

# A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain

Jila Ayubi<sup>1</sup>, Shahram Mohanna<sup>2</sup>, Farahnaz Mohanna<sup>3</sup> and Mehdi Rezaei<sup>4</sup>

<sup>1</sup> Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan,  
Zahedan, 98135987, Iran

<sup>2</sup> Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan,  
Zahedan, 98135987, Iran

<sup>3</sup> Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan,  
Zahedan, 98135987, Iran

<sup>4</sup> Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan,  
Zahedan, 98135987, Iran

## *Abstract*

An effective watermarking algorithm based on the chaotic maps and the discrete wavelet transform for gray scale images is proposed. In the algorithm, the chaotic maps are employed to generate a key space with the length of  $10^{40}$  numbers to increase the degree of security. Additionally, the XOR operator has been replaced by the mutation process for embedding the images. This improved mutation operator has been used to encrypt the watermark logo. Additionally, the upgraded mapping method determines the location of, DWT, Discrete Wavelet Transform, coefficients where the watermark is embedded. To evaluate the robustness and effectiveness of the proposed method, the effect of several attacks has been simulated on the hidden image. Simulation results indicate that the new algorithm can preserve the hidden information against geometric and non geometric attacks.

**Keywords:** *Blind Digital Image Watermarking, Chaos, Discrete Wavelet Transform, Chaotic Map, Mutation Operation.*

## 1. INTRODUCTION

Watermarking technique is one of the active research fields in recent years, which can be used for protection of multimedia information, content authentication, and so on [1]. The watermark should stick to the host such that it cannot be removed by common signal processing operations. Two main requirements for an acceptable watermarking technique are imperceptibility and robustness. Imperceptibility refers to perceptual quality of the data being protected. Robust watermarking embeds information data within the image with an insensible form for human visual system, but in a way that protects from attacks such as common image processing operations.

In authentication watermarking, tamper localization and detection accuracy are two issues performances. However, most of presented methods in the studied literature cannot obtain precise localization.

A watermark typically contains information about origin, status, and/or destination of the host data [2], [3]. Image scrambling is one of the most prevailing encryption algorithms these years [4], [5], [6]. However, these methods are not so many. The majority of watermarking schemes proposed to date, use watermarks generated from pseudo random number sequences [7]. Chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, and Logistic Map have been widely used to generate watermark sequences [8], [9].

Digital Watermarking techniques can be broadly classified into two categories: Spatial and Transform domain methods. These types of watermark generation schemes require two values (the initial value and the function seed), to recreate the same watermark at a later stage. One of the advantages of these Watermarking methods is the possibility to analyze and control their spectral properties. In most spatial domain schemes, watermark signal is embedded in the LSB (least significant bit) of the pixels in host image in which the robustness against attacks is weak i.e. watermark can be detected easily. Wavelet transform is one of the transform among all others which is widely used for DCT digital watermarking, especially after the wavelet transform becoming the basic technology in JPEG2000 standards several years ago [10]. Many watermarking schemes have been proposed based on wavelet transform, where one of the most well-known method is Cox's watermark embedding scheme [11]. Recently, the multidimensional coupled chaotic map methods were employed in the application of Cryptography [12], [13].

In this paper, a new watermarking method has been developed concerning the security (key space) of the results. For enhancing the security of discrete chaotic watermarking, the concept of using multidimensional coupled chaotic map, with an invariant measure in watermarking, was proposed [14]. The chaotic maps are employed to improve the security of a watermarked image, and an improved mutation operator has been used to encrypt the watermark logo. The upgraded mapping method determines the location of DWT coefficients where the watermark is embedded. The proposed method increases the security of watermarking and also it enables to hide more information in the watermarked image. The robustness of the proposed method has been evaluated against various attacks including common signal processing methods and geometric transformations.

This paper is organized as; section II describes chaotic maps for mutation and scrambling process, and section III presents a short introduction of discrete wavelet transform. The details of watermark embedding and extraction are presented in section IV. Some simulation results are discussed in Section V and the paper is concluded in Section VI.

## 2. CHAOTIC COUPLED MAPS

The chaotic sequences exhibit some important characteristics. Chaotic maps such as Logistic and Chebyshev maps can produce white-noise-like sequences whatever the controlling parameter takes [14], [15].

Coupled map lattices are arrays of states whose values are continuous, usually within the unit interval, or discrete space and time [16]. The pair-coupled map with ergodic behavior can be considered as a two-dimensional dynamical map defined as equation 1 [17]:

$$\begin{cases} X_{n+1} = \frac{4\alpha_1^2 X_n (1 - X_n)}{1 + 4(\alpha_1^2 - 1)X_n (1 - X_n)} \\ Y_{n+1} = \frac{4\alpha_2^2 Y_n (1 - Y_n)}{1 + 4(\alpha_2^2 - 1)Y_n (1 - Y_n)} \end{cases} \quad (1)$$

To initialize the above equation in the original image, selecting a suitable key is very important for security reasons. The key space must be large enough to resist all kinds of attacks. The size of the key space depends on the number of encryption/decryption key pairs that are available in the cipher system [18]. Here, the chaotic maps are employed to generate a key space with the length of  $10^{40}$  numbers to increase the degree of security. In this paper the chaotic map has been employed for the following two processes including; the mutation process for encryption and the selection of embedding location.

### 2.1 Mutation process for encryption

In the computations based on the genetic algorithm method, the mutation is defined as the process of randomly changing the values of genes in a chromosome. The main objective of mutation is to introduce new genetic parameters into the population, thereby increasing genetic diversity. Mutation should be applied with care to do not distort the good genetic properties in highly fit individuals [19]. Fig.1 shows the mutation algorithm employed in this research which uses flip bit mutation process.

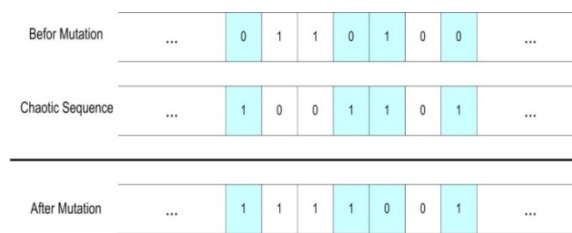


Fig. 1 Example of mutation process.

In the algorithm the mask slides on the chosen bits to find the best value for mutation. (0 goes to 1 and 1 goes to 0). This operates on each pixel of watermark logo as follows:

- Step 1: The initial conditions;  $x_0$  and  $y_0$  as well as the control parameters  $\alpha_1$  and  $\alpha_2$  are set and keep for embedding and data extraction. The Map (Eq. (1)) is computed for  $n=0-999$  which give 1000 numbers to generate the key. This is useful to avoid the transient effect of choosing the initial condition.
- Step 2: Mask is produced by Map (Eq.(1)) for each pixel in the Watermark Logo ( $\text{Mask} \in \{0,1\}$ , if  $X_{n+1} < 0.5$  then  $\text{Mask} = 0$  else  $\text{Mask} = 1$ ).
- Step 3: Apply mutation operator using binary pixel values in the Mask.

### 2.2 Select location embedded

Using the coordinate (i, j), the position of watermark pixel as the initial condition and through setting a value for the control parameter in Eq.(1), chaotic map is iterated after which, the embedding position of the pixels from the watermark image to host image can be obtained. The watermark pixels will get different embedding positions using by chaotic sequence, so, the embedded watermark pixels will spread on the host image randomly.

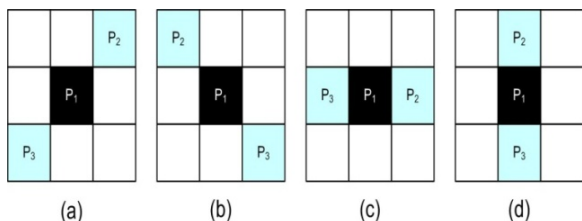


Fig. 2 Types of Neighborhood in the DWT Coefficients.

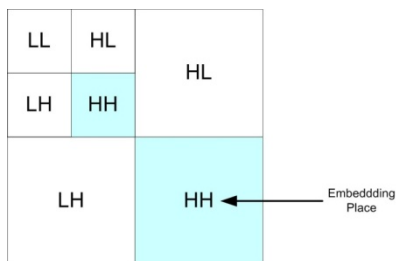


Fig. 3 Discrete wavelet Transform.

### 3. DISCRETE WAVELET TRANSFORM

Discrete Wavelet Transform (DWT) is a multi-resolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains [20]. The basic thought is to decompose the image to sub images with different space and frequency, then, the coefficient is processed.

According, to S. Mallats pyramid algorithm [21] shown in Fig.3, the image after wavelet decomposition is divided into four bands: horizontal direction, vertical direction, diagonal direction and low frequency part which can be decomposed on and on. The wavelet transformed image has three high frequency bands LH<sub>i</sub>, HL<sub>i</sub>, HH<sub>i</sub> (i = 1, 2, 3) and a low frequency band LL<sub>i</sub>, the main energy is concentrated in the low frequency part with a few in horizontal, vertical and diagonal parts.

### 4. WATERMARK EMBEDDING AND EXTRACTION

#### 4.1 Watermark embedding

The embedding process includes the following major steps:

- Mutation operation for encryption of watermark logo is applied.
- Original image using 2D discrete wavelet transform is decomposed into HH, HL, LH and LL coefficients.
- Embedding locations of watermark logo are obtained by chaotic sequence (Eq. (1)).
- Neighborhoods of central coefficient (embedding location) are determined (As shown in Fig. 2).

- Minimum and maximum of the shown coefficients in Fig.2 are calculated and stored in Min, Max variables.
- If pixel value of watermark logo equal to 1, the central coefficient is replaced by  $Max + t$ , else pixel value of watermark logo equal to 0, central coefficient is replaced by  $Min - t$  (t is a threshold value).
- When all pixels were embedded into coefficients, 2D inverse discrete wavelet transform is applied and the watermarked image is obtained. The flowchart of embedding process is shown in Fig.4.

#### 4.2 Watermark extraction

Watermark extraction process is very similar to the embedding process. This process consists of the following major parts:

- The watermarked image is decomposed into HH, HL, LH and LL coefficients by using 2D discrete wavelet transform and HH sub-band is selected for watermark extraction.
- The extraction locations of watermark logo are obtained by chaotic sequence (Eq. (1)).

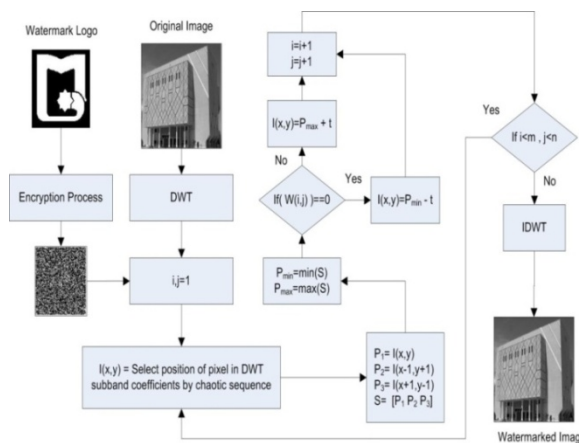


Fig. 4 Embedding flowchart

- Neighborhoods of central coefficient are determined (See Fig.2).
- The median of coefficients shown in Fig.2 is computed and stored in Med variable.
- If the central coefficient is greater than Med, watermark pixel value is 1, else watermark pixel value is 0.
- Mutation operation for encryption of watermark logo is applied.

- When all pixels were extracted from coefficients, the decryption process is applied and final watermark logo is obtained.

The flowchart of extraction process is shown in Fig.5.

## 5. EXPERIMENTAL RESULTS

This section will present and discuss the experimental results of the proposed scheme. Digital watermarking techniques must satisfy the following properties.

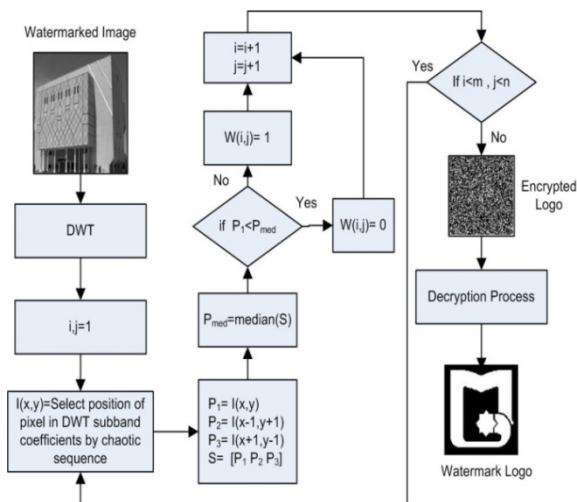


Fig. 5 Extraction flowchart

### 5.1 Evaluation of the effectiveness

To demonstrate the effectiveness of the proposed algorithm, a MATLAB simulation was performed by using a 512×512 pixels gray level image from a building in our university called "Mashhad" as host image and a 64 × 64 pixels binary image that is the logo of our university called "AlReza" as watermark logo.

Fig.6(a) and Fig.6(b) show the original host image and the watermark logo, respectively. The imperceptibility of the proposed watermarking algorithm is demonstrated in these figures. The watermark embedding process is said to be imperceptible if the original data and watermarked data cannot be distinguished. Fig.5(c) - Fig.5(e) show the watermarked image, the extracted watermark logo by correct keys and the extracted watermark logo by incorrect keys, respectively. To quantitatively evaluate the performance of the proposed scheme, the Peak Signal-to-Noise Ratio (PSNR) was adopted to measure the image quality of a watermarked image regarding the original image.

The reliability of the proposed method was measured as the Bit Error Rate (BER) of extracted watermark through this formula:

$$BER = \frac{B}{M \times N} \times 100 \quad (2)$$

Where, B is the number of erroneously detected bits, and M×N is the extracted watermark image dimensions. Therefore, there is no obvious perceptual distortion between the watermarked image and the original one.

### 5.2 Rubustness to attacks

To evaluate the robustness of the proposed method, several attacks have been applied to the watermarked image. In the experiments, both geometric and non geometric attacks were used. The used non-geometric attacks include: JPEG compression:

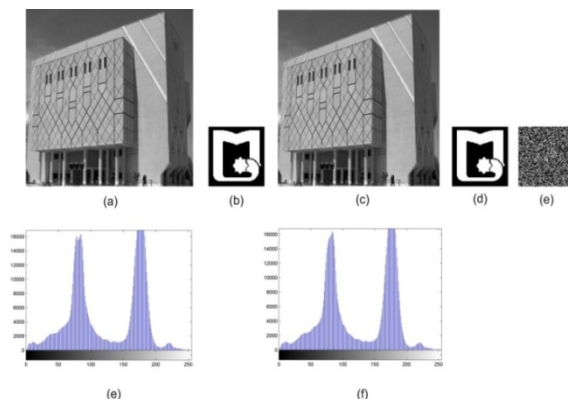


Fig. 6 (a) Original Image, (b) Watermark Logo (c) Watermarked Image (d) Extracted Logo  $\alpha = 0:0.3$ , (e) Extracted Logo  $\alpha = 0:0.33$ .

- JPEG is the first international image compression standard for continuous-tone still images both grayscale and color images [22].
- Median filtering: In median filtering the input pixel is replaced by the median of the pixels contained in the neighborhood [23].
- Low-pass filtering: It produces an output image, which is a smooth version of the original image, devoid of the high spatial frequency components that may present in the image [24].
- Gamma correction: Gamma correction, gamma nonlinearity, gamma encoding, or often simply gamma, is the name of a nonlinear operation used to code and decode luminance or tristimulus values in video or still image systems.
- Blurring: Blurring is used in preprocessing steps, such as removal of small details from an image. Noise reduction can be accomplished by blurring with a linear filter and also by nonlinear filtering [24].

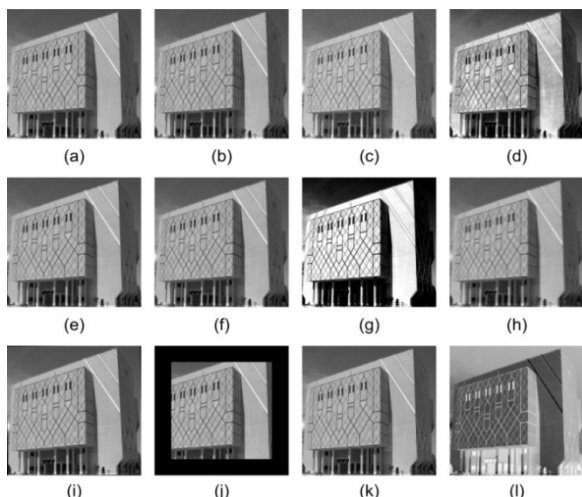


Fig. 7 Watermarked Image under different attacks. (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise (0,0.01), (d)Histogram Equalization, (e) Median filter  $[3 \times 3]$ , (f) low-pass filter  $[5 \times 5]$ , (g) Gamma correction 0.6, (h) motion blur  $45^\circ$  (i) Rotation ( $2^\circ$ ), (j) Cropping (25%), (k) sharpening,(l) complement.

- **Sharpening:** The principal objective of sharpening is to highlight fine details in an image or to enhance detail that have been blurred, either in error or as a natural effect of a particular method of image acquisition.
- **Histogram equalization:** Histogram equalization is a technique which consists of adjusting the gray scale of the image so that the gray level histogram of the input image is mapped onto a uniform histogram [24], [25], [26].
- **Gaussian noise:** Gaussian noise is a statistical noise that has a probability density function of the normal distribution. In other words, the values that the noise can take are Gaussian-distributed. It is most commonly used as additive white noise to yield additive white Gaussian noise [24], [25], [26].
- **Salt and Pepper noise:** Salt and pepper noise is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels [24], [25], [26].

The used geometric attacks include:

- **Rotation:** Rotation of an input image about an arbitrary pivot point can be accomplished by translating the origin of the image to the pivot point, performing the rotation, and then translating back by the first translation offset [24].
- **Cropping:** Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio [24], [27], [28]

### 5.3 The performance of the new algorithm

To evaluate the performance of the new algorithms the PSNR and BER have been computed and compared with some famous benchmarks. The implementation of the new algorithm on Cameraman, Barbara, Peppers and Boat images are presented in the Fig.9 – Fig.11 respectively. The histogram and the extracted logos using different attacks also are presented in the figures. Additionally, Table 1 and Table 2 show the comparison of PSNR and BER for the benchmarks. The results indicate, the proposed watermarking scheme improves the quality of the watermarking as well as increasing the security of images.

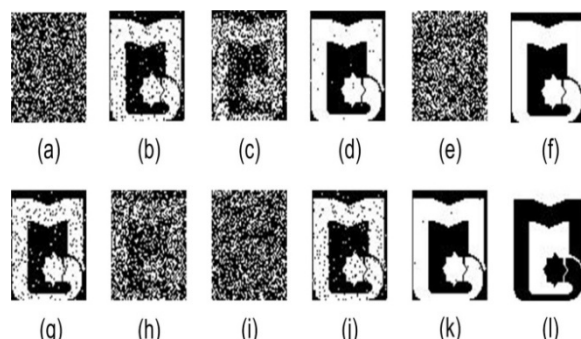


Fig.8 Extracted watermarks under different attacks. (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise (0,0.01),(d) Histogram Equalization, (e) Median filter  $[3 \times 3]$ , (f) Low-pass filter  $[5 \times 5]$ , (g) Gamma correction 0.6, (h) motion blur  $45^\circ$ , (i) Rotation ( $2^\circ$ ), (j) Cropping (25%), (k) sharpening, (l) complement.

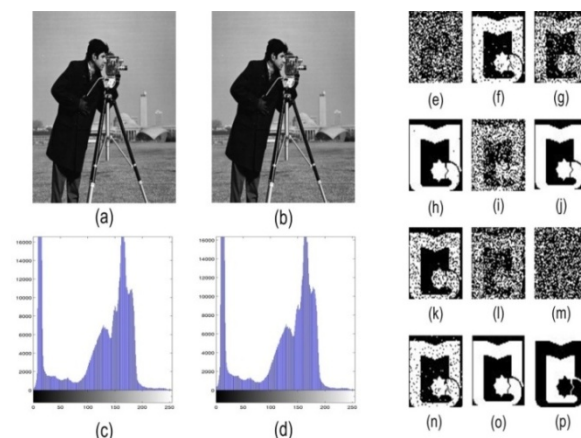


Fig. 9 (a) Original Cameraman image (b) watermarked Cameraman (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include : (e) JPEG compression (f) Salt & pepper noise 10% (g) Gaussian noise (0, 0.01) (h) Histogram Equalization (i) Median filter  $[3 \times 3]$  (j) low-pass filter  $[5 \times 5]$  (k) Gamma correction 0.6 (l) motion blur  $45^\circ$  (m) Rotation ( $2^\circ$ ) (n) Cropping (25%) (o) Sharpening (p) complement.

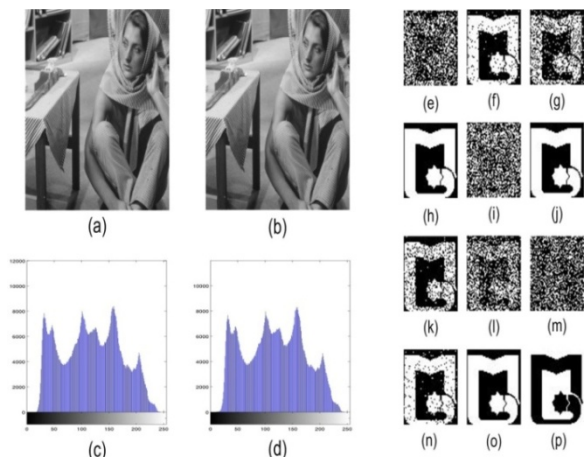


Fig. 10 (a) Original Barbara image (b) Watermarked Barbara (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include: (e) JPEG compression (f) Salt & pepper noise 10% (g) Gaussian noise (0; 0:01) (h) Histogram Equalization (i) Median filter [3\_3] (j) Low-pass filter [5\_5] (k) Gamma correction 0.6 (l) motion blur 45° (m) Rotation (2°) (n) Cropping (25%) (o) Sharpening (p) Complement.

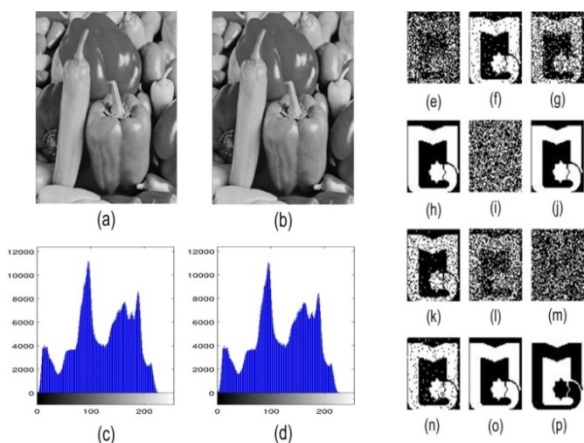


Fig.11. (a) Original Peppers image (b) watermarked Peppers (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include : (e) JPEG compression (f) Salt & pepper noise 10% (g) Gaussian noise (0,0.01) (h) Histogram Equalization (i) Median filter [3x3] (j) low-pass filter [5x5] (k) Gamma correction 0.6 (l) motion blur 45° (m) Rotation (2°) (n) Cropping (25%) (o) Sharpening (p) complement.

## 6. Conclusions

A new watermarking scheme based on the chaotic maps and the discrete wavelet transform was proposed. The scheme was specially designed for the image watermarking and can be used in various multimedia communication applications. The chaotic maps were used for the encryption of the watermarking information and also for the selection of the embedding locations in the transform domain. The proposed algorithm is able to increase the watermarking speed and the level of security.

Without having the correct initial condition, the watermark cannot be successfully detected. The goal was to realize a watermarking method with a private code. Further studies can be done to develop a watermarking method with a public key.

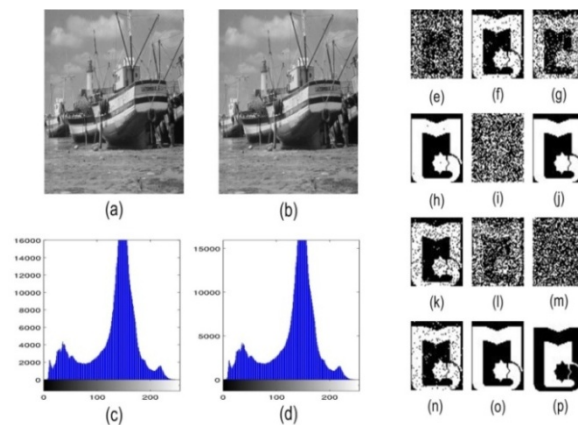


Fig. 12 (a) Original Boat image (b) watermarked Boat (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include : (e) JPEG compression (f) Salt & pepper noise 10% (g) Gaussian noise (0, 0.01) (h) Histogram Equalization (i) Median filter [3x3] (j) low-pass filter [5x5] (k) Gamma correction 0.6 (l) motion blur 45° (m) Rotation (2°) (n) Cropping (25%) (o) sharpening (p) complement.

TABLE 1: SIMULATION RESULTS OF PSNR UNDER DIFFERENT ATTACKS

Attack	Ferdo si Hall	Came ra man	Barba ra	Pepper s	Boat
Without Attacks	45.05	45.85	45.61	45.57	45.56
JPEG compression (75%)	55.12	49.43	44.94	46.27	45.52
Salt & Pepper noise 10%	42.96	43.63	43.32	43.27	43.31
Gaussian noise (0,0.1)	31.46	31.70	31.45	31.51	31.47
Histogram Equalization	28.60	29.41	30.77	29.68	26.99
Median Filtering[3x3]	36.17	49.96	41.79	46.40	44.38
Low pass filter	39.43	51.79	45.90	49.89	48.82
Gamma Correction 0.6	27.13	29.34	26.93	27.22	29.66
Motion Blur 15	30.91	35.62	32.05	35.67	33.76
Rotation 1	31.12	32.90	30.35	32.37	31.09
One quarter cropped	27.67	27.63	27.61	27.67	27.66
Sharpening	30.49	36.62	32.30	34.40	33.33
Complement	27.23	26.59	27.94	27.50	26.00

TABLE 2: SIMULATION RESULTS OF BER UNDER DIFFERENT ATTACKS

Attack	Ferdosi Hall	Camera man	Barbara	Peppers	Boat
JPEG compression (75%)	43.77	42.99	40.11	40.23	39.30
Salt & Pepper noise 10%	4.003	4.63	4.46	4.37	4.63
Gaussian noise (0,0.1)	18.65	21.65	20.62	21.65	20.72
Histogram Equalization	0.31	0.14	0	0.02	0.12
Median Filtering[3×3]	51.87	27.66	44.60	53.07	56.12
Low pass filter	0	0	0	0	0
Gamma Correction 0.6	4.78	12.64	13.57	11.79	8.49
Motion Blur 15	34.30	33.27	34.35	34.00	35.13
Rotation 1	52.56	51.7	52.78	51.85	52.60
One quarter cropped	4.00	4.63	4.46	4.37	4.63
Sharpening	0.024	0	0	0	0
Complement	100	100	100	100	100

## References

[1] Cox IJ, Matthew LM, Jeffrey AB, et al. Digital Watermarking and Steganography. Second edition, Burlington, MA: Morgan Kaufmann Publishers (Elsevier); 2007.

[2] C.H. Huang, J.L. Wua, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences, 179 (2009), pp.791-808.

[3] Y. Liu, J. Zhao, A new video watermarking palgorithm based on 1-D DFT and Radon transform, Signal Processing, 90, (2010), pp.626-639.

[4] H. Wei, M. Yuan, J. Zhao, Z. Kou, Research and Realization of Digital Watermark for Picture Protecting, First International Workshop on Education Technology and Computer Science, IEEE, Vol. 1, 2009, pp.968-970.

[5] X. Li, A New Measure of Image Scrambling Degree Based on Grey Level Difference and Information Entropy, 2008 International Conference on Computational Intelligence and Security, Vol. 1, 2008, pp.350-354.

[6] Z.W. Shen, W.W. Liao, Y.N. Shen, Blind watermarking algorithm based on henon chaos system and lifting scheme wavelet, International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 2009, pp.308-313.

[7] M. Barni, F. Bartolini, A. Piva, Improved wavelet based watermarking through pixel-wise masking, IEEE Trans Image Process 10, (2001), pp.783-791.

[8] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis S. sekeridou, I. Pitas, Markov chaotic sequences for correlation based watermarking schemes, chaos, solitons & fractals 17, (2003), pp.567-573.

[9] S. Nikolaidis, I. Pitas, Comparison of different chaotic maps with application to image watermarking, In: Proceedings of IEEE international symposium on circuits and system Cryptography based on chaotic random maps with position dependent weighting probabilities Chaos, Solitons & Fractals 35, (2008), pp.362-369.

[10] Cox and M.L. Millier, A review of watermarking and the importance of perceptual modeling, Proc. of SPIE 3016 (1997), pp. 92-99.

[11] Cox I, Miliier ML. A review of watermarking and the importance of perceptual modeling. Proc of SPIE 1997;3016:929.

[12] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, Cryptography based on chaotic random maps with position dependent weighting probabilities Chaos, Solitons & Fractals 35, (2008), pp.362-369.

[13] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Physics Letters A, 366, (2007). Pp.391-396.

[14] G. Voyatzis, I. Pitas, Digital image watermarking using mixing systems, Computers & Graphics 22 (1998) 405-416.

[15] R. Ursulean, Reconsidering the Generalized Logistic Map as a Pseudo Random Bit Generator, Elektronika IR Electrotechnika, 56, (2004), pp.10-13.

[16] Kaneko K. Super transients spatiotemporal intermittency and stability of fully developed spatiotemporal chaos. Phys Letter A, 1990;149(2003), pp.10-12.

[17] Jafarizadeh MA, Behnia S, Faizi E, Ahadpour S. Global synchronization and anti-synchronization in n-coupled map lattices. Int J Theor, Phys, 47, 2008, p.10-15.

[18] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.

[19] Andries P. Engelbrecht, Computational Intelligence An Introduction, Second Edition, John Wiley & Sons, 2007.

[20] S. Mallat, The theory for multi-resolution signal decomposition: The wavelet representation, IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, Jul. 1989, pp. 654-693.

[21] S. Mallat, Multi-frequency channel decompositions of images and wavelet models, IEEE Trans. Acoust., Speech, Signal Processing, vol. 37, no. 12, Dec. 1989, pp. 2091-2110.

[22] T. Acharya and P. Tsai, JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures, Wiley, Hoboken, NJ, 2004.

[23] T.S. Huang, G. I. Yang, and G. Y. Tang, A Fast Two-dimensional Median Filtering Algorithm, IEEE Trans. Acoustics, Speech, and Signal processing, ASSP-27, 1, 1979, pp.13-18.

[24] R. C. Gonzalez, R. E. Woods, Digital Image Processing, Addison-wesley, Reading, MA, 1992.

[25] W.K. Pratt, Digital Image Processing, 2nd ed., Wiley, New York, 1991.

[26] A. Rosenfeld, A. C. Kak, Digital Picture Processing, 2nd ed., Vol.1, Academic Press, 1982.

[27] P. Lee, Yi Chenb, S. Pei, Y. Chena, Reply to the comment Keystream cryptanalysis of a chaotic cryptographic method, Computer Physics Communications 160, (2004), pp. 208-214.

[28] M. Falcioni, L. Palatella, S. Pigolotti, Properties making a chaotic system a good pseudo random number generator, Phys. Rev. E 72, (2005), pp.162-170.

**Jila Ayubi** obtained her BSc and degrees in electrical engineering from University of Orumieh, Iran in 2009 and is an MSc student at University

of Sistan and Baluchestan. Her areas of research include signal and image processing.

**Shahram Mohanna** received his BSc and MSc degrees in electrical engineering from the University of Sistan and Baluchestan, Iran and the University of Shiraz, Iran in 1990 and 1994, respectively. He then joined the University of Sistan and Baluchestan, Iran. In 2005, he obtained his PhD degree in communication engineering from the University of Manchester, England. As an assistant professor at the University of Sistan and Baluchestan, his areas of research include signal processing and applied electromagnetic. Dr. Mohanna published several journal papers and attended a number of international conferences.

**Farahnaz Mohanna** received her BSc and MSc degrees in electronic engineering from University of Sistan and Baluchestan and University of Tehran, Iran in 1987 and 1992, respectively. In 1993, she joined the University of Sistan and Baluchestan, Iran. She earned her PhD degree in the field of Computer Vision and Image Processing from the University of Surrey, England in 2003. As an assistant professor at the University of Sistan and Baluchestan, her research interests are signal and image processing. Dr. Mohanna published several Journal and conference papers in the field of signal processing and communications.

**Mehdi Rezaei** received his BSc and MSc degrees in electrical engineering from Amir Kabir University of Technology, Tehran and Tarbiat Modares University of Tehran, Iran in 1992 and 1996, respectively. In 1996, he joined the University of Sistan and Baluchestan, Iran. He earned his PhD degree in communication engineering from the Tampere University of Technology, Finland in 2008. As an assistant professor at the University of Sistan and Baluchestan, his research interests are signal and image processing and video coding. He published several Journal and conference papers in the field of image and video processing. Dr Rezaei got the Nokia Foundation Award in 2005 and 2006.