Wireless Pers Commun (2017) 92:1611–1624
DOI 10.1007/s11277-016-3625-x

Robust and Secure Multiple Watermarking for Medical Images

Abhilasha Sharma[1] · Amit Kumar Singh[1] · Satya Prakash Ghrera[1]

Published online: 19 August 2016

Abstract This paper presents a robust and secure region of interest and non-region of interest based watermarking method for medical images. The proposed method applies the combination of discrete wavelet transform and discrete cosine transforms on the cover medical image for the embedding of image and electronic patient records (EPR) watermark simultaneously. The embedding of multiple watermarks at the same time provides extra level of security and important for the patient identity verification purpose. Further, security of the image and EPR watermarks is enhancing by using message-digest (MD5) hash algorithm and Rivest–Shamir–Adleman respectively before embedding into the medical cover image. In addition, Hamming error correction code is applying on the encrypted EPR watermark to enhance the robustness and reduce the possibility bit error rates which may result into wrong diagnosis in medical environments. The robustness of the method is also extensively examined for known attacks such as salt & pepper, Gaussian, speckle, JPEG compression, filtering, histogram equalization. The method is found to be robust for hidden watermark at acceptable quality of the watermarked image. Therefore, the hybrid method is suitable for avoidance of the patient identity theft/alteration/modification and secure medical document dissemination over the open channel for medical applications.

✉ Amit Kumar Singh
amit_245singh@yahoo.com

Abhilasha Sharma
sharma.abhilasha.cs12@gmail.com

Satya Prakash Ghrera
sp.ghrera@juit.ac.in

[1] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India

Keywords Image watermarking · EPR · DICOM · DWT · DCT · RSA · MD5 · Hamming ECC · ROI and NROI

1 Introduction

In recent years, telemedicine, teleradiology, tele-consultation tele-diagnosis and telematics services are play a significant responsibility in the growth of medical applications. However, management of the EPR data over the network is a potential issue for these services. The digital imaging and communications in medicine (DICOM) standard is defined for the transmission of EPR data over the network. This standard includes a header file with the DICOM medical image which provides the significant information about patient. However, this header may be misplaced, attacked or disordered and further the header needs additional bandwidth. Due to these reasons the watermarking techniques provide alternative solution to the transmission of medical images/patient data [1–7]. Four major importance of the medical image watermarking for e-health services are given in Fig. 1 [8].

The transmitted images are prone to corruption in the transmission medium due to noise. Any distortion in the received images may lead to faulty watermark detection and inappropriate disease diagnosis. The use of ECC not only addresses this problem but also enhances robustness of the watermark. Further, the integrity of the medical data is very important for the e-health services to avoid any wrong diagnoses [8, 9]. In recent year, combined approach of watermarking and cryptography provides dual level security for the EPR data [10]. However, robustness and security against malicious attacks are the potential challenges for a good watermarking system [11].

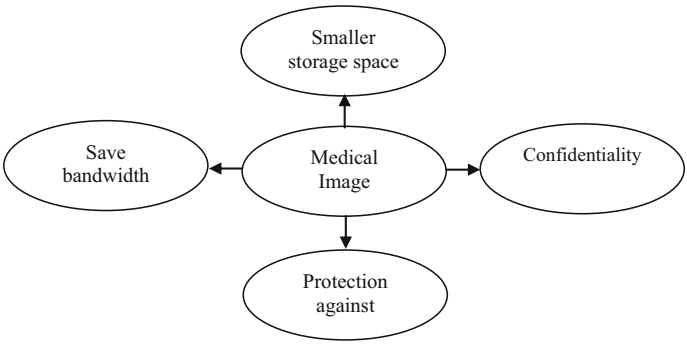


Fig. 1 Importance of medical image watermarking

2 Related Work

In this section, a brief review of reported digital image watermarking methods using DWT is presented below:

The ROI and NROI are the two important parts of the image [12]. The ROI part of the medical image contains the important information, which does not allow any modification in this part [13]. However, NROI part contains the background information of an image, where the watermark information can be embedded for the secure transmission as reported in [14–16]. Recently, DWT based watermarking methods using medical image is reported in [11, 17–21].

Liew et al. [22] proposed a region based medical image watermarking algorithm using least significant bit (LSB) and run-length encoding (RLE). The medical cover image is decomposed into ROI and NROI section, where compressed watermark by applying RLE from ROI are stored in NROI section of an image. Navas et al. [17] proposed a blind watermarking method in ROI images based on integer wavelet transform. The EPR is embedded into the NROI part of selected sub-band of the cover image. Further, the security of the EPR watermark is enhanced by applying the encryption technique prior to embedding into the cover. Moreover, author's claim that the method can embed up to a maximum of 3400 characters and extract all the watermark bits without any distortion. The method can embeds more watermark information at acceptable quality of the image. However, the method is not tested for known attacks.

Nakhaie et al. [23] proposed a region based watermarking method based on spread spectrum and discrete wavelet transform. The medical cover image is decomposed into ROI and NROI, where binary watermark is embedding into DCT transform of NROI part of the cover using spread spectrum embedding method. The visual quality of the image is examined by Peak signal-to-noise ratio (PSNR) and mean squared error (MSE). Raul et al. [24] presents a compression and encryption based data hiding method using image using moment theory for medical images. The DICOM data is considered as watermark is embedding into the cover. The accuracy of the watermark is tested for JPEG and rotation attacks. Kaur [25] proposed medical image watermark method is same as the method presenting in [23]. The proposed method is embedding EPR and binary watermark into the cover image for quality assessment. The performance of the method is good for the JPEG attacks where the quality factor must be greater than or equal to 30 %. Kannammal et al. [26] proposed a encryption based medical images watermarking method using LSB and DWT. The medical image watermark is embedded in each block of cover image in the selected DWT sub-band using LSB. In addition, the security of the cover and watermark is enhanced by encrypting the watermarked image using three different encryption algorithms (AES, RSA and RC4). The experimental results have shown that Rivest Cipher 4(RC4)

algorithm performs better than the other two encryption algorithms. Further, the method is robust and secure for known attacks. Al-Haj and Alaa'Amer [27] described a multiple image watermarking method using LSB, DWT and singular value decomposition (SVD). The method using robust and fragile watermarks are embedding into the cover image. The robust watermarks are embedding into the NROI area of the cover image using DWT and SVD. However, fragile watermarks are embedding into the ROI area of the image by using LSB. The proposed method is robust for JPEG and salt & pepper attacks. For the Teleophthalmology application, Pandey et al. [28] proposed ROI and NROI based medical image watermarking using DWT and SVD. To enhance the security of the method, SHA-512 hash algorithm is applied on the ROI part of the cover image to generate the unique hash value. The EPR/text watermark is encoded with unique hash value and the encoded text and image watermark is embedded into the NROI part of the DWT cover image. The method is extensively evaluated for various attacks including Checkmark attacks. The PSNR and NC values have been compared with other existing method [8].

This study represents the multiple watermarking method using DWT and DCT. The EPR data and image watermark is embedding simultaneously into the NROI and ROI part of the cover object respectively using for ownership identification purpose. Further, EPR watermark is encoded by the RSA cryptography algorithm [29–31], which enhances the security of the watermark. Although, the image watermark is hashed by using the MD5 algorithm [30, 31]. The error correction codes are also applied to the encoded EPR data making the text watermark robust against the signal processing attacks [31, 32]. The final watermarked image is further encrypted to protect from unauthorized access and miscellaneous intruder attacks.

3 Proposed Algorithm

In the proposed method, fusion of DWT and DCT is applied on medical cover image instead of DWT and DC separately. The details of embedding and extraction process of the proposed method are given in Sects. 2.1 and 2.2 respectively. Further, both process is represented diagrammatically in Fig. 2a, b.

3.1 Watermark Embedding Process

STEP 1: Initialization and inputs

STEP 2: Read the Images

Input: Medical cover image (C) of size 512×512.

Logo image watermark (W) of size 256×256 and EPR watermark file (E).

Output: The encrypted watermarked image 'W_d' of size N×N

STEP 3: decompose the cover image into two parts i.e ROI and NROI.

STEP 4: Determine second level DWT of the important parts of the cover

LL_r←LL band of ROI

LL_{nr}←LL band of NROI

STEP 5: Determine third Level DWT and DCT to watermark image 'W'

LL_w←LL band of W

LL_{wc}←DCT (Ll_w)

STEP 6: Format the image watermark

repeat for each value (i,j) of LL_{wc}

do

K(i,j) ←LL_{wc}((i mod W_n)+1, (j mod W_m)+1);

end;

until i, j ≤ ROI;

Hash the image watermark using MD-5.

w1←hash(K(i,j)).

STEP 7: Encrypt and encode the selected EPR (E) data by using RSA and Hamming code respectively

//Encode the encrypted file using Hamming codes

w2← Hamming encoder(encrypt(E));

STEP 8: Embed the watermarks using XOR function

X←ROI + w1;

Y←NROI + w2;

add X and Y to form watermarked image W_d.

W_d ←X+Y;

end;

STEP 9: Encrypt the watermarked

repeat for each value (i, j)

do

E(i,j)= Encrypt(W_d(i,j));

end;

until i ,j ≤ C_n

3.2 Watermark Extraction Process

Start:

STEP 1: Initialization and inputs

STEP 2: Read the Images

Input: Encrypted watermarked image of size C_n

Output: Watermarked image of size M×M and EPR data file.

STEP 3: Decrypt the watermarked image

repeat for each value (i,j)

do

D(i,j) ←decrypt (E(i ,j));

end;

until i,j ≤ C_n

STEP 4: Decompose the cover image into two parts i.e ROI and NROI.

STEP 5: Determine second level DWT of the important areas of the cover

LL_r←LL band of ROI;

LL_{nr}←LL band of NROI;

STEP 6: Determine 3rd level DWT and DCT to watermark image 'W'

LL_w←LL band of W

LL_{wc} ←DCT (LL_w)**;**

STEP 7: Extract the image watermark from ROI and rehash using MD-5.

W1 ←rehash (LL_{wc});

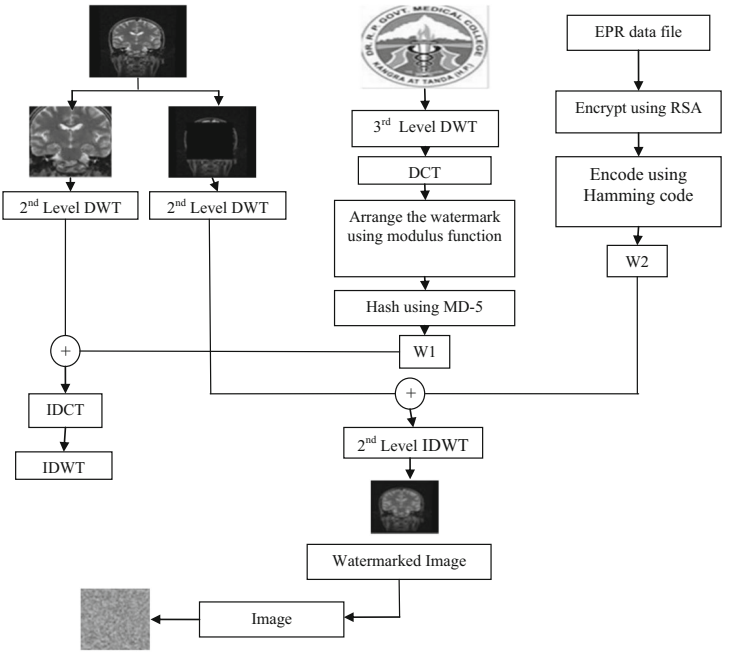
STEP 8: Extract the EPR watermark from NROI, decode it using Hamming code and decrypt using RSA

W2←Hamming decoder (decrypt(NROI));

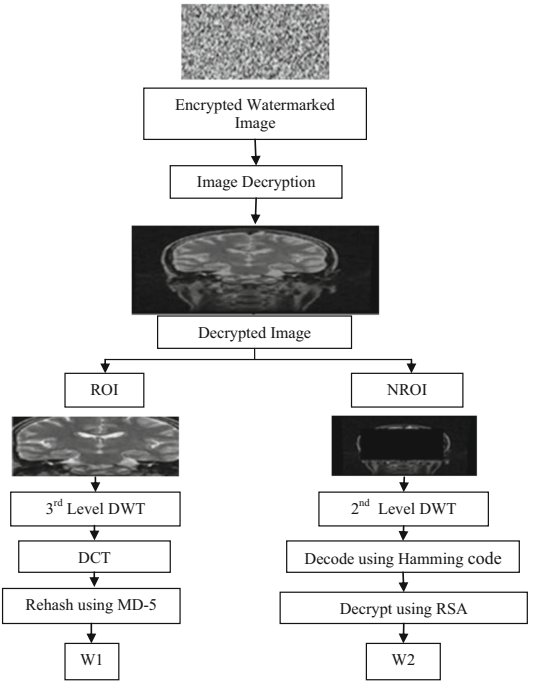
4 Experimental Results and Performance Analysis

The proposed watermarking embedding and extraction method is tested for MRI, CT Scan and ultrasound images [33]. The image size 512 × 512 is used as the cover image is divided into the ROI and NROI regions. For the testing, the image watermark size of 256 × 256. The ROI and NROI part of the cover is decomposed by second level DWT. The hashed watermark image is hidden to the ROI part however, encrypted and encoded EPR data (33 characters) is hidden to the NROI part of the cover. Figure 3a, b shows the original and watermarked image respectively. Figure 4a, b shows the health center logo as image and EPR data as text watermark respectively.

The robustness of the EPR watermark is enhanced by the Hamming code, which is applied on 7-bit binary illustration of the data before embedding into the cover medical image. The performance of the method is examined for different gain factor ranging

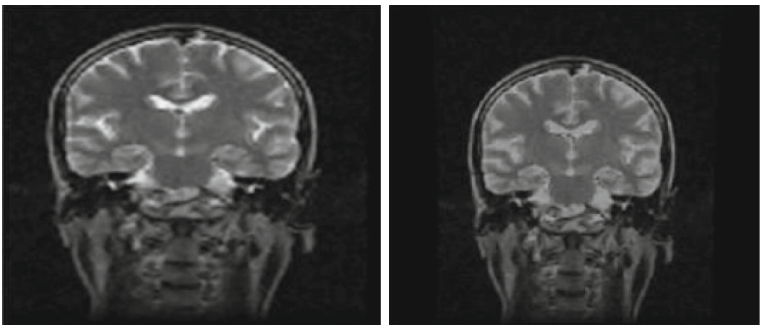


(a)



(b)

Fig. 2 Proposed watermark **a** embedding and **b** extraction process



(a) (b)

Fig. 3 The image considered as **a** cover and **b** watermarked

Abhilasha_30290_JUITWS_BXBPS4951D

(a) (b)

Fig. 4 **a** Image watermark and **b** EPR watermark

Table 1 Gain factors versus NC and BER values for different medical images

Gain factors	NC values				BER values			
	MRI		CT scan		MRI		CT scan	
	Brain	Spine	Brain	Heart	Brain	Spine	Brain	Spine
0.02	1	1	1	1	0	0	0	0
0.05	1	1	1	1	0	0	0	0
0.8	1	1	1	1	0	0	0	0
1	1	1	1	1	0	0	0	0

from 0.02 to 1.0, cover image and known attacks. The degradation in the visual quality cover image is evaluated by PSNR. Further, robustness of the extracted image and EPR watermark is evaluated by NC and BER respectively. Table 1 describes the NC and BER values for watermark 'w1' and 'w2' respectively at different gain factors ranging from 0.01 to 1. It is observed that the robustness performance is increasing with increasing the gain factors. Referring this table, the NC value evaluated at different gain factors and it is observed that the maximum value is obtained at gain factor = 1 for MRI images. For CT scan images, the NC value is 1 at gain factors 0.02–1. Table 2

Table 2 Gain factors versus PSNR values for different medical images

Gain factors	PSNR values (dB)			
	MRI		CT scan	
	Brain	Spine	Brain	Spine
0.02	51.833272	51.17509	52.161197	50.391136
0.05	38.856662	39.475693	40.040889	39.789543
0.8	36.420885	37.042364	37.042364	37.042364
1	36.420885	37.042364	37.042364	37.042364

shows the PSNR performance obtained by the proposed method without the signal processing attacks. From the experimental result it is observed that the PSNR value decreases with the increase in gain factor. For Brain MRI image, the PSNR ranges from 36.420885 to 51.833272 dB at gain factor 1–0.02. However, PSNR value ranges from 37.042364 to 50.391136 dB at the same gain factors for CT-Scan images. Figure 5 show the graphical representation of Table 2.

Table 3 shows the NC and BER values for 'w1' and 'w2' respectively for different noise attacks at gain factor = 1. Referring Table 3, it is observed that the highest NC value is obtained as '1.0' against contrast, histogram equalization and cropping attacks for both MRI and CT scan image. However, the lowest NC value is obtained as 0.899266 against rotation attack for the same images. This table also presents the BER values for the different noise. In this table, we observed that highest BER value for MRI and CT scan images is obtained as 0.1884 and 0.3264 respectively against Gaussian (Mean = 0, variance = 0.00003) noise. However, the lowest BER value is obtained as 0.1233 (except for Gaussian and speckle noise) and 0.1250 (against speckle noise) for the same images. Figure 6a, b show the NC performance of the proposed method for salt & pepper and speckle noise respectively and different noise level. The security of the EPR watermark is enhanced by applying the RSA technique before embedding into the cover. The RSA encoding and decoding time is also evaluated for different EPR watermark at three different values of prime numbers P and Q in Table 4. Referring Table 4, it is observed that the encoding and decoding time is highly

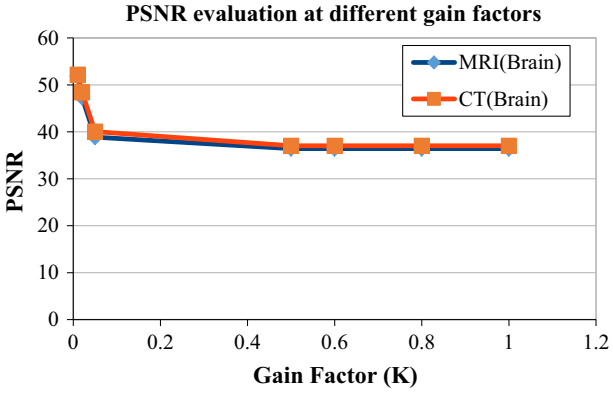


Fig. 5 PSNR performance of the proposed method at different gain

Table 3 NC and BER values obtained by the proposed method for known attacks

Noise	NC values		BER values	
	MRI	CT scan	MRI	CT Scan
Salt & pepper (noise density = 0.001 and 0.002	0.94405 and 0.943998	0.949754 and 0.949720	0.1233	0.1259
Gaussian (mean = 0, variance = 0.00001)	0.944054	0.950014	0.1545	0.263
Gaussian (mean = 0, variance = 0.00003)	0.944001	0.940069	0.1884	0.3264
Speckle (variance = 0.00001)	0.943955	0.949742	0.1276	0.125
Speckle (variance = 0.00002)	0.943951	0.949742	0.1285	0.1328
JPEG compression (QF = 65)	0.949301	0.949301	0.1233	0.1563
Contrast adjustment	1	1	0.1233	0.1563
Histogram equalization	1	1	0.1233	0.1563
Gaussian LPF	0.965043	0.965043	0.1233	0.1563
Rotation (0.01 rad)	0.899266	0.899266	0.1233	0.1563
Cropping	1	1	0.1233	0.1563

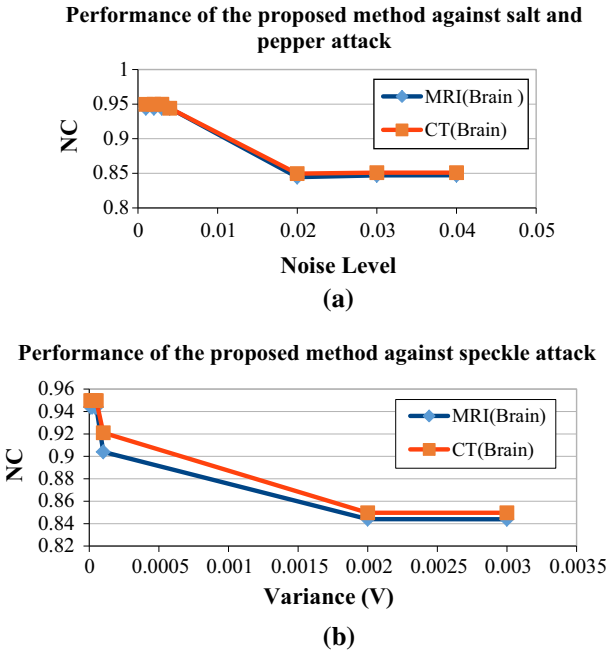


Fig. 6 NC performance of the proposed method for **a** salt & pepper and **b** speckle noise at different noise level

depends on the size of EPR watermark. Due to the limited resource of our experimental setup, we simulated the proposed algorithm on smaller prime numbers. However, it may also perform better for large prime numbers.

Table 4 Encoding and decoding time for different size of EPR watermark

Prime numbers		Different EPRs of different sizes (in bytes)							
		Encoding time (s)				Decoding time (s)			
P	Q	89	110	150	260	89	110	150	260
43	47	0.1563	0.1719	0.2564	0.2867	0.25	0.2656	0.3564	0.3867
89	97	0.2701	0.2786	0.3513	0.3689	0.37	0.39	0.4377	0.4798
131	113	0.4856	0.4999	0.5105	0.5288	0.6066	0.6589	0.7466	0.7534

5 Conclusion

In healthcare domain, the security of EPR data is primary concern to protect the confidential patient reports from the unauthorized access and unwanted tamper. The medical images shared over the internet must be protected from malicious attacks. This paper presents DWT and DCT based multiple watermarking method using RSA and Hamming error correcting codes. The image and EPR watermark is embedded simultaneously into the cover for the purpose of ownership identification and enhanced security of the medical information. Initially, the propose method identified ROI and NROI section of the cover image. Based on importance of the medical information, the EPR and image watermarks are hidden into the NROI and ROI part of the cover medical image respectively. Refereeing Table 1 to Table 4, the PSNR, NC and BER values of the hybrid method is highly depends on noise level, gain factor and the size of the watermark. The main contribution of the research is given below:

1. The proposed hybrid (DWT and DCT) watermarking method enhanced the NC and PSNR performance as compared to DWT and DCT applied individually,
2. RSA and MD5 are applied on EPR and image watermark respectively before embedding into the cover, which provides the extra level security of the watermarks. Further, Hamming code is applied on the encoded EPR watermark, which reduces the error rates as obtained by the proposed method. Moreover, the robustness method is examined for different known attacks, and
3. Two different watermarks are hidden into the cover, which enhanced the security of both watermarks, reduce the bandwidth and storage space requirements. It includes, the multiple watermarking is appropriate for medical applications.

Therefore, the method is suitable for the avoidance of patient identity theft/alteration/modification and secure medical document dissemination over the open channel for medical applications.

Various techniques were combined to make balance between the major benchmark performance parameters (robustness, imperceptibility, capacity and security) of the watermarking system. However, computational complexity of the method needs to be investigated separately in future communication.

References

1. Matheson, L. R., Mitchell, S. G., Shamoon, T. G., Tarjan, R. E., & Zane, F. (1998). Robustness and security of digital watermarks. *Financial Cryptography, 1465*, 227–240.
2. Coatrieux, G., Lecornu, L., Roux, Ch., & Sankur, B. (2006). A review of image watermarking applications in healthcare. In *Proceedings of the 28th annual international conference engineering in medicine and biology society, EMBS'06, IEEE, New York* (pp. 4691–4694).
3. Mohanty, S. P. (2000). *Digital watermarking: A tutorial review*. Report, IISc. Bangalore, India.
4. Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., & Collorec, R. (2000). Relevance of watermarking in medical imaging. In *Proceedings of IEEE conference on information technology applications in biomedicine, Arlington, USA* (pp. 250–255).
5. Moumen, C., & Benslama, M. (2012). Cyrptography of medical images. In *Proceedings of the progress in electromagnetics research symposium, Kuala Lumpur, March 27–30* (pp. 42–48).
6. Chao, H. M., Hsu, C. M., & Miaou, S. G. (2002). A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Transactions on Information Technology in Biomedicine, 6*(1), 46–53.
7. Annamalai, U., & Thanushkodi, K. (2013). Medical image authentication with enhanced watermarking technique through visual cryptography. *Journal of Theoretical and Applied Information Technology, 57*(3), 484–494.
8. Singh, A. K., Dave, M., & Mohan, A. (2015). Robust and secure multiple watermarking in wavelet domain. A special issue on advanced signal processing technologies and systems for healthcare applications. *Journal of Medical Imaging and Health Informatics, 5*(2), 406–414.
9. Rey, C., & Dugelay, J. L. (2002). A survey of watermarking algorithm for image authentication. *EURASIP Journal on Applied Signal Processing, 6*, 613–621.
10. Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. (2014). Watermarking techniques used in medical images: A survey. *Journal of Digital Imaging, 27*(6), 714–729.
11. Singh, A. K., Kumar, B., Dave, M., & Mohan, A. (2015). Robust and imperceptible dual watermarking for telemedicine applications. *Wireless Personal Communications, 80*(4), 1415–1433.
12. Singh, A. K., Dave, M., & Mohan, A. (2014). Wavelet based image watermarking: futuristic concepts in information security. *Proceedings of the National Academy of Sciences, India, Section A: Physical Sciences, 84*(3), 345–359.
13. Zhang, L., & Zhou, P. P. (2010). Localized affine transform resistant watermarking in region-of-interest. *Telecommunication Systems, 44*(3), 205–220.
14. Yang, C. Y., & Hu, W. C. (2010). Reversible data hiding in the spatial and frequency domains. *International Journal of Image Processing, 3*(6), 373–382.
15. Zain, J., & Clarke, M. (2005). Security in telemedicine: Issue in watermarking medical images. In *Proceedings of 3rd international conference on science of electronic, technologies of information and telecommunications, Tunisia*, March 27–31, 2005.
16. Memon, N. A., & Gilani, S. A. M. (2008). NROI watermarking of medical images for content authentication. In *Proceedings of 12th IEEE international multitopic conference, Karachi, Pakistan* (pp. 106–110).
17. Navas, K. A., Thampy, S. A., & Sasikumar, M. (2008). EPR hiding in medical images for telemedicine. In *Proceedings of the world academy of science, engineering and technology, Rome* (pp. 292–295).
18. Singh, A. K., Kumar, B., Dave, M., & Mohan, A. (2015). Multiple watermarking on medical images using selective DWT coefficients. *Journal of Medical Imaging and Health Informatics, 5*(3), 607–614.
19. Paar, C., & Pelzl, J. (2009). *Understanding cryptography: A textbook for students and practitioners* (3rd ed., pp. 29–53). New York: Springer.
20. Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. (2012). A joint encryption/watermarking system for verifying the reliability of medical images. *IEEE Transactions on Information Technology in Biomedicine, 16*(5), 891–899.
21. Wong, P. W., & Memon, N. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, *10*(10), 1593–1601.
22. Liew, S. C., Liew, S. W., & Zain, J. M. (2010). Reversible medical image watermarking for tamper detection and recovery with run length encoding compression. *Proceedings of the World Academy of Science, Engineering and Technology, 4*, 12–29.
23. Nakhaie, A. A., & Shokouhi, S. B. (2011). No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using ROI processing. In *Proceedings of the 24th Canadian conference on electrical and computer engineering, Niagara Falls* (pp. 121–125), 8–11 May 2011.

24. Rodriguez-Colin, R., Claudia, F.-U., Trinidad-Blas, G. D. J. (2007). Data hiding scheme for medical images. In *Proceedings of the 17th international conference on electronics, communications and computers, Cholula, Puebla* (pp. 32–37), 26–28 February 2007.
25. Kaur, R. (2013). A medical image watermarking technique for embedding EPR and its quality assessment using no-reference metrics. *International Journal of Information Technology and computer Science, 02*, 73–79.
26. Kannammal, A., & Rani, S. S. (2014). Two level security for medical images using watermarking/encryption algorithms. *International Journal of imaging system and technology, 24*(1), 111–120.
27. Al-Haj, A., & Alaa'Amer, (2014). Secured telemedicine using region-based watermarking with tamper localization. *Journal of Digital Imaging, 27*(6), 737–750.
28. Pandey, R., Singh, A. K., Kumar, B., & Mohan, A. (2016). Iris based secure NROI multiple eye image watermarking for teleophthalmology. *Multimedia Tools and Applications*. doi:10.1007/s11042-016-3536-6.
29. Sasaki, Y. (2011). Collisions of MMO-MD5 and their impact on original MD5. *Progress in Cryptology*—AFRICACRYPT *2011* (Vol. 6737, pp. 117–133).
30. Sasaki, Y., & Aoki, K. (2008). Preimage attacks on step-reduced MD5. *Information Security and Privacy, 5107*, 282–296.
31. Munuera, C. (2015). Hamming codes for wet paper steganography. *Designs, Codes and Cryptography, 76*(1), 101–111.
32. Lien, B. K., Chen, S. K., Wang, W. S., & King, K. P. (2015). Dispersed data hiding using hamming code with recovery capability. *Genetic and Evolutionary Computing, 329*, 179–187.
33. http://www.bangahospitals.com/mandav_hospital.php.

Abhilasha Sharma Received M.Tech. in Computer Science and Engineering from Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh in 2015. His research interests include Data Hiding and Cryptography. Currently she is working as Assistant Professor in the department of Computer Science & Engineering, NIT Hamirpur, Himachal Pradesh India.

Dr. Amit Kumar Singh is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering at Jaypee University of Information Technology (JUIT) Waknaghat, Solan, Himachal Pradesh-India since April 2008. He was previously associated with Purvanchal University (U.P. State University), Jaunpur as Lecturer and prior to that he was Investigator-I in Rajbhasha Information Technology Application Promotion Programme (RITAP) Project, funded by Information Ministry, Department of Computer Science and Engineering, Indian Institute of Technology BHU Varanasi-India. He has completed his Ph.D. degree from the Department of Computer Engineering, NIT Kurukshetra, Haryana in 2015. He obtained his M.Tech. degree in Computer Science and Engineering from JUIT Waknaghat, Solan, Himachal Pradesh in 2010. He obtained his B. Tech degree in Computer Science and Engineering from Institute of Engineering and Technology, Purvanchal University Jaunpur, Uttar Pradesh in 2005. He has presented and published over 40 research papers in reputed journals and various national and international conferences. His important research contributions includes to develop watermarking methods that offer a good trade-off between major parameters i.e. perceptual quality, robustness, embedding capacity and the security of the

watermark embedding into the cover digital images. His research interests include Data Hiding, Biometrics and Cryptography. Dr. Singh has served as TPC member, reviewers and corresponding guest editor for various conferences and journals.

Prof. Satya Prakash Ghrera after 34 years of service in Corps of Electronics and Mechanical Engineers of the Indian Army, he joined Jaypee Institute of Engineering and Technology in Jan 2006 as Associate Professor in Department of Computer Science and Engineering. With effect from Sep 2006, he has taken over responsibilities of HOD (Computer Science Engineering and IT) at Jaypee University of Information Technology Waknaghat, Dist Solan HP. He has received professional training at Aydin Systems, Mountain View California and Koden Electronics Tokyo. In addition to various technical and techno administrative assignments, he was also Director of Computer Complex HQ Technical Group Delhi, and Head of Department at Military College of Electronics and Mechanical Engineering, Secunderabad teaching B.Tech. and M.Tech. students. He successfully designed, implemented, installed and maintained a number of communication and computer network based real time information systems for strategic functions. For his distinguished service, he was awarded Army Commander's Commendation twice in 2004 and 1988. Fellowship of BCS(British Computer Society) was conferred upon him in 2013, for an extraordinary record of accomplishments. He is also a Senior Member of IEEE.