Multimedia Tools and Applications (2020) 79:21441–21470
https://doi.org/10.1007/s11042-020-08988-2

Embedding in medical images: an efficient scheme for authentication and tamper localization

Nasir N. Hurrah[1] · Shabir A. Parah[1] · Javaid A. Sheikh[1]

Received: 19 May 2019 / Revised: 27 February 2020 / Accepted: 23 April 2020 /
Published online: 6 May 2020

Abstract
In e-healthcare applications integrity of the received information is of prime importance for ensuring the accurate diagnosis. The integrity of electronic medical record (EMR) is possible only when the medical images and other relevant data received are tamper free. Reversibility of medical images after certain degree of processing is always a desired property in medical images as it aids proper diagnosis. This paper proposes a novel reversible image authentication (RIA) scheme for tamper detection and authentication of medical images. In the proposed RIA scheme, the medical image is divided into 4 × 4 blocks followed by embedding fragile watermark bit (for authentication) in each of these blocks. Along with authentication, the localization of tamper is achieved accurately by using LSB embedding along with mean modification approach. The security of the watermark has been enhanced with Arnold cat map, Gray coding and AES-128 encryption. The experimental results show that the scheme offers better fragility against all intentional/unintentional signal processing attacks. The comparison results between proposed RIA scheme and similar state-of-the-art schemes show superiority of our scheme in terms of imperceptivity, fragility and tamper localization. For a payload of 16 kb, the average PSNR achieved for 50 Gray scale images of size 512 × 512 is more than 47 dB. In addition, the scheme offers very less complexity; the embedding and extraction times are around 0.6 s and 0.5 s respectively. Given the features of proposed scheme it could serve as a potential candidate for transfer of EMR in an e-healthcare system.

Keywords E-healthcare · Electronic medical record (EMR) · Security · Reversibility · Watermarking · Tamper detection · Tamper localization

✉ Shabir A. Parah
shabireltr@gmail.com

[1] Department of Electronics and IT, University of Kashmir, Srinagar 190006, India

1 Introduction

The fast growth in communication technology has simplified every domain of life and is making appreciable inroads in various service sectors. As an example, e-healthcare service provides the patients facility to get the diagnosis and treatment of diseases remotely. E-healthcare is steadily replacing conventional patient to doctor physical interaction. However, such systems face challenges with respect to integrity and privacy of the patient information exchanged. From past several years, the healthcare sector has faced several data breaches from the cybercriminals affecting the data of millions of people [9]. The data breaches reported so far throughout the world are in hundreds and have resulted in both loss of privacy as well as millions of dollars [13]. Considering these breaches, for the successful exchange of medical information, the system has to ensure that the received medical data is not tampered by the unauthorized users. The cost and speed factor also needs attention while designing an e-healthcare system so that medical image transmission and embedded patient information does not cause loss instead of gain [1, 12, 25, 26, 32]. Several state-of-the-art techniques have been put forward to tackle security and privacy issues. Of late, data hiding techniques have been used efficiently to ensure the security and authentication of medical data [8]. Data hiding is the the process of embedding secret information in an image using different techniques. Digital watermarking technology, a data hiding technique, offers administrators an efficient choice to meet the security and privacy requirements during the data exchange/storage [17, 18]. Digital watermarking is usually implemented in two domains: spatial domain and frequency domain [15, 21, 27]. The spatial domain-based watermarking techniques involve embedding of watermarking data directly into host cover image without any translation operation performed on the image pixels. Spatial domain schemes offer ease of implementation, low computational complexity and high-quality watermarked image at the cost being less robust to signal processing attacks. In contrast, the frequency domain-based watermarking techniques involves embedding data after performing some transformations on the cover image. However, the payload (embedding capacity) in transform domain is lesser than in spatial one and the complexity is comparatively on the higher end. These transformations may be performed by some transforms including Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Integer Wavelet Transform (IWT) etc., which may be applied alone or in different combinations. The watermarking techniques may also be classified as Fragile, semi fragile or robust. The purpose of fragile watermarking techniques is to accomplish accurate and trustworthy authentication such that a digital image is accepted only if there is no tampering [3, 30]. Robust watermarking schemes in contrast focus on securing the secret information embedded in some cover media. While as fragile watermarking schemes are usually implemented in spatial domain, transform domain techniques are suitable to implement robust watermarking schemes [16]. Reversible data hiding is an approach which ensure that the original cover image is reverted back to pre-embedding form after extraction of embedded information. The reversibility is a desirable factor in medical applications wherein the cover images also contain important diagnostic information.

This work proposes an efficient watermarking algorithm with powerful security mechanism and high tamper detection/localization accuracy. The proposed algorithm also ensures reversibility in a way that the modifications introduced in the cover image are reversed back up to a significant level.

2 Relevant literature

A comprehensive survey of literature shows that many schemes have been used for medical data security and authentication. An SVD based semi-fragile watermarking technique for authentication of digital images is presented in [28]. The watermark is generated by performing a logical operation on content independent sequence obtained using Mersenne Twister algorithm and content dependent sequence obtained using SVD operation on the image blocks. The watermark is embedded in 4 × 4 blocks of approximation sub-bands by employing an adaptive quantization technique. Although the authentication against various tampering attacks is strong, the scheme suffers from complexity issues because of implementation in wavelet domain. Also, there is no provision for tamper localization. A novel digital image authentication framework has been proposed for tamper detection in case of block truncation coding (BTC) compressed images [23]. The authentication code required for tamper detection is obtained using a seed based random number generator. This authentication code is embedded in every block of the BTC compressed cover image using a reference table. For tamper detection at a remote receiver the user is required to have embedded information both in the form of embedded authentication codes and reference table. Here also, there is no provision for tamper localization. For tamper detection and authentication of embedded data in digital images vector quantization approach has been adapted in [33]. Although, the scheme provides good imperceptivity as evident from PSNR value of 42 dB, the authentication, tamper detection and localization results are obtained in a non-blind manner. This requires availability of both the cover image and embedded watermark at the extraction stage. Due to the use of this non-blind approach, the authors have been able to obtain a very low False Positive Rate (FPR) and False Negative Rates (FNR). Reversible watermarking schemes have recently emerged as a strong candidate for ensuring effective services in the applications like e-healthcare, forensics and e-commerce. A reversible watermarking technique is capable to recover the original information data to certain extent from the received watermarked information. As such it is extensively useful to ensure tamper detection, data integrity and ownership right protection [29]. A reversible and fragile watermarking scheme for image authentication in discrete wavelet transform (DWT) domain has been proposed in [24]. The aim of the scheme is complete tamper detection and reversibility while keeping imperceptivity at optimum level. The technique however cannot be used for color images. Further tamper localization is weak and the computational cost factor is high due to its implementation in transform domain. Block based approaches of watermarking have performed well as compared to other schemes due to the flexibility of algorithm to perform different operations without changing much of the original properties of cover media. A hybrid local prediction error based reversible watermarking using difference expansion (DE) has been proposed in [19]. The cover medical image is splitted into, non-overlapping blocks and median edge detection (MED) prediction is used to predict the border pixels in each block. Rest of the pixels in the block are predicted using least square prediction, and the prediction error is expanded. The secret data is embedded into the cover medical image corresponding to the prediction error using the DE method. The predictor is also embedded into the cover medical image to recover the data at detection without any additional information. Although the technique offers good embedding capacity, the imperceptivity is low. A reversible data hiding scheme for medical images which is based on integer-to-integer wavelet transform and histogram-bin-shifting has been presented in [2]. After partitioning the cover image into blocks, entropy is calculated to estimate the smoothness of the blocks. Integer-to-integer wavelet transform is applied over smooth blocks and watermark is embedded in all sub-bands of detail part. Histogram-bin-shifting technique is used to embed the watermark. The scheme achieves reversibility and high imperceptivity at the cost of low payload and high computational complexity. Some other related techniques for authentication and secure transmission of data can be found in [4, 14, 20, 31, 37].

A reliable embedding system has to ensure security of the embedded information in case an adversary cracks the embedding algorithm. To avoid such situations the embedded information is usually encrypted prior to embedding [7, 11]. The watermark should be encrypted using some encryption/encoding technique with highly sensitive keys. There are several state-of-art encryption techniques reported in literature for security of a watermarking system [10, 38]. Some of them aim at transmitting an encrypted image through the network such that an adversary may not be able to decrypt it. The problem with this approach is that a meaningless encrypted data creates doubt in the minds of adversaries regarding the importance of the information content and hence attempts to decipher it increase significantly. A better option is to hide the encrypted data in a simple doubtless image so that it remains safe from any kind tampering. A watermarking scheme based on Independent Component Analysis (ICA) for protection and authentication of digital images could be seen in [35]. The proposed scheme embeds two independent watermarks (encrypted by Arnold transform and an encoding algorithm) in the cover image in order to meet the authentication criteria. Although the scheme provides strong authentication capability, the insertion of two watermarks effects the imperceptivity of the watermarked images. Also, there is no provision for tamper localization and reversibility. In [6] chaotic maps in the form of Arnold and logistic maps have been used to ensure security against various attacks. Arnold encryption is used to scramble the pixel positions of the texture image and the logistic map is used to generate a random sequence of bits. The two sequences are XORed to obtain a secure encrypted watermark to be embedded in the cover image for authentication purposes. The scheme offers very high security to the embedded data but the tamper localization capability is weak. Further there is no provision for reversibility. An improved digital image authentication technique using characteristics of SVD and Arnold encryption for embedding a fragile watermark in a cover image has been proposed in [39]. For tamper detection the binary watermark is extracted from the image and embedded in the LSBs of image pixels after performing block division. At the receiver end the texture image is regenerated from the watermarked image and compared with the extracted decrypted watermark. Although the technique successfully detects the tamper but the localization capability for detecting the nature of tamper is weak. The technique also fails to facilitate the reversibility and the computational cost is high due to implementation in transform domain.

In this work, a novel fragile watermarking algorithm based on block mean modification and LSB embedding has been developed for secure and authentic transmission of the medical information. Key contributions of proposed work are:

i. The authenticity of the information is ensured by embedding a highly fragile watermark (information) in a cover image. The embedding is done in a way such that any minute change in the statistical content of the cover image results in extraction of distorted information with no meaning.

ii. The security is ensured in the proposed scheme using multi-level encryption/encoding techniques. In order to ensure the high security of the content, the watermark information is encrypted using Arnold encryption, AES encryption and Gray encoding. Although the three encryption techniques are simple but their hybrid combination provides an unbreakable level of security.

iii. The proposed scheme is capable of tamper detection and localization. Tamper localization is achieved with block-based approach and as such we easily locate the tampered blocks of the image by storing the localization bit using LSB embedding.

iv. While the authentication and localization bits are stored in a block by pixel manipulation, the reversibility is achieved at the extraction stage by reversing the effect of manipulation on the cover image. The modifications done on the block pixels is reversed by the same factor as done by the embedder to get the image that matches with the original one with high similarity.

The rest of the paper is organised as follows. The Section 3 describes in detail the preliminaries of the proposed scheme. Section 4 describes the embedding and extraction algorithms proposed in this work. The results of comparison with some state of art techniques and other experimental results are shown in Section 5. The paper concludes in section 6.

3 Information security

The security of the user information is one of the most important requirements desired from a data hiding system. For a fragile watermarking framework meant for authentication applications the security of the embedded information becomes even more significant due to possibilities of tampering and other security breaches. In this paper, the security of the user information has been ensured by encrypting and encoding the information using different techniques. Three different encryption techniques used are: Arnold encryption, AES encryption with 128 key space and Gray encoding. Using these techniques and corresponding secret keys the user information is encrypted/encoded before embedding in a cover image.

Arnold transform, like chaos, is a 2D chaotic map for encrypting a 2D matrix like a digital image [5]. Arnold transform is one of the prominent techniques used for encryption in digital watermarking [6, 22, 35]. The unique property of Arnold transform is that it is periodic with the period, t. That means after‘t’ number of iterations the original image is obtained back from the scrambled image. In this way the Arnold transform provides a flexibility to the user to extract back original image if provided with information about number of iterations performed during scrambling. Due to the simplicity of the Arnold cat map, there are chances for the attackers to decipher the information after predicting the iteration count. This can be seen in the Fig. 1, where the watermark is encrypted with ‘t = 55’ iterations and decryption at ‘t = 54’ results in extraction of some visible information. So, there are chances for extracting the information if unauthorized user can perform number of iterations. So, in order to further strengthen the security of the secret information to a level that is unbreakable we need some further technique. This has been achieved in the proposed scheme using AES encryption (with key size of 128) and Gray encoding techniques. The strength of the security provided by the hybrid combination of encryption/encoding is described in Fig. 1. Although the AES algorithm takes too much time for encrypting the gray-scale images, the time for encrypting a binary data is in milliseconds. This approach has been used in the proposed encryption technique to encrypt binary information while keeping complexity at minimum level. Secondly, we have avoided AES-256 and AES-512 due to the same complexity reason.

Gray level encoding is one of the simplest, yet effective techniques that can be used to ensure complete fragility of the watermark even in case of a single bit error. In this paper, the user information is encoded using gray level coding such that the encoded version of the

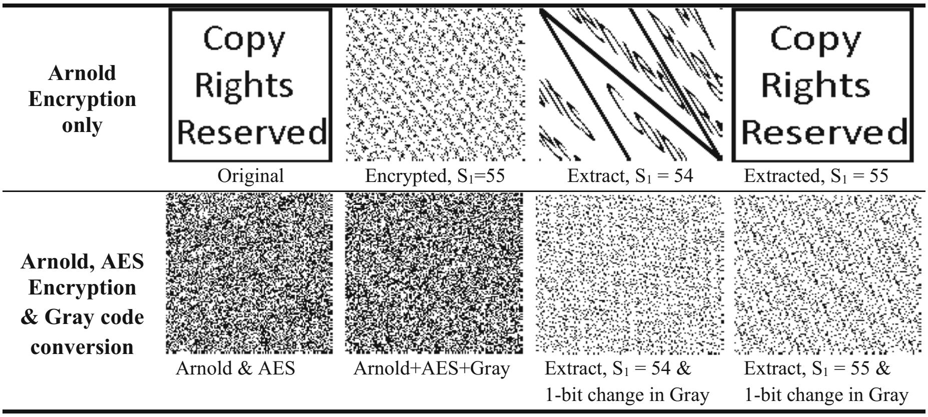


Fig. 1 Original and extracted watermarks of size 128 × 128 after different iterations

information is embedded in the cover image. Since, each of the succeeding bit is dependent on the state of the previous bit, any change in the state of a bit completely changes the state of all the rest of bits. This concept is used in the proposed framework by embedding the gray coded sequence of the information in the cover image.

4 Proposed scheme

In the proposed algorithm, the embedding of the watermark is done using a novel block-based approach which is highly sensitive to any kind of changes keys used for embedding. The proposed scheme is implemented in spatial domain to achieve the highly fragile nature of the watermark for authentication purposes. Before embedding, encryption is performed on the watermark, to make the proposed watermarking technique more secure. The secret encrypted data bits of the watermark are embedded into original pixel values of the image blocks to achieve better fragility against the most of the signal processing attacks. The modified pixels have the least difference with the corresponding original ones such that a strong imperceptivity is achieved. Due to the reason that proposed scheme uses block image processing procedure, it is flexible to adopt any of the image compression standard. The proposed algorithm shows high performance in terms of imperceptibility, security, embedding capacity and fragility. The tamper detection/localization has been achieved by embedding the watermark bits at different locations of the cover image. While embedding the watermark information throughout the image block, the reversibility has also been ensured at the receiver. In section 4.1 and section 4.2, the embedding and extraction processes are discussed in detail.

4.1 Embedding algorithm

In this section, the proposed watermarking algorithm is explained in detail starting with the embedding up to extraction. The proposed technique is aimed to provide better performance in terms of security, imperceptivity and fragility against different attacks. The proposed scheme is blind and watermark is embedded in spatial domain after encrypting it with the Arnold cat map. The generalized flow diagram of the proposed scheme has been shown in Fig. 2. The watermark embedding process takes input in the form of encrypted WM (which generally is a binary logo of size L × L) and a cover image of size M × N. The fragile watermark has been embedded using the following steps:

Step 1: Apply Arnold transform and AES encryption technique to the watermark to get encrypted version, W_e.

Step 2: Divide cover image into p × p blocks, B_x ($x = 1,2,3,\ldots\ M \times N/p \times p$). First select a block from the sequence of all the blocks. If B_i is the current p × p chosen block during ith cycle, randomly select two neighbourhood pixels from all the pixels in a block $B_{i.}$ Among the two pixels one is chosen for watermark embedding and other to store modification factor in LSBs. This pixel is used to recover image after extraction of watermark and its location (r) is selected using secret key 'S_3' as:

$$r = \mathrm{mod}\left\{\left[\frac{(M \times N)-(S_3+p)}{(p \times p)+1}\right], 17\right\} \tag{1}$$

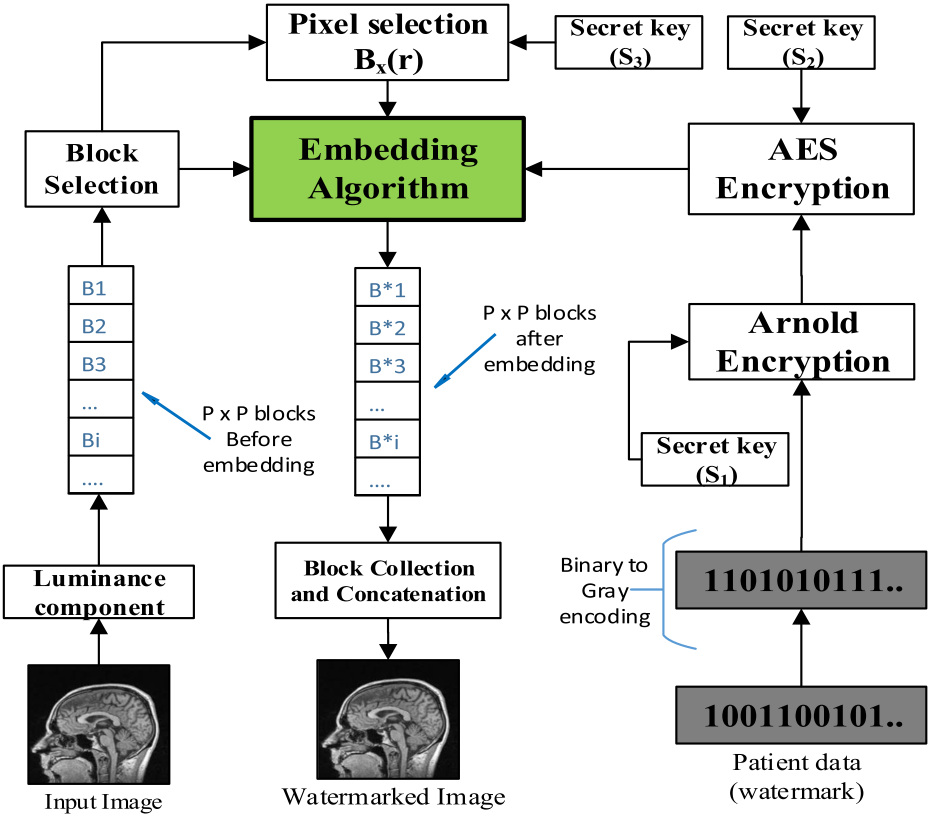


Fig. 2 Block diagram for embedding watermark

A pixel 's' in the neighbourhood of 'r' is selected to store duplicate version of watermark bit for authentication and tamper localization. This pixel is selected as:

$$s = \begin{cases} r{-}1; & if\ r > p \\ r+1; & if\ r < p \end{cases} \tag{2}$$

Step 3: Find the mean (μ) of the block barring the two pre-selected pixels [B_i (r) & B_i (s)]. In order to get a single bit out of the calculated mean we use modulo 2 operation on the calculated mean.

$$\mu_0 = \mu = ceil\left\{\left[\sum_{x=1}^{p}\sum_{y=1}^{p} B_{xy} - B_{xy}(r) - B_{xy}(s)\right] / (p{*}p) - 2\right\} \tag{3}$$

$$M_\mu = mod\ [round(\mu/\zeta_{\mathbf{F}}), 2] \tag{4}$$

Step 4: Embed the watermark bit 'W_a' in the LSB of the pixel 'B_{xy}(s)' as

$$X_{MW} = M_\mu \oplus W_e \tag{5}$$

$$M_s = mod\left(B_{xy}(s), 2\right) \tag{6}$$

$$\psi = M_s - X_{MW} \tag{7}$$

$$B_{xy}(s) = B_{xy}(s) - \psi \tag{8}$$

The symbol "⊕" denotes XOR operation. In order to avoid the pixel modification more than the highest possible intensity value (255 in case of gray scale images), the boundary condition is applied during mean modification by limiting the value to the maximum pixel value of the block.

Step 5: For authentication the watermark bit is stored in the mean of the block by modifying the block pixels with a factor 'Δ'. The calculation of 'Δ' is described in the Fig. 3. In Fig. 3, the for the watermark bit '1' if mean of the block (M_μ) zero, the mean is incremented or decremented by unity till mean of the block becomes 1. Same procedure is carried out when the watermark bit is '0' and M_μ is 1. The value of "β" is computed as

$$\beta = \begin{cases} ceil\left[\max(I) - \frac{\xi_F}{2}\right] & if \max(I) \geq 245 \\ ceil\left[\max(I) + \frac{\xi_F}{2}\right]; & if \max(I) < 240 \end{cases} \tag{9}$$

The value of the embedding factor (ζ_F) is arbitrarily set in the range $1.1 \leq \zeta_F \leq 11.24$ such that for each value of embedding factor less than 11.24 the PSNR is greater than 36 dB.

Step 6: After modifying the mean of the block according to the watermark bit, the modification factor is calculated from the difference of two means as described in Fig. 3.

$$\Delta = \mu' - \mu_0 \tag{10}$$

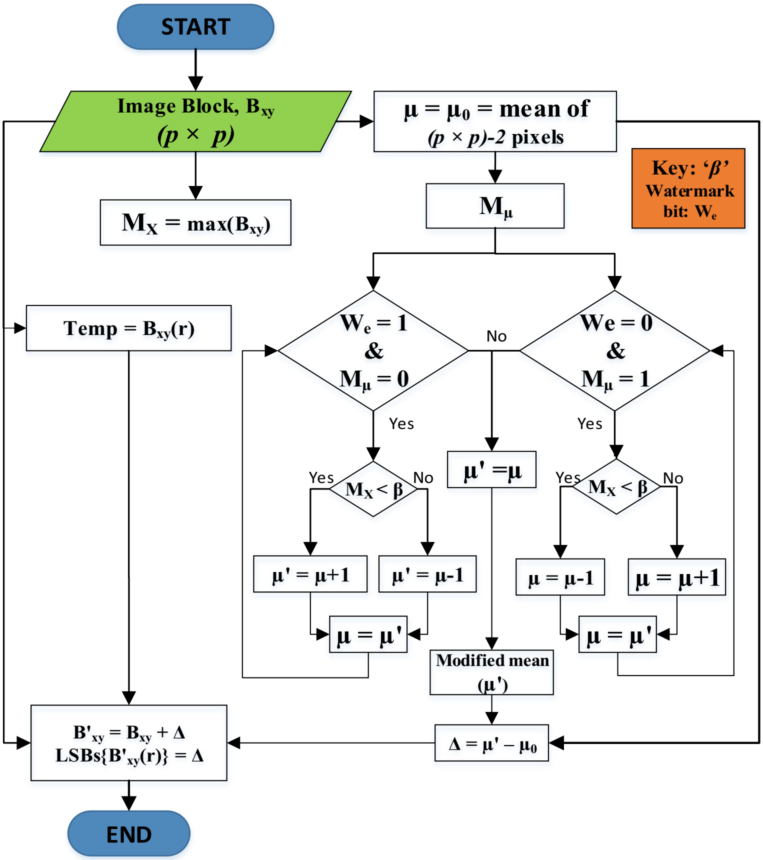


Fig. 3 Watermark embedding flow diagram

Step 7: The watermarked pixel block $\widehat{B}_{\mathrm{xy}}$ is computed as:

$$\widehat{B}_{xy} = B_{xy} - \Delta \tag{11}$$

Step 8: To ensure the reversibility of the original image after extraction of the watermark information, the LSB bits of the barred pixel [$B_{xy}(r)$] in the block are used to store the value of modification factor after embedding process is complete. These bits are used to recover the modification factor and thereby subtract from all the pixels of the block to recover the original image block.

4.2 Watermark extraction and original image recovery

The extraction process starts with watermarked image which may be first processed for necessary extraction of image components in which watermark is embedded. The extraction process used in fragile watermarking is inverse of corresponding embedding process. After doing some necessary pre-processing of the watermarked image the resulting watermark logo is obtained from the image in spatial domain. For an arbitrary block B'$_{\mathrm{xy}}$ (say first block) with dimension's p × p the watermark bit is extracted as per Fig. 4.

Step 1: Divide the watermarked image (luminance component in case of color image) into the $p \times p$ blocks. Randomly select one of the blocks (B'$_{\mathrm{xy}}$) after shuffling for extraction of watermark information.

Step 2: Select the recovery pixel (at location ‘r’) from the block using Eq. 1.

Step 3: Calculate the mean ($\widehat{\mu}$) of each block using Eq. 3.

Step 4: Apply modulus operation to obtain the watermark bit as

$$\widehat{M}_{\mu} = W_{xi} = mod\left[round\left(\widehat{\mu}/\zeta_{\mathbf{F}}\right), 2\right] \tag{12}$$

Step 5: Extract the LSB bits of the barred pixel at location (r) in the block to recover the modification factor. Obtain the modification factor (Δ) from the LSB bits of the pixel, B'$_{\mathrm{xy}}$(r). The extracted modification factor is added to all the block pixels to ensure reversibility and recover the original image block.

$$B_{xy} = \widehat{B}_{xy} + \Delta \tag{13}$$

Step 6: Obtain the authentication bit as

$$\widehat{M}_s = mod\left(\widehat{B}_{xy}(s), 2\right) \tag{14}$$

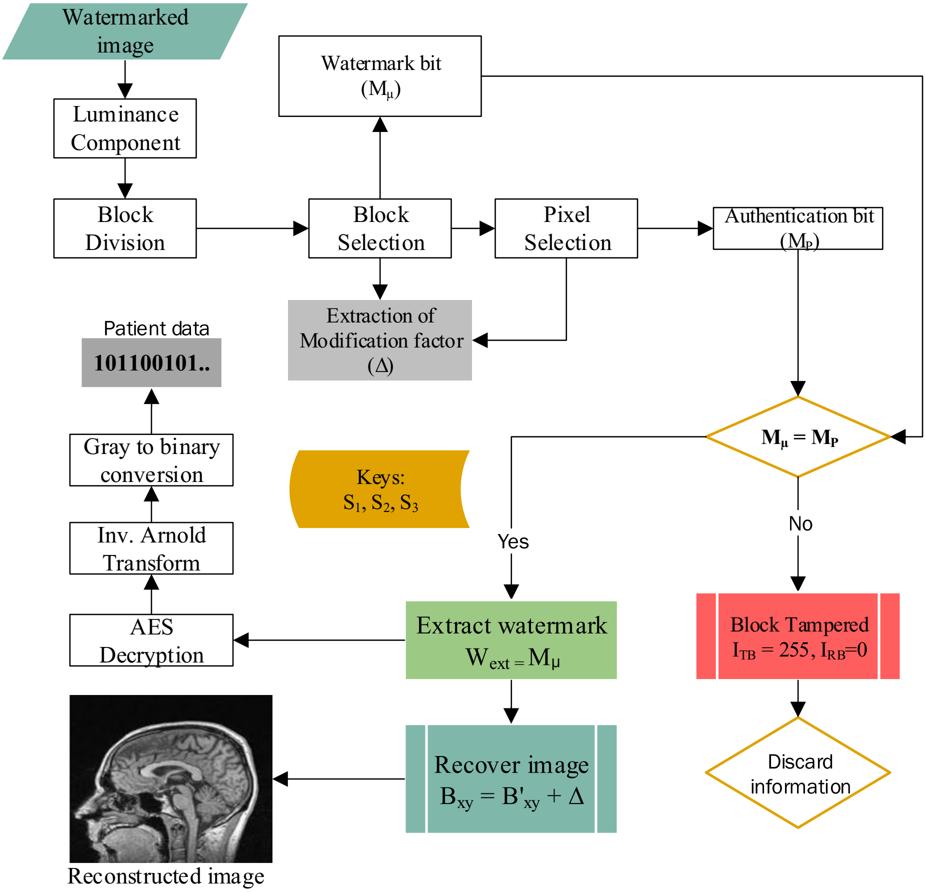


Fig. 4 Flowchart of the watermark extraction, image authentication and Image recovery

Step 7: Localize the tamper using the following conditions:

$$T_{ai} = \left(\widehat{M}_{\mu} \oplus \widehat{M}_{s}\right) \tag{15}$$

$$\Psi = T_{ai} \oplus W_{Xi} \tag{16}$$

$$I_{RB} = \begin{cases} 0; & \mathit{if}\ \psi = 1\ OR\ \widehat{\mu} = \beta_1\ OR\ \widehat{\mu} > \beta_2 \\ \widehat{B}_{xy}; & \mathit{otherwise} \end{cases} \tag{17}$$

$$I_{TB} = \begin{cases} 255 & \mathit{if}\ \psi = 1\ OR\ \widehat{\mu} = \beta_1\ OR \widehat{\mu} > \beta_2 \\ 0; & \mathit{otherwise} \end{cases} \tag{18}$$

Where “I_{RB}” is the recovered cover image block and “I_{TB}” is the tamper localizing block. The parameters β_1 and β_2 are defined to eliminate the effect of cropping attack which can manipulate all the pixels of the block to either a low value or a maximum intensity value.

$$\beta_1 = \begin{cases} \min(I)-1 & \mathit{if}\min(I) > 0 \\ \min(I); & \mathit{otherwise} \end{cases} \tag{19}$$

$$\beta_2 = \begin{cases} \max(I)-5 & \mathit{if}\max(I)\geq 250 \\ \max(I)+5; & \mathit{if}\max(I) < 245 \end{cases} \tag{20}$$

The addition of the modification factor in the step 5 leads us to the reversibility of 15 pixels of that block. The LSB bits of pixel $B'_{xy}(r)$ are further replaced by the mean of its eight neighbourhood pixels in order to ensure better perceptual quality of recovered image. Various possibilities of embedding and extraction of watermark bits are described in the Table 1. From the table it is clear that in all the four cases in the left column, watermark bit ‘1’ is extracted and in the right column watermark bit ‘0’.

5 Experimental results

In this section, subjective and objective quality metrics obtained from the proposed algorithm are presented. Several standard medical and gray scale host cover images of size M × N Like Brain, Hand, Head, CT Scan, Lena, Peppers, etc. have been used for evaluation and experimentation of the proposed scheme. Various test images (512 × 512) and watermarks (128 × 128) have been used for the analysis are shown in Fig. 5. To evaluate the imperceptivity of the watermarked image, the parameter PSNR and SSIM [34] are used. The PSNR should be greater than 36 dB so that human eye will not perceive the embedded information [36]. Similarly, parameters like Bit error rate (BER) and Normalized Cross correlation (NCC) are used for testing the fragility.

The two main evaluation parameters to describe performance of a watermarking scheme are fragility and imperceptibility. Fragility describes the resistance of the watermarking scheme against image manipulations due to attacks such as filtering, cropping, scaling, adding noise, and so on. The fragility is usually measured in terms of NCC and BER with respect to the original watermark and the extracted watermark in the presence of signal processing attacks. The imperceptivity of a watermarking scheme may be defined as measure of similarity between the original image and watermarked image. For evaluating this similarity, the parameter like the peak signal-to-noise ratio (PSNR) is used which may be defined as.

$$\mathrm{PSNR(dB)} = \quad 10\log\frac{(2^v-1)^2}{MSE} \tag{21}$$

Where ‘v’ refers to the number of bits used to represent the pixel intensity levels of an image. MSE, called mean squared error, is the average of the square of the difference between the two images I and $\widehat{I}$ of size M x N images and is given as

Table 1 Eight possibilities of watermark bit embedding and extraction in a block using proposed algorithm

Watermark bit, $W_e = 1$	Watermark bit, $W_e = 0$
Case 1: ***Embed stage:*** $\mathbf{M_\mu = 1, \mathit{M_s} = 1}$ $X_{MW} = M_\mu \oplus W_e = 0$ $\Psi = X_{MW} \oplus M_s = 1$ LSB of $B_{xy}(s)$ is **RESET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 1$	**Case 5:** ***Embed stage:*** $\mathbf{M_\mu = 1, M_s = 1}$ $X_{MW} = M_\mu \oplus W_e = 1$ $\Psi = X_{MW} \oplus M_s = 0$ LSB of $B_{xy}(s)$ is **SET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 0$
Case 2: ***Embed stage:*** $\mathbf{M_\mu = 1, \mathit{M_s} = 0}$ $X_{MW} = M_\mu \oplus W_e = 0$ $\Psi = X_{MW} \oplus M_s = 0$ LSB of $B_{xy}(s)$ is **RESET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 1$	**Case 6:** ***Embed stage:*** $\mathbf{M_\mu = 1, \mathit{M_s} = 0}$ $X_{MW} = M_\mu \oplus W_e = 1$ $\Psi = X_{MW} \oplus M_s = 1$ LSB of $B_{xy}(s)$ is **SET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 0$
Case 3: ***Embed stage:*** $\mathbf{M_\mu = 0, \mathit{M_s} = 1}$ $X_{MW} = M_\mu \oplus W_e = 1$ $\Psi = X_{MW} \oplus M_s = 0$ LSB of $B_{xy}(s)$ is **SET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_{P1} = 1$	**Case 7:** ***Embed stage:*** $\mathbf{M_\mu = 0, \mathit{M_s} = 1}$ $X_{MW} = M_\mu \oplus W_e = 0$ $\Psi = X_{MW} \oplus M_s = 1$ LSB of $B_{xy}(s)$ is **RESET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_{P1} = 0$
Case 4: ***Embed stage:*** $\mathbf{M_\mu = 0, \mathit{M_s} = 0}$ $X_{MW} = M_\mu \oplus W_e = 1$ $\Psi = X_{MW} \oplus M_s = 1$ LSB of $B_{xy}(s)$ is **SET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 1$	**Case 8:** ***Embed stage:*** $\mathbf{M_\mu = 0, \mathit{M_s} = 0}$ $X_{MW} = M_\mu \oplus W_e = 0$ $\Psi = X_{MW} \oplus M_s = 0$ LSB of $B_{xy}(s)$ is **RESET** as per Eq. (8) ***Extract Stage:*** $W = \widehat{M}_\mu \oplus \widehat{M}_s = 0$

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[I(\mathrm{x},\mathrm{y}) - \widehat{I}(\mathrm{x},\mathrm{y})\right]^2 \tag{22}$$

Where 'I' and '$\widehat{I}$' are the two images under comparison and usually one is the original image and second is its modified version. Clearly, if the pixels in error are few in number, then the value of the MSE returned is in the range of acceptable levels.

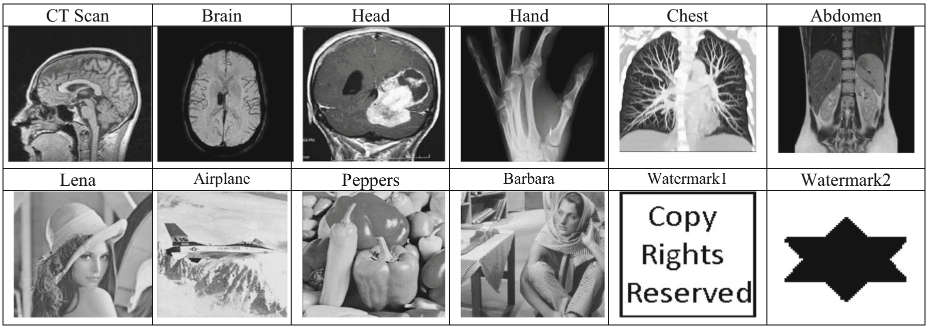


Fig. 5 Medical images, general images and the watermark(s)

The quantitative metric that is commonly used at the extraction stage to evaluate the performance of the watermarking scheme is the Bit Error Rate (BER), which is calculated as follows:

$$BER\ (\%) = 1/PQ\left[\sum_{x=0}^{P-1}\sum_{y=0}^{Q-1} W(x,y) \oplus \widehat{W}(x,y)\right] \times 100 \tag{23}$$

Where (x, y) gives the coordinates of a pixel such that W(x, y) and $\widehat{W}$ (x, y) are the pixel values of the original image and extracted image respectively at location (x, y). The value of BER should be as low as possible for a better watermarking scheme and if BER converges to zero then the original watermark is said to be completely recovered. Similarly, NCC is given mathematically as

$$NCC = \frac{\sum_{x=1}^{P}\sum_{y=1}^{Q} W(x,y)\widehat{W}(x,y)}{\sum_{x=1}^{P}\sum_{y=1}^{Q}[\mathrm{W}(x,y)]^2} \tag{24}$$

The closer the value of NCC to unity the more is the robustness of the watermarking system.

5.1 Imperceptivity analysis

In this section, the perceptual quality of the watermarked images and recovered images has been analysed and presented. For evaluating the perceptual quality of a watermarked image, two quality metrics adopted in this work are SSIM and PSNR. The images of size 512 × 512 and watermark of size 128 × 128 has been used for analysing the proposed algorithm. In this work the average PSNR of the watermarked images is greater than 47 dB while the average PSNR of the recovered images is greater than 57 as shown in Fig. 4. The reported values of PSNR after tamper analysis at the receiver demonstrate the efficacy of the proposed technique in medical applications. The quality of the cover images is maintained while embedding the watermark information by taking due care to ensure that there are not any significant changes in the portions of the images which are critical for diagnosis. This has been taken care of by embedding only small amount of watermark information such that both quality of medical image is kept intact and tamper detection is ensured.

From Fig. 6 it is clear that the proposed technique recovers the original image with high perceptual quality. From the results it is clear that the recovered images at the receiver have high visual quality as compared to the watermarked images and hence the proposed scheme can be used for high quality original image recovery.

Figure 7 shows comparison of proposed scheme against Tiwari [33], Ansari [4], and Qi [28] to validate the efficacy in terms of visual quality.

5.2 Embedding capacity

The embedding capacity of the fragile watermarking scheme with block size and PSNR is shown in the Table 2. Thus, the quality of the watermarked image varies to a desirable range by just varying the embedding capacity. The embedding capacity, also known as payload, is the amount of information (number of bits) embedded in an image. The proposed scheme embeds 1-bit of information per p × p block. The total number of bits that can be embedded depends on the size of image and the block division. As such Table 1 presents the payload information and corresponding effect on imperceptivity. From the table it can be seen that the proposed scheme while embedding large amount of data in an image maintains the visual quality.

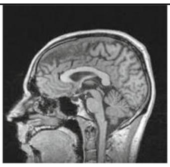
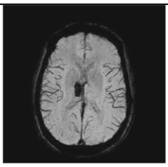
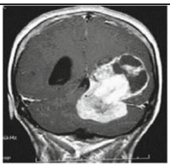
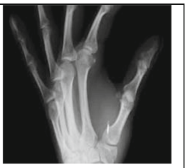
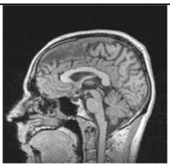
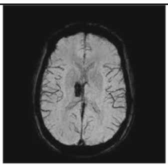
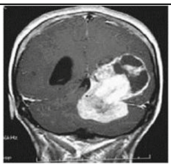
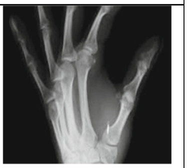
Watermarked Image				
PSNR (dB) **SSIM**	48.12 0.9992	47.50 0.9994	48.79 0.9997	47.32 0.9891
Extracted Watermark				
BER (%) **NCC**	0 1	0 1	0 1	0 1
Recovered Image				
PSNR (dB) **SSIM**	59.27 0.9942	58.50 0.9913	59.17 0.9938	58.90 0.9915

Fig. 6 Imperceptivity results of medical images

A comparison of proposed scheme with some state of art data hiding schemes in terms of embedding capacity is presented in the Table 3 to demonstrate effectiveness.

5.3 Authentication analysis

For the cases like content authentication the fragility of a watermarking scheme is the most important factor. In this section the watermarked image is exposed to several attacks and the results are recorded in Fig. 8. For the said purpose attacks like filtering, noise addition, compression, geometric attacks, etc. are used which may attack the watermarked image during transmission. NCC and BER are the two objective metrics which have been used for

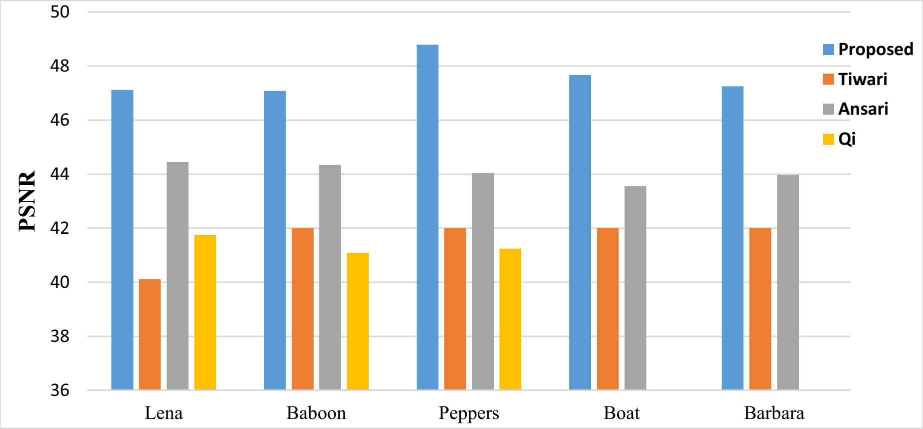


Fig. 7 Comparison of imperceptivity for gray scale images of size 512 × 512

Table 2 Average PSNR and payload with different block sizes for 30 images of size 512 × 512

Cover image size	Watermark size	Block size used	Embedding capacity (bits)	Avg. PSNR (dB)	
				General	Medical
256 × 256	32 × 32	8 × 8	1024 (2^{10})	60.56	62.16
256 × 256	64 × 64	4 × 4	4096 (2^{12})	47.04	48.61
256 × 256	128 × 128	2 × 2	16,384 (2^{14})	42.54	43.30
512 × 512	64 × 64	8 × 8	4096 (2^{12})	61.17	63.07
512 × 512	128 × 128	4 × 4	16,384 (2^{14})	47.40	48.90
512 × 512	256 × 256	2 × 2	65,536 (2^{16})	41.71	42.33

evaluation of the robustness of the proposed scheme. For the authentication purposes a fragile watermark has been embedded in a medical image.

Figure 8 shows the subjective and objective results obtained after different attacks on the watermarked image. From the results it is clear that the proposed scheme does not withstand any of the signal processing attacks and hence suits perfectly for medical and high security applications where a single bit change can totally produce different results. The proposed scheme has proven to achieve temper detection is reported on any kind of attack on the watermarked image through fragile watermark.

5.4 Tamper localization analysis

The most important requirements of a fragile watermarking system include the capability to detect the nature and location of attacks. This requires the capability of localizing the regions of tamper in case of an attack on the watermarked image. The effect of an attack on an image depends on the nature and intensity. While as effect of filtering and noise attacks can be seen on the entire image, the effect of geometric attacks is usually concentrated in a specific region. There are also some attacks where the intruder tries to corrupt or replace some objects and other related stuff from the image. Also, in some case the portions of an image may be replaced with some other information such that a false information is conveyed to the receiver. In all these cases the system should be reliable enough to predict the nature of attacks and hence localize the tamper. The proposed watermarking system is able to correctly localize the tampering regions of an attacked image. In Fig. 9, the localization results after various forgery attacks on watermarked images are presented. These attacks include content removal, copy & paste and text insertion. It can be seen from the results that proposed watermarking system successfully detects the regions of tamper in case of all attacks. It is pertinent to mention here that the watermarked images are manipulated by adding the text ‘ATTACK’ of different sizes at different locations. The subjective results in the figures clearly present the performance visualization of the tamper localization.

Table 3 Comparison of payload for image size 512 × 512

Method	Embedding capacity (bits)
Qi [28]	4096
Ansari [4]	16,380
Proposed	16,386

Attacks	Median Filter [3 3]	Salt and Pepper (1%)	Gaussian Noise (1%)	Gaussian LPF (3 × 3)	Sharpening
Extracted Watermark					
BER (%)	49.16	53.63	61.46	48.15	55.12
NCC	0.597	0.663	0.482	0.688	0.547
Attacks	**Rotation Attack (45º)**	**Scaling Recovery (upscale 50%)**	**JPEG (QF=20)**	**JPEG 2000 (CR = 8)**	**Histogram Equalization**
Extracted Watermark					
BER (%)	57.17	55.33	61.12	59.38	57.22
NCC	0.622	0.524	0.446	0.506	0.541
Attacks	**LSB Reset (bit 1)**	**LSB Reset (bit 2)**	**LSB Reset (bit 1-3)**	**LSB Reset (bits 1-4)**	**Poisson Noise**
Extracted Watermark					
BER (%)	51.33	50.73	57.23	60.92	60.33
NCC	0.60	0.487	0.432	0.411	0.401

Fig. 8 Extracted watermarks (Watermark2) after various attacks on head medical image

The performance of the proposed scheme for tamper localization are presented for content removal, text addition and copy & paste forgery attacks in Fig. 9. In the figure a portion of the watermarked image is pasted with a portion copied from another image. It is evident from the results that the proposed technique successfully localizes even a small copy and paste forgery

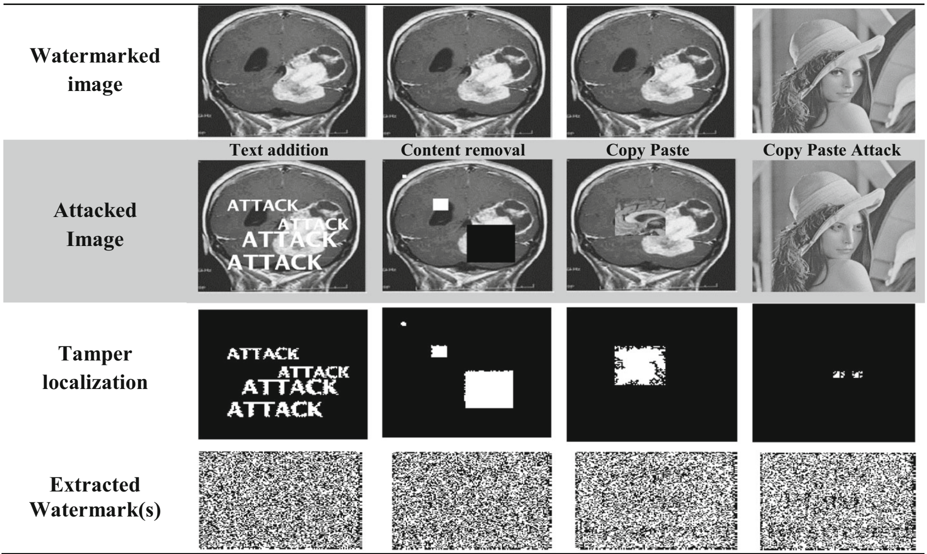


Fig. 9 Temper localization performance under different forgery attacks

attack. The corresponding extracted watermarks (Watermark1) are also shown for every attack. The content removal attack is one of the few tampering attacks suffered by the images during transmission and hence has been analyzed to test the localization performance of the proposed scheme. The subjective results under the content removal attack are shown in the Fig. 9 and clearly describe the effectiveness of the proposed scheme with high level of tamper localization efficiency.

The robustness and tamper localization performance of the proposed scheme are presented for attacks like masquerading cutting and pasting at the four borders of the watermarked image in Fig. 10. The experiments are carried out by replacing five neighboring rows (or columns) of the five border rows (or columns) in a watermarked image. The results clearly describe the efficacy of the proposed technique in terms of tamper detection and localizing for the minor and undetectable modifications.

The proposed watermarking system is also tested for a complicated UCID database comprised of 1338 images and the results for some randomly chosen images are shown in Fig. 11. For rest of the images similar results are obtained. It can be seen that system is able to correctly localize the tampering regions of an attacked image. In order to test the whole database different forgery attacks have been considered as reported in the Fig. 11. The block tamper detection rate and average BER (%) results are obtained for 100 images of the UCID database.

5.4.1 Tampering rates

The accuracy of tampering can be objectively described in terms of various tampering rates [6, 35]. The commonly used objective parameters for tamper detection are: Tamper Detection Rate (TDR), False Positive Rate (FPR) and False Negative Rate (FNR).

