High Capacity and Secure Watermarking for Medical Images using Tchebichef Moments

Azadeh BASTANI, Fatemeh AHOUZ

Dept. of Computer Engineering, Faculty of Engineering, Behbahan Khatam alanbia Univ. of Technology, Behbahan, Iran

{bastani, Ahouz}@bkatu.ac.ir

Abstract. *Using Tchebichef Moments, this study has introduced a new method for imperceptible watermarking of the medical images with a high embedding capacity and robustness against the various attacks. The suggested method applies conditional quantization based on dither modulation to minimize the number of the moment orders that need to be changed. Reduction of modified moments increases the watermark imperceptibility and hence decreases the attacks probability. The proposed method has been examined in the presence of such factors as quantization step and watermark size. Experimental results show that average PSNR is 53.91 dB for 16384 embedding watermark bits. Moreover, the introduced algorithm has been tested for known attacks like scaling, cropping, noise, etc. It has been shown that our proposed method has proper security and robustness against various attacks. In addition, zero false positive rate on non-watermarked images has been obtained.*

Keywords

Medical image, digital watermarking, Tchebichef moments, dither modulation

1. Introduction

In recent years, it has been common to transmit the patients' medical information by the electronic communication. Information transmission from one point to another to enhance the patient health condition via electronic media is called telemedicine [1]. Information transmission is generally aimed for applications such as consultation, diagnosis among clinicians, teleconferences, and distance learning of medical personnel [2]. Medical images are among the data that are frequently transmitted from one place to another and hence their security is of great importance. Modification and tampering with patients' information during transmission can result in misdiagnosis and cause problems in patient healthcare trends. Therefore, it is essential to keep the medical data secure under telemedicine.

Among the existing methods for securing medical images, digital watermarking is prevalent. Normally, medical images and electronic patient report, EPR, are sent separately. When digital watermarking is employed and EPR is added to the medical images, besides securing the data transmitted, the EPR can be embedded into the images. This has the advantage of not only saving memory and bandwidth but also preventing erroneous attribution of EPR to an irrelevant image.

Digital watermarking methods are generally divided into three groups: [2]

Fragile watermarking: In this group, watermark is embedded in a way that with the least changes in the image the watermark is destroyed and the lack of watermark in a watermarked image is regarded as modification and alteration of the image, and therefore this is used for authentication application.

Semi fragile watermarking: In this group, the embedded watermarks are destroyed when unauthorized modifications are applied; however, it remains unchanged towards unwanted and unintentional modifications like compressing, scaling, etc.

Robust watermarking: In this group of methods, the embedment watermarks are in a way that their removal or destruction is not easily accomplishable and they are robust to attacks like compressing, cutting, filtering, etc. These methods are intended for copyright protection.

On the other hand, in recent years, image moments have been widely used in the field of watermarking [3]. The moments are divided into two classes of non-orthogonal (e. g., central and geometrical moments) and orthogonal (e. g., Zernike, pseudo-Zernike, Legendre, and Tchebichef moments). The orthogonal moments, compared to the non-orthogonal ones, are less sensitive to noise and are unaffected by the scaling and translation. These moments are used as image descriptors, can reconstruct images, and are reversible. Due to the low error rate in image reconstruction, the moments can be used for the embedding of the watermarks. Having features such as being independent of translation, rotation, and scaling results in further robustness of the watermarking method. On the other hand, for continuous moments like Zernike and pseudo-Zernike, error occurs in the coordinate transformations and numerical approximations in the computations from continuous to

discrete [4]. Besides, Tchebichef moments [5], [6] are of the type discrete orthogonal moments, which act on the image itself with no need to change the working space. Therefore, no computational complexities and approximation errors exist in these kinds of moments.

Alghoniemy et al. [7] first used moments in watermarking. Subsequently, moments were used in the existing methods in [8–11]. Xin [8] presented a watermarking method based on Zernike moments and pseudo-Zernike moments, which embeds the bit sequence based on the dither modulation (DM). The dither modulation is a particular form of quantization index modulation that was first introduced by Chen in 2001 [12]. In this method, in order to embed a bit sequence, each bit is quantized by a moment. The changed moments are added again to the image, and resultantly the watermark is embedded into the image. Here, in addition to the watermark itself, the auxiliary bits are used to give address for the unit disks in the destroyed images. Before extracting the watermark, the search for the unit disks is done and the watermark bits are rediscovered using minimum distance decoder. In this method, order p and iteration $q = 4m$ are used, and so the applicable moments are reduced to about one fourth. To address this problem, the higher orders of moments must be used, which, in turn, results in the computational errors. Furthermore, the use of higher orders of moments not only limits the watermark size but also reduces imperceptibility and robustness due to the inaccuracies. Therefore, in this work, the watermark length is considered to be 160, and results for watermarks with greater lengths are not taken into account. The average PSNR in this method is 42.5 dB.

Cheng et al. [9] developed a method based on Tchebichef moments. In this method, by using Harris Laplace detector, the reliable feature point is determined and different non-overlapped disks are recognized. The used moments are randomly chosen and are quantized and embedded into each of these disks using the dither modulation. In the watermark extraction stage, the same steps are also taken for watermark discovery. The keys related to the parameters DM and the selected moments are needed in the time of extraction. Compared to the method existing in [8], this method has increased PSNR to about 60 dB, but it suffers from its low capacity of embedded watermark, in which the maximum length is assumed to be 224. Besides, its computations are highly complex.

Wang proposed a method based on the wavelet moments [10]. In this method, compared to the other types of moments, a larger watermark can be embedded into the image using the lower orders of moment. Here, the center of patches is found through multi scale Harris detector. Then, to achieve robustness against rotation, scaling, and translation, the patches are normalized and the watermark is replaced in the chosen moments of each patch using DM. The watermark extraction process is similar to the steps in the watermark embedment. The main disadvantage of this method is the small length of the watermark ($L = 32$).

Elshoura in [13] performed the watermarking based on Zernike, Legendre, and Tchebichef moments. In this method, for each image and watermark pattern, all the moments are calculated to the order of S and then embedded with each other. In the watermark extraction stage, it is necessary to have the original image. Therefore, this method can only be used when the watermark is important. The large amount of computation is the main disadvantage of this method.

The present study on the medical images has developed an innovative method that not only outperforms the previous methods in terms of simultaneously enhancing visual quality and robustness, but it also offers a watermark embedding capacity of 16384 bits and over. The average PSNR is about 54 dB and is also adequately robust against the common attacks. The mechanism is that, first the physician/hospital logo or the patient data is converted into a bit sequence. After that, a hidden key is employed to calculate a certain number of Tchebichef moments that are equal to the watermark size. Through a conditional modulation method inspired from the dither modulation and using minimum distance decoder, the watermark bits are embedded into the moment. In the watermark extraction stage, using the same dither values as used in the embedding stage, the watermark bit sequence is extracted. The used modulation method is that, by reducing the values of the changed moments, the least possible change happens in the original image, hence increasing the visual imperceptibility.

The remainder of this paper is organized as follows. Section 2 represents the Tchebichef moments and how to calculate them. Section 3 shows the watermark embedding algorithm and the extraction process using Tchebichef moments and conditional modulation. Experimental results, method efficiency and robustness against various attacks are discussed in Sec. 4. Concluding remarks are provided at the end of the paper.

2. Tchebichef Moments

These moments are discrete orthogonal moments, the core of which is comprised of Tchebichef polynomials. Tchebichef moment (TM) is directly applied onto the image coordinate space and is appropriate for square digital images. In this moment, as compared to many other moments, the image normalization is not needed and also the image reconstruction error is comparatively low. Tchebichef moment of order $(p + q)$ for image f(x,y) can be defined as follows [5]:

$$T_{pq} = \frac{1}{\tilde{\rho}(p,N)\tilde{\rho}(q,N)}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\tilde{t}_p(x)\tilde{t}_q(y)f(x,y) \quad (1)$$

where

$$\tilde{\rho}(n,N) = \frac{\rho(n,N)}{\beta(n,N)^2},$$

$$\rho(n,N) = \frac{N\left(1-\frac{1}{N^2}\right)\left(1-\frac{2^2}{N^2}\right)......\left(1-\frac{n^2}{N^2}\right)}{2n+1}, \quad (2)$$

$$\beta(n,N) = N^n, \; p,q = 0,1,2,...N-1.$$

The Tchebichef polynomials $\tilde{t}_n(x)$ are given by the following formula

$$\tilde{t}_n(x) =$$

$$\frac{(2n-1)\tilde{t}_1(x)\tilde{t}_{n-1}(x) - (n-1)\left(1-\frac{(n-1)^2}{N^2}\right)\tilde{t}_{n-2}(x)}{n}, \quad (3)$$

$$n = 2,3,...,N-1$$

where

$$\tilde{t}_0(x) = 1, \; \tilde{t}_1(x) = (2x+1-N)/N. \quad (4)$$

The use of the above relations for large image dimensions, due to the large number of computational steps involved, increases the approximation error and so the procedure becomes inefficient. In order to solve this problem, the aforementioned relations are modified and rewritten as follows [14]:

$$T_{pq} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} \tilde{t}_p(x)\tilde{t}_q(y)\mathrm{f}(x,y) \quad (5)$$

where

$$\tilde{t}_n(0) = -\sqrt{\frac{N-n}{N+n}}\sqrt{\frac{2n+1}{2n-1}}\tilde{t}_{n-1}(0), n = 1,2,\dots,N-1, \quad (6)$$

$$\tilde{t}_n(1) = \left(1+\frac{n(1+n)}{1-N}\right)\tilde{t}_n(0), \quad n = 0,1,\dots,N-1, \quad (7)$$

$$\tilde{t}_n(x) = \gamma_1\tilde{t}_n(x) - 1 + \gamma_2\tilde{t}_n(x-2),$$
$$n = 1,2,3,\dots.(N-1), \quad x = 2,3,\dots,\frac{N}{2}, \quad (8)$$

and

$$\gamma_1 = \frac{-n(n+1) - (2x-1)(x-N-1) - x}{x(N-x)},$$
$$\gamma_2 = \frac{(x-1)(x-N-1)}{x(N-x)}, \quad (9)$$

$$\tilde{t}_n(N-1-x) = (-1)^n\tilde{t}_n(x), \quad x = \frac{N}{2},\dots,N-1. \quad (10)$$

The reverse of the Tchebichef moment transformation is calculable using the following relation:

$$f(x,y) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} T_{mn}\tilde{t}_n(x)\tilde{t}_n(y), \quad (11)$$
$$x,y = 0,1,\dots,(N-1).$$

Using corrected equations increases the computational speed and minimizes the propagation of numerical errors in calculations [14].

3. The Proposed Watermarking Method

This section introduces the suggested watermarking method applied through Tchebichef moments and conditional quantization based on the dither modulation. In addition to providing visual imperceptibility and watermark robustness, the proposed method is also able to minimize the number of modified moments. To this end, first a number of Tchebichef moments, equal to the watermark size, are calculated. In the next stage, using the changed dither quantization method, their values are quantized and the bit sequence is generated. Comparison of moments bit sequence with watermark bit sequence shows that the moment changes if any of its related bits is different, and otherwise it remains unchanged and keeps its original value. The suggested model is explained in the following subsections as watermark generation, embedding, and extraction.

3.1 Watermark Generation

For medical images, an embedded watermark can be generated by either of these two ways:

The patient's medical data is converted into a text in the form of ASCII code and each character is shown by 8 bits.

The physician/hospital logo is shown as a binary image with a size of 128×128.

3.2 Watermark Embedding

Watermark embedding block diagram is shown in Fig. 1. The embedding algorithm is as follows.

Step 1 – Selection of the feature vector: In the suggested method, due to the Tchebichef moments capability for image reconstruction and use of the recursive method in their calculation that enhances the calculation precision, it is possible and permissible to apply all the moments. Therefore, based on the number of the embedded bits, L, and using a secret key, K, a series of Tchebichef moments are randomly selected to form feature vector $\mathbf{T} = \left\{T_{p_1,q_1}, T_{p_2,q_2}, \dots, T_{p_L,q_L}\right\}$.

Step 2 – Quantization of the selected moments: here, an efficient quantization method leading to the secure and imperceptible watermarking is adopted [11]. A merit of this method, which is based on dither modulation, is that it reduces the number of the moments that needs changing. Using two dither functions, two quantized values $T^0_{p_i q_i}$ and $T^1_{p_i q_i}$ from the selected Tchebichef moment. $T_{p_i q_i}$ are here calculated via the following formula:

$$\left|T^i_{p_i,q_i}\right| = \mathrm{Round}\left(\frac{\left|T_{p_i,q_i}\right| - d_i(j)}{\Delta}\right) \cdot \Delta + d_i(j), \quad (12)$$
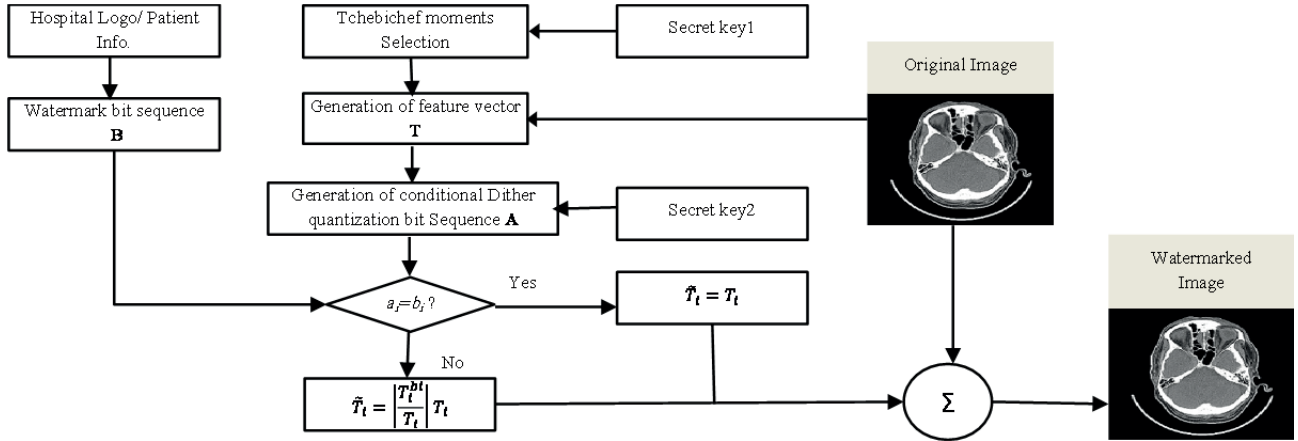
$$i = 1,2,\dots,L \quad \text{and} \quad j = 0,1$$

Fig. 1. Block diagram of watermark embedding.

where Δ is quantization step and $d_i(.)$ is the ith quantization function, so that

$$d_i(1) = d_i(0) + \Delta/2. \tag{13}$$

Now, the values of vector $\mathbf{A} = \{a_i\}$ are calculated based on the following relation:

$$a_i = \arg\min_j \left(\left| T_{p_i, q_i} \right| - \left| T_{p_i, q_i}^j \right| \right)^2, \tag{14}$$

$$i = 1, 2, \ldots, L \quad \text{and} \quad j = 0, 1.$$

The size of the bit vector $\mathbf{A} = \{a_i \in \{0, 1\}, i = 1, 2, \ldots, L\}$ is equal to the embedded watermark bit vector $\mathbf{B} = \{b_i \in \{0, 1\}, i = 1, 2, \ldots, L\}$. For embedding the watermark bit, only the moments that meet $a_i \neq b_i$ change; otherwise, the moment remains unchanged. In view of this, the new moments are changed as follows:

$$\tilde{T}_{p_i, q_i} = \begin{cases} \dfrac{\left| T_{p_i, q_i}^{b_i} \right|}{\left| T_{p_i, q_i} \right|} \cdot T_{p_i, q_i} & \text{if} \quad a_i \neq b_i, \\ T_{p_i, q_i} & \text{else.} \end{cases} \tag{15}$$

According to the above equation, if the embedded watermark bit is equal to bit sequence a_i ($a_i = b_i$), no change happens in the values of moments and image. In the worst case, for all i's, $a_i \neq b_i$ where it is required to change all the moment values. Due to the uniform distribution of function d_i at the interval $[0, \Delta/2]$, half of the selected moments, on the average, remain unchanged, and resultantly fewer changes occur in the image and the embedded watermark has less perceptibility.

Step 3 – Reconstruction of the embedded image: In the last step, the selected modified moments must be replaced in the image. To do so, assume that $f(x,y)$ is the original image and $f_T(x,y)$ is the image that is exclusively generated from the selected moments. f_{Rest} is defined below:

$$f_{Rest}(x, y) = f(x, y) - f_T(x, y). \tag{16}$$

After changing the moments from $\mathbf{T}$ to $\tilde{\mathbf{T}}$, the watermarked image f_{wat} is expressed as follows:

$$f_{wat}(x, y) = f_{Rest}(x, y) + f_{\tilde{T}}(x, y). \tag{17}$$

3.3 Watermark Extraction

The watermark extraction procedure is similar to the generation of bit sequence a_i in the watermark embedding step. First, based on key K, the selected moments are calculated and extracted from the watermarked image. Since it is possible to manipulate the watermarked image, the values of the extracted moments are not necessarily similar to those of the original watermarked image moments and can be represented by $\acute{\mathbf{T}} = \{\acute{T}_{p_1, q_1}, \acute{T}_{p_1, q_1}, \acute{T}_{p_2, q_2}, \ldots \acute{T}_{p_L, q_L}\}$. Using the same functions $d_i(0)$ and $d_i(1)$, the values of $\left| \acute{T}_{p_i, q_i}^0 \right|$ and $\left| \acute{T}_{p_i, q_i}^1 \right|$ are recomputed according to formula (12). Using formula (14), the minimum distance to $\acute{T}_{p_i, q_i}$ is calculated and bit sequence $\hat{\mathbf{B}} = (\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_L)$ is extracted as the embedded watermark from the received image.

4. Practical Results

The suggested scheme was applied onto the medical images [15], a few samples of which are illustrated in Fig. 2. These images are of the types X-ray, MRI, CT scan, and US. The images in gray form and with the dimensions 512×512 were used to examine the efficiency of the suggested method in terms of two factors of watermark imperceptibility and robustness against attacks. The used watermark images are also shown in Fig. 3. These were used as binary images with the dimensions 128×128.

4.1 Performance Measures

The greatness of the PSNR ratio between the original and the watermarked images indicates the amount of similarity between these two images and hence the imperceptibility of the watermark. PSNR is calculated below:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right), \tag{18}$$

$$MSE = \frac{1}{X \cdot Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} \left(f(i, j) - f_{wat}(i, j) \right)^2 \tag{19}$$
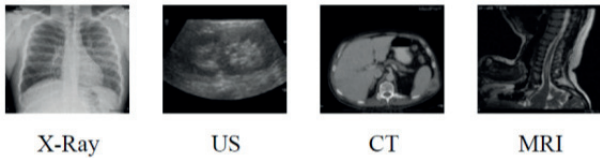
Fig. 2. Examples of the employed medical images.

Fig. 3. The used watermark images.
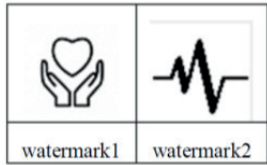

Fig. 4. PSNR value of the suggested method for different values of Δ and L.

where f shows the original image pixels with the size $X \times Y$ and f_{wat} signifies the watermarked image pixels with the same size $X \times Y$.

Watermark robustness is measured by normalized correlation (NC). Normalized correlation shows the amount of similarity between the original and the watermarked images. Relation (20) shows how NC is calculated. Watermark robustness is high in methods with NC close to 1.

$$NC = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} w(i,j) w'(i,j)}{\sum_{i=1}^{n} \sum_{j=1}^{m} w^2(i,j)} \qquad (20)$$

where $w(i,j)$ is the embedded watermark bit and $w'(i,j)$ is the extracted watermark bit at coordinates (i,j); n and m are watermark dimensions.

4.2 Imperceptibility Test

In any watermarking method, the watermarked image must look similar to the original image so that the embedded watermark cannot be observed and discovered. For imperceptibility test, PSNR value is estimated. Two main factors in determining the PSNR value are quantization step Δ and length of the embedded watermark. An increase in Δ increases the watermark robustness but decreases PSNR. Besides, by increasing the length of watermark and fixing Δ, PSNR decreases. Note that, in the suggested method, despite this relation, PSNR shows an acceptable value.

On the other hand, the way the highest order of the moments for watermark embedding is selected is also a key factor. Due to the high precision of Tchebichef moments, the use of all the moment orders is possible. The low order moments contain more image data and their modification results in more changes in the watermarked image, but the changes in the higher order moments have fewer effects on the image. On the other hand, it takes a longer time to calculate the high order moments as they involve a larger number of computational steps. Therefore, in this paper, the maximum moment order is set to be 130. The suggested method is tested with different values of Δ and L for three kinds of watermarks (i.e., random bit sequence, patient's textual data, and watermark images). According to the ob-
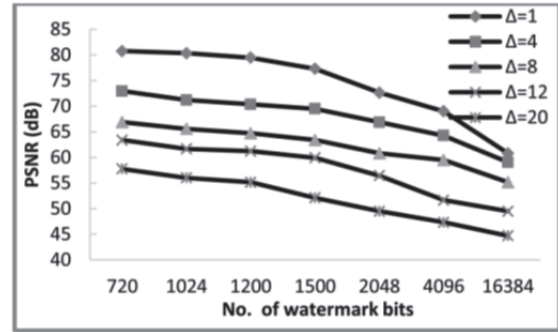
tained results, in the absence of attacks, the embedded watermark is extracted completely correctly and with BER = 0 and NC = 1. That is to say, the reversibility of the suggested method is fully realized. Figure 4 shows the PSNR value with respect to different values of Δ and L for the images under study. Based on this figure, the selection of a smaller Δ results in an increase in PSNR. However, as it will be stated later, in case the watermark is attacked, the increase of Δ is helpful and enhances the NC ratio. Table 1 represents the values of PSNR and NC for L = 16384 concerning two test watermark images for different medical images. It is observed that the PSNR ranges from 60.96 dB to 49.54 dB with Δ = 1 to 12. The best value of PSNR is obtained with Δ = 1 and the lowest value is for Δ = 12.

Table 2 compares the PSNR and NC of the suggested method with two methods in [16] and [17] at the best. The average value of PSNR in the suggested method with Δ = 1 is 60.9 dB, as compared to 37.9 dB and 49.36 dB in [16] and [17], respectively. Moreover, the NC in the suggested method is 1 and equal to the complete extraction of all the watermark bits, as compared to 1 and 0.9618 in [16] and [17], respectively. These values show that the watermark extraction and imperceptibility in our suggested method is better than those in [16] and [17].

4.3 Robustness Test

We have tested the robustness of the suggested method against attacks of median filter, salt and pepper noise, Gaussian noise, scaling and cropping and JPEG compression. Table 3 shows the results based on the NC value using Δ = 10 and compares it with two methods in [17] and [18]. According to the results, this method is more robust against JPEG compression, scaling, mean filter and cropping than the other kinds of attacks. The results show that the proposed method is performed better than existing method [18] under all kind of attacks. Also the proposed method is performed better than existing method [17] in some kind of attacks such as JPEG compression, scaling, mean filter and Gaussian noise.

In Tab. 4 some features of the proposed method are compared with methods in [16–21] that use medical images. Regardless of attacks probability, by using Δ = 1, the average PSNR value of proposed method is 60.9 dB. In this case, the suggested method provides better impercepti-

Test Image	PSNR(dB)		NC	
	Watermark1	Watermark2	Watermark1	Watermark2
(a) For quantization step $\Delta = 1$				
X-ray	60.81	60.69	1	1
CT	60.89	60.74	1	1
MRI	60.92	61.12	1	1
US	60.96	61.10	1	1
(b) For quantization step $\Delta = 4$				
X-ray	59.36	59.16	1	1
CT	59.38	59.14	1	1
MRI	59.37	59.20	1	1
US	59.40	59.21	1	1
(c) For quantization step $\Delta = 8$				
X-ray	55.61	55.32	1	1
CT	55.70	55.34	1	1
MRI	55.71	55.32	1	1
US	55.62	55.39	1	1
(d) For quantization step $\Delta = 12$				
X-ray	49.64	49.54	1	1
CT	49.65	49.91	1	1
MRI	49.55	49.57	1	1
US	49.62	49.82	1	1

Tab. 1. PSNR and NC values of proposed method for different values of quantization step in the absence of attacks.

Test Image	Ref.[17]		Ref.[16]		Proposed method	
	PSNR	NC	PSNR	NC	PSNR	NC
X-ray	55.06	0.9230	-	-	60.81	1
CT	47.18	0.9827	52.16	1	60.89	1
MRI	48.99	0.9692	51.83	1	60.92	1
US	50.27	0.9551	-	-	60.96	1

Tab. 2. Comparison of PSNR of the suggested method with other methods in the absence of attacks.

Attack type	Ref.[18]	Ref.[17]	Proposed scheme
JPEG compression QF=90	0.7394	0.9806	0.9768
JPEG compression QF=70	0.7394	0.7114	0.7876
Scaling (90%)	Not mentioned	Not mentioned	0.9843
Scaling (150%)	Not mentioned	Not mentioned	0.9621
Scaling (200%)	0.07394	Not mentioned	1
Cropping (20%)	Not mentioned	0.9687	0.8682
Salt and pepper noise(d=0.005)	0.7391	0.9002	0.8468
Gaussian Noise(m=0,v=0.01)	0.7335	0.6377	0.7912
Speckle noise	Not mentioned	0.9456	0.9017
Mean Filter	Not mentioned	0.8461	0.8863
Median Filter	0.6736	0.9700	0.8413

Tab. 3. Comparison of NC values in the suggested method with other methods against different attacks.

bility than all other methods. For having more robustness against various attacks, the quantization step Δ is set to 10 which decreases the average PSNR to 53.91 dB. Maximum NC and minimum BER also perform better than all other methods. Furthermore, the proposed method is robust against various attacks.

4.4 False Positive Test

False positive detection (FPD) is used to differentiate authorized from unauthorized images. In case the watermark is extracted from an unauthorized image, then the FPD happens and therefore the system lacks security. In the suggested method, the extraction algorithm has been per-
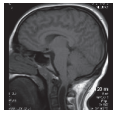
formed on non-watermarked images. Some tested samples along with the values of NC and the extracted watermark images are given in Tab. 5. If we accept the NC values larger than 0.6 for the FPD occurrence, the obtained FPD ration in this method is zero. The acceptable ratio of FPD, for having security, is 10^{-6} [17] and thus the method proves to be adequately secure.
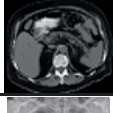
5. Conclusion

This study has presented an imperceptible watermarking method for medical images using Tchebichef moments and conditional dither quantization technique. Tchebichef moments were recursively calculated so as to

Method	Hiding Capacity	Robustness Metric	Average PSNR (dB)	Maximum NC	Minimum BER	Attacks
[16]	High	NC BER	37.9	1	0	Compression Rotation Cropping Histogram equalization Gaussian-Salt & Pepper-Speckle noise
[17]	High	NC	49.36	0.9918	-	Compression Blurring Sharpening Mean, Median Filter Histogram equalization Gaussian-Salt & Pepper-Speckle noise
[18]	High	NC BER	31.92	0.7544	0	Compression Scaling Sharpening Median Filter Histogram equalization Gaussian-Salt & Pepper noise
[19]	High	-	41.6	-	-	-
[20]	High	BER	48	-	0	Scaling Median Filter Average Filter Gaussian-Salt & Pepper noise
[21]	High	BER	59.09	-	0	Rotation Scaling Cropping Flipping Gaussian-Salt & Pepper-Speckle noise
Proposed Method	High	NC	53.91	1	0	Compression Scaling Cropping Median Filter Mean Filter Gaussian-Salt & Pepper-Speckle noise

Tab. 4. Performance comparison of proposed method with methods in [16–21].

Non-watermarked Image	Extracted Watermark1	NC	Extracted Watermark2	NC
		0.525		0.484
		0.481		0.494
		0.510		0.484
		0.501		0.482

Tab. 5. Samples of false positive detection in the suggested method.

decrease the calculation errors and increase the computation speed. In this method, the watermarked image or patient's information was embedded in the binary form into the selected quantized moments. The results have been provided based on the quantization step, watermark size, and type of watermark. As the results show, this method is able to embed large-size watermarks without any significant changes in the image. Besides, compared to some previous approaches on moments that reported a maximum length of 224, this method is efficient for watermarks with a length of 16384. The average of PSNR is 53.91 dB, which is higher than those in [16–20]. The results also indicate that the increase in the quantization step size has a positive effect on the watermark extraction. It is also resulted that the suggested method is effective enough against types of attacks. Therefore, this method, due to its good visual imperceptibility, robustness and zero ratio of FPD, is suitable for telemedicine applications.

References

[1] VELUMANI, R., SEENIVASAGAM, V. A reversible blind medical image watermarking scheme for patient identification, improved telediagnosis and tamper detection with a facial image watermark. In *Proceedings of IEEE Conference on Computational Intelligence and Computing Research*. Coimbatore (India), 2010, p. 1–8. DOI: 10.1109/ICCIC.2010.5705832

[2] MEMON, N. A., GILANI, S. A. M. Watermarking of chest CT scan medical images for content authentication. *International Journal of Computer Mathematics*, 2011, vol. 88, no. 2, p. 265–280. DOI: 10.1080/00207161003596690

[3] TSOUGENIS, E. D., PAPAKOSTAS, G. A., KOULOURIOTIS, D. E., et al. Performance evaluation of moment-based watermarking methods: A review. *Systems and Software*, 2012, vol. 85, p. 1864–1884. DOI: 10.1016/j.jss.2012.02.045

[4] MUKUNDAN, R., ONG, S. H., LEE, P. A. Discrete vs. continuous orthogonal moments for image analysis. In *Proceedings of International Conference on Imaging Science, Systems, and Technology (CISST01)*. Las Vegas (NV, USA), 2001, p. 23–29.

[5] MUKUNDAN, R., ONG, S. H., LEE, P. A. Image analysis by Tchebichef moments. *IEEE Transactions on Image Processing*, 2001, vol. 10, no. 9, p. 1357–1364. DOI: 10.1109/83.941859

[6] KOTOULAS, L., ANDREADIS, I. Fast computation of Chebyshev moments. *IEEE Transactions on Circuits and Systems for Video Technology*, 2006, vol. 16, no. 7, p. 884–888. DOI: 10.1109/TCSVT.2006.877403

[7] ALGHONIEMY, M., TEWFIK, A. H. Image watermarking by moment invariants. In *Proceedings of IEEE International Conference on Image Processing*. Vancouver (BC, Canada), 2000, vol. 2, p. 73–76. DOI: 10.1109/ICIP.2000.899229

[8] XIN, Y., LIAO, S., PAWLAK, M. Circularly orthogonal moments for geometrically robust image watermarking. *Pattern Recognition*, 2007, vol. 40, no. 12, p. 3740–3752. DOI: 10.1016/j.patcog.2007.05.004

[9] DENG, C., GAO, X., LI, X., et al. A local Tchebichef moments-based robust image watermarking. *Signal Processing*, 2009, vol. 89, p. 1531–1539. DOI: 10.1016/j.sigpro.2009.02.005

[10] WANG, X. Y., YANG, Y. P., YANG, H. Y. Invariant image watermarking using multi-scale Harris detector and wavelet moments. *Computers and Electrical Engineering*, 2010, vol. 36, no. 1, p. 31–44. DOI: 10.1016/j.compeleceng.2009.04.005

[11] SINGH, C., RANADE, S. K. Image adaptive and high-capacity watermarking system using accurate Zernike moments. *IET Image Processing*, 2014, vol. 8, no. 7, p. 373–382. DOI: 10.1049/iet-ipr.2013.0382

[12] CHEN, B., WORNELL, G. W. Quantization index modulation methods: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 2001, vol. 47, no. 4, p. 1423–1443. DOI: 10.1109/18.923725

[13] ELSHOURA, S. M., MEGHERBI, D. B. Analysis of noise sensitivity of Tchebichef and Zernike moments with application to image watermarking. *Visual Communication and Image Representation*, 2013, vol. 24, no. 5, p. 567–578. DOI: 10.1016/j.jvcir.2013.03.021

[14] MUKUNDAN, R. Some computational aspects of discrete orthonormal moments. *IEEE Transactions on Image Processing*, 2004, vol. 13, no. 8, p. 1055–1059. DOI: 10.1109/TIP.2004.828430

[15] *MedPixTM Medical Image Database*. [Online] Available at: http://rad.usuhs.mil/medpix/medpix.html, https://medpix.nlm.nih.gov/home

[16] SHARMA, A., SINGH, A. K., GHRERA, S. P. Robust and secure multiple watermarking for medical images. *Wireless Personal Communications*, 2017, vol. 92, no. 4, p. 1611–1624. DOI: 10.1007/s11277-016-3625-x

[17] THANKI, R., BORRA, S., DWIVEDI, V., S., et al. An efficient medical image watermarking scheme based on FDCuT-DCT. *Engineering Science and Technology, an International Journal*, 2017, vol. 20, p. 1366–1379. DOI: 10.1016/j.jestch.2017.06.001

[18] SINGH, A. K., KUMAR, B., DAVE, M., et al., Multiple watermarking on medical images using selective discrete wavelet transform coefficients. *Journal of Medical Imaging and Health Informatics*, 2015, vol. 5, p. 1–8. DOI: 10.1166/jmihi.2015.1432

[19] LOAN, N. A., PARAH, S. A., SHEIKH, J. A., et al. Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications. *Journal of Biomedical Informatics*, 2017, vol. 73, p. 125–136. DOI: 10.1016/j.jbi.2017.08.002

[20] XIAO, B., LUO, J., BI, X., et al. Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking. *Information Sciences*, 2019, vol. 516, p. 545–559. DOI: 10.1016/j.ins.2019.12.044

[21] CEDILLO-HERNANDEZ, M., CEDILLO-HERNANDEZ, A., NAKANO-MIYATAKE, M., et al. Improving the management of medical imaging by using robust and secure dual watermarking. *Biomedical Signal Processing and Control*, 2020, vol. 56, p. 1–16. DOI: 10.1016/j.bspc.2019.101695