Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-018-1158-8

ORIGINAL RESEARCH

An efficient watermarking technique for tamper detection and localization of medical images

Solihah Gull[1] · Nazir A. Loan[1] · Shabir A. Parah[1] · Javaid A. Sheikh[1] · G. M. Bhat[2]

Received: 25 June 2018 / Accepted: 1 December 2018

Abstract

With the exponential rise of multimedia technology and networked infrastructure, electronic healthcare is coming up a big way. One of the most important challenges in an electronic healthcare setup is the authentication of medical images, received by an expert at a far-off location from the sender. With an aim to address the critical authentication issue, this paper presents a fragile watermarking technique capable of tamper detection and localization in medical/general images. We divide the cover image into 4×4 non overlapping pixel blocks; with each block further sub-divided into two 4×2 blocks, called as Upper Half Block (UHB) and Lower Half Block (LHB). The information embedded in LHB facilitates tamper detection while as that embedded in UHB facilities tamper localization. The experimental results show that, in addition to tamper detection and localization capability, the proposed technique has lesser computational complexity when compared to other state-of-art techniques. Further, the proposed scheme results in average PSNR of 51.26 dB for a payload of one bit per pixel (1bpp) indicating that the watermarked images obtained are of high visual quality.

Keywords Watermarking · Tamper detection · Tamper localization · Electronic health record

1 Introduction

Due to abrupt and immense growth in technology, there has been a huge change in the field of healthcare system. Telemedicine has brought the doctors closer to the patients especially in rural areas. It has helped the doctors to be readily available for the patients at any time, which helps in maintaining the regimens of medication. It has solved the problem of keeping the hand written prescriptions safe because the data can now be stored electronically as Electronic Patient Record (EPR). The conventional paper based system of maintaining the records of the patient, has been replaced by upholding these records in digital form. This data includes medical images, health record information which needs to be transferred over the internet. The sensitive nature of such data demands advanced security as there is a huge risk of data being counterfeited intentionally or unintentionally (Aljuaid et al. 2018). Further, the use of intentional/un-intentional attacks on such a sensitive data necessitates content authentication, at the receiver; when this type of data is transmitted over insecure channels. EPR comprises of medical imagery, prescriptions, patient history etc. It is usually transferred to the medical expert siting at other corner of globe in a typical e-health scenario, to have better diagnosis and hence better advice is provided to a patient (Parah et al. 2017a; Loan et al. 2017). Medical imagery forms a major part of EPR, and as such, authentication is of greater importance in case of medical images (Parah et al. 2017a, b, 2018; Singh et al. 2017). This is because even a smallest change in medical image may lead to wrong diagnosis (Khamlichi et al. 2006). In such situation, we need to know whether the digital data is tampered during transit. Many technologies, like digital

✉ Shabir A. Parah
Shabireltr@gmail.com

Solihah Gull
solihahgull@gmail.com

Nazir A. Loan
nazirloan786@gmail.com

Javaid A. Sheikh
sjavaid_29@yahoo.co.in

G. M. Bhat
drgmbhat@gmail.com

[1] Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

[2] Department of Electronics Engineering, Institute of Technology, Zakoora, Srinagar, India

Published online: 12 December 2018

signatures, hashing, fingerprinting, and data hiding have been used for content authentication (Almazrooie et al. 2018; Gutub et al. 2017; Gutub 2010; Marie et al. 2010). However, information hiding has been found to be a best way out to authenticate digital images (Gutub and Aljuaid 2018; Qi and Xin 2015). This is achieved by embedding a very small sized logo, also called as watermark into the cover medium which has to be authenticated. The process of embedding a watermark into a digital cover medium like image, video etc. is called watermarking (Singh and Singh 2016a, b; Singh et al. 2016; Thakur et al. 2018). Watermarking is categorized to into three major type's viz. robust, semi-fragile and fragile watermarking. Robust watermarking can resist both intentional as well as unintentional attacks and is mostly used for ownership identification (Singh 2017; Chauhan et al. 2017), the other one i.e. semi-fragile watermarking can only resist the unintentional attacks or modifications (Zear et al. 2016). The last one, fragile watermarking does not resist any of the attacks and is mostly used for content authentication (Singh and Singh 2016a, b; Ansari et al. 2015; Tong et al. 2013; Caragata et al. 2015). Watermarking is usually carried out either in spatial domain or in frequency domain. Frequency domain embedding is also referred to as transform domain embedding. The main advantage of transform domain embedding is its high degree of robustness to signal processing and geometric attacks. The disadvantage of the transform domain embedding is its higher computational overhead. Some of the commonly used transform domain embedding systems are based on discrete fourier transform (DFT), discrete cosine transform (DCT) and discrete wavelet transform (DWT) etc. (Nguyen et al. 2016; Singh et al. 2018; Parah et al. 2016). Spatial domain embedding, is computationally efficient but less robust in nature. Some of the commonly used spatial domain embedding techniques are least significant bit (LSB) substitution and pixel value differencing (PVD) etc. (Lo and Hu 2014). Sreenivas and Prasad (2018) have given a review of various fragile watermarking techniques that gives an insight for development of spatial domain watermarking techniques. Authors have given a comparison of many fragile watermarking approaches along with cons and pros. Many techniques are able to detect tamper but a large block size results in declaration of whole block as tampered, although a small portion is actually tampered. Some other techniques are able to detect, localize and recover the tampered region along with the drawback of being computationally less efficient is presented in the said review paper. The technique presented in this paper uses spatial domain embedding. It has been found capable of tamper detection and localization, while providing good fidelity and less computational complexity.

The main contributions of this work are:

1. Less computational complexity as the scheme has been implemented in spatial domain.
2. Capability of detecting tamper caused due to any signal processing and/or geometric attack.
3. Capability to localize tamper at resolution of 4 × 4 pixel block.
4. Ability to handle high payload, while maintaining tamper detection and localization characteristics.

