FFT BASED SIGNALING FOR MULTIMEDIA STEGANOGRAPHY

Mahalingam Ramkumar and Ali N. Akansu

Department of Electrical and Computer Engineering
New Jersey Institute of Technology
New Jersey Center for Multimedia Research
University Heights, Newark, NJ, 07102.

ABSTRACT

This paper addresses good choices for the signaling method for multimedia steganography, or data hiding. A novel FFT based signaling method, with many properties that make it especially suitable for steganographic applications is proposed. Use of FFT permits large codebook sizes, without drastically increasing the computational complexity.

1. INTRODUCTION

Data hiding or *steganography* is the art of hiding a *message signal* in a *host signal*, without any *perceptual distortion* of the host signal. For purposes of illustration, we shall assume that the host signal is a vector $\mathbf{c} \in \Re^N$. The process of data hiding consists of an embedder E, and a detector D. If $\mathbf{b}$ is a sequence of bits to be embedded in the vector $\mathbf{c}$, the *stego* content $\hat{\mathbf{c}}$ (the *modified* content with the embedded data) is obtained as $\hat{\mathbf{c}} = E(\mathbf{c}, \mathbf{b}, \mathcal{K})$, where $\mathcal{K}$ is a *key*. We expect $\hat{\mathbf{c}}$ to undergo some modification (like lossy compression) before it reaches the receiver (detector D), where the hidden bit sequence is extracted. Let $\tilde{\mathbf{c}} = \hat{\mathbf{c}} + \nu$ be the received content. Data hiding can be broadly classified into two categories depending on whether the original content is needed for extraction of the hidden bits. *Escrow* methods need the original content for extracting the hidden bits. On the other hand, *oblivious* detection methods extract the hidden bits without any knowledge of the original content $\mathbf{c}$;

$$\tilde{\mathbf{b}} = \begin{cases} D(\tilde{\mathbf{c}}, \mathcal{K}, \mathbf{c}) & \text{escrow} \\ D(\tilde{\mathbf{c}}, \mathcal{K}) & \text{oblivious} \end{cases} \tag{1}$$

In most data hiding methods, the bit sequence to be embedded, *viz.* $\mathbf{b}$, is converted to a form *suitable for embedding* in $\mathbf{c}$. Let $\mathbf{s} = \mathcal{S}(\mathbf{b}) \in \Re^N$. $\mathbf{s}$ is referred to as the *signature* sequence. The complete data hiding and detection scheme can therefore be described by

$$\hat{\mathbf{c}} = \mathcal{E}(\mathbf{c}, \mathbf{s}) \quad \tilde{\mathbf{c}} = \hat{\mathbf{c}} + \nu \quad \tilde{\mathbf{s}} = \mathcal{D}(\tilde{\mathbf{c}}) \quad \tilde{\mathbf{b}} = \mathcal{S}^{-1}(\tilde{\mathbf{s}}). \tag{2}$$

From a signal processing perspective, data hiding methods can be classified into two categories, depending on the type of embedding and detecting operators. In the first category [1, 2] lies methods where $\mathcal{E}$ adds the signature sequence *linearly* to $\mathbf{c}$, and $\mathcal{D}$ detects $\tilde{\mathbf{s}}$ from $\tilde{\mathbf{c}}$ by *correlative processing.* For such linear (or Type I) methods, if the original is not available at the receiver, then $\mathbf{c}$ is noise, for the purpose of detection of the hidden bit sequence $\mathbf{b}$. In the second category $\mathcal{E}$ and $\mathcal{D}$ are *non-linear.* One of the important characteristics of the non-linear methods is their ability to suppress the noise due to $\mathbf{c}$ (or self-noise), even though the $\mathbf{c}$ is not available at the receiver.

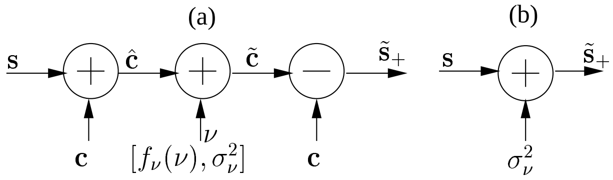

Figure 1: (a) Linear Cover Image Escrow Data Hiding. (b) Equivalent Additive Noise Channel.

In Section 2 we provide a communication theory perspective of data hiding. In Section 3 we briefly describe good choices for the operators $\mathcal{E}$ and $\mathcal{D}$ (see Ref. [3] for details). In Section 4 we investigate options for the operators $\mathcal{S}$ and $\mathcal{S}^{-1}$, which is the signaling scheme employed for data hiding. In Section 5 we propose a FFT-based scheme for this purpose. Section 6 addresses choices for redundant signaling for error correction. Conclusions are presented in Section 7.

2. COMMUNICATION THEORY PERSPECTIVE

Consider the power constrained communication scheme

$$\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{w} + \nu, \tag{3}$$

where $\mathbf{c}, \mathbf{w}, \nu \in \Re^N$, and $c(i) \sim \mathcal{N}[0, \sigma^2], w(i) \sim \mathcal{N}[0, \gamma^2]$ and $\nu(i) \sim \mathcal{N}[0, \sigma_\nu^2]$ $\forall$ i are i.i.d. Further $\mathbf{c}, \mathbf{w}, \nu$ are independent. In the above model $\mathbf{w}$ is power constrained (variance γ^2), $\hat{\mathbf{c}} = \mathbf{c} + \mathbf{w}$ is the transmitted signal, ν is the noise in the channel, and $\tilde{\mathbf{c}}$ is the received signal.

Figure 1 (a) is an illustration of escrow data hiding, which may be considered as a communication scheme similar to Eq. (3), where $\mathbf{w}$ in Eq. (3) is the same as $\mathbf{s}$ in Figure 1, and $\mathbf{c}$ is *available at the receiver.* Figure 1 (b) is the equivalent channel for this communication scheme, and it can be easily seen that one could theoretically achieve a capacity of $C_0 = \frac{1}{2}\log_2\left(1 + \frac{\gamma^2}{\sigma_\nu^2}\right)$ bits per coefficient [4].

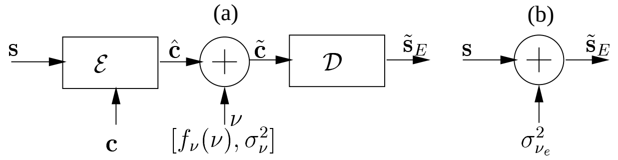

Figure 2: (b) Non-linear Oblivious Detection Data Hiding (d) Equivalent Additive Noise Channel.

Figure 2 is an illustration of oblivious data hiding, where the receiver *does not have access* to $\mathbf{c}$. In this case, in general, $\mathbf{s} \neq \mathbf{w} = \hat{\mathbf{c}} - \mathbf{c}$. For this case, we would expect the *equivalent* additive noise of variance $\sigma^2_{\nu_e}$ in Figure 2 (b) is higher than σ^2_{ν}. This would imply that one could achieve a capacity of $C_1 = \frac{1}{2}\log_2\left(1 + \frac{\gamma^2}{\sigma^2_{\nu_e}}\right)$ for oblivious data hiding.

Costa [5], however, argued that one could achieve capacity C_0 *even if* $\mathbf{c}$ *is not available at the decoder.* Unfortunately, this would require the use of codebooks of size $2^{N(C_0+L)}$ where $L = \frac{1}{2}\log_2\left(1 + \frac{\gamma^2(\gamma^2+\sigma^2+\sigma^2_\nu)}{\sigma^2_\nu(\sigma^2_\nu+\gamma^2)}\right)$. To get a clearer picture of the complexity involved, let us consider a specific case of data hiding in 256×256 images. Some reasonable choices of $N = 8192$ (8192 transform coefficients used for data embedding), $\sigma^2 = 12000$ (variance of the low frequency coefficients used for data hiding), $\gamma^2 = 32$ (distortion of the host signal), and $\sigma^2_\nu = 320$ imply $L \approx 40C_0$.

However, by splitting the signaling mechanism into two parts, $(\mathcal{E}, \mathcal{D})$ and $(\mathcal{S}, \mathcal{S}^{-1})$, the maximum size of the codebook need only be 2^{NC_1}, or 2^{40} times less than that of methods which can achieve capacity C_0. The penalty paid for the drastic reduction in complexity is that $C_1 < C_0$ (or $\sigma_{\nu_e} > \sigma_\nu$). In [6] it was shown that such practical methods, (employing codebook sizes less than 2^{NC_1}, can achieve $\sigma_{\nu_e} < 3\sigma_\nu$.

3. FLOATING SIGNAL CONSTELLATIONS

The non-ideal, but practical solution proposed in [3], viewed the signaling mechanism as employing a *floating signal constellation.* The constellation, with finite support, is defined by $(\mathcal{S}, \mathcal{S}^{-1})$. The job of $(\mathcal{E}, \mathcal{D})$ is to *estimate the origin* of the constellation. Periodic functions were utilized for $(\mathcal{E}, \mathcal{D})$ to *tile* the space of $\mathbf{c}$, with the constellation defined by $\mathcal{S}$.

The operators $\mathcal{E}, \mathcal{D}$ are characterized by two parameters Δ and β. The algorithm for embedding the sequence $\mathbf{s}$ in $\mathbf{c}$ is given by

$$\begin{aligned}
\mathbf{p} &= \mathcal{D}(\mathbf{c}) \qquad (4)\\
e(k) &= s(k) - p(k)\\
e(k) &= (|e(k)| > \frac{\beta}{2}) \;\; ? \;\; \mathrm{sign}(e(k))\frac{\beta}{2} \;\; : \;\; e(k)\\
e(k) &= (\mathrm{rem}\left(\frac{c(k)}{\Delta}\right) > \frac{\Delta}{2}) \;\; ? \;\; -e(k) \;\; : \;\; e(k)\\
\hat{c}(k) &= (c(k) \geq 0) \;\; ? \;\; c(k) + e(k) \;\; : \;\; c(k) - e(k)
\end{aligned}$$

where $\mathcal{D}$ is given by

$$\begin{aligned}
q(k) &= \mathrm{rem}(\frac{|\tilde{c}(k)|}{\Delta}), \quad k = 1 \cdots N\\
\tilde{s}(k) &= (q(k) \geq \frac{\Delta}{2}) \;\; ? \;\; (\frac{3\Delta}{4} - q(k)) \; : \; (q(k) - \frac{\Delta}{4})
\end{aligned}$$

The optimal choice of Δ and β for a given permitted distortion γ^2, and channel noise ν, is obtained by maximizing the expected value of the normalized correlation given by

$$\rho = \frac{2\sum_{i=0}^{\infty}\int_{\frac{i\Delta}{2}}^{\frac{(i+1)\Delta}{2}}(-1)^i(\frac{(2i+1)\Delta}{4} - z)f_Z(z)\mathrm{d}z}{\sqrt{2\sum_{i=0}^{\infty}\int_{\frac{i\Delta}{2}}^{\frac{(i+1)\Delta}{2}}(\frac{(2i+1)\Delta}{4} - z)^2 f_Z(z)\mathrm{d}z}} \qquad (5)$$

subject to the condition $\gamma^2 = \frac{\beta^2}{12\Delta}(3\Delta - 2\beta)$, and

$$\begin{aligned}
f_Z(z) &= \frac{\beta}{\Delta\sqrt{2\pi\sigma^2_\nu}}\mathrm{e}^{\frac{-z^2}{2\sigma^2_\nu}}\\
&+ \frac{1}{2\Delta}\left\{\mathrm{erf}\left(\frac{z + \frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_\nu}\right) - \mathrm{erf}\left(\frac{z - \frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_\nu}\right)\right\}
\end{aligned}$$

where erf(.) denotes the *Gaussian error function*, $\mathrm{erf}(t) = \frac{2}{\pi}\int_0^t \mathrm{e}^{\frac{-y^2}{2}}\mathrm{dy}$.

4. CONVENTIONAL SIGNALING

The conventional signaling part, viz. the pair $(\mathcal{S}, \mathcal{S}^{-1})$, addresses the problem of mapping a K length bit sequence $\mathbf{b}$ to a possibly real valued sequence $\mathbf{s}$ of length N, where $N >> K$. As a simple approach we have

$$\mathbf{s} = [\mathbf{s}_1\, \mathbf{s}_2 \cdots \mathbf{s}_K], \qquad (6)$$

where $\mathbf{s}_i = \mathrm{sign}(b(i))\theta, i = 1 \cdots K$, and θ is random vector (obtained from a random seed or the private key $\mathcal{K}$), of length $\frac{N}{K}$. On the other hand, we could generate 2^K sequences $\mathbf{s}_i, i = 1 \cdots 2^K$ of length N, such that the sequences $\mathbf{s}_k$ are *maximally separable.* Geometrically, the sequences $\mathbf{s}_k$ can be represented by a set of 2^K points in a N-dimensional hyper-sphere. In other words, the minimum distance between any two of the 2^K points should be as high as possible, under the given constraint of the hyper-sphere radius. The binary sequence $[b_1\, b_2 \cdots b_K]$ can be interpreted as a decimal number between 0 and $2^K - 1$. To transmit a particular sequence of bits, whose decimal equivalent is say d, we choose $\mathbf{s} = \mathbf{s}_d$. Detection of the hidden bit sequence, or equivalently the number d can be accomplished as $\tilde{d} = \arg\max_{i=0\cdots 2^K-1}\langle\tilde{\mathbf{s}}, \mathbf{s}_i\rangle$.

While it is assured that the latter scheme, will approach the *channel capacity* closer than the former, in practice, implementation of the second scheme may be prohibitively expensive, especially for large K and/or N. A reasonable compromise might be to choose an alphabet size (or codebook size) between 2 of the former (bit-by-bit signaling) technique, and 2^K of the latter. For example, if the alphabet size is chosen as $2^{\frac{K}{k}}$, then a single member of the alphabet is detected from each of the k sequences of length $\frac{N}{k}$.

An FFT-based signaling method proposed in the next section offers an efficient way to increase the alphabet size used for signaling, while keeping the computational complexity at manageable levels. Furthermore, the maximally separable signal constellation itself is generated from random seeds.

5. FFT BASED SIGNALING

In the FFT-based signaling technique, the maximally separable sequences are constrained to be orthogonal. Let $\mathbf{s}_k \in \Re^{L_k}, L_k = 2^{p_k - 1}$. Maximally separable signature sequences $\mathbf{s}_k^l, l = 1 \cdots 2^{p_k}$, corresponding to p_k bits, are obtained as L_k orthogonal sequences and their negatives. *Random signature spaces* are generated from a seed. This is achieved by constraining the signatures to be *cyclic all-pass sequences.*

5.1. Cyclic All-Pass Sequences

Let $\mathbf{h} \in \Re^N$ and $\mathbf{H} = \mathcal{F}(\mathbf{h})$ where, $\mathcal{F}(.)$ stands for the Discrete Fourier Transform (DFT). Further, let $\mathbf{h}$ be such that $\mid H(n) \mid = 1$ for $n = 0, 1, \cdots, N-1$. Hence $(\mathbf{H}.\mathbf{H}^*) = [1, 1, \cdots, 1]$, or $\mathcal{F}^{-1}(\mathbf{H}.\mathbf{H}^*) = [1, 0, 0, \cdots, 0]$. As $\mathcal{F}^{-1}(\mathbf{H}.\mathbf{H}^*)$ is the *circular autocorrelation* of the vector $\mathbf{h}$, it follows that all circular shifts of $\mathbf{h}$ are mutually orthogonal [7]. As the phases ϕ_n, $n = 0, 1, \ldots, N-1$ of the elements of $\mathbf{H}$ can be arbitrary, we have many degrees of freedom for the choice of vector $\mathbf{h}$ with mutually orthogonal circular shifts. For real $\mathbf{h}$ we have $\frac{N}{2} - 1$ phase values which can be arbitrarily chosen. Thus a pseudo-random all pass sequence of length N can be generated from a pseudo-random (uniformly distributed between π and $-\pi$) sequence of length $\frac{N}{2} - 1$. If

$$\begin{aligned} \phi_k &= \begin{cases} 0 \text{ or } \pi & k = 0, k = \frac{N}{2} \\ \theta_k & k = 0 \cdots \frac{N}{2} - 1 \\ -\theta_{N-k} & k = \frac{N}{2} + 1 \cdots N-1 \end{cases} \\ H(k) &= \cos(\phi_k) + \mathrm{i}\sin(\phi_k), k = 0 \cdots N-1, \end{aligned} \quad (7)$$

where $\theta_k, k = 1 \cdots \frac{N}{2} - 1$ are randomly distributed between π and $-\pi$, $\mathrm{i} = \sqrt{-1}$, then $\mathbf{h} = \mathcal{F}^{-1}(\mathbf{H})$, is a cyclic all-pass sequence.

Alternately, a pseudo-random binary sequence is generated from a seed. Then, the *unique* all-pass sequence "closest" (in the mean-square sense) to the binary sequence is obtained.

Let $\mathbf{f} = [f(0)\ f(1)\ \cdots\ f(N-1)]$ be a random binary sequence. We need to find the all-pass sequence that is closest to $\mathbf{f}$. In other words, we need to find the vector $\mathbf{h} = [h(0)\ h(1)\ \cdots h(N-1)]^T$ that minimizes the error ε defined as

$$\varepsilon = \sum_{n=0}^{N-1} \mid h(n) - f(n) \mid^2, \quad (8)$$

subject to the constraint that $\mathbf{h}$ is a cyclic all-pass sequence. Since the DFT of a (cyclic) all-pass sequence can be written as $\mathbf{H} = [e^{j\phi_0}\ e^{j\phi_1}\ \cdots\ e^{j\phi_{N-1}}]$, let

$$h(n) = \textstyle\sum_{k=0}^{N-1} e^{j(\frac{2\pi kn}{N} + \phi_k)} \quad f(n) = \sum_{k=0}^{N-1} a_k e^{j(\frac{2\pi kn}{N} + \theta_k)}$$

for $n = 0 \cdots N-1$. It can be easily shown that the error ε is given by

$$\varepsilon = N\Big[N - 2\sum_{k=0}^{N-1} a_k cos(\phi_k - \theta_k) + \sum_{k=0}^{N-1} a_k^2\Big]. \quad (9)$$

The error is minimized if we choose $\phi_k = \theta_k$ for $k = 0, 1, \cdots, N-1$. In other words, we choose $\mathbf{H}$ to have the same phase as $\mathbf{F}$, while the magnitude of all coefficients of $\mathbf{H}$ are set to unity.

5.2. Signal Constellation

The procedure employed for generating the maximally separable sequences is as follows.

1. From a random seed, generate a binary (± 1) sequence $\mathbf{e}_k$ of length $L = 2^{p_k - 1}$.
2. Obtain the length-L_k DFT $\mathbf{E}_k$ of the binary sequence.
3. Obtain $\mathbf{S}_k$ from $\mathbf{E}_k$ such that $|S_k(l)| = 1, l = 1 \cdots L_k$ and $\angle S_k(l) = \angle E_k(l), l = 1 \cdots L_k$.
4. Take the length-L_k IDFT of $\mathbf{S}_k$ to obtain $\mathbf{s}_k$. $\mathbf{s}_k$ is a *cyclic all-pass* function. All $L_k = 2^{p-1}$ cyclic shifts of $\mathbf{s}_k$ are orthogonal.
5. $\mathbf{s}_k$ and the other $L_k - 1$ cyclic shifts of $\mathbf{s}_k$, and their negatives are the 2^{p_k} maximally separable sequences.

Note that the inner product of the sequence $\mathbf{s}_k$ of length L_k with each of the $2L_k = 2^{p_k}$ maximally separable sequences can be obtained by one length-L_k cyclic correlation efficiently implemented using the FFT. The index of the maximum absolute value of the cyclic correlation coefficients gives then detected sequence of p bits. Let $0 \le d_k \le 2^{p_k} - 1$ be the decimal representation of $\mathbf{s}_k^d$.

$$\mathbf{s}_k^d = \begin{cases} \alpha\mathcal{C}(\mathbf{s}_k, d_k) & \text{if } d_k < 2^{p-1} \\ -\alpha\mathcal{C}(\mathbf{s}_k, d_k - 2^{p-1}) & \text{if } d_k \ge 2^{p-1} \end{cases} \quad (10)$$

where $\mathcal{C}(\mathbf{x}, q)$ stands for cyclic shift of the vector $\mathbf{x}$ by q (counter-clockwise) positions, and α is a scaling factor that depends on Δ of the operator $\mathcal{E}$. For detection,

$$\mathbf{R}_k = \mathcal{F}(\mathbf{s}_k)\mathcal{F}(\tilde{\mathbf{s}}_k) \quad \mathbf{r}_k = \mathcal{F}^{-1}(\mathbf{R}_k) \quad (11)$$

where $\mathcal{F}$ denotes the DFT, and,

$$\tilde{d}_k = \begin{cases} \arg\max_{i=0\cdots L_k-1} |r_k(i)| & \text{if } r_k(i) > 0 \\ \arg\max_{i=0\cdots L_k-1} |r_k(i)| + L_k & \text{if } r_k(i) \le 0. \end{cases}$$

Though it is simpler to generate cyclic all-pass sequences $\mathbf{s}_k$ using Eq (7) (by choosing the phases randomly), we need binary sequences $\pm\frac{\Delta}{4}$ for the optimality of $\mathcal{E}, \mathcal{D}$ [3] employed to find the origin of the floating signal constellation. Steps 1-4 ensure that the generated signature sequences $\mathbf{s}_k$ is an all-pass sequence *closest in the mean- square sense* to the binary random sequence $\mathbf{e}_k$.

The choice of the length L_k of each segment (which in-turn decides the alphabet size) will depend mainly on the correlation ρ for the particular choice of Δ and β. Typically, lower the value of ρ, higher will be the value of L_k. Obviously, other factors like computational complexity may also influence the choice of L_k.

As the segment lengths are restricted to be powers of 2 for efficient implementation of the FFT, smooth trade-offs between bit-rate and the probability of error can only be achieved by redundant signaling. In the next section we propose a suitable and practical redundant signaling technique for improving the over-all efficiency of the signaling method.

6. REDUNDANT SIGNALING

For the proposed FFT-based signaling technique, we propose a combination of Reed-Solomon coding [8] and introduction of parity for error correction. A sequence of d-bit symbols D_1 to D_n is encoded using Reed-Solomon encoding over $\mathcal{GF}(2^d)$, with block size of $2^d - 1$ (if $n < 2^d - 1$, the "shortened" code can be easily implemented by zero-padding $D_1 \cdots D_n$ to length $2^d - 1$, and considering the non-existent symbols as "erasures" at the decoder). The RS encoded sequence of d-bit symbols is then "appended" with q-parity bits to produce a p-bit symbol sequence, where $p = d + q$.

Signaling with parity can be done efficiently for the FFT-based technique. To introduce one parity bit (or reduce the valid points in the constellation by a factor of 2) we choose only odd values D between 0 and 2^{p-1} and only even values between 2^{p-1} and 2^p. This would correspond to choosing the largest from the *even-indexed* coefficients of $\mathbf{r}_k$ in Eq. (11). If $L_k = 2^{p-1}$ is the length of $\mathbf{r}_k$, the even indexed coefficients $\mathbf{r}_{e_k}$ of $\mathbf{r}_k$ can be obtained as

$$\begin{aligned} R_{2_k}(l) &= R_k(l) + R_k(l + L_K/2), l = 0 \cdots \frac{L_k}{2} - 1 \\ \mathbf{r}_{e_k} &= \mathcal{F}^{-1}_{L_k/2}(0.5\mathbf{R}_{2_k}). \end{aligned} \tag{12}$$

In the above equation, $\mathcal{F}^{-1}_{L_k/2}(.)$ is a $\frac{L_k}{2}$- point IDFT (the factor 0.5 is irrelevant as our intention is only to pick the coefficient with the highest magnitude). For introducing q parity bits, (in the segment L_k representing p bits, where $p = q + d$) valid points in the constellation are given by

$$D = \begin{cases} m2^q - 1 & D < L_k - 1 \\ m2^q & L_k \leq D < 2L_k \end{cases} \quad m = 0, 1, \ldots, \frac{L_k}{2^q} \tag{13}$$

In this case, only coefficients of $\mathbf{r}_k$, with indices which are multiples of 2^q are needed. For $l = 0 \cdots \frac{L_k}{2^q} - 1$,

$$R_{q_k}(l) = \sum_{i=0}^{2^q-1} R_k(l + i\frac{L_k}{2^q}) \quad \mathbf{r}_{q_k} = \mathcal{F}^{-1}_{L_k/2^q}(\mathbf{R}_{q_k}).$$

Signaling with parity is especially useful for very low SNR data hiding (if ρ_{n_t} in Eq. (5) is very small - which results in large p or L_k).

For example, let $\mathbf{c} \in \Re^{8192}$. For a low-noise scenario we may use segment lengths of $L_k = 64$ for each $p = 7$ bit symbol ($L_k = 2^{p-1}$). Under such a scenario, we may use for example two blocks of RS code (127,111) over $\mathcal{GF}(2^7 = 128)$, which can correct up to 8 errors in each block of length 127 (number of source bits = 2blocks $\times$ 111symbols per block $\times$ 7bits per symbol = 1554). However, if the SNR is low, and we use say segment sizes of $L_k = 1024$ ($p = 11$). If we do not employ parity bits, we need to use an RS code, say (2047, 2045). The maximum block size possible is however, 8192/1024 = 8. We need a shortened code. We may start with a source of 6 11-bit symbols (66 bits), zero-padded to length 2045, and then perform (2047,2045) RS encoding, which can correct 1 error out of the 8 transmitted symbols. Obviously this is computationally expensive. An alternative is to use $L_k = 512$ and $p = 10$, and also have say $q = 5$ parity bits. We may now start with 14 5-bit source symbols (70 bits), and zero-pad it to a length 29 symbol block. This is followed by a computationally simple RS encoding (31,29). The first 16 5-bit symbols obtained after RS encoding are then made into 10-bit symbols by introducing 5 parity bits (which is done efficiently in the FFT-based method). For detection, the parity bits are stripped first to obtain a 16 symbol sequence of 5 bit symbols. This may be zero-padded to length 31 and RS decoded.

For data hiding applications where computational complexity of detection is not a serious limitation, or if channel noise is low (implying small p), signaling with parity would be sub-optimal. However, if p is large, and $q = 0$ (or $d = p$), then RS encoding / decoding may become prohibitively expensive.

7. CONCLUSIONS

We have presented a FFT-based signaling scheme especially suited for data hiding. The suitability is a result of three main characteristics of the proposed scheme: (1) ability to use large signal dimensions without increasing the computational complexity drastically, (2) ability to generate *random* signal constellation from a key and (3) efficient introduction of parity. The proposed signaling scheme was used in conjunction with close to optimal operators $(\mathcal{E}, \mathcal{D})$, and Reed-Solomon coding to design efficient magnitude DFT based data hiding technique for images in Ref. [9].

8. REFERENCES

[1] M.Ramkumar, A.N. Akansu, "Information Theoretic Estimates for Data Hiding in Compressed Images", IEEE International Conference on Multimedia Signal Processing, Dec 1998.

[2] M.Ramkumar, A.N. Akansu, A. Alatan, "On the Choice of Transforms for Data Hiding in Compressed Video", IEEE International Conference on Acoustics, Speech and Signal Processing, vol **VI**, pp 3049-3052, March 1999.

[3] M.Ramkumar, A.N. Akansu, "Self-Noise Suppression Schemes for Blind Image Steganography", SPIE's International Symposium on Voice, Video and Data Communications, Multimedia Systems and Applications (Image Security), Vol **3845**, Boston, MA, Sep. 1999.

[4] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Second Edition, John-Wiley and Sons Inc, 1991.

[5] M.H.M. Costa, "Writing on Dirty Paper", IEEE Trans. on Information Theory, **IT-29**, pp 439-441, May 1983.

[6] M.Ramkumar, A.N. Akansu, "Signaling for Multimedia Steganography," submitted to the *IEEE Trans. on Signal Processing.*

[7] M.Ramkumar, G.V. Anand, A.N. Akansu, "On the Implementation of 2-Band Cyclic Filterbanks", IEEE International Conference on Circuits and Systems, vol **3**, pp 234-234, 1999.

[8] S.B Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, Englewood Cliffs, NJ, 1995.

[9] M.Ramkumar, A.N. Akansu, "Some Design Issues for Robust Data Hiding Systems", presented at the 33rd ASILOMAR Conference on Signals, Systems and Computers, Pacific Grove, CA, October 1999.