Chapter 6
Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images

Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan

6.1 Introduction

The significant advancements in information and communication technologies (ICT) [1] has opened up newer opportunities for telemedicine by facilitating medical data transmission across geographical boundaries through Internet, mobile networks, and other wireless/wired communication channels and thus covering rural/remote areas, accident sites, ambulance, and hospitals. However, the transmission of medical data over an open communication channel poses different possibilities of threat that can severely affect its authenticity, integrity, and confidentiality [2]. Digital watermarking studies have always been driven by the improvement of robustness and a current security tool to protect electronic patient record (EPR) [3].

On the contrary, security has received little attention in the watermarking community. The first difficulty is that security and robustness are neighbouring concepts, which are

---

A.K. Singh (✉)
Department of Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat, Solan, India
e-mail: amit_245singh@yahoo.com

B. Kumar
Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad, India
e-mail: singhbasant@yahoo.com

G. Singh
Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat, Solan, India
e-mail: drghanshyam.singh@yahoo.com

A. Mohan
Department of Electronics Engineering, Indian Institute of Technology (BHU), Varanasi, India
e-mail: profanandmohan@gmail.com

© Springer International Publishing AG 2017

A.K. Singh et al. (eds.), *Medical Image Watermarking*, Multimedia Systems and Applications, DOI 10.1007/978-3-319-57699-2_6

hardly perceived as different. Security deals with intentional attacks whereas robustness is observed as degradation in data fidelity due to common signal processing operations. Also, digital watermarking may not be secure despite its robustness [4]. Therefore, security of the watermark becomes a critical issue in various applications. The problem of watermark security can be solved using spread-spectrum scheme [2, 5–10]. Spread-spectrum is a technique designed to be good at combating interference due to jamming, hiding of a signal by transmitting it at low power, and achieving secrecy. These properties make spread-spectrum very popular in present-day digital watermarking.

The subsequent section of the chapter is structured as follows: The related and recent state-of-the-art techniques are provided in Sect. 6.2. The main contribution of the work is summarized in Sect. 6.3. The spread-spectrum Watermark Design is reported in Sect. 6.4. Section 6.5 describes the proposed work. Experimental results and brief analysis of the work is reported in Sect. 6.6. Next, our summary of the chapter is presented in Sect. 6.7.

6.2 Related Work

Brief reviews of recent and related watermarking methods are presented as follows:

Recently, in [2] an image watermarking scheme based on spread-spectrum technique was proposed in which different watermark messages were hidden in the same transform coefficients of the cover image using uncorrelated codes, *i.e.* low cross correlation value (orthogonal/near orthogonal) among codes. The authors have also proposed another algorithm [5] based on spread-spectrum technique in which two different pseudo noise (PN sequence) vectors of size identical to the size of each sub-band column are generated for each watermark message bit. This algorithm further enhances the watermarking capacity in wavelet domain. The performance of the algorithm in [5] has been analysed for text watermark in [10]. These methods are robust and secure against known attacks. D-Ferrer and Sebe´ [11] proposed a spread spectrum based invertible watermarking method for image authentication purpose in lossless format. The method is robust and highly imperceptible. Das et al. [12] proposed a watermarking method based on spread spectrum technique. The method is designed from the analytical study of state transition behavior of non-group cellular automata and the basic cryptography/encryption scheme to provide the data authenticity and security. Multiple messages have been embedded using complimentary modulation function with M–ary modulation. The experimental results have shown that the method is robust against various signal processing attacks. Interleaving and interference cancellation methods are applied to improve the performance of the method as compared to conventional matched filter detection.

Basant et al. [2] proposed a secure spread-spectrum based watermarking algorithms for embedding sensitive medical information such as doctor signature and hospital logo into radiological image for identity authentication purposes. These watermarking schemes used watermarks in binary image format only. In this method, different watermark messages are hidden in the same transform coefficients of the cover image using PN code. Performance of the method has been analyzed by varying the gain factor, sub-band decomposition levels, size of watermarks, wavelet filters and medical image modalities. The simulation results have shown that the proposed method achieved higher security and robustness against JPEG attacks. Also, they proposed another algorithm [5] based on spread-spectrum technique in which, two different pseudo noise (PN sequence) vectors of size identical to the size of each sub-band column are generated for each watermark message bit. So, this algorithm enhanced the watermarking capacity when compared with previous algorithm as proposed in [2]. Performance of the spread-spectrum based watermarking algorithm [5] has been tested for text watermark in [10]. The algorithm is applied for embedding text file represented in binary arrays using ASCII code into host digital radiological image for potential telemedicine applications. In order to enhance the robustness of text watermarks like patient identity code, BCH (Bose, Ray-Chaudhuri, Hocquenghem) error correcting code (ECC) is applied to the ASCII representation of the text watermark before embedding. Robustness and performance of the scheme was tested against some known signal processing attacks like compression, filtering, channel noise, sharpening, and histogram equalization.

Singh et al. [13] presents a robust and secure digital watermarking scheme for its potential application in tele-medicine. The algorithm embeds different medical text watermarks into selected sub-band DWT coefficients of the cover medical image using spread-spectrum technique. In the embedding process, the cover image is decomposed up to third level DWT coefficients. Three different text watermarks are embedded into the selected horizontal and vertical sub band DWT coefficients of the first, second and third level

The medical image watermarking approaches in general have focused on achieving secure and bandwidth efficient transmission of medical data. Multiple watermarking of medical images aims to simultaneously embed various types of medical watermarks on the cover medical image addressing the issues of data security, data compaction, unauthorized access and temper proofing. The proposed multiple watermarking method attempts to simultaneously address these issues consisting of different characteristics and requirements which provide effective protection mechanism for the authenticity of patient identity in the application.

6.3 Main Contribution of the Work

The objective of this method is to provide a valuable solution for different health data management issues to involve hiding multiple watermarks within cover medical image and hidden watermarks can be later recovered at the receiver side for purposes of ownership verification and unique authentication. In order to presents a secure spread-spectrum based multiple watermarking method for medical images in wavelet transform domain. Two different watermarks in the form of image and text are embedding simultaneously into medical cover image. The algorithm uses pseudo-noise (PN) sequences of each image watermark bit, which are embedding column wise into the selected DWT sub-bands coefficients. The selection of the wavelet coefficients for embedding is done by thresholding the coefficient values present in that column. In the embedding process, the cover image is decomposed at second level DWT. The image and text watermark are embedded into the selective coefficients of the first level and second level DWT respectively. In order to enhance the robustness of text watermarks, an error correcting code is applied to the ASCII representation of the text watermark before embedding. The results are obtained by varying the gain factor, sub-band decomposition levels, size of watermark, and different cover images.

The performance of the proposed watermarking method is analyzed against known attacks. The method was found to be robust against such attacks. In addition, the performance of the proposed method has been extensively evaluated for the text watermark along with BCH code and encryption techniques which is presented in Sects. 6.1 and 6.6.2, respectively. The encoded/encrypted text watermark is then embedded at multiple levels of the DWT sub-bands. The performance of the methods are compared with other reported techniques and have been found to be giving superior performance in terms of robustness, imperceptibility, embedding capacity and security as suggested by other authors. Moreover, the performance of the multiple watermarking method is also tested with encryption and BCH error correction code simultaneously in Sect. 6.3. The encryption and BCH error correction code both are applying to the sensitive patient data/report before embedding in to the medical cover image to enhance the security and robustness of the text watermark respectively. The performance of the technique is extensively evaluated and experimental results demonstrated that the method is robust, higher imperceptible, large embedding capacity, and secure than other reported technique.

6.4 Spread-Spectrum Watermark Design

There are two components to build a strong watermark: the *watermark structure* and the *insertion strategy*. For a watermark to be robust and secure, these components must be designed correctly. This can be achieved by placing the watermark explicitly in the perceptually most significant components of the data. Once the significant components are located, Gaussian noise is injected therein. The choice of this distribution gives resilient performance against collusion attacks (the mixing of several watermarked versions of the same content). The Gaussian watermark also gives strong performance in the face of quantization [2].

Watermark Structure: In its most basic implementation, a watermark consists of a sequence of real numbers $X = x_1, x_2, \ldots\ldots x_n$. In practice, a watermark is created where each value x_i is chosen independently according to Gaussian distribution $N(0, 1)$, where $N(\mu, \sigma^2)$ denotes a normal distribution with mean μ and variance σ^2.

Watermarking Procedure: Extract from host digital document D, a sequence of values $V = v_1, v_2, \ldots\ldots v_n$, into which a watermark $X = x_1, x_2, \ldots\ldots x_n$ is inserted to obtain an adjusted sequence of values $W = w_1, w_2, \ldots\ldots, w_n$ and then insert it back into the host in place of V to obtain a watermarked document (D^*).

Inserting Watermark: When X is inserted into V to obtain W, a scaling parameter k is specified, which determines the extent to which X alters V. The method for computing W is

$$w_i = v_i + \propto x_i$$

The factor α can be viewed as a relative measure of embedding strength which is also known as gain factor (α). A large value of α will cause perceptual degradation in the watermarked document.

Choosing the Length 'n' of the Watermark: The choice of length n indicates the degree to which the watermark is spread out among the relevant components of the host image. In general, as the numbers of altered components are increased the extent to which they must be altered decreases.

Extracting and Evaluating the Similarity of Watermarks: It is highly unlikely that the extracted mark X^* will be identical to the original watermark X. Even the act of re-quantizing the watermarked document for delivery will cause X^* to deviate from X. The similarity of X and X^* is measured by

$$sim\left(X,X^*\right) = \frac{X^*.X}{\sqrt{X^*.X}} \tag{6.1}$$

Many other measures are possible, including the standard correlation coefficient. To decide whether X and X^* match, one determines whether $sim(X, X^*) > T$, where T is some specified threshold. Setting the detection threshold is a classical decision estimation problem.

6.5 Proposed Method

For embedding medical text and image watermarks, a new DWT based spread-spectrum watermarking algorithm is proposed that uses medical image as cover. Dyadic sub-band decomposition is performed on the cover image using Haar wavelet transform. Table 6.1 shows the robustness requirement of EPR data at different sub-bands. This table indicates importance of the data according to robustness required. In the proposed method, the image watermark representing health centre name in binary image format is embedded into intermediate frequency sub-bands (HL1 and LH1) of the first level DWT coefficients and the patient's identity/reference as text watermark is embedded into selected sub-band DWT coefficients (HL2 and LH2) of the second level. The important allocation of watermarks according to robustness and capacity criteria at different sub-band is shown in Table 6.1.

The text watermark of eight characters representing patient identification code is converted into binary format using ASCII codes. In the embedding process, sub-band decomposition of the cover medical image is performed to obtain second level DWT coefficients. Different watermark bits are hidden in the same transform coefficients

Table 6.1 Allocation of watermarks according to robustness and capacity criteria at different sub-band

DWT sub-band	Capacity (embeddable coefficients)	Embedded watermark	
		EPR data	Robustness requirements
LH2	16384	Patient's identity/reference	High
HL2	16384	Patient's identity/reference	High
LH1	65356	Health center logo	Low

of the cover image using uncorrelated codes, i.e. low cross correlation value (orthogonal/near orthogonal) among codes. For each message (text and image) bit, two different pseudo noise (PN) sequence vectors of sizes identical to the size of DWT column vector are generated. A PN sequence is a sequence of binary numbers which appears to be random, but is in fact perfectly deterministic. The sequence appears to be random in the sense that the binary values and groups or runs of the same binary value occur in the sequence in the same proportion. PN sequences are a good tool for watermarking because of the following reasons [14]:

(i) PN sequence is having correlation properties, noise like characteristics and resistance to interference.
(ii) PN generator produces periodic sequences that appear to be random.
(iii) PN sequences are generated by an algorithm that uses an initial seed.
(iv) The PN sequence generated is actually not statically random but will pass many test of randomness.
(v) Unless the algorithm and seed are known, the sequence is impractical to predict.

Since, the security level of the watermarking algorithm depends on the strength of its secret key, a gray scale image of size 1 × 35 is used as a strong key for generating pseudorandom sequences.

Based on the value of the bit of the message vector, the respective two PN sequence pairs are then added/subtracted to/from selective columns of wavelet coefficient. This selection is done by thresholding the coefficient values present in that column. In each selected sub-band, the complete coefficient range is grouped in ten equally spaced bins. The bin having the maximum number of coefficients is chosen for embedding. The embedding procedure of the proposed method is shown in Fig. 6.1.

The column wise DWT coefficients of second level horizontal and vertical subbands are taken for embedding. In each column, the coefficients under the threshold criteria are used for embedding and rest of the coefficients remains unchanged. Example embedding process illustrated in Fig. 6.1 shows that values of the coefficients S_2 and S_3 are changed after watermarking as these values lie inside the threshold range while values of coefficient S_1 and S_4 lying outside the threshold criteria remain same. The wavelet coefficients of cover image are divided into *k* number of *bins* having equal width for desired level. From these *k* numbers of *bins*, *max_bin*, having maximum number of coefficients is selected. In medical images, DWT coefficients are mostly concentrated toward the origin. Thus, *max_bin* has coefficients concentrated toward origin.

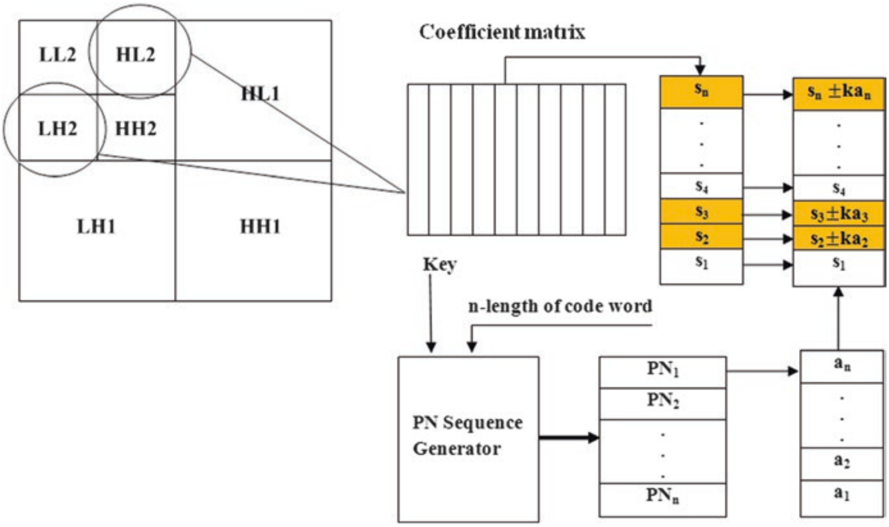


Fig. 6.1 Embedding process of PN sequence in the proposed method

$$\text{Width of each } bin = \frac{\text{maximum coefficient} - \text{minimum coefficient}}{k}$$

b_1 *and* b_2 are the minimum and maximum values within *max_bin.* In each column, the coefficients under the threshold criteria are used for embedding the data bit as follows:

$$W = V + \alpha X \text{ if } b = 0$$

$$W = V - \alpha X \text{ if } b = 1$$

where V is DWT coefficient of the cover image, W is the modified DWT coefficient after watermark embedding, α is the gain factor, X is the PN matrix and b is the message bit that has to be embedded. The corresponding column of the DWT coefficient, to which the generated sequence has to be added/subtracted, is decided by the following relation:

$$p = \begin{cases} \text{modulo}\left(d, \frac{N}{4}\right) \text{if modulo}\left(d, \frac{N}{4}\right) \neq 0 \\ \frac{N}{4}, \qquad \text{else} \end{cases}$$

where p is the column in which sequence has to be added, N/4 is the number of columns in coefficient matrix. Generation of a pair of PN sequences for embedding each bit enhances the security of the watermarking algorithm. In the next subsection process for the embedding of message is discussed.

6.5.1 Message Embedding Algorithm

1. Read the cover image I(M,N) of size M × N.
2. Read the *message* to be hidden and convert it into binary sequences D_d (d=1 to n).
3. Transform the host image using "*Haar*" wavelet transform and get first and second level sub-band coefficients.
4. Generate *n* different PN sequence pairs (PN_h and PN_v) each of $\frac{M}{4}\times 1$ using a secret key to reset the random number generator.
5. for d = 1 to n,

$$p = \begin{cases} \text{modulo}\left(d, \frac{N}{4}\right) & \text{if modulo}\left(d, \frac{N}{4}\right) \neq 0 \\ \frac{N}{4}, & \text{else} \end{cases}$$

Case 1: When message vector bit=0
Hence $1 \leq p \leq (N/4)$, For i=1 to (M/4)

$$ccH(\text{i,p}) = \begin{cases} ccH(\text{i,p}) + \alpha \times PN_{h(i,d)} \text{ if } \text{b}1 < ccH1(i,p) < b2 \\ ccH(\text{i,p}) & \text{otherwise} \end{cases}$$

$$ccV(\text{i,p}) = \begin{cases} ccV(\text{i,p}) + \alpha \times PN\_\text{v}(\text{i,d}) \text{if b}1 < ccV1(i,p) < b2 \\ ccV(\text{i,p}) & \text{otherwise} \end{cases}$$

Case 2: When message vector bit=1
Hence $1 \leq p \leq (N/4)$, For i = 1 to (M/4)

$$ccH(\text{i,p}) = \begin{cases} ccH(\text{i,p}) - \alpha \times PN\_\text{h}(\text{i,d}) \text{if b}1 < ccH1(i,p) < b2 \\ ccH(\text{i,p}) & \text{otherwise} \end{cases}$$

$$ccV(\text{i,p}) = \begin{cases} ccV(\text{i,p}) - \alpha \times PN\_\text{v}(\text{i,d}) \text{if b}1 < ccV1(i,p) < b2 \\ ccV(\text{i,p}) & \text{otherwise} \end{cases}$$

where α is the gain factor used to specify the strength of the embedded data.

6. Apply inverse "Haar" Wavelet transform to get the final watermarked image$I_w(M, N)$.

6.5.2 Message Extraction Algorithm

The DWT coefficients of watermarked image are divided into k number of bins having equal width for desired level. From this k number of bins, *max_bin*, having maximum number of coefficients is selected. To detect the watermark the same PN sequence vectors used during insertion of watermark are generated by using same state key and determine their correlation with the corresponding selected column's detail sub-bands DWT coefficients. Average of n correlation coefficients corresponding to each PN sequence vector is obtained for both LH and HL sub-bands. Mean of the average correlation values are taken as threshold, T for message extraction. During detection, if the average correlation exceeds T for a particular sequence a "0" is recovered; otherwise a "1". The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered. For extracting the watermark, following steps are applied to the watermarked image:

1. Read the watermarked image $I_w(M, N)$
2. Transform the stego image using "Haar" Wavelet transform and get first and second level sub-band coefficients.
3. Generate one's sequences (*msg*) equal to message vector (from *1* to *n*).
4. Generate n different PN sequence pairs (PN_h1 and PN_v1) each of size $\frac{M}{4} \times 1$ using same secret key used in embedding to reset the random number generator.
5. for $d = 1$ to n, Generate PN_h2(d) and PN_v2(d) as

   for $i = 1$ to (M/4)

$$PN\_\mathrm{h2}(\mathrm{i,d}) = \begin{cases} PN\_\mathrm{h1}(\mathrm{i,d}) \text{if } \mathrm{b1} < ccH1(\mathrm{i,p}) < b2 \\ 0 \quad \text{else} \end{cases}$$

$$PN\_\mathrm{v2}(\mathrm{i,d}) = \begin{cases} PN\_\mathrm{v1}(\mathrm{i,d}) \text{if } \mathrm{b1} < ccV1(\mathrm{i,p}) < b2 \\ 0 \quad \text{else} \end{cases}$$

6. Calculate the correlations between the values ccH1 and PN_h2 and store in *corr_H (d)* and ccV1 and PN_v2 *corr_V (d).*

   corr_H (d) = correlation between PN_h2 (d) and ccH1 (p^{th} column)
   corr_V (d) = correlation between PN_v2 (d) and ccV1 (p^{th} column)

$$\mathrm{p} = \begin{cases} \mathrm{modulo}\left(\mathrm{d}, \frac{\mathrm{N}}{4}\right) \text{if modulo}\left(\mathrm{d}, \frac{\mathrm{N}}{4}\right) \neq 0 \\ \frac{\mathrm{N}}{4}, \quad \text{else} \end{cases}$$

   Hence $1 \leq p \leq \frac{N}{4}$

7. Calculate average correlation avg_corr (*d*) = (corr_H (*d*)+corr_V(*d*))/2
8. Calculate the corr(mean) = mean of all the values stored in avg_corr (*d*).
9. Extract the watermark bit stream, using the relationship given below

```
for d = 1 to n
if avg_corr (d) > corr (mean)
Msg (d) = 0.
```

10. Convert the bit sequence to *message watermark* to get the recovered watermark.

6.6 Experimental Results and Performance Analysis

In this section, the performance of combined DWT-SS watermarking algorithm is extensively evaluated for multiple watermarks in the form of image and text. The gray–level MRI image of size 512 × 512 [15] is taken as the cover image. The health centre logo of "NITK" as image watermark and patient's identity/reference "MRI_1031" as text watermarks. Also, BCH code is applied to the ASCII representation of the text and the encoded text watermark is then embedded. The resulting bits are embedded in two different ways: without ECC and coded by BCH (127, 64) ECC code. The encoded text watermark length for BCH is 127 bits. Strength of watermark is varied by varying the gain factor (α) in the watermarking algorithm. For testing the robustness and quality of the watermarked image of the proposed scheme MATLAB is used. The quality of the watermarked image (as shown in Fig. 6.2) is evaluated by the parameter PSNR and robustness by NC (for image) and BER (text). Figure 6.2 shows the cover MRI image and watermarked images obtained at different gain factors. Extracted watermarks along with the original watermarks are shown in Fig. 6.3. Figure 6.4 shows that larger size watermarks are more clearly identified during extraction.

In the experiments, we are using the gain factor (α) as 1.0 to 5.0 and the value of PSNR, NC and BER are illustrated in Table 6.2, 6.3, 6.4 and 6.5. The performance of the proposed method is better in comparison with the existing [2, 5] method shown in the Table 6.6. In Table 6.2, BCH code performance (determined PSNR and NC values) up to 127 text bits has been evaluated without any noise attack. The maximum PSNR value is 31.92 dB and BER = 0.0472 at α = 1.0 to 5. Figure 6.5 shows the comparison of BER performance as obtained by the proposed method using/without using BCH code. Table 6.3 shows the NC and BER performance of the proposed method against eight different attacks. The highest NC value of 0.7402 has been obtained against the Histogram equalization attack however; the lowest NC is 0.2162 against the Median Filtering attack. The highest BER is obtained as 0.0551 against the Median Filtering attack. However, without BCH code it was 0.0629 for the same attack. It is observed that larger the gain factor, stronger is the robustness and smaller the gain factor, better is the image quality.

Figure 6.6 shows the graphical representation of the BER performance obtained by the proposed method with and without BCH code against different attacks. Table 6.4 shows the effect of watermark size on the PSNR, NC and BER

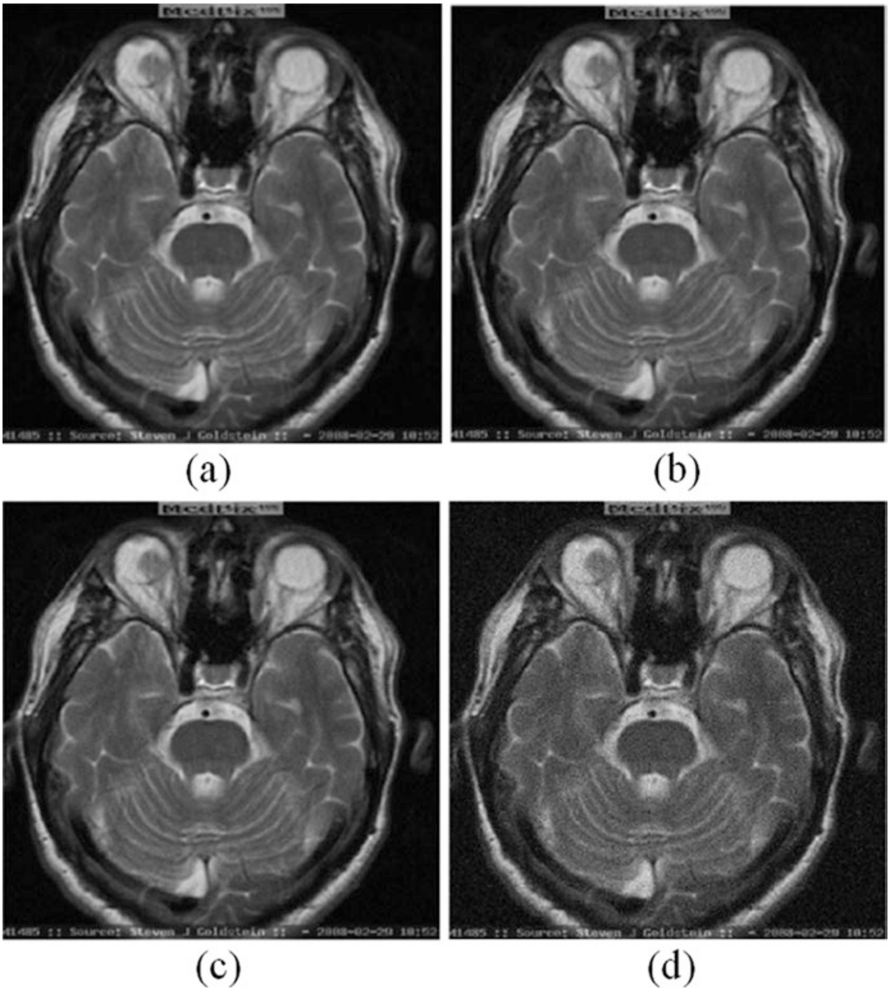


Fig. 6.2 Original and watermarked MRI images (**a**) original image and watermarked images with gain factor; (**b**) 1.0; (**c**) 1.5 and (**d**) 5.0

performance of the proposed watermarking method. It is found that PSNR performance of the watermarked image decreases with the increase in the size of the watermark, but subsequently an improvement in the correlation between original and extracted watermarks is observed. Table 6.5 shows the effect of cover image at $\alpha = 1.5$ on PSNR, NC and BER. The highest NC and BER value were obtained with Ultrasound and MRI image respectively. However, the highest PSNR value (29.82 dB) has been obtained with MRI image. Table 6.6 provides the comparison of PSNR and NC performance obtained by the proposed technique with other reported methods. The maximum NC value with proposed method has been obtained as 0.7544 against 0.659 and 0.3572 obtained by Basant et al. in [2, 5], respectively.

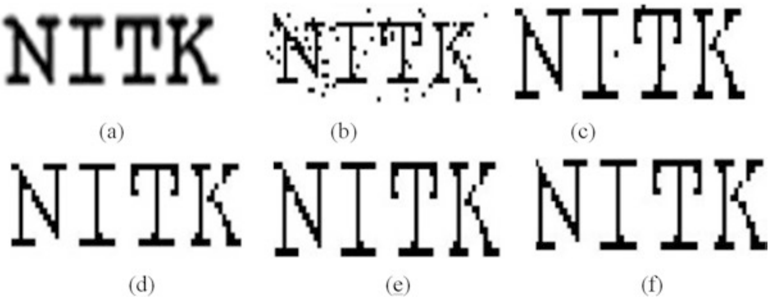


Fig. 6.3 Image watermark (**a**) original and recovered watermark with gain factor α = (**b**) 0.5; (**c**) 1.0; (**d**) 2.5; (**e**) 4.0 and (**f**) 5.0

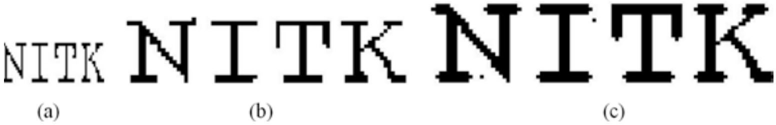


Fig. 6.4 Recovered watermark of different size at gain factor = 5 (**a**) 64 × 20; (**b**) 80 × 25; (**c**) 99 × 31

Table 6.2 Effect of BCH coding on PSNR and BER at different gain factors

	Without using BCH coding		Using BCH coding	
Gain factor (α)	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)
1.0	32.48	0.0629	31.92	0.0472
1.5	29.82	0.0551	28.55	0.0314
2	27.15	0.0472	26.14	0.0314
2.5	25.29	0.0314	24.29	0.0157
3	23.12	0.0078	22.77	0
4	21.94	0.0078	20.40	0
5	19.73	0.0078	18.57	0

The maximum PSNR value obtained with [2, 5] methods are 37.518 dB and 52.04 dB respectively. However, the maximum PSNR value by the proposed method is 37.75 dB. Overall, the proposed method is better than the existing methods [2, 5]. Figure 6.7 shows the graphical representation of the comparison of robustness (determined NC values) offered by the proposed method with that of [2] at different gain factors.

Table 6.3 Effect of BCH coding on NC and BER against different attacks at gain factor (α) = 5

	Without using BCH coding		Using BCH coding	
Attacks	Image watermark (NC value)	Text watermark (BER value in %)	Image watermark (NC value)	Text watermark (BER value in %)
JPEG compression (QF = 10)	0.5306	0.0551	0.5413	0.0314
JPEG compression (QF = 20)	0.7218	0.0393	0.7247	0.0236
JPEG compression (QF = 30)	0.7335	0.0236	0.7335	0
JPEG compression (QF = 50)	0.7364	0.0314	0.7364	0
JPEG compression (QF = 70)	0.7394	0.0236	0.7394	0
JPEG compression (QF = 90)	0.7394	0.0157	0.7394	0
Sharpening mask (threshold = 0.1 and 0.9	0.7394	0.0629 and 0.0472	0.7364	0.0314 and 0
Median filtering [2 2] and [3 3]	0.6736 and 0.2216	0.0629	0.6662 and 0.2162	0.0551 and 0.0472
Scaling factor 2	0.7394	0.0157	0.7364	0
Scaling factor 2.5	0.7394	0.0314	0.7364	0
Scaling factor 5	0.7335	0.0472	0.7335	0.0078
Gaussian LPF (standard deviation = 0.6 and 0.9)	0.7394 and 0.7102	0.0236 and 0.0472	0.7364 and 0.7102	0 and 0.0393
Gaussian noise (mean = 0,Var = 0.01)	0.7335	0.0629	0.7394	0.0157
Gaussian noise (mean = 0,Var = 0.05)	0.6964	0.0551	0.6994	0.0472
Salt & pepper noise (density = 0.02)	0.7391	0.0314	0.7394	0
Salt & pepper noise (density = 0.1)	0.7155	0.0629	0.7072	0.0472
Histogram equalization	0.7394	0	0.7402	0

Table 6.4 Effect of different size of image watermark on PSNR, NC and BER at gain factor (α) = 1.5

	Without using BCH coding		
Watermark size	PSNR (dB)	NC	BER (%)
64 × 20	29.82	0.7394	0.0551
80 × 25	27.03	0.7396	0.0472
99 × 31	23.94	0.9621	0.0472

6.6.1 *Performance Evaluation of the Proposed Method for Text Watermarking Using BCH Code*

In this subsection, the performance of the above discussed method has been extensively evaluated for text watermark only using BCH code. During the embedding process, the cover image is decomposed up to third level DWT coefficients. For identity authentication purposes, the method uses three different watermarks

Table 6.5 Effect of different cover image on PSNR, NC and BER at gain factor (α) = 1.5

	Without using BCH coding		
Cover image	PSNR (dB)	NC	BER (%)
MRI	29.82	0.7394	0.0551
CT Scan	28.91	0.7384	0.0472
Ultrasound	28.7	0.7395	0.0157

Table 6.6 The comparison results under PSNR and NC value at different gain factors

	Basant et al. [2]		Basant et al. [5]		Proposed method	
Gain factor (α)	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC
0.5	37.518	0.376	Not reported		37.75	0.6148
1	31.497	0.535	52.04	0.0805	31.92	0.7276
3	21.955	0.657	Not reported		22.77	0.7398
4	19.456	0.659	Not reported		20.4	0.741
5	Not reported		39.02	0.3572	18.57	0.7544

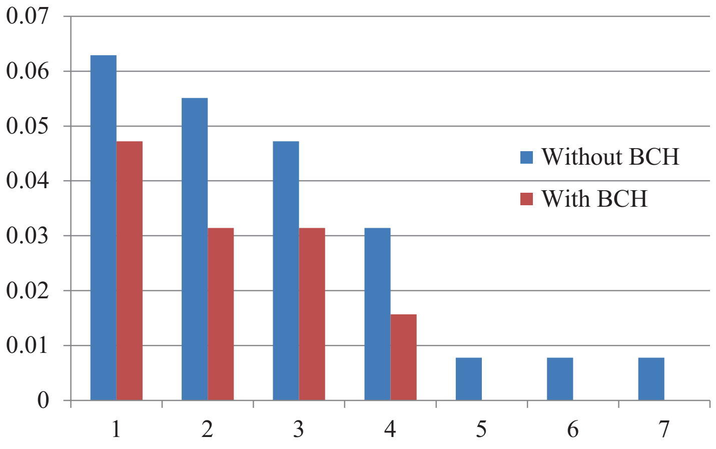


Fig. 6.5 BER performance of the proposed method at different gain factors

representing the text watermark such as personal and medical record of the patient, diagnostic/image codes and doctor code/ signature. According to the importance of robustness requirements, three different text watermarks are embedded into the selected horizontal and vertical sub-band DWT coefficients of the first, second and third level, respectively. Selection of these coefficients for embedding purpose is based on threshold criteria defined above in the chapter. It is found that the proposed scheme correctly extracts the embedded watermarks without error and provides high degree robustness against known attacks while maintaining the imperceptibility of watermarked image.

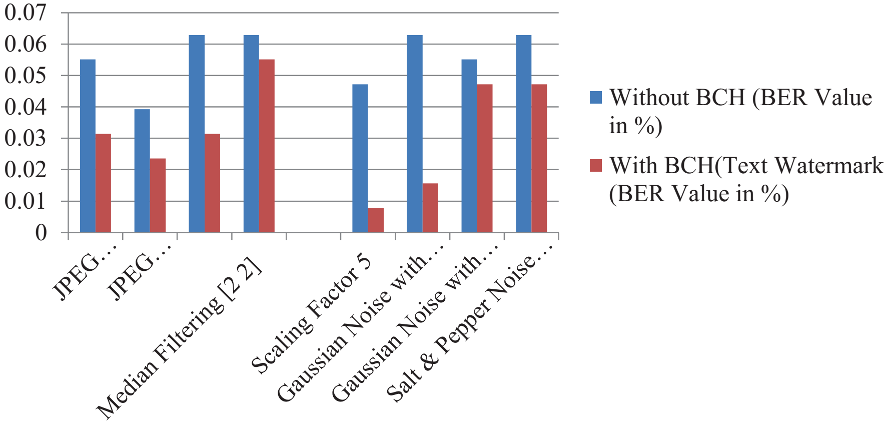


Fig. 6.6 BER performance of the proposed method against different attacks

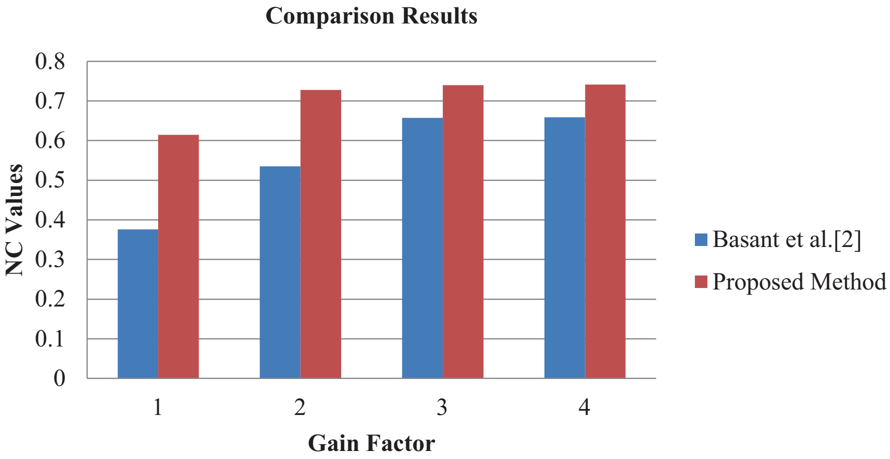


Fig. 6.7 Comparison results under NC values at different gain factors

In this method, the doctor's identification code of eight characters, image/diagnostic code of eight characters and patient name of eight characters are embedded into third level HL3 and LH3 sub-bands, second level HL2 and LH2 sub-bands and the first level HL1 and LH1 sub-bands respectively. Also, BCH error correcting code is applied to the ASCII representation of the text and the encoded text watermark is then embedded into the cover medical images. The resulting bits are embedded in two different ways: without ECC and coded by BCH (127, 64) code. Performance of the proposed method has been extensively evaluated against known attacks and results are compared with other technique [10]. The proposed method gives superior robustness performance without significant degradation of the image quality of the watermarked image. The encoded text watermark length for BCH is

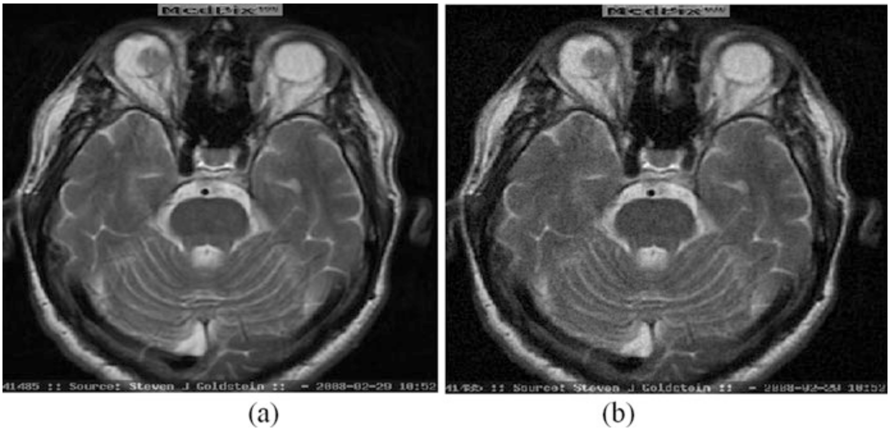
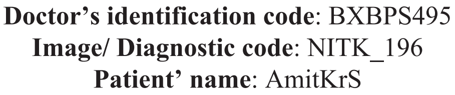

MedPix
41485 :: Source: Steven J Goldstein :: - 2008-02-29 10:52
MedPix
41485 :: Source: Steven J Goldstein :: - 2008-02-29 10:52
(a) (b)

Fig. 6.8 (**a**) Cover image (**b**) Watermarked image at gain factor (α) = 15

Fig. 6.9 Extracted text watermark at gain factor (α) = 15


Doctor's identification code: BXBPS495
Image/ Diagnostic code: NITK_196
Patient' name: AmitKrS

381 bits. The strength of the watermark is tested by varying the gain factor (α) in the watermarking algorithm. Imperceptibility performance of the scheme is evaluated by calculating the PSNR between cover image and watermarked image where as robustness performance is measured by calculating BER between original and the extracted watermark.

Fig. 6.8 shows original MRI image and watermarked image at α = 15. Figure 6.9 shows the extracted watermark image at α = 15. PSNR and BER performance of the proposed watermarking scheme with and without BCH coder are illustrated in Table 6.7. Referring this table it is observed that the highest PSNR obtained without and with BCH coder are 43.96 dB and 40.48 dB respectively (at α = 5) whereas BER obtained without and with BCH coder are 0.0236 and 0.0183 respectively. It is also observed that the watermarking scheme with BCH coder achieves desired '0' BER at gain factor of 15 but its PSNR performance is slightly compromised i.e. 29.46 dB as compared to 34.95 dB achieved without coder.

In Table 6.8, robustness performance of the proposed algorithm with and without BCH coder has been tested at α = 10 against different attacks. With BCH coder, BER value = 0 is obtained against JPEG compression (Quality Factor (QF) = 90) whereas without BCH code it comes out to be 0.0052. It is also observed from the table that the implementation of BCH coder improves the BER performance for sharpening mask noise attack with threshold = 1. Table 6.9 shows PSNR and BER performance of the proposed algorithm for different imaging modalities at varying gain factor. It is observed that Ultrasound image gives maximum PSNR = 41.30 dB at gain factor of 5 whereas minimum BER value = '0' is obtained with MRI image at gain factor of 11. Table 6.10 provides the performance (determined PSNR and

Table 6.7 PSNR and BER performance of the proposed method with and without BCH code

	Without using BCH coding		Using BCH coding	
Gain factors (α)	PSNR (dB)	BER value (%)	PSNR	BER value (%)
5	43.96	0.0236	40.48	0.0183
10	38.43	0.0078	31.31	0.0052
15	34.95	0.0052	29.46	0
20	32.66	0	29.01	0

Table 6.8 BER performance of proposed method with and without BCH code against different attacks at gain factor (α) = 10

	Without using BCH coding	Using BCH coding
Attacks	BER value (%)	BER value (%)
JPEG compression (QF = 90)	0.0052	0
JPEG compression (QF = 50)	0.0183	0.0131
JPEG compression (QF = 30)	0.0157	0.0183
JPEG compression (QF = 15)	0.0367	0.0314
JPEG compression (QF = 5)	0.0629	0.0603
Sharpening mask (threshold = 1.0)	0.0052	0
Median filtering [2 2] and [3 3]	0.0236 and 0.0446	0.0183 and 0.0367
Gaussian LPF (standard deviation = 0.5)	0.0157	0.0131
Gaussian noise (mean = 0,Var = 0.01)	0.0288	0.0209
Gaussian noise (mean = 0,Var = 0.1)	0.0367	0.0314
Salt & pepper noise (density = 0.001)	0	0
Salt & pepper noise (density = 0.05)	0.0314	0.0262
Motion Blur (Len = 9, Theta = 0)	0.0314	0.0288

BER values) comparison with the existing methods. The maximum BER value with proposed method has been obtained as zero against 1.5306 obtained by Kumar et al. in [10] method. The maximum PSNR value is obtained with this method is 45.51 dB. However, the maximum PSNR value is obtained by the proposed method is 49.12 dB. The existing method [10] can embed only 196 bits only whereas 381 bits can be embedded by the proposed method. Overall, the proposed method is better than the existing method in terms of image quality of the watermarked image, robustness of the extracted watermark and embedding capacity also.

From the above extensive discussion, we have observed some important remarks:

As shown in Table 6.3, the highest value of NC = 0.7402 is obtained for Histogram equalization attack whereas its lowest value of 0.2162 is achieved for median filtering attack. The lowest BER value 0 is obtained for JPEG compression (QF = 30, 50, 70, 90), Sharpening mask (threshold = 0.9), Scaling factor (2 and 2.5), Gaussian LPF (standard deviation = 0.6), Salt and pepper noise (density = 0.02) and Histogram equalization attacks, however, higher value of BER = 0.0551 is observed for median filtering attack. The higher robustness as indicated by NC value = 0.7544 is achieved

Table 6.9 Effect of cover images on PSNR and BER performance at different gain factors

Cover image	Gain factor (α) = 5		Gain factor (α) = 11		Gain factor (α) = 15	
	PSNR (dB)	BER value (%)	PSNR (dB)	BER value (%)	PSNR (dB)	BER value (%)
MRI	40.47	0.0209	33.83	0	31.3	0
CT Scan	41.15	0.0183	34.49	0.0131	31.79	0
Ultrasound	41.3	0.0157	34.65	0	31.95	0

Table 6.10 The comparison results under PSNR and BER value

Gain factor	Kumar et al. [10]		Proposed method	
	PSNR (dB)	BER value (%)	PSNR (dB)	BER value (%)
3	45.51	1.5306	49.12	0
5	41.07	0	45.76	0
10	35.05	0	39.01	0
15	31.53	0	35.35	0

in our proposed method as compared to other reported techniques [2, 5]. Referring Table 6.6 it is seen that maximum value of NC = 0.7544 is achieved at gain factor '∝' = 5 as compared to its corresponding maximum NC values of ‘0.6590’ and ‘0.3572’ in [2, 5] respectively. Further, it is also evident from Table 6.6 that the proposed method offers up to 63.51% superior performance in terms of robustness over reported techniques [2, 5]. The performance of the proposed watermarking method has been extensively evaluated only for text watermark at multilevel DWT sub-bands. This is carried out by applying BCH code on the EPR data as text watermark before embedding into the cover. The BER of the text watermark has been evaluated against different known attacks as in Table 6.8. The BER = 0 is obtained for JPEG compression (QF = 90), sharpening mask (threshold = 1.0) and Salt and pepper noise (density = 0.001), however, higher value of BER = 0.0603 is obtained for JPEG compression attacks (QF = 5). The PSNR and BER performance of the proposed method is also compared with [10] as shown in Table 6.10 from which it is evident that the proposed method offers up to 7.93% enhancement in visual quality of the watermarked image and 1.53% reduction in BER over [10].

6.6.2 *Performance Evaluation of Proposed Method Using Multilevel Encrypted Text Watermarking*

In order to enhance the security of the text watermark, reduce save the massage encryption/decryption time and address the health data management issues, the encrypted text watermark is embedding into the appropriated DWT sub-bands. In this subsection, simultaneous embedding of three watermarks (i.e. doctor code,

Table 6.11 Allocation of watermarks according to robustness and capacity criteria at different sub-band

DWT sub-band	Capacity (embeddable coefficients)	Embedded watermark	
		EPR data	Robustness requirements
LH3	4096	Identification code of the doctor and Patient's diagnostic/image codes	Very high
HL3	4096	Identification code of the doctor and Patient's diagnostic/image codes	Very high
LH2	16384	Patient's medical and personal records	High
HL2	16384	Patient's medical records	High

image reference code and patient record) using multilevel watermarking of cover medical image has been proposed to address the issues of medical data confidentiality, data security, data compaction, unauthorized access and temper proofing. The suggested method uses wavelet based spread-spectrum watermarking where the encrypted text watermarks are embedded at multiple levels of the DWT sub-bands of the cover image. The performance of the developed scheme was evaluated and analyzed against known attacks by varying watermark size and the gain factor. It is found that the proposed multilevel watermarking method enhances the security of the patient data. The advantage of the work is summarized as follows:

(i) *Improved capacity*: The method proposed by Basant et al. [10] and Singh et al. [13] has been embedded 196 and 381 bits respectively. However, in our proposed method we can embed 728 bits (116 characters) with the acceptable performance in terms of robustness and imperceptibility.
(ii) *Enhanced security of the text watermark*: security of the medical text watermark may be enhanced by using simple encryption method to save execution time. For tele-diagnosis, the encryption and decryption speed has become an important factor if the situation demands.
(iii) *Reduced bandwidth requirements*: The EPR data in the form of three different text watermarks are embedding in the same medical cover image which reduce the bandwidth requirements as essential importance in medical applications
(iv) *Health data management*: Further, the proposed method addressing the medical data management issues data security, data compaction, unauthorized access and temper proofing, having different characteristics and requirements. This has been achieved by allocation of watermarks according to robustness and capacity requirements at different DWT sub-band of the cover image. The allocation of the watermarks is presented in Table 6.11 [16].

In this method, the personal and medical record of the patient is embedded into selected sub-bands of the second level. However, identification code of the doctor and patient's diagnostic/image codes of the patient are embedded into selected sub-bands of the third level. The doctor identification and image reference codes are embedded into third level HL3 and LH3 sub-bands, while the patient record is embedded into HL2 and LH2 sub-bands of second level DWT sub-band. Also, encryption is applied to the ASCII representation of the text watermark and the encrypted text watermark is then embedded. Thus, the method enhances security of the text watermark. The encryption method used in the present work is simple to reduce the execution time during encryption and decryption. The EPR data is encrypted and decrypted using the equations 1 and 2, respectively as given in section "Encryption and decryption process for text watermark" of chapter "Robust and Imperceptible Hybrid Watermarking Techniques for Medical Images".

The performance of the proposed watermarking method was tested for encrypted text medical watermark considering gray–level medical images of size 512 × 512 [15] as cover image. Two different text watermarks doctor identification code of ten characters and radiological image reference code of five characters are embedded into third level HL3 and LH3 sub-bands, while the patient record of varying size is embedded into HL2 and LH2 sub-bands of second level DWT as the third watermark. Encryption is applied to the ASCII representation of these text watermarks and the encrypted text watermarks are then embedded providing the extra level of security during embedding process. The strength of watermark is varied by varying the gain factor (α) in the watermarking algorithm. Figure 6.10 shows the cover CT Scan image and watermarked images obtained at different gain factors. Figure 6.11 shows the EPR data using as text watermarks. In the experiment, values of PSNR and BER are illustrated in Tables 6.12, 6.13, and 6.14 for varying gain factors (α) in the range of 5.0 to 15.0.

Table 6.12 shows the effect of gain factor on the performance (determined PSNR and BER values) of the proposed method for different sizes of watermark. With the encryption, maximum PSNR value is 40.02 dB and BER = 0.1538 against maximum size of watermark at $\alpha = 5$. However, PSNR value is 31.05 dB and BER = 0 at $\alpha = 15$.

Table 6.13 shows the effect of encryption on BER performance as obtained by the proposed multilevel watermarking method against ten different attacks. The highest BER value of 0.3846 is obtained against JPEG compression attack with quality factor (QF) = 10 with encryption which is slightly better than the BER performance without encryption (BER = 0.4326). Further, from Table 6.3 it is evident that the proposed technique reduces BER up to 0.124% while providing extra level of security of the text watermark using encryption compared to the method without using the encryption of text watermark.

Table 6.14 shows the effect of cover medical images on PSNR and BER performance as obtained by the proposed method at gain factor (α) = 15. It is observed that the highest PSNR and BER were obtained with MRI image, which is also shown in Figs. 6.12 and 6.13, respectively. Figure 6.14 shows BER performance of the proposed multilevel watermarking method against known attacks at gain factor (α) = 15.

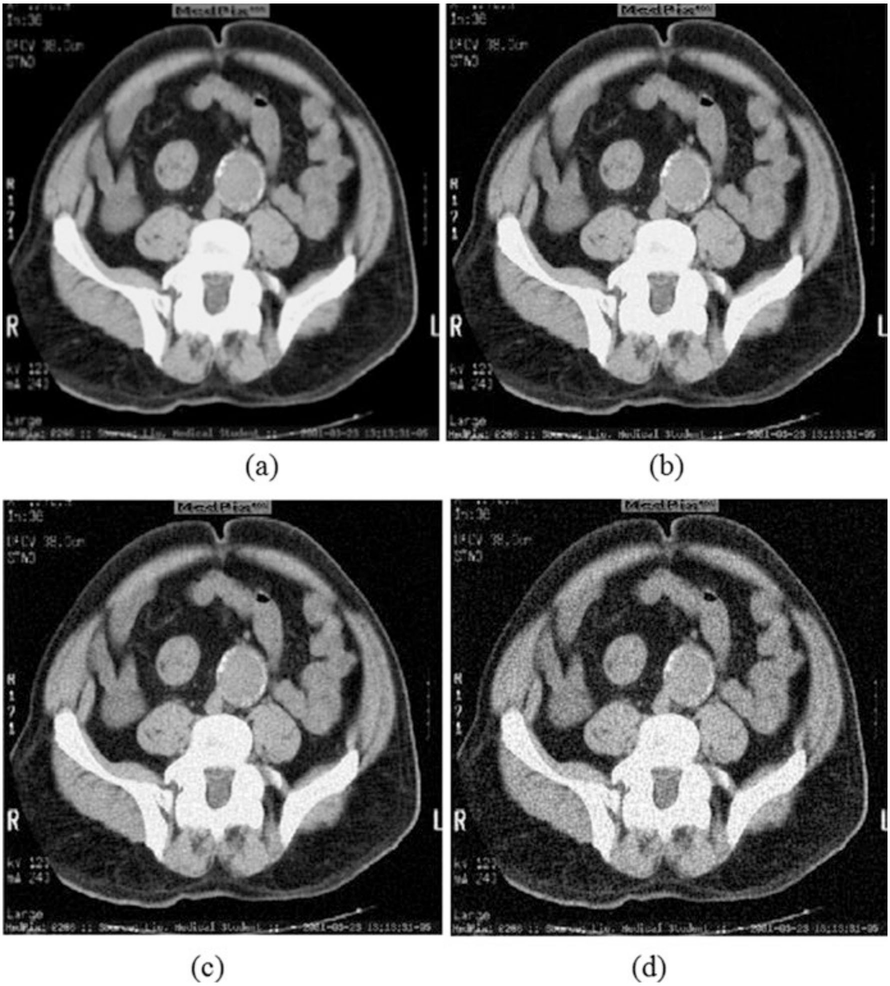


Fig. 6.10 Cover and watermarked CT Scan images (**a**) original image and watermarked images with gain factor; (**b**) 5; (**c**) 15 and (**d**) 40

Doctor's and Image code: BXBPS4951D_NIT01
Patient's Record:
OPD_051_NITKurukshetra_Stroke_amennea_BPositive_AmitSingh_20-05-80_DrBasantKumar_2017

Fig. 6.11 EPR data as text watermark

Table 6.12 Effect of gain factor on PSNR and BER for different sizes of watermark

Gain factor (α)	With encryption				Without encryption			
	104 characters		60 characters		104 characters		60 characters	
	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)
5	40.02	0.1538	42.49	0.0961	40.06	0.1923	42.53	0.1250
10	34.24	0.0576	36.71	0.0288	34.27	0.0769	36.8	0.0480
15	31.05	0	33.29	0	31.08	0.0192	33.32	0.0096

Table 6.13 Effect of encryption on BER for different attacks at gain factor (α) = 15

Attack	With encryption	Without encryption
	BER (%) for 104 characters	BER (%) for 104 characters
JPEG compression (QF = 10)	0.3846	0.4326
JPEG compression (QF = 50)	0.0096	0.0288
JPEG compression (QF = 90)	0	0.0192
Sharpening mask (threshold = 0.2 and 0.1)	0.0192 and 0	0.0288
Median filtering [3 3] and [2 2]	0.0480 and 0	0.0769 and 0.0288
Scaling factor 2.5,1.5 and 0.5	0.0769, 0.0576 and 0	0.1057, 0.0673 and 0.0288
Motion Blur (len = 2 and theta = 9)	0.0192	0.0192
Motion Blur (len = 1 and theta = 9)	0	0.0192
Disk (radius = 1)	0.0288	0.0480
Disk (radius = 0.5)	0	0.0192
Gaussian LPF (standard deviation = 0.2,0.5 and 0.9)	0, 0.0096 and 0.0673	0.0192, 0.0192 and 0.0865
Gaussian noise (mean = 0,Var = 0.05)	0.0769	0.1057
Gaussian noise (mean = 0,Var = 0.01)	0.0288	0.0480
Gaussian noise (mean = 0,Var = 0.005)	0	0.0192
Salt & pepper noise with (density = 0.05)	0.0961	0.1153
Salt & pepper noise (density = 0.01)	0.0288	0.0384
Salt & pepper Noise (density = 0.005)	0	0.0192
Histogram equalization	0.0961	0.1250

Table 6.14 PSNR and BER performance using different cover images at gain factor (α) = 15

Cover image	With encryption	
	PSNR (dB)	BER (%)
CT Scan	31.03	0
Ultrasound	30.37	0
MRI	31.23	0.0480

Fig. 6.12 PSNR performance of proposed method using different cover images

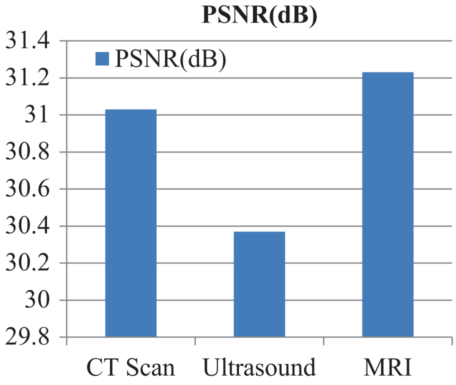
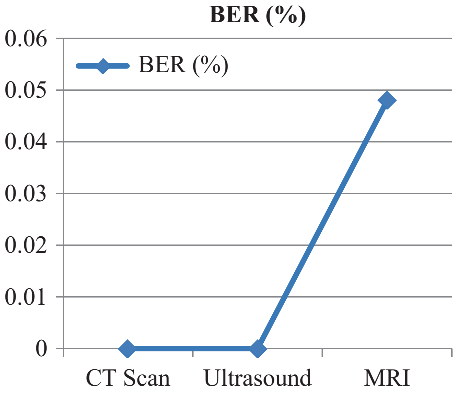


Fig. 6.13 BER performance of the proposed method using different cover images



6.6.3 Performance Evaluation of the Proposed Method for Image and Text Watermarking Using Encryption and BCH Code Simultaneously

The performance of the method is also tested for multiple watermarks using encryption and BCH code simultaneously. For the extensive analysis of the proposed work, we have tested the method with some minor changes as follows:

1) The methods discussed in Sects. 6.1 and 6.2 using threshold criteria for the embedding purpose. However, the watermark bits are embedding here without using the threshold criteria.
2) The method using the same algorithm for image watermark, as disused in Sect. 6.5. However, the text watermark embedding and extraction process is different, as discussed detail in [17].

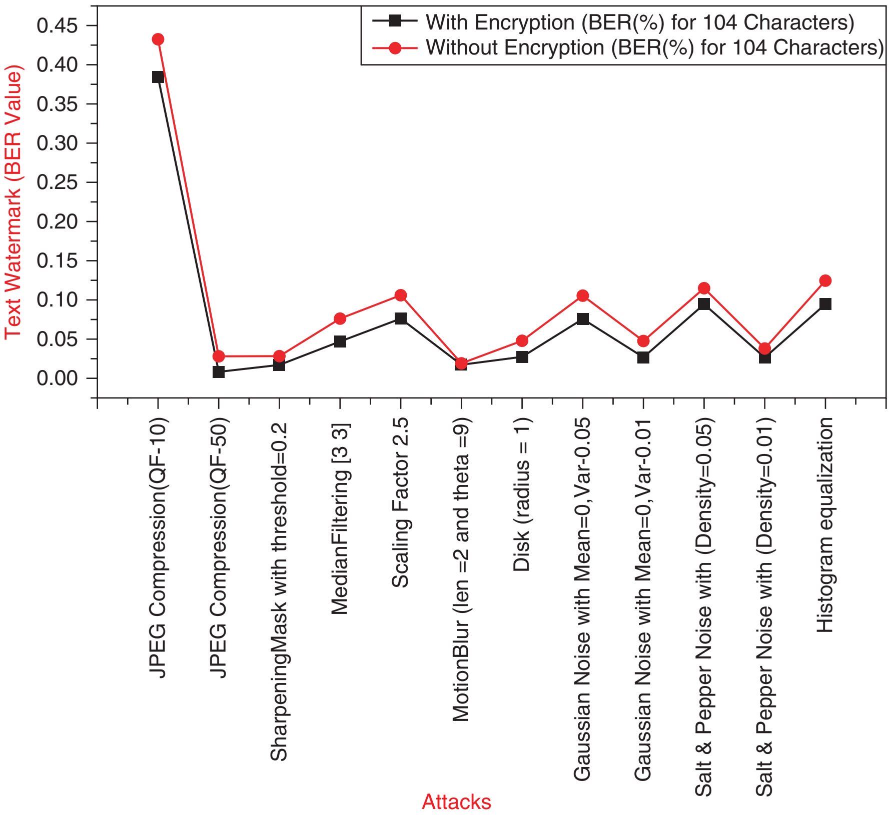


Fig. 6.14 BER performance of the proposed method against known attacks

In this context, the method adopts to extend two existing single watermarking techniques [5, 17] to achieve several goals in medical image watermarking like security, high capacity and robustness. Figure 6.15 show the embedding process of the proposed technique. The proposed dual watermarking algorithm embeds *health centre's logo as image watermark* using spread spectrum watermarking technique and embedding of sensitive *patient's information* as text watermark (up to 150 Characters) into the high frequency component (HH2 Sub-band) of the DWT cover image is considered.

Further, the proposed dual watermarking method is embedding two different watermarks in cover medical image simultaneously, which has fewer constraints than the other two dual watermarks methods [18–20]. The main contribution of the work is summarized as follow:

(i) *Dual watermarking and improved capacity*: The method reported in [6, 21–29] has embedded only one watermark. The proposed technique is embedding multiple watermarks simultaneously in non-interfering way [20] to enhance the security and capacity of the hidden watermark and reduce the bandwidth

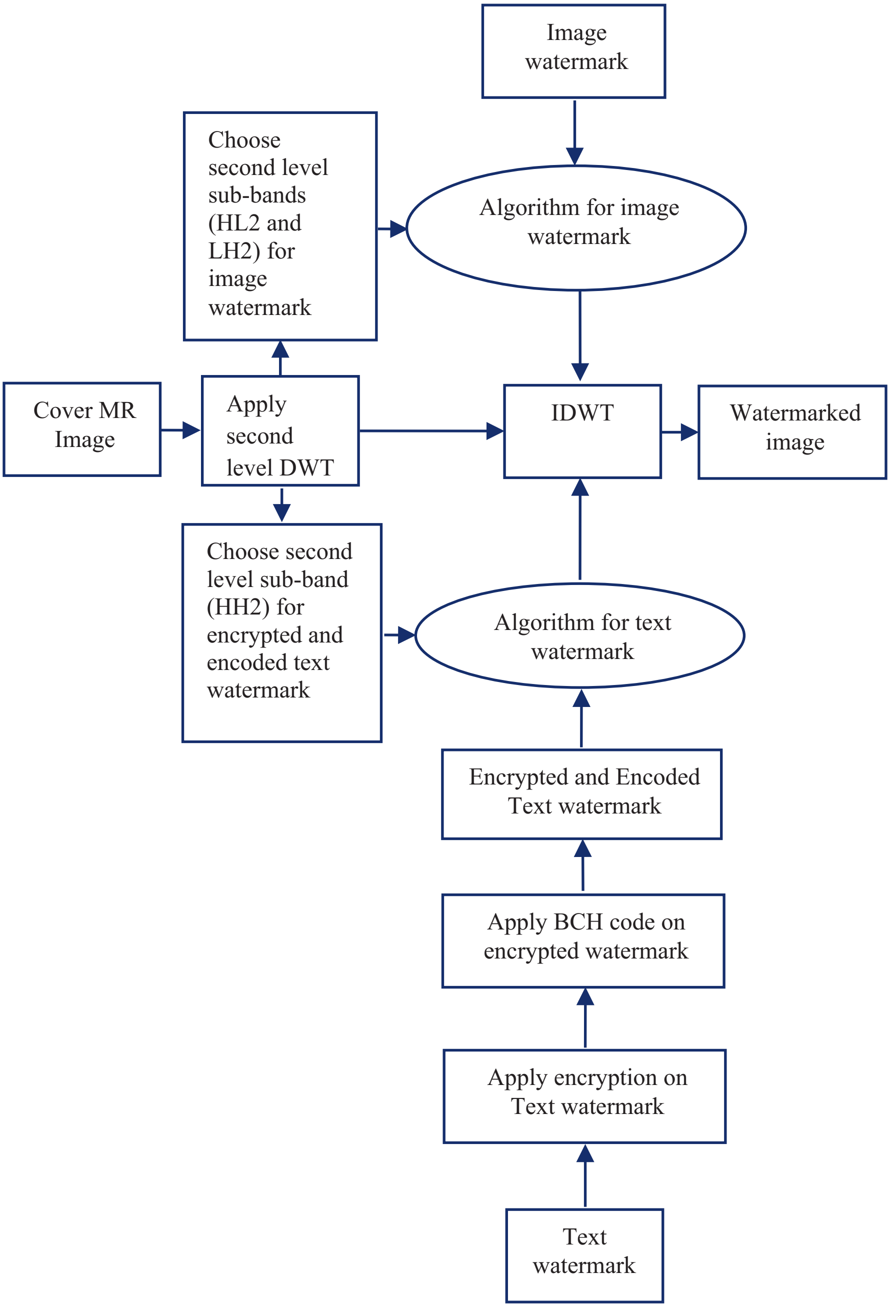


Image watermark
Choose second level sub-bands (HL2 and LH2) for image watermark
Algorithm for image watermark
Cover MR Image
Apply second level DWT
IDWT
Watermarked image
Choose second level sub-band (HH2) for encrypted and encoded text watermark
Algorithm for text watermark
Encrypted and Encoded Text watermark
Apply BCH code on encrypted watermark
Apply encryption on Text watermark
Text watermark

Fig. 6.15 Proposed dual watermark embedding method

and storage requirements for medical applications. The proposed technique can embeds up to 150 characters with acceptable visual quality of the watermarked image. However, the methods reported in [10, 13, 16] can embed only 196 bits, 381 bits and 728 bits respectively.

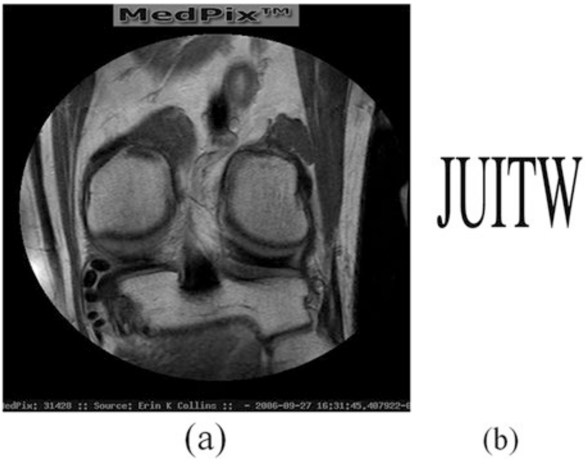
(ii) *Improved performance*: In Table 6.18, robustness and security performance of text watermark have been improved using encryption technique and BCH channel coding. Further, the encryption technique [14] along with BCH coding based method is compared with only BCH coding based method and performance of the proposed scheme has been observed in terms of robustness of the image and text watermark against different signal processing attacks. The proposed method using the combination of encryption and watermarking to protecting the sensitive patient data.

(iii) The proposed technique is also addressing the *health data management issue* [14, 16] in which more important patient/doctor data is embedding at higher level DWT and the less important data is embedding at lower level DWT.

The PSNR NC and BER Performance of the proposed dual watermarking algorithm is extensively evaluated for medical data. The 8-bit grey scale MR image of size 512 × 512 [15], health centre's logo of different sizes and patient's information of 150 characters and are considered as cover image, image and text watermark respectively. The perceptual quality (as determined by PSNR) of the cover image with hidden watermark and the robustness of the extracted watermarks (as determine by NC for image and BER for text watermark) is evaluated at varying gain factors. We have noticed that the perceptual quality is better at lower gain factor, however, stronger the robustness at higher gain values. In BCH error correcting code, redundant bit information is added in binary sequence such that error is distributed over redundant bits and hence, the BER value in the extraction process is reduced. Figure 6.16a, b show the cover MR and watermark health centre logo image respectively. Figure 6.17a–c presents the watermarked images at different gain factors. Figure 6.18 show the patient data as text watermark.

Table 6.15 shows the PSNR and NC performance of the proposed dual watermarking method at different gain factors using varying number of characters. The highest PSNR (38.63 dB) has been obtained for the maximum size of the text watermark (151 characters) at gain = 1. However, highest NC (0.8673) has been obtained for the same size of the text watermark at gain = 7. Referring this table, it is observed that PSNR decreases for increasing number of characters embedded and chosen gain factors. However, robustness (NC values) of the image watermark is increasing at higher gain factors. In addition, the value of gain factor = 5 provides a good balance between visual quality of the watermarked image and the robustness of the extracted watermark. Table 6.16 shows the PSNR, NC and BER performance of the proposed method for different sizes of the image watermark at gain = 5. It is observed that the NC values have been found ranges from 0.5794 to 0.8026 for different size of image watermark. However, BER for recovered text watermark (size = 145 characters = 1015 bits) is '0' for all cases using BCH error correcting code, indicating a perfect recovery of the text watermark. Table 6.17 presents the PSNR,

Fig. 6.16 (**a**) Cover MR and (**b**) watermark logo image



(a) (b)

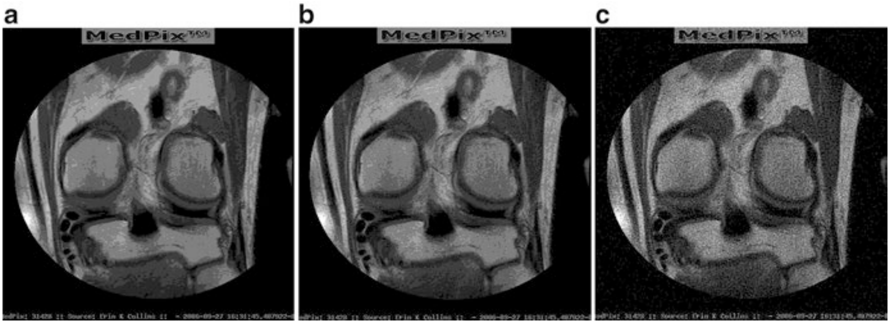
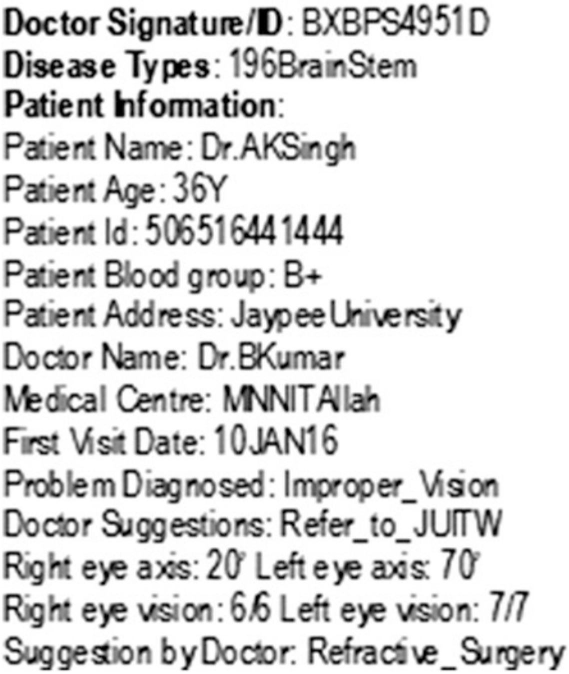


Fig. 6.17 Watermarked MR image at (**a**) Gain = 1 (**b**) Gain = 5 and (**b**) Gain = 15

NC and BER performance of the proposed method for different cover images such as MRI, Brain CT Scan, Ultrasound, Barbara and Lena images at gain factor = 5. In this table, the PSNR values are above than 30.00 dB for all the considered cover images. The highest PSNR were obtained with Lena image (PSNR = 37.04dB). The range of NC values from 0.7254 to 0.8657. The highest NC value were obtained for MRI image (NC = 0.8657). However, the lowest NC value were obtained for CT Scan image (NC = 0.7254). Referring this table, it is observed that all the BER values have been found ‘0’ except the Ultrasound image which is greater than ‘0’.

Table 6.18 shows the NC and BER performance of the proposed dual watermarking method against known attacks at gain factor = 3 using text bits = 140. Without using the encryption, the highest NC value (0.9615) has been obtained for Gaussian LPF and sharpening mask and the lowest NC value of 0.3498 is obtained against salt and pepper attacks. The highest BER (12.85%) has been found against median filtering attack, whereas lowest BER (0%) is found against Gaussian low pass filtering, sharpening mask, JPEG compression, histogram equalization and cropping. Referring this table, it is observed that all the NC values (with encryption) is greater



Doctor Signature/ID: BXBPS4951D
Disease Types: 196BrainStem
Patient Infomation:
Patient Name: Dr.AKSingh
Patient Age: 36Y
Patient Id: 506516441444
Patient Blood group: B+
Patient Address: JaypeeUniversity
Doctor Name: Dr.BKumar
Medical Centre: MNNITAllah
First Visit Date: 10JAN16
Problem Diagnosed: Improper_Vision
Doctor Suggestions: Refer_to_JUITW
Right eye axis: 20° Left eye axis: 70°
Right eye vision: 6/6 Left eye vision: 7/7
Suggestion by Doctor: Refractive_Surgery

Fig. 6.18 Patient information as text watermark

than the NC values as obtained without using the encryption method except for Gaussian LPF and sharpening mask. Table 6.19 presents the NC and BER performance of the proposed dual watermarking method against known attacks at gain factor = 5 using text bits = 1015. It is observed that all the NC values (with encryption) are greater than 0.7 except for Gaussian Noise (Mean = 0, Var-0.01), Salt & Pepper Noise (with density = 0.05), JPEG Compression (QF-10), Median Filtering (3 x 3). It is also observed that the BER performance is highly dependent on the noise variations. The results indicate that the proposed dual watermarking method is robust against various signal processing attacks. In addition, the performance of the proposed method highly depends on size of the watermarks, gain factor and noise variations.

6.7 Summary

In this chapter, the authors presents spread-spectrum based methods for secure multiple watermarking of medical images in wavelet domain which simultaneously embeds text and image both or text watermarks only into a cover medical image. The use of spread-spectrum technique secures the image watermark whereas improvement in robustness of the text watermark has been achieved using BCH code before embedding. Experimental results were obtained by varying watermark

Table 6.15 PSNR, NC and BER Performance of the proposed method at different gain factors

Gain factor	PSNR (dB)				NC				BER			
	20 char	40 char	123 char	151	20 char	40 char	123 char	151 char	20 char	40 char	123 char	151 char
1	39.51	39.10	38.63	38.63	0.3776	0.3814	0.3902	0.3886	0	0	0	0.0066
3	36.01	35.82	35.59	35.59	0.7118	0.7131	0.7118	0.7093	0	0	0	0.0066
5	32.77	32.68	32.57	32.57	0.8181	0.8181	0.8174	0.8159	0	0	0	0.0132
7	30.25	30.20	30.14	30.14	0.8682	0.8690	0.8665	0.8673	0	0	0	0.0132

Table 6.16 PSNR, NC and BER Performance of the proposed method at different size of the image watermark

Size of image watermark	PSNR (dB)	NC	BER (%)
50 × 12	36.33	0.6257	0
85 × 19	33.69	0.8026	0
89 × 19	33.57	0.8009	0
100 × 25	32.28	0.7204	0
100 × 40	30.6	0.5794	0

Table 6.17 PSNR, NC and BER Performance of the proposed method for different cover image

Cover image	PSNR (dB)	NC	BER (%)
Medimix	35.93	0.81.59	0
MRI	33.15	0.8657	0
CT Scan	31.87	0.7254	0
Ultra sound	32.97	0.7991	0.1310
Lena	37.04	0.8362	0
Barbara	30.19	0.7802	0

Table 6.18 NC and BER performance of the proposed method against different attacks

	Using BCH and without using encryption		With BCH and encryption	
Attacks	NC	BER	NC	BER (%)
Gaussian noise (M = 0,V = 0.01)	0.3568	5	0.5091	0.1
Salt & pepper noise (D = 5%)	0.3498	8.5714	0.4416	0.2
Gaussian LPF (STD = 0.6)	0.9615	0	0.6435	0
Gaussian LPF (std = 0.5)			0.6729	0
Scaling (F = 6)	0.6758	7.1429	0.6703	0.15
Sharpening mask (threshold = 0.8 and 0.1)	0.9615	0	0.7922 and 0.8062	0
JPEG compression (QF-90)	0.6831	0	0.6868	0
JPEG compression (QF-70)	0.6397	0	0.6424	0
JPEG compression (QF-50)	0.6059	0	0.6091	0
Median filtering [2 2]	0.5631	12.85	0.5541	0
Histogram equalization	0.7838	0	0.7859	0

size, gain factor and medical cover image modalities. The performance of the developed technique was tested against the known attacks. The method is also compared with other reported techniques and has been found to be giving superior performance for robustness with acceptable perceptual quality of the watermarked image suggested by other reported techniques. The proposed method offers up to 63.51% superior performance in terms of robustness over other reported techniques.

Table 6.19 NC and BER performance of the proposed method for different attacks

	Proposed technique	
Attacks	NC	BER
Gaussian noise (M = 0,V = 0.0001)	0.8094	0.034
Gaussian noise (M = 0,V = 0.001)	0.7800	0.282
Gaussian noise (M = 0,V = 0.01)	0.6598	0.841
Salt & pepper noise (D = 0.001)	0.8124	0
Salt & pepper noise (D = 0.005)	0.7788	0.0413
Salt & pepper noise (D = 0.05)	0.5904	0.724
Gaussian LPF (std = 0.05)	0.8151	0
Gaussian LPF (std = 0.1)	0.8159	0
Gaussian LPF (std = 0.5)	0.7894	0.0068
Scaling (F = 2)	0.7911	0.2551
Sharpening mask (threshold = 0.8 and 0.1)	0.8879 and 0.8706	0.0827 and 0.0620
JPEG compression (QF-90)	0.802	0
JPEG compression (QF-50)	0.7559	0.4068
JPEG compression (QF-10)	0.4656	0.9793
Median filtering [2 2] and [3 3]	0.7047 and 0.6837	0.7655 and 0.6620
Histogram equalization	0.8596	0.0413

Further, the performance of the proposed watermarking method has been extensively evaluated only for text watermark at multilevel DWT sub-bands by applying BCH code on the watermark considered as EPR data before embedding into the cover has been investigated. The performance of the developed technique was tested against the known attacks. The PSNR and BER performance of the proposed method is also compared with other reported technique. It is evident that the proposed method offers up to 7.93% enhancement in visual quality of the watermarked image and 1.53% reduction in BER over the reported techniques. Moreover, the method is also addressing the health data management issue where the encrypted text watermarks are embedded at multiple levels of the DWT sub-bands of the cover image. From the above discussion, we have observed that method reduces BER up to 0.124% while providing extra level of security of the text watermark using encryption method. Moreover, the performance of the method is also tested for multiple watermarks using encryption and BCH code simultaneously.

The proposed techniques is providing a potential solution to existing problem of secure medical data transmission over open and bandwidth constrained network. It also deals the problem of patient identity theft, which is a growing and dangerous concern in this area. For improvement in error correction capability of extracted text watermark bits, length of the error correction code may be suitably increased. Correlation and security of the method can be improved further by using other extended PN sequences such as random sequence, maximal length sequence, gold sequence and Kasami sequence.

References

1. O. Vikas, Multilingualism for cultural diversity and universal access in cyberspace: an Asian perspective, UNESCO, May 2005
2. B. Kumar, H.V. Singh, S.P. Singh, A. Mohan, Secure spread-spectrum watermarking for telemedicine applications. J. Inf. Security **2**(2), 91–98 (2011)
3. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, Relevance of watermarking in medical imaging, in Proceeding of the Information Technology Applications in Biomedicine, pp. 250–255, 2000
4. C. Pujara, A. Bhardwaj, V.M. Gadre, Secured watermarking fractional wavelet domains. IETE J. Res. **53**(6), 573–580 (2007)
5. B. Kumar, A. Anand, S.P. Singh, A. Mohan, High capacity spread-spectrum watermarking for telemedicine applications. World Acad. Sci. Eng. Technol. **5**, 58–62 (2011)
6. I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. **6**(12), 1673–1687 (1997)
7. H.S. Malvar, D.A.F. Florencio, Improved spread spectrum: a new modilation technique for robust watermarking. IEEE Trans. Signal Process. **51**(4), 898–905 (2003)
8. L. Perez-Freire, F. Perez-Gonzalez, Spread-spectrum watermarking security. IEEE Trans. Inf. Forensics Security **4**(1), 2–24 (2009)
9. G. Xuan, C. Yang, Y. Zheng, Y.Q. Shi, Z. Ni, Reversible data hiding based on wavelet spread spectrum, in IEEE International Workshop on Multimedia Signal Processing, Siena, Italy, pp. 211–214, 2004
10. B. Kumar, S.B. Kumar, D.S. Chauhan, Wavelet based imperceptible medical image watermarking using spread-spectrum, in Proceeding of 37th International Conference on Telecommunications and Signal Processing, Berlin, Germany, pp. 660–664, 2014
11. J. Domingo-Ferrer, F. Sebé, Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images, in Proceedings of the International Conference on Information Technology: Coding and Computing, pp. 1–6, 2002
12. T.S. Das, V.H. Mankar, S.K. Sarkar, Spread spectrum based robust image watermark authentication, in International Conference, Madurai, India, pp. 673–676, 2007
13. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible spread-spectrum watermarking for telemedicine applications. Proc. Natl. Acad. Sci., India, Sect. A: Phys. Sci. (2015). doi:10.1007/s40010-014-0197-6
14. A.K. Singh, M. Dave, A. Mohan, Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain. Wirel. Pers. Commun. **83**(3), 2133–2150 (2015)
15. MedPix TM Medical Image Database available at http://rad.usuhs.mil/medpix/medpix.html
16. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Secure and efficient health data management through multiple watermarking on medical images. Med. Biol. Eng. Comput. **44**, 619–631 (2006)
17. N. Terzija, M. Repges, K. Luck, W. Geisselhardt, Digital image watermarking using DWT: performance comparison on error correcting codes, in Visualization, Imaging, and Image Processing Proceeding (364), 2002
18. K. Wu, W. Yan, J. Du, A robust dual digital-image watermarking technique, in International Conference on Computational Intelligence and Security Workshop, pp. 668–671, 2007
19. C. Chemak, M.S. Bouhlel, J.C. Lapayre, A new scheme of robust image watermarking: the double watermarking algorithm, in Proceedings of the 2007 Summer Computer Simulation Conference, SCSC 2007, San Diego, CA, USA, pp. 1201–1208, 2007
20. H. Shen, B. Chen, From single watermark to dual watermark: a new approach for image watermarking. Comput. Electr. Eng. **38**, 1310–1324 (2012)
21. A. Singh, A. Tayal, Choice of wavelet from wavelet families for DWT–DCT–SVD image watermarking. Int. J. Comput. Appl. **48**(17), 9–14 (2012)

22. M.I. Khan, M.M. Rahman, M.I.H. Sarker, Digital watermarking for image authentication based on combined DCT, DWT, and SVD transformation. Int. J. Comput. Sci. **10**(5), 223–230 (2013)
23. A. Srivastava, P. Saxena, DWT-DCT-SVD based semi blind image watermarking using middle frequency band. IOSR J. Computer Eng. **12**(2), 63–66 (2013)
24. N.J. Harish, B.B.S. Kumar, A. Kusagur, Hybrid robust watermarking techniques based on DWT, DCT, and SVD. Int. J. Adv. Electr. Electron. Eng. **2**(5), 137–143 (2013)
25. B.L. Gunjal, R.R. Manthalkar, An overview of transform domain robust digital image watermarking algorithms. J. Emerg. Trends Computer Inf. Sci. **2**(1), 13–16 (2011)
26. F. Chen, H. He, Y. Huo, H. Wang, Self-recovery fragile watermarking scheme with variable watermark payload, Proceedings of the 10th International Conference on Digital-Forensics and Watermarking, Atlantic City, NY, pp. 142–155, 2011
27. N.H. Divecha, N.N. Jani, Image watermarking algorithm using DCT, DWT and SVD, in *Proceedings on National Conference on Innovative Paradigms in Engineering and Technology*, vol. 10, 2012, pp. 13–16
28. K.A. Navas, A.M. Cheriyan, M. Lekshmi, S.A. Tampy, M. Sasikumar, DWT–DCT–SVD based watermarking, in Proceedings of the 3rd International Conference on Communication Systems Software and Middleware and Workshop, Bangalore, pp. 271–274, 2008
29. B. Wang, J. Ding, Q. Wen, X. Liao, C. Liu, An image watermarking algorithm based on DWT DCT and SVD, in IEEE International Conference on Network Infrastructure and Digital Content, Beijing, pp. 1034–1038, 2009