Tamper detection rate (R_{TD}) It is the detection rate of pixel tampering and hence calculated using the actual pixel tampering rate. If 'D_t' is the number of tampered pixels detected and 'P_t' is the actual number of pixels tampered, then:

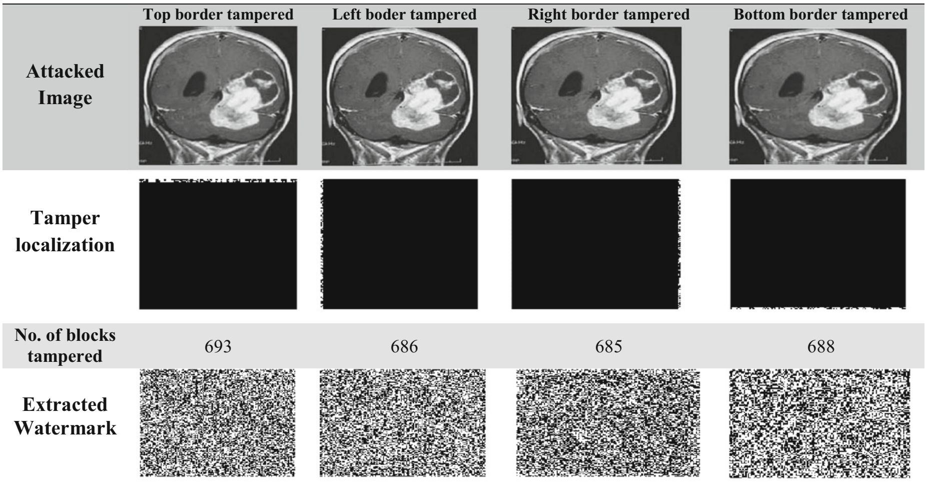


Fig. 10 Temper localization performance for masquerading cutting and pasting at borders

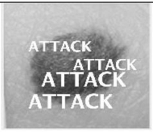
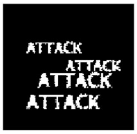
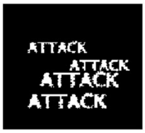
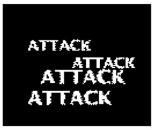
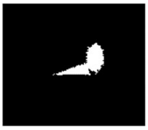
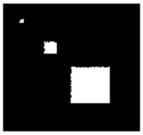
Attacked sample image					
Tamper localization					
Tampered Blocks	1337	1345	1378	570	1482
Avg. BER (%)	55.27	55.48	55.86	54.23	56.19

Fig. 11 Temper localization results for images from UCID database

$$R_{TD} = \frac{D_t}{P_t} \times 100\% \tag{25}$$

False Positive Rate (R_{FP}) It is the false rate of pixel tamper detection and gives the percentage of pixels that are not tampered but are detected as tampered. If 'D_{NT}' represents the detected number of tampered pixels which are not tampered and 'P_N' is the number of pixels in the untampered region, then

$$R_{FP} = \frac{D_{NT}}{P_N} \times 100\% \tag{26}$$

False Negative Rate (R_{FN}) It is the percentage of pixels that are tampered in actual but are not detected as tampered. If T_{ND} gives the total number of undetected tampered pixels and 'P_t' is number of pixels in tampered region, then:

$$R_{FN} = \frac{D_{TN}}{P_t} \times 100\% \tag{27}$$

Figure 12 shows the accuracy of tamper detection for various images tampered by different percentages. The tampering has been done by cropping the watermarked images by cropping with different sizes. It can be seen from the figure that accuracy of more than 99% is achieved using the proposed algorithm. It can be noted that for small tampering sizes the accuracy is less than in case of bigger sizes.

A comparison between Benrhouma [35] and Zhang [6] for FPR and FNR rates is shown in the Fig. 13. It can be seen from the figures that the proposed scheme offers better tamper localization. It may be noted that for small tampering percentages the FPR is slightly higher than rest of the two schemes under comparison.

5.5 Reversibility analysis

A medical image is usually required in the original form for the accurate diagnosis and treatment of a disease. The proposed technique considers this requirement and

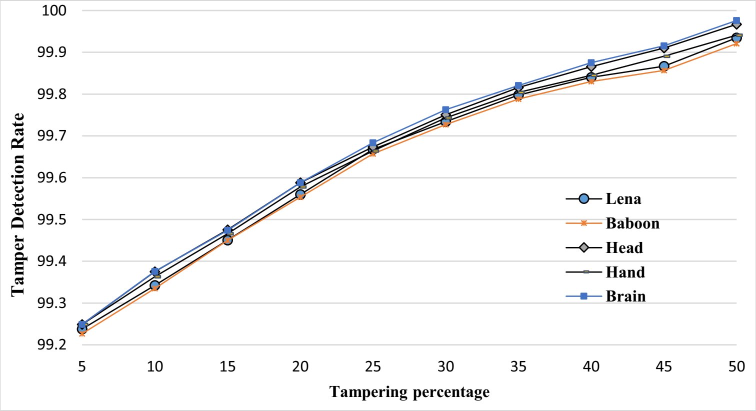


Fig. 12 Tamper detection performance analysis in terms of TDR for variable tampering percentages

devises the algorithm in a way that we can recover the original image with high accuracy after extraction of the watermark information. In order to prove the claim, we perform reversibility analysis on a set of different images. As the secret data is authenticated and extracted from the watermarked image, the change induced by the modification factor 'ζ_F' are reversed to get the high-quality version of recovered image, whose statistical properties are highly similar to that of original image. The recovered images have very high imperceptivity with PSNR more than 57 dB. In Fig. 14, various cover images and their corresponding recovered versions are shown along with the difference performed in between. It is evident from the figure that the proposed data hiding framework successfully recovers the images with pixel intensities almost same as that of original ones. Thus, proposed design ensures tamper detection and localization without deteriorating the original images and hence can be efficiently used in e-healthcare where the cover images are as important as the private data.

It is pertinent to mention here that the modification factor is subtracted back from the block pixels which leads to the reversibility of 15 pixels of that block. The LSB bits of pixel $B'_{xy}(r)$

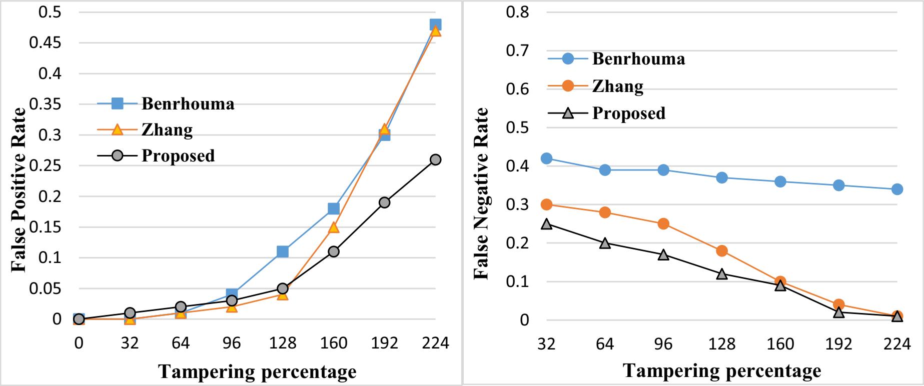


Fig. 13 Tamper detection performance analysis in terms of FPR and FNR for variable tampering percentages

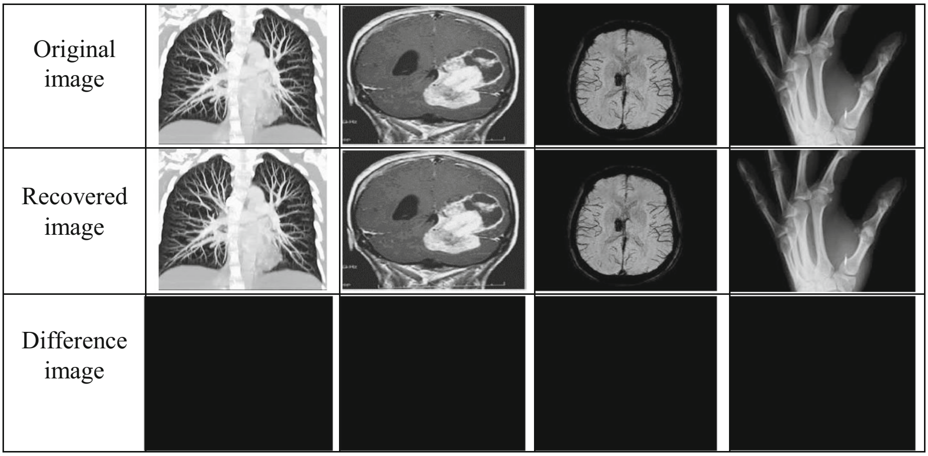


Fig. 14 Reversibility analysis of various images

are further replaced by the mean of its eight neighbourhood pixels in order to ensure better perceptual quality of recovered image.

5.5.1 Histogram analysis

The efficiency of reversibility offered by a data hiding system can be studied by performing histogram analysis of the original and recovered images. This sub-section is dedicated for histogram analysis and hence effectiveness of reversibility of proposed scheme. In e-healthcare, the medical images carry information and are required by the authentic receivers to perform proper diagnosis. Therefore, it becomes extremely important that the statistical information of the medical images remains intact. So, for an efficient data hiding system the histograms, which show the statistical information in an image, should be similar. Since, only 3 out of 128 information bits are modified in a 4×4 block for the various objectives in the proposed framework, the effect on the visual quality of the cover images remains almost intact. Also, the modification factor which changes the intensity of all the block pixels is reversed with 100% accuracy at the receiver by the authentic user having decoding keys. Hence the histogram of the recovered images matches the original image with high degree of accuracy. In Fig. 15 the histograms of the original (general and medical) and recovered images is shown. It can be seen from the figure that there is no evident deviation in the histograms of cover and recovered images. This is an important requirement in e-healthcare applications where the quality of the medical images needs to be kept intact for proper diagnosis.