2 Related work

A detailed literature reveals that a good amount of work has been carried out in the area of medical image watermarking. The work reported in open literature involves integrity check, copy protection, copyright protection and data hiding in medical images. In this section we provide a brief literature review about the watermarking techniques for medical images with a focus on integrity and authentication of medical images. Khamlichi et al. (2006) have proposed a watermarking technique in which authenticity and integrity of medical image is ensured. They embedded the encrypted data in LSB bit plane which consists of EPR and Digest. At the receiving end after decryption, the digest so obtained is compared with the original digest that is encrypted in the medical image. The similarity coefficient shows the integrity of the image. Qasim et al. (2018) have presented a survey of various state-of-art techniques for development of trust in medical image transmission. The flaws of various approaches in medical image watermarking have been presented. The authors have concluded, for proper and accurate diagnosis it not only peak signal to noise ratio (PSNR) and structural similarity index matrix (SSIM) that matters but the validation given by the experts is also necessary. Another technique, has been presented by (Qi and Xin 2015), wherein they modify a single approximation coefficient of each non-overlapping block, such that it becomes robust to unintentional attacks and fragile to intentional attacks. Embedding capacity of this approach is less. Ansari et al. (2015) reported a technique using fragile watermarking for localization and recovery of digital images. The image is divided into 4 × 4 blocks and singular value decomposition (SVD) is carried out on each block. The codes for both tamper detection as well as self-recovery are inserted in 2 LSB's of each block in the original image. The scheme provides about 99.5% success rate of detection and reports a recovery rate of 50% for tamper localization. Tong et al. (2013) have proposed a scheme using cross chaotic map in which embedding is done in sister block that helps in improving the recovery of the tampered region even if the tampered region is large. An effective fragile watermarking technique has been proposed by (Nguyen et al. 2016). A randomly generated authentication code has been embedded in 2nd DWT sub band having low frequency. The algorithm has been tested for medical images and military images. Lo and Hu (2014) proposed a reversible scheme for image authentication. The authors have generated the authentication codes using random number seed. The generated codes are embedded in residual values of each block for which histogram shifting process has been used. This technique is feasible for tamper detection of medical images, remote sensing images and military images. Azeroual and Afdel (2017) have proposed a fragile watermarking scheme for detecting the tampered region and at the same time localizing the said region in real time. The authors use faber-schauder discrete wavelet transform (FSDWT) for watermark generation and embedding. The time required for embedding the watermark is very less. However, the perceptual quality of the image is not up to the mark. Singh and Singh (2016a, b) have proposed a technique for detection and localization of the region which is tampered. The reported technique has the capability of tamper recovery as well. The authentication bits have been embedded in in three LSB's of each block, while as the recovery bits are embedded into the mapped block. The technique has 50% accuracy for recovery of tampered regions. Zhang et al. (2013) proposed a technique of self-embedding using fragile watermarking. The original image is divided into 2 × 2 blocks and then DCT coefficients of each block are embedded into the block which is mapped to it. This mapping is generated using non-linear chaotic sequence which improves the algorithm security. The scheme helps in both tamper detection as well as recovery of the region that was tampered. Lee and Lin (2008) presented a technique for embedding two watermarks in an image so that if some block of image is tampered, it could be recovered from another block easily. The authors use a secret key along with watermark and recover the image using public chaotic mixing algorithm. However, using dual watermark increases the embedding payload. Also the scheme is not that much secure since it uses linear transform for mapping the blocks. Tiwari et al. (2017) have presented a technique that uses two watermarks one of which is robust; used for verification and other one is Semi-fragile; used for authentication. Patra and Patra (2012) have proposed a self-recovery watermarking scheme for authentication, based on Chinese reminder theorem (CRT). The proposed scheme has been shown to be computationally efficient due to usage of modular arithmetic and is fully able to recover tampered contents effectively. Mohanty et al. (2017) have presented a thorough discussion regarding the various aspects of watermarking. They have given a detailed information of the current trends and applications in watermarking for different areas. Issues like tampering probability have also been discussed. Besides the authors have emphasized the usage of watermarking for security, robustness and run-time complexity. Sengupta (2015) has shown that watermarking can play a significant role for protection of not only software but also hardware designs; from being copied and illegally distributed. With an aim to detect and localize tamper in medical and other general images, which pertain to real time constraints, a computationally efficient fragile watermarking technique based on embedding the watermark bits in UHB and LHB has been presented in this paper. The scheme has been seen, to exhibit various properties that make it an ideal candidate to be used for real time applications like e-healthcare.

3 Proposed technique

The flow diagram of the proposed scheme is presented in Fig. 1a. The complete process of watermark embedding in UHB and LHB has been discussed in section A. The watermark extraction, which informs whether the received image is tampered or not, has been discussed in detail in section B.

3.1 Embedding algorithm

The detailed embedding procedure has been carried out using following steps.

Step 1 Divide the original image I of dimensions M × N into 4 × 4 non overlapping blocks, with each block represented by B_x.

Step 2 Set the LSB and first Intermediate Significant Bit (ISB) of each pixel in every block to zero by performing logical AND operation. The resultant block whose LSBs are set to zero are represented by B_A.

Step 3 Compute arithmetic mean of each block, B_A. In case mean comes out to be a fraction, the value is represented by the next higher integer.

Step 4 Each 4 × 4 block, B_x is divided into two halves, the Upper Half Block (UHB) and the Lower Half Block (LHB) as shown in Fig. 1 (c). The UHB pixels represented by T_{Bn} (where $n = 1$ to 8) are used for embedding data to ensure tamper detection, while as the LHB pixels represented by D_{Bn} (where $n = 1$ to 8) contain the watermark information.

Step 5 Perform the logical XOR operation of the arithmetic mean obtained in step 4 with the watermark pixel, which is an 8 bit sequence (as watermark is a grayscale one).

