EURASIP Journal on Applied Signal Processing 2004:14, 2102–2112

Linear and Nonlinear Oblivious Data Hiding

Litao Gang
InfoDesk, Inc., 660 White Plains Road, Tarrytown, NY 10591, USA
Email: lxg8906@njit.edu

Ali N. Akansu
Department of Electrical and Computer Engineering (ECE), New Jersey Institute of Technology,
University Heights, Newark, NJ 07102-1982, USA
Email: akansu@njit.edu

Mahalingam Ramkumar
Department of Computer Science and Engineering, Mississippi State University, MS 39762-9637, USA
Email: ramkumar@cse.msstate.edu

Received 31 March 2003; Revised 6 October 2003

The majority of the existing data hiding schemes are based on the direct-sequence (DS) modulation where a low-power random sequence is embedded into the original cover signal to represent hidden information. In this paper, we investigate linear and nonlinear modulation approaches in digital data hiding. One typical DS modulation algorithm is explored and its optimal oblivious detector is derived. The results expose its poor cover noise suppression as the hiding signature signal always has much lower energy than the cover signal. A simple nonlinear algorithm, called set partitioning, is proposed and its performance is analyzed. Analysis and simulation studies further demonstrate improvements over the existing schemes.

Keywords and phrases: data hiding, watermarking, ML detection, data security.

1. INTRODUCTION

Multimedia data hiding is the art of hiding information in a multimedia content cover signal, like image, video, audio and so forth. Its potential applications include, but not limit to authentication, copyright enforcement, piracy tracking, and others. Various data hiding techniques are deployed in different scenarios. For instance, fragile data hiding is often used for multimedia content authentication, while the robust data hiding techniques are mostly employed for copyright and ownership proof, illegal replication prevention, and the like. The requirements and techniques in different applications vary considerably. This paper focuses on the robust data hiding techniques.

Transparency and robustness are the two basic requirements in the robust data hiding applications. The former requires that the information embedding not compromise the multimedia perceptual quality; and the latter guarantees that the embedded information can be reliably identified under unintentional attacks and malicious tampering efforts. The data hiding employment can be further classified into two categories, *oblivious* and *escrow* cases. In the oblivious scenarios, the hidden information can be extracted without reference to the original signal; by contrast, the cover signal is necessary for embedded message identification in escrow cases. In practice, the most useful and challenging application is the oblivious data hiding since the original cover signal is often unavailable at the decoder. Most work in the paper is devoted to the oblivious data hiding.

Among the existing robust message embedding schemes, direct-sequence (DS) modulation algorithms have been extensively studied and widely employed [1, 2, 3, 4]. The algorithms based on this principle embed a key-generated direction vector **s** into the cover signal. Perceptual models are usually employed to constrain the introduced artifacts. Although originally proposed for escrow applications, the DS schemes have also been used in oblivious cases, such as message embedding in video [4, 5], audio [1, 6], and images [7, 8]. However, the performance limitations of these algorithms are not fully investigated. We try to fill the gap in the literature. In the first part of the paper, the performance of the DS modulation and its corresponding detection algorithms is analyzed. Both theoretical analysis and simulation studies highlight the inefficiency of these algorithms for the cover noise suppression. This result is intuitive as the hiding signals have very low energy compared to the original content signals. In the second part, a novel data hiding algorithm is proposed, and its performance is analyzed and compared with existing schemes.

The rest of this paper is organized as follows. In Section 2, the performance of a widely used DS modulation is investigated. Both analytical and simulation studies unveil its inferior results in oblivious applications. Further analysis also reveals that the ubiquitously-used correlation detector is not optimal. This paper proposes the maximum likelihood (ML) detector and its performance is analyzed. In Section 3, a modified version of the scheme is presented and its performance gains are validated through simulation studies. Instead of linearly superimposing a hiding signal into the cover signal, a nonlinear hiding scheme called *set partitioning* is proposed in Section 4. The distortion introduced for data embedding is calculated, and the corresponding ML detector and suboptimal detectors are discussed in Section 5. In Section 6, the data embedding and detection performance is measured in terms of bit error rate (BER) versus distortion-to-noise ratio (DNR). Simulation results demonstrate performance improvements of the set partitioning technique over the DS and existing nonlinear data hiding schemes. Finally, the conclusion is presented in Section 7.

2. DIRECT-SEQUENCE MODULATION EMBEDDING

2.1. Modulation and correlation detection

Most of the existing DS modulation schemes are based on the simple idea: embedding a low-energy random sequence into the cover signal while keeping the distortion transparent. The hidden information is usually extracted via a correlation decoder. Perceptual threshold analysis is often necessary to shape the artifacts introduced. And it is a requisite to guarantee that the distortion is below the just noticeable distortion (JND) threshold to meet the data hiding transparency requirement. On the other hand, it is favorable to inject the maximum permissible embedding energy (*deep embedding*) that enhances the detection reliability without perceptual degradation.

The hidden information is usually embedded in a transform domain of discrete cosine transform (DCT) and wavelets are the most frequently used domains for image data hiding, for instance. Given an original coefficient value c_i in the hiding domain, we exercise one of the most popular deep-hiding schemes [2], and the resulting coefficient x_i is expressed as

$$x_i = \begin{cases} c_i + w_i\,|\,c_i\,|\,\alpha & \text{to hide bit value 1,} \\ c_i - w_i\,|\,c_i\,|\,\alpha & \text{to hide bit value 0,} \end{cases} \tag{1}$$

where α is the perceptual threshold ratio and w_i is a binary random value of either $+1$ or -1. The value of α can be obtained from empirical experiments or perceptual models. The bit is embedded into an original sequence $\mathbf{c}$ instead of one single coefficient in practice. If $\mathbf{w}$ is the key-generated random sequence, given a received sequence $\mathbf{r}$ resulting from a noisy channel transmission of signal $\mathbf{x}$, the test statistic in the escrow correlation detector is obtained as

$$q = \sum_{i=0}^{N-1} (r_i - c_i) w_i = \sum_{i=0}^{N-1} (x_i + n_i - c_i) w_i, \tag{2}$$

where N is the sequence length and $\mathbf{n}$ is the channel noise. If $q > 0$, and a bit value 1 is decided, and a bit value 0 otherwise.

In the oblivious data hiding applications where the original cover signal $\mathbf{c}$ is not available, (2) still works. Assume that the embedded information bit value is 1; the correlation-like detector output is calculated as

$$q = \sum_{i=0}^{N-1} r_i w_i = \sum_{i=0}^{N-1} c_i w_i + \sum_{i=0}^{N-1} n_i w_i + \sum_{i=0}^{N-1} \alpha\,|\,c_i\,|. \tag{3}$$

Compared with (2), the first term in (3) is a disturbance term that degrades detection reliability. Considering the independence of $\mathbf{c}$ and $\mathbf{w}$, we can make the approximation

$$\sum_{i=0}^{N-1} c_i w_i \approx 0 \tag{4}$$

if the sequence length N is sufficiently large.

In the oblivious hiding scenarios, the original signal is unavailable and therefore treated as a noise (known as "cover noise") by the decoder. Its energy dominates the channel noise. For simplicity, in the oblivious detection discussion, merely the cover noise is considered, that is, assuming $n_i = 0$. Subsequently, (3) is reduced to

$$q = \sum_{i=0}^{N-1} r_i w_i = \sum_{i=0}^{N-1} \left(c_i w_i + \alpha\,|\,c_i\,|\right) = \sum_{i=0}^{N-1} p_i, \tag{5}$$

where

$$p_i = c_i w_i + \alpha\,|\,c_i\,|. \tag{6}$$

Note that w_i assumes a value of either $+1$ or -1; therefore, $p_i = c_i + \alpha|c_i|$ or $p_i = c_i - \alpha|c_i|$. Due to the symmetry of the probability density function (PDF) of c_i, the statistical distribution of p_i is independent of the specific value of w_i. It has the same mean value and variance as the random variable

$$y_i = c_i + \alpha\,|\,c_i\,|. \tag{7}$$

Suppose that the original coefficient c_i is identically and independently distributed (i.i.d.) with the Gaussian PDF $c_i \sim N(0, \sigma^2)$. The expectation of y_i is computed as

$$E[y_i] = 2\alpha \int_0^{\infty} \frac{x}{\sqrt{1/\pi}\sigma} e^{-x^2/2\sigma^2} dx = \sqrt{\frac{2}{\pi}}\sigma\alpha. \tag{8}$$

The variance of y_i becomes

$$E\left[\left(y_i - E[y_i]\right)^2\right] = E\left[\left(y_i - \sqrt{\frac{2}{\pi}}\sigma\alpha\right)^2\right] = (1 + \alpha^2)\sigma^2. \tag{9}$$

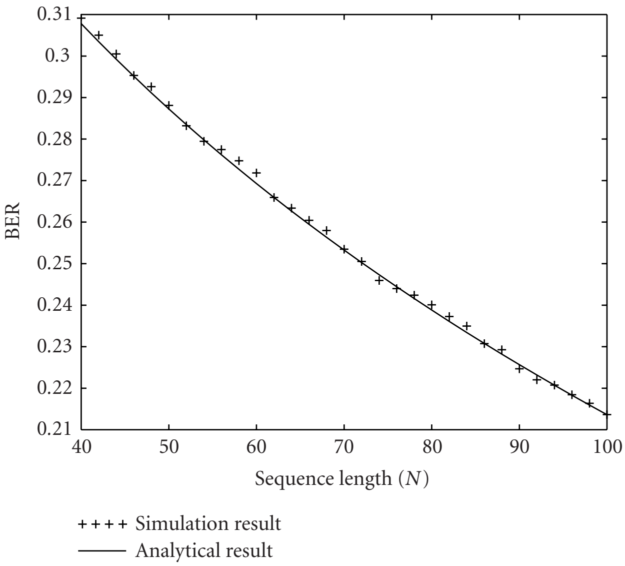


Figure 1: Correlation detection performance.

For a large value of N, the test statistic q in (5) is approximately Gaussian distributed,

$$q \sim N\left(\sigma\alpha N\sqrt{\frac{2}{\pi}}, N(1+\alpha^2)\sigma^2\right). \tag{10}$$

Similarly, if a bit value 0 is embedded, the probability distribution results in

$$q \sim N\left(-\sigma\alpha N\sqrt{\frac{2}{\pi}}, N(1+\alpha^2)\sigma^2\right). \tag{11}$$

If the decision threshold is set as $\gamma = 0$, then the BER is expressed as

$$\text{BER} = Q\left(\alpha\sqrt{\frac{2N}{(1+\alpha^2)\pi}}\right), \tag{12}$$

where $Q(\cdot)$ is the Gaussian-PDF tail integral function.

Our simulation results are depicted in Figure 1. The distortion threshold ratio is chosen as $\alpha = 0.1$ in the simulation and the original coefficient x_i is Gaussian distributed with zero mean and variance $\sigma^2 = 50^2$. The information bit is embedded and decoded using (1) and (3), respectively. The above analysis result in (12) agrees perfectly with the simulation output. Equation (12) gives us a good performance estimate of the DS embedding scheme. In fact, the above BER holds even if c_i is not Gaussian distributed, according to the central limit theorem (CLT) [9]. This result unveils the inadequacy in the DS approach. Lower BER can only be achieved with a very large value of N. In other words, the hidden information detection reliability can only be obtained at the sacrifice of the hiding capacity.

2.2. Maximum likelihood detection

The modulated signal is not independent of the noise in the above deep-hiding oblivious scheme (1). Hence the correlator-like detection may not be optimal.

Provided a received sequence $\mathbf{r}$, the decoder deals with the hypothesis testing problem

$$\begin{aligned} &\text{H1:} \quad r_i = c_i + |c_i| k_i, \quad \text{bit value 1 is embedded,} \\ &\text{H0:} \quad r_i = c_i - |c_i| k_i, \quad \text{bit value 0 is embedded,} \end{aligned} \tag{13}$$

where $k_i = w_i\alpha$ (k_i is either $+\alpha$ or $-\alpha$).

The ML ratio is expressed as

$$R = \frac{P(\text{H1}|\mathbf{r})}{P(\text{H0}|\mathbf{r})}. \tag{14}$$

According to the previous assumption that c_i is Gaussian distributed, the conditional PDF immediately follows:

$$\begin{aligned} &f(r_i|\text{H1}) \\ &\quad = \begin{cases} \dfrac{1}{\sqrt{2\pi}\sigma(1+k_i)} \cdot \exp\left[\dfrac{-r_i^2}{2(1+k_i)^2\sigma^2}\right] & (r_i > 0), \\ \dfrac{1}{\sqrt{2\pi}\sigma(1-k_i)} \cdot \exp\left[\dfrac{-r_i^2}{2(1-k_i)^2\sigma^2}\right] & (r_i < 0), \\ \dfrac{1}{\sqrt{2\pi}\sigma}, & (r_i = 0). \end{cases} \end{aligned} \tag{15}$$

Similarly, $f(r_i|\text{H0})$ can be obtained. If H1 and H0 have equal a priori probabilities, $P(\text{H0}) = P(\text{H1})$, the ML ratio yields

$$\frac{P(r_i|\text{H1})}{P(r_i|\text{H0})} = \begin{cases} \left(\dfrac{1-k_i}{1+k_i}\right) \cdot \exp\left[-\beta \cdot s(k_i) r_i^2\right] & (r_i > 0), \\ \left(\dfrac{1+k_i}{1-k_i}\right) \cdot \exp\left[+\beta \cdot s(k_i) r_i^2\right] & (r_i < 0), \\ 1 & (r_i = 0), \end{cases} \tag{16}$$

where $s(\cdot)$ is the sign function defined as

$$\begin{gathered} s(x) = \begin{cases} +1, & x > 0, \\ -1, & x < 0, \\ 0, & x = 0, \end{cases} \\ \beta = \gamma\frac{1}{\sigma^2}, \\ \gamma = \frac{1}{2(1+\alpha)^2} - \frac{1}{2(1-\alpha)^2}. \end{gathered} \tag{17}$$

If one single bit is embedded in a sequence $\mathbf{x}$, the final ML ratio in (14) becomes

$$R = \prod_{i=0}^{N-1}\left(\frac{1-k_i}{1+k_i}\right)^{s(r_i)} \cdot \exp\left[\sum_{i=0}^{N-1} -s(r_i) \cdot s(k_i) \cdot r_i^2\beta\right]. \tag{18}$$

If $R > 1$, a bit value 1 is decoded, or 0 otherwise. Nevertheless, the above ML detector is quite complicated and computationally extensive. Moreover, the accurate value of the noise variance σ^2 is usually unavailable. A suboptimal computation efficient detector is a must in real-world applications. One straightforward observation from (18) is that for

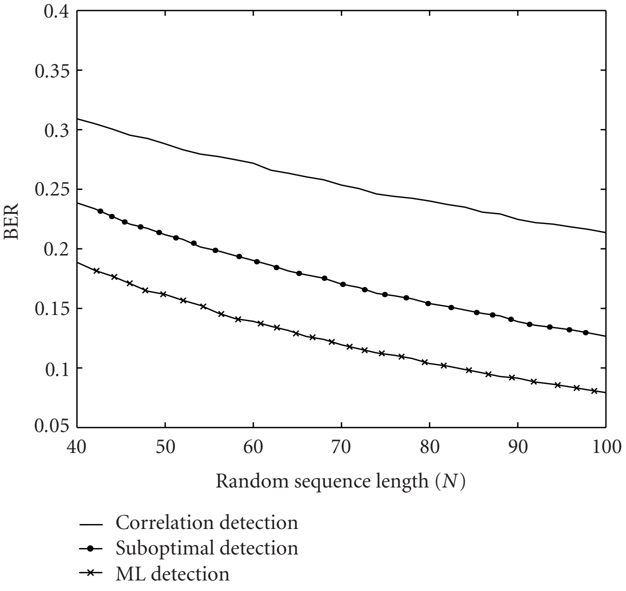


FIGURE 2: Detection performance comparison.

sufficiently large sequence length N,

$$\prod_{i=0}^{N-1}\left(\frac{1-k_i}{1+k_i}\right)^{s(r_i)} \approx 1. \tag{19}$$

This assumption is reasonable as a randomly generated sequence implies that the counts of -1's and $+1$'s are roughly equal. Under this approximation, a suboptimal detector statistic can be derived immediately from (18),

$$q = \sum_{i=0}^{N-1} -s(r_i)\cdot r_i^2\gamma\cdot s(k_i). \tag{20}$$

The suboptimal detector has comparable computational complexity as (5). Nevertheless, it outperforms the latter as depicted in Figure 2. In our simulation studies, one single information bit is embedded into an original coefficient sequence using (1). The coefficients in the sequence are i.i.d. distributed with zero mean and variance $\sigma = 50^2$. The perceptual distortion threshold ratio value is chosen as $\alpha = 0.1$. The embedded bit is detected using (2), the ML detector using (18), and the suboptimal detector using (19), respectively. The embedding and decoding process is repeated for different sequence lengths N, and the BER-N plot is shown in Figure 2. The suboptimal detector improvement over the correlation-type detector is impressive although it is still inferior to the optimum detector (18) due to the approximation (19).

Any data hiding scheme alters some statistical properties of the original cover signal. In the embedding operation, the main impact of the hiding operation (1) is the modification of variance value of x_i. The ML decoder bases the detection decision on the variance value distinction, while the correlation-like test statistics targets at the mean value. The gains in the suboptimal detection are intuitive in this perspective.

In the next section, we make further attempts to boost the hiding performance.

3. LINEAR MODULATION AND DETECTION

In the hiding scheme aforementioned, we remove the absolute value operator. The data-hiding hypotheses testing becomes

$$\begin{aligned} &\text{H1:}\quad r_i = c_i + c_i k_i, \quad \text{bit value 1 is embedded,}\\ &\text{H0:}\quad r_i = c_i - c_i k_i, \quad \text{bit value 0 is embedded.}\end{aligned} \tag{21}$$

After embedding, the variance of the modified coefficients is equal to $\sigma_1^2 = (1+\alpha)^2\sigma^2$ or $\sigma_0^2 = (1-\alpha)^2\sigma^2$.

Similar to the analysis in Section 2, the ML ratio on r_i yields

$$\frac{P(r_i|\text{H1})}{P(r_i|\text{H0})} = \left(\frac{1-k_i}{1+k_i}\right)\cdot\exp\left[\sum_{i=0}^{N-1} -s(k_i)\cdot r_i^2\gamma\right] \quad (r_i \neq 0). \tag{22}$$

In the above equation, if the sequence length N is even and $\mathbf{w}$ has the equal number of $+1$'s and -1's, it can be easily shown that

$$\prod_{i=0}^{N-1}\frac{1-k_i}{1+k_i} = 1. \tag{23}$$

Finally, the detection test statistic is obtained as

$$q = \sum_{i=0}^{N-1} s(k_i)\cdot r_i^2\gamma \tag{24}$$

and the decision threshold value is $q = 0$.

The above detector is easy to implement. To guarantee that the sequence $\mathbf{w}$ has equal number of $+1$'s and -1's, we can simply set $\mathbf{w} = [\mathbf{p}, -\mathbf{p}]$, where $\mathbf{p}$ is an $N/2$ random sequence length. The shortcoming of this adaptation is the sequence security compromise.

The detection performance is computed as follows. In this hiding scheme, all the original coefficients c_i can be divided into two sets, A and B, based on the variance value modification polarity. Suppose that the variance values of the elements in A are increased while the variances of those in B are decreased; the statistic test follows as

$$q = \sum_{\{r_i\in A\}} r_i^2\gamma - \sum_{\{r_i\in B\}} r_i^2\gamma. \tag{25}$$

After we define two variables $t_1 = \sum_{\{r_i\in A\}} r_i^2$ and $t_0 = \sum_{\{r_i\in B\}} r_i^2$, it can be proved mathematically that both t_1 and t_0 have $M = N/2$ degree of freedom Γ distribution whose PDF is expressed as

$$f(t_i) = \frac{t_i^{M/2-1}\cdot e^{-t_i/2\sigma_i^2}}{\sigma_i^M\cdot 2^{M/2}\cdot\Gamma(M/2)}. \tag{26}$$

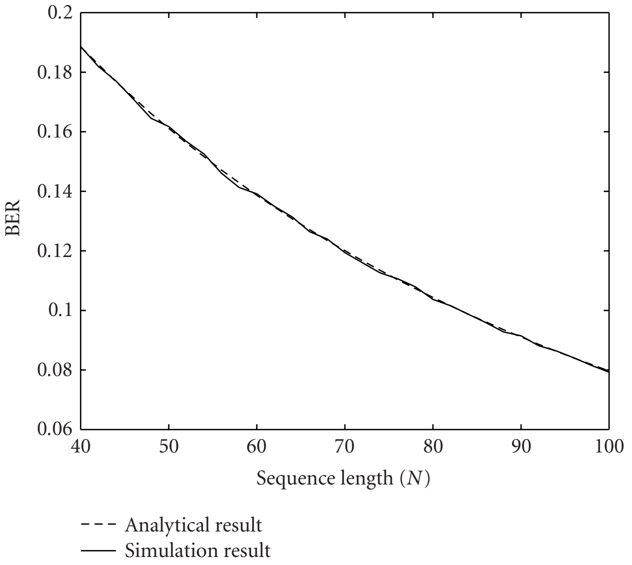


FIGURE 3: Performance comparison in the linear modulation.

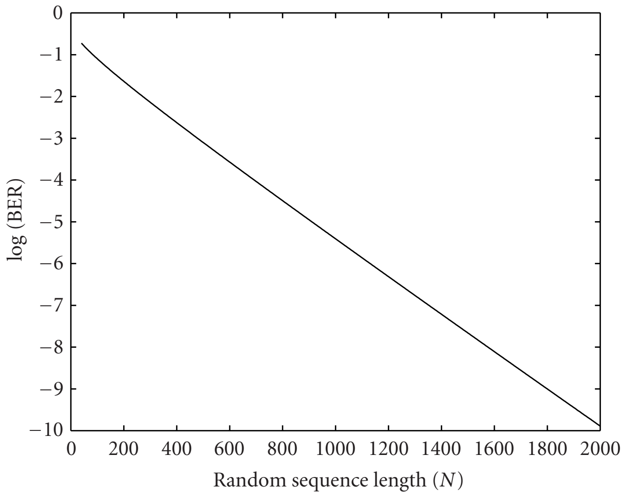


FIGURE 4: Analytical result in the linear modulation.

