

A Multiple Description Framework for Oblivious Watermarking*

R. Chandramouli^a, Benjamin M. Graubard^b, and Colin R. Richmond^b

^a Dept. of Electrical and Computer Engineering, Stevens Institute of Technology

^b Dept. of Electrical and Computer Engineering, Iowa State University

ABSTRACT

It is believed that digital watermarking can be a powerful tool that can be used to protect digital contents from illegal copying and distribution. Detecting the presence/absence of a watermark in a given digital content such as image/video data without using the unwatermarked original data is called oblivious watermark detection and the watermarking process is oblivious watermarking. Oblivious watermarking has many important practical applications such as secure video streaming or wireless image/video transmission where the intended receiver typically has access only to the received data.

We propose for the first time a multiple description framework for oblivious watermarking. Parallels between multiple description source coding and the watermarking are drawn. An information theoretic definition of the problem is given. A spread-spectrum watermarking algorithm for DCT based multiple descriptions is described. Performance of the proposed framework for various attack channels such as additive white Gaussian noise, JPEG compression, and random bit error channels shows that the proposed method performs reasonably well compared to non-oblivious schemes.

We believe the proposed framework can be further improved in conjunction with other methods such as error control coding. This framework can find applications in scalable watermarking (such as scalable video coding), rate controlled multimedia multicasting, secure wireless transmission, watermarking for distributed storage, and packet networks.

Keywords: Watermarking, Extraction, Multiple Description, Stenography, Data hiding

1. INTRODUCTION

Use of digitized information has become common place in today's society. This has given way to the urgent need for the creation and implementation of novel methods for copyright protection. While conventional data encryption prevents unauthorized data access it does not prevent piracy of the decrypted data. A method to address this problem by *tagging* the digital data is watermarking. Currently there are two classification of watermarking techniques: *public* (oblivious) and *private*. Private watermarking requires the possession of the original non-modified data for verification and detection of a watermark; while public watermarking does not. Watermark extraction at the receiver can aid in *learning* the behavior of an unknown transmission channel and design corresponding counter-measures. This can be a stepping stone to the development of intelligent watermarking methods. Therefore, our goal is the development of public watermarking techniques that allow the extraction of a watermark without the original data. In response to this issue, we propose a multiple descriptions based framework for watermark encoding and decoding.

We note that the proposed framework has other potential applications such as scalable watermarking, robust watermarking for wireless transmission, and streaming media. Practical applications of this framework can also be found in robust watermarking for packet transmission where re-transmission may not be an option due to delay constraints.

The paper is organized as follows. Section 2 deals with the description of multiple descriptions and the proposed multiple description watermarking framework. Watermark insertion, extraction, and detection procedures are also described. Experimental analysis of these algorithms are given in Section 3. Conclusions can be found in Section 4.

To appear in Proc. of Security and Watermarking of Multimedia Contents III, SPIE vol. 4314, 2001.

Further author information:

B. Graubard: E-mail: bgraubar@iastate.edu

R. Chandramouli: E-mail: rchandr1@stevens-tech.edu

C. Richmond: E-mail: crichmon@iastate.edu

2. MULTIPLE DESCRIPTION WATERMARKING

We describe the concept of multiple descriptions in the next section. This is then followed by the multiple description watermarking framework.

2.1. Multiple Descriptions

Using multiple descriptions of a source to improve the performance of coding and error-resilience has been studied by the source coding community.¹⁻³ Information theoretic analysis of the multiple description source coding problem and the achievable rates were initially studied by Wolf *et. al.*¹ and El-Gamal *et. al.*² We refer the reader to these papers for the fundamental mathematical formulation of the multiple description coding problem. The idea behind using multiple descriptions of a source is to partition the source information into various *descriptions* such that by using one or more of these source descriptions a receiver will be able to reconstruct the original source within some prescribed distortion constraints. The challenge here is to optimize the choice of descriptions, coding techniques and the rates for the different descriptions. We note that there are some important similarities and differences between the conventional use of multiple descriptions for source coding (MDC) and its proposed use in digital watermarking (MDW). Some of them are as follows :

