Journal of Information Security, 2011, 2, 91-98
doi:10.4236/jis.2011.22009 Published Online April 2011 (http://www.scirp.org/journal/jis)

Secure Spread-Spectrum Watermarking for Telemedicine Applications

Basant Kumar[1], Harsh Vikram Singh[2], Surya Pal Singh[3], Anand Mohan[3]
[1]*Motilal Nehru National Institute of Technology, Allahabad, India*
[2]*Kamla Nehru Institute of Technology, Sultanpur, India*
[3]*Institute of Technology, Banaras Hindu University, Varanasi, India*
Emails: singhbasant@yahoo.com
Received December 5, 2010; *revised January* 10, 2011; *accepted April* 12, 2011

Abstract

This paper presents a secure spread-spectrum watermarking algorithm for digital images in discrete wavelet transform (DWT) domain. The algorithm is applied for embedding watermarks like patient identification/ source identification or doctors signature in binary image format into host digital radiological image for potential telemedicine applications. Performance of the algorithm is analysed by varying the gain factor, subband decomposition levels, size of watermark, wavelet filters and medical image modalities. Simulation results show that the proposed method achieves higher security and robustness against various attacks.

Keywords: Watermarking, Spread-Spectrum, Discrete Wavelet Transform, Telemedicine

1. Introduction

In recent years image watermarking has become an important research area in data security, confidentiality and image integrity. Despite the broad literature on various application fields, little work has been done towards the exploitation of health-oriented perspectives of watermarking [1-7]. While the recent advances in information and communication technologies provide new means to access, handle and move medical information, they also compromise their security against illegal access and manipulation. Sensitive nature of patient's personal medical data necessitates measures for medical confidentiality protection against unauthorized access. Source authenticcation and data integrity are also important matters relating to health data management and distribution. Data hiding and watermarking techniques can play important role in the field of telemedicine by addressing a range issues relevant to health data management systems, such as medical confidentiality protection, patient and examination related information hiding, access and data integrity control, and information retrieval. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Security requirements of medical information, derived from strict ethics and legal obligations imposed three mandatory characteristics: confidentiality, reliability and availability [8]. *Confidentiality* means that only authorized users have access to the information. *Reliability* has two aspects; 1) *Integrity*: the information has not been modified by non-authorized people, and 2) *Authentication*: a proof that the information belongs indeed to the correct source. *Availability* is the ability of an information system to be used by entitled users in the normal scheduled conditions of access and exercise. Authentication, integration and confidentiality are the most important issues concerned with EPR (Electronic Patient Record) data exchange through open channels [1,5]. All these requirements can be fulfilled using suitable watermarks. General watermarking method needs to keep the three factors (capacity, imperceptibility and robustness) reasonably very high [9]. Robustness is the ability to recover the data in spite of the attacks in the marked image, imperceptibility is the invisibility of the watermark and capacity is the amount of data that can be embedded. These requirements are hindering each other. There must be some trade off among these requirements according to the applications. Two common approaches of information hiding using image covers are spatial domain hiding and transform (frequency) domain hiding. Spatial domain techniques perform data embedding by directly manipulating the pixel values, code values or bit stream of the host image signal and they are computationally simple and straightforward. *LSB substitution*, *patchwork*, and *spread spectrum image steganography* are some of

the important spatial domain techniques [10,11]. In transform domain hiding, data are embedded by modulating coefficients in transform domain, such as DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform). Transform techniques can offer a higher degree of robustness to common image processing operations, compared to spatial domain techniques. Wavelet domain watermarking has recently received considerable attention due to its ability to provide both spatial and frequency resolution [12-14]. Many wavelet based watermarking schemes were proposed for medical images [15-18]. Watermarking technique can be further classified into two categories, reversible and irreversible [19,20]. The main idea behind reversible watermarking is to avoid irreversible distortion in original image (the host image), by developing techniques that can extract the original image exactly. Medical image watermarking is one of the most important fields that need such techniques where distortion may cause wrong diagnosis. The strict specifications regarding the quality of medical images could be met by reversible watermarking, which allows the recovery of the original image without any loss of information. Medical identity theft has been a serious security concern in telemedicine [21]. This demands development of secure watermarking schemes. Digital watermarking studies have always been driven by the improvement of robustness. On the contrary, security has received little attention in the watermarking community. The first difficulty is that security and robustness are neighboring concepts, which are hardly perceived as different. Security deals with intentional attacks whereas robustness is observed as degradation in data fidelity due to common signal processing operations. Digital watermarking may not be secure despite its robustness [22,23]. Therefore, security of the watermark becomes a critical issue in many applications. The problem of watermark security can be solved using spread-spectrum scheme [24-27]. Spread-spectrum is a military communication scheme invented during World War II [28]. It was designed to be good at combating interference due to jamming, hiding a signal by transmitting it at low power, and achieving secrecy. These properties make spread-spectrum very popular in present-day digital watermarking.

This paper proposes a new secure spread-spectrum based watermarking algorithm for embedding sensitive medical information like physician's signature/identifycation code or patient identity code into radiological image for identity authentication purposes. This medical information in binary image form is taken as watermarks. The proposed algorithm relies on n distinct pseudo-random (PN) matrices pairs with low correlation, where *n* is the number of bits that are to be hidden. The rest of the paper is organized as follows. Section 2 provides a brief overview of spread-spectrum image watermarking schemes in wavelet domain. Working of the proposed spread-spectrum algorithm is explained in Section 3. Performance of the new algorithm has been analyzed in Section 4 and Section 5 provides conclusion of overall work.

2. Spread Spectrum Watermarking in Wavelet Transform Domain

Wavelet-based watermarking has recently gained great attention due to its ability to provide excellent multi-resolution analysis, space-frequency localization and superior HVS modeling [12]. DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition. The dyadic frequency decomposition of wavelet transform resembles the signal processing of the HVS and thus allows adapting the distortion introduced by either quantization or watermark embedding to the masking properties of human eye [29]. The watermarks are inserted in different decomposition levels and subbands depending on their type, and in locations specified by a random key; thus, they can be independently embedded and retrieved, without any interference among them. It is evident that the energy of an image is concentrated in the high decomposition levels corresponding to the perceptually significant low frequency coefficients; the low decomposition levels accumulate a minor energy proportion, thus being vulnerable to image alterations. Therefore, watermarks containing crucial medical information like *doctor's signature, patient identification code or patient identification codes* require ing great robustness are embedded in higher subbands. In general, horizontal and vertical subbands have more or less the same characteristics and behavior, in contrast to diagonal ones. Thereupon, watermark embedding in the horizontal and vertical subbands guarantees increased robustness, since their energy compaction makes them less vulnerable to attacks.

The proposed image watermarking scheme uses spread-spectrum technique in which, different watermark messages are hidden in the same transform coefficients of the cover image using uncorrelated codes, *i.e*. low cross correlation value (orthogonal/near orthogonal) among codes. A brief overview of spread-spectrum watermarking technique is presented below:

2.1. Spread-Spectrum Watermarking Principle

The watermark should not be placed in insignificant regions of the image or its spectrum, since many common signal and geometric processes affect these components.

The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum while preserving fidelity. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise. This problem can be addressed by applying spread-spectrum watermarking which can be easily understood with spread-spectrum communications analogy in which frequency domain of the image is viewed as a *communication channel*, and correspondingly, the watermark is viewed as a *signal* that is transmitted through it [24]. Attacks and unintentional signal distortions are treated as *noise* that the immersed signal must be immune to. In spread-spectrum communications, one transmits a narrowband signal over a much larger bandwidth, such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into single output with high signal-to-noise ratio (SNR). However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures sufficiently small energy in any single coefficient. A watermark that is well placed in the frequency domain of an image will be practically impossible to see.

2.2. Spread Spectrum Watermark Design

There are two parts to building a strong watermark: the *watermark structure* and the *insertion strategy*. In order for a watermark to be robust and secure, these two components must be designed correctly. This can be achieved by placing the watermark explicitly in the perceptually most significant components of the data, and that the watermark is composed of random numbers drawn from a Gaussian ($N(0,1)$) distribution (where $N(\mu,\sigma^2)$) denotes a normal distribution with mean μ and variance σ^2). Once the significant components are located, Gaussian noise is injected therein. The choice of this distribution gives resilient performance against collusion attacks. The Gaussian watermark also gives strong performance in the face of quantization [30].

- *Watermark Structure:* In its most basic implementation, a watermark consists of a sequence of real numbers $X = x_1, x_2, \cdots, x_n$. In practice, we create a watermark where each value x_i is chosen independently according to $N(0,1)$.

- *Watermarking Procedure*: We extract from host digital document *D*, a sequence of values $V = v_1, v_2, \cdots, v_n$, into which we insert a watermark $X = x_1, x_2, \cdots, x_n$ to obtain an adjusted sequence of values $W = w_1, w_2, \cdots, w_n$ and then insert it back into the host in place of *V* to obtain a watermarked document *D**.

- *Inserting and Extracting the Watermark*: When we insert *X* into *V* to obtain *W*, a scaling parameter *k* is specified, which determines the extent to which *X* alters *V*. Formula for computing *W* is

$$w_i = v_i + kx_i$$

We can view *k* as a relative measure of embedding strength which is also known as gain factor. A large value of *k* will cause perceptual degradation in the watermarked document.

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

- *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 requantizing the watermarked document for delivery will cause *X** to deviate from *X*. We measure the similarity of *X* and *X** by

$$sim(X, X^*) = \frac{X^*.X}{\sqrt{X^*.X}} \quad (1)$$

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 threshold. Setting the detection threshold is a classical decision estimation problem [31].

3. Proposed Algorithm

This paper proposes a new DWT based spread-spectrum watermarking algorithm using medical image cover. Dyadic subband decomposition is performed on the radiological image using Haar wavelet transform. The watermark used in the algorithm is in binary image form. Different watermark messages are hidden in the same transform coefficients of the cover image using uncorrelated codes, *i.e*. low cross correlation value (orthogonal/ near orthogonal) among codes. For each message bit, two different Pseudo Noise (PN) matrices namely of size identical to the size of the wavelet coefficient matrices, are generated. Since the security level of the watermarking algorithm depends on the strength of its secret key, a

grey scale image of size 1 × 35 is used as a strong key for generating pseudorandom sequences. Based on the value of the bit for the message vector, the respective two PN sequence matrices are then added to the corresponding second level HL and LH coefficients matrices respectively according to the data embedding rule as follows:

$$W = V + kX \quad \text{if} \quad b = 0$$

Where V is wavelet coefficient of the cover image, W is the wavelet coefficient after watermark embedding, k is the gain factor, X is the PN matrix and b is the bit of watermark that has to be embedded. Generation of a pair of PN matrices for embedding each bit enhances the security of the watermarking algorithm. Following steps are applied in data embedding process.

3.1. Data Embedding

Read the host image $I(M,N)$ of size $M \times N$

1) Read the message to be hidden and convert it into binary sequences D_d ($D_d = 1$ to n)
2) Transform the host image using "Haar" Wavelet transform and get second level subband coefficients ccA, ccH, ccV, ccD
3) Generate n different PN-sequence pairs (PN_h and PN_v) each of size $\frac{M}{4} \times \frac{N}{4}$ using a secret key to reset the random number generator
4) For $D_d = 1$ to n, add PN sequences to ccH and ccV components when message = 0

ccH = ccH + *k**PN_h;

ccV = ccV + *k**PN_v;

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

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

3.2. Extraction of Hidden Data

To detect the watermark we generate the same pseudorandom matrices used during insertion of watermark by using same state key and determine its average correlation with the two detail subbands DWT coefficients. Average of n correlation coefficients corresponding to each PN matrices is obtained for both LH and HL subbands. 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 stego image $I_w(M,N)$
2) Transform the stego image using "Haar" Wavelet transform and get ccA1,ccH1,ccV1,ccD1 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 $\frac{M}{4} \times \frac{N}{4}$ using same secret key used in embedding to reset the random number generator
5) For *i* = 1 to *n*
   Calculate the correlations store these values in *corr_H (i)* and *corr_V (i)*.

   $corr\_H(i)$ = correlation between PN_h1(i) and ccH1(i)

   $corr\_V(i)$ = correlation between PN_v1(i) and ccV1(i)
6) Calculate average correlation

   $avg\_corr(i) = \left(corr\_H(i) + corr\_V(i)\right)/2$
7) Calculate the

   $corr(n)$ = mean of all the values stored in $avg\_corr(i)$
8) Extract the hidden bit 0, using the relationship given below
   For *j* = 1 to *n*

   if $avg\_corr(j) > corr(n)$, $msg(j) = 0$
9) Rearrange these extracted message

4. Performance Analysis

Performance of the proposed spread-spectrum watermarking algorithm was tested for telemedicine applications. Experiments were carried-out using 8-bit grey scale CT scan image of size 512 × 512 available in reference [32]. Medical information such as telemedicine origin centre (watermark 1) and doctor's signature (watermark 2) were embedded into host CT scan image as watermarks. These watermarks are in binary image formats which add robustness by allowing recovery of the watermarks even at low correlation between original and extracted watermarks. Strength of watermarking is varied by varying the gain factor in the watermarking algorithm. Perceptual quality of the watermarked radiological image is measured by calculating PSNR between host and watermarked image. At the receiver side, watermark is extracted from the watermarked image. Extracted watermark is evaluated by measuring its correlation with the

original watermark. **Figure 1** shows the host CT scan image and watermarked images obtained by applying watermarking algorithm in second level LH and HL subband DWT coefficients at different gain factors. Extracted watermarks along with the original watermarks are shown in **Figures 2** and **3**. It is observed from **Table 1** that with the increase in the gain factor, PSNR of the watermarked image decreases and the degree of similarity between original and extracted watermark increases. To show the effect of the decomposition levels, proposed algorithm with gain factor 2.0 was applied for embedding watermark in the horizontal and vertical subband coefficients of level 1, 2 and 3. It is observed from **Table 2** that the PSNR value of the watermarked image increases and correlation between original and extracted watermark decreases with the increase in subband level for watermarking. **Figure 4** shows the watermarks extracted from different levels of subband DWT coefficients. Performance of the watermarking algorithm also depends on the size of watermark. **Table 3** shows the effect of watermark size on the performance of the proposed watermarking algorithm. It is obvious that the PSNR performance of the watermarked image decreases with the increase in the size of the watermark, but subsequently we observe an improvement in the correlation between original and extracted watermarks. It can be also observed from **Figure 5** that larger size watermarks are more clearly identified during extraction. To observe the effect of host image, proposed algorithm was tested for other medical images like MRI and ultrasound images where watermarking is done in second level subband coefficients considering a gain factor of 1.5 and watermark size of 32 × 64. Host and watermarked MRI and ultrasound images are shown in **Figure 6**. It is observed from **Table 4** that the PSNR performance of all watermarked medical images are same where as there is a little variation in the similarity performance of original and

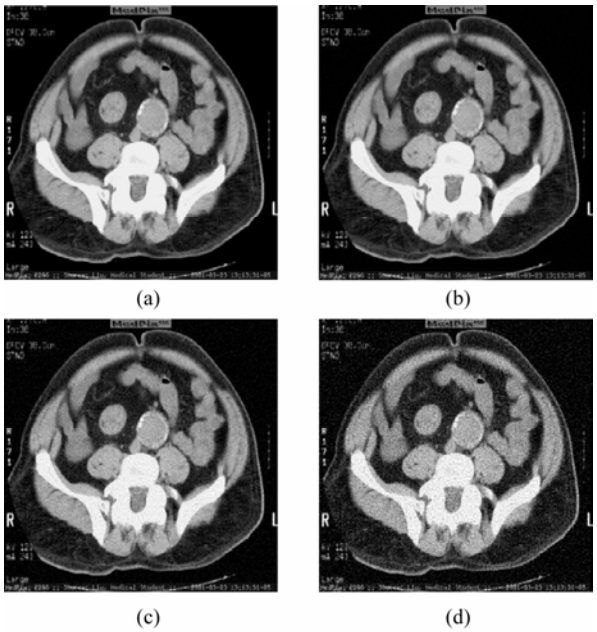

Figure 1. Original and watermarked CT scan images (a) original image and watermarked images with gain factor; (b) 0.5; (c) 1.5 and (d) 3.0.

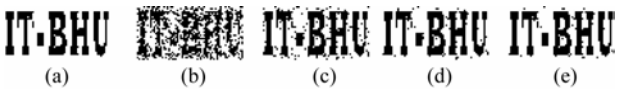

Figure 2. Telemedicine centre watermarks (a) original and extracted watermarks with gain factor; (b) 0.5; (c) 1.5; (d) 3.0 and (e) 4.0.

Figure 3. Doctor's signature watermarks (a) original and extracted watermarks with gain factor; (b) 0.5; (c) 1.5; (d) 3.0 and (e) 4.0.

Table 1. Effect of gain factor.

Gain Factor	Watermark 1 (Origin centre)		Watermark 2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
0.5	37.518	0.376	39.680	0.295
1.0	31.497	0.535	33.659	0.289
1.5	27.976	0.597	30.138	0.461
2.0	25.477	0.635	27.639	0.485
3.0	21.955	0.657	24.117	0.527
4	19.456	0.659	21.614	0.562

Table 2. Effect of subband levels (gain factor 2.0).

Levels	Watermark 1 (Origin centre)		Watermark 2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
1	19.421	0.677	21.659	0.638
2	25.477	0.635	27.639	0.485
3	31.541	0.413	33.706	0.229

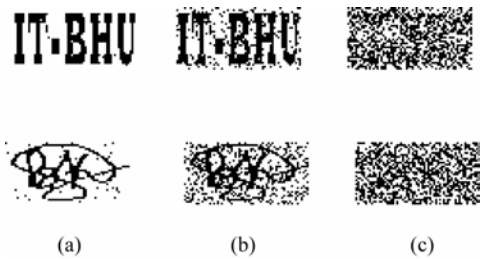

Figure 4. Extracted watermarks from (a) level 1 (b) level 2 and (c) level 3.

Table 3. Effect of watermark size.

Watermark size	Watermark 1 (Origin centre)		Watermark 2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
16 × 32	36.852	0.259	41.412	0.149
20 × 50	32.057	0.468	36.871	0.194
30 × 50	30.249	0.469	33.126	0.297
32 × 64	27.976	0.598	30.138	0.461
40 × 80	26.730	0.487	30.138	0.461

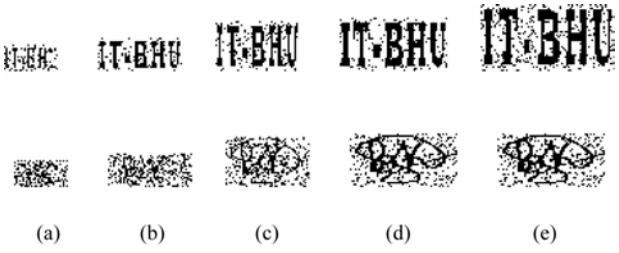

Figure 5. Extracted watermarks of different size (a) 16 × 32; (b) 20 × 50; (c) 30 × 50; (d) 32 × 64; (e) 40 × 80.

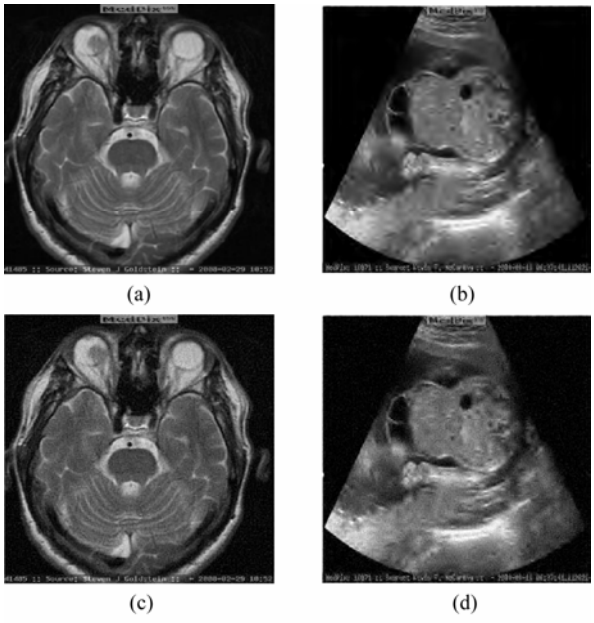

Figure 6. Original and watermarked MRI and US images (a) original MRI image (b) original US image (c) watermarked MRI image and (d) watermarked US image.

Table 4. Effect of host images.

Image type	Watermark1 (Origin centre)		Watermark2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
CT Scan	27.976	0.598	30.138	0.461
MRI	27.976	0.653	30.138	0.523
Ultrasound	27.976	0.653	30.138	0.564

extracted watermark for different medical images as shown in **Figure 7**. Effect of various wavelet filters on the proposed watermarking algorithm has also been analyzed. It can be observed from **Table 5** that the Bior 6.8 wavelet filter shows slightly better performance in terms of PSNR of the watermarked image and the correlation of extracted watermark with the original watermark. The scheme was also tested in terms of robustness of the image watermarks to JPEG compression. **Table 6** illustrates the robustness of the watermarks, which were extracted from a CT scan image after it was JPEG compressed by varying the quality factor in the range of 40 to 80. Watermarks were extracted intact after JPEG compression with different quality factors.

5. Conclusions

This paper presented a secure spread-spectrum watermarking scheme in wavelet transform domain. Performance of the scheme was tested for telemedicine applications by watermarking radiological images with sensi-

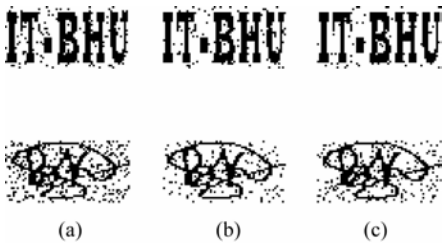

Figure 7. Extracted watermarks from different host medical images (a) CT scan; (b) MRI; (c) US image.

Table 5. Effect of wavelet filters.

Wavelet filter	Watermark1 (Origin centre)		Watermark2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
Db1 (Haar)	27.976	0.598	30.138	0.461
Db2	27.943	0.626	30.176	0.486
Db3	27.944	0.627	30.184	0.491
Bior 6.8	28.428	0.617	30.571	0.470

Table 6. Effect of JPEG compression.

Quality factor	Watermark1 (Origin centre)		Watermark2 (Doctor's Signature)	
	PSNR	Correlation	PSNR	Correlation
80	38.138	0.378	41.176	0.228
70	36.819	0.437	39.456	0.297
60	35.316	0.506	36.325	0.384
50	32.672	0.583	34.629	0.421
40	27.859	0.616	30.148	0.498

tive medical information in binary image format.

6. References

[1] H. M. Chao, C. M. Hsu and S. G. Miaou, "A Data-Hiding Technique with Authentication, Integration, and Confidentiallity for Electronic Patient Records," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 6, No. 1, March 2002, pp. 46-53. doi:10.1109/4233.992161

[2] U. R. Acharya, D. Anand P. S. Bhat and U. C. Niranjan, "Compact Storage of Medical Images with Patient Information," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 5, No. 4, December 2001, pp. 320-323. doi:10.1109/4233.966107

[3] X. Kong and R. Feng, "Watermarking Medical Signals for Telemedicine," *IEEE Transaction on Information Technology in Medicine*, Vol. 5, No. 3, 2001, pp. 195-201. doi:10.1109/4233.945290

[4] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, "Relevance of Watermarking in Medical Imaging," *Proceedings of the 3rd Conference on Information Technology Applications in Biomedicine*, Arlington, 2000, pp. 250-255.

[5] K. A. Navas, S. A. Thampy and M. Sasikumar, "ERP Hiding In Medical Images for Telemedicine," *Proceedings of World Academy of Science and Technology*, Vol. 28, 2008.

[6] B. Planitz and A. Maeder, "Medical Image Watermarking: A Study on Image Degradation," *Proceedings of the Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing*, Brisbane, February, 2005, pp. 3-8.

[7] G. Coatrieux, L. Lecornu, C. Roux and B. Sankur, "A Review of Image Watermarking Applications in Healthcare," *Engineering in Medicine and Biology Society*, Vol. 1, 2006.

[8] R. C Raul, F. U. Claudia and T. B. Gershom, "Data Hiding Scheme for Medical Images," 17*th International Conference on Electronics, Communications and Computers*, Cholula, 26-28 February 2007, pp. 32-32.

[9] G. C. Langelaar, I. Setyawan and R. L. Lagendijk, "Watermarking Digital Image and Video Data. A State-of-the-Art Overview," *IEEE Signal Processing Magazine*, Vol. 17, No. 5, September 2000, pp. 20-46. doi:10.1109/79.879337

[10] N. Nikolaidis and I. Pitas, "Digital Image Watermarking: An Overview," *IEEE International Conference on Multimedia Computing and Systems*, Florence, Vol. 1, June 7-11, 1999, pp. 1-6.

