SET PARTITIONING IN OBLIVIOUS DATA HIDING

Litao Gang, Ali N. Akansu and Mahalingam Ramkumar

New Jersey Center for Multimedia Research
ECE Dept., New Jersey Institute of Technology
University Heights, Newark, NJ 07102.
{lxg8906, ali, mxr0096}@njit.edu

ABSTRACT

In oblivious steganography, host noise suppression is a great concern as the watermark signal energy is usually much less than that of the host signal. In this paper, we model the data hiding as a more general H0/H1 hypothesis testing problem. Decision making is based on the statistical distinction between H0 and H1. A simple embedding scheme, viz., set partitioning, is proposed. The coefficients are divided into two sets to represent bit value 1 and 0. The average distortion introduced is calculated. Its optimum and suboptimal detection is discussed in detail. Analysis and simulation studies show improvement over existing schemes.

1. INTRODUCTION

Digital watermarking or data hiding is the art of hiding information in a cover signal (image, audio, video, etc.). The technique provides a potential solution for multimedia copyright protection. Two requirements in watermarking are *robustness* and *transparency*.

In oblivious applications where the original cover signal is not available, the host noise suppression is a great concern, since the energy of the host signal is much larger than that of the watermark signal.

In Section 2, we model data hiding as a general hypothesis testing problem. The decoder needs to answer the question, Yes/No (watermark detection) or bit value 1/0 (data hiding). The two hypotheses H0 and H1 must have different statistical properties. A simple method, viz., *set partitioning* is proposed.

The average distortion introduced by this scheme is calculated in Section 3.

In Section 4, decoding is discussed in detail, including hard and soft detectors. As the ML detector is quite complicated and infeasible to implement, two suboptimal algorithms are proposed and their PE (Probability of Error) versus SNR performances are analyzed.

In Section 5, some experimental results are presented. Simulation studies demonstrate improvement over existing schemes.

Conclusions are presented in Section 6.

This work is partly supported by Panasonic Technologies, NJ

2. HYPOTHESIS TESTING AND SET PARTITIONING

Watermarking or data hiding is, in essence, a hypothesis testing problem. Suppose c is an original coefficient in some watermark domain (could be a DCT or wavelet coefficient, for instance) in which one bit is to be embedded. Let x denote the coefficient after embedding. The two hypotheses are

H0: bit value 0 embedded in x.

H1: bit value 1 embedded in x.

Obviously, H0 and H1 have different statistical properties. A good watermarking algorithm should modify the statistical property of a cover signal without much perceptual degradation.

Many methods, for example, Patchwork [2], Spread Spectrum (SS) [4] superimpose a random sequence in the original cover signal. These methods, while successful in escrow applications, are not very effective in oblivious scenarios.

In a noise free scenario, how can the decoder make a reliable decision H1/H0 on a given x? Answer is simple and straight forward, make H0 and H1 have *no* element in common. Thus decoder can always make a correct decision.

In a noisy environment, detection is not as reliable as in noise-free cases. To increase its robustness to noise, we can simply keep the element in H0 and H1 some distance apart.

This simple watermarking idea could be extended to the following data hiding scheme, which we will discuss in detail in this paper. Two separate sets are constructed on the real axis (Fig. 1). The embedded coefficient value should be kept in a set according to the bit value to be hidden.

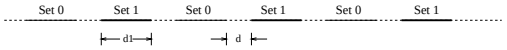

Figure 1: Set Partitioning Scheme

To embed bit value 1, the coefficient x should be kept in set 1. If the original value of c is already in set 1, no modification is needed. Otherwise it is replaced by the nearest element in set 1. Similarly, after embedding bit value 0, x is kept in set 0.

To hide one bit information in a coefficient sequence $\mathbf{c}$, we need to define a deterministic pattern to represent bit values. For example to embed 1 bit in a 5-coefficient

sequence, we can define two patterns

Pattern A (bit 1): {set 1, set 0, set 1, set 0, set 1},

Pattern B (bit 0): {set 0, set 1, set 0, set 1, set 0}.

To hide a bit, the modified sequence **x** should comply with Pattern A (to hide bit 1) or Pattern B (to hide bit 0). For example, to hide bit value 1, $x_0 \in$ set 1, $x_1 \in$ set 0, $x_2 \in$ set 1, $x_3 \in$ set 0 and $x_4 \in$ set 1.

We name this method *set partitioning*.

3. AVERAGE DISTORTION

In the following analysis, we assume c is uniformly distributed in the region $(-a, a)$.

Denote the error introduced in embedding as $e = x - c$. As depicted in Fig. 2, suppose bit value 1 is to be embedded, consider the typical region AD.

If c is in the range AB, no modification is needed, $e = 0$.

If c is in the range BD, e is uniformly distributed in $(-d - d1/2, d + d1/2)$. The conditional probability can be expressed as, $P(c \in AB | c \in AD) = \frac{d1}{2d1+2d}$, $P(c \in BD | c \in AD) = \frac{2d+d1}{2d1+2d}$. The average distortion is

$$D = \frac{(2d+d1)}{(2d1+2d)} \cdot \frac{(2d+d1)^2}{12} = \frac{1}{12}\frac{(2d+d1)^3}{(2d+2d1)}. \quad (1)$$

This result holds if bit value 0 is embedded instead.

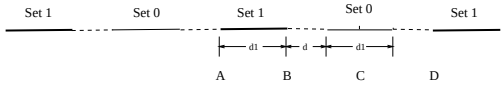

Figure 2: Average Distortion Calculation

4. DETECTION

4.1. Hard Decision Detection

Suppose one bit is embedded in an N-coefficient sequence **c**.

The simplest detection rule is majority vote. That is hard decision based on individual coefficient. Real axis is divided into decision region 1 and 0 (Fig. 3). If received coefficient r falls in Region 1, it is decided the transmitted signal x comes from set 1. Otherwise we assume it comes from set 0. In the example just mentioned, if a received sequence pattern is {set 0, set 1, set 0, set 1, set 0}, which is more similar to pattern A (2 coefficient difference) than to Pattern B (3 coefficient difference), the decision is made in favor of bit value 1.

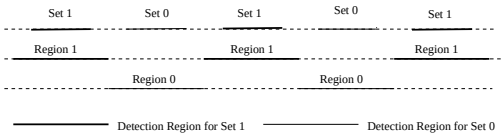

Figure 3: Hard Decision Region

4.2. Maximum Likelihood Detection in Gaussian Noise

A better solution is Maximum Likelihood (ML) detector.

Denote x as the transmitting signal and r is the received coefficient after Gaussian channel, $n \sim N(0, \sigma^2)$.

The ML likelihood ratio [5] is

$$R = \frac{P(x \in \text{set } 1 | r)}{P(x \in \text{set } 0 | r)}, \quad (2)$$

where $P(y|x)$ is the probability of y given x.

Rewriting the above equation using different variables u and v

$$R = \frac{\sum_{u \in \text{set } 1} P(u|r)}{\sum_{v \in \text{set } 0} P(v|r)}. \quad (3)$$

where

$$P(u|r) = \frac{P(u) f(r|u)}{f(r)}. \quad (4)$$

The above becomes

$$R = \frac{\sum_{u \in \text{set } 1} P(u) f(r|u)}{\sum_{v \in \text{set } 0} P(v) f(r|v)}. \quad (5)$$

Gaussian noise probability density function is

$$f(r|u) = \frac{1}{\sqrt{2\pi}\sigma} \cdot exp(\frac{-(r-u)^2}{2\sigma^2}). \quad (6)$$

The original coefficient c is uniformly distributed, its probability density function $f(x) = \frac{1}{2a} \quad -a \le x \le a$. After embedding information bit value 1, the probability of the transmitting signal $P(u)$ is depicted in Fig. 4.

Note the probability pulses at the end points. They happen with greater probability because any c out of the set 1 is replaced by the end points.

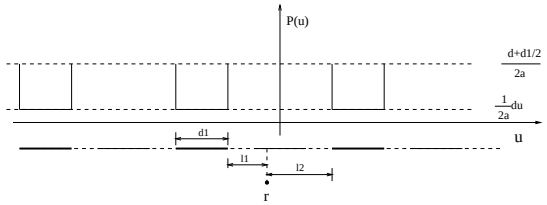

Figure 4: Calculation of ML ratio

$$\sum_{u \in \text{set } 1} P(u) f(r|u) = \frac{1}{2a} \int_{r-l_1-d1}^{r-l_1} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(u-r)^2}{2\sigma^2}} du + \frac{1}{\sqrt{2\pi}\sigma} \frac{d+d1/2}{2a} e^{\frac{-l_1^2}{2\sigma^2}} + \frac{1}{2a} \int_{l_1-2d-3d1}^{l_1-2d-2d1} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(u-r)^2}{2\sigma^2}} du + .. \quad (7)$$

In the same way, $\sum_{u \in \text{set } 0} P(v) f(r|v)$ can be calculated and yields a result similar to (7). However, a closed-form result of ML ratio in (2) can not be obtained. Besides, as noise power σ^2 is usually unknown at decoder, the detector is infeasible in practice.

The challenge in the decoding is that the transmitted signal could be any value in these two sets. The ML ratio calculation thus involves all elements in set 1 and set 0. In the following suboptimal methods, we assume the transmitted signal is discrete instead of continuous.

4.3. Suboptimal Detection 1

In this approximation, we simply assume the transmitted signals are at the center of the continuous segments, the signaling is a pattern like xoxo as depicted in Fig. 5 (A). Signal points x and o occur with equal probability.

ML ratio can be expressed as:

$$R = \frac{P(x \in \text{set } 1|r)}{P(x \in \text{set } 0|r)}. \quad (8)$$

Still there are many x and o points to be considered.

Our simulation studies show that we can further simplify it by merely considering the nearest x and o points. Thus (8) reduces to

$$R = \frac{P(r|x = x_1)}{P(r|x = x_0)}, \quad (9)$$

where x_1/x_0 is the nearest points x/o in set 1 and set 0.

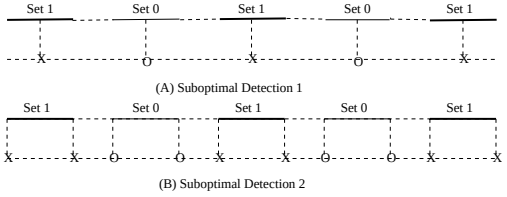

Figure 5: Suboptimal Detection in Set Partitioning

4.4. Suboptimal Detection 2

In Fig. 4, it is observed that the endpoints are transmitted with higher probability. Another reasonable approximation assumes the transmitted signals have xxoo pattern as shown in Fig. 5 (B).

Only the nearest end points are considered as transmitting signal, that yields the same results as (9).

In the case where one information bit is embedded in an N-coefficient sequence, sequence detector can be constructed.

In the example just mentioned above, a 5-coefficient sequence $\mathbf{r}$ is received. The nearest x and o points to r_i are denoted as u_i (in set 1) and v_i (in set 0). According to the given pattern in Section 2, two sequence candidates are constructed,

Pattern A Type: $\mathbf{u} = \{u_0, v_1, u_2, v_3, u_4\}$.

Pattern B Type: $\mathbf{v} = \{v_0, u_1, v_2, u_3, v_4\}$.

If $||\mathbf{r} - \mathbf{u}|| < ||\mathbf{r} - \mathbf{v}||$, the received sequence is more similar to the Pattern A, bit value 1 is decided. Otherwise, bit value 0 is decided.

5. SIMULATION AND EXPERIMENTAL RESULTS

To evaluate the scheme, we measure the watermark distortion against extracted Probability of Error (PE) in Gaussian noise environment. SNR is redefined as the ratio of distortion energy S over noise power σ^2.

The comparison of the detection algorithms is shown in Fig. 6. The sequence is composed of 11 coefficients. The ratio $d/d1 = 1$. The result shows that Method 2 outperforms Method 1. Further simulation shows decoding performance in Method 2 is almost the same as ML detector. Both suboptimal methods far outperform the hard decision decoder.

It is observed that PE-SNR is only affected by the ratio of $d/d1$. Fig. 7 is the result of embedding 1 bit in an 8-coefficient sequence. It shows that the smaller $d/d1$ performs better at lower SNR. However at higher SNR, larger $d/d1$ is more advantageous. Because in practice, data hiding always works at lower SNR, usually $SNR < 1$ (watermark distortion is not expected to be larger than moderate or severe compression distortion), smaller $d/d1$ is more suitable.

A very effective oblivious scheme, Quantization Index Modulation (QIM) [1] [3], is just a special case of the set partitioning scheme with $d1 = 0$. In that scheme, the marked coefficient x is discrete instead of continuous (Fig. 8).

The set partitioning scheme offers us the flexibility to choose different value of $d/d1$. In most applications where SNR is low, signaling with $d/d1 = \infty$ (QIM) is not a good choice.

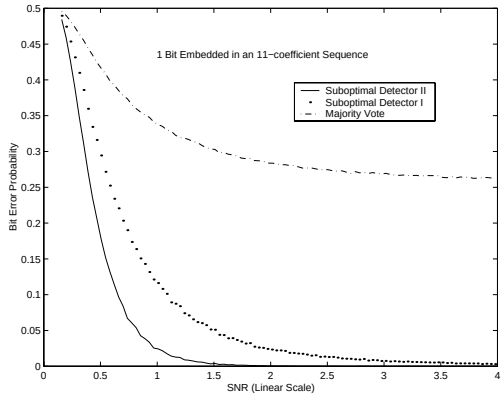

Figure 6: Detection Performance Comparison

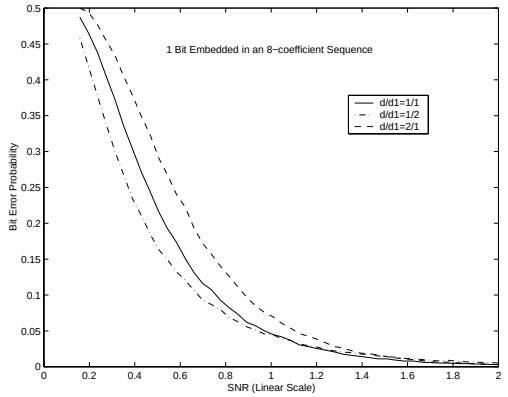

Figure 7: PE-SNR at different $d/d1$

Figure 8: QIM Embedding

In Fig. 9, one bit is embedded in a 4-coefficient sequence. Several $d/d1$ selections outperform QIM. The improvement is noticeable. At higher SNR, QIM performs slightly better than the signaling with $d/d1 = 1/1$, as shown in Fig. 10. However, the latter is more promising due to the fact SNR is mostly low in practice. In other words, the proposed set partitioning method is more reliable in noisy scenario.

Given same distortion energy, the maximum error e in $d/d1 = 1$ signaling is larger than that in QIM scheme. Under the same maximum error constraint (which implies

less distortion energy in $d/d1 = 1$ signaling), the former still demonstrates significant advantage over QIM scheme at lower SNR.

In practice, it may be desired that the set partition be kept secret. For example, we can apply a shifted set partition in Fig. 1 in embedding. The shift value is a random variable only known at decoder. A randomly selected set partitions are used for different coefficients in a sequence. That can enhance its security.

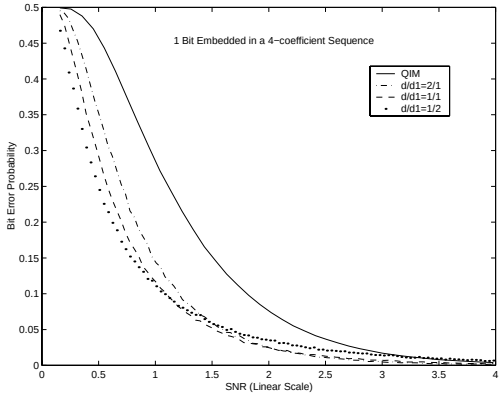

Figure 9: PE-SNR at Lower SNR

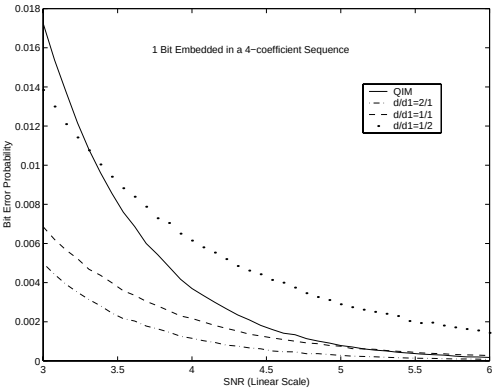

Figure 10: PE-SNR at Higher SNR

This scheme can be employed instead of SS modulation. It could be used in various watermark domains. In our image data hiding experiments, information bits are embedded in the DFT amplitude domain. A pattern is embedded in the medium frequency coefficients. In our experiment, 64 bits are embedded in a 256x256 images. Fig. 11 and Fig. 12 show the original and marked images. Experiments demonstrates its robustness against common compression and filtering attacks. More precise artifacts control and higher hiding capacity are under further investigation.

6. CONCLUSIONS

In this paper, a new oblivious data hiding scheme is proposed. It is based on hypothesis testing. Its goal is not to "modulate" a signal, but to change the statistical properties. The ML detection is analyzed and two very effective suboptimal detection methods are discussed and compared. Simulation studies shows it is a promising steganographic scheme.

7. REFERENCES

[1] B.Chen and G.W. Wornell. "Dither Modulation: A new approach to digital watermarking and information embedding". *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, 3657:344–353, Jan 1999.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Technique for data hiding". *IBM System Journal*, 35(3-4):313–336, 1996.

[3] B. Chen and G. W. Wornell. "Digital watermarking and information embedding using dither modulation". *Proc. of 1998 IEEE 2nd Workshop on Multimedia Signal Processing*, pages 273–278, Dec 1998.

[4] I. J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. "A Secure, Robust Watermark for Multimedia". *Workshop on Information Hiding*, May 1996.

[5] Steven M. Kay. "Fundamentals of statistical signal processing". *Volume 2*, Prentice-Hall PTR, 1993.

Figure 11: Original Lenna Image

Figure 12: Marked Lenna Image