Robust Digital Images Watermarking Technique Based on Eigenvectors

Alyaa Jaber Jalil
College of Science, University of Basrah
aliaa.jaber@yahoo.com

Abstract

The growth of new imaging technologies has created a need for techniques that can be used for copyright protection of digital images. In this paper, a new and robust spread spectrum based watermarking scheme has been proposed. The proposed scheme depend on both Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). First, we decompose the image by DWT into a single level. Then, the approximation part is divided into blocks. The embedding is done in an adaptive fashion depending on the Eigenvalues (*Ev*) of the block. A chaotic sequence of real numbers, depends on a secret key, is embedded as a watermark in the DCT coefficients of the selected blocks. Detection stage generates a watermark which would be compared with the original watermark, by the correlation measure, to determine the existing of the watermark or not. Different tests have been experimented to explain the transparency and the robust of the proposed scheme.

Keywords: Image watermarking, Wavelet transform, Chaos theory, Transparency,
Uniqueness of watermark, Eigenvectors ,Eigenvalues.

تقنية علامة مائية متينة للصور الرقمية المعتمدة على المتجهات الذاتية

علياء جابر جليل
فظ عِلمِك ثتزكئة ككبطكعكلم جئلعبطكبسب.
E-mail: aliaa.jaber@yahoo.com

المستخلص

النمو الحالي في تكنولوجيا الصور ولدت الحاجة إلى تقنيات استخدمت لحماية حقوق الطبع للصور الرقمية. في هذا البحث, تم اقتراح منهج علامة مائية جديد ومتين معتمد على الطيف المنتشر. المنهج المقترح يعتمد على كل من التحويل المويجي المنفصل (DWT) والتحويل ألجيبي المنفصل (DCT). أولا, قمنا بتحليل الصورة إلى مستوى واحد باستخدام (DWT). بعد ذلك تم تقسيم جزء التقريب إلى كتل. التضمين تم بطريقة متكيفة وذلك بالاعتماد على القيم الذاتية للكتلة. سلسلة مشوشة جدا من الأرقام الحقيقية, المولدة بالاعتماد على مفتاح سري, تم اعتبارها علامة مائية سيتم تضمينها في معاملات DCT من الكتل المختارة. مرحلة اكتشاف العلامة المائية تولد علامة يتم مقارنتها مع العلامة الأصلية, باستخدام مقياس الارتباط, لتحديد وجود العلامة المائية أو عدمه. عدة فحوصات تم اختبارها لتوضيح الشفافية والمتانة للمنهج المستخدم.

الكلمات المفتاحية: العلامة المائية للصور, التحويل المويجي, نظرية التشويش, الشفافية, وحدانية العلامة المائية, المتجهات الذاتية , القيم الذاتية.

Introduction

The need for watermarking of images has gained importance in the past few years [1,2,3], owing to the rapid growth of such digitized media over the Internet. Images can now easily be copied and distributed, with little or no control of ownership. Traditional encryption systems exist, which allow only valid key-holders to access data. However, once decrypted, this data is again susceptible to unauthorized reproduction. Therefore, digital watermarking schemes are needed in order to serve as standalone or complementary copyright protection systems. A digital watermark is a secret code carrying identification information about the copyright owner or creator. Generally, a watermark is embedded such that it is invisible. In order to be effective, a watermark should satisfy certain basic criteria:

Transparency: The watermark should not degrade or affect the image quality in any perceptible manner.

Robustness: It should be resistant to attacks, both intentional and unintentional, such as digital-to-analog conversion, analog-to-digital conversion, re-sampling, re-quantization and compression distortion (e.g. JPEG).

False positive rate (uniqueness of watermark): A false positive is a detection of a watermark in an image that does not actually contain that watermark.

Two major applications of digital watermarking are copyright protection (proving ownership of data) and data authentication (for use as evidence against crimes). In such cases, the data needs to be proved reliable and unmodified. Current techniques for watermarking concentrate mainly on images and can be classified into two groups. The first group is based on spatial domain techniques, which embed the watermark by directly modifying the pixel values in the image. The second group comprises of transform domain methods, which embed the watermark by modulating the transform domain coefficients of the data. The transform methods are more complex, but more robust than the spatial methods [1].

Many watermarking algorithms have been proposed in recent years. In related works, Cox et al [4] realized that in order to obtain a robust

watermark, the watermark should be embedded in the low frequency components of the image. They argue that the most common image processing operations mainly change the high frequency components. Moreover, if low frequency components are changed, the image quality is degraded and the watermark becomes meaningless. Drawback of Cox et al is its complexity, as the global DCT is performed before embedding the watermark. Xia et al [5] the basic idea of Cox et al is extended to DWT, and the watermark is embedded in the largest coefficients of the high frequency subbands. The multiresolution nature of wavelet transform is exploited to obtain perceptually invisible watermark. However, embedding the watermark in high frequency subbands makes this technique vulnerable to attacks such as compression and lowpass filtering. Improvements in performance can be obtained by exploiting the characteristics of the human visual system (HVS) in the watermarking process [6, 7]. Using the visual mask, the watermark is embedded in detail subbands at the first level of the decomposition [7]. Robustness to attacks that remove high frequency components of the image is achieved by embedding the watermark in the low frequency components [8].

The rest of the paper is organized as follows: Section 2 provide an overview of chaos system. Wavelet transform is presented in Section 3. Section 4 details our based watermarking scheme. In Section 5, experimental results has been discussed. While the conclusion marks are listed in Section 6.

2. Chaos Theory

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit extreme sensitivity to initial conditions and have random-like behaviors. Since its discovery by Lorenz E. N. in 1963 [9], chaos theory has become a new branch of scientific studies today such as in cryptography. For simplicity, one-dimensional maps are discussed. Consider a discrete dynamical system in the general form of:

$$x_{k+1} = f(x_k), \quad f : I \longrightarrow I, \; x_0 \in I \qquad \ldots(1)$$

where f is a continuous map on the interval $I = [0, 1]$. The most important feature of the chaotic system is its sensitivity to the initial conditions [10].

$$\exists \delta > 0, \; \forall x_0 \in I, \; \varepsilon > 0 \;\; \exists n \in N, y_0 \in I : |x_0 - y_0| < \varepsilon \Rightarrow |f^n(x_0) - f^n(y_n)| > \delta \qquad \ldots(2)$$

The sensitivity to initial conditions of chaos is commonly utilized for the keys of cryptosystems. In this paper, the chaotic Logistic map has been used. It is defined as follows [10]:

$$x_i = (B*(A^{\wedge 2} - x_{i-1}^{\wedge 2}))-A \quad \ldots(3)$$

Where x_0 is initial condition, A and B are two parameters, $0 > I >= L$ (length of the sequence). We set A = 0.5, B = 4. Figure(1) explain the great difference between two sequences generated by very similar initial conditions.

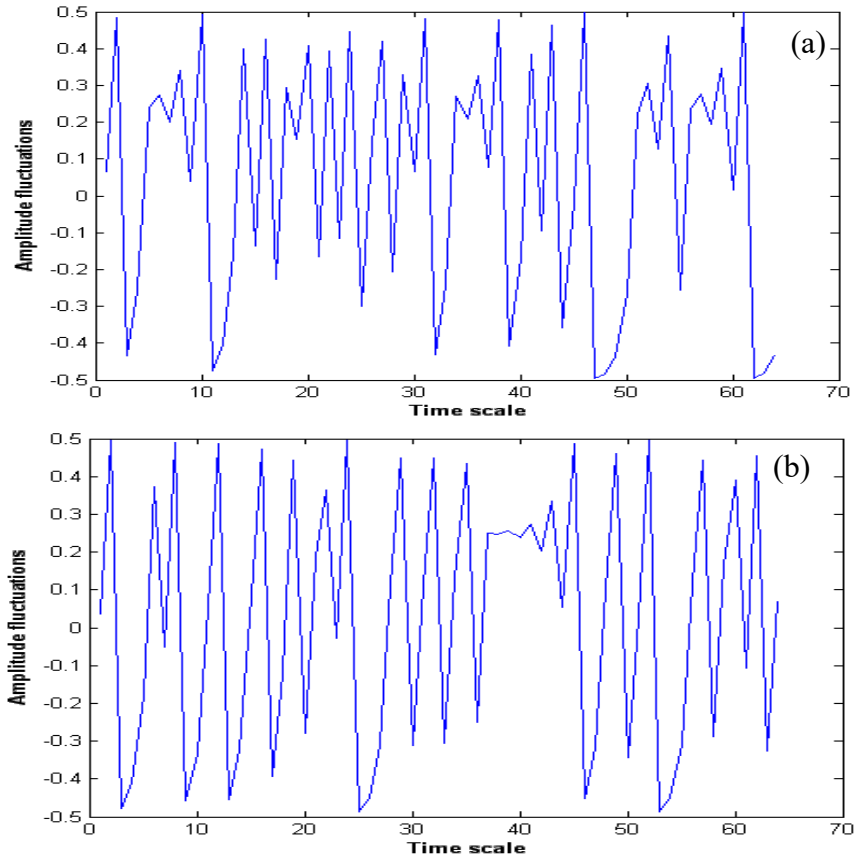

Figure (1): a) chaotic of length 64 generated by X_0 = -0.33.

Wavelet Transform

The discrete wavelet transform is used to transform image signal from spatial domain to wavelet domain. The wavelet transform performs an octave subband decomposition of an image. The output of the first analysis stage is the low-low (LL) subband (an approximation of the original image), which is the most important part, since it holds the low frequency content; the high-low (HL) subband (the horizontal detail); the low-high (LH) subband (the vertical detail); and the high-high (HH) subband (the diagonal detail) are together hold the high frequency, as shown in Figure (2). The LL subband can be decomposed to produce multiple scale wavelet decomposition.

Wavelet decomposition for birds's image in 1-level of wavelet transform using Haar filter is shown in Figure (3). The original signal can be reconstructed by applying inverse DWT (IDWT) on those coefficients. More information about wavelet transform can be found in [11, 12].

One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the DCT [13]. This allow us to embed high energy watermarks in the regions that the HVS less sensitive to it, such as detail bands {LH, HL, HH}. And embed robust watermarks in the approximation band {LL}.

LL (Approximation)	HL (Horizontal)
LH (Vertical)	HH (Diagonal)

Figure (2) : Wavelet Subband Images of 2-D, 1-level.

Figure (3): The original image and 1-level wavelet decomposition of birds's image.

4. The Proposed Watermarking Scheme

The model of our scheme is given in Figure (4). The inputs of the system are watermark (W), which is a sequence of chaotic real numbers. The watermark generated depending on the initial condition (key) to achieve system security. The x is the original input image. In the first stage, the watermark (W) is embedded in the cover (x) (host image) to produce the watermarked image (y). Which is transmitted over the channel. This accounts for all the manipulations the watermarked image may undergo after embedding stage. After the watermarked image (y) has passed through channel, it enters the detector, whose scope is to retrieve the hidden information. Beside the watermarked image, inputs to the detector are: the key used in the process of embedding the original image (x) and the original watermark (W). The output of the watermark recovery process is the recovered watermark (W'), which is compared with W to decide if it equal to W or not .

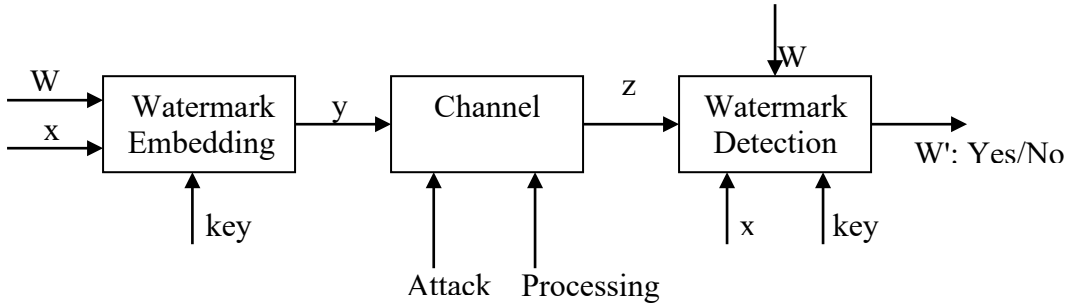

Figure (4): Model of the proposed watermarking scheme.

Embedding Steps

The proposed embedding algorithm consist of the following steps:

1- Generate the watermark sequence (W), which is chaotic real numbers generated using equation (3).

$W = \{w_1, w_2, \ldots, w_L\}$

where L is the length of the watermark sequence, which is equal to 64 The input key is x_0.

2- The original image (x) is decomposed into 1-level by using DWT as in Figure (2). In our approach, the watermark will be embedded in the only approximation part (LL), for more robust.

3- Divide the approximation part into blocks of the same size (8x8).

4- Compute the entropy (*H*) for each block, which is computed as follows:

$$H = -\sum_{i=1}^{n} P(x_i).\log(P(x_i)) \quad \ldots(4),$$

where $P(x_i)$ is the probability of x_i of 1-D vector of the entered block, n is the vector length 64.

Figure (5) explain the H of the approximation (LL) blocks (8x8) of birds's image.

5- Select only the blocks that have *H* higher than a given threshold value (Thr).

6- For each selected block, compute the DCT, then embed the watermark W to DCT coefficients as follows:

$$V_i' = V_i + \alpha w_i \quad \ldots(5),$$

where V_i is the 1-D vector of the original DCT coeffiecints, V'_i is the adjested coefficients, and α is the scalling factor (determines watermark strength).

7- Compute the inverse DCT for each watermarked block.

8- Reconstruct the image through synthesis the approximation and the details by using the inveres DWT (IDWT) to obtain the watermarked image (y).

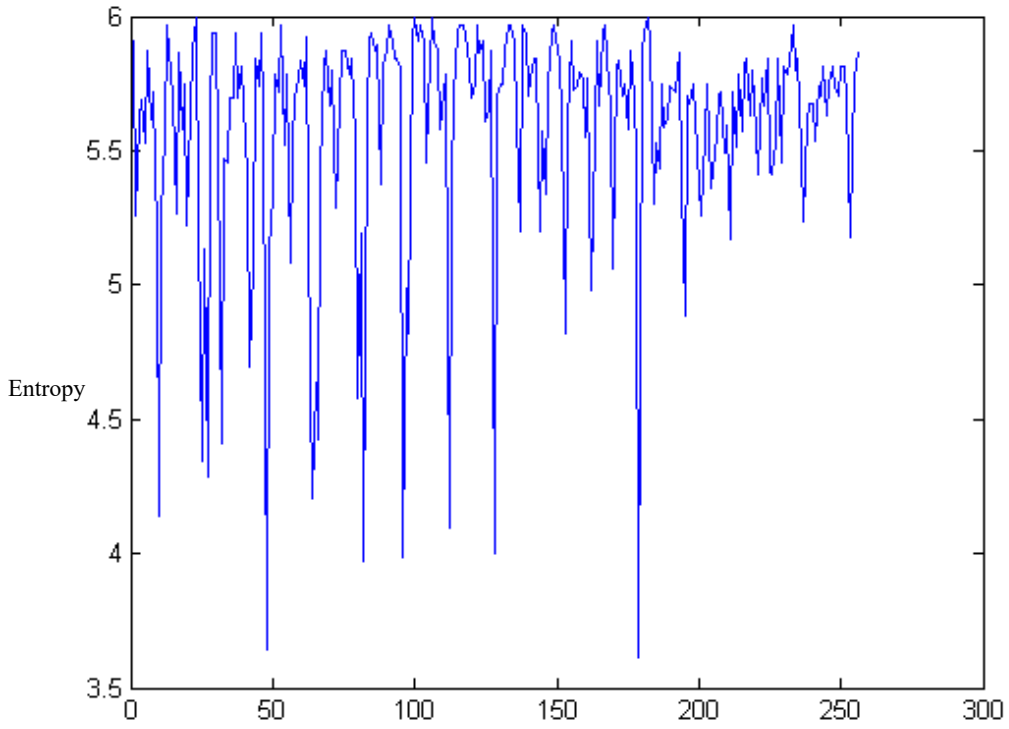

Figure (5): Entropy of the approximation blocks of birds's image

Detection Steps

The proposed detection algorithm consist of the following steps:

1- Generate the same watermark W using the same secret key that has been used in

step (1) of the embedding steps.

2- Decompose the watermarked image y, and the original image x into 1-level using DWT.

3- Divide the approximation part of image y, and image x into blocks of the same size (8x8).

4- Select any block B_Y has an *H* higher than threshold from the blocks of image y. And select any block B_X also has an higher *H* from the blocks of image x.

5- Compute the DCT coefficients B_X', B_Y' for the blocks B_X and B_Y, respectively.

6- Compute the reconstructed watermark W' by subtract B_Y' from B_X',

$$W'=B_Y'-B_X'. \qquad \ldots(6)$$

7- Compare W and W' using the correlation (R) as the similarity measure, is computed as:

$$R = \frac{\sum_{i=1}^{n}(W_i - A)(W'_i - B)}{\sqrt{(W_i - A)^2 (W'_i - B)^2}} \qquad \ldots(7),$$

where A=mean(W), B=mean(W') , n is vector length.

8- Detection is successful if the R value exceeds experimentally determined threshold of 0.6.

5. Principle Component Analysis(17,18)

PCA is the simplest of the true Eigenvector based multivariate analysis. Mathematically, it is an orthogonal linear transformation that transforms the data to a new coordinate system. The use of Eigenvalues and vectors is commonly called as Principal Component Analysis. With PCA, the image must be used of same size and they are normalized to a particular size for the usage. In PCA, dimension of data is reduced and decomposes the image structure into orthogonal and uncorrelated components which are the Eigenvector. The image can be represented as a weighted sum of the Eigenvectors. Mathematically, principal component analysis approach converts a set of correlated variables into a set of linearly uncorrelated variables. Each image in the training set contributes to the Eigenvectors. This can be displayed as an Eigenvector expresses the data in such a way as to highlight the similarities and differences.

6. Calculations Of Eigenvalues And Eigenvectors(19,20,21):

In linear algebra, the Eigenvectors of a linear operator are non-zero vectors which, when operated on by the operator, result in a scalar multiple of them. The scalar is then called the Eigenvalue (λ) associated with the Eigenvector(X).

Eigenvector is a vector that is scaled by a linear transformation. It is a property of a matrix. When a matrix acts on it, only the vector magnitude is changed not the direction.

$$AX=\lambda X \qquad (1)$$

Where A is a matrix

By using equation(1), following equation has been derived :-

$$(A-\lambda I)X=0 \qquad (2)$$

Where I is the n x n Identity matrix. This is a homogeneous system of equations, and from fundamental linear algebra, it has been proved that a nontrivial solution exists if and only if.

It should immediately be clear that, no matter what A and λ are, the vector x = 0 (that is, the vector whose elements are all zero) satisfies this equation.

$$D(A-\lambda I)=0 \quad (3)$$

Where D denotes determinant. When evaluated, becomes a polynomial of degree n. This is known as the characteristic equation of A, The characteristic polynomial is of degree n. If A is n x n, then there are n solutions or n roots of the characteristic polynomial. Thus there are n Eigenvalues of A satisfying the equation,

$$A\ Xi=\lambda\ Xi \quad (4)$$

Where i=1, 2, 3….n If the Eigenvalues are all distinct, there are n associated linearly independent Eigenvectors, whose directions are unique, which span an n dimensional Euclidean space.

7. Experiment Results

To show the robustness of the proposed algorithm under common image processing

operations, such, we have processed the watermarked image using the following operations:

the transparency of embedded data, the uniqueness of watermark, and the compression [14].

To measure the similarity between the original image x and the watermarked image y, PSNR measure has been used [15]. Typical PSNR values ranges between 20 and 40 decibels (dB). In this paper, different experiments has been tested to explain the robust and the transparency of the proposed watermarking scheme. In all experiments, birds's image has been used as a cover (an gray level image of size [256x256]), and the watermark of Figure (1 (a)), so, key = x_0 = -0.33. Haar filter has been used in DWT. α is set to 0.5.

Experiment 1

In this experiment, the transparency has been tested for different threshold values (Thr). In Table (1), different thresholds have been used. First column gives the threshold value, the second column gives PSNR, while the third column gives the number of selected blocks which has entropy higher than threshold.

Table (1): Experimental results for different thresholds.

Threshold (Thr) value	PSNR (dB)	No. selected blocks in LL
5.0	51.1568	235
5.1	51.1622	232
5.2	51.1525	225
5.3	51.1625	215
5.4	51.1310	207
5.5	51.0946	192
5.6	51.0455	170
5.7	50.9672	138
5.8	50.8019	89
5.9	50.6616	41

Experiment 2

In this experiment, the uniqueness of watermark has been tested. 500 random watermarks were generated, out of which only one matched the original watermark. The output of the detector is shown in Figure (6). The response of the correct watermark is 0.85713, which is much stronger than the threshold value of 0.8. This indicates that the proposed algorithm has very low false positive response rates.

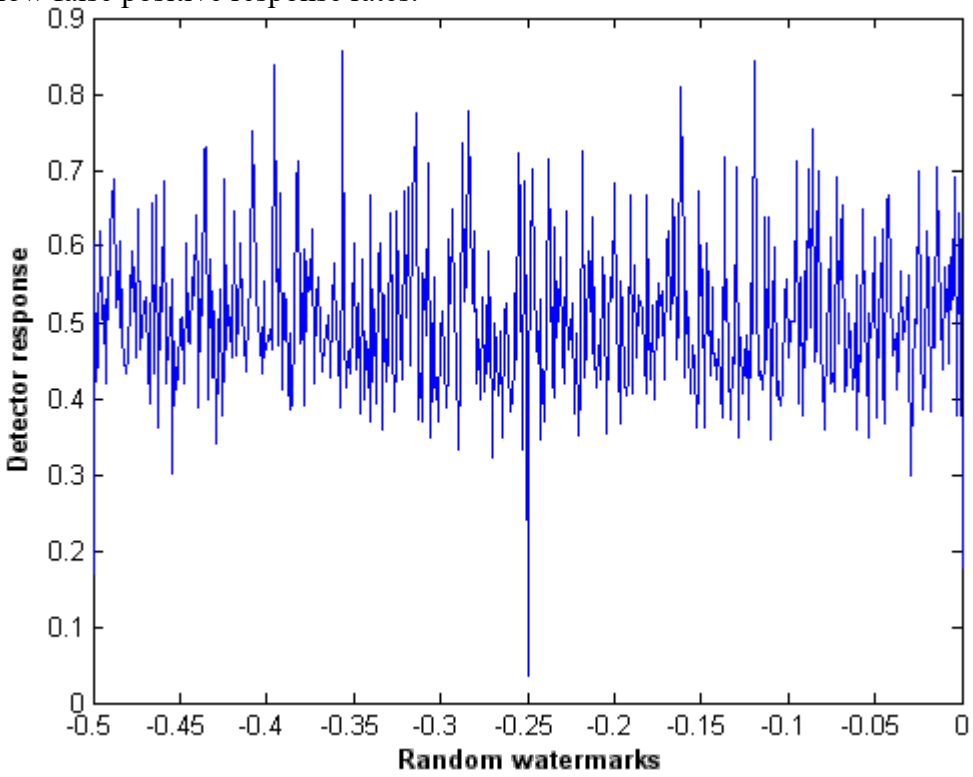

Figure (6): Uniqueness of watermark.

Experiment 3

In this experiment, the compression distortion has been tested. The watermarked image has been compressed by using the hard-compression technique, which depends on the wavelet transform. More information about this technique in [16]. The detector output 0.85713 when the watermarked image compressed in 80, 100, and 120 threshold values. Figure (7) explain the compressed cover in 80 threshold, which explain the resistance of the proposed scheme against compression attack.

(a) (b)

Figure (7): (a) original image, (b) Compressed watermarked image in 80 threshold value.

Experiment 4

In this experiment, our embedding has been compared to the only DCT-based watermarking scheme. In Table (2), different thresholds have been used. From Table (2), we notice the lower PSNR than the proposed scheme in Table (1).

Table (2): Experimental results for different thresholds values to only the DCT-based watermarking scheme.

Threshold (Thr) value	PSNR (dB)	No. selected blocks
5.0	48.6982	211
5.1	48.6015	168
5.2	48.5240	132
5.3	48.4738	107
5.4	48.4040	72
5.5	48.3497	46
5.6	48.3170	30
5.7	48.2762	9
5.8	48.2655	4
5.9	48.2587	0

8. Conclusions

Experimental results show that the proposed algorithm is robust to common image processing operations such as, the transparency of embedded data, the uniqueness of

watermark, and the compression.

We have presented a new, robust wavelet-DCT-based watermarking scheme, based on spread spectrum approach. Based on the results obtained and detailed in the previous sections, we include the following:

- During our experiment 1, we find that as the threshold value is increased, the No. of the selected blocks is decreased and vice versa. Figure (8) shows No. of the selected blocks versus the threshold value to wavelet-DCT-based watermarking scheme.

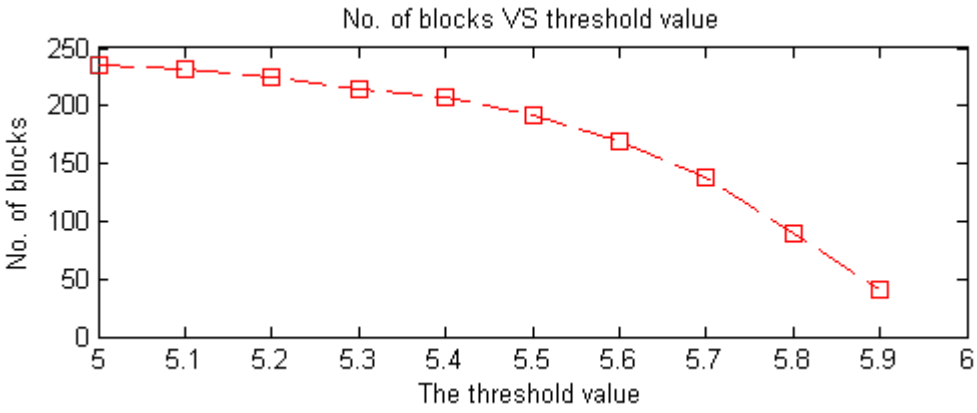

Figure (8): PSNR versus threshold value for birds's image.

- The proposed scheme is shown to be resistant against false positive rate. So, 500 random watermarks were generated, out of which only one matched the original watermark as shown in experiment 2.

- Figure (7) explain the compressed cover in 80 threshold, which explain the resistance of the proposed scheme against compression attack.

- Our scheme has very high PSNR than only DCT-based method as in experiments 1 and 4. Thus, the use of wavelet transform makes the watermarked images more robustness and transparency embedded data in the cover.

9. References

[1] JavadiAbhari Ali ., *"Digital Image Watermarking: ELE 488 final project, , Princeton University, fall 2011.*

[2] Khan A., Tahir S. F, and Majid A., and Choi, *"Machine Learning Adaptive*

Watermarking Decoding in iew of Anticipated Attack", Pattern Recognition, Vol.

41, No. 8, pp. 2594-2610, August 2008.

[3] Zheng D., Wang S., and Zhao J., *"RIS Invariant Image Watermarking Algorithm*

with Mathematical Modeling and Analysis of the Watermarking Processes", IEEE

Trans. Image Processing, Vol. 18, No. 5, pp. 1055-1068, 2009.

[4] Bianchi Tiziano and Piva Alessandro,*"Secure Watermarking for Multimedia Content Protection",* IEEE single processing magazine, March 2013.

[5] Kumar Anubhav, Member, IACSIT, and Anuradha, *"A Novel Watermarking Algorithm for Color Images Based on Discrete Wavelet Transform",* International Journal of Computer and Electrical Engineering, Vol. 6, No. 4, August 2014.

[6] Podilchuk C. I. and Zeng W., *"Image-adaptive Watermarking Using Visual*

Models", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp.

525-539, May 1998.

[7] Barni M., Bartolini F., and Piva A., *"Improved Wavelet Based Watermarking*

Through Pixel-wise Masking", IEEE Trans. Image Processing, Vol. 10, No. 5, pp.

783-791, May 2001.

[8] Tiwari Gangadhar, Nandi Debashis , "Non-Invertible Wavelet Domain Watermarking using Hash Function", August 2014 .

[9] Dr. Luri M. Robert, *" A Review and Demonstration of The Essence of Chaos by Edward N. Lorenz ,* Essence of Chaos review of book and adaptation to Mathematica Version9 submitted 2013.

[10] Feldman P. David, "*Introduction to Chaos and Dynamical Systems ",*Exploring Complexity froman SFIP erspective ,Feb.6–8- 2011.

[11] Burrus C. Sidney , Gopinath Ramesh, Guo Haitao.,*" Wavelets and Wavelet Transforms", July 22, 2015.*

. [12] Saito Naoki., *"Frequently Asked Questions on Wavelets"*, Department of Mathematics University of California Davis, CA 95616 USA email:saito@math.ucdavis.edu January 6, 2014.

[13] *Salunkhe Tejaswita, Nayak Chhaya*, *"Review of Digital Watermarking Techniques"*,

International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2015.

[14] Deshpande Ketki, and Kamble D. Nagesh, "Application of Data Hiding in Audio-Video using Advance Algorithm", Department of Computer Science & Engineering, Shreeyash College of Engineering & Technology, Aurangabad, India ,Vol.5, No.6 (Dec 2015)

[15] *Chetan , Sharma Deepak,"A Review on Image Compression & Steganogaphy ",*

India, ISSN: 2277 128X , Volume 5, Issue 4, 2015.

[16] *Rathee Monikam ,Vij Alka,"Image compression Using Discrete Haar Wavelet Transforms", M-Tech Scholar, PDM college of Engineering, Bahadurgarh,* Volume 3, Issue 12, June 2014.

[17] Richardson Mark " Principal Component Analysis" May 2009.

[18] At-Sahaliay Yacine , Xiuz Dacheng "Principal Component Analysis of High Frequency Data"Department of Economics Princeton University and NBER, October 7, 2016.

[19] Joyce D "Eigenvalues, eigenvectors, and eigenspaces of linear operators" Math 130 Linear Algebra, Fall 2015.

[20] Geuvers H.Kissinger A. ," Matrix Calculations : Eigenvalues and Eigenvectores", Institute of computing and Information Science , Radboud University Nijmegen, Spring 2016.

[21] Jauregui Jeff, "Principal component analysis with linear algebra",August 31, 2012.