[11] I. J. Cox and M. L. Miller, "The First 50 Years of Electronic Watermarking," *EURASIP Journal on Applied Signal Processing*, No. 2, 2002, pp. 126-132. doi:10.1155/S1110865702000525

[12] P. Meerwald and A. Uhl, "A Survey of Wavelet-Domain Watermarking Algorithms," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents*, San Jose, Vol. 4314, 2001, pp. 505-516.

[13] S. Hajjara, M. Abdallah and A. Hudaib, "Digital Image Watermarking Using Localized Biorthogonal Wavelets," *European Journal of Scientific Research*, Vol. 26, No. 4, 2009, pp. 594-608.

[14] A. H. Paquet and R. K. Ward, "Wavelet-Based Digital Watermarking for Authentication," *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Winnipeg, Vol. 2, 2002, pp. 879-884.

[15] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, "Secure and Efficient Health Data Management through Multiple Watermarking on Medical Images," *Medical Biological Engineering & Computing*, Vol. 44, 2006, pp. 619-631. doi:10.1007/s11517-006-0081-x

[16] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management," *IEEE Transactions on Information Technology in Biomedicine*, 2006, pp. 722-732.

[17] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, "A Medical Image Watermarking Scheme Based on Wavelet Transform," *Proceedings* 25*th Annual International Conference of IEEE-EMBS*, Cancun, 2003, pp. 856-859.

[18] S. Dandapat, J. Xu, O. Chutatape and S. M. Krishnan, "Wavelet Transform Domain Data Embedding in a Medical Image," *Proceedings 26th Annual International Conference of IEEE-EMBS*, San Francisco, September 2004, pp. 1541-1544.

[19] J. B. Feng, I. C. Lin, C. S. Tsai and Y. P. Chu, " Reversible Watermarking: Current and Key Issues," International Journal of Network Security, Vol. 2, No. 3, May 2006, pp. 161-170.

[20] S. Lee, C. D. Chang and T. Kalker, "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform," *IEEE Transaction on Information Forensics and Security*, Vol. 2, No. 3, September 2007, pp. 321-330. doi:10.1109/TIFS.2007.905146

[21] M. Terry, "Medical Identity Theft and Telemedicine Security," *Telemedicine and e-Health*, Vol. 15, No. 10, December 2009, pp. 1-5.

[22] F. Cayre, C. Fontaine and T. Furon, "Watermarking Security: Theory and Practice," *IEEE Transactions on Signal Processing*, Vol. 53, No. 10, October 2005, pp. 3976-3987. doi:10.1109/TSP.2005.855418

[23] L. P. Freire, P. Comesana, J. R. T. Pastoriza and F. P. Gonzalez, "Watermarking Security: A Survey," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006, pp. 41-72.

[24] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, Vol. 6, No. 12, 1997, pp. 1673-1687.

[25] H. S. Malvar and D. A. F. Florencio, "Improved Spread Spectrum: A New Modilation Technique for Robust Watermarking," *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, 2003.

[26] L. Perez-Freire and F. Perez-Gonzalez, "Spread-Spectrum Watermarking Security," *IEEE Transactions on In-*

formation Forensics and Security, Vol. 4, No. 1, 2009.

[27] G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, "Reversible Data Hiding Based on Wavelet Spread Spectrum," *IEEE International Workshop on Multimedia Signal Processing*, Siena, 2004. doi:10.1109/MMSP.2004.1436530

[28] D. Kahn, "Cryptology and the Origins of Spread Spectrum," *IEEE Spectrum*, Vol. 21, September 1984, pp. 70-80.

[29] M. Unser and A. Aldroubi, "A Review of Wavelets in Biomedical Applications," *Proceedings of the IEEE*, Vol. 84, No. 4, 1996, pp. 626-638. doi:10.1109/5.488704

[30] F. Ergun, J. Kilian and R. Kumar, "A Note on the Limits of Collusion-Resistant Watermarks," *EUROCRYPT*'99 *Proceedings of the* 17*th International Conference on Theory and Application of Cryptographic Techniques*, Vol. 1592, 1999, pp. 140-149.

[31] C. W. Therrien, "Decision Estimation and Classification: An Introduction to Pattern Recognition and Related Topics," Wiley, New York, 1989.

[32] MedPix™ Medical Image Database available at http://rad.usuhs.mil/medpix/medpix.html