Step 6 Convert the result obtained in step 5 to equivalent bit stream and embed this bit stream (of eight bits) into LHB (LSBs of each pixel) in the selected 4 × 4 block.

Step 7 Convert the mean value of the block, obtained during step 4, into its equivalent bit stream (of eight bits). Embed this bit-stream into LSB of each UHB pixel to facilitate tamper localization.

3.2 Extraction algorithm

The extraction algorithm has been discussed in detail in this section. Figure 1b shows the flow diagram of logo extraction.

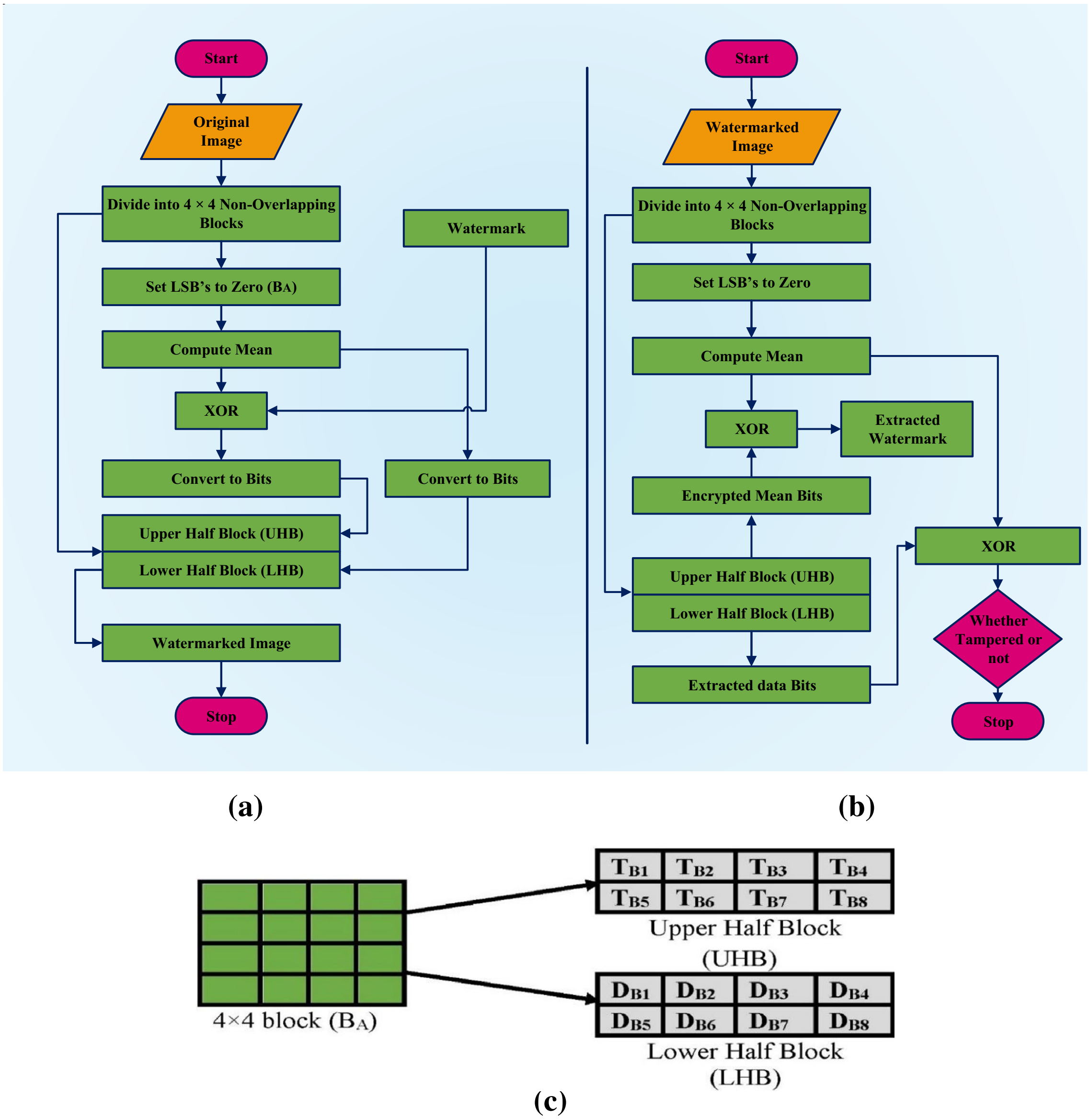


Fig. 1 Flow diagrams: **a** flow diagram for embedding, **b** flow diagram for extraction, and **c** division of blocks

Following steps have to be performed for the extraction of the embedded information.

Step 1 Divide the watermarked image of dimensions M × N into 4 × 4 non overlapping blocks.

Step 2 Set first two LSB's of each block to zero and compute mean of each block.

Step 3 Perform logical XOR operation between the computed mean in step 3 and extract logo data. The resultant information will be the data corresponding to embedded logo.

Step 4 Compare the computed mean with the one extracted from UHB. In case the values match, the block is not tampered otherwise it is a tampered block.

A simple example of the proposed approach is presented in Fig. 2. Figure 2a presents, the procedure of embedding in a single 4 × 4 block while Fig. 2b gives the procedure of extraction from the marked 4 × 4 block when the image has undergone no attack.

