A New Robust Blind Crypto-Watermarking Method for Medical Images Security

Mohamed Boussif, Oussema Boufares, Aloui Noureddine, Adnene Cherif

Sciences Faculty of Tunis, Laboratory of analysis and processing of electrical and energy Systems, University of Tunis El-Manar, El Manar, PB 2092, Tunisia.

Abstract
In this paper, we propose a novel robust blind crypto-watermarking method for medical images security based on hiding of DICOM patient information (patient name, age…) in the medical imaging. The DICOM patient information is encrypted using the AES standard algorithm before its insertion in the medical image. The cover image is divided in blocks of 8x8, in each we insert 1-bit of the encrypted watermark in the hybrid transform domain by applying respectively the 2D-LWT (Lifting wavelet transforms), the 2D-DCT (discrete cosine transforms), and the SVD (singular value decomposition). The scheme is tested by applying various attacks such as noise, filtering and compression. Experimental results show that no visible difference between the watermarked images and the original images and the test against attack shows the good robustness of the proposed algorithm.

Keywords:
Crypto-Watermarking, Robust, Blind, Medical Images Security

1. Introduction

Telemedicine [1-4] is a booming healthcare practice that has facilitated the exchange of medical data, diagnostics and expertise between healthcare entities. With this fast evolution, the need for securing these data become very important. Currently digital watermarking and cryptography are widely used to protect intellectual property in the network environment and they became important applications to protect and secure the medical images. Ensuring the security of medical data must respect imperceptibility of electronic patient record while hidden in the cover image, to make sure no distortion is visible for a credible diagnostic and have maximum robustness to different type of attack. Many algorithms and methods have been proposed in literature for medical images watermarking such as in [5] where Narong Mettripun has proposed a robust medical images watermarking based on DWT (discrete wavelet transform) for patient identification. M. Jamali et al [6] have proposed a robust watermarking in non-ROI of medical images based on DCT (discrete cosine transform) and DWT. Bum-Soo Kima et al [7] have proposed a digital image watermarking method Robust against geometrical attacks. A new QIM-based watermarking method robust to gain attack has been proposed by Yevhen Zolotavkin et al [8]. Manuel Cedillo-Hernandez et al [9] have proposed a robust watermarking method in the DFT domain for effective management of medical imaging. Zulfiqar Ali et al [10] have proposed a new watermarking algorithm using Hurst Exponent for the protection of privacy in telemedicine. Rayachoti Eswaraiah et al [11] have proposed a robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. Rohit Thanki et al [12] have proposed a medical image watermarking algorithm based on FDCuT–DCT. Y. Gangadhar et al [13] have proposed a watermarking approach for securing medical images in invariant discrete wavelet transformation. Priya Selvam et al [14] have proposed reversible watermarking technique based on hybrid transform for medical images security in telemedicine. Frank Y. Shih et al [15] have proposed high-capacity watermarking method for medical images.

In this paper, we propose a new robust blind crypto-watermarking system for the security of medical images. As shown in Fig 1, we encrypt the watermark (DICOM patient information) before inserted in the imaging. We propose a watermarking algorithm based on the LWT-DCT-SVD transforms which allow inserting the encrypted data block by block in the cover image. Our contributions can be summarized as follows:1) hide the information of patients in the related images. 2) attach an imaging with the patient relative.

The rest of the paper is organized as follows. We present the proposed watermarking system in Section II. Then, the experimental result and simulation are presented in Section III. Section IV presents the comparative study where we compare the proposed method with others proposed method. Section V concludes the paper.