- In MDC, each description must carry enough information about the source so that the reception of at least one of them will lead to an acceptable reconstruction of the source. In the same spirit, in MDW, each description must carry enough information about the watermark such that the reception of one or more descriptions will allow the receiver to detect or reconstruct the watermark within certain acceptable reliability measure.
- The above requirement on the information content of each description could result in redundant correlation between the various descriptions if all the descriptions were received; thus, leading to a higher source coding rate. While this is seen as a drawback in source coding, for watermarking the redundant correlation between the descriptions maybe necessary in order to extract the watermark reliably even with fewer number of received descriptions.
- Sending descriptions over different channels with different noise characteristics could lead to an improvement in the received signal quality. In the same sense, if an attacker does not have access to all the descriptions and/or does not know which descriptions contain a watermark it will not be possible to destroy/attack the watermark completely. Suppose a power-constrained attacker has access to all the descriptions, due to the lack of knowledge of which description(s) contain a watermark, the attacker will be forced to distribute the power of attack among all the descriptions, thus making the attack on any one particular description weaker. On the other hand if the attacker decides not to attack all the descriptions but selects only a subset of descriptions, it can be shown that the probability of successfully attacking the watermark decreases.
- If the sender knows *a priori* the transmission channel for each description, key parameters such as error-control coding, watermarking strength etc. can be adjusted accordingly to improve the watermark robustness.

From the above discussions we observe that many existing theories from MDC can be adapted for MDW while new constraints and requirements of watermarking systems pose additional challenges.

Multiple descriptions of a source can consist of spatial (time) domain or transform domain information. Many popular multiple description coders are based on transform domain techniques.⁴⁻⁶ Both orthogonal and non-orthogonal transforms have been used.⁴ Based on the type of application one of these descriptors can be chosen.

2.2. Multiple Description Watermarking Framework

The proposed multiple description watermarking framework is shown in Figure 1. The information content of a host signal is decomposed into M descriptions. These descriptions can either be orthogonal or have some amount of correlation between them. For watermarking application it is desirable to have some degree of correlation between the descriptions so that the reception of one or more of these descriptions will still make it possible to recover or detect the watermark with certain confidence probability. We define the multiple description watermarking problem for two descriptions and three decoders under the assumption of noiseless channels (or suitably error protected/corrected channels) as follows. Generalizations to M descriptions follows similarly. Let the original source be represented by $\{X_k\}_{k=1}^N$, $\{\tilde{X}_{k,1}\}_{k=1}^N$ denotes the reconstructed description at decoder 1 using only the first description, $\{\tilde{X}_{k,2}\}_{k=1}^N$

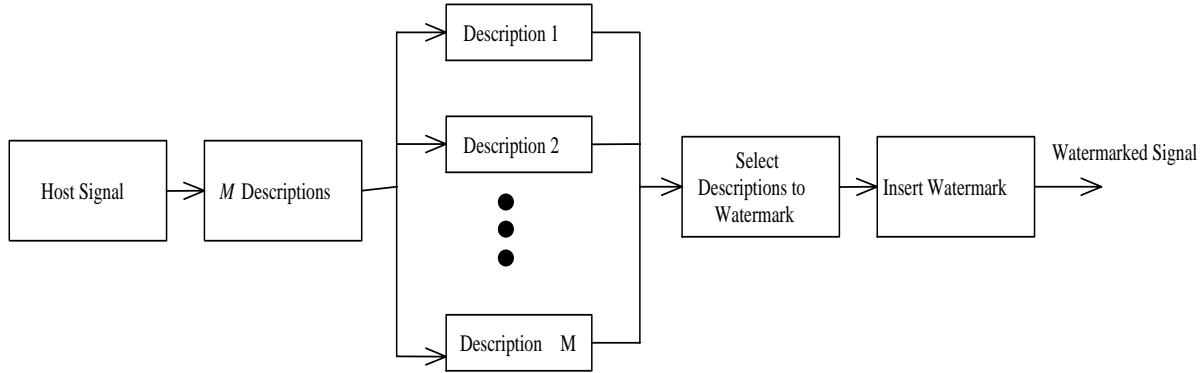


Figure 1. Multiple description watermarking framework



Figure 2. First description of Lena

denotes the reconstructed description at decoder 2 using only the second description, and $\{\tilde{X}_{k,0}\}$ denotes the reconstructed description at decoder 0 using both the descriptions. Let the watermarking rate for description i be R_i , $i = 1, 2$. Then we have the following distortions,

$$D_i = \frac{1}{N} \sum_{k=1}^N E[\phi(X_k, \tilde{X}_{i,k})], \quad i = 1, 2, 3 \quad (1)$$

where ϕ is a non-negative, real-valued distortion measure. Then the MDW problem is to find the set of achievable values for $(R_1, R_2, D_0, D_1, D_2)$, *i.e.*, find values $(r_1, r_2, d_0, d_1, d_2)$ such that for sufficiently large values of N there exists coding-decoding pairs such that $R_i \leq r_i$, $i = 1, 2$ and $D_i \leq d_i$, $i = 1, 2, 3$. We do not give a solution to this theoretical formulation of the MDW problem in this paper. However, we attempt to motivate such procedures through some MDW algorithms and their performance analysis.

We now explain the proposed framework with an example for image watermarking using discrete cosine transform (DCT) and $M = 2$. Depending on the host signal characteristics, application, and the watermarking procedure a subset of the descriptions are chosen for watermark insertion. The multiple descriptions are then *added* together to form the watermarked signal. Figure 2 and Figure 3 show the two description of the Lena image. The descriptions were obtained by grouping the alternate the DCT coefficients into two sets and then taking the inverse DCT. All the odd-indexed DCT coefficient (*i.e.*, AC_1, AC_3, \dots) belong to the first description and the even-indexed coefficients to the second description. At the start of each row and the next DCT block the strategy is reversed. This process is continued until all the DCT blocks and its coefficients have been grouped into two descriptions. This is then followed



Figure 3. Second description of Lenna

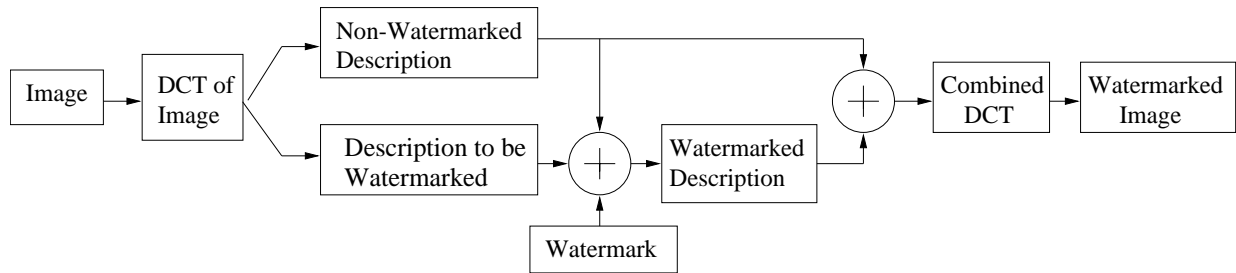


Figure 4. DCT based watermark insertion procedure for $M = 2$

by watermarking. Figure 4 shows the schematic of the watermark insertion procedure. One of the descriptions is chosen for watermark insertion while the other description serves as a reference. A relationship (watermark key) between the watermarked coefficients in one descriptions and the corresponding non-watermarked coefficients in the other is computed. This relationship will be used during the watermark extraction process. After inserting the watermark, the DCT coefficients of both the descriptions are arranged in their original positions and the inverse DCT is taken to obtain the watermarked image.

2.2.1. Watermark Insertion

As discussed previously, a relationship between the watermarked and non-watermarked description is first computed. This relationship is used during the watermark extraction process without resorting to the original host signal. We use a simple technique to decide the relationship. We discuss this technique for the case of two descriptions based on DCT. The same holds for more than two descriptions. First, one description is chosen for watermarking. Then, the DCT coefficients in the non-watermarked description are zig-zag ordered and the first few high magnitude coefficients from the ordered list are chosen. These chosen coefficients replace the corresponding coefficients in the description to be watermarked by using a simple search criterion. The reason we do this is because the non-watermarked description serves as the reference for watermark extraction. Also, the high magnitude coefficients of this description are more resilient to attacks. Therefore, this will aid in extracting the watermark even after sufficiently strong attacks. This was also confirmed through numerous experiments with different types of search and replacement techniques. Figure 5 shows the search and replacement strategy that was adopted. When a coefficient from the non-watermarked description is selected after zig-zag ordering, its value and location are noted. This value is compared to the DCT coefficient values of the valid surrounding blocks in the watermark-description as shown in Figure 5. A distance measure given by $|x - x'|$ is computed where x is the value of the coefficient from the non-watermarked description and x' is the value from the description that will be watermarked. The coefficient with the smallest distance is

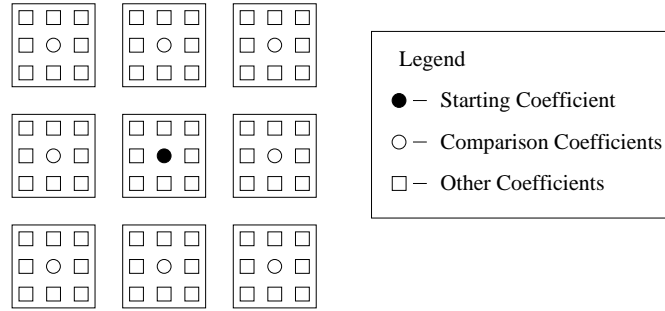


Figure 5. Search strategy

selected and used to replace the corresponding coefficient in the watermark-description and then a watermark is inserted. The reasons this replacement technique does not cause much visible distortion is due to the following : the descriptions are symmetric, *i.e.*, each description contains the same amount of information, and natural images have a high amount correlation. These facts have also been successfully exploited in reconstructing lost DCT coefficients by smoothing.⁵ Figure 6 is the watermarked Lena image using two descriptions. The watermark insertion algorithm



Figure 6. Watermarked Lena

can be summarized as follows.

Watermark Insertion Algorithm:

- Step1: Separate the image into blocks (typically 8×8) and take the DCT transform of each block.
- Step2: Separate the DCT coefficients into two descriptions.
- Step3: Select one of the descriptions to be watermarked, in this case description 2 (D_2) (see, Figure 4).
- Step4: Select DCT coefficients from description 1 (D_1) (see, Figure 4), using the method described previously.
- Step5: Remove selected coefficients from list of eligible coefficients for insertion.
- Step6: Place the location of the coefficient from D_1 into the *Key*.
- Step7: Use the value and location of the coefficient to find, replace and mark the appropriate coefficient in D_2 by the method explained previously. The watermark insertion is given by $v'_i = v_i(1 + \alpha x_i)$ where v'_i , v_i , and x_i denote the i^{th} watermarked DCT coefficient, original DCT coefficient, and the watermark, respectively. Different values of α can be used, but $\alpha = 0.1$ seems to give good performance.⁷
- Step8: Remove the coefficient from the list of eligible coefficients for insertion.
- Step9: Place the location of the coefficient from D_2 into the watermark key.

- Step10: Repeat Step4-Step9 until the entire watermark is inserted. *Note: the length of the watermark cannot exceed the size of the image.*
- Step11: Recombine D_1 and the watermarked description, D_2 .
- Step12: Take the inverse DCT to obtain the watermarked image.

2.2.2. Watermark Extraction and Detection

Given a watermarked image and the watermark key, Figure 7 shows how to extract the watermark. We summarize

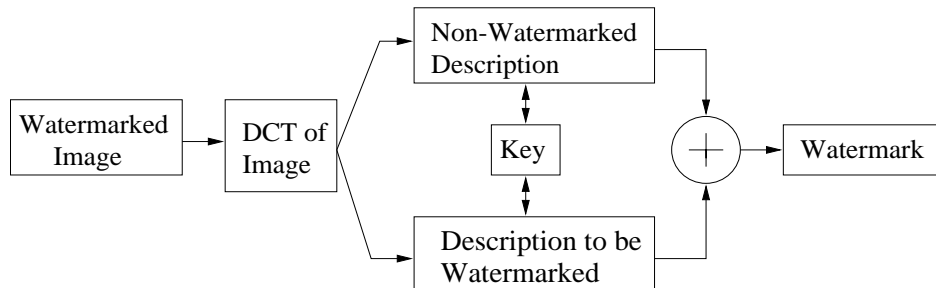


Figure 7. Watermark Extraction Method

the watermark extraction and detection in the following.

- Step1: Separate the image into blocks (typically 8x8) and compute the DCT transform of each block.
- Step2: Separate the DCT coefficients into two descriptions.
- Step3: Using the watermark key compute the difference of the watermarked coefficients (in the watermarked description) and non-watermarked coefficients to extract the watermark as follows: $x_i^* = \begin{cases} \frac{v_i' - 1}{\alpha} & : v_i \neq 0 \\ 0 & : v_i = 0 \end{cases}$ where x_i^* are the i^{th} extracted watermark.
- Step4: The extracted watermark can be compared to the original watermark using the similarity measure: $sim = \sum_{i=1}^n \frac{x_i^* * x_i}{\sqrt{x_i^* * x_i^*}}$ where x_i^* is the extracted watermark, x_i is the original watermark.

3. NUMERICAL RESULTS

We performed various simulation experiments to study the performance of the proposed multiple description watermarking framework. The ability to successfully extract and detect the watermark was investigated. Some of the experimental results are described in this section. Performance of the multiple descriptions framework for attack channels that include additive white Gaussian noise, JPEG compression, and bit error channels are given in this section. It is important to study the effect of bit errors on watermarks because, if watermarks are used in wirelessly transmitted signals they are highly prone to bit errors. The spread spectrum watermark with a Gaussian (zero mean, unit variance) distributed watermark of length 100 and α equal to 0.1 was used in all the experiments. The results are given for 256 gray level Lena image.

An additive white Gaussian noise attack was simulated in the DCT domain. Figure 8 shows the image when its DCT coefficients are corrupted by additive Gaussian noise. Clearly, the visual quality of the image is greatly degraded. By using the watermark key and the non-watermarked description as a reference, the watermark was extracted and then a detection test was performed by computing the similarity measure with the aid of the original (uncorrupted) watermark. Figure 9 compares the performances of the MDW based watermark extraction/detection method and the non-oblivious watermark detection procedure. Each value in the graph was obtained by averaging over 50 runs of the simulation. We see from the figure that even for very high noise powers the MDW based watermark extraction process without using the original host image produces reasonable performance. The difference between MDW based oblivious detection and the non-oblivious detection may be narrowed by using some kind of error protection coding for the embedded watermark. Similar performances were seen for spatial domain additive noise attacks.



Figure 8. Additive noise attack in the DCT domain.

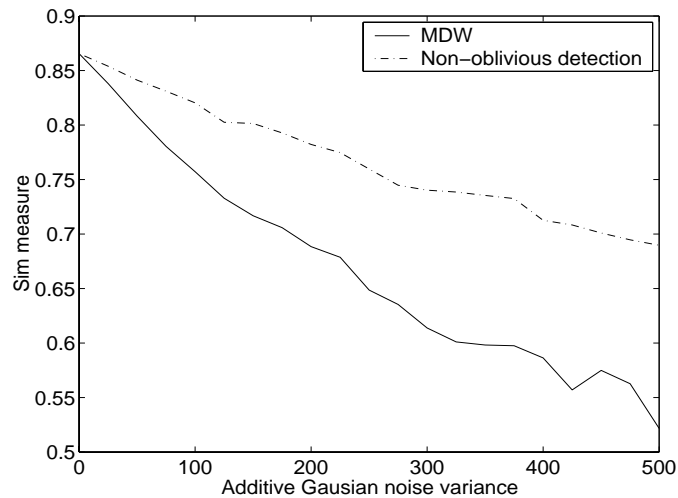


Figure 9. Performance comparison of MDW and non-oblivious watermark detection for DCT domain additive white Gaussian noise.

Next, we consider the effect of JPEG compression on the watermark. Figure 10 shows the performance results for various JPEG compression quality factors. It is seen that up to a quality factor of 10, the watermark can be reliably extracted and detected.

While additive noise attack and JPEG compression are important real-life channel attacks, in order to capture the characteristics of the effects due to a bit-error channel we simulated the effect of bit errors on the watermark. The combined effect of compression and bit-errors was investigated. The DCT coefficients were quantized after inserting the watermark. The AC coefficients were quantized using a uniform quantizer with different levels of quantization ranging from 8 to 32 (3-bit to 5-bit quantizers). A binary symmetric channel with different bit error probabilities (P_e) was used to simulate a bit-error channel. Figure 11 shows the watermark inserted image quantized in the DCT domain using a 3-bit uniform quantizer and $P_e = 10^{-3}$. Table 12 gives the performance of the proposed watermarking method. The algorithm performs poorly when the encoder bit rate is three. As the bit rate increases the algorithm becomes reasonably resistant to bit errors, except for very high error rates. We again believe that error control coding could improve the performance at the cost of a loss in the watermarking rate.

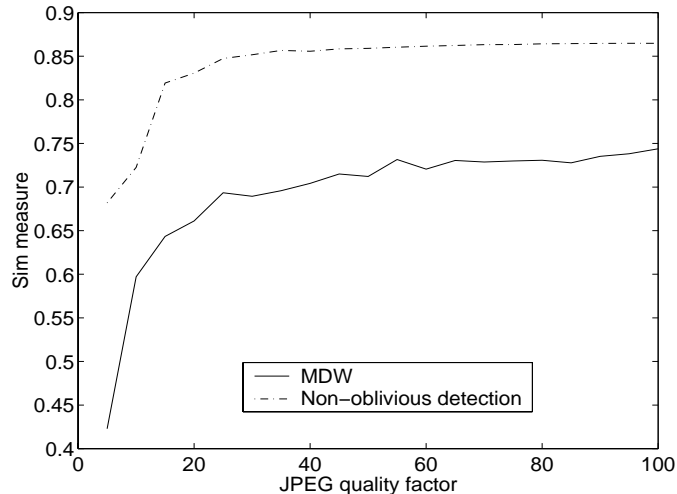


Figure 10. Performance comparison of watermark detection for MDW (oblivious detection) and watermark detection using the host image for various JPEG compression factors.



Figure 11. Watermarked image quantized in the DCT domain using a 3-bit uniform quantizer and transmitted over a binary symmetric channel with $P_e = 10^{-3}$.

4. CONCLUSION

We propose for the first time a multiple description framework for oblivious watermarking. Information theoretic definition of the problem is given. An algorithm for watermarking for DCT based multiple descriptions is described. Performance of the proposed framework for various attack channels such as additive white Gaussian noise, JPEG compression, and random bit error channels shows that the proposed method performs reasonably well compared to non-oblivious schemes. Further investigation is needed to improve the performance. Our future work will study the usage of error control coding combined with multiple description watermarking for improving the performance.

REFERENCES

1. J. Wolf, A. Wyner, and J. Ziv, "Source coding for multiple descriptions," *Bell System Technical Journal* **59**, pp. 1417–1426, October 1980.
2. A. El-Gamal and T. Cover, "Achievable rates for multiple descriptions," *IEEE Transactions on Information Theory* **28**, pp. 851–857, November 1982.

Similarity Measure			
P_e	Number of quantization bits		
	3	4	5
0	0.5699	0.8688	0.99
10^{-5}	0.5699	0.8688	0.9611
10^{-4}	0.56	0.6177	0.9
10^{-3}	0.5	0.55	0.9

Figure 12. Performance of MDW in the presence of compression and random channel bit-errors.

3. Y. Wang, M. Orchard, and A. Reibman, "Multiple description image coding for noisy channels by pairing transform coefficients," *Proc. Workshop on Signal Processing*, June 1997.
4. D.-M. Chung and Y. Wang, "Multiple description image coding using signal decomposition and reconstruction based on lapped orthogonal transforms," *IEEE Transactions on Circuits and Systems for Video Technology* **9**, pp. 895–908, September 1999.
5. J. Ridge, F. Ware, and J. Gibson, "Permuted smoothed descriptions and refinement coding for images," *IEEE Journal on Special Areas in Communications* **18**, pp. 915–926, May 2000.
6. V. Vaishampayan, "Design of multiple description scalar quantizers," *IEEE Transactions on Information Theory* **39**, pp. 821–834, May 1993.
7. I. Cox, J. Kilian, T. Leighton, and T. Shanon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing* **6**, pp. 1673–1687, December 1997.