Watermarking Based Biomedical Image Integrity Control with DCT Lossless Compression

Mina K. Baby
Applied Electronics & Instrumentation
Electronics & Communication Department
MCET, Kerala, India
minakbaby@yahoo.com

Aswathy Madhu
Assistant Professor
Electronics & Communication Department
MCET, Kerala, India
aswathymadhu19@gmail.com

Abstract— In the recent years, with the advancement in the communication & information technology, the biomedical images play a very important role in the fields of Teleconsulting, Telediagnosis, and Telesurgery. In these cases, the medical data needs to be securely transferred over the insecure public network. In the field of Remote Telesurgery, the surgeon & patient is separated by significant distances. For the network transferred image, the integrity and confidentiality is a major issue, as the tampering of the medical images, results in serious issues in diagnosis and also treatment. And this would seriously affect the credibility of the health care institution. So, this shows that the image authentication in the medical field is of utmost importance. From this point of view, this paper focuses on enhancing the integrity of the network transferred medical data. The segmentation of the Region Of Interest(ROI) of the preferred medical image and the determination of its coordinates, and then the computation of the hash digest of the ROI by the Message Digest5(MD5) algorithm, would perform the partial encryption. Then, as a two-level security technique, Watermarking of the marked image with ROI and, it is followed by the Steganography with the concatenated hash digest, ROI coordinates & patient data. Finally, a Discrete Cosine Transform (DCT) based lossless compression is performed, for the sake of bandwidth & storage space during transmission.

Index Terms— Biomedical Image Integrity, Watermarking, Steganography, Message Digest5, DCT Lossless Compression

I. INTRODUCTION

Medical images are very crucial in diagnosis, treatment and are an important part of the medical information. The Medical Data can be defined as the information, contributing to diagnosis realization, a healing action for the prevention of health of an individual or a group of individuals. The medical images in a number of medical applications require atmost safety, security and confidentiality, as the information enclosed in these medical images makes critical judgements. Thus in the medical field, the biomedical image security becomes an important field of research and is continuously growing[1].

Digital Information Systems, Hospital Information Systems(HIS), and its special case like the Radiology Information Systems(RIS) and Picture Archiving & Communication Systems(PACS) form the information infrastructure of the modern health care[2]. Medical images are diagnosed by Radiologists by accessing through the intranet. If these medical images need to get a second advice from an expert foreign doctor, it should be transmitted through the public network. Specially in the field of telemedicine, which is the future of global health care[3]. It is a collective standard of medical information systems and information technology, where the computers store and forward medical information for long distances health care, for e.g., Remote Telesurgery[4]. In Telesurgery, the surgeons carry out minimally invasive operations with more control using robotic tools , as shown in Fig. 1. In Remote Telesurgery, the surgeon and patient are separated by miles of distances, as shown in Fig.2. The security concerns are of atmost importance, since any alteration of the medical data affects the patient care and health.

For the network transferred medical image, confidentiality is a major issue. The tampering of the medical image may cause serious issues in medical treatments like the loss of decisive information, misdiagnosis by physicians etc., potentially shaking the credibility of the health care institution. So, in Hospital Information System the major challenges existing are the techniques to verify the integrity of the crucial diagnostic

information.This demands for the adoption of security measures to assure data integrity and authenticity[5].

Fig.1. Remote Telesurgery

The rest of the paper is organized as follows. In section II, the related work is discussed. Section III provides a brief overview of the proposed system. In section IV, the studies of the proposed approach with the experimental results are discussed. Finally, in section V, the conclusions and future works have been discussed.

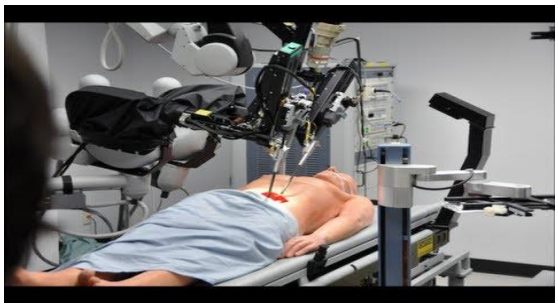


Fig. 2. Remote Telesurgery with Robotic Control Arms

.