With two defined variables $A_i = 1/\sigma_i^M \cdot 2^{M/2} \cdot \Gamma(M/2)$ and $C_i = 1/2\sigma_i^2$, (26) can be rewritten as

$$f(t_i) = A_i \cdot t_i^{n-1} e^{-C_i t_i}, \tag{27}$$

where $n = M/2 = N/4$.

Suppose that the bit value 1 is embedded; detection probability BER turns out to be

$$\begin{aligned} \text{BER} = P(t_1 < t_0) &= \int_0^{+\infty} f(t_0)\,dt_0 \cdot \int_0^{t_0} f(t_1)\,dt_1 \\ &= \int_0^{+\infty} f_0(t_0) \int_0^{t_0} A_1 t_1^{n-1} e^{-C_1 t_1}\,dt_1\,dt_0. \end{aligned} \tag{28}$$

For an integer n, using the formula

$$\begin{aligned} \int x^n e^{-ax} dx = -\frac{e^{-ax}}{a^{n+1}} \cdot \big[&(ax)^n + n(ax)^{n-1} \\ &+ n(n-1)(ax)^{n-2} + \cdots + n!\big], \end{aligned}$$
$$\int_0^{+\infty} s^n e^{-as} ds = \frac{n!}{a^{n+1}}, \tag{29}$$

after some algebraic steps, the final result is

$$\begin{aligned} \text{BER} = &\left[\left(1 + \frac{C_0}{C_1}\right)(2n-2)! + \sum_{i=2}^{n} \frac{(n-1)!}{(n-i)!}\left(1 + \frac{C_0}{C_1}\right)^i\right] \\ &\cdot \frac{-A_0 A_1}{C_0 + C_1^{2n}} + \frac{A_0 A_1 \left[(n-1)!\right]^2}{(C_0 C_1)^n}. \end{aligned} \tag{30}$$

Figure 3 illustrates the BER curves obtained from (30) and the simulation results. In our simulations, the cover signal vector is of N components that are i.i.d. with zero mean and variance $\sigma^2 = 50^2$. One single information bit is embedded via (3) and thereafter extracted using (24). Again, the distortion threshold ratio is chosen as $\alpha = 0.1$. The embedding and detection operations are repeated for different sequence lengths.

This scheme boasts a simple ML detector and its performance matches the optimum detection in the previous scheme (1). Bear in mind that the latter has only theoretical values but limited meanings in practice. Compared with the feasible suboptimal detector (20), the improvement in the former is substantial. Furthermore, the neat and compact BER result allows us to predict performance with high accuracy for a specific hiding parameter set.

In spite of all the optimizations, the DS schemes are still unsuitable for oblivious data hiding. Figure 4 depicts the achievable performance at different sequence lengths with the distortion ratio fixed at $\alpha = 0.1$. To embed one single bit into a 1000-coefficient sequence, the BER upper limit is $\text{BER} = 3.91 \cdot 10^{-6}$. To achieve BER performance up to $\text{BER} \le 10^{-9}$, the sequence length must be $N > 1800$. It is the theoretical limit for the DS approaches (1) and (3). The poor performance is explained by the inherent limitations of the DS schemes.

It should be stressed that the Gaussian distributed original coefficients are assumed in the above analysis. In practice, c_i is usually a coefficient in some transform domain. The PDF of c_i is often modeled as a generalized Gaussian or Laplacian distribution [10]. In such cases, the ML detectors are no longer optimal. Nevertheless, with embedding scheme (1), the suboptimal detector (20) still outperforms (3).

Figure 5 displays simulation results for Laplacian distributed coefficients using embedding algorithm (1). The original coefficients are Laplacian distributed with zero mean and variance $\sigma^2 = 50^2$. The various detector performances in (3), (20), and (18) (not optimal) are compared. The JND threshold ratio α is chosen as $\alpha = 0.1$. The Laplacian simulation result is very close to that obtained in the Gaussian coefficient scenarios. Our further studies establish that the

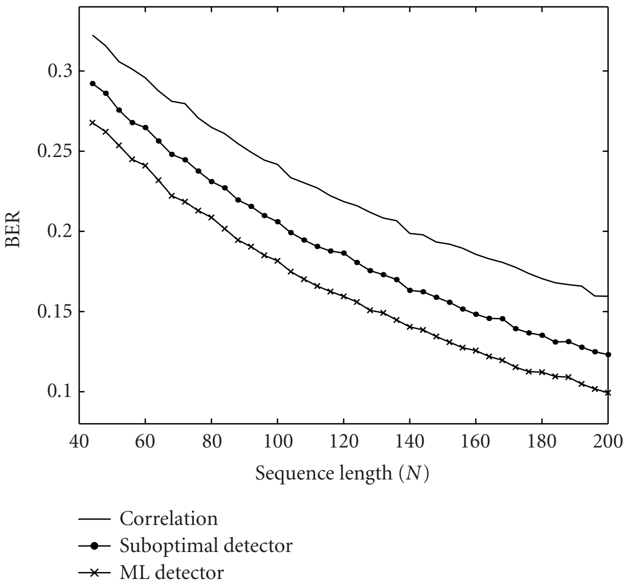


Figure 5: Performance with Laplacian distributed data.

linear data hiding scheme (3) exceeds the DS embedding (1). It should be noted that the channel noise is neglected in the above discussions. Even if it is taken into consideration, further simulations and studies show that the proposed linear embedding still beats the DS embedding approach and correlation-like detection.

4. HYPOTHESIS TESTING AND SET PARTITIONING

The shortcoming of the DS schemes lies in its inefficiency in the cover noise suppression. The hidden signal energy is much lower than that of the original cover signal which acts as noises. The inferior performance stems from the very low signal-to-noise ratio (SNR).

Hidden data detection in essence is a hypothesis testing problem. Suppose c is an original coefficient in which one bit information is embedded, x denotes the resulting coefficient after embedding, and r refers to the received coefficient. The two hypotheses are

$$\begin{aligned} &\text{H0:} \quad \text{bit value 0 is embedded in } r, \\ &\text{H1:} \quad \text{bit value 1 is embedded in } r. \end{aligned} \tag{31}$$

Obviously, H0 and H1 have different statistical properties. Otherwise, it is not possible to achieve reliable detection. A good hiding algorithm should modify the statistical properties of the original signal without perceptual degradation.

In a noise-free scenario where $r = x$, how can the decoder make a reliable decision H1 or H0 on a given r? The answer is simple and straightforward—just to make H0 and H1 have *no* element in common. Since the conditional probability $P(\text{H0}|x) = 0$ or $P(\text{H1}|x) = 0$, a correct decision is always expected.

In order to increase the robustness in a noisy environment, we can simply keep the elements in H0 and H1 some distance apart. This simple data hiding idea thus leads to *set partitioning* scheme. Two separate sets are constructed on the real axis (Figure 6). The coefficient after embedding should be kept in a set according to the bit value to be hidden. To embed a bit value 1, the coefficient x should be kept in Set 1. If the value of the original coefficient c is already in Set 1, no modification is needed. Otherwise, it is replaced by the nearest element in Set 1 to minimize distortion. Similarly, the value of x is kept in Set 0 to embed a bit value 0.

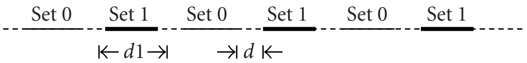


Figure 6: Set partitioning scheme.

To embed one bit information in a coefficient sequence $\mathbf{c}$, the simplest solution is to define a pattern to represent bit values. In our example, one bit is embedded in a 5-coefficient sequence. Two sequence patterns, similar to the antipodal signaling, are defined as follows:

$$\begin{aligned} \text{Pattern A (bit 1):} &\quad [\text{Set 1, Set 0, Set 1, Set 0, Set 1}] \\ \text{Pattern } -\text{A (bit 0):} &\quad [\text{Set 0, Set 1, Set 0, Set 1, Set 0}]. \end{aligned} \tag{32}$$

The modified sequence $\mathbf{x}$ should comply with Pattern A to hide the bit value 1, or Pattern $-$A to hide the value 0. For instance, the resulting sequence should be $x_0 \in$ Set 1, $x_1 \in$ Set 0, $x_2 \in$ Set 1, $x_3 \in$ Set 0, and $x_4 \in$ Set 1 in order to embed the value 1.

To further measure the hiding performance, the distortion injected in the scheme is evaluated as follows. In many transform domains, c is assumed to be Laplacian distributed or generalized Gaussian distributed. For simplicity, here we make approximations and assume c is uniformly distributed in the limited range $(-a, a)$, where a is some big value. This assumption is reasonable because analytical and simulation results for uniform distributed data are quite close to those obtained with Laplacian distributed data. This assumption is a good compromise between accuracy and ease of analytical work. The hiding distortion can be easily proved independent of the specific value of a.

Denote the error introduced in embedding as $e = x - c$, in the case where a bit value 1 is embedded, and consider the typical region AD as depicted in Figure 7.

If c is in the range AB, no modification is needed, thus $e = 0$. If c is in the range BD, e is uniformly distributed in the range $(-d - d1/2, d + d1/2)$. The conditional probability can be expressed as

$$\begin{aligned} P(c \in AB | c \in AD) &= \frac{d1}{2d1 + 2d}, \\ P(c \in BD | c \in AD) &= \frac{2d + d1}{2d1 + 2d}. \end{aligned} \tag{33}$$

The average distortion follows immediately,

$$D = \frac{(2d + d1)}{(2d1 + 2d)} \cdot \frac{(2d + d1)^2}{12} = \frac{1}{12} \frac{(2d + d1)^3}{(2d + 2d1)}. \tag{34}$$

Needless to say, this result also holds if the bit value 0 is embedded.

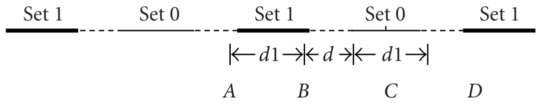


Figure 7: Average distortion calculation.

5. DETECTION IN SET PARTITIONING

5.1. Hard decision detection

In the N-coefficient sequence embedding, the simplest detector is the majority vote which is a hard decision decoder based on individual coefficients. In this approach, a real axis is divided into decision Regions 1 and 0 (Figure 8). If the received coefficient r_i falls in Region 1, it is decided that the transmitted signal x comes from Set 1. Otherwise, it is assumed to originate from Set 0. In the example mentioned in Section 4, if a received sequence pattern is {Set 0, Set 0, Set 1, Set 0, Set 0}, which is more similar to Pattern A (2-coefficient difference) than to Pattern −A (3-coefficient difference), the decision is made in favor of the bit value 1.

5.2. Maximum likelihood detection in Gaussian noise

The detection reliability can be enhanced using a soft decision detector. Provided the received coefficient r_i after the Gaussian channel transmission, the ML ratio is [11]

$$R = \frac{P(x_i \in \text{Set } 1 | r_i)}{P(x_i \in \text{Set } 0 | r_i)}. \tag{35}$$

The above equation can be written by introducing variables τ_i and ξ_i:

$$R = \frac{\sum_{\tau_i \in \text{Set } 1} P(\tau_i | r_i)}{\sum_{\xi_i \in \text{Set } 0} P(\xi_i | r_i)}, \tag{36}$$

where

$$\begin{aligned} P(\tau_i | r_i) &= \frac{P(\tau_i) f(r_i | \tau_i)}{f(r_i)}, \\ P(\xi_i | r_i) &= \frac{P(\xi_i) f(r_i | \xi_i)}{f(r_i)}. \end{aligned} \tag{37}$$

The ML ratio is expressed as

$$R = \frac{\sum_{\tau_i \in \text{Set } 1} P(\tau_i) f(r_i | \tau_i)}{\sum_{\xi_i \in \text{Set } 0} P(\xi_i) f(r_i | \xi_i)}, \tag{38}$$

where $f(r_i | \tau_i)$ is the Gaussian-noise conditional probability density,

$$f(r_i | \tau_i) = \frac{1}{\sqrt{2\pi}\sigma} \cdot \exp\left[\frac{-(r_i - \tau_i)^2}{2\sigma^2}\right]. \tag{39}$$

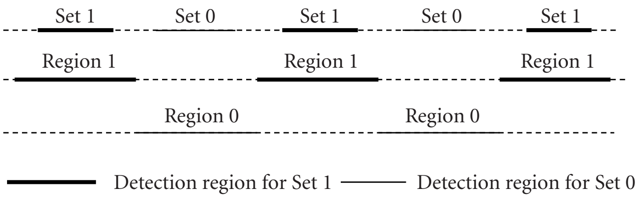


Figure 8: Hard decision region.

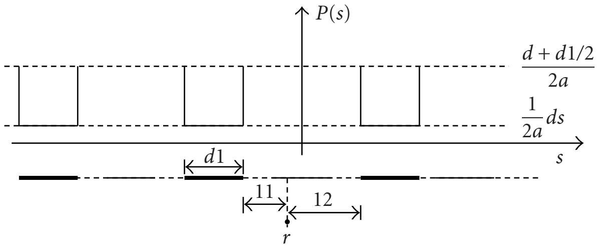


Figure 9: Calculation of ML ratio.

Under our previous assumption that the original coefficient c_i is uniformly distributed, the PDF $f(c_i) = (1/2a)$ $(-a \le c_i \le a)$. The probability of the transmitted signal $P(\tau_i)$ is depicted in Figure 9 after embedding the bit value 1. Note that the probability pulses appear at the endpoints. These signal points are transmitted with higher probability because any c_i out of Set 1 is replaced by these endpoints. The probability can be expressed as

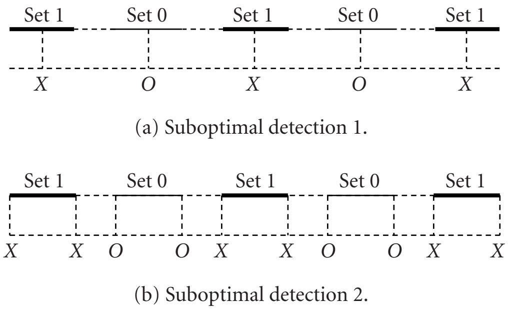
$$\begin{aligned} \sum_{\tau_i \in \text{Set } 1} & P(\tau_i) f(r_i | \tau_i) \\ &= \frac{1}{2a} \int_{r_i - l_1 - d1}^{r_i - l_1} \frac{1}{\sqrt{2\pi}\sigma} e^{-(\tau_i - r_i)^2 / 2\sigma^2} d\tau_i \\ &\quad + \frac{1}{\sqrt{2\pi}\sigma} \frac{d + d1/2}{2a} e^{-l_1^2 / 2\sigma^2} \\ &\quad + \frac{1}{2a} \int_{l_1 - 2d - 3d1}^{l_1 - 2d - 2d1} \frac{1}{\sqrt{2\pi}\sigma} e^{-(\tau_i - r_i)^2 / 2\sigma^2} d\tau_i + \cdots . \end{aligned} \tag{40}$$

In the same manner, $\sum_{\xi_i \in \text{Set } 0} P(\xi_i) f(r_i | \xi_i)$ can be calculated and a similar result is obtained. Nevertheless, this result does not lead to any closed-form result of ML ratio. Moreover, as the noise power σ^2 is usually unavailable at the decoder, this detector is infeasible in practice.

The challenge in detection is that the transmitted signal can assume any values in these two sets. The ML ratio calculation involves all elements in Set 1 and Set 0, thereby greatly increases the computational cost. In the following suboptimal methods, we assume that the transmitted signals are discrete instead of continuous.

5.3. Suboptimal detection 1

As a first approximation, it is simply assumed that the transmitted signals are at the centers of the continuous segments, and the signaling has a pattern like $XOXO$ as depicted in Figure 10. Signal points X and O have equal a priori probabilities.



(a) Suboptimal detection 1.

(b) Suboptimal detection 2.

FIGURE 10: Suboptimal detection in set partitioning.

The ML ratio thus follows as in (35).

This result greatly simplifies the ML ratio calculation, but it still involves infinite X and O points. Our simulation studies show that we can further simplify it by merely considering the nearest X and O points. Thus (35) reduces to

$$R = \frac{P(r_i | x_i = u_i)}{P(r_i | x_i = v_i)}, \tag{41}$$

where u_i/v_i is the nearest points X/O in Set 1 and Set 0.

5.4. *Suboptimal detection 2*

In Figure 9, it is observed that the endpoints are transmitted with much higher probabilities. Another reasonable approximation assumes that the transmitted signals have $XXOO$ pattern (Figure 10b).

Given a received signal coefficient r_i, only the nearest endpoints in those two sets are considered. Therefore, two signal candidates u_i and v_i are identified. This yields the same ML ratio as in (41). The only difference is the selection of possible transmitted signal candidates.

In the case where one single bit is embedded in an N-coefficient sequence, a sequence detector can be employed. In the aforementioned example in Section 4, given a received 5-coefficient sequence $\mathbf{r}$, we denote the nearest X and O points to r_i as u_i (in Set 1) and v_i (in Set 0), respectively. Complying with the predefined pattern in Section 4, two sequence candidates are constructed as follows:

$$\begin{aligned} \text{Pattern A type:} \quad \mathbf{a} &= [u_0, v_1, u_2, v_3, u_4], \\ \text{Pattern } -\text{A type:} \quad \mathbf{b} &= [v_0, u_1, v_2, u_3, v_4]. \end{aligned} \tag{42}$$

If $\|\mathbf{r} - \mathbf{a}\| < \|\mathbf{r} - \mathbf{b}\|$, the received sequence is more "similar" to Pattern A, leading to decoding the bit value 1. Otherwise, a bit value 0 is decided.

6. RESULTS OF SET PARTITIONING

6.1. *Performance analysis*

Data hiding is the game played between distortion and robustness and there is a tradeoff between these two factors. The more the distortion introduced is, the more reliable it could be. To evaluate the performance of set partitioning scheme, detection of BER is measured for various SNRs in a Gaussian noise environment. As the data hiding signal energy is equivalent to distortion injected, the DNR is used instead of SNR in the following discussions. The DNR is defined as the ratio of distortion energy D to the noise variance σ^2, that is, DNR $= D/\sigma^2$. It should be noted that the distortion energy D is less than the noise energy in most practical cases.

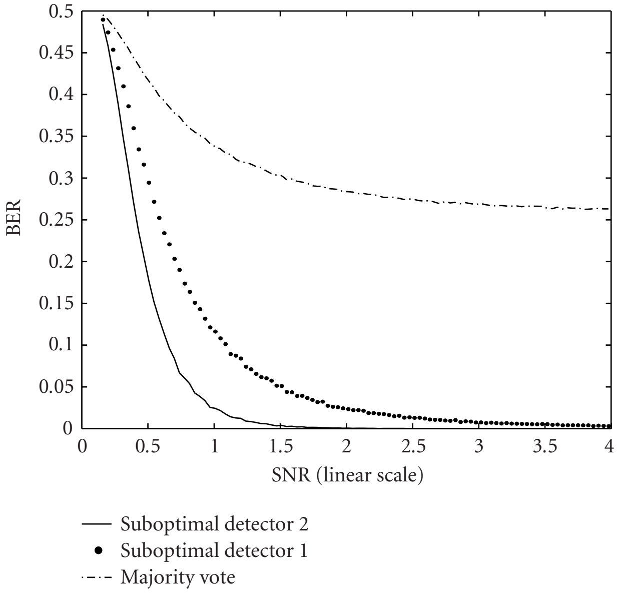


FIGURE 11: Detection performance comparison (1 bit embedded in an 11-coefficient sequence).

Our simulation studies use the following Monte Carlo procedure. A generated random sequence $\mathbf{c}$ is composed of N i.i.d. random variables with zero mean and variance $\sigma^2 = 50^2$. The above set partitioning embedding algorithm is applied to the sequence to hide the bit value 1 or 0. Subsequently, a noise vector $\mathbf{n}$ with N zero-mean Gaussian random variables is added to $\mathbf{c}$, which simulates the effect of the additive Gaussian channel transmission. Given the received signal sequence, the information bit is extracted using the aforementioned detectors. To validate our algorithms, the simulation procedure is repeated for different values of sequence length N, signaling parameters d, $d1$, and Gaussian channel noise variance.

Figure 11 depicts the simulation result for the suboptimal detectors and majority vote detector. One information bit is embedded into an 11-coefficient sequence. The signaling ratio is chosen as $d/d1 = 1$. It is evident that both suboptimal methods far outperform the hard decision decoder. Moreover, the result shows that suboptimal decoder Method-2 offers remarkable performance improvements over Method-1. Further simulations and analysis studies reveal that the performance in Method-2 is in good agreement with the optimum ML numerical integral result obtained from (36).

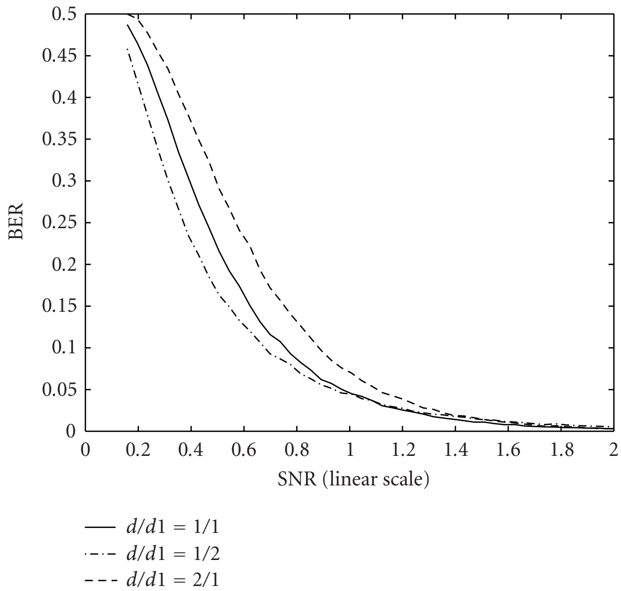


Figure 12: BER-DNR at different $d/d1$ (1 bit embedded in an 8-coefficient sequence).

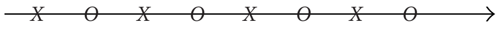


Figure 13: QIM embedding.

It is established that the BER-DNR is only related to the ratio of $d/d1$, not the individual values of d and $d1$. Figure 12 displays the performance in one 1 bit/8-coefficient sequence embedding. It is apparent that the $d/d1$ performs better at lower DNR. However, larger $d/d1$ is more advantageous at higher DNR because in practice, data hiding distortion is not expected to be more than moderate or severe compression distortion. Consequently, data hiding always works at lower DNR, usually DNR < 1. Hence smaller $d/d1$ is advisable in the real world.

6.2. Comparison with existing schemes

An existing oblivious data hiding scheme, quantization index modulation (QIM) [12, 13], is a special case of the set partitioning scheme where the value of $d1$ is selected as $d1 = 0$. In the QIM scheme, the embedding output coefficient X is discrete instead of continuous (Figure 13). In contrast, the set partitioning scheme provides us with the flexibility to choose different values of d and $d1$. In most applications where DNR is low, we will see that the signaling with $d/d1 = \infty$ (QIM) is not well suited.

In Figure 14, one single bit is embedded into a 4-coefficient sequence. Several $d/d1$ ratio selections demonstrate substantial improvements over the QIM scheme. The performance gain is remarkable at lower DNR. At the higher DNR, the QIM scheme performs only slightly better than the signaling scheme $d/d1 = 1$, as shown in Figure 15. The proposed set partitioning method offers the designer an improvement over the QIM technique by choosing an appropriate signaling ratio $d/d1$. The reason to select smaller values of $d/d1$ ratio in data hiding is twofold; first, data hiding operates at lower DNR in practice; second, this selection guarantees a fair detection performance even at severe compressions or tampering attacks. In contrast, the QIM scheme does not survive noisy channels well.

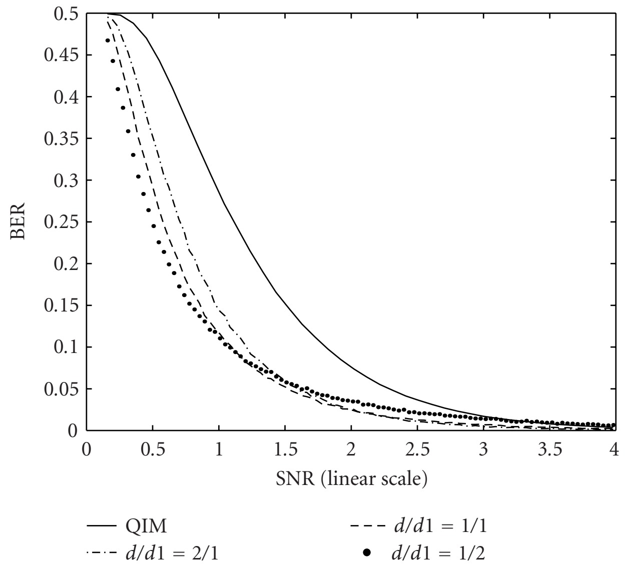


Figure 14: BER-DNR at lower DNR (1 bit embedded in a 4-coefficient sequence).

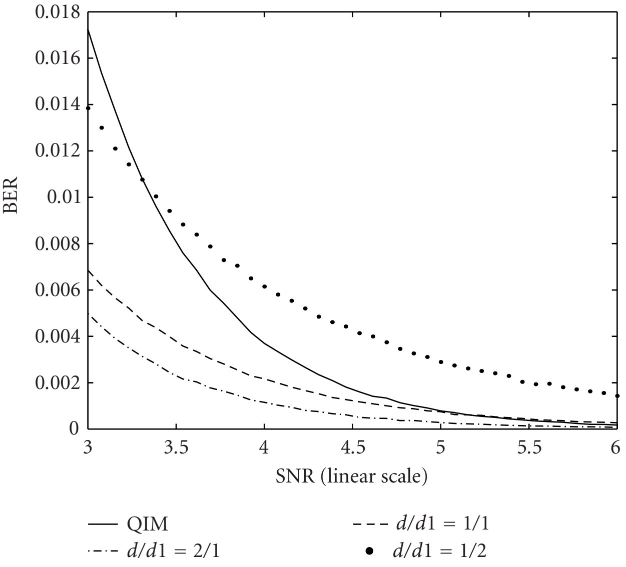


Figure 15: BER-DNR at higher DNR (1 bit embedded in a 4-coefficient sequence).

It should be remarked that given the same distortion energy, the maximum error e in $d/d1 = 1$ signaling is larger than that in the QIM scheme. However, even under the same

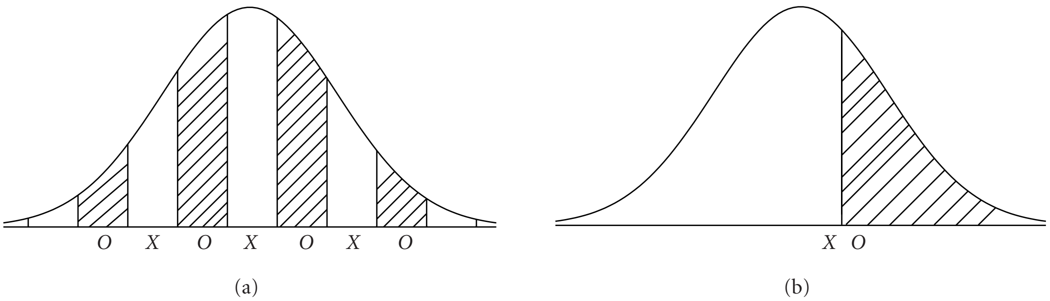


FIGURE 16: BER in (a) periodic signaling and (b) nonperiodic signaling.

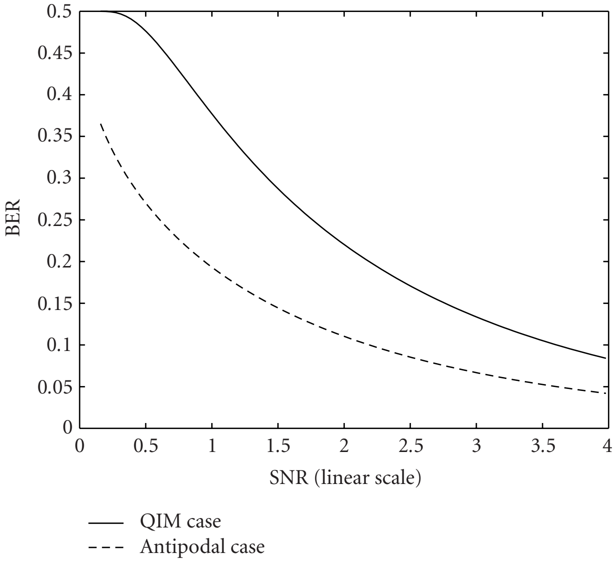


FIGURE 17: BER-SNR in QIM and antipodal cases.

maximum error constraint, which implies less distortion energy in $d/d1 = 1$ signaling, the proposed scheme still demonstrates significant improvements over the QIM scheme at lower DNR.

Bear in mind that the BER in QIM scheme is different from the BER in the antipodal signaling case. Chen and Wornell [12] point out that the BER in QIM could be calculated the same way as the binary antipodal signaling communication model. Derived from that, the performance in the antipodal case is BER $= Q(d/2\sigma)$, where $Q(\cdot)$ is the Gaussian-PDF tail integral [13]. Actually this conclusion is not quite accurate for most data hiding scenarios, especially considering that the data hiding often takes place at lower DNR in the real world. It is readily see that the BERs are the area of the shadowed regions in Figure 16,

$$\begin{aligned}\text{BER} &= \int_{-d}^{0} \frac{1}{\sqrt{2\pi}\sigma} e^{-(x+d/2)^2/2\sigma^2} dx \\ &\quad + \int_{d}^{2d} \frac{1}{\sqrt{2\pi}\sigma} e^{-(x+d/2)^2/2\sigma^2} dx + \cdots .\end{aligned} \tag{43}$$

The analytical BER curves in QIM scheme and the antipodal signaling case are depicted in Figure 17. The gap between these two schemes is explained by the shadowed area difference in Figure 16. A more general and rigorous mathematical analysis on QIM data hiding was recently presented by Perez-Gonzalez [14]. Although the closed-form BER cannot be obtained, an accurate upper bound is produced in the work.

The proposed nonlinear scheme can be employed in place of the direct-sequence hiding presented in Sections 2 and 3. The algorithm can be employed in various data hiding domains. In our image data hiding experiments, information bits are embedded in the discrete Fourier transform (DFT) amplitude domain. A signaling pattern is embedded in the medium frequency coefficients. The results validate the proposed set partitioning scheme, and have demonstrated robustness to common compression and various filtering attacks.

The above set partitioning scheme is just a very simple nonlinear scheme. Its detection is mostly heuristic as seen from the above discussions. More accurate analysis is very difficult if not impossible at all. Our detectors are simplified versions from the ML detection analysis. The above results and conclusions are derived from our simulations and experiments. They may not be true in all scenarios. For example, the detection comparisons between Method-1 and Method-2 may not be true at all $d/d1$ ratios. Premature as they are, the algorithms give good results in practice. Rigorous analysis is under further investigation. More accurate artifacts control and higher hiding capacity are also our next research topics.

7. CONCLUSIONS

In this paper, the DS modulation schemes in oblivious data hiding are investigated. Both analytical and simulation studies demonstrate that the correlation-like detection widely used in practice is not optimal. The ML and suboptimal detectors are analyzed, and the performance gain due to the latter is demonstrated. The results show that the inferior performance in the linear schemes is due to the cover noise interference. This limits their employment in oblivious applications. To facilitate hypothesis testing, a nonlinear set partitioning scheme is proposed. Its distortion calculation, detection and performance analysis, and comparison with the existing algorithms are further discussed. Both simulation studies and theoretical analysis demonstrate improvements over current data hiding algorithms.

ACKNOWLEDGMENT

The authors would like to thank Dr. Y. Tang for his editorial contributions.

REFERENCES

[1] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals," in *Proc. 3rd IEEE International Conference on Multimedia Computing and Systems*, pp. 473–480, Hiroshima, Japan, June 1996.

[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *Proc. Workshop on Information Hiding*, pp. 185–206, Cambridge, UK, May 1996.

[3] F. Hartung, P. Eisert, and B. Girod, "Digital watermarking of MPEG-4 facial animation parameters," *Computers and Graphics*, vol. 22, no. 4, pp. 425–435, 1998.

[4] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol. 66, no. 3, pp. 283–301, 1998.

[5] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 540–550, 1998.

[6] M. Ikeda, K. Takeda, and F. Itakura, "Audio data hiding by use of band-limited random sequences," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing (ICASSP '99)*, vol. 4, pp. 2315–2318, Phoenix, Ariz, USA, March 1999.

[7] I. Cox and M. L. Miller, "Review of watermarking and the importance of perceptual modeling," in *Human Vision and Electronic Imaging II*, vol. 3016 of *Proceedings of SPIE*, pp. 92–99, Bellingham, Wash, USA, February 1997.

[8] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, 1998.

[9] A. Leon-Garcia, *Probability and Random Processes for Electrical Engineering*, Addison-Wesley Publishing Company, Reading, Mass, USA, 1994.

[10] M. Barni, F. Bartolini, A. Piva, and F. Rigacci, "Statistical modelling of full frame DCT coefficients," in *Proc. 9th European Signal Processing Conference (EUSIPCO '98)*, vol. 3, pp. 1513–1516, Island of Rhodes, Greece, September 1998.

[11] S. M. Kay, *Fundamentals of Statistical Signal Processing. Vol. 2: Detection Theory*, Prentice Hall PTR, Englewood Cliffs, NJ, USA, 1998.

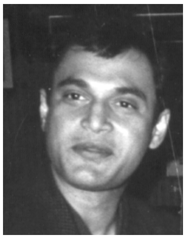
[12] B. Chen and G. W. Wornell, "Digital watermarking and information embedding using dither modulation," in *Proc. 2nd IEEE Workshop on Multimedia Signal Processing*, pp. 273–278, Redondo Beach, Calif, USA, December 1998.

[13] B. Chen and G. W. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," in *Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 342–353, San Jose, Calif, USA, January 1999.

[14] F. Perez-Gonzalez, F. Balado, and J. R. H. Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 960–980, 2003.

Litao Gang received the B.S. and M.S. degrees in electrical engineering from Beijing Institute of Technology, China, and the Ph.D. degree from New Jersey Institute of Technology, Newark, New Jersey, in 2001. He is currently a software engineer in InfoDesk Inc, Tarrytown, New York, USA. His research interests include multimedia signal processing, multimedia copyright protection management, watermarking and data hiding, and software/hardware implementations of multimedia algorithms.

Ali N. Akansu received the B.S. degree from the Technical University of Istanbul in 1980, and the M.S. and Ph.D. degrees from the Polytechnic University in 1983 and 1987, respectively, all in electrical engineering. Since 1987, he has been with the New Jersey Institute of Technology, where he is a Professor of electrical and computer engineering. He was the Founding Director of the New Jersey Center for Multimedia Research (NJCMR) between 1996 and 2000, and NSF Industry-University Cooperative Research Center for Digital Video between 1998 and 2000. Dr. Akansu was the vice president of R&D of IDT Corporation (NYSE: IDT) between June 2000 and September 2001. He was also the Founding President and CEO of PixWave (IDT subsidiary). He was an Academic Visitor at IBM T. J. Watson Research Center and at GEC-Marconi Electronic Systems Corp. during the summers of 1989 and 1996, and 1992, respectively. He has been a Consultant of the industry and he sits on the boards of several companies. His current research interests include signal theory, linear transforms and algorithms, signal processing for digital communications, Internet multimedia including security aspects, and genes & signals. Dr. Akansu has published more than 200 refereed conference and journal articles and four books.



Mahalingam Ramkumar received his B.S. degree from the University of Madras, India, 1987, M.S. degree from Indian Institute of Science, Bangalore, India, 1997, and Ph.D. degree from New Jersey Institute of Technology, Newark, NJ, (all degrees in electrical engineering). Since August 2003, he has been an Assistant Professor with the Department of Computer Science and Engineering, Mississippi State University. Between September 2002 and August 2003 he was a Research Professor with the Department of Computer and Information Science, Polytechnic University, Brooklyn, NY. He was the CTO of PixWave Inc., Newark, NJ, between March 2000 and August 2002. His research interests include sensor/ad hoc networks, cryptography, data hiding, and data compression.