Improve Watermark Security Via Wavelet Transfrom And Cdma Techniques

Yhya. R. Kuraz
yhya.kuraz@gmail.com

Modar A.H.
modar.a.h@gmail.com

Computer Department, College of Engineering, University of Mosul, IRAQ

Abstract

With the growth of multimedia systems in distributed environments, the research of multimedia security as well as multimedia copyright protection becomes an important issue. As a potential and effective way to solve this problem, digital watermarking becomes a very active research area of signal and information processing. Many watermark algorithms have been proposed to address this issue of ownership identification. Discrete Cosine Transform (DCT) based spread-spectrum watermarking is one of the famous techniques. Another possible domain for watermark embedding is the wavelet domain. One of the many advantages over the Discrete Wavelet Transform (DWT) is that more accurately model aspects of the human visual system (HVS).

In this paper a proposed algorithm is defined based on the combination between the benefits provides by using wavelet domain and profits of Code division multiple access (CDMA) spread-spectrum technique. A pseudo-random sequence (key) that related to hidden message is embedded into the significant DWT coefficients of a cover image to produce a watermarked image. Experimental results demonstrate that the proposed algorithm is perceptual invisible and robust against many attacks such as lossy image compression and Additive White Gaussian Noise (AWGN).

Keywords: digital watermark, wavelet transform, CDMA technique.

تحسين امن العلامات المائية باستخدام التحويل المويجي وتقنيات الوصول المتعدد بواسطة تقسيم الشفرة

د. يحيى رجب محمد
كلية الهندسة/جامعة الموصل

مضر أحمد حمودي
كلية الهندسة/جامعة الموصل

الخلاصة

إن تنامي أنظمة الوسائط المتعددة في الحياة العملية أدى إلى جعل البحث في مشكلة سرية الوسائط المتعددة بالإضافة إلى حماية عملية نسخ الوسائط المتعددة أمرا مهما.لحل هذه المشكلة بطريقة جيدة برزت طريقة العلامة المائية الرقمية كطريقة فعالة جدا وأخذت مكانا واسعا في حيز بحوث معالجة الإشارة والمعلومات . اقترحت طرائق عديدة لطمر العلامة المائية وذلك لإثبات حق الملكية كمثال على ذلك تحويل الجيب تمام المقطع المعتمد على الطيف الممتد (المنتشر) والتي تعد من تقنيات العلامة المائية المشهورة. يمكن الاستفادة من التحويل المويجي المقطع في صنع العلامة المائية لما له من مزايا عديدة في ناحية معالجة الإشارة الرقمية إذ انه يعتبر النموذج الأكثر دقة في مراعاة نظام الرؤيا البشرية. تم اقتراح طريقة لإنشاء العلامة المائية وذلك بالمزج مابين مزايا التحويل المويجي المقطع ومحاسن الطيف المنتشر في تقنيات الوصول المتعدد.إذ تم استخدام إشارة تسلسل عشوائي غامض لها علاقة بالمعلومات المراد إخفائها و الصور هي المميزة الناتجة من التحويل المويجي المقطع للصورة التي استعملت كغطاء للمعلومات لإنتاج ما يسمى بالصورة المحتوية على العلامة المائية.أبرزت النتائج العملية بأن الطريقة المقترحة تعطي علامة مائية مخفية بشكل موثوق و صامدة أمام المؤثرات على الصور الرقمية مثل كبس الصور ذو الفقد و الضوضاء الكاوسية البيضاء المضافة .

Received 24 May 2007 Accepted 6 Sept 2007

1. Introduction:

As multimedia data becomes wide spread, such as on the internet, there is a need to prevent (or at least deter) the illegal copying, forgery and distribution of such data (digital images, video and audio).

Many approaches are available for protecting digital data; these include encryption, authentication and time stamping. One approach to protect images is to add an invisible structure to the image data itself that can be used to authenticate it. These structures are known as digital watermarks. If the image is copied and distributed, the watermark is distributed along with the image. Figure1 shows the general watermarking embedding procedure. The message (**M**) is embedded into a cover image (**C**) with use of a key (**K**) producing a watermarked image (**WM**). Ideally the watermarked image is undistinguished from the cover image, appearing as no other information has been encoded or in other ward the cover image has no degradation.

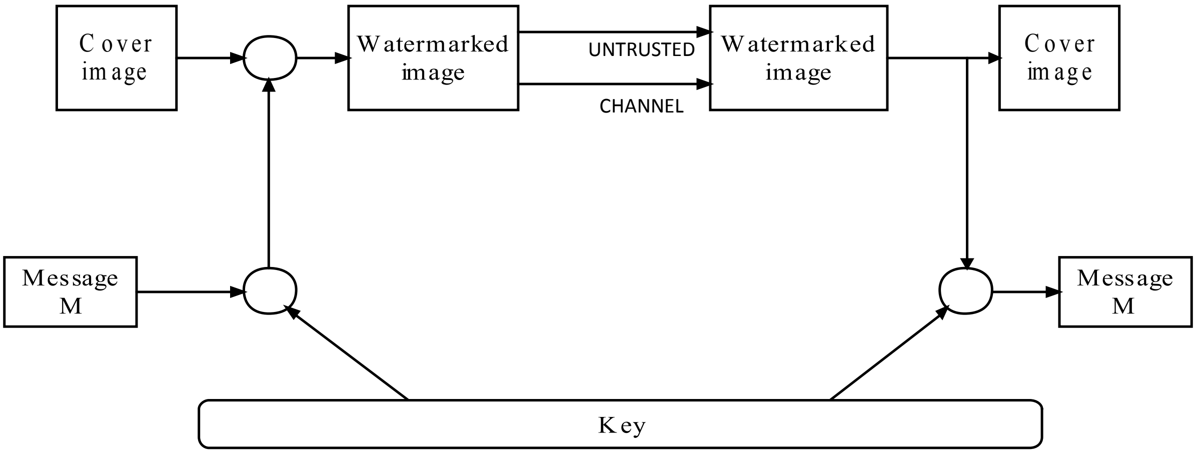


Figure 1: general watermarking embedding procedure

Digital Watermarking of image data could be visible or could be perceptually invisible. Visible watermarks are designed to be easily perceived by the viewer, and clearly identify the owner(background transparent signature); the watermark must not detract from the image content itself ,so the visible watermark acts like a deterrent but may not be acceptable to users in some contexts, however. Due to that most research currently focuses on invisible watermarks, which are imperceptible under normal viewing conditions. In order to be effective, an invisible digital watermark technique must satisfy the following two properties:

(1) The embedded watermark should be statistically and Perceptually invisible.

(2) The watermark must be difficult to remove.

It should also be robust to common signal processing and geometric distortion, such as compression, adding noise and scaling. [1]

Previous work on embedding invisible watermarks (signatures) can be broadly grouped into spatial domain and transform domain methods. Typically, the data used to represent the digital watermarks are a very small fraction of the host image data. Such signatures include, for example, pseudo-random numbers, trademark symbols and binary images. Spatial domain methods usually modify the least-significant bits of the host image [2], and are, in general, not robust to operations such as low-pass filtering. Much work has also been done in modifying the data in the transform domain. These include DCT domain techniques and wavelet transforms [3,4].

Cox et al. [5] propose a DCT based spread spectrum watermarking technique. A pseudo-random sequence is embedded into the significant DCT coefficients and is retrieved by calculating the similarity function of the original watermark and extracted watermark. Su et al. [6] proposes a wavelet-based watermark algorithm.

Based on the work of Cox [5] in the DCT domain, Kim [7] utilizes DWT coefficients of all subbands including the approximation image to equally embed a random Gaussian distributed watermark sequence in the whole image. Perceptually significant coefficients are selected by level-adaptive thresholding to achieve high robustness. However, the location of the watermark information is not protected and open for malicious attacks.

Following the design of his multi-threshold wavelet coding scheme, Wang [8] proposes a watermarking algorithm that refines Kim's thresholding scheme and selects significant coefficients on a per subband basis.

Kundur [9] is embedding a binary watermark by modifying the amplitude relationship of three transform-domain coefficients from distinct detail subbands of the same resolution level of the host image. The security of this scheme lies entirely in the pseudo-random selection of coefficient locations. To strengthen the blind watermark extraction process, Kundur resorts to repetition and a reference mark.

2. Data Hiding And Selection Of Hidiing Area:

As mentioned earlier, for copyright protection and authentication purposes it is important that the watermarked images are robust to typical image processing operations.

Compression techniques, such as JPEG, and noise attacks typically affect the high frequency components. This is also true with most perceptual coding techniques. The degradation in low frequency components of an image is more noticeable to the (HVS), inserting signature in low frequency components creates problems if one is interested in invisible watermarks. This is particularly true in data hiding applications where the data to be hidden could be a significant percentage of the original data.

For these reasons, a digital signature should be placed in perceptually salient regions in the data. For techniques based on frequency domain modifications, this implies embedding the signature in middle frequency components. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [10]. The use of a wavelet transform to hide signature information in different frequency bands is used in this paper because DWT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image.

2.1 Wavelet Domain Watermarking:

Wavelet transform are a relatively new concept. There is a push toward the use of wavelets in signal processing and analysis in place of (or in addition to) the discrete cosine transform (DCT), which is used in the jpeg standard for image compression. The techniques that are currently being used in working with images can be generalized for use with wavelet transforms. There are numerous applications for wavelets, and the uses of wavelets in signal processing seem to be endless. This paper will discuss wavelet-based techniques for watermarking.

The 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 figure (2).

$$W(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{+\infty} f(x)\psi^{*}(\frac{x-b}{a})dx \qquad (1)$$

Where $W(a,b)$ is the wavelet coefficient of the function $f(x)$, $\psi(x)$ is the analyzing wavelet, a *and* b are the scale parameter and the position parameter respectively.

The goal of digital watermarking is to hide a watermark (signature) within the image, so that the visual quality of the image is not perceptually visible to the human eyes, but also so that it is robust enough to withstand the various kinds of transformations.

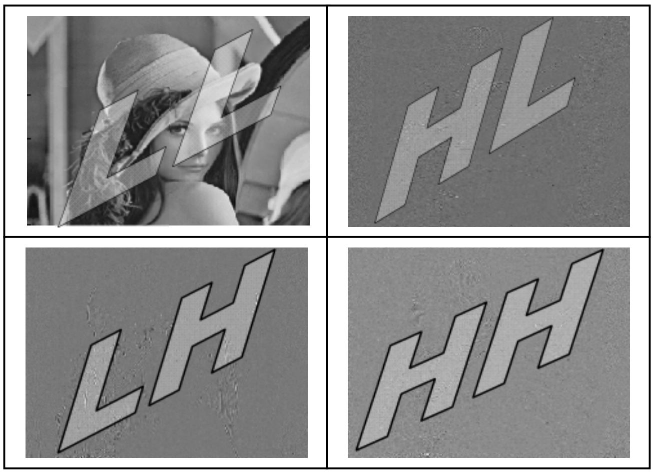


Figure 2: 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that believing to more accurately model aspects of the HVS as compared to the FFT or DCT. This allow to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow increasing the robustness of the watermark, at little to no additional impact on image quality [10].

The proposed scheme distributes the signature information in the discrete wavelet transform (DWT) domain of the host image. Spatial distribution of the DWT coefficients helps to recover the signature even when the images are compressed using JPEG lossy compression. In some of the recent work on using wavelets for digital watermarking, the signatures were encoded in all DWT bands. Such an embedding is sensitive to operations that change the high frequency content without degrading the image quality significantly. Examples of such operations include low pass filtering for image enhancement and JPEG lossy compression. In contract, the proposed scheme here focuses on hiding the signature mostly in the mid detail frequency bands, and stable reconstruction can be obtained even when the images are transformed, quantized (as in JPEG).

2.2 Cdma Spread-Spectrum Technique In Wavelet Domain Watermarking:

Early experimentation with CDMA demonstrated exceptional robustness with relation to noise and high-level JPEG compression, with flawless recovery of the embedded watermark from the pristine image. CDMA in the spatial domain however suffers from several problems that limit its usefulness. The main drawback of CDMA is that its message capacity is more limited then similar correlation-based techniques. One reason for this is that watermark recovery drops off quickly at higher message sizes. Good results were obtainable using the small watermark; however results with the normal-sized watermark were disappointing that being said, CDMA performed wonderfully using the smaller message.

The main limitations of CDMA in the spatial domain however remain it's limited capacity and high processing requirements. The embedding of large watermarks using CDMA requires the embedding gain k to be lowered to preserve the visual quality of the image. As more PN sequences are added to the cover image however, larger gains are required to preserve correlation between like sequences. This underlying conflict is the reason that CDMA in the spatial domain will remain more limited in capacity than other techniques.[10]

In this paper a proposed algorithm is defined based on the combination between the benefits provides by using wavelet domain and a profits of CDMA spread-spectrum technique. CDMA spread-spectrum techniques can be employ to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping.

A pseudo-random sequence (key) that related to hidden message is embedded into the significant DWT coefficients of a cover image to produce a watermarked image, and then the message is retrieved by calculating the similarity function between the key and DWT coefficients of the watermarked image.

3. Proposed watermarking scheme:

The block diagrams of watermark embedding and detection are shown in Fig.3.

3.1 Watermark embedding:

The embedding process in this research combines between DWT and CDMA technique. The wavelet domain offers perhaps the most promising environment for robust watermarking due to it's computationally efficient modeling of the HVS. CDMA technique (spread-spectrum pseudo-noise) in wavelet domain supports the watermarking robustness as mentioned before. The embedding process in simply is to embed a pseudo-random noise (PN) patterns into the mid detail frequency bands of the DWT coefficients of a cover image. These PN patterns are related with watermark (or the bit of the message).

For each value of the watermark, a PN sequence is generated using an independent seed. These seeds could either be stored, or themselves generated through PN methods. The summation of all of these PN sequences represents the watermark, which is then scaled and added to the cover image [9]. The equation shown below clarifies the embedding of a CDMA sequence (PN) in the detail bands:

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases} \qquad (2)$$

Where $I_{W_{u,v}}$ is the watermarked image, W_i denotes the coefficient of the transformed image, X_i the bit of the watermark to be embedded, and α scaling factor, u is the row position and v is the column position.

3.2 Watermark detection:

Watermark detection is accomplished without the original image. To detect the watermark, same pseudo-random sequence ,used in CDMA generation, is used in the detector to determine its correlation with the two transformed detail bands named LH and HL. If the correlation exceeds some threshold T, the watermark is detected.

This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which are then added to the detail coefficients as in the above equation. During detection, if the correlation exceeds T for a particular sequence a "1" is recovered; otherwise a zero.

The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered.

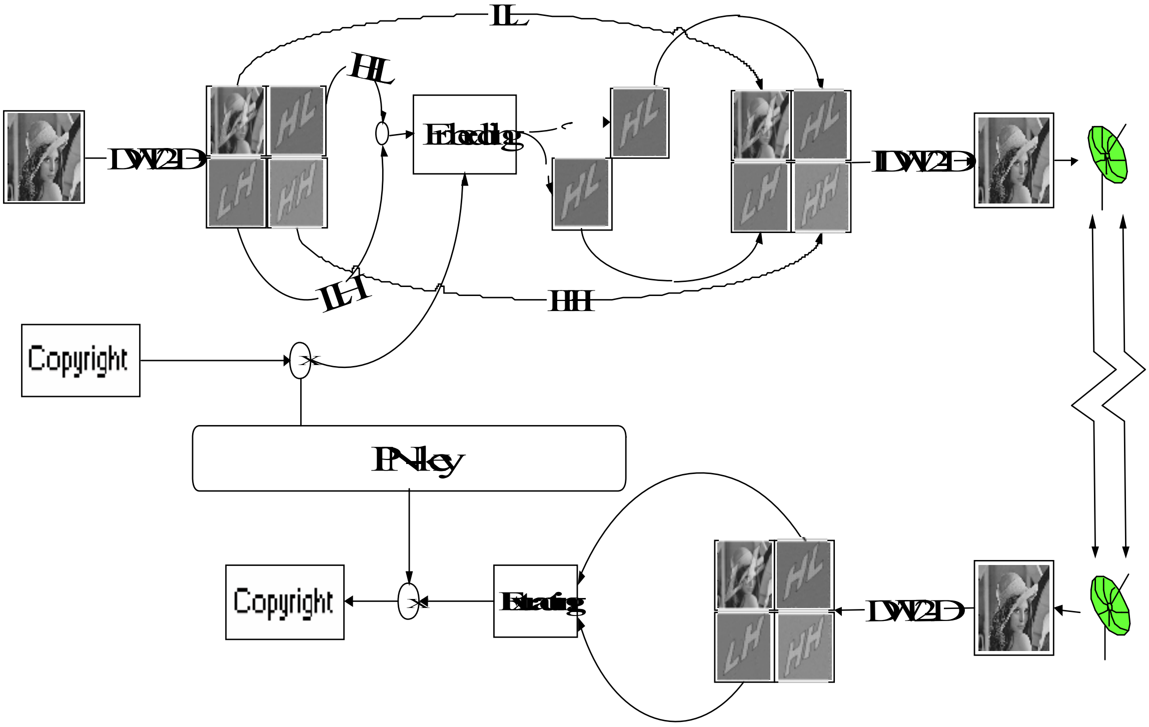


Figure 3: block diagrams of watermark embedding and detection

4. Experimental results:

Robustness evaluations of the proposed watermarked algorithm were limited to testing against unintentional and intentional attacks (watermarking attacks), JPEG compression and the addition of random noise attacks, with constant gain factor, is well beyond the scope of this paper. All the experiments described below use the discrete Haar wavelet basis, and adopting this method to other wavelet basis is reasonably straightforward. The PSNR of each watermarked image will be given below each figure; however these figures are only to be taken lightly. PSNR does not take aspects of the HVS into effect so images with higher PSNR's may not necessarily look better then those with a low PSNR. This will prove particularly true in the case of DWT domain techniques.
The equations shown below clarify the calculation of the PSNR in all watermarked images:

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j}^{N}\left\| S_{i,j} - \hat{S}_{i,j} \right\|^2 \qquad (3)$$

$$PSNR = \frac{\max_{i,j}(S^2)}{MSE} \qquad (4)$$

Algorithm was implemented in the most straightforward way, not the most computationally optimal. Furthermore, MATLAB may handle certain programming constructs differently from other languages, thus the best performing algorithm may vary for each language and implementation.
As a cover image, standard (Lena) image with 512x512 Pixels is used figure (4).

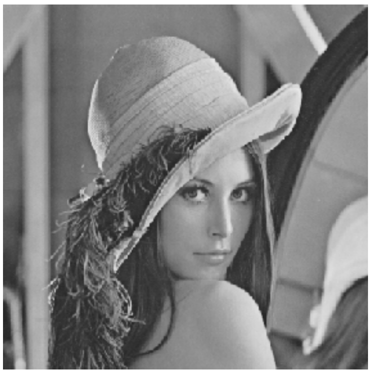


Figure 4: Lena Reference Image (512 x 512 Pixels)
Figure (5) show the 1000-bit (20x50 Pixels) normal message that used as embedded text message inserted into the cover with moderate gain.

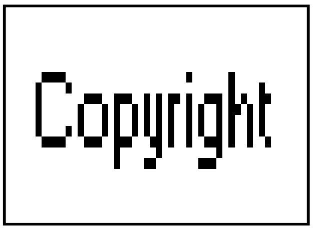


Figure 5: 1000-bit normal message

Through experimentation, the gain factor k=2 was arrived at as a good balance between visual quality and watermark robustness.

4.1 Watermark Performance on JPEG Compression:

JPEG is widely used as a lossy compression format for images because of its high rate compression performance. This kind of compression suffers of information detail losses. The effects of these losses, particularly, on compressed watermarked image can be very severe. Therefore watermark have to be robust in this type of distortion.

(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j)

Figure 6: Results of Compressed Watermarked Lena

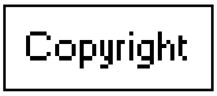
a)Origin,

b)Watermarked,

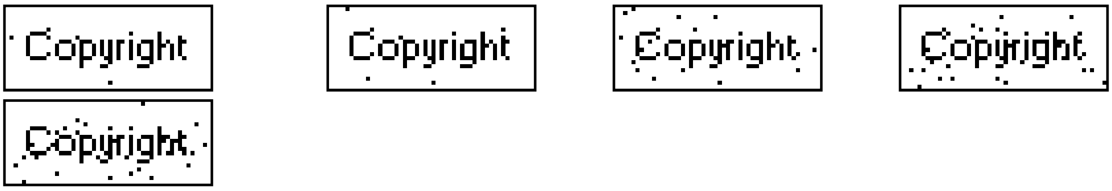
c)Compression 15% of watermarked image,

d) Compression 25% of watermarked image,

e) Compression 40% of watermarked image,



(a) (b) (c) (d)
(e)



(f) (g) (h) (i)
(j)

Figure 7: Recovered Watermark

a) Message, **b)** Recovered, **c)** Recovered of 15% compression, **d)** Recovered of 25% compression, **e)** Recovered of 40% compression, **f)** Recovered of 50% compression, **g)** Recovered of 60% compression, **h)** Recovered of 70% compression, **i)** Recovered of 80% compression, **j)** Recovered of 90% compression.

Table 1: Comparison between Several Ratios of Compression

Compression ratio		0%	15%	25%	40%	50%	60	70	80	90
Watermarked image	MSE	102.2244	110.8153	113.8343	111.4374	103.8290	93.6512	83.8872	75.1039	68.5833
	PSNR	55.5168	54.8159	54.5824	54.7673	55.3815	56.2776	57.2340	58.1946	58.9835
Text recovery	MSE	65.0250	65.0250	65.0250	195.0750	260.1000				
	PSNR	60	60	60	50.4576	47.9588				

Text recovery	MSE	455.1750	1.1705e+3	1.9508e+3	1.8857e+3
	PSNR	43.0980	34.8945	30.4576	30.752

Its can be clearly defined from table 1 and figures 6 and 7 that compressing Lena watermarked image up to 25% of its nominal size using JEPG gave no change on PSNR of the recovered text. While compression the watermarked image by 40% decrease PSNR by 10db, with accepted readable results to recover embedded text. Another degradation of 10db can be observed in 70% JPEG recovered text result; with respect to 60% JEPG recovered text, but the text still recognizable. Compression above 70% gave unrecognized recovered text.

From above results the observer can be obviously mention that the watermarked image didn't affected to JPEG and text recovery.

4.2 Watermark Performance in AWGN:

Noise is one of common distortion in image processing and transmission. In the experiment, here several number of standard deviation of Gaussian noise added into the watermarked object as shown in Figs. 8. The watermark can still be retrieved successfully, and the responses of the watermark detector good.

The test has been done to examine the rigidity of proposed method against Additive White Gaussian Noise AWGN.

As seen in table 2 and figures 8and 9, the proposed method seems didn't affected to noise up to standard deviation $\sigma = 15$. For $\sigma = 25$ the recovered text message seems difficult to recognize.

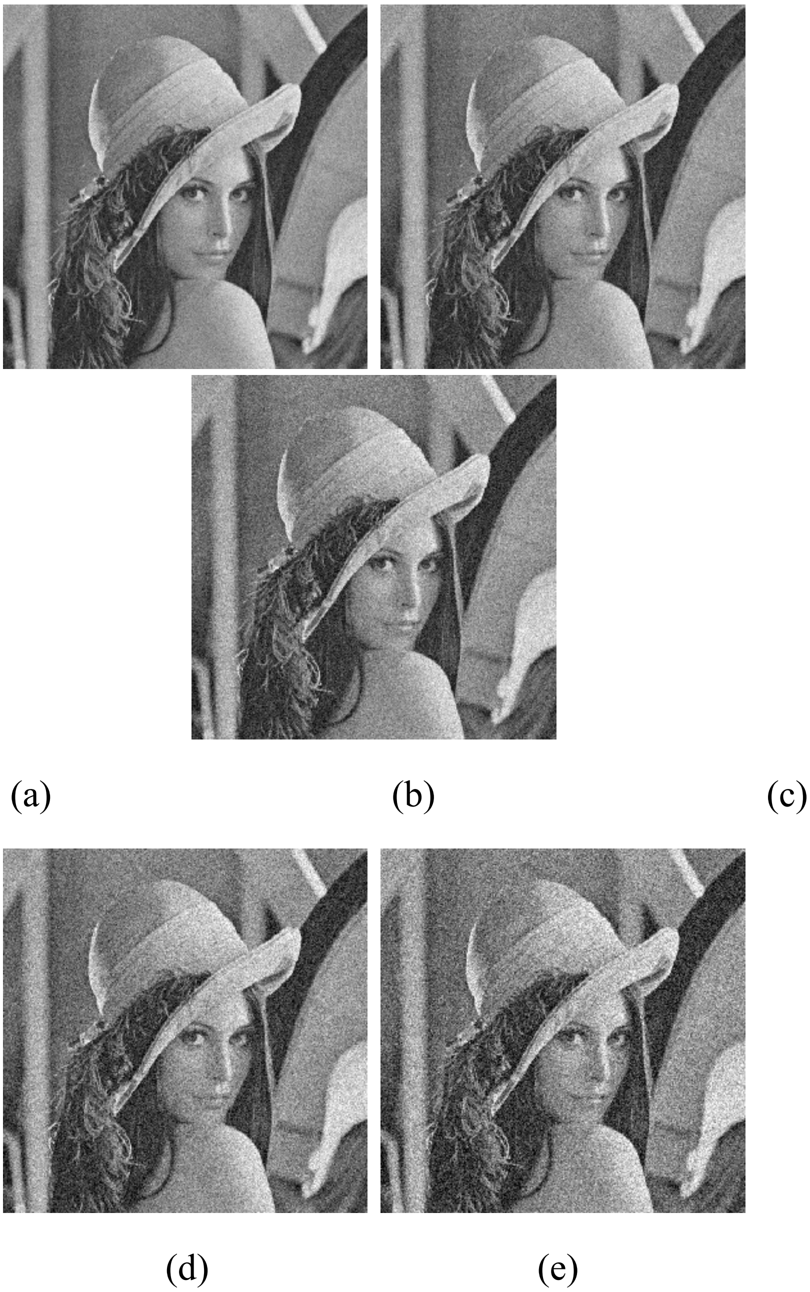


Figure 8: Watermarked results of noisy Lena

a) Noisy Watermarked Lena with $\sigma = 5$ AWGN, **b)** Noisy Watermarked Lena with $\sigma = 10$ AWGN, **c)** Noisy Watermarked Lena with $\sigma = 15$ AWGN, **d)** Noisy Watermarked Lena with $\sigma = 20$ AWGN, **e)** Noisy Watermarked Lena with $\sigma = 25$ AWGN.

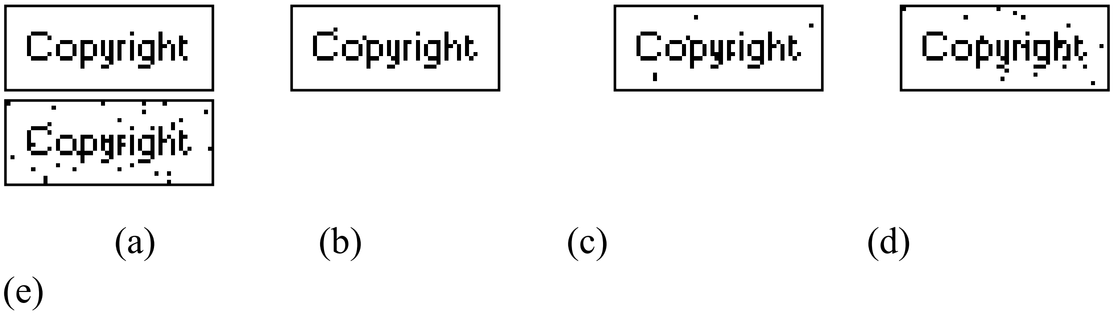


Figure 9: Recovered Watermark

a) Recovered of $\sigma = 5$, **b)** Recovered of $\sigma = 10$, **c)** Recovered of $\sigma = 15$, **d)** Recovered of $\sigma = 20$, **e)** Recovered of $\sigma = 25$.

Table 2: Comparison between Several standard deviation of AWGN

Standard deviation		Without noise	$\sigma = 5$	$\sigma = 10$	$\sigma = 15$	$\sigma = 20$	$\sigma = 25$
Watermarked image	MSE	102.2244	127.5167	201.8351	327.7180	500.6558	718.1180
	PSNR	55.5168	53.5965	49.6079	45.3979	41.7171	38.5840
Text recovery	MSE	65.0250	65.0250	195.0750	520.2000	1.2355e+003	1.9508e+003
	PSNR	60	60	50.4576	41.9382	34.4249	30.4576

5. Conclusion:

This study has introduced an approach for the watermarking of digital images. The wavelet domain as well proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. This is all the more impressive when one considers that the wavelet technique described here is one of the most primitive currently known. More sophisticated wavelet-domain techniques will almost certainly improve on both of these, and hopefully lower it's computational requirements.

The wavelet domain may be one of the most promising domains for digital watermarking yet found.

It can be concluded, Based on the results of figures 6-9, that CDMA in the spatial domain easily meets the requirements for “moderate” robustness, provided that the encoding messages are relatively small. The results are particularly impressive when you consider that the watermarked image used for figure was entirely unrecognizable after the addition of $\sigma = 25$ gaussian noise.

The algorithm seemed to have no problem retrieving the normal watermark from the watermarked image with only minimal degradation of the cover image during embedding. Even with a minimal gain, the algorithm was still able to provide moderate robustness to gaussian noise and JPEG compression as shown in figure 7 & 9. The recovered watermark was even recognizable under heavy degradation of the cover such as $\sigma = 15$ gaussian noise or JPEG compression upto 70% of its nominal.

Refrences:

1. Xiangwei Kong, Yu Liu, Huajian Liu, Deli Yang “Object watermarks for digital images and video”Image and Vision Computing ,Vol.22 ,pp.583–595, 2004.

2. R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, “A Digital Watermark,” *Proceeding of IEEE International Conference of Image Processing,* Vol. 2, pp. 86-90, Austin, Nov., 1994.

3. M. M. Yeung, and F. C. Mintzer, “Digital Watermarking for High-quality Imaging,” *IEEE first workshop on the Multimedia Signal Processing,* pp. 357-362, 1997.

4. B. Tao and B. Dickison, “Adaptive Watermarking in the DCT Domain,” *1997 IEEE International Conference Acoustics, Speech, and Signal Processing,* Vol. 4, pp. 2985-2988, Munich, Germany, April, 1997.

5. Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon, “Secure spread spectrum watermarking for multimedia,” in *Proc. ICIP*, Santa Barbara,CA, USA, vol. 6, pp. 1673 – 1687, Oct. 1997.

6. P. Su, C.J. Kuo, H.M. Wang, “ Blind digital watermarking for cartoon and map images”, IS and T/SPIE Conference on Security and

Watermarking of Multimedia Contents, San Jose, California, pp. 296–305 ,January, 1999.

7. Jong Ryul Kim and Young Shik Moon, “A robust wavelet-based digital watermark using level-adaptive thresholding,” in *Proc. ICIP*, Kobe, Japan, pp.202-212, Oct. 1999.

8. Houng-Jyh Wang and C.-C. Jay Kuo, “Watermark design for embedded wavelet image codec,” in *Proc. SPIE*, San Diego, CA, USA,Vol. 3460, pp.288 – 398, July 1998.

9. Deepa Kundur, “Improved digital watermarking through diversity and attack characterization,” in *Proc. ACM Workshop on Multimedia Security*, Orlando, FL, USA, pp. 53 – 58, Oct. 1999.

10. G. Langelaar, I. Setyawan, R.L. Lagendijk, “Watermarking Digital Image and Video Data”, in IEEE Signal Processing Magazine, Vol 17, pp. 20-43, September 2000

The work was carried out at the college of Engg. University of Mosul