II. LITERATURE SURVEY

Osamah M. Al- Qershi & Khoo Bee Ee [6] explained a very high embedding capacity Reversible ROI-based Watermarking scheme, where firstly the Region Of Interest(ROI) of the medical image is defined as a polygon and this ROI is compressed by JPEG2000, which can be used as a means of recovery in case of tamper detection. The ROI is divided into blocks of 16×16 pixels. Then the hash message of ROI is computed by Message Digest5(MD5) algorithm. The patient data is concatenated with the hash message and the resulting bit stream is Reed Solomen (RS) coded, which forms the watermark. This coded information is inserted into a pre-defined area in the Region Of Non-Interest (RONI) of the medical image.

Sonika C. Rathi and Vandana S. Inamdar [7] described a multiple watermarking embedding procedure, for the exchange of medical reference data between hospitals situated in different geographical locations. The medical images when transmitted through insecure network causes undesirable outcomes, thus demands higher security. The technique followed is: the host medical image is taken and from that the ROI is removed and saved. The remaining image with RONI is named as the original image. Multiple watermarks, which is to be embedded into the image is obtained from the patient information file, and is converted to binary. Now, to this binary converted file, the 4-level Haar Lifting Wavelet Transform is applied. The obtained watermark is inserted to the binary converted file to obtain the pre-watermarked image, which is followed by the application of the Inverse Wavelet Transform. To the obtained result, the ROI is combined to form the resultant watermarked image.

Anisha Joseph and Deepa S. S explained[8] that, in biomedical field, the transmission of medical images through insecure network causes the tampering of the image, especially the ROI, causing the mis-diagnosis by the physicians. So, the ROI region should be protected, for which a cryptographic one way hash of SHA-1 is used for the integrity control. The SHA-1 produces a hash message of 160 bit, which is embedded into the RONI of the image. The hash value of the image obtained after transmission is compared with the hash value computed before transmission, inorder to verify the integrity of the medical image transmitted.

Jagan Raj J., and Prasath S. [9] introduced a Steganography method with good security aspect for the medical images, where the image and text, both are intact and the mis-interpretation doesn't happen in the receiving end. The technique followed is: Firstly, the host medical image is read, and then the text message is also read, which is embedded in the image. Now, the hash digest of the resultant image is obtained by MD5/SHA-1/SHA-2. A Start Of Marker (SOM) is specified at the end of the image file and the obtained hash digest is appended to it, and then again the End Of Marker (EOM), is specified in the image. The resultant image is the output Steganography image, with the embedded checksum technique.

Abhishek Patanwar, and Shikha Singh [10] followed a simple to follow Least Significant Bit(LSB) Watermarking procedure. The technique is explained as: get the host medical image and convert the image pixels into binary values. Now, get the image, which is to be embedded as the watermark information. The information on the LSB plane of the cover image is replaced with the MSB plane of the watermark. After, the watermarked

image is obtained; a matrix with elements initialized to zeros, with the same dimension of the watermarked image is taken. Then, XOR-ing of each of the pixel of the watermarked image and the original image is done , and it is stored in the initially created matrix. During, the extraction phase, along with the watermarked image, this matrix is also transmitted. The elements in the matrix is checked, if it is 1, then the watermarked images
LSB, for each of the pixel is to be changed, otherwise keep the same.

III . PROPOSED SCHEME

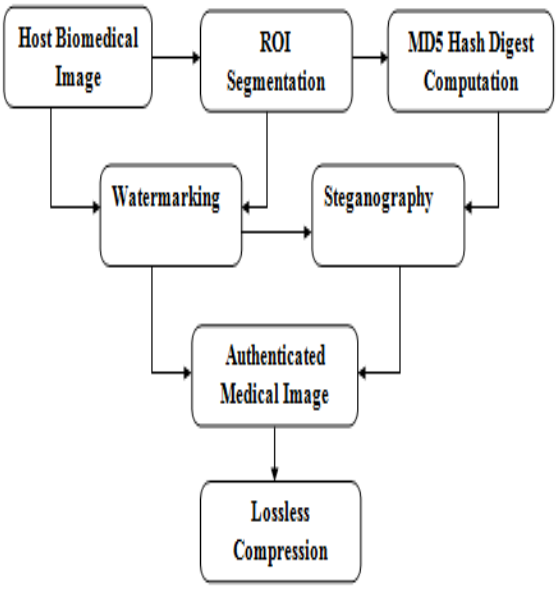
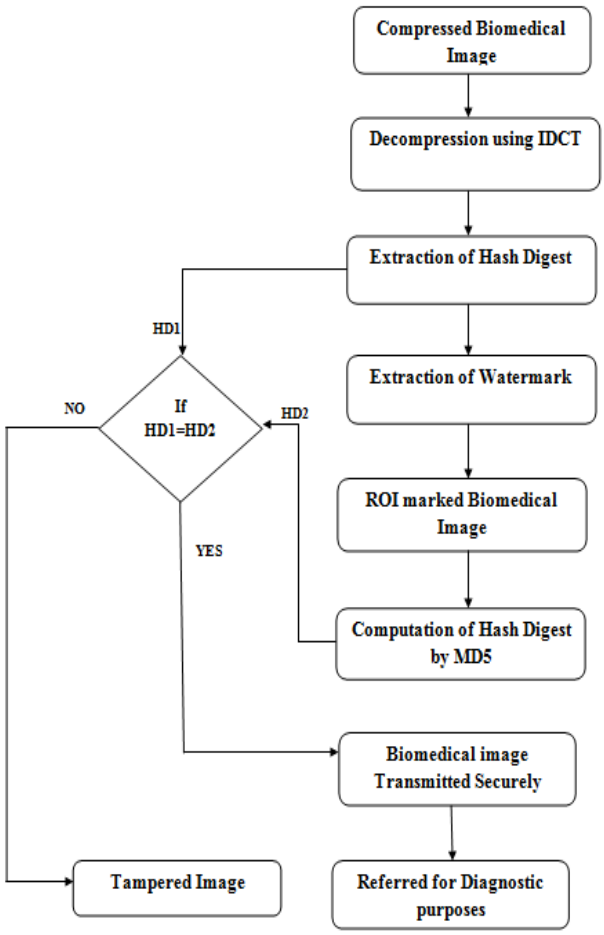


Fig. 3. Block Diagram of Transmitting side

The block diagram of the proposed method for the biomedical image transmission through the open network safely is shown in Fig. 3. For the host biomedical image, the ROI of the image is obtained and saved separately, and then the co-ordinates of the segmented ROI are determined. The hash digest of the segmented ROI is computed by means of Message Digest-5 (MD5) cryptographic algorithm, which performs the partial encryption. After this, the Digital Watermarking is performed, with the host image as the Base Image and the ROI as the Mark Image. Here, the LSB of the cover object, which contain no visual information, is replaced with the MSB of the ROI containing the most visual information. After which, the watermarked image is obtained. The hash digest produced is embedded in the first bit plane of the watermarked image, in order to obtain the steganographed image. The authenticated medical



images are compressed by means of the Discrete Cosine Transform (DCT) based Lossless Compression by dividing the images into 8-by-8 blocks.

Fig. 4. Block Diagram of Receiving Side

Fig. 4. shows the block diagram of the proposed system for the extraction of the biomedical image and the verification of the image integrity. Firstly, the network transmitted biomedical image will be decompressed by using Inverse Discrete Cosine Transform(IDCT) , which will be followed by the extraction of Hash Digest embedded in the image This is the Hash obtained after the transmission and is noted as HD1. Again, the extraction of the embedded watermark is performed. The blind extraction of the watermark is done, which does not need any information about the embedded watermark and will resolve the watermark easily by combining the LSBs from the different blocks of the Watermarked Image. Thus, the ROI marked biomedical image is obtained, from which the ROI co-ordinates can be determined and the Hash Digest can be computed for this, and is noted as HD2. Now, a comparison process happens between HD1 and HD2, whether HD1 = HD2. If HD1 = HD2, then the integrity of the transmitted image is verified successfully

and can be referred for the diagnostic purposes, but in the other case, image tampering has occurred.

A. Digital Watermarking

Digital Watermarking or Watermark embedding inserts the hidden information into the multimedia data. The multimedia data is called the cover media and the hidden information as the Watermark. After the watermark is embedded, the original cover media will be slightly modified and modified content is called Watermarked Data[11]. The LSB Watermarking technique used is in the Spatial Domain. This is the simplest approach of watermarking, which is used in this work and it would also mark the watermark recovery process less complex and time consuming.

Least Significant Bit Watermarking

In an 8-bit image, consisting of 8 bit planes, the Biplane 0 is the Least Significant Biplane and the Bit plane 7 is the Most Significant Biplane. The most visual information lies in the MSB of the image and the visual information starts to degrade when going from MSB plane to LSB plane of the image. The LSB plane of the image doesnot contains any important information. So, the LSB plane of the image is used for watermarking process [12], [13]. In Least Significant Bit (LSB) Modification technique, the MSB's of the watermark are replaced with LSB of the host digital data. The main advantage of this technique is that, after the embedding process, the quality of the host digital data is not affected by watermark data.

B. Steganography

Steganography is a technique of hiding the secret information within another digital media. The importance of steganography is that, it hides the existence of the secret data. That is, only the legitimate person knows about the presence of data. The concept of LSB embedding is simple. It exploits the fact that the precision in many image formats is far greater than that is perceived by the average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original image by a human being, just by looking at it[14].

LSB Steganography

The binary equivalent of the message, which is to be embedded into the image, is converted to binary, with each character consisting of 8 bits. This is distributed among the LSBs of each pixel in the image. The image pixels in the binary pattern are considered and the eight consecutive pixels from top left corner of the image is selected and the LSBs of the selected pixels are replaced by the MSBs of the binary equivalent of the text message[15].

C. Cryptographic Hash Functions

A Hash function maps a bit string of arbitrary length to a fixed length bit string. A typical data hash will process an input file to produce an alphanumeric string unique to the data file[16]. The Hash function is publicized, so that anyone can calculate the Hash and verify a received image.

Message Digest-5

This algorithm takes as input a message of arbitrary length and produces a message digest of 128-bit, and it is computationally infeasible to produce two messages having the same message digest. Suppose the message is a b-bit input. The computation of the message digest has given in the following steps:

Step – 1: Append padded bits.
The message is padded so that its length is congruent to 448, modulo 512. Single “1 bit is appended to the message, then 0” bits are appended.

Step -2: Append length.
A 64-bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.

Step – 3: Initialize MD buffer
A four-word buffer (A, B, C, and D) is used to compute the message digest. Each of the A, B, C, and D is a 32-bit register. These registers are initialized to the following values in hexadecimal.
Word A: 0x 01 23 45 67
Word B: 0x 89 ab cd ef
Word C: 0x fe dc ba 98
Word D: 0x 76 54 32 10

Step – 4: Process message in 16-word blocks
Four auxillary functions that take as input three 32-bit words and produce as output one 32-bit word.

Step – 5: Output
The message digest produced as output is A, B, C, and D. The output begins with the low-order byte of A and end with the high-order byte of B [17]-[18].

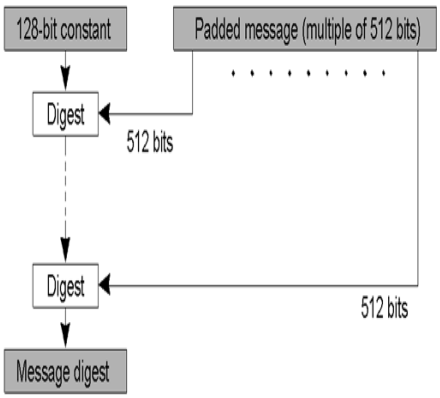


Fig. 3. MD5 Hash Digest

D. DCT Based Lossless Compression

DCT can be used in the image compression. The input image is divided into 8-by-8, and the two-dimensional DCT is computed for each block. The DCT coefficients are then quantized. In the decoding side, the quantized DCT coefficient are decoded, computes the inverse two-dimensional DCT of each block, and then puts the blocks back together into a single image [18]. The compression process is shown in Fig. 5.

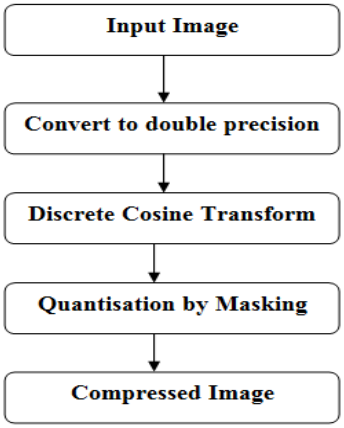


Fig. 5. DCT Lossless Compression

V. RESULTS & DISCUSSIONS

In this section, the performance of the proposed scheme for biomedical image integrity is evaluated. Five images as shown in Fig. 6-10 from different imaging modalities are used for evaluating the results.

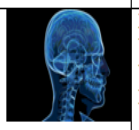
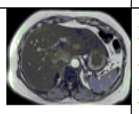
Sl. No.	Input Image	ROI Coordinates	Segmented ROI	Message Digest
1.		X1 = 210 Y1 = 110 W = 60 H = 75		Hash=24b2d8e73a76d333fb9e8971e2da71af
2.		X1 = 171 Y1 = 122 W = 71 H = 98		Hash=60998359a01301dd3ede538824c1171a
3.		X1 = 117 Y1 = 176 W = 99 H = 83		Hash=537722b72f5f5c2e2e9ec224a333283a
4.		X1 = 143 Y1 = 121 W = 44 H = 41		Hash=224476f95a1e277930449d2f1f8fb739
5.		X1 = 233 Y1 = 162 W = 69 H = 70		Hash=fb162bafe3fc53511db23f38a7a3dffd

Table. I. ROI coordinates & Hash Digest of various Input Images

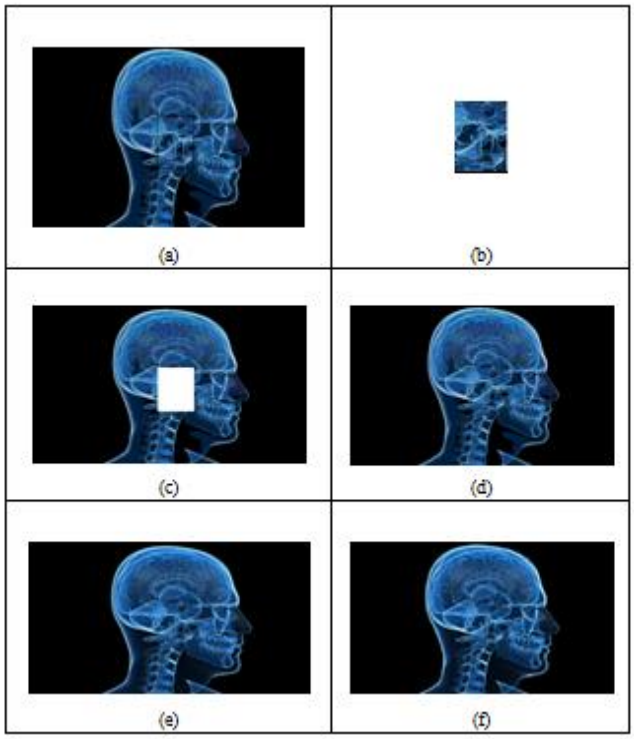


Fig. 6. Scanned Human Brain. (a)Input Image (b) Region Of Interest (c) Region Of Non-Interest (d) Watermarked Image (e) Steganographed Image (f) Lossless Compressed Image.

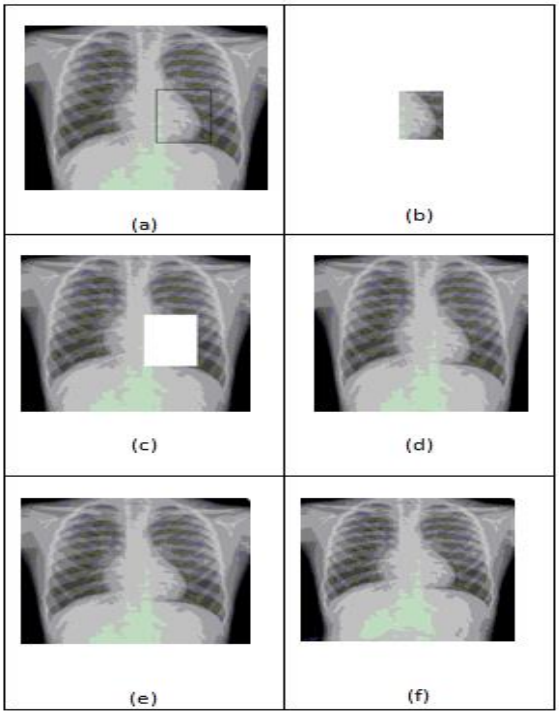


Fig. 7. Lungs Radiography (a)Input Image (b) Region Of Interest (c) Region Of Non-Interest (d) Watermarked Image(e) Steganographed Image (f) Lossless Compressed Image

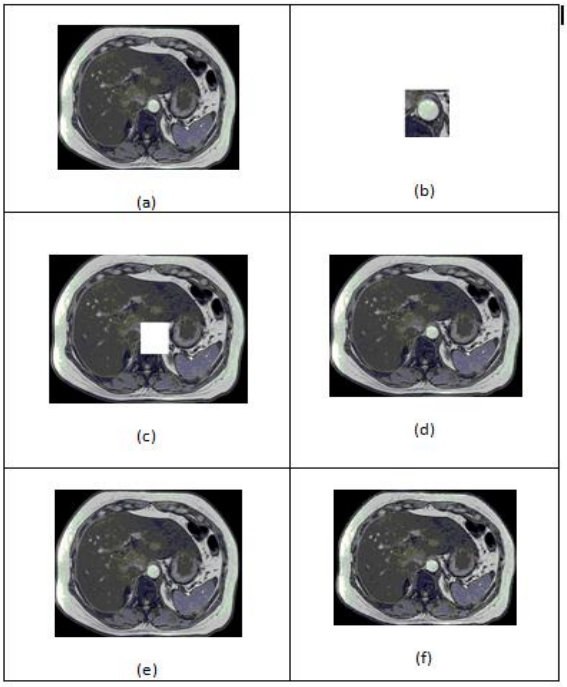


Fig. 10. Human Liver MRI. (a)Input Image (b) Region Of Interest (c) Region Of Non-Interest (d) Watermarked Image(e) Steganographed Image (f) Lossless Compressed Image

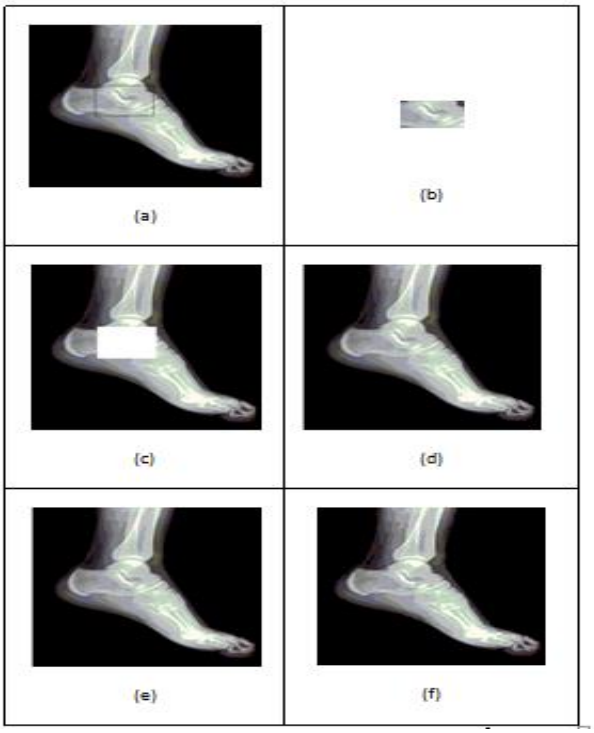


Fig. 8. Human Ankle Radiography. (a)Input Image b) Region Of Interest (c) Region Of Non-Interest (d) Watermarked Image (e) Steganographed Image (f) Lossless Compressed Image

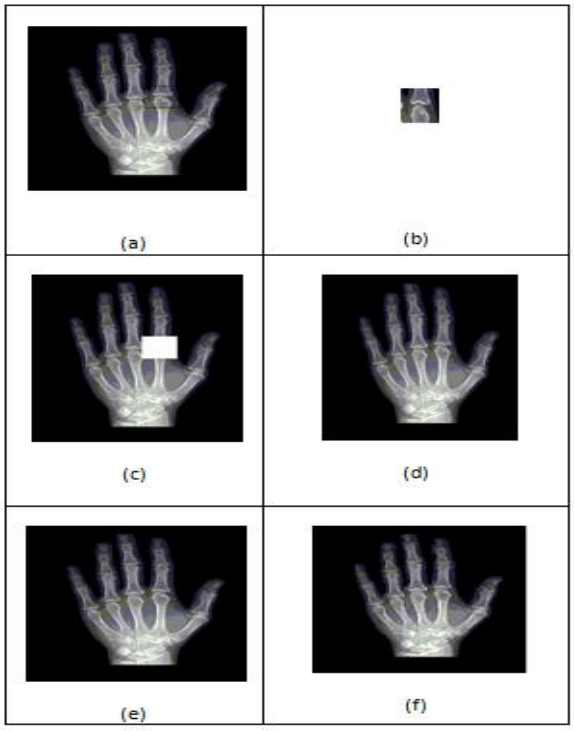


Fig. 9. Human Hand Radiography. (a)Input Image (b) Region Of Interest (c) Region Of Non-Interest (d) Watermarked Image (e) Steganographed Image (f) Lossless Compressed Image

Sl.no.	Images	Input Image (Kb)	Lossless Compressed Image (Kb)
1.	Scanned Human Brain	366 Kb	9.87 Kb
2.	Lungs	321 Kb	9.801 Kb
3.	Human Ankle	537 Kb	9.30 Kb
4.	Human Liver	508 Kb	19.002 Kb
5.	Hand	259 Kb	5.87 Kb

Table II: Comparison of size of input and compressed image

V. CONCLUSION & FUTURE WORKS

In this work, a three-level security technique, which not only provides the biomedical integrity, but also the lossless compression of the data files provided. The techniques used are Digital Water marking, namely Least Significant Bit Watermarking, Message Digest-5 hash digest algorithm, Steganography, and the DCT based Lossless Compression. The images were analyzed and compared based on the performance metrics such as MSE, PSNR. This proposed algorithm provides the patient authentication, information secrecy, reliability, secure transmission, can save storage space and also bandwidth during transmission through an open network.

For the future works, Digital Watermarking can be employed in the transform domain, which will be very much robust against attacks. Similarly, the Steganography can also be used in transform domain. The hash digest could be computed by the SHA-1, producing 128-bit hash digest. In the Lossless Compression part, the wavelet transform could be used.

ACKNOWLEDGEMENT

This work is technically supported by Institute of Human Resource Development (IHRD), Kerala, in particular Mr. Aneesh R. P., provided many useful discussions.

REFERENCES

[1] Katherine P. Andriole, "*Security of Electronic Medical Information and Patient Privacy: What You Need to Know",* Journal of the American College of Radiology/Vol. 11 No. 12PB December 2014

[2] S. Kolodner, Falmless Radiology, Collection Health Informatics. Springer Verlag, NewYork, USA, 1999.[3] John Craig and Victor Patterson, "*Introduction to the practice of Telemedicine*", Journal of Telemedicine and Telecare, Vol. 11, No. 1,2005.

[4] S.G. Petropoulou And M.P. Bekakos, "*Current Medical Digital Applications – Telesurgery*", Health Informatics Laboratory, Department of Nursing, National and Capodistrian University of Athens, Hellas.

[5] Ahmed Mahmood, Charlie Obimbo, Tarfa Hamed, and Robert Dony, "*Improving the Security of Medical Images*", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 9, 2013.

[6] Osamah M. Al- Qershi, Khoo Bee Ee, "*Authentication and DataHidingusing a Reversible ROI-based Watermarking Scheme for DICOM Images*'',Proceedings of World Academy of Science, Engineering and Technolgy, Vol.38, Feb. 2009 ISSN:2070-3740.

[7] Sonika C. Rathi & Vandana S. Inamdar, "*Medical Image Authentication through Watermarking Preserving ROI*", Health Informatics-An International Journal (HIIJ) Vol.1, No.1, August 2012.

[8] Anisha Joseph, Deepa S. S."*An Efficient Watermarking Based Integrity Control System for Medical Images*", IEEE International Conference on Control, Communication & Computing India (ICCC) 19-21, November 2015.

[9] Jagan Raj J., Prasath S., "*Validating Data Integrity in Steganographed Images using Embedded Checksum Technique*", International Journal of Computer Applications, 2015.

[10] Abhishek Patanwar, and Shikha Singh, "*A Comparative Study of Reversible Watermarking Techniques*", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, No.4, 2015.

[11] Frank Hartung, Martin Kutter, "*Multimedia Watermarking Techniques",* Proceedingsof the IEEE, Vol. 87, No.7,pp, July 1999, 1085-1103

[12] Puneet Sharma nd Rajni, "*Analysis of Image Watermarking Using Least Significant Bit Algorithm* ", International Journal of Information Sciences and Technique, Vol. 2, No. 4, 95-101.

[13] Patil V. A., S. S. Tamboli, "*Image Watermarking Using Least Significant Bit Algorithm*", International Journal of Trend in Research and Development , Vol. 3, ISSN: 2394-9333, May-June2016

[14] Champakamala B. S., Padmini K., Raadhika D. K., "*Least Significant Bit Algorithm for Image Steganography*", International Journal of Adavnced Computer Technology(IJACT), Vol. 3, No. 4, 1SSN: 2329-7900.

[15] Ankush R. Patil, V. K. Patil, "*A Review of Image Watermarking Methods*", International Journal of Engineering Sciences & Research, ISSN: 2277-9655.

[16] Jan C. A., "Basic Methods of Cryptography ", Faculty of Information Technology and System, Delft University of Technology.

[17]infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/MD5.pdf

[18]https://in.mathworks.com/help/images/discrete-cosine-transform.html