Medical Image Security Analysis and Enhancement for Telemedicine Applications

Vijay Krishna Pallaw, Graphic Era Hill University, Dehradun, India
Email: vijaykpallaw@gmail.com
Corresponding Author: Kamred Udham Singh, Graphic Era Hill University, Dehradun, India
Email: kamredudhamsingh@gmail.com

Abstract:

With the remarkable development of digital medical images and high-speed transmission networks and computer technologies in current year, authenticity and security of the medical images have been big issues for E-health application. In order to this many different remarkable watermarking strategies and concepts have been introduced by researchers. In this paper we concentrate on the possibilities for assurance of medical images using the principle of digital watermarking. There are many methods it looks from their basic perspective. One of them perspective is security to ensure authenticity and copyrights. Other we discuss watermarking methods classification which are based on different parameters such as: insertion domain (spatial and frequency domains)..

Keywords: Watermarking, security, DICOM, medical images, transform domain.

1. Introduction

Due to exceptional improvement of the computer technologies and transmission networks, the present-day medical systems are based on sharing of the medical data across the different parts of the world among distinctive doctors or health professionals for different purposes via unsecured transmission networks like Internet. So, it is necessary to provide security to assure medical information during the transmission, because of any modification of the medical information will affect in the specialist diagnostics [27]. It is very important to secure physical access & electronic access to whole part of system, starting with capturing modalities, data storage, communication media, server, and ending with doctor's diagnostic workstations. This is possible to be made with standard & proven methods, which are used in communications, it is important to secure data of medical images itself. Currently, data hiding techniques provide remarkable grandness for data assurance of medical images [1].

The digital watermarking is data embedded into the host object like audio, video, image, or other computerized information, without any changing its visual quality. With help of watermarking strategies medical images are secured beside the electronic patient information (EPI) [2] [3]. The watermarking of medical images has been broadly identified as an important strategy for improving information security, authenticity, picture devotion and content confirmation in present E-health framework where digital medical images are kept, recovered and transmitted over communication network. Medical image watermarking saves the quality of images which are essential for medical diagnosis and treatment [29]. In order to study of medical images, it is necessary to build advanced data storing & archiving called picture archiving & communication system (PACS). PACS may be a medical imaging innovation which give temperate capacity & helpful get to pictures from numerous modalities which is described in [1] [2]. Data of medical images are generated by several modalities like CT scan, MRI, X-rays, and ultrasound. As standard for transmission, storing medical images & data used international standard protocol called DICOM. DICOM (Digital Imaging & Communications in Medicine) may be standard protocol for administration & forwarding of medical images & related information over public network and is utilized in numerous healthcare offices. DICOM images contain information and metadata in header such as patient name, patient ID, Date of Birth, and test details such as doctor's name, date & time of image capture and device type on image which was taken.

2. Digital Watermarking

Digital watermarking is used for authentication, copyright protection, medical images, and other applications. The concepts of watermarking are related with two areas: Steganography, & Cryptography. Cryptography could be a technique to send encrypted information over public network that as it were authorized individual can be decoded [4] [5]. When the message is decoded it is not ensured any longer and typically the basic difference between Cryptography. Steganography is the technique of hiding secret data inside an ordinary, non-secret object (Image, audio, video) in order to avoid detection, whereas the aim of watermarking is to insert a data in such a way that it can't be removed [6]. The technique describes the embedding of digital watermark (such as logo, hallmark) in a cover for identifying any ownership dispute that can arise.

Table-1: Comparison among cryptography, steganography and digital watermarking

	Cryptography	**Steganography**	**Digital Watermarking**
Definition	Cryptography is a technique to send encrypted information over public network that only authorized person can be decoded.	Steganography is a technique of hiding secret data within an ordinary non-secret object (image, audio, video)	The digital watermarking is data embedded into the host object such as image, audio, video or other digital data, without any changing its visual quality.
Usage	Encoded data is to be transfer for integrity purpose.	Insert a secret message inside the cover for a communication between two parties.	Digital watermarking is used to authenticate the ownership of the entity.
Provide security related application	Confidentiality, Electronic money, secures network communication.	Copyright protection, access control, secret communication	Copyright protection, digital forensic, smart healthcare, remote education

According to human perception, watermark is two types: Visible watermark & Invisible watermark. Visible watermark is one which likes text or logos that clearly distinguish the ownership of picture or video. However, visible watermark offers poor imperceptibility & allow recognizing through human sensory system. Invisible watermarks which cannot be seen by sensorial organs of human, but it is possible to be detected by algorithm, if method of insertion is known. Now, there are three sub categories of invisible watermarks: fragile, semi-fragile and robust. The fragile watermark may be deformed by little changes as it were. It is more applicable for integrity and ownership authenticity. The semi fragile method makes the hidden information secure against various attacks. Robust watermarking methods are generally protecting against various benchmark attacks & suitable for copyright protection.

According to detection-based watermarking the embedded information may be identified with the following methods: Blind, semi – blind and non-blind. The blind strategy does not need of the original signal to identify a watermark. The semi – blind strategy detects a watermark by using some information. The non-blind strategy needs the original signal to identify a watermark. Among all these three watermarking strategies, a non-blind watermarking strategy is the most robust against to attacks [6].

Table-2: Comparison among blind, semi-blind & non-blind methods.

	Blind	**Semi-blind**	**Non-blind**
Definition	There is no required original information to draw out the watermark	Semi-blind required some information to draw out the watermark.	Non-blind required both original information and secrete key to draw out the watermark.
Application	Healthcare, copyright security, remote education, E-voting, authentication	Image authentication, copyright, wireless & ad hoc network	Copyright security convert communication.

Now, the domain-based watermarking techniques are further classified into two sub categories called spatial domain & transform domain. In spatial watermarking strategy, the pixel, or sequence of bits (0 & 1) of the cover image are modified specifically in arrange to insert the watermark [13]. LSB, spread spectrum, and correlation techniques are existed in this domain. The transform domain is also called frequency domain is partitioned into sub categories like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) & Fast Fourier Transform (FFT).

Table-3: A comparison table of spatial domain & transform domain [14].

	Spatial Domain	**Transform Domain**
Complexity	Low	High
Capacity	High	Low
Robustness	Low	High
Processing Time	Less	More
Imperceptibility	Low	High

2.1 Medical image watermarking

Due to exceptional development of the computer innovations, the modern healthcare systems are based on sharing the digital medical data over transmission network such as Internet can be accessed from any region of the world by doctor’s or specialists to recognize disease & remote diagnosis. This has resulted in increased attacks such as deleting, copying, modification on digital data or unauthorized use of medical data. Any alteration of medical image context will influence in the specialist diagnostics. Therefore, it is essential to provide the assurance during the transmission. So that, the medical images ought to be kept unbroken in any circumstance & some time recently any operation they must be checked for:

- **Integrity verification** the main goal of integrity verification is to determine whether any modifications such as rotation, scaling, translation or compression has been done on the medical image or not. Semi-fragile or fragile watermarking techniques ought to be connected, which isn’t robust against content alteration.
- **Authentication** is a valuable implementation in medical area for guaranteeing a realness of patient data at the time of the transmission of digital medical image.

- **Data hiding** Data hiding is utilized to stow away an expansive sum of information subtly into the medical image such as electronic patient report (EPR).

Basically, there are two sections of a medical image called Region of interest (ROI) & Region of non-interest (RONI). Patient information is inserted into the ROI region with help of Difference Expansion watermarking method. Tamper detection information and pixels area outline are encoded into the RONI portion with help of DWT based robust strategy. The shortcoming of this method is required for manual recognizable proof of ROI, to extend the payload capacity. The ROI section compromises the instructive area of the picture which is used for diagnosis and need to protect beyond any distortion. Utilizing the ROI portion for stowing away the watermark may distort the pixel intensity, which may lead to error and thus misdiagnosis. Any little modification in medical image can cause a big issue for right treatment. Utilizing RONI as it were watermarking, watermarks are put away as it were in parts that don't contain data imperative to pathologist. Determination of RONI may be manual or automatic. The dependability of automatic observation of imperative portion depends upon selected strategy. In hone, distinctive strategies of automatic RONI portion are generally utilized [30] [31] [32]. There's significant similitude to already known watermarking strategies applied to the RONI portion, but from another point of view, there's need of assurance within a portion of the restorative picture which is outstanding.

3. Domains of watermarking insertion

Many watermarking techniques for medical images have been described by using spatial domain & transform domain approaches. This section describes both transform domain & spatial domain based on watermarking insertion approach.

3.1 Spatial domain-based watermarking approach:

In this approach, the binary bit stream (0,1) or pixels of the cover image is modified directly to insert the digital watermark. The subcategories of spatial domain are spread spectrum, LSB and correlation-based technique [7]. In least significant bit, the digital watermark is hidden by exchanging the least significant bit of the binary representation (0 & 1) of the cover image pixels [8]. It is high embedding capacity and very simple technique. The spread spectrum technique helps in distribution of the information in frequency bins with very less energy and so, it is not predictable [9]. Now, brief description of spatial watermarking technique for medical field:

Author [10] introduced watermarking approach to get better transfer and more robustness and storage of the medical images' interleaves with data of patient. The signal graph & text data are considered as a watermark. Author [11] proposed a scheme for ultrasound images based on LZW for minimising watermark capacity without any loss of data and insert the watermark in ROI region.

Table-4: Spatial domain techniques

Ref No.	Techniques used	Important Features	Size of Cover Image	Size of Water mark Image	Limitations /Suggestions	Imag e Used
[12]	LSB (Least significant Bit) and encryption algorithm	Improve the reliability and robustness by using BCC on encrypted watermark	128 x 128		Noise effect may be reduced by using ECCs.	MRI, ECG, X-Ray
[13]	Least significant Bit and cryptography	Reduce noise during transmission	128 x 128		Convolutional Codes may be used.	ECG, MRI

		with help of ECC.				
[14]	LSB (Least significant Bit), magic rectangle and bi linear transformation.	Reversibility is achieved through interpolation.	512 x 512	128 x 128	resizes the cover image to which is required more memory to store.	
[15]	LSB (Least significant Bit) and SVD	Self-recovery bits and authentication. For this, Arnold transform is used neighbour blocks.	512 x 512		technique robust against operations image scaling, resize, rotation etc.	
[16]	LSB (Least significant Bit) and arithmetic compression	Security and payload capacity may be increased using SHA-256 on ROI.	768 x 562 And 330 x 330	10,000 characters	Runtime complexity more.	CT scan, MRI.
[17]	LSB (Least significant Bit)	SHA-1 is used on signature and merged with watermark and encoded with help of turbo code technique.		1700 bits.	For Gaussian noise, the watermark cannot be taken out properly.	IRM and Echo graphic images

3.2 Transform Domain-Based Watermarking.

In the transform domain, inserting of watermark provides high robustness as compare to spatial domain. As compare with spatial domain, transform domain is stronger against attack. The transform domain watermarking is classified into following categories. Some of these are:

- DCT (Discrete cosine transform)
- DWT (Discrete wavelet transform)
- DFT based watermarking

Table 5: DCT based watermarking techniques

Ref No.	Techniques used	Important Features	Size of Cover Image	Size of Watermark Image	Limitations /Suggestions	Image Used
[18]	RSA with 128 bits key, stream cipher.	Watermark is compressed with help of RSA algorithm with secret key.			Other Encryption algorithms may be applied to improve the performance.	X-Ray of chest.

[19]	SVD and DWT	For superior security, watermark is pre-prepared with help of DCT and SVD.	512× 512	256×256	After attacks Watermark gets damaged, AI concepts may be used.	Retina, Fingerprint, Teeth, Ultrasound,
[20]	SVD, DWT, BPNN, BCH coding and encryption	Use encryption to increase robustness. Minimize distortion Using BPNN	512× 512	128×128 And 100 characters	Runtime complexity is more.	Kidney, Lena
[21]	SVD, DWT, BPNN	Insert Scrambled watermark by utilizing Arnold transform. To evacuate noise impact applied BPNN.	512×512	256×256 And 190 characters	Runtime complexity is more. Performance may be increased.	CT-scan, Brain, Mammography, Ultrasound, MRI.l
[22]	MD5, LT, BCH codes	Enhanced secrecy and reduced channel noise mutilation using MD5 & BCH codes.	512×512	64×64 And 80 characters	Performance may be enhanced for other multimedia applications	Patient, Earth, magazine, Peppers.

Table6: DWT watermarking techniques

Ref No.	**Techniques used**	**Important Features**	**Size of Cover Image**	**Size of Water mark Image**	**Limitations /Suggestions**	**Image Used**
[23]	Arnold transform, BPNN	High robustness and authentication	256 × 256	25×25	Runtime complexity is very high.	Lena
[24]	BCH codes, HVS	To increase robustness	512 × 512	128x364, & a456 bits	Strategy may be integrated with JPEG2000 compression;	CT, MRI
[25]	Spread spectrum, encryption algorithm	Insert encrypted watermark	512 × 512	15 fixed characters & EPR.	Security and correlation may be increased by utilizing other valuable groupings.	CT Scan, MRI, Ultrasound

[26]	Spread spectrum, BCH coding.	Using PN sequences, Insert watermark with help of spread spectrum approach.	512 × 512	8 characters	Security and correlation may be increased by utilizing other valuable groupings.	CT Scan, MRI, Ultrasound
[28]	ROI, HS compression, EZW	Watermark shrinks with help of EZW, embedded around Region of interest.		64×64	We can be used other progressive coding algorithm for compression of watermark.	MRI, Ultrasound

Table 7: Comparison table of LSB, DCT, DWT and DFT [34]

DFT based watermarking

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks such as translation, cropping, rotation, etc. It is decomposed an image into two forms: sine and cosine. In DFT, there are two ways to embed the watermark: direct embedding and the template-based embedding. In the direct embedding approach, we are modifying DFT magnitude and phase coefficients and then the watermark are embedded. The template based embedding approach introduces the concept of templates. In DFT domain, during embedding process, we embedded the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched, and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark [33].

Techniques	Merits	Demerits
Least Significant Bit (LSB)	1. It is easy to understand 2. It is simple to actualize. 3. Its perceptual transparency is high.	• It is less robust. • It is delicate to noise. • It is delicate to cropping, translating and scaling.
Discrete Cosine Transform (DCT)	1. The image can be transformed by DCT into three sub categories: Low, Middle & High frequency coefficients. 2. DCT is more useful for watermarking technique, because of excellent energy compaction property. 3. Basically, a very good selection for embedding of watermarking is middle frequency coefficients of DCT [3], because, the middle frequency coefficients, the detectable quality of picture has not get affected and in case there is attack on watermarked data, the watermark isn't detachable.	• Some greater frequency components show suppress throughout the quantization process.
Discrete Wavelet Transform (DWT)	1. DWT slits a picture into four different frequencies level called HH, LL, LH, and HL.Where, LL holds low frequency & HH holds high frequency information. HL & LH sub-bands are intermediate frequency information. 2. DWT provides greater compression proportion.	• Its complexity is high. • Its compressing time is more.

	3. DWT based watermarking is more useful for medical images & other applications.	
Discrete Fourier Transform (DFT)	1. Since DFT is scaling, rotation & translation invariant. Therefore, DFT is utilized to recoup geometric deformations.	• Its usage is complex. • Its complexity is high.

4. The performance of watermarking image

Watermark medical image perceptibility is calculated by utilizing a number of important quality metrics [36] such as PSNR, MSE, NC & SSIM.

Peak -Signal to Noise Ratio (PSNR)

It is the most commonly used to evaluate the ratio of noise between actual image & watermarked image. With greater value of PSNR is very less dissimilarity between actual image & watermarked image. The perfect PSNR value always great than 30 db.

$$\text{PSNR} = 10 \log_{10} \frac{(MAX)^2}{MSE}$$

Here, **MAX** means a maximum pixel value of actual image. (**MAX**=255)

The Mean Square Error (MSE):

$$\text{MSE} = \frac{1}{M\,X\,N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [\,I(i,j) - I_w(i,j)]^2$$

Here,

I (i, j): represents an actual image

I_w (i, j): represents watermarked image and M & N represent dimensions of image.

Normalized Correlation (NC)

Normalized correlation is measured the likeness between actual image and extricated watermark. NC value exists between 0 to 1, an ideal NC value = 1, but acceptable value more than 0.7

$$\text{NC}= \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I(i,j) - I_w(i,j))}{\sum_{j=0}^{M-1} \sum_{j=0}^{N-1} [I(i,j)]2}$$

Where, I (i, j): represents actual image

I_w (i, j): represents watermarked image and M & N represent dimensions of image.

Structural Similarity Matric Index (SSIM)

It is utilized to evaluate the likeness between the actual image and watermark image. SSIM value lies between -1 to +1, if SSIM=1, then, both actual image and watermark image are exactly similar.

$$\text{SSIM}\ (x, y) = \frac{(\ 2\mu_x\mu_y\ +\ c_1)\ (2\sigma_{xy}+c_2)}{(\mu_x^2\ +\ \mu_y^2\ +\ c_1)\ (\sigma_x^2+\ \sigma_y^2+c_2)}$$

Where $\mu_{x\ :}$ the average of actual image and μ_y: the average of watermarked image.

$\sigma^2{}_x$: the variance of original cover and $\sigma^2{}_y$: the variance of watermarked image with covariance σ_{xy}. Where, $c_1$and c_2 are free parameters.

Table 4 shows the performances comparison of different watermarking scheme based on performance majors' parameters like PSNR, NC and SSIM. Figure1 and figure2 depict the that the highest PSNR achieved in scheme [9] and better SSIM achieved in [19] and [13] and the scheme [20] [16] [9] [13] achieved the good NC.

Table8: PSNR, NC and SSIM comparison of different watermarking schemes

	PSNR	**NC**	**SSIM**
Ref. [17]	44.51		
Ref. [24]	46.66		
Ref. [20]	34.88	.9944	
Ref. [19]	33.3870		0.9920
Ref. [16]	41.3784	1	0.9879
Ref. [9]	74.6099	1	0.7457
Ref. [13]	67.5717	1	1
Ref. [12]	60.783		

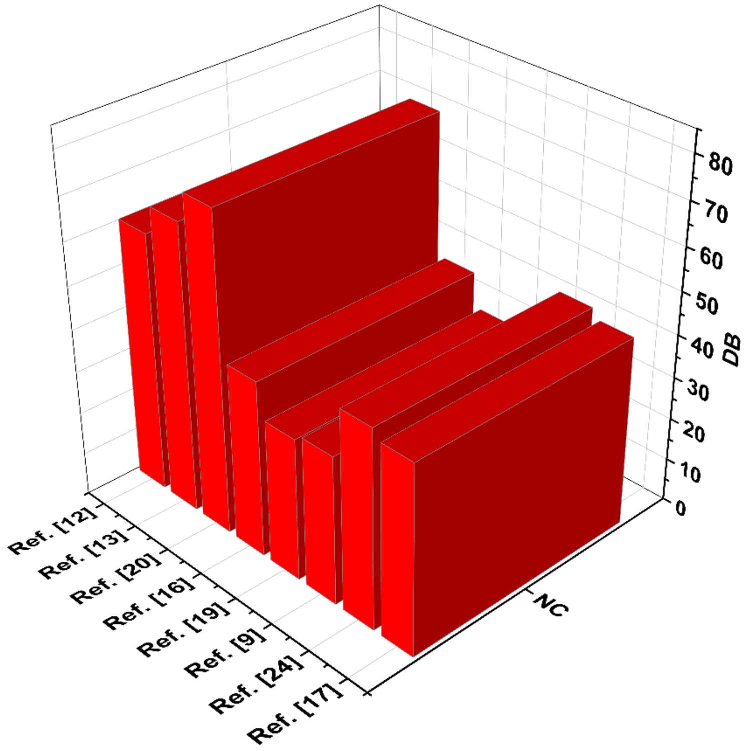

Figure1: PSNR comparison of different watermarking schemes

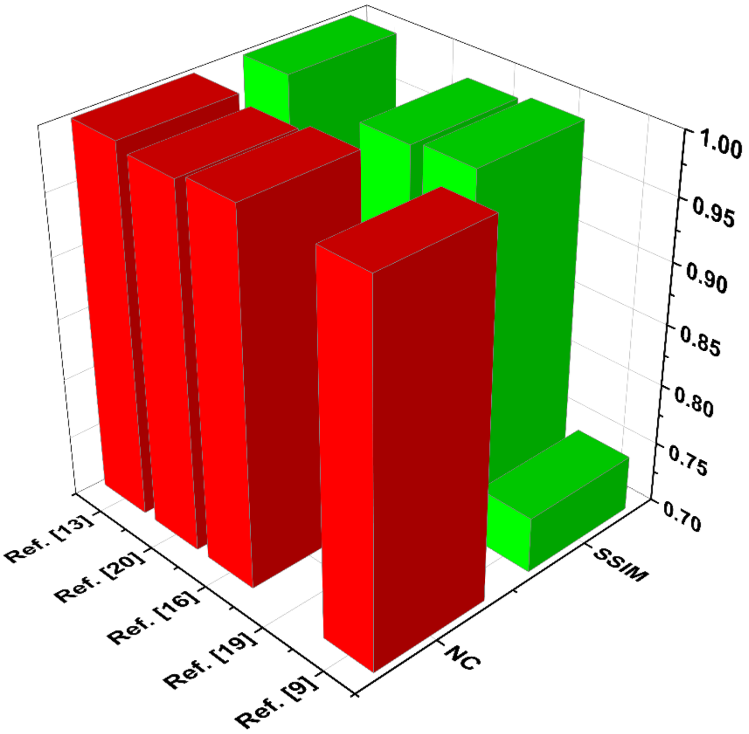

Figure2: NC and SSIM comparison of different watermarking schemes

5. Conclusion

The fast growth of modern e-health care system and requires to distribution of the digital medical information over unsecure communication network among hospitals & doctors. All the challenges make an assurance of information of patient on priority of need of e-health framework. Due to great potential of medical image watermarking technique, it provides a better solution for different issues of e-health framework. This paper is presenting different types of watermarking techniques, type of attacks and problems with medical image watermarking. At last, we summarized the suitable watermarking techniques is necessary for secure communication of medical information over communication network.

6. References

[1] Singh AK, Kumar B, Singh G, Mohan A (2017) Medical Image Watermarking: Techniques and Applications, book series on multimedia systems and applications, Springer, USA

[2] M. Javornik, O. Dostal, K. Slavicek, Reginal Medical Imaging System, World Academy of Science, engineering & Technology, Thailand 2011, vol. 7, no. 79, ISSN 2010-376X, pp. 389-393.

[3] K. Slavicek, O. Dostal, M. javornik,Technology background of international collaboration on medicine multimedia knowledge base establishment, proceedings of the 2nd WSEAS International conference on Computer Engineering & Applications (CEA '08'). Acapulco, Mexico, 2008: published by WSEAS press, 2008, Acapulco, mexico. ISBN 978-960-6766-33-6, pp. 137-1442.

[4] Chawla, G., Saini, R., & Yadav, R. (2012). Classification of watermarking based upon various parameters. *International Journal of Computer Applications & Information Technology*, *1*(II).

[5] Boreiry, M., & Keyvanpour, M. R. (2017, April). Classification of watermarking methods based on watermarking approaches. In *2017 Artificial Intelligence and Robotics (IRANOPEN)* (pp. 73-76). IEEE.

[6] Song, C., Sudirman, S., & Merabti, M. (2009, October). Recent advances and classification of watermarking techniques in digital images. *Proceedings of post graduate network symposium* (pp. 1-6).

[7] Lee, Sin-Joo, Jung, Sung-Hwan (2001), A survey of watermarking techniques applied to multimedia, In. ISIE, IEEE International Symposium on Industrial Electronics Proceedings, pp 272–277

[8] Prabhishek S, Chadha RS (2013) A survey of digital watermarking techniques, applications and attacks.

a. International Journal of Engineering and Innovative Technology (IJEIT) 2(9):165–175.

[9] Thakur, S, Singh, A. K, Ghrera, S.P, Dave, M (2018) Watermarking Techniques and Its Applications in

a. Tele-Health: A Technical Survey, In: Cryptographic and Information Security Approaches for Images and Videos By S. Ramakrishnan Chapter −17, pp. 467–511.

[10] J. Nayak, , P. S. Bhat, M. S. Kuniar, R. Acharya U (2004) Reliabletransmission and storage of medical images with patient information using error control codes, in. IEEE INDICON, First India Annual Conference, pp 147–150.

[11] Badshah G, Liew S-C, Zain JM, Ali M (2016) Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. J Digit Imaging 29(2):216–225

[12] Hajjaji MA, Mtibaa A, Bourennane E-B (2011) A watermarking of medical image: method based "LSB".

a. Journal of Emerging Trends in Computing and Information Sciences 2(12):656–663

[13] Hassan B, Ahmed R, Li B, Hassan O (2019) An imperceptible medical image watermarking framework

a. for automated diagnosis of retinal pathologies in an eHealth arrangement. IEEE Access 7:69758–69775

[14] Lach, J, Mangione-Smith, W. H, Potkonjak, M (1998) FPGA fingerprinting techniques for protecting

a. intellectual property, IEEE Custom Integrated Circuits Conference, pp 299–302

[15] Liu Q, Xuemei J (2006) Design and Realization of a Meaningful Digital Watermarking Algorithm Based

a. on RBF Neural Network, in. Sixth World Congress on Intelligent Control and Automation, WCICA 1: 2878–2881.

[16] Jia S, Zhou Q, Zhou H (2017) A novel color image watermarking scheme based on DWT and QR

a. decomposition. Journal of Applied Science and Engineering 20(2):193–200

[17] Jung K, Yoo K (2009) Data hiding method using image interpolation. Comput Stand Interfaces 31:465–447.

[18] Puech, William, Rodrigues, José M (2004) A new crypto-watermarking method for medical images safe transfer, In. 12th European Signal Processing Conference, pp 1481–1484.

[19] Al-qdah M (2018) Secure watermarking technique for medical images with visual evaluation. Signal & Image Processing: An International Journal (SIPIJ) 9(1):1–9.

[20] Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A (2018) Multiple watermarking technique for securing online social network contents using Back propagation neural network. Futur Gener Comput Syst 86:926–939.

[21] Aditi Z, Singh AK, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT,

a. DCT and SVD for application in medicine. Multimed Tools Appl 77(4):4863–4882.

[22] Singh AK (2019) Robust and distortion control dual watermarking in LWT domain using DCT and error

a. correction code for color medical image. Multimed Tools Appl 78:30523–30533.

[23] Thakur S, Singh AK, Ghrera SP, Elhoseny M (2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl 78(3):3457–3470.

[24] Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Medical & Biological Engineering & Computing 44(8):619– 631.

[25] Singh AK, Dave M, Mohan A (2015) Multilevel encrypted text watermarking on medical images using spread-Spectrum in DWT domain. Wirel Pers Commun 83(3):2133–2150

[26] Singh AK, Kumar B, Dave M,Mohan A (2015) Multiple watermarking on medical images using selective

a. discrete wavelet transforms coefficients. Journal of Medical Imaging and Health Informatics 5(3):607–614

[27] Singh, K. U., Singh, V. K., & Singhal, A. (2018). Color Image Watermarking Scheme Based on QR Factorization and DWT with Compatibility Analysis on Different Wavelet Filters. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(06), 1796-1811.

[28] Wakatani, A (2002) Digital watermarking for ROI medical images by using compressed signature image, In. 35th Annual Hawaii International Conference on System Sciences.

[29] Singh, K. U., & Singhal, A. (2018). Channelized Noise Augmentation to Endorse DICOM Medical Image for Diagnosing. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(06), 2228-2247.

[30] F. Rahimi, H. Rabbani, A dual adaptive watermarking scheme in contourlet domain for DICOM images, BioMed. Eng. Online (2011), http://www.biomedical-engineering-online.com/content/10/1/53.

[31] O.M. Al-Qershi, B.E. Khoo, Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images, J. Digit. Imaging 24(February (1)) (2011) 114–125.

[32] Ch. K. Tan, J. Ch. Ng, X. Xu, Ch. L. Poh, Y.L. Guan, K. Sheah, Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability, J. Digit. Imaging 24 (June (3)) (2011) 528–540.

[33] V. M. Potdar, S. Han and E. Chang, “A Survey of Digital Image Watermarking Techniques”, 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[34] Xuehua, Jiang. "Digital watermarking and its application in image copyright protection." 2010 International Conference on Intelligent Computation Technology and Automation. Vol. 2. IEEE, 2010.

[35] Singh, A. K., Sharma, N., Dave, M., & Mohan, A. (2012, December). A novel technique for digital image watermarking in spatial domain. In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (pp. 497-501). IEEE.

[36] Naveed, A., Saleem, Y., Ahmed, N., & Rafiq, A. (2015). PERFORMANCE EVALUATION AND WATERMARK SECURITY ASSESSMENT OF DIGITAL WATERMARKING TECHNIQUES. Science International, 27(2).

[37] Abhishek Kumar, et al. "The state of the art of deep learning models in medical science and their challenges". Multimedia Systems. (2020).

[38] Abhishek Kumar, et al. "Efficient data transfer in edge envisioned environment using artificial intelligence based edge node algorithm". Transactions on Emerging Telecommunications Technologies. (2020).

[39] Ambeth Kumar, V.D. et al. "Active volume control in smart phones based on user activity and ambient noise". Sensors (Switzerland) 20. 15(2020): 1-17.

[40] Vengatesan, K. et al. "Analysis of Mirai Botnet Malware Issues and Its Prediction Methods in Internet of Things". Lecture Notes on Data Engineering and Communications Technologies 31. (2020): 120-126.

[41] Vimal, V. et al. "Artificial intelligence-based novel scheme for location area planning in cellular networks". Computational Intelligence. (2020).

[42] Kumar, A. et al. "Comparative Analysis of Data Mining Techniques to Predict Heart Disease for Diabetic Patients". Communications in Computer and Information Science 1244 CCIS. (2020): 507-518.

[43] Sayyad, S. et al. "Digital Marketing Framework Strategies Through Big Data". Lecture Notes on Data Engineering and Communications Technologies 31. (2020): 1065-1073.

[44] Kumar, V.D.A. et al. "Exploration of an innovative geometric parameter based on performance enhancement for foot print recognition". Journal of Intelligent and Fuzzy Systems 38. 2(2020): 2181-2196.

[45] Vengatesan, K. et al. "Secure Data Transmission Through Steganography with Blowfish Algorithm". Lecture Notes on Data Engineering and Communications Technologies 35. (2020): 568-575.

[46] Lone, T.A. et al. "Securing communication by attribute-based authentication in HetNet used for medical applications". Eurasip Journal on Wireless Communications and Networking 2020. 1(2020).

[47] Vengatesan, K. et al. "Simple Task Implementation of Swarm Robotics in Underwater". Lecture Notes on Data Engineering and Communications Technologies 35. (2020): 1138-1145.

[48] Kesavan, S. et al. "An investigation on adaptive HTTP media streaming Quality-of-Experience (QoE) and agility using cloud media services". International Journal of Computers and Applications. (2019)

[49] Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, V.D. Ambeth Kumar, B.K. Panigrahi, Kalyana C. Veluvolu, Black Hole Attack Detection in Vehicular Ad-Hoc Network Using Secure AODV Routing Algorithm, Microprocessors and Microsystems, 2020, 103352, https://doi.org/10.1016/j.micpro.2020.103352