4 Experimental results and discussions

Various test images (general images and medical images) have been used to carry out experiments using the proposed algorithm. To verify and validate our work, Nine, generally used test images (grey scale) and 14 medical images of size 256 × 256 have been used. The medical images have

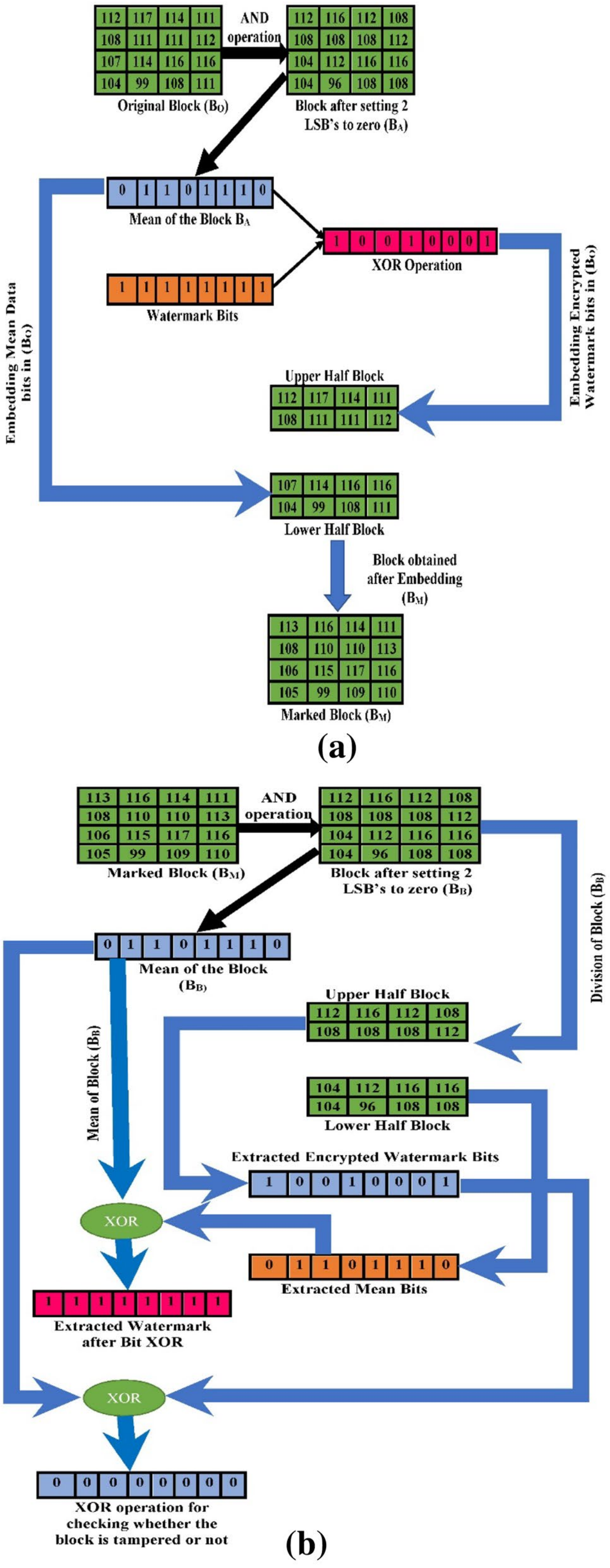


Fig. 2 Example of proposed approach, **a** procedure of embedding, **b** procedure of extraction

been taken from OPENi medical image database. All these test images are shown in Fig. 3 and grey-scale watermark of size 64 × 64 is also shown, which has been embedded in every image. The experimentation was carried out using MATLAB 2017a (version 9.2.0 538062). In order to testify the performance of our scheme we have carried out fidelity, tamper detection, computational complexity and payload analysis. The fidelity analysis has been discussed in section A while as section B presents tamper detection analysis. The sections C, D and E present tamper localization, computational complexity and payload analysis respectively. It is pertinent to mention that we have evaluated our scheme in terms of various objective quality metrics like Peak Signal to Noise ratio (PSNR) [9, 14], Bit Error Rate (BER) and Structural Similarity Index (SSIM).

4.1 Fidelity analysis

The perceptual quality of image and its fidelity is an important factor in data hiding. To compare the perceptual quality of the watermarked image with that of the original image we go for fidelity analysis. Figure 4 shows both the subjective as well as objective quality indices of our scheme. It is clear from average value of PSNR which is 51.26 dB and SSIM of 0.9950, that the proposed scheme has very good fidelity. It is worth mentioning here that the performance of the proposed technique for watermark of different sizes is also evaluated and the objective results so obtained are reported in Table 1. In order to validate our scheme with the state of art we have compared it with various existing methods. The comparison results have been shown in Table 2. These results show that the proposed technique outperforms various state of art techniques.

4.2 Tamper detection analysis

We have subjected the watermarked images to various signal processing and geometric attacks, to analyze the tamper detection ability of our scheme. The results obtained have been presented in Fig. 5. The fact that we are not able to extract a clean watermark after watermarked image is subjected to a particular attack coupled with the high degree of bit error rate are testimony that our scheme is capable of detecting all the signal processing and geometric attacks.

4.3 Tamper localization capability

In addition to above mentioned attacks we have tested the proposed scheme for its ability to localize tamper, if any caused due to attacks. Figure 6 shows the subjective quality of our scheme, when various watermarked images are subjected to attacks like text insertion, copy and paste, and content removal respectively. It could be seen that our