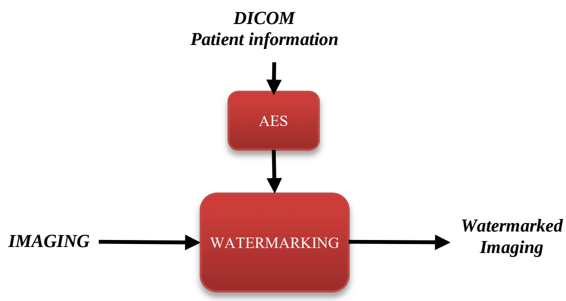


Fig. 1. *The proposed crypto-watermarking system.*

2. The proposed watermarking approach

This section details the proposed robust blind watermarking algorithm for the security of medical images. So, a brief description about the lifting wavelet transform

Manuscript received March 5, 2024
Manuscript revised March 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.3.11

(LWT) and discrete cosine transform (DCT) and the singular value decomposition (SVD) is presented.

1.1. The Lifting Wavelet Transform

As shown in Fig. 2, a lifting wavelet is a schema of implementation of a wavelet transformation different from that realized by the filter banks. It is an optimized process in the number of operations to execute and in memory occupation. For example, the calculation time of computing the LWT is half the time of computing the FFT.

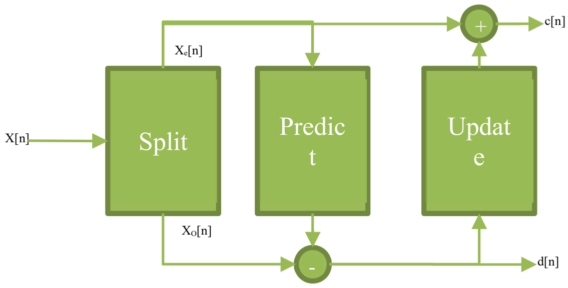


Fig. 2. The lifting wavelet transform

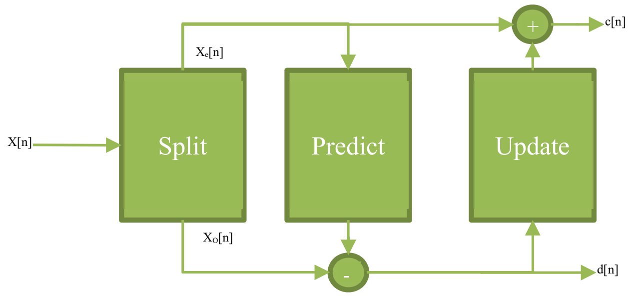
The principle is, first, to split the signal to be transformed, then to improve its properties by alternating the prediction and update steps as shown in Fig 2: 1) Split: The original signal set $x[n]$ is divided into two subsets with no common elements, whose length are the half of original data. Generally, the original signal is divided into odd subset $x_o[n] = x[2n+1]$ and even subset $x_e = x[2n]$. Predict: The odd series $x_o[n]$ is predicted according to even series $x_e[n]$ by the predict operator P, and the errors are called wavelet coefficients d [n] as in the next equation:

$$d[n] = x_o[n] - P(x_e[n]) \quad (1)$$

Update: The update operators U are put on wavelet coefficients d[n], and then the results add the odd series $x_e[n]$, which are called scale coefficients c [n] as in next equation:

$$c[n] = x_e[n] + U(d[n]) \quad (2)$$

A decomposition in lifting wavelet of Lena image is presented in Fig 4.



.

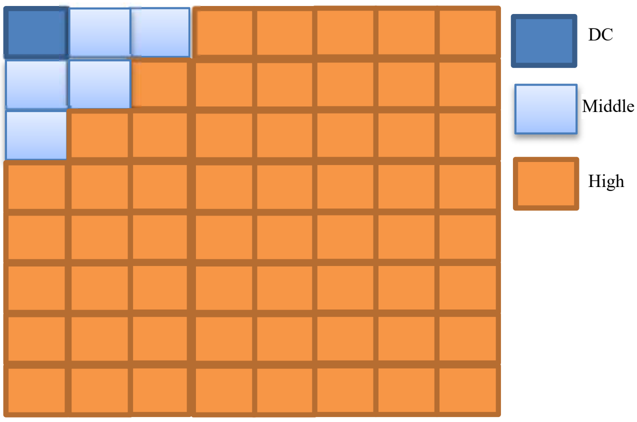


Fig. 3. *The frequency bands of the DCT*

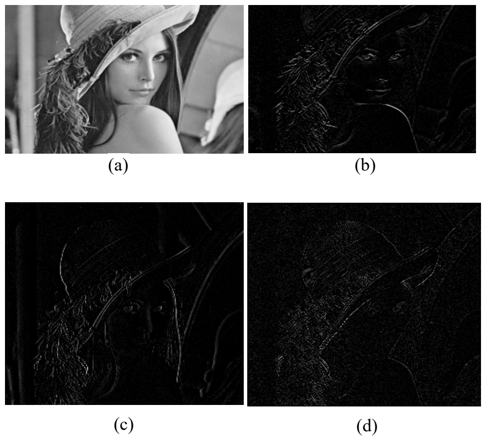


Fig.4. *Original image Lenna; (a) Sub-band LL; (b) Sub-band LH; (c) Sub-band HL; (d) Sub-band HH.*

1.2. The Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is a transformation close to the Discrete Fourier Transform (DFT). The projection kernel is a cosine and therefore creates real coefficients, in contrary the DFT, whose kernel is a complex exponential and therefore creates complex coefficients. However, the DCT can be expressed as a function of the DFT, which is then applied to the symmetrized signal. DCT is one of the most popular technique used in digital watermarking. So, as shown in Fig 3, it transforms the image into three frequency bands as lower or DC, middle and higher frequency bands. Middle frequency bands are preferred for watermarking due to less vulnerability towards attacks. It gives better results against attacks like compression and has better efficiency.

1.3. The Singular Value Decomposition

In mathematics, the singular value decomposition (SVD) is a linear algebra method of a matrix. it is an important tool for factoring, real or complex rectangular matrices. Its applications range of signal processing to statistics and meteorology. Let M be an mxn matrix whose coefficients belong to the field K, where K = ℝ or K = ℂ. Then there is a factorization of the form:

$$M = USV' \tag{3}$$

with U a unitary matrix mxm on K, S a matrix mxn whose diagonal coefficients are positive reals or nulls and all the others are null, and V 'is the adjoint matrix of V, unitary matrix nxn on K. This factorization is called the singular value decomposition of M.

2.4 The insertion/extraction process

As shown in Fig 5, The proposed algorithm possesses the imaging in block of sizes 8x8. For each block, we determine the coefficient 2-D LWT of this block, then, we applied the transformation 2-D DCT for the 4x4 LL coefficient of the LWT. we compute the matrix U, S and V using the SVD transformation of the 4 middle coefficients (matrix of 2x2) of the DCT. The insertion is done in the second diagonal coefficient of the matrix S i.e. S_{22}. The coefficient S_{11} must be remains greater than S_{22}, so, after the insertion of the watermark in S_{22} we add π/f to S_{11} so that it remains greater than S_{22}.

$$\begin{gathered} S_{22} = M(S_{22}) \\ S_{11} = S_{11} + \frac{\pi}{f} \end{gathered} \tag{4}$$

M and f are the insertion function and the strength of watermarking, respectively.

After the insertion process, we compute the inverse SVD by the matrix multiplication of U, watermarked S, and the transposed of V. We replace the watermarked low coefficient, then, we applied the inverse DCT. finally, we obtain the watermarked bloc by applied of the inverse LWT. The number of bits embedded for each bloc are 1 bit which is sufficient for insert all data of DICOM patient information, for example, for an image of 512x512 size we can hide 4096 bits. The function of insertion which allow insert a bit in a coefficient is defined as bellow:

$$M(S_{22}, w) = \frac{\pi}{f}\left[\overline{w} + 2Round\left(f\frac{S_{22}}{2\pi}\right)\right] \tag{5}$$

Where f, M, and w are the strength of watermarking, the insertion function, and the watermark bit, respectively. The inverse function which used for extract the watermark from the watermarked image is given by the next equation:

$$w_{ex} = M^{-1}(S_{22}^{w}) = \cos f \times S_{22}^{w} \tag{6}$$

Where S_{22}^{w} and w_{ex} are the watermarked coefficient and the extracted watermark, respectively.

3. Experiment result and discussion

Experiments were conducted on six sets of medical images of different modality, sizes and depth: Magnetic Resonance imaging, modality MRA, of 256x256 pixels and 16-bit depth, Magnetic Resonance imaging, modality MR, of 576x448 pixels and 12-bit depth, Radio Fluoroscopy imaging, modality RF, of 512x512 pixels and 8-bit depth. Computed radiography imaging, modality CR, of 2570x2040 pixels and 12-bit depth. Magnetic Resonance imaging, modality MRA, of 320x240 pixels and 12-bit depth. Magnetic Resonance imaging, modality MR, of 512x512 pixels and 12-bit depth. Some samples of our dataset are given in Fig. 6(a-f). We decided to use the peak signal to noise ratio (PSNR) in order to measure the distortion between an imaging I and its watermarked imaging I_w:

$$\begin{gathered} PSNR(I, I_w) = 10Log_{10}\left(\frac{[2^{dep} - 1]^2}{MSE(I, I_w)}\right) \\ MSE(I, I_w) = \frac{1}{L}\sum_{k=1}^{L}[I(k) - I_w(k)]^2 \end{gathered} \tag{7}$$

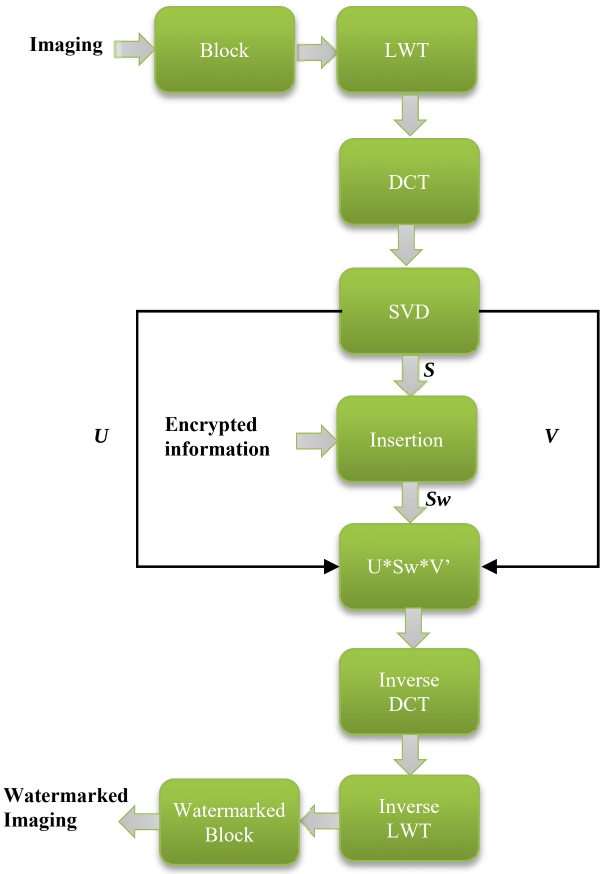


Fig. 5. *The proposed watermarking algorithm.*

Where L corresponds to the number of pixels of the image I, and dep corresponds to its depth. We use the correlation coefficients NC to measure the distortion between the watermark w and the extracted watermark w_{ex}:

$$NC(w, w_{ex}) = \frac{Cov(w, w_{ex})}{\sigma_w \sigma_{w_{ex}}} \tag{8}$$

Where $Cov(x, y)$and σ_x are the covariance of x and y and the standard deviation of x, respectively.

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})\,(y_i - \bar{y})$$
$$\sigma_x = \sqrt{E[x^2] - E[x]^2}$$
$$E[x] = \sum_{i=1}^{n} x_i p_i \tag{9}$$

Where $\bar{x}$ and p_i are the average value of x and the probability of x_i, respectively.

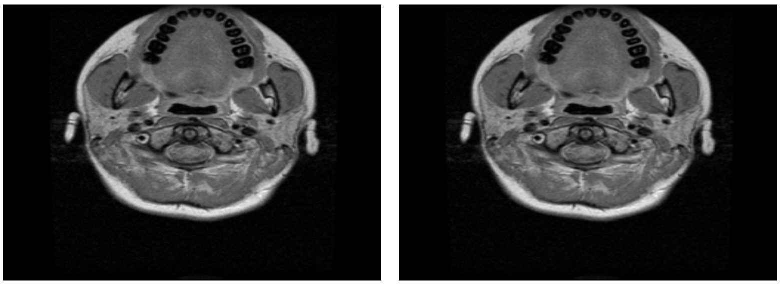
As shown in Fig. 6 no visible difference between the watermarked images and the original images, so, the watermark is imperceptible. From Table 1 we can conclude that the average PSNR equal to 58 which emphasize the performance of the proposed algorithm. The NC of the attacked watermarked images close to 1, therefore, the proposed algorithm robust to different attack such as contrast adjustment, cropping, filtering, Noise, and jpeg compression. The robustness of the proposed algorithm to different attack are given in Table 2.

Table 1 Performance evolution of the proposed watermarking system in term of PSNR

Images	a	b	c	d	e	f
PSNR	56.0702	61.1835	57.0012	58.0191	60.4521	56.1234

TABLE 2 robustness of the proposed algorithm to attacks

Attack	Metric	value	NC	Authentication
		0.5	0.9978	Yes
Contrast adjustment	Contrast factor	2	0.9996	Yes
		2.5	0.9941	Yes
		1/10	0.9320	Yes
Cropping	-	1/8	0.9014	Yes
		1/6	0.8927	Yes
		1x1	1	Yes
Filtering	-	2x2	0.9932	Yes
		3x3	0.9875	Yes
		0.002	1	Yes
Noise	Density	0.005	1	Yes
		0.01	0.9811	Yes
		100%	1	Yes
Compression	Factor quality	90%	1	Yes
		76%	1	Yes



(a) (a')

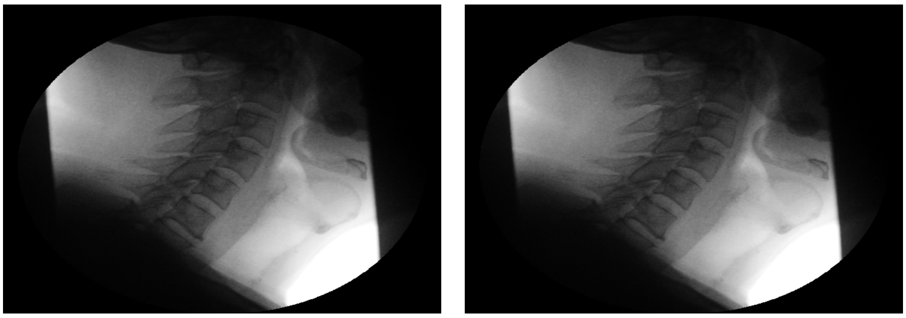


Fig. 6. *(a) and (b) are the original medical images. (a') and (b') are the watermarked medical images, respectively*

