Redundant Representations as a Means of Transmitting Data Covertly

Jody R. Miotke

MSc by Research in Pattern Analysis and Neural Networks

ASTON UNIVERSITY

September 2003

ASTON UNIVERSITY

Redundant Representations as a Means of Transmitting Data Covertly

JODY R. MIOTKE

MSc by Research in Pattern Analysis and Neural Networks, 2003

Thesis Summary

The lack of uniqueness arising from a redundant representation for a signal is shown to provide a way of transmitting additional hidden information. A coding/decoding system developed on the basis of such a possibility is proposed. The system is devised with the double purpose of a) enabling the transmission of an arbitrary signal b) allowing for the transmission of a hidden code.

Keywords: frame, signal, redundant representation, oversampling

Acknowledgements

First and foremost I would like to thank my supervisor, Laura Rebollo-Neira, for her endless support and advice on this project. I would also like to thank my friends and colleagues at Aston in the MSc PANN course for the camaraderie and support that they have provided over the past year. I would also like to thank the Neural Computing Research Group at Aston University for the financial support it has provided during this program. Last but certainly not least, I would like to express my gratitude to my family for their love and support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Signal transmission (coupled with that signal's accurate recovery) is a fundamental problem in applied mathematics and engineering. Redundant representations are one way of dealing with this problem. A redundant representation is a way of characterising a signal by a non-unique set of numbers. Notably, redundant representations have a good deal of resilience to noise that may be added in the transmission process.

In this thesis we propose and explore a novel approach to sending information covertly, embedded within a predetermined signal. This method takes advantage of the presently evolving methods and theory behind redundant representations for such signals, commonly referred to as *frames*. We propose an encoding/decoding procedure, which will enable the transmission of additional 'hidden' information when transmitting some arbitrary signal. The problem is viewed using multiple representations for the signal and the effect of additive noise in the transmission channel is also considered.

1.2 Thesis Outline

We begin in Chapter 2 with some basic definitions and preliminary results. Specifically, we will lead up to the definition of a basis as a means for obtaining a unique and convenient way to represent elements in a vector space. Then we will naturally move

to frames as a sort of overcomplete basis where the representation is no longer unique. Some useful theorems and properties will be discussed.

In Chapter 3 we will look at three examples of frames. The three frame types examined - Fourier, Gabor and Mexican hat wavelets - will provide a sampling of possible redundant representations. Chapter 4 will detail the focus of this thesis - an encoding/decoding system which can be used to transmit a hidden code while transmitting an arbitrary signal.

The following three chapters will give the experimental results of this encoding/decoding system with the three frame types seen in Chapter 3. At the end of each of these three chapters we will summarize the results for that representation. Finally we will have a summary chapter with composite conclusions.

1.3 Notes

Before we begin, we need to take particular note of a few items:

- This thesis is intended to illustrate the possibility of a novel way for using the theory of frames and redundant representations for transmitting data covertly while also transmitting an arbitrary signal. We do not attempt here to prove this method's usefulness or robustness in real-world scenarios.
- Unless otherwise noted all plots of complex variables show the real component only.

Chapter 2

Frame Theory

The central theme we present here is that of overcompleteness, or redundancy, of a representation which is treated in the context of the theory of frames. We start by giving some basic definitions and properties which will be relevant to our work. Most of the theory presented in this chapter is taken from [2] and [12]. We refer to those books for further details.

2.1 Preliminaries

Finite Energy Functions

We will choose to restrict our applications to L^2, which is the space of complex-valued finite energy signals defined on the real line $\mathbb{R}$. The *norm* of an element $f \in L^2(\mathbb{R})$ is

$$||f|| := \left(\int_{-\infty}^{\infty} |f(t)|^2 dt \right)^{1/2} < \infty.$$

The inner product on $L^2(\mathbb{R})$ is defined as

$$\langle f, g \rangle := \int_{-\infty}^{\infty} f(t)\overline{g(t)}dt \text{ for } f, g, \in L^2(\mathbb{R}).$$

where $\overline{g(t)}$ denotes the complex conjugate of $g(t)$.

The *span* of a sequence of functions $\{f_n\}$ is the set of functions generated from arbitrary linear combinations of $\{f_n\}$; i.e.

$$\text{span}\{f_n\} = \left\{ \sum c_n f_n : c_n \in \mathbb{C} \right\}$$

Finite Energy Sequences

$\ell^2(\mathbb{Z})$ is the space of complex-valued finite energy sequences defined on the integers $\mathbb{Z}$. The *norm* of an element $c \in \ell^2(\mathbb{Z})$ is

$$||c|| := \left(\sum_{n=-\infty}^{\infty} |c_n|^2 \right)^{1/2} < \infty.$$

The ℓ^2 inner product on $\ell^2(\mathbb{Z})$ is defined as

$$\langle c, d \rangle := \sum_{n=-\infty}^{\infty} c_n \overline{d_n} \text{ for } c, d, \in \ell^2(\mathbb{Z}).$$

As we continue with definitions, we will assume that V and W are finite dimensional vector spaces over $\mathbb{C}$ each equipped with an inner product and a norm.

Orthogonality and Normality

Two elements $x, y \in V$ are *orthogonal* if $\langle x, y \rangle = 0$; and the *orthogonal complement* of a subspace U of V is

$$U^{\perp} := \{x \in V : \langle x, y \rangle = 0, \forall y \in U\}.$$

An element $x \in V$ has been *normalized* if $||x|| = 1$.

Open and Closed Sets

A set O of real numbers is called *open* if for each $x \in O$ there exists a $\delta > 0$ such that all y satisfying $|x - y| < \delta$ are also in O.

A set F is called *closed* if the complement of F is open.

Operators

Given a linear operator $T : V \to W$, the *adjoint* operator $T^* : W \to V$ is characterized by

$$\langle Tx, y \rangle = \langle x, T^* y \rangle, \ x \in V, \ y \in W.$$

The *kernel* or *null space* for T is

$$\text{Null}(T) := \{x \in V : Tx = 0\}$$

The *range* for T is

$$\text{Range}(T) := \{Tx : x \in V\}.$$

It is important to note that Null(T)=Range(T^*)$^\perp$.

T is *surjective* or *onto* if $T(V) = W$. T is called *injective* or *one-to-one* when $Tf = Tg$ if and only if $f = g$. An operator that is both injective and surjective is called *bijective.*

$U_T(t)$ is called the *characteristic* or *indicator* function on the interval $[-T, T]$ if

$$U_T(t) = \begin{cases} 1 & \text{if } t \in [-T, T] \\ 0 & \text{otherwise.} \end{cases}$$

An operator T is said to be *bounded* if there exists a constant $k > 0$ such that

$$||Tv||_W \leq k\,||v||_V, \forall\ v \in V.$$

Additionally, three specific classes of operators will be of importance later: *translation*, *modulation* and *dilation.* Their definitions are:

$$\text{Translation by } a \in \mathbb{R},\ T_a : L^2(\mathbb{R}) \to L^2(\mathbb{R}), (T_a f)(x) = f(x-a);$$

$$\text{Modulation by } b \in \mathbb{R},\ E_b : L^2(\mathbb{R}) \to L^2(\mathbb{R}), (E_b f)(x) = e^{2\pi \imath b x} f(x);$$

$$\text{Dilation by } a \neq 0,\ D_a : L^2(\mathbb{R}) \to L^2(\mathbb{R}), (D_a f)(x) = \frac{1}{\sqrt{|a|}} f(\frac{x}{a}).$$

Inverse

The *inverse* of an operator $T : V \to W$ is defined by $T^{-1} : W \to V$ such that for all $v \in V$ and $w \in W$ we have $T^{-1}(T(v)) = v$ and $T(T^{-1}(w)) = w$.

It is often desirable to find some kind of inverse for an operator which is not invertible in the strict sense. If $T : V \to W$ where W is closed, then the *pseudo-inverse* of T is the unique operator $T^\dagger : W \to V$ satisfying

1. $TT^\dagger$ and $T^\dagger T$ are both self-adjoint

2. $TT^\dagger T = T$

3. $T^\dagger TT^\dagger = T^\dagger$.

Proposition 2.1. *$T^\dagger$ has the property that for a system of equations $Tx = y$ it provides the minimal norm solution to the system.*

For proof please see [2].

Basis

Definition 2.2. *A sequence $\{f_k\}_{k=1}^M$ in V is a basis if the following two conditions are satisfied:*

1. *$V = span\{f_k\}_{k=1}^M$;*

2. *If $\sum_{k=1}^M c_k f_k = 0$ for some scalar coefficients $\{c_k\}_{k=1}^M$, then $c_k = 0$ for all $k = 1, \ldots, m$.*

Condition 2 above is called *linear independence.*

The definition of a basis gives us necessary and sufficient conditions such that every $f \in V$ has a unique representation in terms of the basis elements. That is, there exist unique scalar coefficients $\{c_k\}_{k=1}^M$ such that

$$f = \sum_{k=1}^{M} c_k f_k. \tag{2.1}$$

Additionally, if $\{f_k\}_{k=1}^M$ is an *orthonormal basis*, i.e., a basis for which

$$\langle f_k, f_j \rangle = \delta_{k,j} = \begin{cases} 1 & \text{if } k = j \\ 0 & \text{if } k \neq j \end{cases}$$

then the coefficients $\{c_k\}_{k=1}^M$ can be obtained by taking the inner product of f in (2.1) with an arbitrary f_j:

$$\langle f, f_j \rangle = \left\langle \sum_{k=1}^{M} c_k f_k, f_j \right\rangle = \sum_{k=1}^{M} c_k \langle f_k, f_j \rangle = c_j,$$

so

$$f = \sum_{k=1}^{M} \langle f, f_k \rangle f_k. \tag{2.2}$$

2.2 Frames

Of particular interest in this thesis, will be a sequence $\{f_k\}_{k=1}^{M}$ which is not linearly independent, i.e. where property 2 for a basis is not satisfied. Such a set is no longer a basis but instead a *frame*.

Definition 2.3. *A countable family of elements $\{f_k\}_{k\in I}$ in V is a frame for V if there exist constants $A, B > 0$ such that*

$$A\|f\|^2 \leq \sum_{k\in I} |\langle f, f_k \rangle|^2 \leq B\|f\|^2, \forall\, f \in V. \tag{2.3}$$

The numbers A and B are called *frame bounds*. One should note that these bounds are not unique. The *optimal lower frame bound* is the supremum over all lower frame bounds, and the *optimal upper frame bound* is the infimum over all upper frame bounds. The frame is *normalized* if $\|f_k\| = 1, \forall\, k \in I$.

For the purposes of practicality and applicability we will consider only finitely many elements $\{f_k\}_{k=1}^{M}, M \in \mathbb{N}$. With this restriction, the Cauchy-Schwarz' inequality shows that

$$\sum_{k=1}^{M} |\langle f, f_k \rangle|^2 \leq \sum_{k=1}^{M} ||f_k||^2 ||f||^2, \forall f \in V,$$

i.e. the upper frame condition is automatically satisfied with the upper bound $\sum_{k=1}^{M} ||f_k||^2$. In order for the lower condition in 2.3 to be satisfied, it is necessary that $\text{span}\{f_k\}_{k=1}^{M} = V$.

Theorem 2.4. *Let $\{f_k\}_{k=1}^{M}$ be a sequence in V. Then $\{f_k\}_{k=1}^{M}$ is a frame for span$\{f_k\}_{k=1}^{M}$.*

For proof we refer to [2].

Corollary 2.5. *A family of elements$\{f_k\}_{k=1}^{M}$ in V is a frame for V if and only if $V =$ span$\{f_k\}_{k=1}^{M}$.*

By this corollary, we see that every basis is a frame, but the converse is not necessarily true. That is, the elements of a frame are not necessarily linearly independent. Every frame in a finite-dimensional space contains a subfamily which is a basis for the same subspace. If $\{f_k\}_{k=1}^M$ forms a frame but not a basis, we will refer to it as *overcomplete*, *redundant* or *oversampled*. These redundant representations are of central interest here for reasons we will see later.

