

Computationally efficient joint imperceptible image watermarking and JPEG compression: a green computing approach

Rohini Srivastava¹ · Basant Kumar¹ ·
Amit Kumar Singh² · Anand Mohan³

Received: 29 October 2016 / Revised: 1 September 2017 / Accepted: 8 September 2017 /
Published online: 22 September 2017
© Springer Science+Business Media, LLC 2017

Abstract This paper presents a computationally efficient joint imperceptible image watermarking and joint photographic experts group (JPEG) compression scheme. In recent times, the transmission and storage of digital documents/information over the unsecured channel are enormous concerns and nearly all of the digital documents are compressed before they are stored or transmitted to save the bandwidth requirements. There are many similar computational operations performed during watermarking and compression which lead to computational redundancy and time delay. This demands development of joint watermarking and compression scheme for various multimedia contents. In this paper, we propose a technique for image watermarking during JPEG compression to address the optimal trade-off between major performance parameters including embedding and compression rates, robustness and embedding alterations against different known signal processing attacks. The performance of the proposed technique is extensively evaluated in the form of peak signal to

✉ Amit Kumar Singh
amit_245singh@yahoo.com

Rohini Srivastava
srivastava.rohini14@gmail.com

Basant Kumar
singhbasant@yahoo.com

Anand Mohan
profanandmohan@gmail.com

¹ Department of Electronics & Comm. Engineering, Motilal Nehru National Institute of Technology, Allahabad, Uttar Pradesh, India

² Department of Computer Science & Engineering, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, India

³ Department of Electronics Engineering, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh, India

noise ratio (PSNR), correlation, compression ratio and execution time for different discrete cosine transform (DCT) blocks and watermark sizes. Embedding is done on DCT coefficients using additive watermarking.

Keywords Watermarking · Compression · Jpeg · DCT · Quantization · Checkmark attacks

1 Introduction

The transmission, storage and sharing of digital information over the unsecured channel have become intense in recent years. This requires high degree of security, authenticity, reproducibility and copyright protection [12]. Digital asset and right management systems (DARMS) are always using the digital information in encoded form [9]. Digital image watermarking provides an efficient protection of digital information for various applications including Telemedicine, real time video and audio delivery, electronic advertising, digital libraries, broadcast monitoring, e-governance, e-commerce applications, copy control, media identification and tracking, e-Voting Systems, remote education, web publishing and protecting driver license [13].

It has been observed that the JPEG/JPEG2000 compression technique (which is used to apply on the majority of the digital information/data to reduce the bandwidth requirements during transmission) is one of the most common and unavoidable attacks to watermarking systems [4, 17]. Generally, ‘watermarking’ and ‘compression’ are performed in two different steps and there are many common/ redundant computational operations carried out in these steps. Combining the two, reduces the computation cost and machine time which are the main motives of the green computing approach. In order to achieve the goals of green computing and low delay, some of the researchers have been studying combined watermarking and compression using quantization [3, 18].

2 Related work

The recent watermarking methods related to the proposed scheme are presented below:

Tian [14] presented a lossless compression of bi-level image based blind watermarking technique using integer wavelet transform (IWT) for the use of copyright protection. The hash value of the cover digital image (as measured by SHA256) and the compressed bits of the wavelet transformed coefficients of the cover image were embedded simultaneously. The performance of the method was calculated in terms of accuracy. Xie and Arce [15] have proposed combined watermarking and set partitioning in hierarchical tree (SPIHT) compression method in discrete wavelet transform (DWT) domain. The performance of the algorithm was determined in terms of embedding capacity with quantization level. Zargar and Singh [5] proposed a lossy BTC (Block Truncation Coding) compression based watermarking method in DWT domain. In this paper, BTC compression was applied on watermark image before embedding into the cover. The robustness and transparency performance of the proposed method are better than fractal-based compression. Guo et al. [4] proposed a joint watermarking and compression technique using BTC. The method addressed the problem of blocking effect and false contour problem as suffered by BTC. The performance of the proposed method was extensively evaluated by using HVS-PSNR and BER parameters and the method was found to

be robust for various known attacks except JPEG and JPEG2000. Further, the method achieved superior robustness than other reported techniques [6]. Goudia et al. [2] proposed a robust joint JPEG 2000 compression and watermarking technique using DWT and quantization. The experimental results indicated that the method was robust for different attacks at higher quantization step size with minimum degradation in the visual quality of the watermarked image. A lossless compression based watermarking technique was proposed by Badshah et al. [1] using tele-radiology images. The Region-of-interest (ROI) part of the watermark was considered along with a key to generate a new watermark. The generated watermark was compressed by Lempel-Ziv-Welch (LZW) technique and the compressed watermark was embedded into the ROI part of the cover image. The performance of the different compression methods was investigated and it was found that the LZW compression technique offered better compression ratio performance than other conventional compression techniques. The method also verified the tempering in the watermark after extraction and decompression processes. Zear et al. [16] proposed a robust and secure hybrid multiple watermarking techniques through DWT, DCT, singular value decomposition (SVD) and neural network using medical images. Two different text watermarks were compressed and encoded by arithmetic and hamming error correction code respectively. The compressed and encoded text watermark was embedded into the cover image. Further, Arnold transform was applied on the image watermark before embedding into the cover. The performance of the algorithm was extensively evaluated in terms of PSNR, NC and BER. Mary et al. [9] proposed an encryption and compression based watermarking method in LSB domain in which the encrypted watermark was embedded into JPEG 2000 compressed cover image using LSB watermarking technique. Lin et al. [7] also proposed a DCT based color image watermarking where the watermark information was embedded into the low frequencies coefficients of the DCT transformed cover image. The method was found to be robust and imperceptible for different modulus values.

3 Main contribution of the work

This paper presents implementation of a watermarking technique during JPEG compression using DCT coefficients to address the optimal trade-off between major performance parameters which include embedding strength, compression rate and robustness against various attacks. The additive watermarking is implemented at the time of JPEG compression in two different ways: 1) watermarking after obtaining DCT operation and 2) watermarking after quantization operation. The performance of the method is evaluated in terms of PSNR, correlation (robustness), compression ratio, different quantization matrices (Q-factors for DCT), watermark and DCT block sizes. Further, the performance of the watermarking after quantization is compared with watermarking after DCT. The experimental results are showing that the watermarking after quantization performs better in terms of PSNR, correlation and execution time. Further, the performance of the algorithm is tested with ‘Checkmark’ attacks [10].

The rest of the paper is organized as follows. Section 4 presents the proposed joint watermarking and compression schemes. Performance analysis along with experimental results is discussed in Section 5. Finally, the conclusions and future scopes are drawn in Section 6.

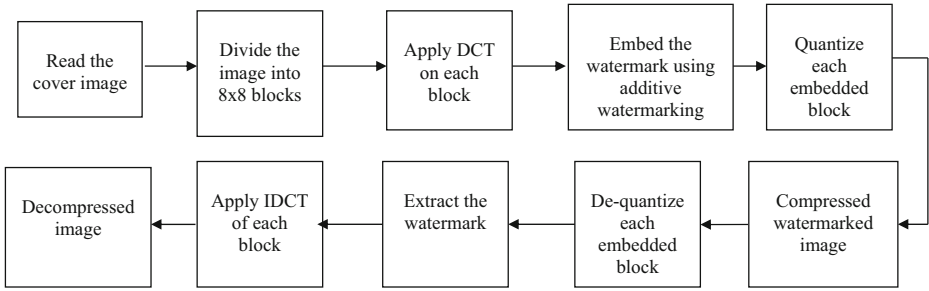


Fig. 1 JPEG additive watermarking after DCT operation

4 Proposed method

The main motive of proposed algorithm is to embed the watermark using additive watermarking at the time of JPEG compression. The first problem is to select the location in the JPEG encoder where the watermarking is to be embedded. The possible locations are after DCT block or after quantization of the DCT coefficients. The proposed algorithm for additive watermarking at the time of JPEG compression is implemented considering the two possible variations (watermarking after DCT or after quantization) which are discussed in subsections 4.1 and 4.2 respectively. Subsection 4.3 presents the detail procedure of quantized DCT coefficient block selection for embedding.

4.1 JPEG additive watermarking after DCT operation

This algorithm evolves the additive watermarking after taking DCT of 8×8 blocks of the cover image. The watermark is embedded into the middle frequency DCT coefficients or into the high frequency components. The lower frequency components remain unchanged as they are the most significant coefficients. Figure 1 shows the embedding process for JPEG additive watermarking after DCT operation. The DCT block is to be quantized after the embedding of watermark. The watermark embedding algorithm used here is simple additive method represented by Eq. (1):

$$I_w = I_{DC} + \alpha W_o \tag{1}$$

Where; I_{DC} is DCT of the cover image, W_o is the original watermark, α is scale factor and I_w is the watermarked image.

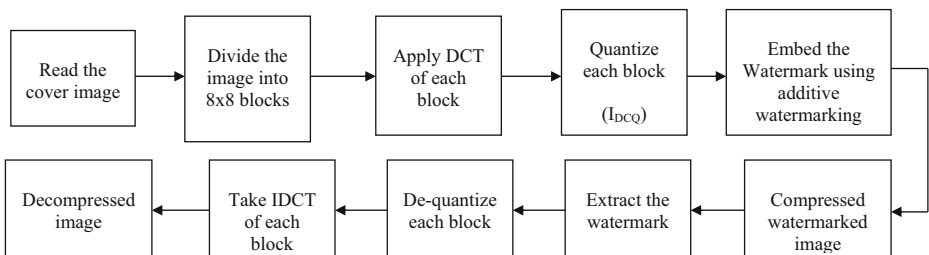


Fig. 2 JPEG additive watermarking after quantization operation



Fig. 3 a Cover and watermarked image (b) after DCT (c) after quantization

The extraction of the watermark is done by just reversing the embedding process and the extracted watermark W_{ex} is represented as:

$$W_{ex} = (I_W - I_{DC}) / \alpha \tag{2}$$

4.2 JPEG additive watermarking after quantization operation

This algorithm involves additive watermarking after quantizing the DCT coefficients. This algorithm is simpler than the algorithm discussed in subsection 4.1. It is observed that most of the 8×8 blocks of the image after quantization possesses only one significant value. Some of the blocks are having more than one coefficient but only one coefficient among them is having the most significant value and that can easily be recognisable by the coding matrix. Fig. 2.shows embedding process for JPEG additive watermarking after quantization. In this process, the watermark embedding and extraction algorithms are same as shown in eq. (1) and Eq. (2).

4.3 Quantized DCT coefficient block selection procedure for embedding

In this process, if the watermark is of size $N \times M$ then size of quantized DCT coefficient block should be selected in such a manner that each block may embed only one pixel of the watermark, so that watermark is uniformly distributed over each block of DCT coefficients. If the cover image is of size $A \times B$ then the size of each quantized DCT block will be:

$$\frac{(A \times B)}{(N \times M)} = \text{Size of each DCT block} \tag{3}$$

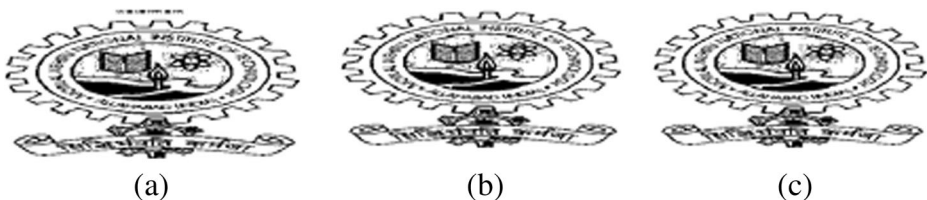


Fig. 4 a Watermark and extracted watermark (b) after DCT (c) after quantization

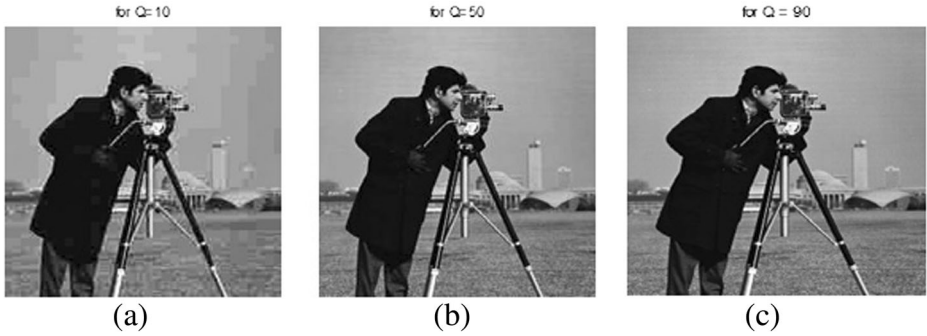


Fig. 5 watermarked image at (a) $Q = 10$, (b) $Q = 50$, (c) $Q = 90$

For example, if the cover image of size 256×256 and watermark image of size 32×32 then the DCT block size should be $\frac{256 \times 256}{32 \times 32} = 8 \times 8$. In this case, each quantized DCT block of the cover image will embed only one pixel of the watermark. Therefore, embedding watermark pixels are uniformly distributed over various DCT coefficient blocks with the help of the above algorithm to achieve imperceptible watermarking. It can be observed from the Fig. 9 that 8×8 DCT coefficient block has only one significant coefficient for embedding. Therefore, it is very obvious that for robust watermarking, DCT coefficient block to be selected for embedding single bit should have a size of $\geq 8 \times 8$ which will be verified through experimental results obtained in the next section. Subsequently, the capacity of the watermark for a given cover image can also be calculated as $Watermark\ Capacity = \frac{A}{8} \times \frac{A}{8}$.

5 Experimental results and performance analysis

In this section, the performance of the proposed joint watermarking and JPEG compression algorithm is evaluated in terms of PSNR, correlation (robustness), compression ratio and robustness against various checkmark attacks. Figure 3 (a)-(c) shows the standard grayscale cameraman image of size 256×256 pixels as an original image, watermarked image after DCT process and watermarked image after quantization process respectively. Figure 4 (a)-(c) shows the binary image watermark of size 32×32 , extracted watermark after DCT and extracted watermark after quantization respectively. The quality (Q)-factor indicates the quality of decompressed image, high Q-factor reflects finer quantization and low compression ratio. A

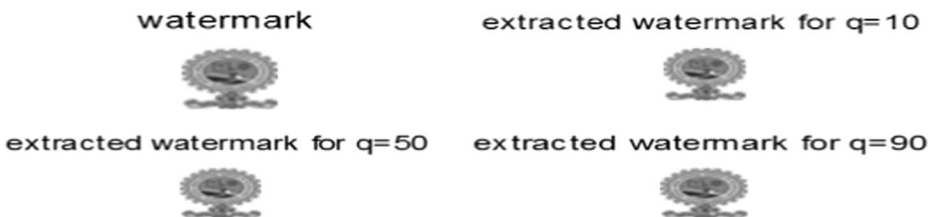


Fig. 6 watermark and extracted watermark at $Q = 10, 50$ & 90



Fig. 7 Watermarked image at (a) block size 32×32 , (b) block size 16×16 (c) block size 8×8

good trade-off between image quality and degree of compression is achieved by selecting $Q = 50$. Variation in compression rate can be performed just by changing the values of this quality matrix. Performance of the proposed joint watermarking and compression algorithm is evaluated by varying watermark size, DCT block size, and compression rate in terms of Q -factor. Size of the DCT block is selected in such a manner that each block will embed one pixel value of the watermark.

Figure 5 shows the watermarked image obtained at different Q factors. Image watermark along with the extracted watermarks obtained at varying Q factors is shown in Fig. 6. Further, performance of the algorithm is examined by variation in size of watermark and block size. In this process, the cover image is divided into blocks. This variation is very useful because it provides the information about the efficient watermark size and its corresponding block size. Figures 7 and 8 show the watermarked images and the subsequent extracted watermarks for the block size variations of 32×32 , 16×16 and 8×8 .

The performance of the proposed algorithms is examined and represented in Tables 1, 2 and 3. Table 1 shows the performance comparison of watermarking carried out after DCT block operation and after quantization operations in terms of PSNR, correlation (robustness) and compression ratios at a Q -factor of 50. Referring this table it is established that the PSNR values between cover and watermarked image is obtained for the two proposed schemes i.e. watermarking after quantization and watermarking after DCT are 36.24 dB and 36 dB respectively. It is observed that the PSNR performance of the watermarking after quantization





Watermark Size	Block Size	Watermark	Extracted Watermark
16x16	16x16		
32x32	8x8		

Fig. 8 Watermark and extracted watermark at block size 16×16 and 32×32

Table 1 Comparative analysis of after DCT algorithm and after Quantization algorithm

Performance parameters	Watermarking after DCT	Watermarking after quantization	Improvements
PSNR (dB)	35.9	36.4	0.5
Correlation	0.04	1	0.06
Compression ratio	0.83	0.83	0
Execution time (in sec)	1.73	1.71	0.02
Size of compressed image(in kB)	10.5	10.5	0

algorithm is 0.23 dB better than the watermarking after DCT algorithm. It is also observed that the correlation between original and extracted watermark obtained for the two watermarking algorithms are 1 and 0.0383 respectively whereas compression ratio obtained in both methods are same. It is therefore, very much clear that watermarking applied just after DCT block fails as extracted watermark shows unacceptable correlation. The cover image is of size 63.5kB and the compressed image after DCT as well as after quantization technique both are having the same size of 10.5kB. Therefore, all further performance analysis will be done for the watermarking after quantization algorithm. In Table 2, the performance of the algorithm (watermarking after quantization) is examined at different quality factors ranging from 10 to 90. In this variation, it is observed that there is a trade-off between performance parameters (i.e. PSNR and correlation) and the compression ratio. With the increase in quality factor value, the PSNR and correlation are increasing at the cost of decrease in compression rate. Quality factor around 50 is found to be the optimum quality factor for which the achieved PSNR is above 35 dB (benchmark value for imperceptible watermarking) and correlation value is also more than 0.99. However, moderate compression ratio of 0.83 is obtained at $Q = 50$. Table 3 shows the performance of the proposed watermarking algorithm by varying the watermark size. Referring this table, it is observed that the PSNR, correlation and compression ratio are increasing with decreasing size of the watermark and increasing DCT block size, which is calculated using eq. (3). It is noticed that the performance of the proposed algorithm degrades significantly when the calculated DCT block size is smaller than 8×8 . It can be clearly understood from the quantized DCT matrix presented in Fig. 9 which shows that there is only one significant coefficient available for embedding in an 8×8 block. Further, Fig. 10 shows that there is no significant DCT coefficient available in most of the 4×4 DCT blocks. Therefore, it is observed that the block size 2×2 is having worst results both in terms of compression ratio as well as visual quality. Block size 4×4 is having moderate result and block size 8×8 and above show good PSNR value and constant correlation i.e. 0.99. Furthermore, it is observed that for a given cover image size of 256×256 , the maximum watermark size will be of 32×32 in order to have embedding block size of 8×8 . As it can be observed from the dct_quantized matrix that if the block size for embedding each pixel is less

Table 2 Performance of the method at different Q-factor

Quality factor	PSNR of cover image and watermarked image	Correlation between original and extracted watermarks	Compression ratio	Remark for display Quality
Q = 10	34.04	0.87	0.88	Poor
Q = 50	36.23	0.99	0.83	Edges are visible
Q = 80	39.15	0.99	0.66	Smooth
Q = 90	43.07	0.99	0.55	Exactly like original

Table 3 Performance of the proposed method for different size of watermark and block

Watermark size	DCT Block size	PSNR (dB) of Cover image and watermarked image	Correlation between original and extracted watermarks	Compression ratio	Visual Quality
128 × 128	2 × 2	24.37	0.84	0.40	Blocking artifacts are present
64 × 64	4 × 4	24.37	0.85	0.63	Little blurred
32 × 32	8 × 8	36.23	0.99	0.83	Edges are visible
16 × 16	16 × 16	36.04	0.99	0.83	Edges are visible
8 × 8	32 × 32	35.99	0.99	0.83	Edges are visible
4 × 4	64 × 64	35.98	0.99	0.83	Edges are visible

than 8 × 8, there is non-availability of significant coefficients which may result into poor embedding and compression.

From Table 3, it can be clearly observed that when the size of the DCT block is less than 8 × 8, PSNR deteriorates significantly. The reason has been explained with the help of dct_quantized matrix shown in Fig. 9. The performance of the method is also tested for Checkmark attacks presented in Table 4. Referring this Table, it is established that the method is robust against motion blur, Poisson and Speckle attacks and acceptable visual quality of the watermarked image (> = 27 dB) is obtained in each case. It is noticed that the proposed method is not performing well against other various Checkmark attacks. This may be due to the reason that the checkmark attacks are applied on the data which is already been compressed. It is found that PSNR performance is moderate for most of the attacks considered in experiment whereas correlation performance is poor for sharpening, median filtering and Gaussian filtering and moderate for rest of the attacks under consideration which appears to be the only limitation of the presented method. Table 5 represents the comparison between the nearly related earlier existing works and the proposed work. It is observed that the PSNR of the proposed algorithm is much better than the reported techniques in [8, 11]. Further, CPU time of

14 _(1x1)	-	-	15 _(1x9)	-	-0 _(1x256)
-	-	-	-	-	-
-	-	-	-	-	-
-	-	(8x8)	-	-	-
14 _(9x1)	-	-	16 _(9x9)	-	-0 _(9x256)
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	0 _(256x256)

Fig. 9 DCT quantized matrix for 8 × 8 block

$14_{(1 \times 1)}$	-	-	-	$15_{(1 \times 9)}$	$-0_{(1 \times 256)}$
-	-	-	-	-	-
-	-	-	-	-	-
-	(4×4)	-	-	-	-
$14_{(9 \times 1)}$	-	-	-	$16_{(9 \times 9)}$	$-0_{(9 \times 256)}$
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	$0_{(256 \times 256)}$

Fig. 10 DCT quantized matrix for 4x4block

the proposed method is smaller than the method reported in [8]. However, CPU time for [11] scheme is less than the proposed method. It is noticed that the method proposed in [11] was using spatial domain technique where as the proposed scheme is performed in transform domain.

6 Conclusion and future directions

The proposed method presented a fusion of watermarking and image compression technique for fast and secure data transmission applications to address the efficient trade-off between major performance parameters including embedding and compression rates, robustness and embedding alteration against different known signal processing attacks. The geometric attacks can't be applied on the compressed watermarked image as JPEG itself is treated as an attack, so any other attack can't be applied on it except noise. The performance of the proposed technique was extensively evaluated in the form of PSNR, correlation, compression ratio and execution time for different DCT blocks and watermark sizes. Further, experimental results demonstrated that the method was robust against JPEG and some Checkmark attacks with acceptable visual quality of the watermarked image and achieved high compression ratios. The suggested methods of data hiding along with compression techniques can be potentially used

Table 4 Effect of Checkmark attacks

Checkmark attack	PSNR of cover image and watermarked image	Correlation between embedded and extracted watermark
Sharpening	31.24	0.23
Median filtering	27.41	0.02
Gaussian ($M = 0$, $V = 0.01$)	29.48	0.04
Motion blur	30.46	0.71
Poisson	27.55	0.75
Salt & pepper	27.43	0.49
Speckle	27.43	0.79

Table 5 Comparison with other schemes

Parameters	Qureshi and Nair [11]	Maheshwari et al. [8]	Proposed scheme	Observation (s)
PSNR(dB)	33.39	28.91	36.23	PSNR is better as compared to both schemes. CPU time for [11] scheme is less just because it was implemented in spatial domain where as the proposed scheme is performed in transform domain.
CPU time(sec)	0.359	1.98	1.31	

for communication and multimedia applications. In future, we will improve the performance of the proposed method with other important transform domain techniques such as DWT and SVD and fusion of the both. The performance can also be improved by considering the other compression schemes such as SPIHT, EZW and EBCOT in place of JPEG to make this scheme more computationally efficient and robust against various attacks.

References

1. Badshah G, Liew S-C (2016) J M Zain and M Ali, watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. *J Digit Imaging* 29(2):216–225
2. Goudiaa D, Chaumont M, Puech W, Said NH (2011) A joint JPEG2000 compression and watermarking system using a TCQ-based quantization scheme, in: *visual information processing and communication II(VIPC 2011)*, 78820C–78820C
3. Guillemot L and Moureaux J (2006) Indexing lattice vectors in a joint watermarking and compression scheme, vol 2. In: *IEEE Int. Conf. Acoustics, Speech, Signal Processing*, Toulouse, pp 329–332
4. Guo J-M, Liu Y-F (2010) Joint compression/watermarking scheme using majority parity guidance and Halftoning-based block truncation coding. *IEEE Trans Image Process* 19(8):2056–2069
5. Javeed A, Singh AK (2016) Robust and imperceptible image watermarking in DWT-BTC domain. *Int J Electro Sec Digit Foren Inder Sci* 8(1):53–62
6. Lin MH, Chang CC (2004) A novel information hiding scheme based on BTC. In: *Proc Int Conf Computer and Information Technology*, Wuhan, pp 66–71
7. Lin SD, Shie S-C, Guo JY (2010) Improving the robustness of DCT-based image watermarking against JPEG compression. *J Comp Stand Inter* 32(1–2):54–60
8. Maheshwari JP, Kumar M, Mathur Garima, Yadav RP, Kakerda RK (2015) Robust digital image watermarking using DCT based pyramid transform via image compression. In: *Proc of 2015 International Conference on Communications and Signal Processing*, Melmaruvathur, pp 1059–1063
9. Mary SJJ, Christopher CS, Joe SSA (2016) Novel scheme for compressed image authentication using LSB watermarking and EMRC6 encryption. *Circuits Syst* 7(8):1722–1733
10. Pereira S, Voloshynovskiy S, Madueño M, Marchand-Maillet S, Pun T (2001) Second generation benchmarking and application oriented evaluation. *Information hiding workshop III*, Pittsburgh, In, pp 340–353
11. Qureshi S, Nair S (2013) LSB Based Image Watermarking with Hybrid Compression-Encryption Technique. *Advance EngTechnol Series* 6:161–165
12. Singh AK, Kumar B, Singh G, Mohan A (2017) *Medical image watermarking: techniques and applications*, book series on multimedia systems and applications. Springer, USA
13. Singh AK, Kumar B, Dave M, Ghreera SP, Mohan A (2016) *Digital image watermarking: techniques and emerging applications*. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global, USA, pp 246–272.
14. Tian J (2002) Wavelet based reversible watermarking for authentication. In: *Proceedings of SPIE security watermarking multimedia contents IV*. CA, San Jose, pp 679–690
15. Xie L, Arce GR (1998) Joint wavelet compression and authentication watermarking, In *Proceedings of the 5th IEEE International Conference on Image Processing*

16. Zear A, Singh AK, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools and Applications*. <https://doi.org/10.1007/s11042-016-3862-8>
17. Zhou Y (2010) Joint robust watermarking and image compression, *IEEE International Workshop on Information Forensics and Security*, 12-15 Dec
18. Zhou Y and Yang E-H (2009) Joint robust watermarking and compression using variable-rate scalar quantization in proc. of The 11th Canadian Workshop on Information Theory, Ottawa, Canada, May



Rohini Srivastava received her M Tech Degree from the department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad Uttar Pradesh, India in 2016. She has completed her B Tech degree in Electronics Engineering from Institute of Engineering & Rural Technology (IERT), Allahabad, Uttar Pradesh, India in 2011. Her main research interests include digital image processing, watermarking and image compression.



Dr. Basant Kumar is currently working as Assistant Professor in Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad. He has more than 13 years of teaching and research experience. He obtained his B.Tech. degree in Electronics and Instrumentation Engineering from Bundelkhand Institute of Engineering and Technology, Jhansi, Uttar Pradesh, and M.E. degree in Communication Engineering from Birla Institute of Technology and Science, Pilani, in 1999 and 2002 respectively. He received Ph.D. in Electronics Engineering from Indian Institute of Technology, Banaras Hindu University, Varanasi, India (IIT-BHU) in 2011. His area of research includes telemedicine, data compression, data hiding, multimedia communication and medical image processing. He has published more than 30 research papers in reputed international journals/conferences.



Dr. Amit Kumar Singh is currently working as Assistant Professor in the Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT) Wahnaghat, Solan, Himachal Pradesh-India since April 2008. He has completed his PhD 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 Wahnaghat, 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 50 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 & Cryptography.



Prof. Anand Mohan is a Professor of Electronics Engineering at Indian Institute of Technology (IIT), Banaras Hindu University where he has held as several important administrative positions namely Member of Executive Council, Head of the Department of Electronics Engineering, Coordinator, Centre for Research in Microprocessor Applications (established by MHRD), and In charge, University Science Instrumentation Centre. Prof. Mohan has 35 years rich experience of serving both academia and industry in various capacities. Prof. Mohan obtained Ph.D., PG, and UG degrees in Electronics Engineering from Banaras Hindu University in 1994, 1977, and 1973 respectively. He has made notable contributions to the academic and research development in Electronics Engineering at Banaras Hindu University by creating dedicated research groups of eminent academic experts from the country and abroad. He conducted high quality research in the emerging areas like *fault tolerant/ survivable system design*, *information security*, and *embedded systems*.