

Performance Evaluation of New-Fangled Digital Watermarking Techniques

Ajay Goel^[1], O.P.Sahu^[2],
Sheifali Gupta^[3], Rupesh Gupta^[4]
goelajay1@gmail.com, ops_nitk@yahoo.co.in,
sheifali@yahoo.com, rup_esh100@yahoo.co.in

GJCST Computing Classification
1.4.m, B.8.2 & D.4.6

Abstract- The use of digital formatted data offers several advantages over analog media such as high quality, easy editing, or high fidelity copying. The development of multimedia services and environments and thus the ease by which digital media can be duplicated and distributed, requires new concepts to support the protection of the media during the production and the distribution. In this work, I intend to disseminate the general concept of digital watermarking. I will illustrate the properties of a digital watermark and a description of methods used to insert watermarks in media and then move on to a discussion of what requirements a watermarking system must meet, as well as new-fangled methods are discussed for evaluating the strengths of various algorithms. This paper will focus almost exclusively on the watermarking of digital images; however most of these same ideas could easily be applied to the watermarking of digital video and audio [4] [5].

Keywords- Watermarking Techniques, Least Significant Bit Modification, Correlation-Based Techniques, Stenography.

I INTRODUCTION

Unlike analog media that are becoming obsolete by now, digital media can be stored, duplicated, and distributed easily and with no loss of fidelity. It is clear that documents in digital form present a lot of advantages, but they also create problems, for parties who wish to prevent unauthorized reproduction and distribution of valuable digital medium (copyrighted, commercial, sensitive, secret documents...). Encryptions technologies can be used to prevent unauthorized access to the digital document - protect the content during the transmission of the file, but once it is received and decrypted, the document is no longer protected and is in clear. As a complement to encryption and/or copy protection, digital watermarking has been proposed as "last line of defense" against document misuse. Digital watermarking describes the process of embedding additional information into a digital media, without compromising the media's value. Hiding this piece of information to anybody besides a special designed detector is achieved by using a special watermarking technique called steganography. The watermark is then hidden in such a way that it may be imperceptible to a human observer, but easily detected by a computer. The development of watermarking methods involves several design tradeoffs due to the properties that a digital watermark should fulfill, and depending on the application field [1]. The framework,

requirements, properties, evaluation and the design constraints will be discussed more throughout this paper.

A. Digital Watermarking

The Framework That watermark can be detected or extracted later to make an assertion about the media. For example, a very simple yet widely used digital watermarking technique[2] would be for images to add a visible seal on top of an existing image as shown as in the following figure 1:-

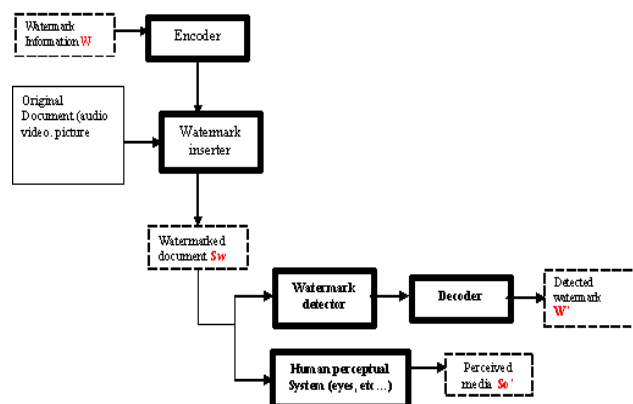


Figure-1: Generic Digital Watermarking Insertion & Recovery.

As illustrate in the above figure 1 the first step is to encode the watermark into a form that will be easily inserted with the media. The watermark inserter then combines the encoded representation of the watermark with the document. If the watermarking insertion process is design correctly, the result is media that appears identical to the original when perceived by a human, but which yields the encoded watermark information when processes by a watermark detector.

B. Choice Of a Watermark-Object

The most straight-forward approach would be to embed text strings into an image, allowing an image to directly carry information such as author, title, date...and so forth. The drawback however to this approach is that ASCII text in a way can be considered a form of LZW compression, which each letter being represented with a certain pattern of bits.

By compressing the watermark-object before insertion, robustness suffers [11].

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be quite easy for even a simple task such as JPEG compression to reduce a copyright string to a random collection of characters. Rather than characters, why not embed the information in an already highly redundant form, such as a raster image? Not only do images lend themselves to image watermarking applications, but the properties of the HVS can easily be exploited in recognition of a degraded watermark [3] [7].

Watermark



Figure 2 - Ideal Watermark-Object vs. Object with 25% Additive Gaussian Noise

II THE WATERMARKING TECHNIQUES

A. Least Significant Bit Modification

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [6]. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success.

LSB substitution [12] however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or loopy compression is likely to defeat the watermark. LSB embedding is one of algorithm that uses spatial domain. When LSB is applied in the spatial or temporal domains, these approaches modify the Least Significant Bits (LSB) of the host data. The invisibility of the watermark is achieved on the assumption that the LSB data are visually insignificant [13]. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party. LSB modification proves to be a simple and fairly powerful tool for steganography, however lacks the basic robustness that watermarking applications require.

B. Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image [9]. A pseudo-random noise (PN) pattern $W(x,y)$ is added to the cover image $I(x,y)$, according to the equation shown as below in equation 1.

$$I_w(x, y) = I(x, y) + k * W(x, y) \dots (1)$$

In equation 1, k denotes a gain factor, and I_w the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the

same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T , the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block [10].

This basic algorithm can be improved in a number of ways. First, the notion of a threshold being used for determining a logical “1” or “0” can be eliminated by using two separate pseudo-random noise patterns. One pattern is designated a logical “1” and the other a “0”. The above procedure is then performed once for each pattern, and the pattern with the higher resulting correlation is used. This increases the probability of a correct detection, even after the image has been subject to attack [9].

We can further improve the method by pre-filtering the image before applying the watermark. If we can reduce the correlation between the cover image and the PN sequence, we can increase the immunity of the watermark to additional noise. By applying the edge enhancement filter shown below in figure 3, the robustness of the watermark can be improved with no loss of capacity and very little reduction of image quality [9].

$$F_{edge} = \frac{1}{2} \begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

Figure 3 - FIR Edge Enhancement Pre-Filter [9]

Rather than determining the values of the watermark from “blocks” in the spatial domain, we can employ CDMA spread-spectrum techniques to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping. The watermark is first formatted as a long string rather than a 2D image. 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].

To detect the watermark, each seed is used to generate its PN sequence, which is then correlated with the entire image [13]. If the correlation is high, that bit in the watermark is set to “1”, otherwise a “0”. The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation [14]

III RESULTS

In general, algorithms were implemented in the most straightforward way, not the most computationally optimal. Three different watermarks were used, based on the theoretical and experimental information capacity of the watermarking algorithm, as shown in figures 4 & 5



Figure 4 - Small Watermark (12 x 9 pixels)



Figure 5 - Normal Watermark (50 x 20 pixels)

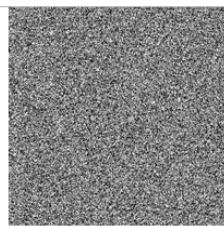
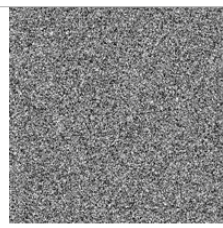
For our reference image, the ever-popular r (Lena) image is used, as shown below in figure 6.



Figure 6 - Lena Reference Image (512 x 512 Pixels)

Results from LSB substitution were as expected. The watermarked image shows little not noticeable degradation, while the large watermark was recovered perfectly.

Least Significant Bit Substitution	
	
Figure 7(a) - Recovered Watermark after addition of 1% Gaussian Noise	Figure 7(b) - Recovered Watermark after JPEG Compression with Quality 95
Least Significant Bit Substitution	
	
Figure 8(a) - Watermarked Image PSNR= 102 dB	Figure 8(b) - Recovered Watermark

Least Significant Bit Substitution	
	
Figure 9(a) - Recovered Watermark after addition of 1% Gaussian Noise	Figure 9(b) - Recovered Watermark after JPEG Compression with Quality 95

Although the watermark was recovered perfectly in the ideal case, the addition of any amount of noise, or compression of the image using JPEG fully destroys the embedded watermark, leaving nothing but noise. Even worse, the watermark can be removed with no perceivable change to the watermarked image. The message capacity of LSB embedding however is quite good, a 1:1 correlation with the size of the image.

The results of threshold-based correlation showed a vast improvement over LSB substitution in terms of robustness. Several parameters however must be discussed before we move on to results of this technique. A gain factor of $k = 5$ was chosen experimentally, however larger factors might be used for increased robustness at the expense of visual quality [8]. Another issue with threshold-based techniques is the choosing of a suitable threshold for detection. Use of a smaller watermark will allow larger blocks to be used, increasing the strength of correlation and thus system robustness. Using the normal sized watermark, the largest possible block size $\{8,16,32,\dots\}$ is determined by:

$$1000 \leq \frac{512 * 512}{16^2}, \quad \text{for a maximum block size of 16.}$$

Threshold-Based Correlation, $K = 5$ BlockSize=16

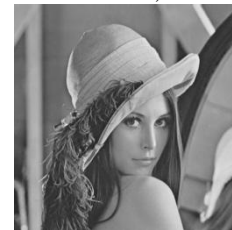


Figure 10a - Watermarked Image



Figure 10b - Recovered Watermark

The outcome PSNR =20 As shown, the addition of the watermark is context-sensitive, to make it harder to remove. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation.

IV CONCLUSION

A digital watermarking scheme is presented with the properties of digital watermark and requirement of a watermarking system. We also illustrate to insert different watermark into different image. We analysis and apply for the three different watermark to embedded directly into the LSB of channels of the pixel based on intensity of pixel, without using additional transformations and in correlation based technique with additive pseudo-random noise patterns. LSB substitution is not a very good candidate for digital watermarking due to its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable. Furthermore if one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even altered by a third party. It would appear that LSB will remain in the domain of steganography due to its tremendous information capacity and Correlation-Based Techniques improves on the robustness of the watermark appreciably with more mathematical operation and additional computational time.

V REFERENCES

- 1) S.Craver, N. Memon B.-L. Yeo, and M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications," *IEEE Trans. On Selected Areas of Communications*, vol. 16, no. 4, pp. 573–586, 1998.
- 2) Stephen Wolthusen "On the limitations of digital watermarks". Fraunhofer-Institute for Computer Graphics 64283 Darmstadt, Germany.
- 3) Gustavus, J. Simmons "The prisoner's problem and the subliminal channel". 51-67
- 4) R. Walker, "Audio watermarking". BBC Research & Development, White Paper WHP 057
- 5) Raymond B Wolfgang, Christine I. Podilchuk, Edward J. Delp, "Perceptual Watermarks for Digital Images and Video".
- 6) J.J.K.Ó Ruanaidh, W.J. Dowling G.M. Boland, "Watermarking Digital Images for Copyright Protection".
- 7) Jonathan K. Su, Frank Hartung, Bernd Girod "Digital Watermarking of Text Image and Video Document." Telecommunications Laboratory; Universität of Erlangen-Nuremberg, Germany
- 8) R. G.Van Schyndel, A. Z. Tirkel, N. Mee, C. F. Osborne "A Digital Watermark, Processing of the IEEE International Conference on Image Processing." November 1994 Austin, Texas, vol. 2, pp. 86-90.
- 9) Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in *IEEE Signal Processing Magazine*, Vol 17, pp 20-43, September 2000
- 10) Cox, J. Kilian, F. T. Leighton, and T. Shamoan, "A secure, robust watermark for multimedia," in *Information Hiding: First Int. Workshop Proc. (R. Anderson, ed.)*, vol. 1174 of *Lecture Notes in Computer Science*, pp. 185–206, Springer-Verlag, 1996.
- 11) Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," in *Proc. of the Int. Conf. on Digital Media and Electronic Publishing*, 1994.
- 12) W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3/4, pp. 313–336, 1996.
- 13) Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information hiding-a survey. Proceedings of the IEEE", July 1999 Special Issue "Identification and protection of multimedia information".
- 14) F.A.P. Petitcolas, "Watermarking Schemes Evaluation" ", in *IEEE Signal Processing Magazine*, Vol 17, pp 58-64, September 2000