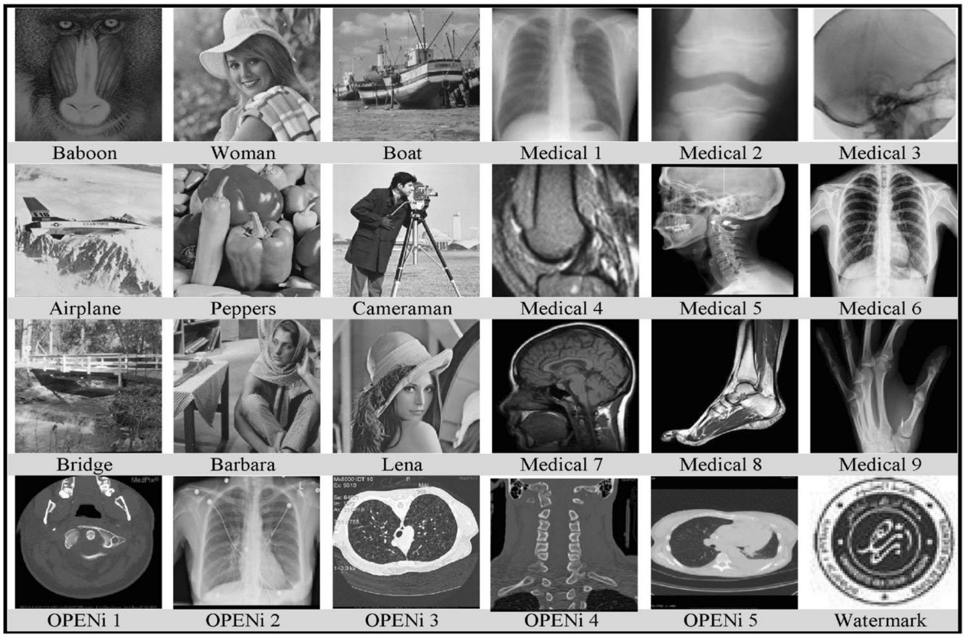
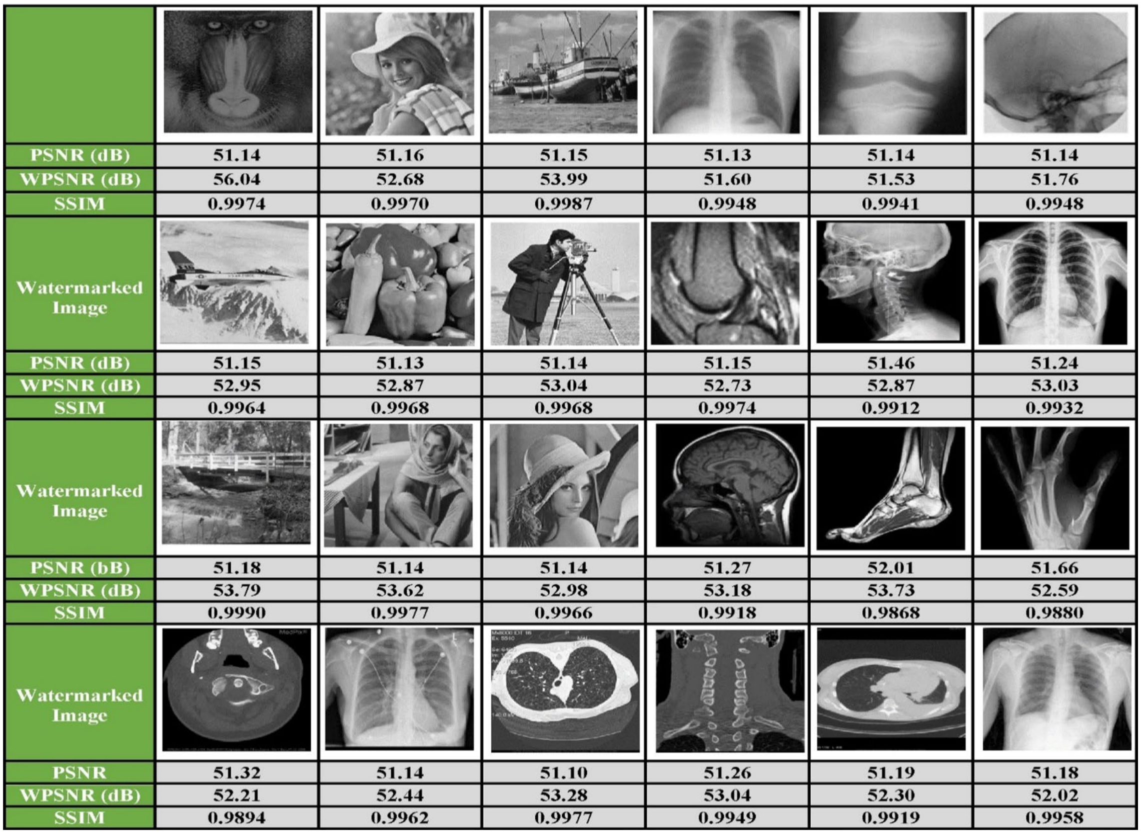


Fig. 3 General and medical test images and watermark



PSNR (dB)	51.14	51.16	51.15	51.13	51.14	51.14
WPSNR (dB)	56.04	52.68	53.99	51.60	51.53	51.76
SSIM	0.9974	0.9970	0.9987	0.9948	0.9941	0.9948
Watermarked Image						
PSNR (dB)	51.15	51.13	51.14	51.15	51.46	51.24
WPSNR (dB)	52.95	52.87	53.04	52.73	52.87	53.03
SSIM	0.9964	0.9968	0.9968	0.9974	0.9912	0.9932
Watermarked Image						
PSNR (bB)	51.18	51.14	51.14	51.27	52.01	51.66
WPSNR (dB)	53.79	53.62	52.98	53.18	53.73	52.59
SSIM	0.9990	0.9977	0.9966	0.9918	0.9868	0.9880
Watermarked Image						
PSNR	51.32	51.14	51.10	51.26	51.19	51.18
WPSNR (dB)	52.21	52.44	53.28	53.04	52.30	52.02
SSIM	0.9894	0.9962	0.9977	0.9949	0.9919	0.9958

Fig. 4 Subjective and objective quality analysis of watermarked images

algorithm is efficient enough to localize even the smallest region that is tampered. It is pertinent to mention that we have used watermarked medical image 1 (Medical 1) and watermarked image "cameraman" for evaluating our scheme to text insertion attack. These images have been modified by addition of the text 'TEXT' in them. This text has been

Table 1 Performance under watermark of different size

Image	PSNR (dB)	SSIM
Watermark of size (32×32)		
Barbara	57.21	0.9994
Lena	57.10	0.9991
Medical 5	57.53	0.9985
Medical 6	57.25	0.9987
Watermark of size (16×16)		
Barbara	66.25	0.9999
Lena	66.21	0.9999
Medical 5	65.80	0.9997
Medical 6	65.78	0.9998
Watermark of size (128×128)		
Barbara	33.08	0.8914
Lena	33.09	0.8584
Medical5	33.51	0.7481
Medical6	33.23	0.8055

added at various locations in the image and the results show that our scheme is successfully able to localize the text that is inserted in the watermarked image. This Figure also shows the performance of proposed scheme under copy and paste attack wherein we have copied a portion of one image into another. It is seen that the algorithm has the ability to detect large as well as small region at any location that is altered because of tampering.

The tamper localization performance of proposed algorithm under content removal attack, wherein we remove some content of the image, has also been shown in Fig. 6. The results show that detection and localization at 4×4 block size is easily possible using our algorithm.

4.4 Computational complexity analysis

Computational complexity is a vital parameter while developing a watermarking algorithm for content authentication. The importance of this parameter is enormous for real time applications such as authentication of medical imagery in an electronic healthcare setup. Spatial domain embedding based on simple LSB substitution, has been used in the proposed technique that makes it suitable to be used for real time applications and reduces its computational overhead. Table 3 shows the comparison of embedding time of the proposed scheme with a similar scheme reported in (Singh and Singh 2016a, b). The results show that the proposed method is about 7 times faster than the already existing scheme (Singh and Singh 2016a, b).

4.5 Payload analysis

Payload also called as embedding capacity has also been calculated so as to check the total number of bits that could be embedded into the cover image. In proposed technique, the cover image is divided into 4×4 blocks and in each block 16 bits (eight bits of watermark and eight bits of mean) are embedded. Therefore, the total number of bits that can be embedded into an image of size 256×256 is equal to 65,536. Hence the true capacity of proposed scheme is one bit per pixel (1bpp). We have compared the payload capability of our scheme with various similar schemes. These results show that the proposed scheme out performs the other state-of-art techniques under comparison. The results are reflected in Table 4.

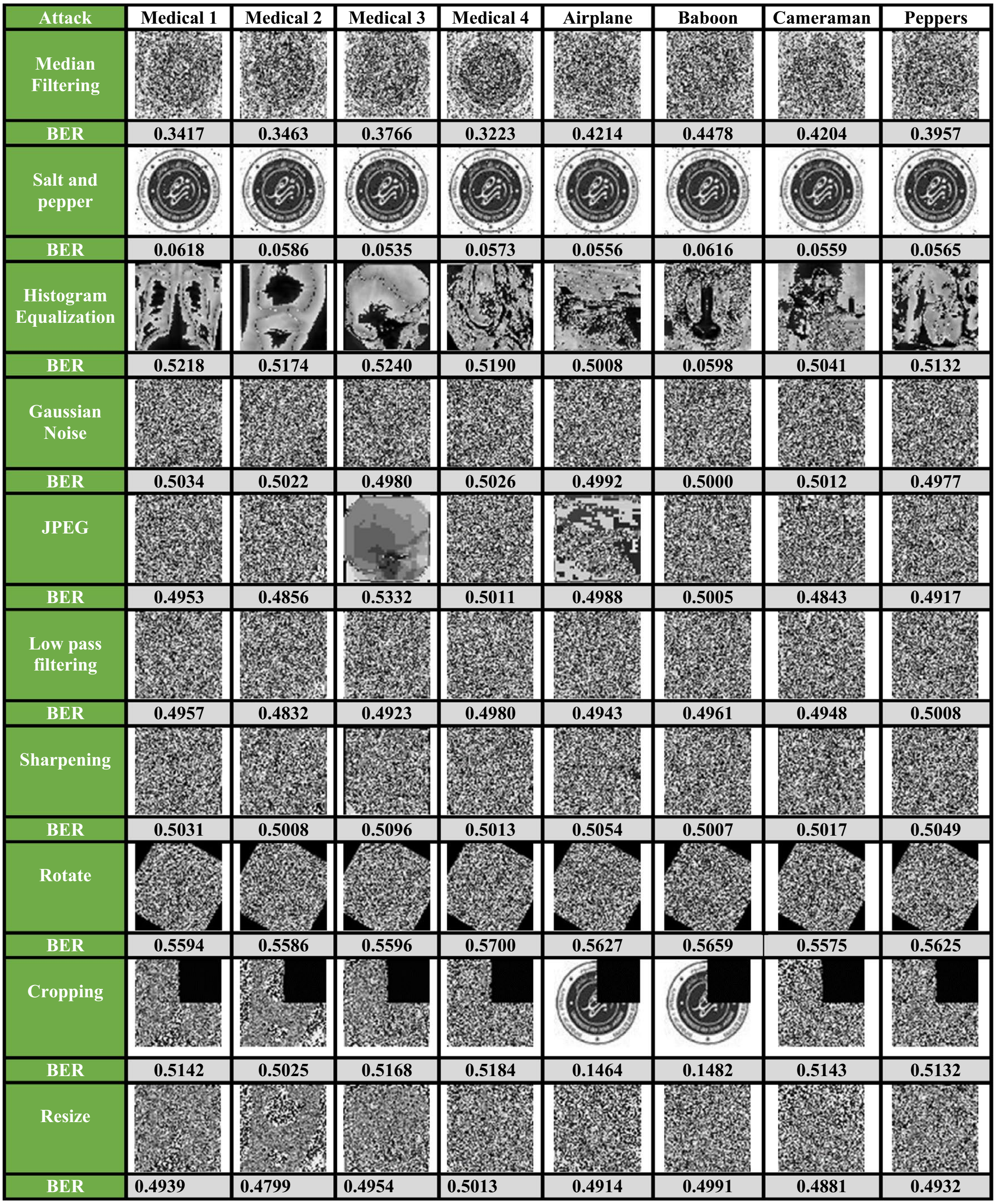
5 Conclusions

A computationally efficient fragile watermarking technique for tamper detection and localization of medical/general images has been proposed in this paper. The cover image has been divided into 4×4 non overlapping pixel blocks; with each block further sub-divided into two 4×2 blocks, called as Upper Pixel Block (UHB) and Lower Pixel Block (LPB). The watermark information and local characteristics of each block have been used to generate two bit streams; one for tamper detection and second one

Table 2 Comparison of PSNR for watermarked images with other methods

Image	PSNR(dB)						
	Patra et. al	Qi and Xin	Ansari et. al	Tong et. al	Singh and Singh	Zhang et.al	Proposed
Baboon	43.15	41.09	44.35	40.71	37.49	44.30	51.14
Lena	43.94	41.76	44.45	40.73	37.59	44.16	51.14
Boats	43.45	–	43.56	40.58	–	44.22	51.15
Peppers	43.94	41.24	44.04	40.32	–	44.28	51.13
Barbara	43.43	–	43.98	40.46	–	44.26	51.15
Airplane	–	41.04	–	40.86	–	–	51.15
Cameraman	–	41.80	–	–	37.17	–	51.14
Average	43.58	41.38	44.07	40.72	37.41	44.24	51.14

– Data not available



Attack	Medical 1	Medical 2	Medical 3	Medical 4	Airplane	Baboon	Cameraman	Peppers
Median Filtering								
BER	0.3417	0.3463	0.3766	0.3223	0.4214	0.4478	0.4204	0.3957
Salt and pepper								
BER	0.0618	0.0586	0.0535	0.0573	0.0556	0.0616	0.0559	0.0565
Histogram Equalization								
BER	0.5218	0.5174	0.5240	0.5190	0.5008	0.0598	0.5041	0.5132
Gaussian Noise								
BER	0.5034	0.5022	0.4980	0.5026	0.4992	0.5000	0.5012	0.4977
JPEG								
BER	0.4953	0.4856	0.5332	0.5011	0.4988	0.5005	0.4843	0.4917
Low pass filtering								
BER	0.4957	0.4832	0.4923	0.4980	0.4943	0.4961	0.4948	0.5008
Sharpening								
BER	0.5031	0.5008	0.5096	0.5013	0.5054	0.5007	0.5017	0.5049
Rotate								
BER	0.5594	0.5586	0.5596	0.5700	0.5627	0.5659	0.5575	0.5625
Cropping								
BER	0.5142	0.5025	0.5168	0.5184	0.1464	0.1482	0.5143	0.5132
Resize								
BER	0.4939	0.4799	0.4954	0.5013	0.4914	0.4991	0.4881	0.4932

Fig. 5 Extracted watermarks and corresponding BER for various attacks

for tamper localization. The two bit streams that are a function of watermark information and block arithmetic mean are embedded in UHB and LHB. The information embedded in in LHB facilitates tamper detection while as that used UHB facilities tamper localization. The experimental investigation reveals that the proposed technique is capable of detecting and localizing tamper caused to the watermarked images during its transit to receiver. This scheme is found to be efficient with an average embedding time of about 0.4570s and average PSNR of 51.26 dB at payload of 65,536 bits. The high image fidelity, lesser computational complexity and better payload make the proposed scheme a better candidate for authenticating the medical imagery for real time applications like e-healthcare. The drawback of the proposed work is that we are

Fig. 6 Tamper detection and localization

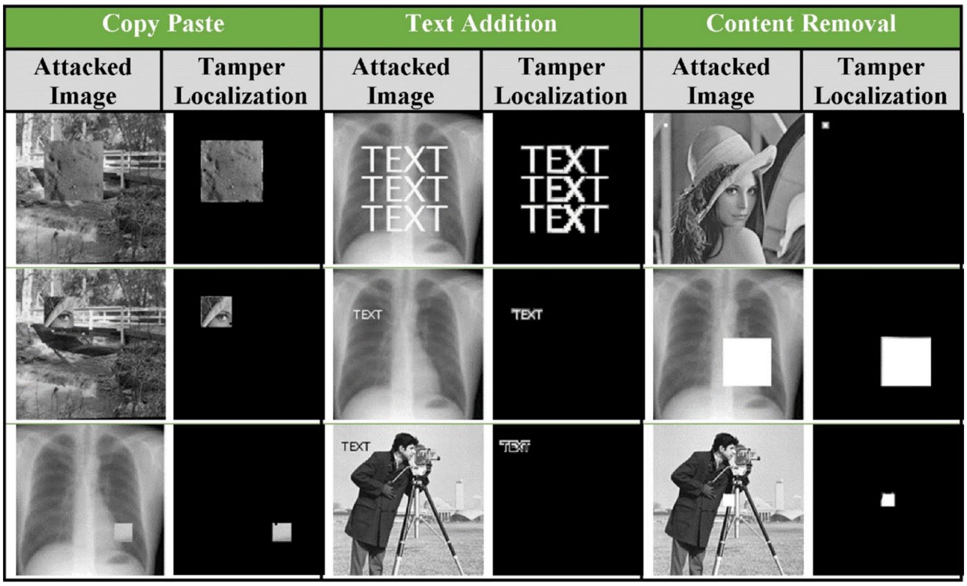


Table 3 Comparison of embedding time (s)

Cover image	Embedding time (s) (Singh and Singh)	Proposed (s)
Lena	6.7548	0.4844
Cameraman	6.8484	0.3906
Baboon	6.9264	0.5000
Woman	6.7860	0.4531

Table 4 Comparison of embedding capacity (bits)

Method	Embedding capacity (bits)
Qi and Xin	8192
Ansari et.al	16,380
Singh and Singh	49,152
Proposed	65,536

only able to detect the tampered region in the image. The future work would focus on correction of detected tampered areas.

Acknowledgements The authors would like to thank the Department of Science and Technology (DST) New Delhi, Government of India for providing financial support under DST Inspire Fellowship Scheme.