5.6 Computational complexity analysis

The computational efficiency of a data hiding scheme is an important factor for high speed and real time applications like Internet of Things (IoTs), mobile communication, social media, defence, e-healthcare etc. Computational cost of a watermarking scheme is determined by the time taken for performing embedding and extraction of information. Since proposed data

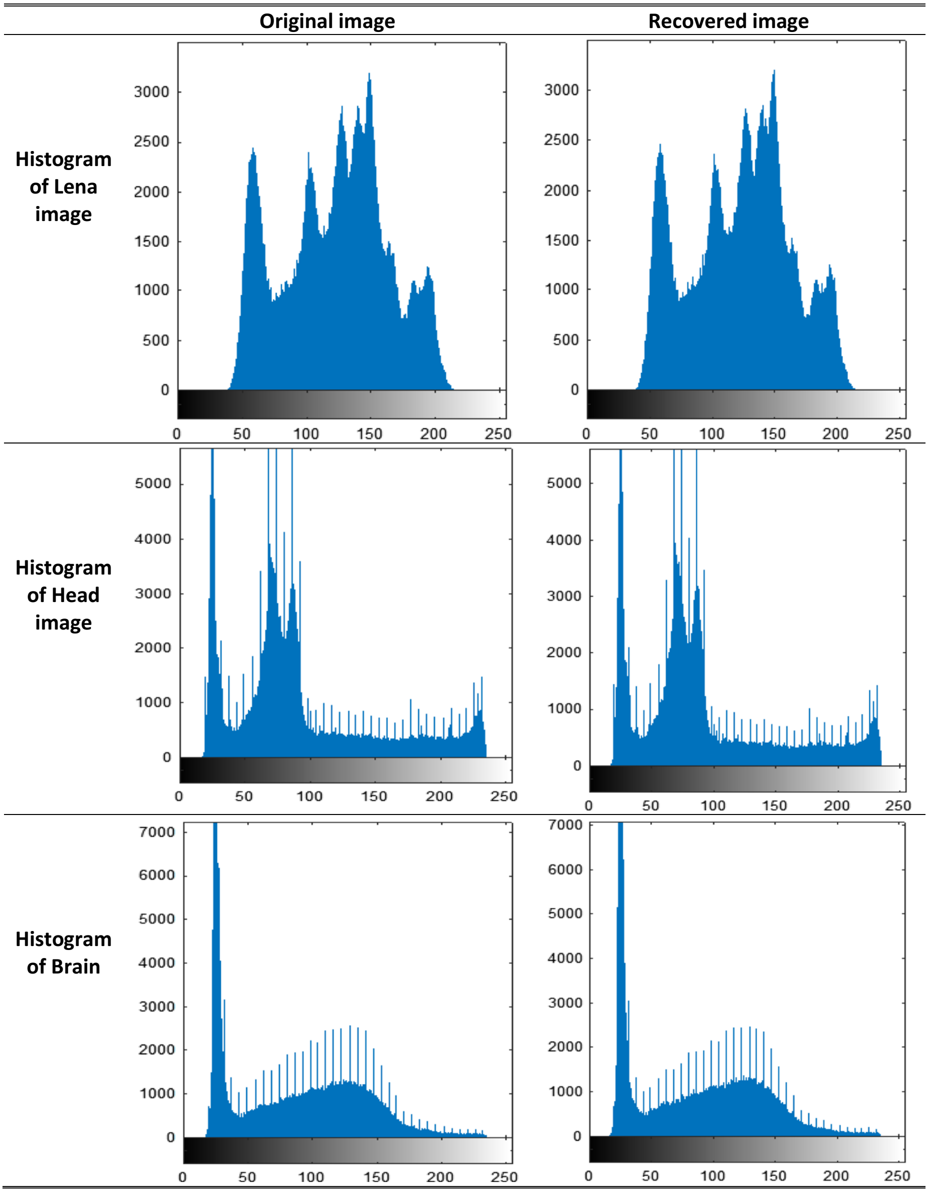


Fig. 15 Histogram analysis of various images

hiding technique is based on spatial domain and the embedding has been done by modification of LSB bits only within a block, the computational cost is minimum. The embedding and extraction time taken for data hiding in various images is shown in Table 4.

It can be seen from the results that proposed scheme operates very fast and as such time taken for extraction/embedding is less than a second. It is pertinent to mention here that these times do not include the time taken for encrypting the watermark which is less than 1.15 s as shown in the Table 5. In the proposed technique, the watermark of maximum size 128 × 128 is embedded in an image.

Table 4 Embedding and extraction time(s) for watermark of size 128 × 128

Test Image	Singh [31]	Embed Time	Extraction Time
Lena	6.5520	0.6688	0.5438
Cameraman	6.5833	0.6213	0.5313
Baboon	6.3930	0.6189	0.5256
Peppers	NA	0.6412	0.5312
Brain	NA	0.6484	0.5966
Head	NA	0.6264	0.5838
Hand	NA	0.6860	0.6199
Average	6.5094	0.6444	0.5617

5.7 Security analysis

In order to strengthen the security of the information hidden secretly in a cover image several levels of security procedures are adopted in the proposed scheme. Arnold transform along with AES encryption and gray level encoding have used as encryption of the secret information before embedding watermark. So, in order to extract the embedded information correctly, the number of iterations (t) and value of other secret keys have to be exactly same as that used in the embedding. To enhance that security up to an unbreakable level multiple secret keys are used at different stages of embedding so that embedding algorithm remains resilient to any attack. The parameters like embedding factor and embedding location are made secret keys of the embedding algorithm. The value of the embedding factor ($\zeta_{\mathbf{F}}$) lies in the range $1.1 \leq \zeta_{\mathbf{F}} \leq 11.24$ and for the value of embedding factor higher than 11.24 the PSNR is less than 36 dB. The other private keys vary in length, each set with the bit length from up to 10 bits such that we can use any of the 1024 values (2^{10}).

The Kerckhoffs's desideratum states that a cryptosystem should be secure as long its encryption key is secret even if rest of the algorithm becomes public. The key selection hence is a critical factor to determine the level of security of a cryptographic system. The strength of a key of any secure system is analyzed through its length and sensitivity. The sensitivity of the proposed watermarking method can be described to such an extent that a single bit change in the key will result in failure of the whole extraction/decryption process and no meaningful data will be recovered. Hence, an undesired intruder will have no chance to decrypt the information data without accurate possession of the decryption keys.

5.7.1 Key sensitivity analysis

In order to prove the efficiency of the proposed scheme in terms of security, various tests can be performed. One is the check on the sensitivity test. The sensitivity of an encryption key to any unauthorized alteration is defined by the level of change results in the extraction of watermark. For an efficient encryption technique, the minute change in the secret key during extraction should result in unrecognizable watermark. The sensitivity of the private keys like embedding factor 'ζ_F' is tested by changing only a single bit and the effect on extracted information is seen in terms of various parameters. The subjective and objective results hence obtained are shown in Fig. 16. As can be seen from the figure, the watermarks extracted are totally unrecognizable which prove high sensitivity of private keys. Similar tests have been performed on other keys like that of iteration count corresponding to Arnold transform and the results are reported in Fig. 16. The last three rows of Fig. 16 show the extracted versions of

Table 5 Embedding (E_T) and extraction (D_T) time(S) for watermarks of different sizes

Watermark	Size	Arnold *(t = 55)*	AES	Arnold + AES + Gray Coding	
				E_T	D_T
Watermark1	32 × 32	0.1532	0.1331	0.4671	0.4344
	64 × 64	0.2044	0.1821	0.4524	0.4461
	128 × 128	0.2653	0.2423	0.7043	0.7013
Watermark2	64 × 64	0.2014	0.1762	0.4546	0.4302
	128 × 128	0.2743	0.2402	0.7175	0.7063
	256 × 256	0.3754	0.3473	1.1406	1.1216

watermark at different iterations (t') including the original encryption count (t) and the corresponding encryption count (t'), respectively. As seen, the encrypted watermark images exhibit excellent uncorrelated and random-like (non-periodic) properties. Thus, the proposed encryption technique offers very high sensitivity of the secret keys and as such even a single bit change results in totally unrecognizable watermark.

Consider the case of changing the value of embedding factor in the proposed algorithm wherein the value of 'ζ_F' used for embedding is changed a fractional value when used for extraction. Different values of 'ζ_F' used for embedding and corresponding values used for extraction are shown in the figure along with extracted watermarks. Similarly, using different values of iteration 't' at encryption and decryption stage (say from $t = 8$ for encryption and t' = 10 for decryption), the sensitivity of the watermark is analysed and the extracted watermarks are shown in lower half of Fig. 16. It is evident from the results reported in figure that the secret keys used in the proposed framework offer very high sensitivity to even a small change and thus providing high security to the embedded information.

Clearly, keys used in the proposed algorithm as very sensitive to any change. Even a single bit change in the key will give the results that are totally meaningless. As the extracted message does not match with the original data, the proposed algorithm should be proved to be highly sensitive to any minute alteration.

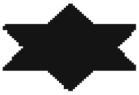
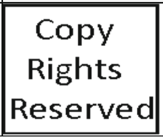
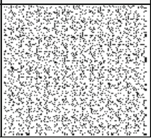
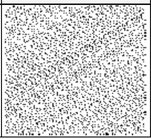
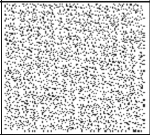
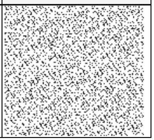
Embedding factor	$\zeta_F = 1.10$	$\zeta_F = 1.11$	$\zeta_F = 3.95$	$\zeta_F = 8$	$\zeta_F = 11.24$
Extraction Factor	$\zeta_F = 1.10$	$\zeta_F = 1.12$	$\zeta_F = 3.96$	$\zeta_F = 8.01$	$\zeta_F = 11.23$
Extracted Watermark 2					
Arnold Iterations at encryption	**t = 8**	**t = 8**	**t = 55**	**t = 55**	**t = 55**
Arnold Iterations at decryption	**t' = 8**	**t' = 10**	**t' = 60**	**t' = 62**	**t' = 100**
Extracted Watermark 1 with iteration count (t')					

Fig. 16 Original and extracted watermarks after different iterations

5.8 Brief discussion about the results

An overall discussion about the performance of the proposed data hiding scheme is presented in this section. The main aim of this scheme has been on the development of a data hiding framework to secure secret data in a cover image and ensure both tamper detection and localization along with cover image reversibility. In the process of attaining said goals the proposed scheme has been implemented with handsome payload, high imperceptivity and better security. Tamper detection has been achieved by embedding a watermark bit while modifying LSBs of each 4 × 4 image block. Thus, effect on visual quality of the cover image remains negligible. The authentication of the watermark bit in process decides whether the specific block is tampered or not. This ensure tamper localization without any significant overhead problems. The reversibility has been ensured during the embedding process by selecting a modification factor which modifies the whole block during the process. And as the watermark bit is extracted at the receiver without any error from the image, the effect of modification factor on the image is reversed. The value of the modification factor is stored in LSB bits of an unmodified block pixel. It is pertinent to mention here that both image block selection and corresponding pixel selection has been done randomly at each cycle of embedding process. The average value of PSNR obtained for various images after embedding 16 kb information is 47 dB and 57 dB after recovery, thus very high imperceptivity is achieved. To validate the performance of the scheme various objective and subjective tests have been carried under different case scenarios in section 4. From the comparison results it is evident that the proposed scheme offers better results in terms of fragility, imperceptivity, computational cost and authentication. From the section 4.5, it is evident that the scheme accurately detects any small alteration in any portion of the watermarked image. And it is evident from the results that any small tamper completely corrupts the watermark information (indicating the tamper) and as such watermark is totally unrecognizable. The objective results obtained in terms of BER, higher than 50% for all types of images, further strengthen the claim our scheme offers very high fragility to the embedded information and hence suits for authentication applications. In case of tamper less reception of the watermarked images, the cover image is recovered with high degree of resemblance with the original one as authenticated by results in section 5.4 and 5.5. Table 6 presents a detailed comparison of some of the state-of-the-art the techniques referred in this paper with the proposed scheme in terms of different key parameters. Clearly, the proposed scheme outperforms the rest of the schemes. It is here pertinent to mention that the complexity is shown high for algorithms implemented in transform domain and low for algorithms implemented in spatial domain. Also, the payload is mentioned as not available (NA) for the techniques used for tamper detection where no external watermark is embedded in the cover image.

6 Conclusion and future work

In this paper, a reversible image authentication scheme for embedding EMR in medical images for e-health applications has been presented. A fragile watermark has been embedded into the cover images to ensure content authentication at the receiver. Tamper localization is achieved accurately by using LSB embedding along with mean modification approach. Reversibility has been achieved by using an efficient embedding approach in spatial domain. During embedding procedure different embedding factors are added for embedding bit ‘0’ and bit ‘1’. After data

Table 6 Performance comparison of various schemes cited in the paper

Technique	Blind	Imperceptivity (PSNR)	Payload	Complexity	Watermark embedded	Localization accuracy	Fragility	Reversibility
Al-otum [3]	Yes	48 dB	16 Kb	High	Yes	Poor	NA	No
Daniel [30]	Yes	50 dB	NA	High	No	Poor	NA	No
Qi [28]	Yes	41.39 dB	16 Kb	High	Yes	Poor	NA	Yes
Tiwari [33]	No	42 dB	16 Kb	Low	Yes	Moderate	Weak	Yes
Ansari [4]	Yes	45 dB	16 Kb	High	Yes	Moderate	NA	Yes
Ming [20]	Yes	42 dB	16 Kb	Medium	No	Poor	NA	Yes
Hong [14]	Yes	50.40 dB	NA	High	No	Moderate	NA	Yes
Wojtowicz [35]	Yes	46 dB	NA	High	No	NA	Strong	No
Benrhouma [6]	Yes	51.14 dB	262 Kb	Low	No	Poor	Medium	No
Zhang [39]	Yes	51 dB	65 Kb	High	No	Poor	Medium	No
Proposed	Yes	47 dB, 57 dB	16 Kb	Low	Yes	Strong	Strong	Yes

extraction, the same embedding factors are subtracted from the image to get the pre-embedding image and hence to maintain reversibility. The security of embedded patient record has been ensured using multiple levels of encryption prior to embedding. The experimental results reveal that the scheme has better performance in terms of tamper detection, tamper localization, reversibility and security of watermark. In addition, compared to most tamper detection and localization schemes, the proposed scheme is blind in nature. Given the various benefits of the scheme it could serve as a potential candidate for transfer of EMR in an e-healthcare system.

References

1. Abd El-Latif AA, Abd-El-Atty B, Hossain MS, Rahman MA, Alamri A, Gupta BB (2018) Efficient quantum information hiding for remote medical image sharing. IEEE Access 6:21075–21083. https://doi.org/10.1109/ACCESS.2018.2820603
2. Agrawal S, Kumar M (2016) Reversible Data Hiding for Medical Images using Integer-to-Integer Wavelet Transform. IEEE Student's conference on electrical, Electronics and Computer Science. https://doi.org/10.1109/SCEECS.2016.7509266
3. Al-Otum HM (2014) Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. J Vis Commun Image Represent 25(5):1064–1081
4. Ansari IA, Pant M, Ahn CW (2016) SVD based fragile watermarking scheme for tamper localization and self-recovery. Int J Mach Learn Cybern 7(6):1225–1239
5. Arnol'd VI, Avez A (1968) Ergodic problems of classical mechanics. Benjamin, New York
6. Benrhouma O, Hermassi H, El-Latif AAA, Belghith S (2016) Chaotic watermark for blind forgery detection in images. Multimed Tools Appl 75:8695–8718
7. Chang CC, Chen KN, Lee CF, Liu LJ (2011) A secure fragile watermarking scheme based on chaos-and-hamming code. J Syst Softw 84(9):1462–1470
8. Cox I, Miller M, Bloom J, Miller M, Fridrich J, Kalker T (2007) Digital watermarking and steganography. Morgan Kaufmann, San Francisco
9. Digital Guardian. Top 10 biggest healthcare data breaches of all time (2018). Available at: https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time.
10. Hamza R, Muhammad K, Lv Z, Titouna F (2017) Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive and Mobile Computing 41:436–450
11. Hamza R, Titouna F (2016) A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective 25(4–6):162–179
12. Hassan B, Ahmed R, Li B, Hassan O (2019) An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement. IEEE Access 7:69758–69775
13. Health Care IT News. The biggest healthcare data breaches in 2018 (so far). (2018) Available at: https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.
14. Hong W, Chen M, Chen TS (2017) An efficient reversible image authentication method using improved PVO and LSB substitution techniques. Signal Process Image Commun 58:111–122
15. Huang Y, Niu B, Guan H, Zhang S (2019) Enhancing image watermarking with adaptive embedding parameter and PSNR guarantee. *IEEE Transactions on Multimedia* 21(10):2447–2460
16. Hurrah NN, Loan NA, Parah SA, Sheikh JA (2017) A transform domain based robust color image watermarking scheme for single and dual attacks. 2017 Fourth International Conference on Image Information Processing (ICIIP), vol 00, no pp 1–5 IEEE
17. Hurrah NN, Parah SA, Loan NA, Sheikh JA, Elhoseny M, Muhammad K (2018). Available at) Dual watermarking framework for privacy protection and content authentication of multimedia. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2018
18. Hurrah NN, Parah SA, Sheikh JA, Al. Turjamaan F, Mohammad K (2019) Secure data transmission framework for confidentiality in IoTs. In ad hoc networks, Elsevier
19. Kumar VC, Natarajan V (2016) Hybrid local prediction error-based difference expansion reversible watermarking for medical images. Comput Electr Eng 53:333–345
20. Li M, Xiao D, Zhang Y (2016) Attack and improvement of the fidelity preserved fragile watermarking of digital images. Arab J Sci Eng 41(3):941–950

21. Liu X, Lin C, Yuan S (2018) Blind dual watermarking for color images' authentication and copyright protection. *IEEE Transactions on Circuits and Systems for Video Technology* 28(5):1047–1055
22. Nazir AL, Nasir NH, Shabir AP, Lee JW, Javaid AS, Bhat GM (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access 6:19876–19897
23. Nguyen TS, Chang CC, Chung TF (2014) A tamper-detection scheme for BTC compressed images with high-quality images. KSII Trans Internet Inf Syst 8(6):2005–2021
24. Nguyen TS, Chang CC, Yang XQ (2016) A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. AEU-International Journal of Electronics and Communications 70(8):1055–1061
25. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM (2017) Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl 76(8):10599–10633
26. Parah SA, Sheikh JA, Dey N, Bhat GM (2017) Realization of a new robust and secure watermarking technique using DC coefficient modification in pixel domain and chaotic encryption. Journal of Global Information Management (JGIM) 25(4):80–102
27. Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digital Signal Processing 53:11–24
28. 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
29. Roy A, Chakraborty RS (2019) Towards optimal prediction error expansion based reversible image watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*. https://doi.org/10.1109/TCSVT.2019.2911042,1
30. 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
31. Singh D, Singh SK (2017) DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimed Tools Appl 76(1):953–977
32. Sivakannan S, Thirugnanam G, Sheeba JC (2016) An efficient ICA and DWT combined approach for medical image watermarking technique. World Appl Sci J 34(9):1197–1203
33. Tiwari A, Sharma M, Tamrakar RK (2017) Watermarking based image authentication and tamper detection algorithm using vector quantization approach. AEU-International Journal of Electronics and Communications 78:114–123
34. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
35. Wojtowicz W, Ogiela MR (2016) Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. J Vis Commun Image Represent 38:1–10
36. Wu NI, Hwang MS (2007) Data hiding: current status and key issues. IJ Network Security 4(1):1–9
37. Wu Y, Xiang Y, Guo Y, Tang J, Yin Z (2019) An improved reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Trans Multimed 1
38. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 273:329–351
39. Zhang H, Wang C, Zhou X (2017) Fragile watermarking for image authentication using the characteristic of SVD. Algorithms 10(1):27

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

Nasir N. Hurrah is a doctoral student in the Department of Electronics and IT, University of Kashmir. He is pursuing Ph. D under VISVESVARAYA PHD Scheme for Electonics and I.T., sponsored By Ministry Of Electrinics & Information Technology Government Of India.

Shabir A. Parah has completed his M. Sc and M. Phil and Ph.D in Electronics from University of Kashmir, Srinagar in the year 2004, 2010 and 2013 respectively in the field of Signal processing and Data hiding. He is working as Assistant Professor in the department of Electronics and I. T, University of Kashmir, Srinagar. His fields of interest are Signal Processing, Secure Communication, Digital Watermarking and Steganography. He has published more than one hundred papers in the journals and conferences of international repute.

Javaid A. Sheikh has completed his M.Sc., M. Phil and Ph. D in Electronics from University of Kashmir, Srinagar in the year 2004, 2008 and 2012 respectively in the field of communications and Signal Processing. He is working as Assistant Professor in the department of Electronics and I. T University of Kashmir, Srinagar. His fields of interest are Wireless Communications, design and development of efficient MIMO-OFDM based wireless communication techniques, Spread Spectrum modulation, Digital Signal Processing, Electromagnetics. He has published about sixty research papers in International and National journals and conference proceedings.