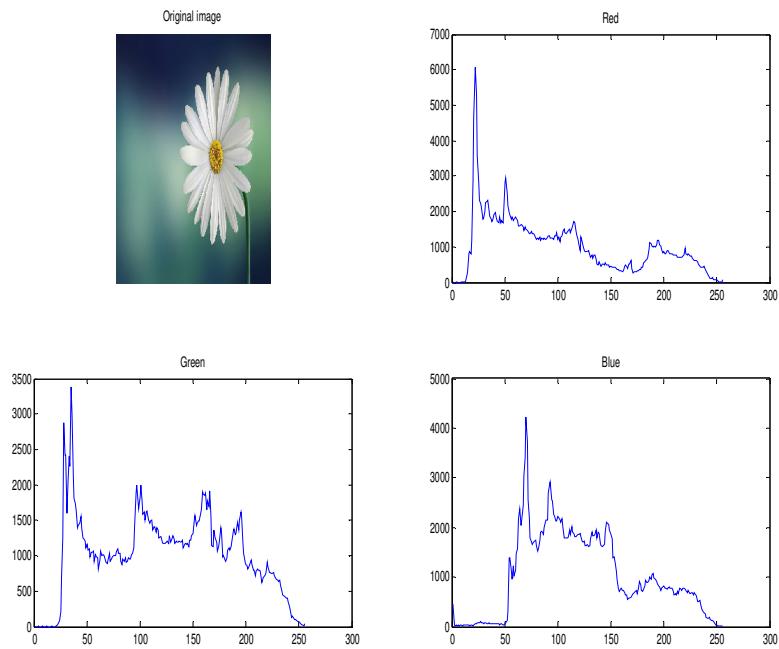


Figure 7. Histogram realization of stego host image 1.

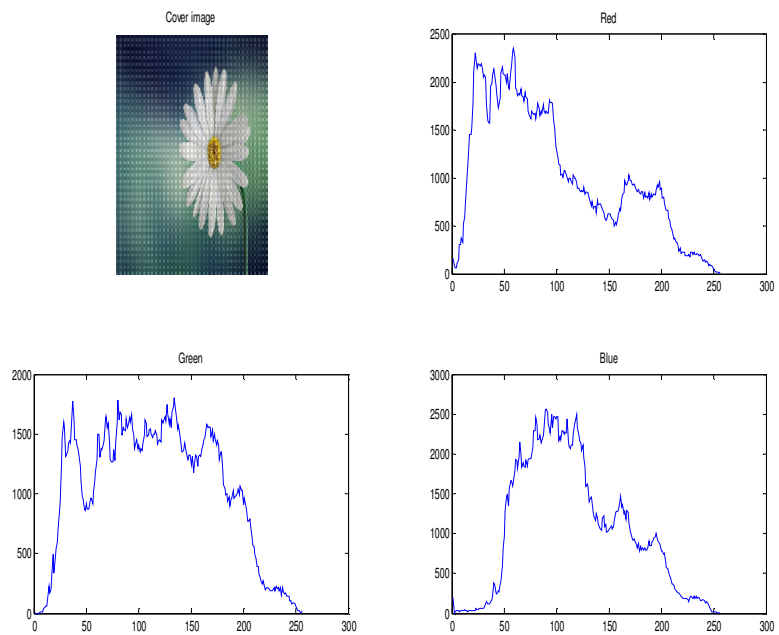


Figure 8. Histogram realization of cover image 1

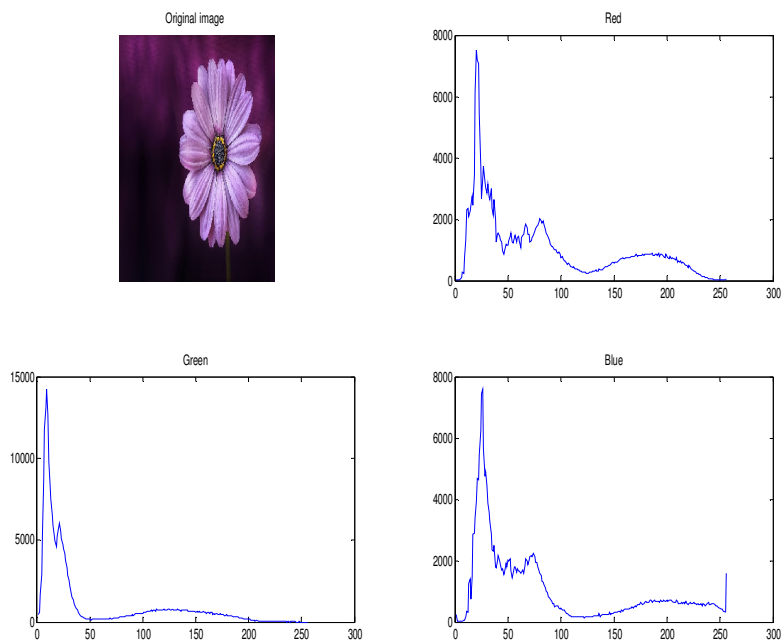


Figure 9. Histogram realization of host image 2

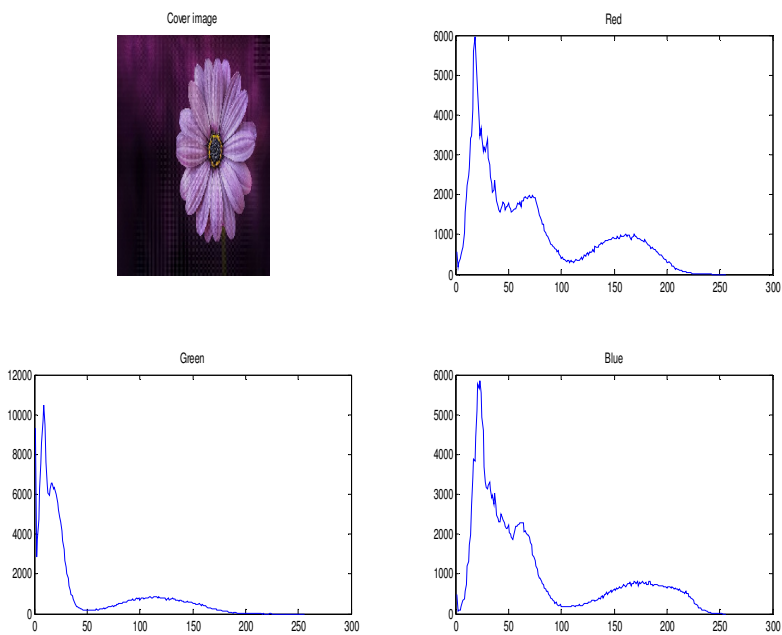


Figure 10. Histogram realization of cover image 2

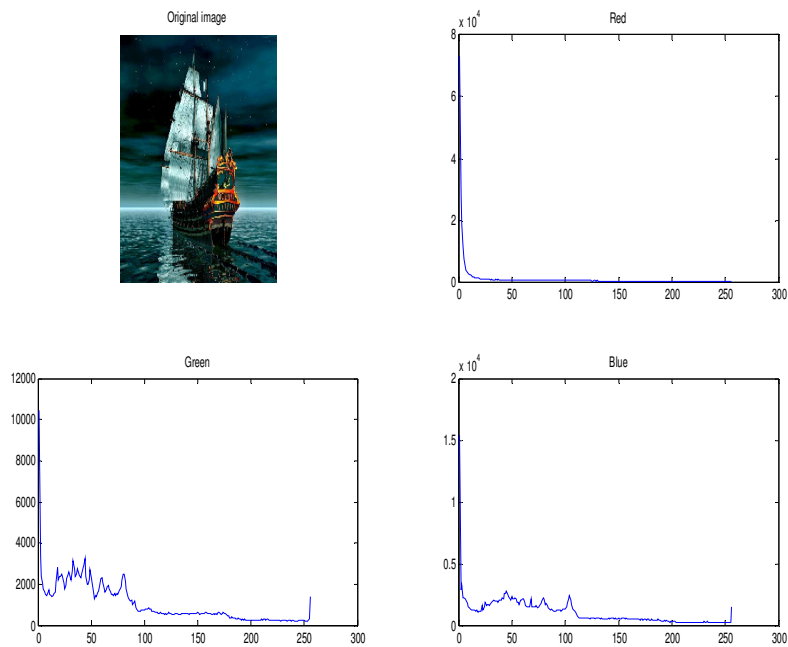


Figure 11. Histogram realization of cover image 3

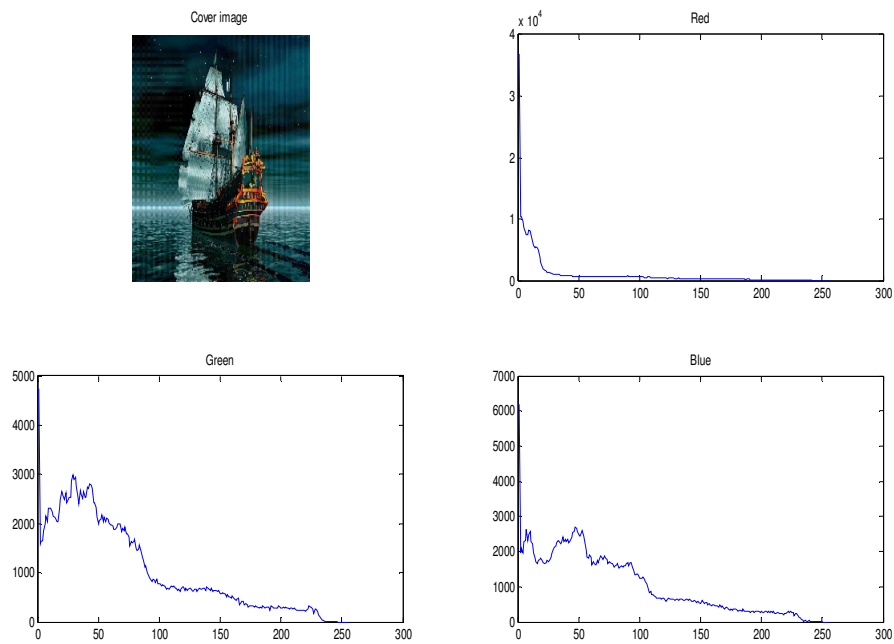


Figure 12 Histogram realization of cover image 3

4. COMPARATIVE ASSESSMENT WITH SIMILAR TRANSFORM DOMAIN IMAGE WATERMARKING SCHEME

The developed enhanced transform domain image watermarking technique for EHRs was compared with other existing techniques in literature. Transform domain techniques like Agarwal *et al.*, (2015), Yahya *et al.*, (2015) and Santhoshi *et al.*, (2015). From the comparative study, it can be inferred that the developed enhanced transform domain image watermarking technique performed better in terms of imperceptibility of cover image, high robustness to malicious attacks, using quantitative performance metrics from literature such as PSNR, MSE and SSIM values.

Table 7 shows the comparison of the developed enhanced transform domain image watermarking technique with other existing techniques from literature, the numerical comparison of PSNR metric values with existing image watermarking techniques with respect to cover images. The developed model was 30.58% and 21.32% better than Agarwal (2015) and Santhoshi *et al.*, (2015) respectively.

Table 7: Metrics comparison with similar works from literature

<i>S/N</i>	<i>Similar Transform Domain Image Watermarking Technique</i>	<i>PSNR (dB)</i>	<i>Percentage of Comparison (%)</i>	<i>SSIM</i>
1	Agarwal (2015)	45.12	30.58	0.9958
2	Yahya <i>et al.</i> , (2015)	60	8.33	0.9998
3	Santhoshi <i>et al.</i> , (2015)	51.14	21.32	0.9998
4	The developed technique	65		0.9998

5. CONCLUSION AND SCOPE FOR FUTURE RESEARCH ENDEAVORS

In this paper, we have proposed an enhanced image watermarking technique implemented in transform domain. The developed algorithm maintains and preserves patient's medical data confidentiality. The proposed image transform domain algorithm meets the requirements of high imperceptibility and adequate robustness. The algorithm was developed by embedding patient data in three level discrete decomposition LL sub bands of the host image. The obtained experimental results confirm the excellent imperceptibility of the extracted watermarks, as compared to related works in literature.

In future, further enhancement of medical data security will be to embed the encrypted image in different sub bands of the wavelet transform more like scrambling the text around the sub bands. Also, since DWT mechanism requires more computational power, more efforts will be made to further reduce the computational energy. This work will also be extended in future with hybrid optimization algorithms to enhance the contrast and luminance efficiency of the medical image.

REFERENCES

1. Abdulsalam S. Y., Olaniyi, O. M., Ahmed A., Olaniyan O. M., (2017). "Developing a Secure Distributed Electronic Health System using Information Hiding Techniques", Proceedings of 8th International Conference on Engineering and Technological Research, Caleb University, Imota, Lagos, Nigeria, pp 595-604.
2. Agarwal, C., Mishra, A., & Sharma, A. (2015). A novel gray-scale image watermarking using hybrid fuzzy-BPN architecture. *Egyptian informatics journal*, 16 (1), 83-102.
3. Aibinu A., Najeeb A. R., Salami M. J., & Shafie, A. A., (2008), "Optimal Model Order selection for Transient Error Autoregressive Moving Average (TERA) MRI Reconstruction Method", World Academy of Science, Engineering and Technology (WASET) Journal, 42(9), 161-165.
4. AL-mawee, W. (2012). *Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey*. Masters of Computer Science, Western Michigan University
5. Angst, C. M. (2009). Protect my privacy or support the common-good? Ethical questions about electronic health information exchanges. *Journal of Business Ethics*, 90(2), 169-178.
6. Femi E., Temitope O., Foluso A., Vekima N., Carole D., & Victor M., (2016). "Telemedicine Diffusion in a Developing Country: A Case of Nigeria". *Science Journal of Public Health*. 5(4), 341-346. doi: 10.11648/j.sjph.20170504.20
7. Kannammal, A., & Subha Rani, S. (2012). Authentication of DICOM medical images using independent component analysis (ICA). *International Journal of Medical Engineering and Informatics*, 4(2), 165-175.
8. Kobayashi, L. O. M., Furuie, S. S., & Barreto, P. S. L. M. (2009). Providing integrity and authenticity in DICOM images: a novel approach. *IEEE transactions on information technology in Biomedicine*, 13(4), 582-589.
9. Kumar, B., Kumar, S. B., & Chauhan, D. S. (2015). *Wavelet based imperceptible medical image watermarking using spread-spectrum*. Paper presented at the 38th International Conference on Telecommunications and Signal Processing (TSP).
10. Kumar, N., & Kalpana, V. (2015). A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. *Indian Journal of Science and Technology*, 8(16), 1-9.
11. Kumar, N., & Kalpana, V. (2015). A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. *Indian Journal of Science and Technology*, 8(16), 10-15.
12. Mayoka, K. G., Rwashana, A. S., Mbarika, V. W., Isabalija, S. (2012) "A framework for designing sustainable telemedicine information systems in developing countries", *Journal of Systems and Information Technology*, 14(3), 200 – 219.
13. Navas, K., Thampy, S. A., & Sasikumar, M. (2008). EPR hiding in medical images for telemedicine. *International Journal of Biomedical Sciences*, 3(1), 245-256.
14. Neubauer, T., & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International journal of medical informatics*, 80(3), 190-204.
15. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Okediran O. O (2014), "Performance Evaluation of Modified Stegano-Cryptographic Model for Secured E-Voting", *International Journal of Multidisciplinary in Cryptology and Information Security(IJMCIS), India, 3(1): 1-8*
16. Partala, J., Keräneny, N., Särestöniemi, M., Hämäläinen, M., Iinatti, J., Jämsä, T., . . . Seppänen, T. (2013). *Security threats against the transmission chain of a medical health monitoring system*. Paper presented at the IEEE 15th International Conference on e-Health Networking, Applications & Services (Healthcom).
17. Rathi, S. C. (2012). *Medical Image Authentication through Watermarking Preserving ROI*. MTech, College of Engineering, Pune, Pune.
18. Santhoshi B., Arghya R., Avishake G., Ananya R., (2015), "Image Steganography and Visible Watermarking using LSB Extraction Technique" IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) pp 500-556.
19. Singh, P., & Chadha, R. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9), 165-175.
20. Vallathan, G., Devi, G. G., & Kannan, A. V. (2016). *Enhanced data concealing technique to secure medical image in telemedicine applications*. Paper presented at the Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference.
21. Yahya A., Hameed A. J., Ainuddin W., Rafiddah M. N., (2015), " Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural networks". *Journal of King Saud University - Computer and Information Sciences*. 25(1), 393-401.
22. Zain, J., & Clarke, M. (2005). Security in telemedicine: issues in watermarking medical images. *Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia*.
23. Zain, J. M., Baldwin, L., & Clarke, M. (2014). *Reversible watermarking for authentication of DICOM images*. Paper presented at the Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE.