Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-07971-w

Image tamper detection and self-recovery using multiple median watermarking

Vishal Rajput [1] · Irshad Ahmad Ansari [1]

Received: 5 January 2019 / Revised: 16 May 2019 / Accepted: 10 July 2019
Published online: 31 July 2019

Abstract
Photographs play a very crucial role in our lives, be it in the field of forensic investigation, military intelligence, scientific research, and publications. Nowadays, most of these photographs are in the digital format; which can be easily edited in any photo editing software without requiring any special knowledge of the field. It has become quite hard to identify whether an image is real or fake. This can be very crucial in the cases of forensic investigation or authorization of images. So, we need a solution, which not only identifies the attacks from different schemes like collage attack, crop attack, etc. but also recovers the edited or tampered portion. In proposed work, 4 reduced-size copy of the original image is hidden in the original image's 4-LSB using four pseudo-random codes. Later on, these copies are used for tamper detection. As image gets tampered, recovery images (which are stored in the 4-LSB's of the original image) also get tampered. So, before recovering the edited portion using the median image (or one out of the four recovery images) various filters like median filters, sharpening filters, and noise removal filters are used to enhance the quality. The proposed scheme recovers the host better than the many recently proposed schemes.

Keywords Tamper detection · Self-recovery · Median watermarking · Image watermarking · Image security

1 Introduction

With the advent of computers, most of the information has been transformed or generated in digital format. Images are no exception to it. It is a well-known fact that digital data is susceptible to cyber-

✉ Irshad Ahmad Ansari
irshad@iiitdmj.ac.in

Vishal Rajput
vishalrajput@iiitdmj.ac.in

[1] Electronics and Communication, PDPM Indian Institute of Information Technology Design and Manufacturing, Jabalpur, M.P, India

attacks or tampering. Tampering of sensitive information can be really harmful, like in cases of criminal activity or military activities. Techniques that can determine the authenticity of the images along with the ownership of the image needs to be developed. Apart from checking the authenticity, a system that can recover the lost data needs to be built. Tampering may not always be the case, digital data can also be lost due to viruses or software malfunctioning, so data should be recovered in those cases too. Images can be subjected to different kinds of attacks like, Collage attack, in which an image is overlaid with another image or by crop attack, in which some part of the image is removed. Other attacks include multi-region and multi-attack tampering. To solve the above-mentioned problems, various watermarking schemes are used. Depending upon the application, digital watermarking can be divided into two main categories namely, Robust watermarking [9, 21] and fragile watermarking [11]. Robust watermarking can resist various attacks including malicious attacks and unintentional modifications like JPEG compression, which makes it the most preferred technique used for copyright protection. On the other hand, a fragile watermarking scheme is susceptible to almost all types of attacks. Fragile watermarking is also divided into two categories: fragile watermarking for tamper localization [7] and fragile watermarking with recovery ability [12, 13]. The former [7] can easily locate the tampered portion but the later [12, 13] has additional functionality of recovering the tampered portion. There is another watermarking technique that is the blend of the fragile watermarking and robust watermarking known as semi-fragile watermarking [16]. This technique combines the advantages of both the watermarking methods. It has robustness against some common signal processing operations along with some sensitivity to different malicious attacks.

2 Related work

Till date, various signature-based image authentication techniques [2, 5, 10, 22, 24] have been developed for integrity verification. Integrity verification in these techniques is done by digital signature. These techniques do not recover the edited portion but only tells whether the image is edited or not. Generally, attaching any digital signature requires additional bandwidth. Above methods store an invisible fragile watermark susceptible to all the editing or tampering in the image. The watermark should be localized in such a way that it is able to detect different types of attacks like VQ (vector quantization) counterfeiting attack [17], CA (collage attack), CAA (constant-average attack) and four-scanning attack [4].

Yang et al. [23] proposed a VQ counterfeiting attack, which attacks block-wise independent watermarking schemes. In some cases, people were able to create the forgery even without the knowledge of added watermark. To prevent VQ attack block-wise dependency should be removed.

Another attack proposed in [23] is called CA (collage attack), which forms an entirely new image made up of several watermarked images by intermixing some portion of every image, without disturbing the spatial location of the image. This attack was capable of tampering any block and producing a forged image with no prior information on the embedding sequence.

In Lin et al. [15] method, a hierarchical digital watermarking is used for tamper detection and recovery. Each block watermark was comprised of 2-bit authentication data and 6-bit recovery data. Tamper localization accuracy is improved by a hierarchical detection algorithm.

The method resists VQ attack easily, and the precision of tamper detection and localization was also quite good after 2nd and 3rd level inspections. However, it was susceptible to attacks like averaging attack and four scanning attacks.

Chang et al. [3] used a technique that blocked various attacks by using intensity-relation check and parity check. Their scheme effectively resisted VQ, collage and averaging attack. Their performance could have been improved by using more than 2 LSB.

In Singh et al. [20], the DCT transform of 2×2 was used as recovery data. For every 2×2 block, the 12-bit watermark was generated out of which two were authentication bits and rest were recovery bits generated from 5 MSB's of the pixel. Recover quality get reduced significantly when the attack was of complex shape. During the tamper detection, it provided many false positives which decreased the recovered image quality.

Sarreshtedari et al. [18] used a source-channel coding technique for self-recovery and image protection. 1 bpp SPIHT compressed code is used as recovery data and watermarking is done by Reed Solomon code. Original source encoded image was retrieved using erasure location detection. However, it failed to do a self-recovery in case of more than n-k erasures in the tampered portion for RS (n, k) code.

Cao et al. [1] proposed a hierarchical recovery capable watermarking scheme. They used the different number of bits for saving the scrambled MSB's. The efficiency of reference bits get increased because of their hierarchical extension ratios of MSB-layer bits, and higher MSB layers of tampered portion have more chance of recovery than the lower MSB layers. Recovered image quality is degraded rapidly when tamper detection was not perfect.

Shehab et al. [19] proposed a method, in which, original image was divided into blocks of size 4×4 and a singular value decomposition (SVD) operation is performed by inserting the little portions of block-wise SVD into the least significant bit of the image pixels to find out the all the transformations that happened in the original image.

Zhang et al. [25] used a technique, which divided the original image into non-overlapping blocks of size 4×4. It classified blocks into two categories namely textured and smooth blocks based on the image's texture. Recovery watermark generation used error correcting codes and homogeneous blocks, which were embedded with the help of mapping to the corresponding smooth block. The information that was generated by the error-correcting codes and homogeneous blocks was embedded into the corresponding texture block and non-embedded smooth block via mapping. Then finally, to identify the tampering status of a sub-block, features of a block were calculated and the corresponding block was used for the watermark based matching of recovery information.

3 Proposed methodology

The proposed methodology is mainly based on the embedding of multiple watermarks into the host, so that the recovery chances can be increased. The algorithm of the proposed method is as follows:

3.1 Algorithm

1) Original image is divided into 4 parts (w, x, y, z).
2) Save a half-sized copy of the original image into another variable.
3) Write binary equivalent of image pixels of step 2 and take out its 4 MSB and form a 256×256 matrix.

4) Use 4 different pseudo-random order of size 256 × 256 to save step three's matrix into the 4 LSB's of w, x, y, and z. Random order is kept constant because it will be used in the extraction process. Image encoding is completed.
5) For the recovering process, 4 LSB's are extracted from the tampered image, 4 images of size 256 × 256 are recovered from these 4 LSB's using the same random order used for encoding.
6) Using 4 recovered images, a median image is formed, which is later used for the recovery process.
7) Median image is passed through filters like sharpening filter and median filter to remove the noise created because of the tampered portion and to increase the quality of the image for a better recovery.
8) To find the tampered region, median image and tampered image are compared and a binary image is formed showing the tampered portion.
9) After creating the binary image, the original tampered image is recovered by using either the median image or any one part (out of the four copies) of watermarked images.
10) Whichever quadrant has the least tampered portion in the binary image of step 9 is used for the final recovery. If all the quadrants have similar tampered amount then the median image is used for recovery (Fig. 1).

4 Results and discussion

The capability of image recovery is generally measured by the quality of the restored image. If the recovered image has better quality, it indicates that the watermarking

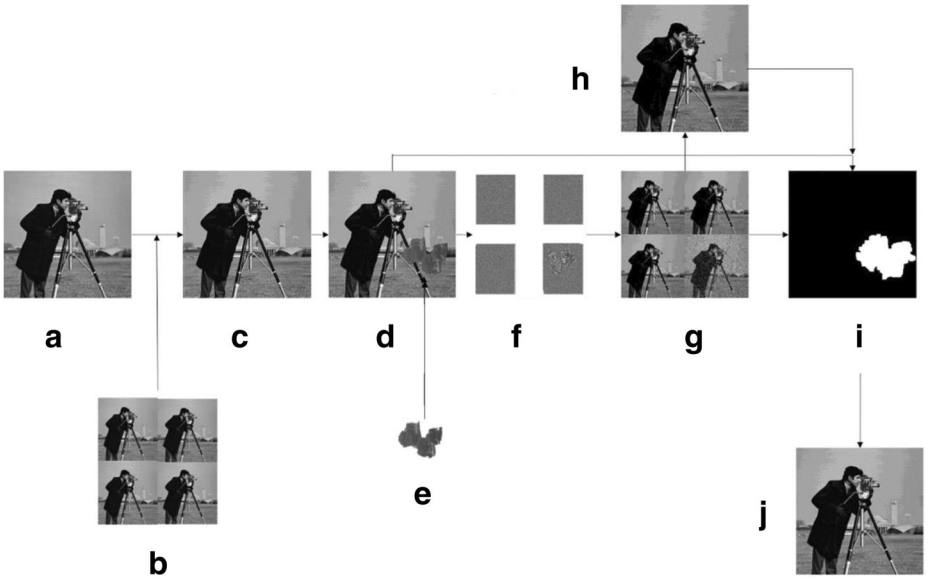

Fig. 1 Flow chart of proposed scheme: (A) original image, (B) 4 resized copy of A, (C) encoded image using 4 random sequences, (D) attacked image, (E) attack portion, (F) tampered image's 4 LSB, (G) 4 recovery images from same random sequence used in C, (H) mean image created from G and resized by 2 times, (I) tamper detection using G,H and D, (J) recovered image from G,H and I

technique has good recovering properties. The peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) index [8] are the most common parameters for evaluation of image recovery. For a P × Q image, PSNR is calculated as:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \tag{1}$$

$$MSE = \frac{\sum_{P,\ Q}[I_1(p,q) - I_2(p,q)]}{P*Q} \tag{2}$$

Where MSE represents the mean square error between the original image I_1 and the processed image I_2.

Although PSNR is the most widely used evaluation parameter, it doesn't consider the human visual system. Sometimes, PSNR is not consistent with human perception. In other words, even a high PSNR image can look worse as compared to low PSNR image. SSIM overcomes the defect of PSNR and provides a better index for the human visual system. SSIM is defined as:

$$\mathrm{SSIM}(a,b) = \left[l(a,b)^{\alpha} \cdot c(a,b)^{\beta} \cdot s(a,b)^{\gamma}\right] \tag{3}$$

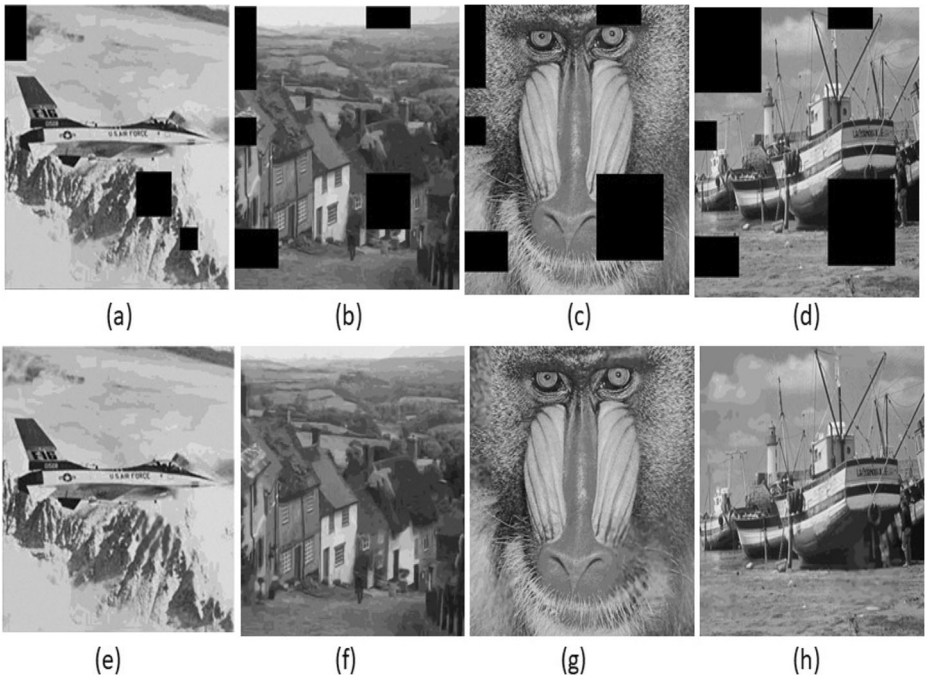

Fig. 2 (**a**) Airplane attacked image (5%), (**b**) Goldhill attacked image (10%), (**c**) Baboon attacked image (15%), (**d**) Sailboat attacked image (20%), (**e**) Airplane recovered image (PSNR 40.31 dB), (**f**) Goldhill recovered image (PSNR 39.19 dB), (**g**) Baboon recovered image (PSNR 27.56 dB), (**h**) Sailboat recovered image (PSNR 34.07 dB)

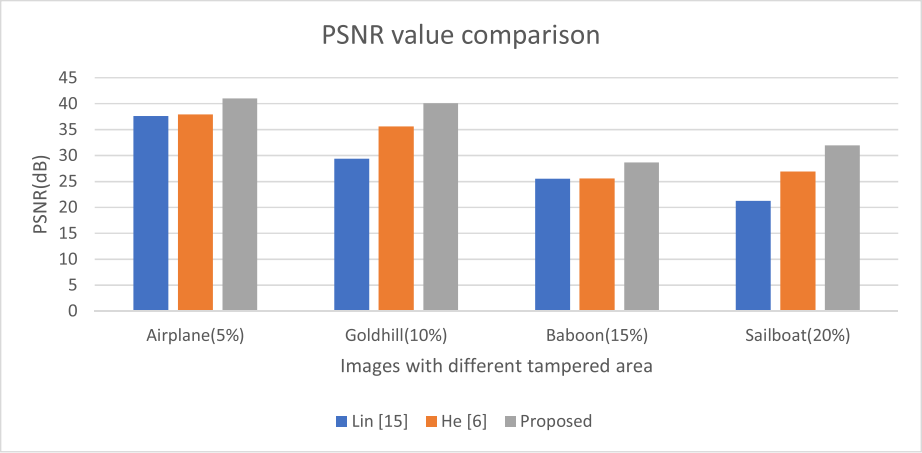

Fig. 3 Multi-region attack PSNR performance comparison of Lin [15], He [6] and proposed with the tampered area of 5%, 10%, 15% and 20% on the respective Airplane, Goldhill, Baboon and Sailboat image

where.

$$l(a,b) = \frac{2\mu_a\mu_b + C_1}{\mu^2{}_a + \mu^2{}_b + C_1}$$

$$c(a,b) = \frac{2\sigma_a\sigma_b + C_2}{\sigma^2{}_a + \sigma^2{}_b + C_2}$$

$$s(a,b) = \frac{\sigma_{ab} + C_3}{\sigma_a\sigma_b + C_3}$$

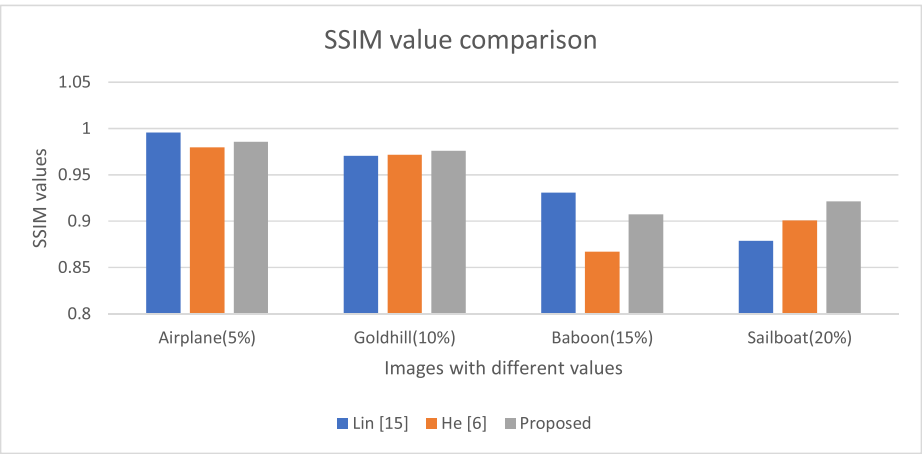

Fig. 4 Multi-region attack SSIM performance comparison of Lin [15], He [6] and proposed with the tampered area of 5%, 10%, 15% and 20% on the respective Airplane, Goldhill, Baboon and Sailboat image

Table 1 PSNR and SSIM values of proposed Scheme on Airplane (5%), Goldhill (10%), Baboon (15%), and Sailboat (20%) images at 10 different attack locations keeping the crop proportion constant along with mean, standard deviation, and variance

IMAGES	AIRPLANE (5% crop)		GOLDHILL (10% crop)		BABOON (15% crop)		SAILBOAT (20% crop)	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM
1	41.46	0.9852	40.28	0.976	27.79	0.8976	34.79	0.9162
2	38.33	0.9866	38.13	0.9725	28.58	0.9069	31.15	0.9068
3	40.69	0.9854	36.85	0.9712	29.67	0.9155	30.55	0.9212
4	42.84	0.9845	37.66	0.9718	29.68	0.9124	33.05	0.9254
5	44.07	0.9862	41.12	0.9787	26.78	0.8929	33.73	0.9155
6	43.03	0.9852	41.56	0.9791	28.87	0.9118	32.04	0.946
7	42.81	0.9877	42.42	0.9799	29.35	0.9151	31.26	0.9159
8	39.27	0.9873	42.35	0.9783	27.46	0.8965	30.84	0.9126
9	39.13	0.9845	40.36	0.9759	28.61	0.9071	30.65	0.9244
10	38.68	0.9855	40.42	0.9776	29.73	0.9163	32.05	0.9283
MEAN	***41.03***	***0.9858***	***40.11***	***0.9761***	***28.65***	***0.9072***	***32.01***	***0.9212***
STD	2.095145	0.001106	1.949759	0.003211	1.025517	0.008651	1.430738	0.010854
VAR	4.389632	0.000001	3.801561	0.000010	1.051684	0.000075	2.047010	0.000118

where μ_a, μ_b, σ_a, σ_b and σ_{ab} are the local means, standard deviations, and cross-covariance for images *a, b*. The average PSNR and SSIM between the original and watermarked images are found to be 33.46 dB and 0.8763 respectively.

4.1 Multi-region attacks

In the Multi-region tampering, an image is attacked at multiple locations with different amount of cropping at each location. In this case, four images are used with the different amount of tampering area (%) namely Airplane (5%), Goldhill (10%), Baboon (15%) and Sailboat (20%) shown in Fig. 2(a, b, c, d) respectively. Different sized blocks are removed from these four images, random cropping locations are selected to check the performance of the proposed scheme against multi-region attacks. Recovered image quality can vary a little bit with the same amount of tampering but at different locations, because the detailing in each part is a little different. Results of this attack have been compared with the Lin [15] and He et al. [6] on two parameters namely SSIM (Structural Similarity), which measures the structural similarity of two images and PSNR (Peak Signal to Noise Ratio), shown in Figs. 3 and 4 respectively. Table 1 shows the performance of multi-region attack on different images. Each image is attacked 10 times keeping the proportion of attack constant but changing the location of attack so that every portion of the image is attacked. This table also shows the mean, standard

Table 2 PSNR and SSIM values of Lin [15], He [6] and Proposed Scheme on Airplane (5%), Goldhill (10%), Baboon (15%), Sailboat (20%) images

Images	Tampered area	Lin [15] (SSIM, PSNR)	He [6] (SSIM, PSNR)	Proposed (SSIM, PSNR)
Airplane	5%	0.9958, 37.60 dB	0.9797, 37.96 dB	0.9858, 40.31 dB
Goldhill	10%	0.9706, 29.38 dB	0.9719, 35.62 dB	0.9761, 37.82 dB
Baboon	15%	0.9306, 25.55 dB	0.8669, 25.60 dB	0.9072, 27.56 dB
Sailboat	20%	0.8788, 21.25 dB	0.9008, 26.93 dB	0.9212, 34.07 dB

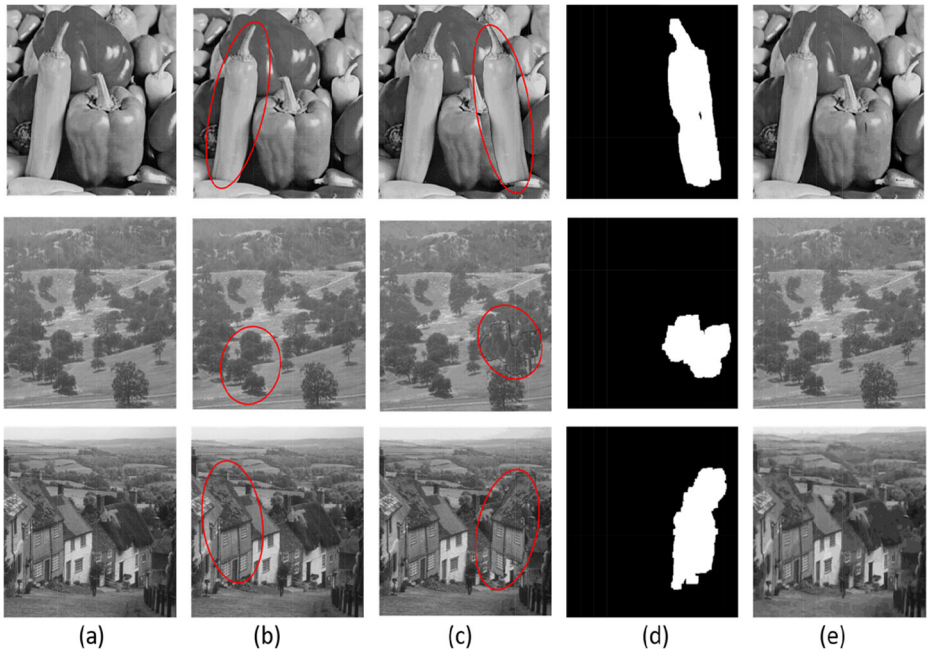

Fig. 5 Peppers, Forest, and Goldhill (**a**) original image, (**b**) red portion used for attacking original images, (**c**) attacked images (red circle: edited portion), (**d**) tamper detection, (**e**) recovered Image (PSNR 33.59 dB, 41.44 dB, and 40.15 dB)

deviation, and variance taken for 10 values. Quantitative result comparison is shown in Table 2.

4.2 Collage attacks

Attack I: This kind of collage attack hampers an image by copying a portion from a watermarked image and pasting it in a random location in the same image. For this attack standard 512 × 512px Peppers, Forest and Goldhill image are used, a portion is cropped from the watermarked images as shown by the red marking in Fig. 5(b) and pasted in the same watermarked image at a different location as shown by the red marking in Fig. 5(c). A quantitative comparison is made with Singh [20] and Chang [3] on Peppers image on the exact same attack. The proposed method led to better results than both of the mentioned technique as shown in Table 3. Tamper detection results for all the images are shown in Fig. 5(d). Proposed method recovered the Peppers, Forest, and Goldhill images with the PSNR of 33.59 dB, 41.44, and 40.15 dB respectively and the recovered images are shown in Fig. 5(e). Chang's [3] method left out some portion while recovering the image whereas Singh's [20]

Table 3 Results of Chang [3], Singh [20] and proposed scheme on collage attack I

Schemes	PSNR (dB)
Chang [3]	25.03
Singh [20]	21.93
Proposed	33.59

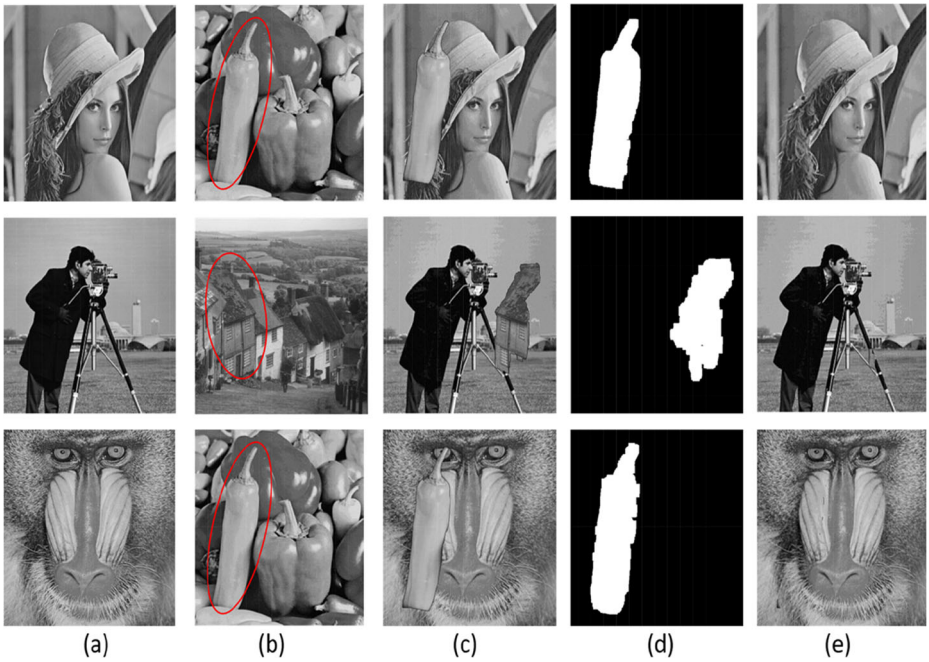

Fig. 6 Lena, Cameraman, and baboon (a) original image, (b) red portion used for attacking original images, (c) attacked images, (d) tamper detection result, (e) recovered Image (PSNR 32.22 dB, 33.60 dB, and 29.82 dB)

method has many false positive blocks spread over the entire image, thus decreasing the recovered image's PSNR.

Attack II: This type of collage attack hampers the watermarked image by combining portion from several authenticated images while maintaining their relative spatial locations [14]. In this attack, a portion from Peppers and Goldhill image is cropped which is shown by the red marking in Fig. 6(b) and pasted on adjacent original images, attacked images are shown in Fig. 6(c). Tamper detection result and recovery results of this attack are shown in Fig. 6(d, e) respectively. Recovered Lena, Cameraman, and Baboon images give the PSNR of 32.22 dB, 33.60 dB, and 29.82 dB respectively. A quantitative comparison is made with Singh [20] and Chang [3] on Baboon image on the exact same attack, the result of Baboon image is shown in Table 4. In this attack also both the mentioned techniques faced the same problem as in the collage attack 1. It is very clear from the results of collage attack 1 and 2, that the proposed scheme easily detects the tampering and recovers the image very well. Result comparison of collage attack 1 and 2 is also shown in Fig. 7.

Table 4 Collage attack II performance of Chang [3], Singh [20] and proposed scheme

Schemes	PSNR (dB)
Chang [3]	23.26
Singh [20]	22.55
Proposed	29.82

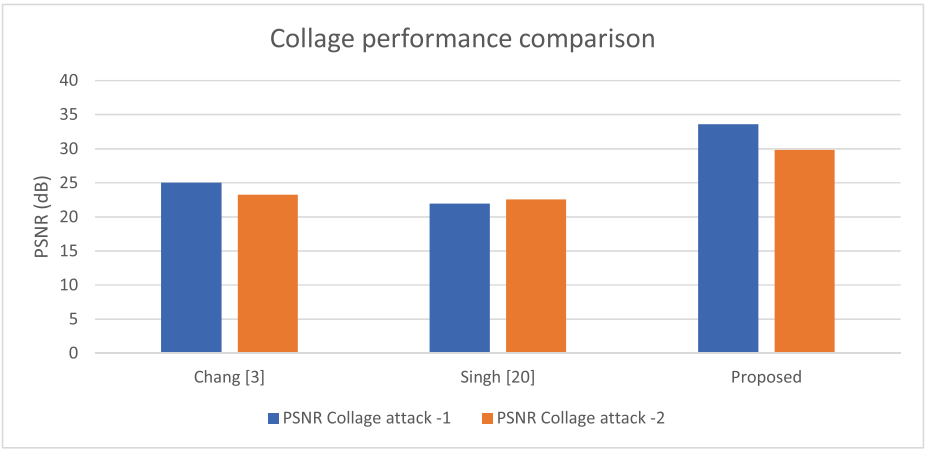

Fig. 7 Chang [3], Singh [20] and the proposed scheme result on the collage attack 1 and 2

Fig. 8 Row 1: Earth, Lena, Sailboat, and Goldhill; Row 2: Cameraman, Forest, Satellite, and Bee

Fig. 9 (**a**) Worst case for crop attack (the attack is distributed to all four quadrants) (**b**) Best case for crop attack (No attack in the 4th quadrant)

Table 5 Proposed scheme performance on Crop attacks in best-worst scenario

Tampered area	PSNR in dB (worst case)	PSNR in dB (best case)
5%	39.56	44.44
10%	36.49	40.65
15%	34.39	38.30
20%	32.63	36.46
25%	30.63	35.10
30%	28.03	33.88
35%	24.60	33.16
40%	39.56	44.44

Table 6 PSNR (dB) values of different images for different tampering area (BEST case)

Tampered area	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%
Earth	49.38	44.44	41.24	38.31	36.39	34.94	33.98	33.21	32.47	31.19
Lena	44.00	40.48	38.55	36.57	34.80	33.84	33.37	32.87	32.54	31.58
Sailboat	43.32	39.98	36.51	34.98	32.84	31.33	30.49	29.66	28.93	28.09
Goldhill	42.49	38.55	36.19	34.56	33.37	32.75	32.22	31.75	31.30	30.54
Cameraman	44.98	41.93	40.17	37.30	36.01	33.52	32.96	32.77	32.53	31.67
Forest	43.73	40.43	38.49	37.34	36.62	35.42	34.78	34.15	33.72	32.51
Satellite	44.46	41.41	39.53	38.75	38.02	36.87	35.49	34.56	33.62	32.09
Bee	43.12	38.01	35.70	33.86	32.76	32.35	32.02	31.76	31.63	30.90

4.3 Crop attacks

In Crop attack, a different sized block from a watermarked image is removed. The proposed scheme performance against crop attack is tested by using various images shown in Fig. 8. Results are divided into two parts worst and best case. The worst case is shown in Fig. 9(a), when the tampering is distributed equally all over the image and the best case is shown in Fig. 9(b), when the tampering is not present in any one of the quadrants (1/4th part of the entire image). Table 5 shows the average performance of crop attack at different tampering levels. It is evident from the quantitative results mentioned in Table 6 and Table 7 that the proposed scheme resists the cropping attack to a very large extent both in the worst and best case. Tables 6 and 7 also tells about the change in performance when the attack is localized to one quadrant as compared to attack distributed to all quadrants. In the worst case scenario, after cropping more than 35% recovered image quality decreases significantly whereas best case can handle attacks up to 75% cropped portion. Cao's [1] result comparison with the proposed

Table 7 PSNR (dB) values of different images for different tampering area (WORST case)

Tampered area	5%	10%	15%	20%	25%	30%	35%
Earth	38.46	35.32	33.47	31.75	29.95	27.54	24.45
Lena	38.99	35.78	33.58	31.78	29.59	27.11	23.77
Sailboat	36.14	33.41	31.80	30.20	28.45	25.97	22.99
Goldhill	39.11	36.10	34.13	32.39	30.67	28.28	25.02
Cameraman	37.55	33.64	31.54	29.64	27.68	25.52	23.05
Forest	41.28	38.56	36.81	35.20	33.17	29.94	25.71
Satellite	42.62	39.19	36.97	35.24	32.89	29.52	24.79
Bee	42.36	39.92	36.77	34.88	32.63	30.35	27.01

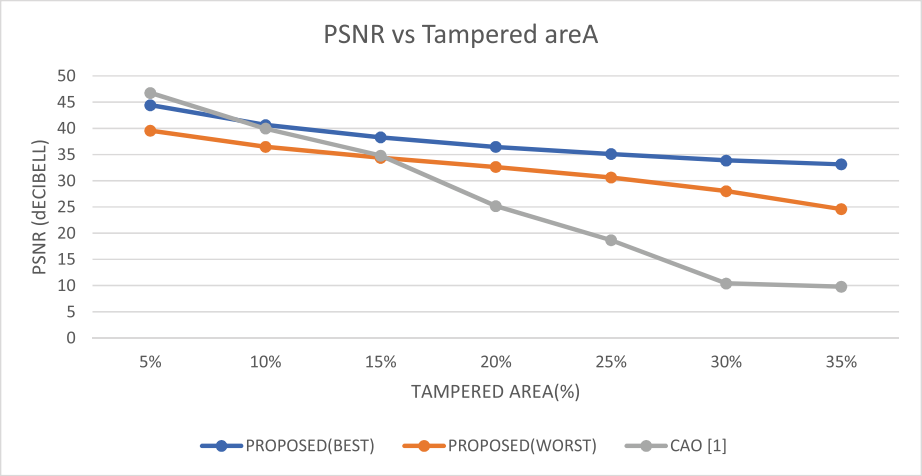

Fig. 10 PSNR vs tampered area graph for crop attack in the best and worst case of the proposed scheme and Cao [1]

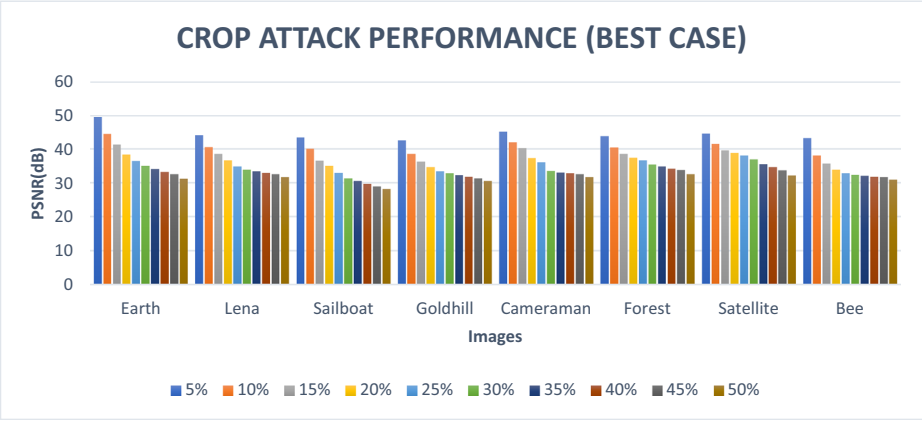

Fig. 11 Best case crop attack performance for different images at crop % of 5,10,15,20,25,30,35,40,45, and 50

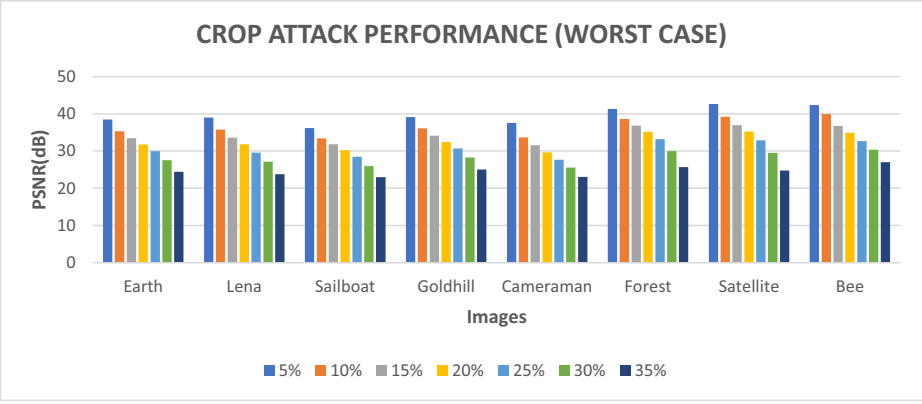

Fig. 12 Worst case crop attack performance for different images at crop % of 5,10,15,20,25,30, and 35

Table 8 Crop attack performance of Singh [20] and Proposed Scheme on Img1 (Lena's) and Img2 (Cameraman)

Tampered area	PSNR (dB) (Singh [20]) Img1	PSNR (dB) (Proposed) Img1	PSNR (dB) (Singh [20]) Img2	PSNR (dB) (Proposed) Img2
5%	43.26	43.7	41.21	41.54
10%	39.57	41.06	37.82	38.6
15%	37.8	38.92	36.23	36.99
20%	36.15	37.38	34.86	35.41
25%	35.31	36.05	33.93	34.03
30%	34.35	35.39	32.9	33.04
35%	33.53	34.01	32.18	31.52

scheme on crop attack for different tampering area (%) is shown in Fig. 10. Analyzing the trend lines of Fig. 10 indicate that Cao's [1] scheme is quite good for the small tamper detection but as soon the tampering amount goes beyond 20% it starts to fall out rapidly whereas the proposed method trend line declines very gradually in both the worst and best case. The proposed method is also compared with the Singh [20] on Lena and Cameraman image on the exact same attack used in Singh's [20] paper. Graphical results of crop attack of all the images for both best and worst case are shown in Figs. 11 and 12. Quantitative result comparison of these two images is shown in Table 8 along with its graphical representation of recovered image quality at different amount of tampering in Figs. 13 and 14. Here cropping is limited to only half of the image because Singh's [20] performance decreases rapidly when image tampering is distributed all over the image. Every image has been tested with different amount of tampering area (%). Sample cropped images, tamper detection and recovery result are shown in Fig. 15 (top row, middle row, last row respectively).

4.4 Time analysis

Proposed algorithm has multiple steps, which take a different amount of time depending upon the type and the size of the attack. For all the testing, a core i7 8GB ram system was used. For

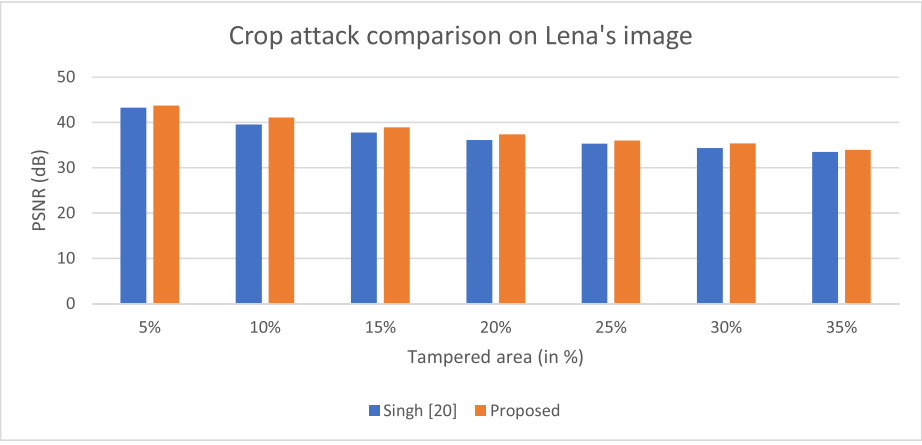

Fig. 13 PSNR vs Tampered area graph of Proposed scheme and Singh [20] in Crop attack on standard 512 × 512 Lena image

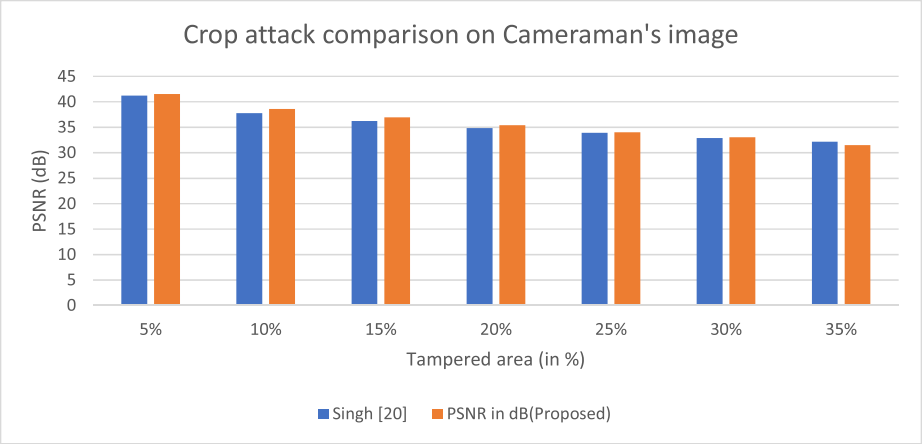

Fig. 14 PSNR vs Tampered area graph of proposed scheme and Singh [20] in Crop attack on standard 512 × 512 cameraman image

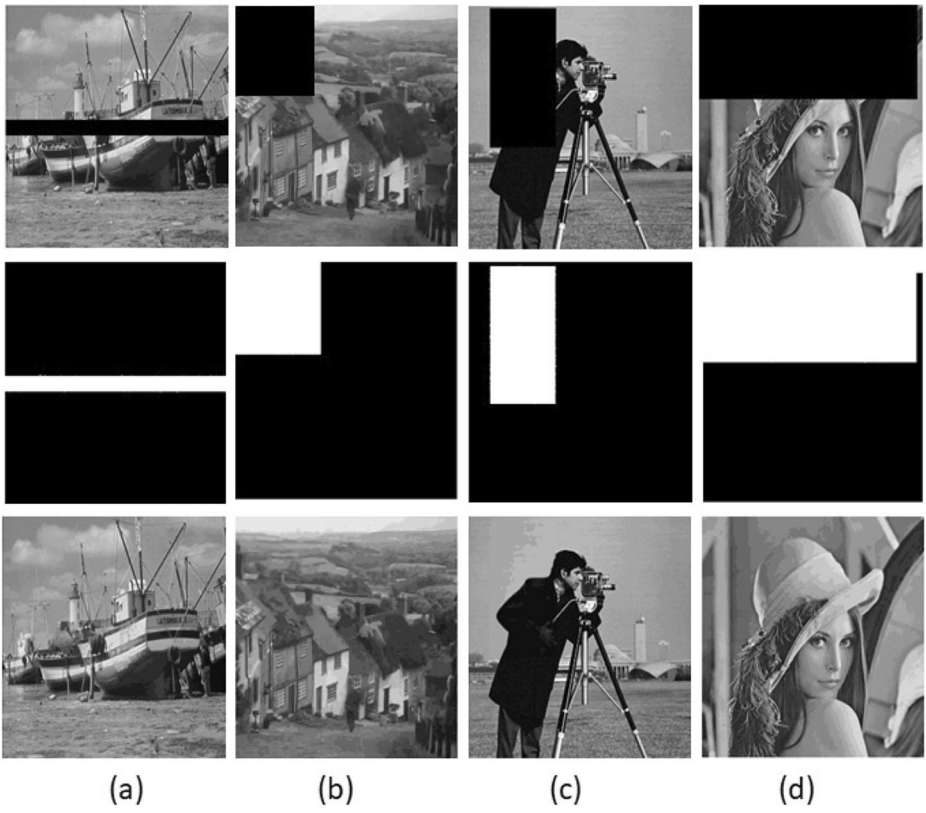

Fig. 15 (a) Sailboat (Attacked image, tamper detection, recovered image), (b) Hill (Attacked image, tamper detection, recovered image), (c) Cameraman (Attacked image, tamper detection, recovered image), (d) Lena (Attacked image, tamper detection, recovered image)

generating the 4 random sequences of size 256×256 (which are used in encoding), it takes about 0.03 s. For the encoding of the image 2.37 s are elapsed. Extracting the watermark out of the attacked image takes about 2.9 s and image recovery (Tamper detection and Image recovery) takes about 0.55 s.

5 Conclusion and future work

From all the results shown here, it is evident that the algorithm presented in this paper works quite effectively against different types of attack mentioned above. Proposed algorithm easily detected the tampered portion and recovered the image with high accuracy. Methods like Chang [3] and Singh [20] struggled to recover the image against collage attack but the proposed method easily recovered the image against such attacks. The proposed method recovered images from a large amount of tampering whereas Cao's [1] method failed completely as soon as tampering reached beyond 25%. In the future, tamper detection precision can be increased and the distributed attack (equal tampering in the entire image) problem can be minimized.

Acknowledgements This work was supported by Faculty Initiation Grant of PDPM Indian Institute of Information Technology Design and Manufacturing Jabalpur, India.

References

1. Cao F, An B, Wang J, Ye D, Wang H (2017) Hierarchical recovery for tampered images based on watermark self-embedding. Displays 46:52–60
2. Celik MU, Sharma G, Saber E, Tekalp AM (2002) Hierarchical watermarking for secure image authentication with localization. IEEE Trans Image Process 11(6):585–595
3. Chang YF, Tai WL (2013) A block-based watermarking scheme for image tamper detection and self-recovery. Opto-Electron Rev 21(2):182–190
4. Chang CC, Fan YH, Tai WL (2008) Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recogn 41(2):654–661
5. Fridrich J (2002) Security of fragile authentication watermarks with localization. In Security and Watermarking of Multimedia Contents IV (Vol. 4675, pp 691–701). International Society for Optics and Photonics
6. He HJ, Zhang JS, Chen F (2009) Adjacent-block based statistical detection method for self-embedding watermarking techniques. Signal Process 89(8):1557–1566
7. He H, Chen F, Tai HM, Kalker T, Zhang J (2012) Performance analysis of a blockneighborhood-based self-recovery fragile watermarking scheme. IEEE Trans Inf Forensics Secur 7(1):185–196
8. Hore A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. In 2010 20th International Conference on Pattern Recognition (pp 2366–2369). IEEE
9. Islam M, Roy A, Laskar RH SVM-based robust image watermarking technique in LWT domain using different sub-bands. Neural Comput Applic 1–25
10. Izquierdo E, Guerra V (2003) An ill-posed operator for secure image authentication. IEEE Trans Circuits Syst Video Technol 13(8):842–852
11. Korus P, Dziech A (2014) Adaptive self-embedding scheme with controlled reconstruction performance. IEEE Trans Inf Forensics Secur 9(2):169–181
12. Kundur D, Hatzinakos D (1999) Digital watermarking for telltale tamper proofing and authentication. Proc IEEE 87(7):1167–1180
13. Lee TY, Lin SD (2008) Dual watermark for image tamper detection and recovery. Pattern Recogn 41(11): 3497–3506
14. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur 10(3):507–518

15. Lin PL, Hsieh CK, Huang PW (2005) A hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recogn 38(12):2519–2529
16. Qi X, Xin X (2015) A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J Vis Commun Image Represent 30:312–327
17. Qian Z, Feng G, Zhang X, Wang S (2011) Image self-embedding with high-quality restoration capability. Digital Signal Process 21(2):278–286
18. Sarreshtedari S, Akhaee MA (2015) A source-channel coding approach to digital image protection and self-recovery. IEEE Trans Image Process 24(7):2266–2277
19. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. IEEE Access 6:10269–10278
20. Singh D, Singh SK (2016) Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. J Vis Commun Image Represent 38:775–789
21. Verma VS, Jha RK, Ojha A (2015) Digital watermark extraction using support vector machine with principal component analysis based feature reduction. J Vis Commun Image Represent 31:75–85
22. Wong PW, Memon N (2001) Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans Image Process 10(10):1593–1601
23. Yang CW, Shen JJ (2010) Recover the tampered image based on VQ indexing. Signal Process 90(1):331–343
24. Yeung MM, Mintzer F (1997) An invisible watermarking technique for image verification. In Image Processing, 1997. Proceedings, International Conference on (Vol. 2, pp 680–683). IEEE
25. Zhang Z, Sun H, Gao S, Jin S (2018) Self-recovery reversible image watermarking algorithm. PLoS One 13(6):e0199143

Vishal Rajput is a final year B. tech student at PDPM Indian Institute of Information and Technology Design and Manufacturing Jabalpur, M.P., India. His major research interest includes Image processing, Machine learning and Artificial Intelligence. He has authored a book chapter on Indian news analysis published by Springer and another paper on character segmentation of handwritten words in DAR 2018. Apart from this he has worked on various image processing and machine learning projects like real time object detection, virtual mouse, etc.

Dr. Irshad Ahmad Ansari is working as an Assistant Professor, in the discipline of Electronics and Communication Engineering at PDPM Indian Institute of Information and Technology Design and Manufacturing Jabalpur, M.P., India. He completed his PhD from IIT Roorkee with MHRD teaching assistantship, and subsequently joined Gwangju Institute of Science and Technology, South Korea as a Postdoctoral fellow. His major research interest includes Image Processing, Signal Processing, Soft Computing, Data Classification, Brain Computer Interface. He has authored more than 15 research papers in various reputed international journals/ conferences of publishers like IEEE, Elsevier, Springer etc. He is also serving as an active and potential technical reviewer for various journals of repute.