Consider now a vector space V equipped with a frame $\{f_k\}_{k=1}^M$ and define the linear mapping

$$T : \mathbb{C}^M \to V, \;\; T\{c_k\}_{k=1}^M = \sum_{k=1}^M c_k f_k.$$

T is usually called the *pre-frame operator*. The *adjoint* operator is given by

$$T^* : V \to \mathbb{C}^M, \;\; T^* f = \{\langle f, f_k \rangle\}_{k=1}^M,$$

and is sometimes called the *analysis operator*. By composing T with its adjoint T^* we obtain the *frame operator*:

$$S : V \to V, \;\; Sf = TT^* f = \sum_{k=1}^M \{\langle f, f_k \rangle f_k.$$

Lemma 2.6. *Let $\{f_k\}_{k=1}^M$ be a frame for V with frame operator S. S is invertible and self-adjoint.*

For proof please see [2].

Note that in terms of the frame operator,

$$\langle Sf, f \rangle = \sum_{k=1}^M |\langle f, f_k \rangle|^2, \;\; f \in V. \tag{2.4}$$

Theorem 2.7. *If $\{f_k\}_{k=1}^M$ is a frame for V with frame operator S then every $f \in V$ can be represented as*

$$f = \sum_{k=1}^M \langle f, S^{-1} f_k \rangle f_k \tag{2.5}$$

Proof: Let $\{f_k\}_{k=1}^M$ be a frame for V with frame operator S. Then

$$f \;\; = \;\; SS^{-1} f$$

$$
\begin{aligned}
&= TT^*S^{-1}f \\
&= \sum_{k=1}^{M} \langle S^{-1}f, f_k \rangle f_k \\
&= \sum_{k=1}^{M} \langle f, S^{-1}f_k \rangle f_k \text{ since } S \text{ (and hence } S^{-1}) \text{ is self-adjoint.} \quad \square
\end{aligned}
$$

Theorem 2.8. *If $f \in V$ has the representation $f = \sum_{k=1}^{M} c_k f_k$ for some scalar coefficients $\{c_k\}_{k=1}^{M}$ where $\{f_k\}_{k=1}^{M}$ is a frame for V with frame operator S , then*

$$\sum_{k=1}^{M} |c_k|^2 = \sum_{k=1}^{M} |\langle f, S^{-1}f_k \rangle|^2 + \sum_{k=1}^{M} |c_k - \langle f, S^{-1}f_k \rangle|^2. \tag{2.6}$$

For proof we refer to [2].

The consequence of this result will be of central importance to us as we progress, so we will state it in the following Corollary:

Corollary 2.9. *Of all possible representations satisfying $f = \sum_{k=1}^{M} c_k f_k$, the set of coefficients of minimal 2-norm are*

$$c_k = \langle f, S^{-1}f_k \rangle. \tag{2.7}$$

The set $\{\langle f, S^{-1}f_k \rangle\}_{k=1}^{M}$ is generally called the set of *frame coefficients.* Note that because $S : V \to V$, is bijective, the sequence $\{g_k\}_{k=1}^{M} = \{S^{-1}f_k\}_{k=1}^{M}$ is also a frame; it is called the *canonical dual* of $\{f_k\}_{k=1}^{M}$ [2].

Theorem 2.10. *Let $\{f_k\}_{k=1}^{M}$ be a frame for $\mathbb{C}^n$, with pre-frame operator T and frame operator S. Then*

$$T^\dagger f = \{\langle f, S^{-1}f_k \rangle\}_{k=1}^{M}, \forall f \in \mathbb{C}^n. \tag{2.8}$$

Proof: Let $f \in \mathbb{C}^n$. Expressed in terms of the pre-frame operator T, the equation $f = \sum_{k=1}^{M} c_k f_k$ means that $T\{c_k\}_{k=1}^{M} = f$. The result now follows from Corollary 2.9 and Proposition 2.1.

Computationally, the operator in (2.8) means that

$$T^\dagger = T^*(TT^*)^{-1},$$

a formula that is known to hold generally for the pseudo-inverse of an arbitrary surjective operator T.

Definition 2.11. *A frame is said to be tight if we can choose $A = B$ such that*

$$\sum_{k=1}^{M} |\langle f, f_k \rangle|^2 = A\|f\|^2, \forall f \in V \tag{2.9}$$

where A is called the frame bound.

This definition together with Theorem 2.4 leads directly to the following:

Corollary 2.12. *If $\{f_k\}_{k=1}^M$ is a tight frame for V with frame bound A, then $S = AI$ (where I is the identity operator on V), and*

$$f = \frac{1}{A}\sum_{k=1}^{M}\langle f, f_k\rangle f_k, \quad \forall f \in V \tag{2.10}$$

This result gives us the fact that when $\{f_k\}_{k=1}^M$ is a tight frame, the minimum-norm coefficients satisfying $f = \sum_{k=1}^M c_k f_k$ are defined by

$$c_k = \frac{1}{A}\langle f, f_k\rangle. \tag{2.11}$$

Furthermore, tight frames can lead us back to the idea of an orthonormal basis.

Proposition 2.13. *If $\{f_k\}_{k=1}^M$ is a tight frame for V with frame bound $A = 1$ and $||f_k|| = 1$ for all $k \in \{1, 2, \ldots, M\}$, then $\{f_k\}_{k=1}^M$ forms an orthonormal basis for V.*

For proof please refer to [4].