References

Aljuaid NA, Gutub AA, Khan EA (2018) Enhancing PC data security via combining RSA cryptography and video based steganography. J Inform Secur Cybercrimes Res (JISCR) 1(1):8–18

Almazrooie M, Samsudin A, Gutub AA, Salleh MS, Omar MA, Hassan SA (2018) Integrity verification for digital Holy Quran verses using cryptographic hash function and compression. J King Saud Univ Comput Inform Sci Elsevier. https://doi.org/10.1016/j.jksuci.2018.02.006

Ansari IA, Pant M, Ahn CW (2015) Svd based fragile watermarking scheme for tamper localization and self-recovery. Int J Mach Learn Cybern 7(6):1225–1239

Azeroual A, Afdel K (2017) Real-time image tamper localisation based on fragile watermarking and Faber-Schauder wavelet. Int J Commun (AEÜ) 79:207–218

Caragata D, Assad SE, Luduena M (2015) An improved fragile watermarking algorithm for jpeg images. Int J Electron Commun 69(12):1783–1794

Chauhan DS, Singh AK, Adarsh A, Kumar B, Saini JP (2017) Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images. Multimedia Tools Appl. https://doi.org/10.1007/s11042-017-5348-8

Gutub AA (2010) Pixel indicator technique for RGB image steganography. J Emerg Technol Web Intell (JETWI) 2(1):56–64

Gutub AA, Aljuaid NA (2018) Multi-bits stego-system for hiding text in multimedia images based on user security priority. J Comput Hardw Eng. https://doi.org/10.63019/jche.v1i2.513

Gutub AA, Aljuaid NA, Khan EA (2017) Counting-based secret sharing technique for multimedia applications. Multimedia Tools Appl Int J Springer. https://doi.org/10.1007/s11042-017-5293-6

Khamlichi YI, Zaz Y, Afdel K (2006) Authentication system for medical watermarked content based image. Wseas Trans Signal Process 5:826–830

Lee TY, Lin SD (2008) Dual watermark for image tamper detection and recovery. Pattern Recogn 41(11):3497–3506

Lo CC, Hu YC (2014) A novel reversible image authentication scheme for digital images. Signal Process 98:174–185

Loan NA, Parah SA, Sheikh JA, Akhoon JA, Bhat GM (2017) Hiding Electronic Patient Record (EPR) in medical images: a high capacity and computationally efficient technique for e-healthcare applications. J Biomed Inform 73:125–136

Marie WA, Gutub AA, Mansou HA (2010) Image based steganography using truth table based and determinate array on RGB indicator. Int J Signal Image Process (IJSIP) 1(3):196–204

Mohanty SP, Sengupta A, Guturu P, Kougianos E (2017) Every you want to know about watermarking from paper marks to hardware protection. IEEE Consum Electron Mag. https://doi.org/10.1109/MCE.2017.2684980

Nguyen TS, Chang CC, Yang XQ (2016) A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. Int J Electron Commun 70(8):1055–1061

Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind Watermarking technique in DCT domain using inter-block coefficient differencing. Digital Signal Process Elsevier, https://doi.org/10.1016/j.dsp.2016.02.005

Parah SA, Ahad F, Sheikh JA, Bhat GM (2017a) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform. https://doi.org/10.1016/j.jbi.2017.01.006

Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM (2017b) Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools Appl 76(8):10599–10633

Parah SA, Sheikh JA, Akhoon JA, Loan NA (2018) Electronic health record hiding in Images for smart city applications: a computationally efficient and reversible information hiding technique for secure communication. Future Gener Comput Syst Elsevier. https://doi.org/10.1016/j.future.2018.02.023

Patra B, Patra JC (2012) Crt-based fragile self-recovery watermarking scheme for image authentication and recovery. In: IEEE international symposium on intelligent signal processing and communication systems, (ISPACS2012), pp. 430–435

Qasim AF, Meziane F, Aspin R (2018) Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. Comput Sci Rev Elsevier 27:45–60

Qi X, Xin X (2015) A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J Visual Commun Image Represent 30:312–327

Sengupta A (2015) Intellectual property cores protection designs for CE products. IEEE Consumer Electron Mag. https://doi.org/10.1109/MCE.2015.2484745

Singh AK (2017) improved hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools Appl Springer 76(6):8881–8900. https://doi.org/10.1007/s11042-016-3514-z US

Singh D, Singh SK (2016a) DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimedia Tools Appl 76(1):953–977

Singh D, Singh SK (2016b) Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. J Visual Commun Image Represent 38:775–789

Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A (2016) Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Gener Comput Syst Elsevier. https://doi.org/10.1016/j.future.2016.11.023

Singh AK, Kumar B, Singh G, Mohan A (2017) Medical image watermarking: techniques and applications, book series on multimedia systems and applications. Springer, USA **(ISBN: 978–3319576985)**

Singh S, Singh R, Singh AK, Siddiqui TJ (2018) SVD-DCT based medical image watermarking in NSCT domain. In: Hassanien AE et al. (eds) Quantum computing: an environment for intelligent large scale real application. Studies in big data, vol 33. Springer, Cham, pp. 467–488. https://doi.org/10.1007/978-3-319-63639-9_20 **(Print ISBN 978-3-319-63638-2)**

Sreenivas K, Prasad VK (2018) Fragile watermarking schemes for image authentication: a survey. Int J Mach Learn Cybern Springer 9(7):1193–1218

Thakur S, Singh AK, Ghrera SP, Mohamed E (2018) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimedia Tools Appl Springer. https://doi.org/10.1007/s11042-018-6263-3

Tiwari A, Sharma M, Tamrakar RK (2017) Watermarking based image authentication and tamper detection algorithm using vector quantization approach. Int J Commun (AEÜ) 78:114–123

Tong X, Liu Y, Zhang M, Chen Y (2013) A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process Image Commun 28(3):301–308

Zear A, Singh A, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools Appl. https://doi.org/10.1007/s11042-016-3862-8

Zhang J, Zhang Q,.Lv H (2013) A novel image tamper localization and recovery algorithm based on watermarking technology. Optik Int J Light Electron Opt 124(23):6367–6371

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.