4. Performance and comparison

In this section, we compare the robustness of the proposed method against attacks with the method proposed in [5], and [16-20]. In [5] Narong Mettripun has proposed a robust medical image watermarking using the 2-D discrete wavelet transform level-2. T. Amornraksa et al [16] have proposed an images watermarking algorithm based on amplitude modulation. Thitiporn Pramoun et al [17] have proposed a color image watermarking scheme based on coefficients modification in LL sub-band. Rita Choudhary et al [18] have proposed DWT-based image watermarking is proposed using level. Sy C. Nguyen et al [19] have proposed an efficient image watermarking scheme using the Laplacian pyramid based on projection. Tamirat Tagesse Takore et al [20] have proposed a blind image watermarking scheme based on DWT, DCT and SVD. Rita Choudhary et al [21] have proposed image watermarking algorithm based on DWT using level. Sy C. Nguyen et al [22] have proposed an efficient image watermarking scheme using the laplacian pyramid based on projection. As shown in Fig. 7, the average watermarked images PSNR of the proposed method is great than Narong Mettripun et al [5] and T. Amornraksa [16], T. Pramoun et al [17], Rita Choudhary et al [21], Sy C. Nguyen et al [22], Tamirat Tagesse Takore et al [18]and Bambang Harjito et al [19]. The average NC of the proposed method obtained from jpeg attack at various quality factor is great than Narong Mettripun [5], T. Amornraksa et al [16], T. Pramoun et al [17] and R.O. Preda et al [20] (see Fig. 8). As shown in Fig. 9, the average NC of the proposed method obtained by contrast attack at various brightness factor is more robust than Narong Mettripun [5], T. Pramoun et al [17] and T. Amornraksa et al [16]. The comparison of average NC of the proposed method obtained from gaussian and pepper noise attack at various noise variance and density is more robust than Narong Mettripun [5], T. Amornraksa et al [16], T. Pramoun et al [17], Tamirat Tagesse Takore et al [18], and Bambang Harjito et al [19] (see Fig .10 and Fig 11).

Fig. 6. (a) and (b) are the original medical images. (a') and (b')are the watermarked medical images, respectively

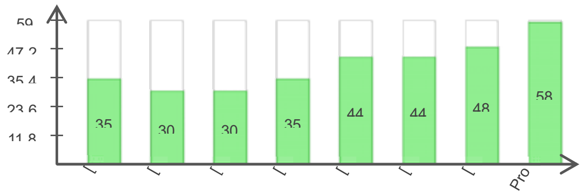


Fig. 7. *The performance comparison in term of PSNR.*

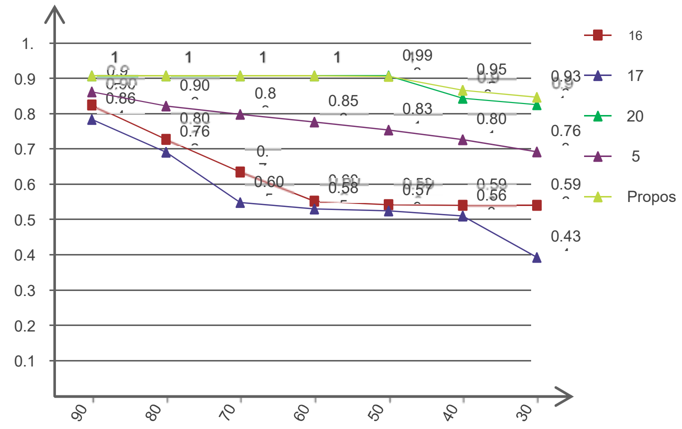


Fig. 8. *Comparison of average NC obtained from jpeg attack at various quality factor.*

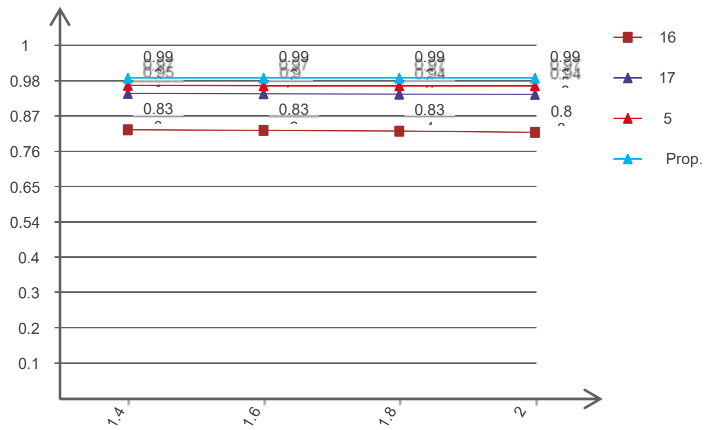


Fig.9. *Comparison of average NC obtained contrast attack at various brightness factor.*

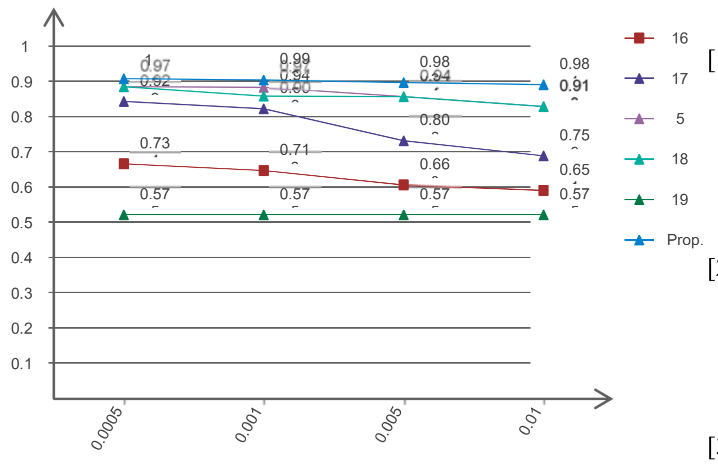


Fig. 10. *Comparison of average NC obtained from gaussian noise attack at various variance.*

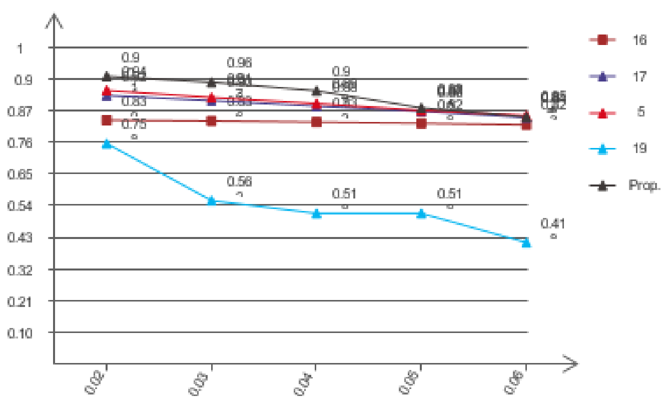


Fig. 11. *Comparison of average NC obtained from salt and pepper noise attack at various noise density.*

5. Conclusion

In this paper, we have proposed a robust blind crypto-watermarking algorithm based on hybrid transform(LWT-DCT-SVD) for the security of medical images. Therefore, we insert the encrypted information of patient in the relative medical images. We tested the proposed algorithm by applying various attacks such as noise, filtering and compression where we show that the proposed robust against different type of attack.

6. Acknowledgements

We are grateful to the reviewers for their valuable comments that helped us to improve the quality of the paper.

References

[1]. Abdulellah Alaboudi, Anthony Atkins, Bernadette Sharp, Mohammed Alzahrani, Ahmed Balkhair," Perceptions and Attitudes of Clinical Staff Towards Telemedicine Acceptance in Saudi Arabia," IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 Nov.-2 Dec. 2016.

[2]. Arshbeer Kaur, M.Tech., Sikander S. Cheema," A Hybrid Multi-Agent based Particle Swarm Optimization for Telemedicine System for Neurological Disease," International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 23-25 Dec. 2016.

[3]. Sebastian Thelen, Michael Czaplik, Philipp Meisen," Using off-the-Shelf Medical Devices for Biomedical Signal Monitoring in a Telemedicine System for Emergency Medical Services," IEEE Journal of Biomedical and Health Informatics, Volume: 19, Issue: 1, Jan. 2015.

[4]. Gagandeep Kaur, Dhiraj Sharma, and Vikramjit Kaur," Telemedicine in Transient Phase: Emergence of M-Health Care Services," Indian Journal of Science and Technology, Vol 9(15), DOI: 10.17485/ijst/2016/v9i15/90463, April 2016.

[5]. Narong Mettripun," A Robust Medical Image Watermarking Based on DWT for Patient Identification," 2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON).

[6]. M. Jamali, S. Samavi, N. Karimi, S.M.R. Soroushmehr, K. Ward, K. Najarian," Robust Watermarking in Non-ROI of Medical Images Based on DCT-DWT," 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC).

[7]. Bum-Soo Kim,, Jae-Gark Choi, Chul-Hyun Park, Jong-Un Won, Dong-Min Kwak, Sang-Keun Oh, Chang-Rim Koh, Kil-Houm Park," Robust digital image watermarking method against geometrical attacks," Real-Time Imaging 9 (2003) 139–149.

[8]. Yevhen Zolotavkin, andMartti Juhola," A New QIM-Based Watermarking Method Robust to Gain Attack," International Journal of Digital Multimedia Broadcasting Volume 2014, Article ID 910808, http://dx.doi.org/10.1155/2014/910808.

[9]. Manuel Cedillo-Hernandez, Francisco Garcia-Ugalde, Mariko Nakano-Miyatake, Hector Perez-Meana," Robust watermarking method in DFT domain for effective management of medical imaging," Signal, Image and Video Processing July 2015, Volume 9, Issue 5, pp 1163–1178.

[10]. Zulfiqar Ali, M. Shamim Hossain, Ghulam Muhammad, Muhammad Aslam," New Zero-Watermarking Algorithm Using Hurst Exponent for

Protection of Privacy in Telemedicine," IEEE Access, Volume: 6, pp. 7930 – 7940.

[11]. Rayachoti Eswaraiah, Edara Sreenivasa Reddy," Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest," IET Image Processing, Volume: 9, Issue: 8, 8 2015, pp. 615 – 625.

[12]. Rohit Thanki, Surekha Borra, Vedvyas Dwivedi, Komal Borisagar," An efficient medical image watermarking scheme based on FDCuT–DCT," Engineering Science and Technology," an International Journal, Volume 20, Issue 4, August 2017, pp. 1366-1379.

[13]. Y. Gangadhar, V.S. Giridhar Akula, P. Chenna Reddy," An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation," Biomedical Signal Processing and Control, Volume 43, May 2018, pp. 31-40.

[14]. Priya Selvam, Santhi Balachandran, Swaminathan Pitchai Iyer, Rajamohan Jayabal," Hybrid transform based reversible watermarking technique for medical images in telemedicine applications," Optik - International Journal for Light and Electron Optics, Volume 145, September 2017, pp. 655-671.

[15]. Frank Y. Shih, Xin Zhong," High-capacity multiple regions of interest watermarking for medical images," Information Sciences, Volumes 367–368, 1 November 2016, pp. 648-659.

[16]. T. Amornraksa, K. Janthawongwilai, "Enhanced Images Watermarking based on Amplitude Modulation," Image and Vision Computing, vol. 24, no. 2, 2006, pp. 111-119.

[17]. T. Pramoun and T. Amornraksa "Improved Image Watermarking Scheme based on DWT Coefficients Modification in LL Sub-band," Int. Proc. of IEEE on the 9th Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON-2012), May,16-18, 2012, Phetchaburi, Thailand, pp. 1-4.

[18]. Tamirat Tagesse Takore, Dr. P. Rajesh Kumar, Dr.G.Lavanya Devi," A Modified Blind Image Watermarking Scheme Based on DWT, DCT and SVD domain Using GA to Optimize Robustness," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).

[19]. Bambang Harjito and Esti Suryani," Robust image watermarking using DWT and SVD for copyright protection," AIP Conference Proceedings 1813, 040003 (2017); doi:10.1063/1.4975968.

[20]. R.O. Preda and D.N. Vizireanu," Watermarking-based image authentication robust to JPEG compression," ELECTRONICS LETTERS 5th November 2015 Vol. 51 No. 23 pp. 1873–1875.

[21]. Rita Choudhary, Girish Parmar," A Robust Image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT)," 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS).

[22]. Sy C. Nguyen, Ha Hoang Kha, Hoang M. Nguyen," An Efficient Image Watermarking Scheme Using the Laplacian Pyramid based on Projection," 2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom).