Analysis of Image Watermarking Algorithms

Naman Goel
Department of Computer Engineering
Indian Institute of Technology, (BHU),
Varanasi, India

Nitish Chandra
Department of Computer Engineering
Indian Institute of Technology, (BHU),
Varanasi, India

ABSTRACT

A digital image watermark is a signal permanently embedded into a digital image that can be detected or extracted later by means of some operations for authentication purposes. This paper discusses the results of evaluating three conventional image watermarking algorithms for performance and robustness. The findings are based on experiments on a standard LENA image and thus a comparative analysis between the algorithms becomes apparent and very clear. Three algorithms namely LSB (Least Significant Bit), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) were implemented in MATLAB and various results were collected with respect to performance and robustness. LSB embedded watermarks were easily removed using techniques that do not visually degrade the image to the point of being noticeable. Cosine transform algorithm was good in both performance and robustness. The wavelet domain proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation but the original image was significantly affected by the embedding. The numeric data included in the paper make this comparison more formal.

General Terms

Image processing, Image watermarking.

Keywords

Image watermarking, DCT, DWT, LSB, MSE, SSIM, PSNR.

1. INTRODUCTION

The fast development of the Internet in recent years has made it possible to easily produce, create copy, transmit, and distribute digital data. Consequently, this has led to a strong demand for reliable and secure copyright protection techniques for digital data. Digital watermarking addresses the growing concerns of theft and tampering through the use of advanced signal processing strategies to embed copyright and authentication information within media content.

A digital image watermark is a signal permanently embedded into a digital image that can be detected or extracted later by means of some operations for authentication purposes. The hidden watermark should be inseparable from the host image, robust enough to resist any manipulations while preserving the image quality. Thus through watermarking, intellectual properties remains accessible while being permanently marked.

For any watermarking technique to be valid, it must satisfy at least two important requirements namely perceptual invisibility and robustness against various image processing attacks. Recently, many watermarking algorithms have been proposed in the literature. Some of them operate either in the frequency domain using for example the DCT and DWT or in the spatial domain

In this paper, we study the most prominent watermarking algorithm DCT, DWT, LSB and analyze their working when the images are subsequently attacked (cropping, up-scaling and downscaling compression and noise attacks-salt and pepper). The results show the simple but subtle aspects of these algorithms.

2. ALGORITHMS

We will first discuss the basics involved in the algorithms to be studied.

2.1 Discrete Cosine Transform (DCT)

A **discrete cosine transform** (**DCT**) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions [1]. In particular, a DCT is a Fourier-related transform but using only real numbers. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT".

2.2 Discrete Wavelet Transform (DWT)

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. Since the bandwidth of the resulting coefficient sets is smaller than that of the original image, the coefficient sets can be down sampled without loss of information. Reconstruction of the original signal is accomplished by up sampling, filtering and summing the individual sub bands. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution coefficient sets, a lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. Due to its excellent patio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. Embedding in the low frequency coefficient sets, however, could increase robustness significantly. On the other hand, the high frequency coefficient sets HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such coefficient sets [2][3].

2.3 Scalar Watermarking (LSB)

In the basic Least Significant Bit (LSB) watermarking method each pixel is modified to carry 1 bit of information by changing the LSB to the required value. Since changing the LSB alters its value by 1 unit at most, the visual impact is typically minimal. Moreover if the information being embedded is independent of the pixel LSB value on average only 50% of the pixel will be changed [4].

3. EVALUATION OF ALGORITHMS

We implemented all the three algorithms in MATLAB with a straight forward approach. Several calculations were made to evaluate the watermarking algorithms. The watermarked images were examined and suitable tests were performed as explained below.

3.1 Imperceptibility

The imperceptibility of the watermark is tested through comparing the watermarked image with the original one. Several tests are generally used in this regard.

3.1.1 Mean Squared Error

Mean Squared Error is one of the earliest tests that were performed to test if two pictures are similar. A function could be simple written as per the following equation:

$$M.S.E = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - X_i^*\right)^2$$

3.1.2 Peak Signal to Noise Ratio

PSNR is a better test since it takes the signal strength into consideration (not only the error). Equation is as follows:

$$PSNR = 10.\log_{10}\left(\frac{MAX_i^2}{MSE}\right)$$

3.2 Results of Imperceptibility Tests

When the above tests were performed and enough calculations were made through MATLAB to find PSNR and MSE, we obtained following results. The results have been formatted in a table to ease comprehension, make comparisons and hence draw conclusions.

Table 1. Results of Imperceptibility Tests

Tests	Algorithms		
	LSB	DCT	DWT
MSE	0.23904	12.1421	85.4954
PSNR	116.791	77.5125	57.9947

The resultant images (right) obtained by application of the three algorithms on a standard Lena image along with the watermark image used (left) are shown below.

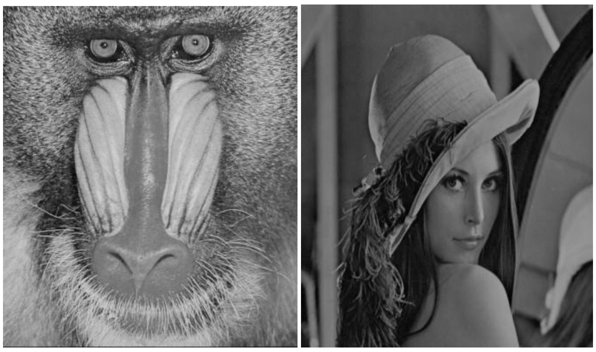

Fig 1: LSB Result

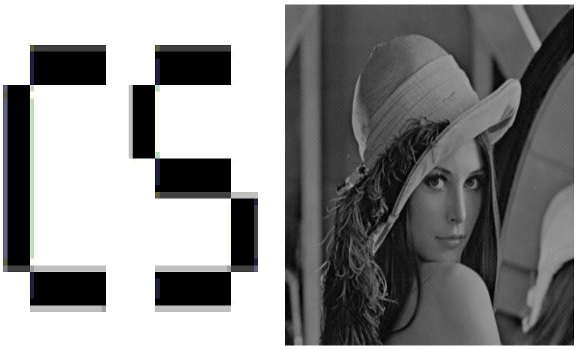

Fig 2: DCT Result

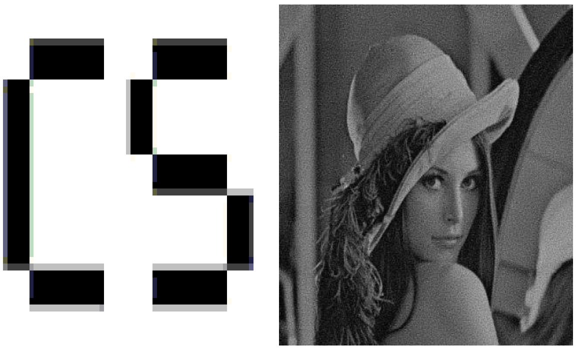

Fig 3: DWT Result

3.3 Robustness

The robustness of a watermark method can be evaluated by performing attacks on the watermarked image and evaluating the similarity of the extracted message to the original one. We performed some common image manipulation attacks like cropping, compression, adding noise, scaling etc. on the watermarked image and then tried to recover the embedded watermark. It was interesting to know that some attacks were enough to destroy the watermark. However, DCT and DWT were found to show a good resistance to JPEG (lossy) compression attack.

3.4 Results of Robustness Test

Below we summarize the results obtained on performing the above attacks:

3.4.1 Cropping Attack

We cropped the watermarked image in several positions. Only LSB image showed resistance to cropping attack whereas the trivial DCT and DWT did not.

3.4.2 Compression Attack

The watermarked image was compressed as per JPEG format (mode= 'lossy' and quality = 75 in MATLAB). Both DCT and DWT showed good resistance to compression whereas LSB didn't (as expected) because in lossy compression, it is the least significant bit information that is lost first.

3.4.3 Noise Attack

Gaussian, Poisson, Salt & Pepper and Speckle are among the noises that could be used here. Salt & Pepper noise was added to the watermarked image in our experiment. And then the watermark was extracted. All the three algorithms passed this test.

3.4.4 Scaling

We scaled up and scaled down the watermarked image. None of the algorithms passed this test. However, with a little modification in the algorithms, we can expect them to show some resistance to cropping (at least LSB).

Table 2. Results of Robustness Tests

Attacks	Algorithms		
	LSB	DCT	DWT
Cropping	Pass	Fail	Fail
Compression	Fail	Pass	Pass
Noise	Pass	Pass	Pass
Scale Up	Fail	Fail	Fail
Scale Down	Fail	Fail	Fail

4. SOME OTHER RESULTS

We noted some other results for better understanding of performance of the algorithms when these attacks are made.

4.1 After Salt and Pepper Noise Attack

As noted earlier, all the three algorithms passed this attack. However, for a better comparison, we compared the extracted watermark with the original watermark image.

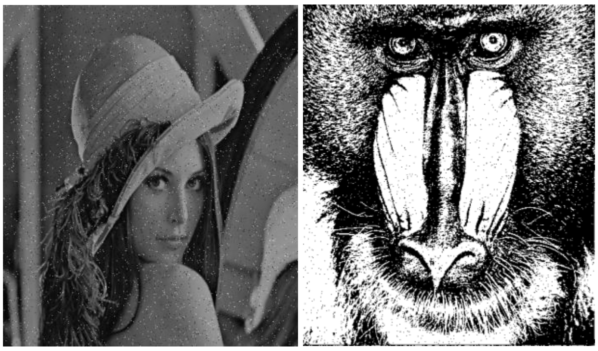

Fig 4: LSB Extract

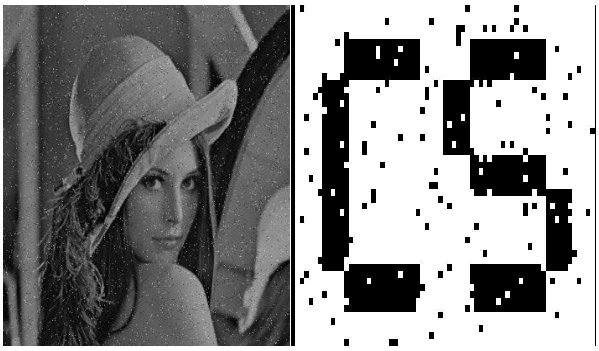

Fig 5: DCT Extract

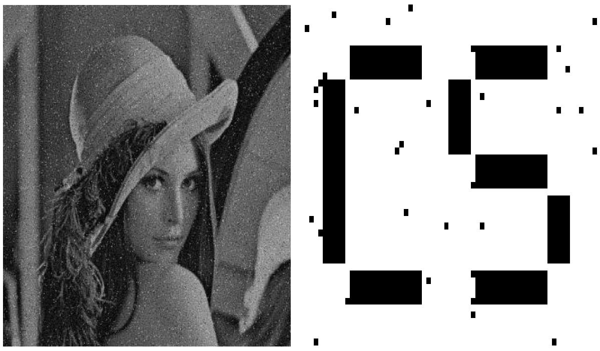

Fig 6: DWT Extract

4.2 After JPEG Compression Attack

Both DCT and DWT had passed this test but here is a closer look to compare. We are skipping the compressed images to be displayed here in this paper because they were not visually different from original watermarked image. Only the metrics' values have been included in the table given below.

Table 3. Recovered Watermark after Compression Attack

Tests	Algorithms		
	LSB	DCT	DWT
MSE	128.508	8.79433	0.913433
PSNR	60.2017	89.0842	111.731

Table 4. Recovered Watermark after Noise Attack

Tests	Algorithms		
	LSB	DCT	DWT
MSE	121.731	15.3069	2.13134
PSNR	60.7435	83.5423	103.258

Table 5. Time (For corresponding implementations* in MATLAB)

Time(sec)	Algorithms		
	LSB	DCT	DWT
MSE	0.4680	2.0280	22.9945
PSNR	0.4056	1.0764	33.9146

* Run on Intel Core i3 – 3 GB RAM, Windows 7

5. CONCLUSION

As can be inferred from Table.1 LSB suffers from minimum mean square error whereas DWT has the maximum mean square error. In layman terms it means that LSB watermarking technique introduces minimum distortion in the image to be watermarked. DWT on the other hand introduces the maximum distortion in the original image. DCT lies between the two extremes. This can be easily accounted for by the fact that in LSB only 1 bit is modified. PSNR ratio which is another measure for imperceptibility of the watermarked images also shows that LSB algorithm scores over all other algorithms as far as preserving the integrity and imperceptibility of images are concerned.

Robustness is another parameter that is very important to be examined for any watermarked algorithm. In fact it is the heart of watermarking process. Preserving the integrity and securing the watermark during various image manipulation attacks is the essence of the robustness process. Analyzing from the results, we can infer that DCT and DWT show a good resistance to JPEG compression attack. Cropping attack which probably is the most common attack is another area where LSB is dominant and scores over DCT and DWT. LSB algorithm stores the watermark information in Least Significant Bit which is the target of compression algorithms, so it obviously can’t retain the watermark after compression attack. All three algorithms pass noise test which suggests the fact that all are equally resistant to addition of unwanted signals in the image. Our Algorithms show little resistance to scaling attacks but these simple algorithms can be modified with little effort to resist such attacks keeping the underlying approach same.

6. ACKNOWLEDGMENTS

We are greatly indebted to Prof Arun Kumar Agrawal, Senior Professor and Former Head at Department of Computer Engineering, Indian Institute of Technology, (BHU), Varanasi for his able and dedicated guidance and encouragement throughout the project .We would also like to thank Head, Department of Computer Engineering, Indian Institute of Technology, (BHU), Varanasi for allowing us to use the resources of the department in our study and research.

7. REFERENCES

[1] Communications in Computer and Information Science – Azizah Adb Manaf, Akram Zeki, Majdak Zamani, Suriayati Chuprat, Eyas El-Qawasmeh(Eds.).

[2] Combined DWT-DCT Digital Image Watermarking - Ali Al-Haj.

[3] Communications in Computer and Information Science – Vinu V Das, R. Vijaykumar et al.(Eds.) (page 37)

[4] Digital Watermarking and Steganography - Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker. (page 175)

[5] A Dual Digital Image Watermarking Technique - Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, Senior Member IEEE.

[6] Robust Digital Image Watermarking based on Joint DWT and DCT- Saeed K. Amirgholipour, Ahmad R. Naghsh-Nilchi, Computer Engineering Dept., Isfahan University, IRAN .

[7] Digital Watermarking Using Matlab - Pooya Monshizadeh Niani- University of Tehran, Iran.

[8] DCT: Theory and Application – Syed Ali Khayam, Department of Electrical and Computer Engineering, Michigan State University.

[9] Attacks on Copyright Marking Systems - Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn