Cryptographic Transmission For Secured Medical Images Using DCT, DWT And SHA

P. Ramya Rani [1], K. Chaitanya [2]
[1]Master Degree, Digital image processing
[2]Assistant Professor, Dept of CSE
[1, 2] Acharya Nagarjuna University, Andhra Pradesh

Abstract- *Cryptographic transmission for secured medical images is proposed in the present study. Brain tumor is the leading cause of most deaths in the world. The present paper deals with categorization of Brain tumor, i.e. benign based on coefficients extracted from multi resolution analysis based on two different wavelet transforms like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).The discrete wavelet representations of each position are given by applying a DWT, discrete cosine transform is a block based technique and Secure Hash Algorithm (SHA) are used to embed a watermark on the recover image. By using the growing technologies like telecommunication and information technologies better communication can be achieved in telemedicine healthcare practice. This has given rise to protected telemedicine utilization that will provide confidentiality, authentication and integrity by the transmitted medical images. The performance of the telecommunication in the present study is calculated with respect to imperceptibility, robustness, and tamper localization of dissimilar medical images.*

Keywords- Confidentiality, Authentication, Integrity, DICOM standard DWT, DCT and SHA

I. INTRODUCTION

The information technology contributes to the medical service improvement that is provided to people.[1]Hussein introduces a cryptography which is a method for sending a message in a secure format that only the authorized person can decode and read. This is known as a “secret writing”. Appreciation to the detail accessibility of inexpensive movable gadgets, such as smart mobiles and tabs is at everyone search proposed by Piazza Leonardo [2].Al-Haj [3] introduces the up to date health protection system like Hospital Information System (HIS) and Picture Archiving and Communication System (PACS) providing the health sector with the digital medical images.

According to the working domain, the spatial domain watermarking bits are inserted in carrier image by modifying its pixel values. The second kind of watermarking methods were based on the transform domain. Spatial domain methods have some advantages like overcome cropping attacks, but their main drawback is their weaknesses against noise or ‘LOSSY’ compression attacks.

Despite extensive research undertaken in this area, there is still no method available to fulfill all the requirements of Medical Image Watermarking (MIW) introduced by Al-Haj [5]. Al-Haj [5] refers that spatial domain approaches cannot survive against noise or loss less compression attacks. Hussein [6] suggested that, the main priority in handling of medical images was to secure protection for the patient’s documents against any act of tampering by unauthorized persons. The fragile method allows the watermark to easily remove by the smallest modifications. After a long time, this paper focuses on supporting the health care system by implementing a secure, strong and privacy system for the intact giving and usage of the medical image. This paper investigated the watermarking cryptography approaches and applied them to telemedicine. This paper, focus on the complexity and security issues in the existing cryptography approaches. It provides watermarking solution with low computational difficulty, high robustness, and high inappreciable and low degeneration [7].

II. PRELIMINARIES

2.1 Digital Image Processing (DIP)

The field of DIP refers to processing digital image by means of digital computer. Digital image is composed of a finite number of elements, each of which has a particular location & value. The elements are called pixels. Pixel is the term used most widely to denote the elements of a digital image.

2.2 DICOM

Digital Imaging and Communications in Medicine (DICOM) established to be the standard format of medical image that may store, transmit, save, and use it. DICOM was developed by the corporation between the American College of Radiology (ACR) and National Electrical Constructor

Association (NEMA) to produce standard for data transfer in 1983. Fig.1 shows the DICOM security standard does not pretend the confidentiality, authentication and integrity of the medical image data. This way it can provide a standard guarantee of confidentiality and integrity of the data.

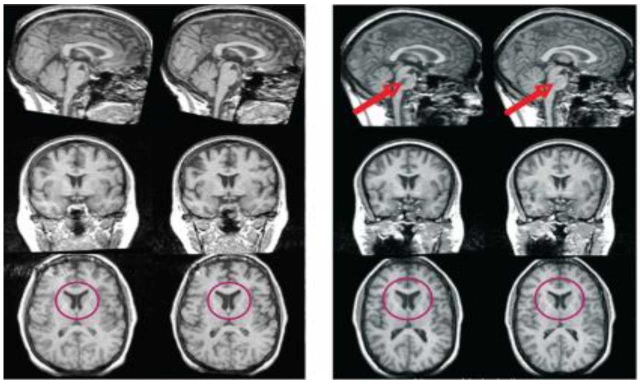


Fig.1 Benchmark medical images with ROIs shown in polygons. a MRI image, b ultrasound image, and c X-ray image

2.3 DWT

DWT is a mathematical model to decompose a signal. The present study utilizes one level DWT for both the watermark and original images. Fig.2 shows the various levels of signal decomposition. It is valuable for handling of a non-final signals. In fact, this decompose can have several levels called n-levels, multi-resolution field. Wiley [8] refers; the result of this dissolve gives four sub-bands: Low-Low (LL), Low-High (LH), High-Low (HL) and High-High (HH). The LL sub-band contains the estimated original image while the other sub-bands contain the missing details.

.

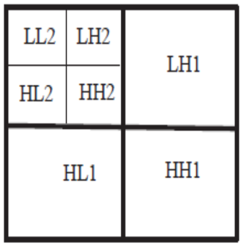


Fig.2 frequency decomposition of DWT

2.4 DCT

DCT transforms a signal from the spatial domain to frequency domain. It provides a high strongest against the Joint Photographic Expert Group (JPEG) standard for image compression. The DCT-based method is a block-based technique. By using this transform, the image will be divided into three frequency bands: low (FL), middle (FM), and high (FH) [5]. By using this equation (1) and 2, it transforms the image into non-overlay m × m blocks. Generally, the block size is 8 × 8 items. DCT splits the image into three different frequency bands: low, middle and high frequency. This study uses middle frequency components to insert an image and it contains both information and details as the low frequency contains the major information about the image while the high frequency contains the image details. If the watermark is inserted in the low frequency, the watermark will be robust but visible. Meantime, if it is inserted in the high frequency, the watermark will be invisible but less strong. Patel P [9] recommended, that DCT fully transforms frame which means any modification will be noticeable through the whole image.

$$F(u,v)=\frac{2}{N}c(u)c(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)\cos[\frac{\pi}{N}\;u(x+\frac{1}{2})]\cos[\frac{\pi}{N}\;v(y+\frac{1}{2})] \quad \textbf{(1)}$$

$$f(x,y)=\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}c(u)c(v)F(u,v)\cos[\frac{\pi}{N}\;u(x+\frac{1}{2})]\cos[\frac{\pi}{N}v(y+\frac{1}{2})] \quad \textbf{(2)}$$

2.5 ROI and RONI

A computer aided tool, separates the given medical image into two non-overlapping zones: region of interest (ROI) and region of non-interest (RONI). The ROI zone contains the significant information that the physicians utilize for diagnosis. Since the RONI zone does not contribute to diagnosis, its integrity does not need to be preserved and thus it can be used for the insertion of robust watermarks.

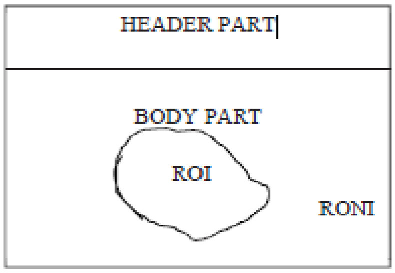


Fig.3 ROI and RONI

2.6SECURE HASH ALGORITHM (SHA)

A secure hash algorithm is actually a set of algorithms developed by the National Institutes of Standards and Technology (NIST) and other government and private parties. Within the family of secure hash algorithms, there are several instances of these tools that were set up to facilitate better digital security. The first one, SHA-0, was developed in 1993. Like its successor, SHA-1, SHA-0 features 16-bit hashing.

The next secure hash algorithm, SHA-2, involves a set of two functions with 256-bit and 512-bit technologies, respectively. All of these secure hash algorithms are part of new encryption standards to keep sensitive data safe and prevent different types of attacks by using this fig (4). It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password.

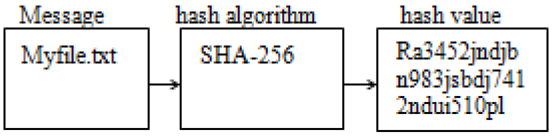


Fig.4 SHA algorithm

2.6 WATERMARKS GENERATION

The proposed watermarking algorithm consists of three procedures: watermark embedding, watermark extraction, and integrity. The first procedure embeds the authenticity and integrity watermarks into the RONI, while the second extracts the watermarks from the same. The three watermarks and their pre-assigned embedding locations are described below.

1. The patient information watermark is a 64 × 64 binary image created from several attributes of a sample patient's information as shown in Fig (5). For image authentication patient's information was embedded in the HHr sub-band.

2. The hospital logo watermark is a 64 × 64 binary image shown in Fig (6). To authenticate the source of origin of the image, it is embedded in the HLr sub-band.

3. ROI of an MRI brain image can be displayed shown in Fig (7). The watermark is used to verify the strict integrity of ROI of image and is embedded in the LHr sub-band.

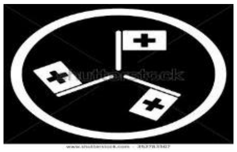
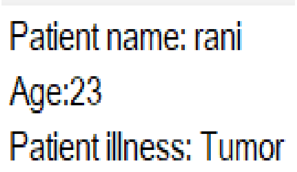


Fig.5 Hospital logo watermark



Patient name: rani
Age:23
Patient illness: Tumor

Fig.6 Patient information watermark

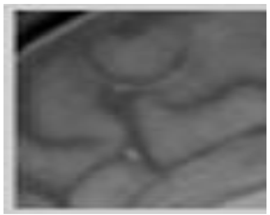


Fig.7 ROI hash watermark

III. PROPOSED METHOD

3.1 Watermark Embedding TECHNIQUE

The embedding procedure inserts the bit-patterns of the three watermarks in the RONI of each sub-band according to the following assignment: the patient information watermark in the HHr sub-band, the hospital logo watermark in the HLr sub-band and the hash watermark in the LHr sub-band. The operational steps of the procedure are depicted in Fig.8 and described below in detail.

Step1: Read the brain image as the cover image divide the brain image into ROI and RONI regions as specified in section 2.1.

Step2: Apply 1-level DWT to the brain image and it decomposes the brain image into four sub-bands namely LLr, LHr, HLr and HHr.

Step3: Divide LLr, LHr, HLr, HHr sub-bands into 8×8 non over lapping blocks.

Step4: Apply the DCT technique, to each 8×8 RONI block of LHr, HLr and HHr.

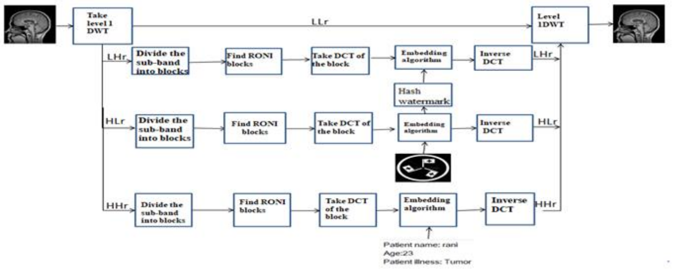


Fig.8watermarking embedding

Step5: Calculate hash value for the ROI region of the brain image and embedded this hash value as the first watermark into the mid frequency coefficients of each 8×8 DCT blocks of LHr sub-band.

Step6: Take the 64×64 grey level hospital logo as the second watermark and convert into binary form and embedded into the mid frequency coefficients of 8×8 DCT blocks of HLr sub-band.

Step7: Take the 64×64 grey level patient information as the third watermark and convert into binary form and embedded into the mid frequency coefficients of 8×8 DCT blocks of HHr sub band.

Step8: Apply inverse DWT to original LLr modified LHr, HLr, HHr sub-bands to get the watermarked image.
3.2 Watermark extraction procedure

The proposed algorithm is blind in the sense that it does not require the cover image in the extraction process and it only requires the watermarked image. The following step describes the watermark extraction process and also shown in Fig.9:

Step1: Read the watermarked image and divided into ROI and RONI regions.

Step2: Apply 1-level DWT to the watermarked image and it decomposes the watermarked image into four sub-bands namely LLr, LHr, HLr and HHr.

Step3: Divide LHr, HLr and HHr sub-bands into 8×8 non-overlapping blocks.

Step4: Apply the DCT to each 8×8 RONI block of LHr, HLr and HHr.

Step5: Extract the hospital logo details into the mid frequency coefficients of each 8×8 DCT blocks of LHr sub-band.

Step6: Extract the patient information into the mid frequency coefficients of 8×8 DCT blocks of HHr sub-band.

Step7: Extract the hash value into the mid frequency coefficients of 8×8 DCT blocks of HHr sub-band.

Step8: The physicians at the receiving side authenticate the image in terms of control and source of origin. The image is authenticate and verifying the extracted patient's information watermark. The image source of origin is authenticate and verifying the extracted hospital logo watermark. Similarly, authentication and confidentiality is verified by extracted hash watermark.

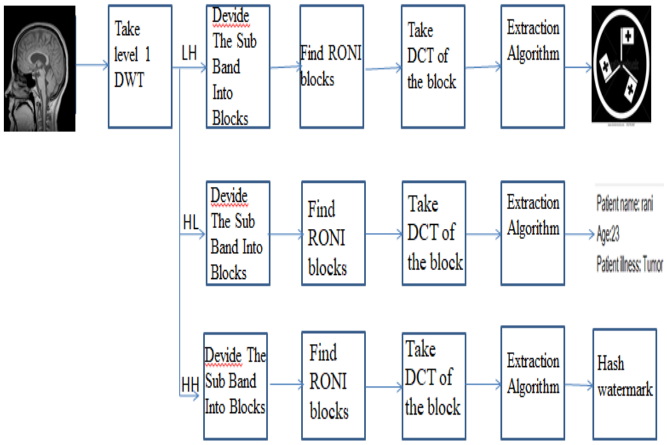


Fig.9 Watermark extraction procedure

IV. PERFORMANCE ANALYSIS

A large set of 8-bit grey ratio medical images have been used to evaluate the performance of the proposed algorithm. From the following equation (3), the higher Peak Signal Noise Ratio (PSNR) gives a better quality of the compressed or reconstructed image. The mean square error (MSE) and the PSNR are the two error metrics used to compare image compression quality. In the previous equation, R is the maximum fluctuation in the input image data type.

$$MSE= \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|Aij-Bij|)}{x*y} \quad (3)$$

Aij -is original image,Bijwater marked image
$x*y$-are the rows and columns of the image

For better assessment, PSNR was used as an imperceptibility objective metric and obtained the following PSNR values: 35.1797.

Equation (4) represents a common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password.

$$PSNR\ (dB) = 10*\log\left(\frac{255^2}{MSE}\right) \quad (4)$$

Compute the hash value of ROI, the received watermarked image I extracted from the RONI. Fig.10 shows the strict integrity verification of ROI image.

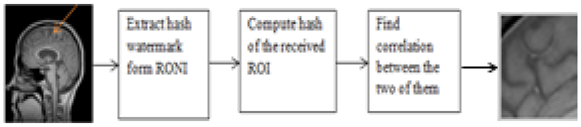

Extract hash watermark form RONI
Compute hash of the received ROI
Find correlation between the two of them

Fig.10 Strict integrity verification of ROI image

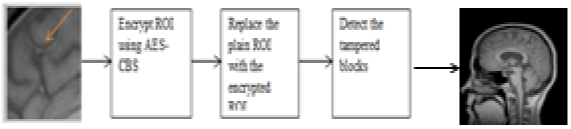

Encrypt ROI using AES-CBS
Replace the plain ROI with the encrypted ROI
Detect the tampered blocks

Fig.11 Localized tamper detection procedure

It was obvious from the robustness results shown in fig.11, that robustness has been achieved to that extent that authentication and verification can be done with confidence using the extracted watermarks.

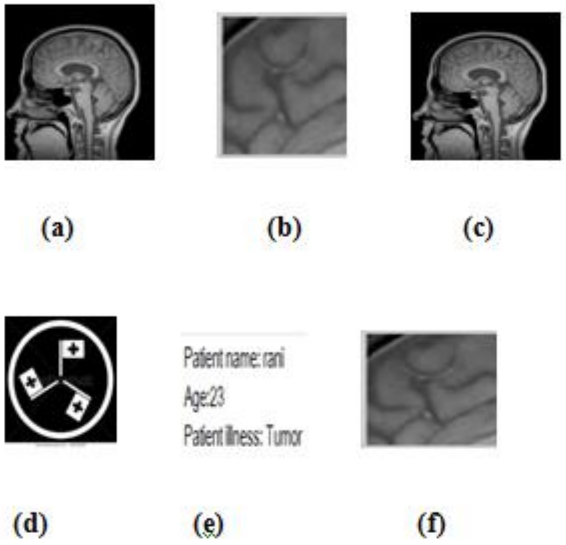


Fig.12 a. original image b. hash watermarked image c. recover image d. log image watermark e. patient information watermark f. hash image watermark.

4.1 JPEG compression

JPEG compression is widely adopted in image transmission and storage. Tampering the encrypted ROI using additive white noise, additive salt and pepper noise and “LOSSY” JPEG compression caused the decryption process to produce random output instead of the original ROI.

As shown in Table (1), the patient information and hospital logo watermarks can be faithfully used to authenticate the source of origin of the image, and the hash watermark to verify the strict integrity of the ROI of the image. Similar results have been achieved for the X-ray and ultrasound images.

Table.1: Robustness of the watermarked MRI image against JPEG compression

Watermarked image	Watermarks	Correlation					
		JPEG compression quality					
		100	96	92	88	84	80
MRI	Patient information	0.979	0.977	0.974	0.969	0.966	0.95
	Hospital logo	0.96	0.954	0.931	0.919	0.935	0.891
	Hash	1.00	1.00	1.00	1.00	1.00	1.00

4.2 Comparison with Other Algorithms

4.2.1 Data Payload

The embedding capacity provided by the algorithm depends on size of the image, the relative size of ROI and RONI segments, block size, and number of DWT decomposition levels. Equation(3) represents the embedding capacity, larger images, smaller block size, and higher DWT levels will provide higher embedding capacity. It is instructive to note here that the capacity equation has been derived in such a way that capacity calculation is confined to three sub-bands (LH, HL, HH), since sub-band (LL) has been excluded from watermark embedding.

$$C = 3 * \text{number of blocks} * 4^{\text{DWT LEVEL-1}} \quad (5)$$

Where,

$$\text{Number of Blocks} = \frac{\text{total image size}}{\text{number of blocks}} \quad (6)$$

Table.2: Comparison between the available and required payload capacities

Watermark name	Watermark size (bits)	Embedding location (DWT band)	Available capacity (MRI)	Available capacity (US)	Available capacity (X-ray)
Patient’s information	19,584	RONI (LH band)	59,915 bits	29,528 bits	20,374 bits
Hospital’s logo	512	RONI (HH band)	59,915 bits	29,528 bits	20,374 bits
ROI hash	256	RONI (HL band)	59,915 bits	29,528 bits	20,374 bits

Both crypto-based DICOM standard and proposed algorithm maintains confidentiality header, authenticity pixels and integrity pixel. As compared to DICOM standard, proposed algorithm maintains confidentiality pixel, authenticity header and integrity header authenticity. Integrity was achieved as described in image processing section, and confidentiality is achieved by virtue of encrypting the ROI before transmission.

Table.3: Comparison between the proposed algorithm and the DICOM standard

Algorithm	Confidentiality (header)	Confidentiality (pixels)	Authenticity (header)	Authenticity (pixels)	Integrity (header)	Integrity (pixels)
DICOM Standard	√			√		√
Proposed Algorithm	√	√	√	√	√	√

IV. METHODOLOGY

Green Internet of Things focuses on the energy efficiency in the IoT principles. Green IoT is defined as the energy efficient way in IoT either to reduce the greenhouse effect caused by existing applications .IoT will help in eliminating or reducing the greenhouse effect. Few ways to eliminate green house effect or carbon emission is shown .

A. Green approaches techniques

There are many green approaches used , this techniques are used according to its application . There are theoretical as well as practical approaches used. This will not reduce toxic gases emission to large extent but will help to reduce in some amount. some of these techniques are mentioned below, they are:

- Green approach in ICT.

Reduces use of hardware devices or dematerialization , to improve manufacturing process, Virtualization , e-commerce.

- Green approach using RFID.

Organic , it has free energy management module , saves upto 60% of power , Energy efficient algorithm.

- Green approach to cloud computing.

Consolidation , Migration.

- Green approach using WSN.

Devices are bio-degradable, mainly focuses on energy efficiency.

B. Green technique using scrubber.

Figure 4 shows green technique using scrubber, CO2 will flow through the first pipe and there gas sensor is placed to know the quantity of co2 if it is over the limit gas will be directed towards an scrubber using actuator(motor) here active charcoal is used as scrubber . active charcoal absorbs the toxic gases like co2 from gas and gives pure gas as output. If quantity of co2 is below limit then no need to pass it through active charcoal it is directly given to output without any purification.

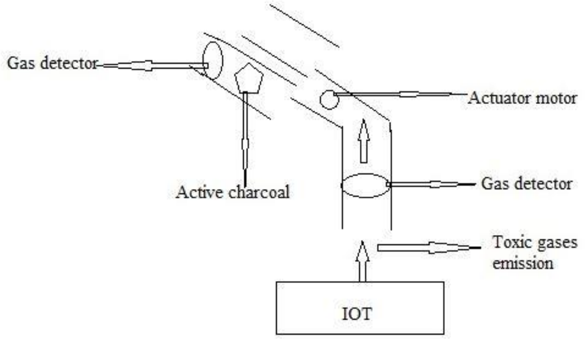


Fig 4: Green technique using charcoal

Figure 5 shows Flow chart for Green technique using scrubber. Correct live value of carbon emission is given by air quality sensor .Node MCU processes and further directs air to be flown in which pipe depending upon logic set. Active charcoal filters are placed in order to reduce carbon from air. If carbon level is below the predetermined level or desired level then air is directly given to the outlet.

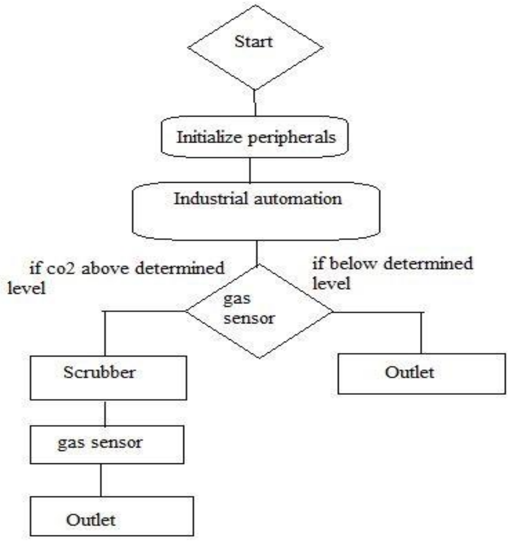


Fig 5: Flow chart for Green technique using scrubber.

V. FEATUREEXTRACTION

Image feature extraction is extremely required in image processing technique to detect and isolate desired portions of an image. The term feature can be stated as an interesting part of an image. Consequent to image preprocessing, the features are extracted either at the tissue.

VI. CONCLUSION

In this paper, analyzing was done using DWT and DCT by regarding combined. The experimental work done by subset of tumor disease image acquire from DWT and DCT framework. Healthcare management can now consider increased planning, decreased costs, better patient care and quality of services and safety when they are planning to implement new information and communication technology (ICT) based applications.

VII. ACKNOWLEDGEMENT

I am greatly thankful and deeply indebted to my guide Mrs. K.CHAITANYA, Assistant Professor, Acharya Nagarjuna University, for giving me an opportunity to work under her guidance.

REFERENCES

[1] Al-Haj A, Amer A: Secured telemedicine using region-based watermarking with tamper localization. J Digit Imaging 8(3):737–750, 2014

[2] Al-Haj A, Abandah G, Hussein N: Crypto-based algorithms for secured medical image transmission. IET InSecure 9(6):365–373, 2015

[3] The Health Insurance Portability and Accountability Act (HIPAA), March 2009. [Online]. Available at: http://www.hhs.gov/ocr/privacy/index.html

[4] Al-Haj A: Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. J Digit Imaging 28(2): 179–187, 2014

[5] Mousavi S, Naghsh A, Abu-Bakar S: Watermarking techniques used in medical images: a survey. J Digit Imaging 27(6):714–729, 2014

[6] Saranummi N: In the spotlight: health information systems. IEEE Rev Biomed Eng. 6:21–23, 2013

[7] Al-Haj A, Hussein N, Abandah G: Combining cryptography and digital watermarking for secured transmission of Medical images. In: Proc. of the IEEE International Conference on Information Management. UK, 2016

[8] Image Tampering Localization via Estimating the Non-Aligned Double JPEG compression LanyingWua , Xiangwei Kong*a , Bo Wanga , ShizeShanga a School of Information and Communication Engineering, Dalian University of Technology, Dalian, China, 116024

[9] Patel P, Patel Y: Secure and authentic DCT image steganography through DWT-SVD Based Digital Watermarking with RSA Encryption. In: Proc. of the IEEE fifth International Conference on Communication Systems and Network Technologies, 2015, pp. 736–739

[10] Thodi D, Rodríguez J: Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16:721–30, 2007

[11] B. Schneier, Applied Cryptography, 2nd ed. New York: Wiley, 1996

[12] Multi-Clue Image Tampering Localization Lorenzo Gaborini∗ , Paolo Bestagini† , Simone Milani† , Marco Tagliasacchi† , Stefano Tubaro† ∗Dipartimento di Matematica “Francesco Brioschi” †Dipartimento di Elettronica, Informazione e BioingegneriaPolitecnico di Milano, Piazza Leonardo da Vinci 32, 20133, Milano, Italy