Some comments:

We now discuss how overcomplete frames can be useful in signal transmission. If we wish to transmit a signal f, all we need to do is transmit the frame coefficients $\{c_k\}_{k=1}^M$ to the intended receiver which he/she may use to reconstruct the signal, provided that the receiver has knowledge of the frame functions $\{f_k\}_{k=1}^M$. It is important to note that in the case where $\{f_k\}_{k=1}^M$ forms a basis, the elements f_k are linearly independent, and hence the representation

$$f = \sum_{k=1}^{M} c_k f_k \tag{2.12}$$

is unique and is exactly that which was described in (2.5). If the frame $\{f_k\}_{k=1}^M$ is not a basis, i.e. the elements f_k are not linearly independent, and hence the set of scalar coefficients $\{c_k\}_{k=1}^M$ satisfying (2.12) is not unique, the representation given in (2.5) is only one of the many possibilities.

Let us now consider the case where the frame elements are *not* linearly independent (i.e overcomplete or redundant). The redundancy inherent in a set $\{f_k\}_{k=1}^M$ which is not linearly independent implies that there exist non-zero sequences $\{c'_k\}_{k=1}^M$ such that

$$\sum_{k=1}^{M} c'_k f_k = 0 \tag{2.13}$$

(i.e. $T\{c'_k\}_{k=1}^M = 0$). It is useful to note that if we take the inner product of both sides of (2.13) by an arbitrary frame element f_j we get

$$\left\langle \sum_{k=1}^{M} c'_k f_k, f_j \right\rangle = \sum_{k=1}^{M} c'_k \langle f_k f_j \rangle = 0.$$

This can also be written as

$$G\vec{c'} = 0 \tag{2.14}$$

where the matrix G is defined elementwise by

$$g_{m,n} = \langle f_n, f_m \rangle \tag{2.15}$$

Therefore, any vector $\vec{c'} \in \text{Null}(G)$ satisfies the following:

$$f = \sum_{k=1}^{M} \langle f, S^{-1} f_k \rangle f_k + \sum_{k=1}^{M} c'_k f_k. \tag{2.16}$$

This is exactly what we will use in Chapter 4 to devise a method of sending information covertly.

Now that we have the basics down, we will dive right into some specific examples of frames in Chapter 3. Three different frame representations will be explored. We will then proceed to the proposed encoding/decoding system in Chapter 4 and apply those methods given in Chapter 5-7.

Chapter 3

Examples of Frames

In this chapter we begin to look at some different ways of representing signals by using redundant representations (frames). We will explore three types of these common frame expansions used in signal analysis: Fourier, Gabor, and Mexican hat wavelets. These three examples are meant to demonstrate how the method of transmitting a hidden code along with a predetermined signal can be accomplished with varied signal representations.

3.1 The Fourier Case

Fourier analysis attempts to break down a signal into constituent sinusoids of different frequencies. So one may think of Fourier analysis as a frequency-based mathematical technique for breaking down a signal. We will pay particular attention to the Fourier methods because they provide a good foundation to explain our novel way of transmitting a hidden code along with a signal.

We start by the standard use of complex exponentials as a basis for the space of periodic functions, then naturally extend it to an overcomplete representation.

Theorem 3.1. *The set* $\{\varphi_k U_T\}_{k\in\mathbb{Z}}$ *with* φ_k *defined by*

$$\varphi_k(t) = \frac{1}{\sqrt{2T}}\, e^{\imath\frac{k\pi t}{T}}$$

forms an orthonormal basis for $L^2[-T,T]$.

For a proof of this theorem the reader is referred to [12].

Hence any $f \in L^2[-T,T]$ has the representation

$$f = \sum_{n=-\infty}^{\infty} c_k \varphi_k$$

where

$$c_k = \langle f, \varphi_k \rangle = \frac{1}{\sqrt{2T}} \int_{-T}^{T} f(t) e^{-\imath \frac{k\pi t}{T}} \, dt. \tag{3.1}$$

3.1.1 Oversampled Fourier

Now to bring in the redundancy required for our method of hiding information, we consider the re-scaling operation: $t \to at$, with $a \in \mathbb{R}(0,1]$. If the restriction $t \in [-T,T]$ is maintained, the exponentials $\{e^{\imath \frac{ak\pi t}{T}}\}_{-\infty}^{\infty}$ are not linearly independent. Furthermore, the functions $\varphi_{ak} = \frac{\sqrt{a}}{\sqrt{2T}} e^{\imath \frac{ak\pi t}{T}}$ no longer form a basis but instead a tight frame with frame-bound $A = 1$ [8].

Theorem 3.2. *For a positive real number $a \leq 1$, the set $\{\varphi_k(at) U_T(t)\}_{k \in \mathbb{Z}}$ defined by*

$$\varphi_k(at) = \varphi_{ak}(t) = \frac{\sqrt{a}}{\sqrt{2T}} \, e^{\imath \frac{ak\pi t}{T}}$$

forms a tight frame with frame-bound $A = 1$ for the space of time-limited functions such that $f(t) = 0$ for $|t| > T$.

Proof: Let $f \in L^2(\mathbb{R})$ such that $f(t) = 0$ for $|t| > T$. We must show that

$$\sum_{n=-\infty}^{\infty} |\langle f, \varphi_{ak} \, U_T \rangle|^2 = \|f\|^2.$$

By extension of Theorem 3.1, the functions $\{\varphi_{ak}\}_{k \in \mathbb{Z}}$ constitute an orthonormal basis for $L^2[-\frac{T}{a}, \frac{T}{a}]$, so we have

$$f(t) = \sum_{k=-\infty}^{\infty} c_k \varphi_{ak}(t)$$

with

$$c_k = \langle f, \varphi_{ak} \rangle$$

and then from Parseval's identity

$$\|f\|^2 = \sum_{k=-\infty}^{\infty} |c_k|^2.$$

Now because $f(t) = 0$ for $|t| > T$, $f(t) = f(t)\,U_T(t)$ and hence

$$\begin{aligned} c_k &= \langle f, \varphi_{ak} \rangle \\ &= \frac{\sqrt{a}}{\sqrt{2T}} \int_{-T/a}^{T/a} f(t) U_T(t) e^{-\imath \frac{ak\pi t}{T}}\, dt \\ &= \frac{\sqrt{a}}{\sqrt{2T}} \int_{-T}^{T} f(t) e^{-\imath \frac{ak\pi t}{T}}\, dt \quad \text{for } a \leq 1 \\ &= \langle f, \varphi_{ak}\, U_T \rangle. \end{aligned}$$

Thus we finally have

$$\|f\|^2 = \sum_{k=-\infty}^{\infty} |c_k|^2 = \sum_{k=-\infty}^{\infty} |\langle f, \varphi_{ak}\, U_T \rangle|^2. \quad \square$$

Notice that $||\varphi_{ak} U_T|| = a$ so we will only fall under the jurisdiction of Proposition 2.13 (and hence have an orthonormal basis) when $a = 1$.

Consequently we have

$$\begin{aligned} f(t) &= \sum_{k=-\infty}^{\infty} c_k\, \varphi_{ak}(t)\, U_T(t) \\ &= \frac{\sqrt{a}}{\sqrt{2T}} \sum_{k=-\infty}^{\infty} c_k e^{\imath \frac{ak\pi t}{T}}\, U_T(t) \end{aligned} \tag{3.2}$$

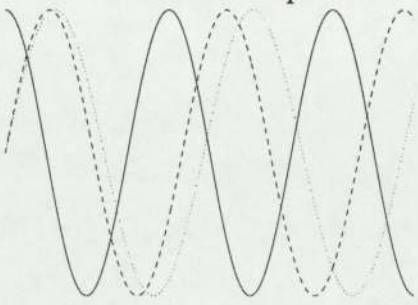
where

$$\begin{aligned} c_k &= \langle f, \varphi_{ak}\, U_T \rangle \\ &= \frac{\sqrt{a}}{\sqrt{2T}} \int_{-T}^{T} f(t) e^{-\imath \frac{ak\pi t}{T}}\, dt. \end{aligned} \tag{3.3}$$

For practical reasons we will use a finite approximation of (3.2)

$$f(t) = \frac{\sqrt{a}}{\sqrt{2T}} \sum_{k=-M}^{M} c_k\, e^{\imath \frac{ak\pi t}{T}}\, U_T(t). \tag{3.4}$$

Figure 3.1: Three Fourier Expansion Functions



3.1.2 Using the FFT computational algorithm

The aforementioned calculations can also be computed by using the highly efficient FFT and IFFT algorithms. We will treat these methods roughly for the purpose of demonstrating the applicability for our method of transmitting hidden information. For a more complete treatment of the methods, uses and advantages of the FFT please see [1] and [10].

The FFT algorithm is defined by the discrete Fourier transform

$$X(k) = \sum_{n=1}^{M} x(n) \exp\left[-i\frac{2\pi(k-1)(n-1)}{M}\right], \text{ for } k \in \{1, \ldots, M\}. \tag{3.5}$$

The inverse DFT (computed by IFFT) is given by

$$x(n) = \frac{1}{M}\sum_{k=1}^{M} X(k) \exp\left[i\frac{2\pi(k-1)(n-1)}{M}\right], \text{ for } n \in \{1, \ldots, M\}.$$

That is, the number of points at which our signal is evaluated is necessarily equal to the number of coefficients that we will use to estimate the signal. To simulate the oversampling then, we will 'pad' the signal with zeros. Let us see an example of how this is done.

First, we translate horizontally such that we have

$$\begin{aligned} c_k &= \frac{\sqrt{a}}{\sqrt{2T}} \int_{-T}^{T} f(t) e^{-\imath \frac{ak\pi t}{T}} dt \\ &= \frac{\sqrt{a}}{\sqrt{2T}} \int_{0}^{2T} f(t-T) e^{-\imath \frac{ak\pi (t-T)}{T}} dt \\ &= \frac{\sqrt{a}}{\sqrt{2T}} e^{iak\pi} \int_{0}^{2T} f(t-T) e^{-\imath \frac{ak\pi t}{T}} dt \end{aligned}$$

which we can estimate by the Riemann sum where f is evaluated at N points

$$c_k = \frac{\sqrt{a}}{\sqrt{2T}} e^{iak\pi} \sum_{n=1}^{N} f(\Delta(n-1) - T) e^{-\imath \frac{\pi a k (n-1)\Delta}{T}} \Delta$$

where $\Delta = \frac{2T}{N}$. Now we find

$$c_k = \frac{\sqrt{2Ta}}{N} e^{iak\pi} \sum_{n=1}^{N} f\left(\frac{2T}{N}(n-1) - T\right) e^{-\imath \frac{2\pi a k (n-1)}{N}}.$$

Now if we are considering M coefficients, then by setting $N = aM$ and $f\left(\frac{2T}{N}(n-1) - T\right) = 0$ for $n > N$ we find that

$$c_k = \frac{\sqrt{2T}}{\sqrt{a}M} e^{\imath a\pi k} \sum_{n=1}^{M} f\left(\frac{2T}{aM}(n-1) - T\right) e^{-\imath \frac{2\pi k (n-1)}{M}}. \tag{3.6}$$

Note that except by the constant and a phase factor this is equivalent to (3.5).

So, if we consider the signal f to be transmitted represented by an N-dimensional data vector and we desire an oversampling parameter $a \in (0, 1)$ then we will need to add $\frac{N(1-a)}{a}$ zeros to the end of our vector f to achieve the desired number of coefficients $M = \frac{N}{a}$.

3.2 Gabor Frames

Another common example of a frame expansion is that of *Gabor frames.*

Definition 3.3. *A Gabor frame is a system* $\{g_{m,n}\}_{m,n\in\mathbb{Z}}$ *defined by*

$$g_{m,n}(x) = e^{2\pi \imath max} g(x - nb) \quad a, b \in \mathbb{R}^+, \; g \in L^2(\mathbb{R}) \tag{3.7}$$

that also satisfies the frame condition (2.3).

Gabor frames are sometimes also called *Weyl-Heisenberg frames* [4].

Basically, a Gabor frame is a series of elementary functions, which are constructed from a single building block by translation and modulation. This type of representation has a relative strength over the Fourier expansions discussed previously because it yields a method of frequency analysis that, unlike Fourier, is local in time [4] [5] [10]. Two

particular choices for g for which the system $\{g_{m,n}\}_{m,n\in\mathbb{Z}}$ can produce an orthogonal basis are [12]

$$g(x) = \begin{cases} 1 & 0 \leq x < 1, \\ 0 & \text{otherwise} \end{cases} \tag{3.8}$$

and

$$g(x) = \frac{\sin \pi x}{\pi x}. \tag{3.9}$$

Not all values of a and b in (3.7) will yield a frame, but we may classify these systems according to the corresponding sampling density of the time-frequency lattice [4] and [6]:

1. *oversampling* - $ab < 1$: Frames with excellent time-frequency localisation exist (a particular example are frames with Gaussian g and appropriate oversampling rate).

2. *critical sampling* - $ab = 1$: Frames and orthonormal bases are possible, but without good time-frequency localization.

3. *undersampling* - $ab > 1$: In this case any Gabor family will be incomplete, in the sense that the span is a proper subspace of $L^2(\mathbb{R})$.

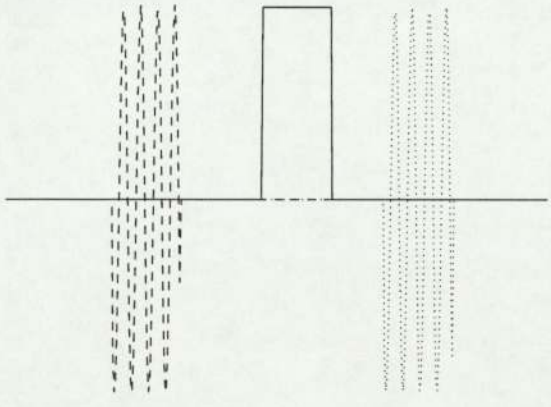


Figure 3.2: Three Gabor Functions with g defined in (3.8)

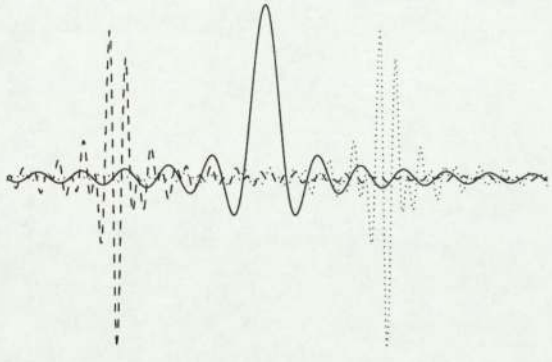


Figure 3.3: Three Gabor Functions with g defined in (3.9)

3.3 Mexican Hat Wavelets

Wavelets are another way to create a frame to represent a signal. Wavelet analysis replaces the complex exponential building blocks of Fourier analysis with more flexible units, the wavelet functions [4], [5], [9].

Definition 3.4. *A wavelet frame is a set of functions* $\{\psi_{m,n}\}_{m,n\in\mathbb{Z}}$ *for* $L^2(\mathbb{R})$ *consisting of functions of the form*

$$\psi_{m,n}(x) = a^{-m/2}\psi(a^{-m}x - nb) \quad a, b \in \mathbb{R}^+$$

where ψ *is a unit vector in* $L^2(\mathbb{R})$ *that also satisfies the frame condition (2.3).*

The function ψ that generates the basis is called a *wavelet.* A sample wavelet is the *Mexican hat function*, the second derivative of the Gaussian $e^{-x^2/2}$; if we normalise it so that $||\psi|| = 1$, then

$$\psi(x) = \frac{2}{\sqrt{3}}\pi^{-1/4}(1 - x^2)e^{-x^2/2}.$$

Although we will choose to restrict our later applications to the Mexican hat wavelet, two other well-known choices for ψ for which the system $\{\psi_{m,n}\}_{m,n\in\mathbb{Z}}$ constitutes an orthonormal basis for $L^2(\mathbb{R})$ are

$$\psi(x) = \begin{cases} 1 & 0 \le x < \frac{1}{2}, \\ -1 & \frac{1}{2} \le x < 1, \\ 0 & \text{otherwise} \end{cases}$$

known as the *Haar wavelet* and

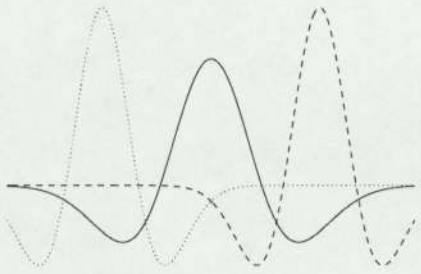
$$\psi(x) = \frac{\sin 2\pi x - \sin \pi x}{\pi x}$$

called the *Shannon wavelet* [12].

Wavelet expansions are especially useful when modelling a function with discontinuities or sharp spikes. For more details on wavelets and their uses please see [4], [7], [1], etc..

With these three frame examples in hand (Fourier, Gabor and Mexican hat wavelet)

Figure 3.4: Three Mexican Hat Wavelets



we proceed to the real purpose of this thesis: to propose an encoding/decoding system capable of sending a hidden code while utilising the structure already in existence for sending a signal.

Chapter 4

Proposed Encoding/Decoding System

Let us now assume that we have an overcomplete frame $\{f_k\}_{k=1}^M$ for the space of time-limited functions $L^2[-T,T]$. As previously explained in Chapter 2, any $f \in L^2[-T,T]$ can be written as $f = \sum_{k=1}^M c_k f_k$ with $c_k = \langle f, S^{-1} f_k \rangle$ and furthermore, because of the overcompleteness,

$$f = \sum_{k=1}^{M} c_k f_k + \sum_{k=1}^{M} c'_k f_k = \sum_{k=1}^{M} c''_k f_k \tag{4.1}$$

with $c''_k = c_k + c'_k$ where $\vec{c'} \in \text{Null}(G)$ where G is defined elementwise by

$$g_{m,n} = \langle f_n, f_m \rangle \tag{4.2}$$

for $n, m \in \{1, \ldots, M\}$. That is, for any possible vector $\vec{c'} \in \text{Null}(G)$, all coefficients $\vec{c''} = \vec{c} + \vec{c'}$ reproduce an identical signal as coefficients $\vec{c}$. This provides us with the foundation to construct an encoding/decoding scheme for transmitting hidden information. The vectors $\vec{c}$, $\vec{c'}$ and $\vec{c''}$ will hereafter be refereed to as *signal coefficients*, *hidden code coefficients* and *transmitted coefficients* respectively.

$$\begin{aligned} \vec{c} &= \{\langle f, S^{-1}f_k\rangle\}_{k=1}^{M} && \text{minimum norm coefficients} \\ \vec{c'} &\in \text{Null}(G) && \text{hidden code coefficients} \\ \vec{c''} &= \vec{c} + \vec{c'} && \text{transmitted coefficients} \end{aligned}$$

The key idea that we present here is that, as long as the vector $\vec{c'}$ is in the Null space of G, that vector's presence and attributes would not be obvious to an unintended receiver. So, we are transmitting two pieces of information - the signal and the hidden vector $\vec{c'}$. It is a fairly easy and straightforward process to recover the signal from the transmitted coefficients $\vec{c''}$ for a given frame expansion. However, an uninformed person might assume that the signal is the entire body of transmitted information, when it is not.

Once we agree that the presence of, and hence the information contained in, the vector $\vec{c'}$ is not obvious to an uninformed party, we now set up a way in which to use the vector $\vec{c'}$ to transmit the desired hidden information. We explore a very simple method whereby our hidden information is a sequence of real numbers, each used as a coefficient on eigenvectors of G that are also in Null(G). This method was chosen because of its simplicity since our purpose here is to show only that such a way of disseminating information is possible, although many other ways in which to code information into the vector $\vec{c'}$ can be imagined which may have additional desirable properties. A few of these will be mentioned later.

4.1 The Encoding-Decoding System

Let us assume that, in addition to transmitting an arbitrary signal f through an overcomplete frame expansion $\{f_k\}_{k=1}^{M}$ and we also wish to transmit a hidden code $\vec{h}$ consisting of K numbers. Consider that G is an $(M) \times (M)$ square matrix of elements as given in (4.2). We select K eigenvectors of G corresponding to zero eigenvalue, which are orthonormal, and construct a vector $\vec{c'} \in \text{Null}(G)$ as follows:

$$\vec{c'} = U\vec{h} \tag{4.3}$$

where U is a $M \times K$ matrix, the columns of which are the K selected eigenvectors.

Encoding process

Consider that the signal f to be transmitted is discretised as an N-dimensional data vector and proceed as follows:

- Compute the minimum 2-norm signal coefficients $\vec{c}$ through (2.11) if $\{f_k\}_{k=1}^{M}$ is a tight frame or as in (2.8) if not.
- Compute the hidden code coefficients $\vec{c'}$ as prescribed in (4.3).
- Transmit the coefficients $\vec{c''} = \vec{c} + \vec{c'}$ to receiver.

Decoding Process

- Use the received vector $\vec{c''}$ for recovering the signal f as in (4.1).
- Use the signal f and knowledge of the frame $\{f_k\}_{k=1}^{M}$ to compute the signal coefficients $\vec{c}$ as in (2.11) or (2.8).
- Compute vector $\vec{c'} = \vec{c''} - \vec{c}$.
- Recover the hidden vector $\vec{h}$ by noticing that, since the columns of matrix U in (4.3) are orthonormal vectors, we have

$$\vec{h} = U^* \vec{c'}$$

  where U^* indicates the transpose conjugate of matrix U.

In practice, the vector $\vec{c'}$ is generally scaled so as to make desired ratios with the minimum norm coefficients $\vec{c}$ and the noise (as will be discussed later). As such, we choose to transmit $\vec{c''} = \vec{c} + s\vec{c'}$ where s is some scalar.

Summing up, what the receiver needs to know is:

1. The transmitted coefficients $\vec{c''}$.

2. The frame expansion $\{f_k\}_{k=1}^{M}$ used.

3. The scaling value s used to desirably size the hidden code coefficients $\vec{c'}$.

4.2 Noise and the Quality of the Data Recovery

It provides a far more interesting a practical investigation if we also include a discussion on the effect of noise on the recovery of a hidden code in the prescribed system. As such, we will attempt to explore the interplay between redundancy and its effect on the noise apparent in signal reconstruction and the recovery of a hidden code. Much literature is available on how oversampling can be used to reduce noise when transmitting an arbitrary signal. For examples please see [5], [7], [8].

As in any system, there is a tradeoff between the amount of noise that is present and the quality of the data recovery. In our system, consider that we transmit the coefficients c_k'' through a noisy channel such that the receiver obtains $c_k'' + \epsilon$ where $\mathrm{E}(\epsilon) = 0$ and $\mathrm{Var}(\epsilon) = \sigma^2$. Remembering, of course, that $\vec{c''} = \vec{c} + \vec{c'}$ where $\vec{c}$ contains the information necessary to reconstruct the signal and $\vec{c'}$ contains the information necessary to reconstruct the hidden code, we will need the noise ϵ to be small with respect to both $\vec{c}$ and $\vec{c'}$.

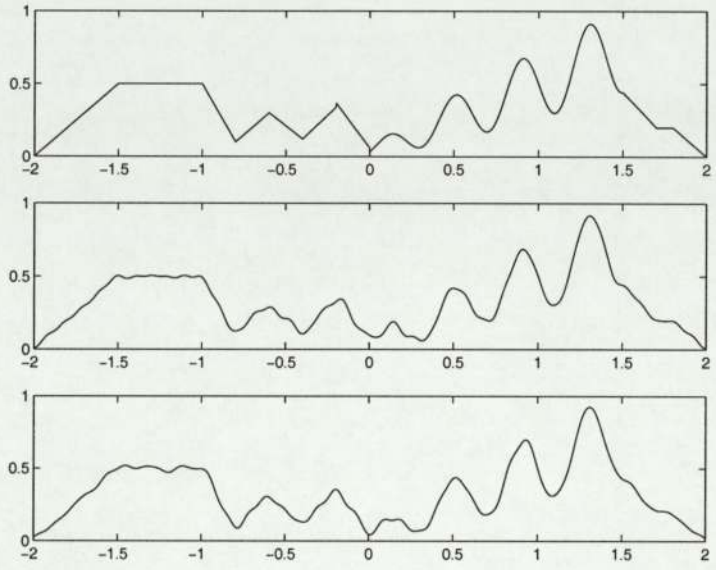
We define the signal-to-noise ratio as

$$S/N = 10 \log\left(\frac{V_S}{V_N}\right) \text{ where } V_S = \frac{||\vec{c}||^2}{\dim(\vec{c})} \text{ and } V_N = \sigma^2 \tag{4.4}$$

where $\dim(\vec{c})$ is the size of the vector $\vec{c}$. The signal-to-noise ratio will give us some measure of how well we will be able to reconstruct the signal. We will limit our experiments to two levels of the signal-to-noise ratio - 10 and 20 dB. An illustration of what a signal recovery might look like when $S/N = 10$ dB is given in Figure 4.1. This signal recovery was accomplished through a Fourier expansion as in 3.2 where $N = 40$ (and $M = N/a$) in each case for $a = 0.05$ and $a = 0.5$. The recovered signals are shown in Figure 4.1. We take particular note that when $a = 0.5$ we (Figure 4.1c) we recover a noisy signal, when we increase redundancy ($a \to 0$ as in Figure 4.1b) less noise is apparent in the reconstruction [8] [7]. From this point on, we will consider the variance

of the noise σ^2 to be fixed with respect to the signal coefficients at a level equivalent to $S/N = 10$ or 20 dB. In the case where $S/N = 20$ dB we have less noise with respect to the coefficients $\vec{c}$ and even a non-redundant representation only has a small amount of visible noise in the reconstruction.

Figure 4.1: Illustration of Signal Reconstruction with S/N=10 dB



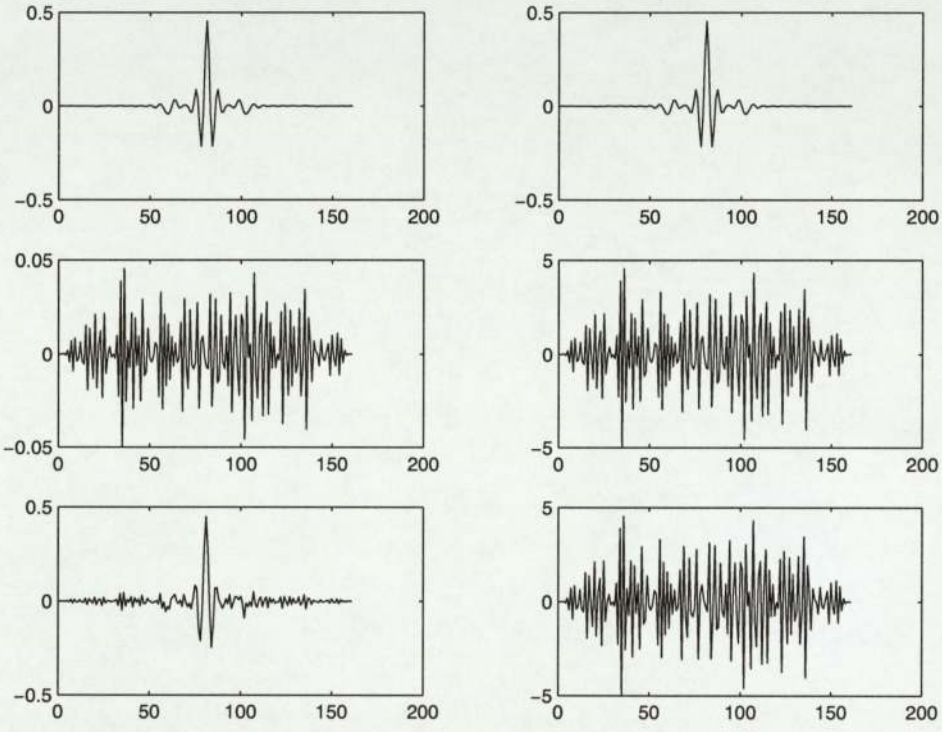
Figures 4.1a-4.1c, from top to bottom. 4.1a depicts the signal, 4.1b the signal reconstruction with S/N=10 dB and $a = 0.05$, and 4.1c the signal reconstruction with S/N=10 dB and $a = 0.5$.

Additionally, we need to be concerned with the size of the hidden coefficients $\vec{c'}$ with respect to the noise. We define this relationship by

$$\rho = \frac{\max(c)}{\max(c')}. \tag{4.5}$$

Consider the illustrations in Figure 4.2 of the coefficient systems $\vec{c}$, $\vec{c'}$, and $\vec{c''}$ (from top to bottom respectively) are shown for $\rho = 10$ on the column on the left and $\rho = 0.1$ for the column on the right. As can be seen in Figure 4.2, by defining ρ to be either small or large we will be able to dictate whether the transmitted coefficients look more like the minimum norm coefficients or the hidden code coefficients. We will take advantage of this in the following chapter to obtain the desired accuracy in the recovery of the hidden code.

Figure 4.2: Coefficient systems resulting from $\rho = 10$ and $\rho = 0.1$



Figures 4.2a-4.2f, from top to bottom, left to right. 4.2a-c in the first column depicts the signal coefficients, hidden coefficients and transmitted coefficients respectively for the case where $\rho = 10$ while 4.2d-f in the second column show the signal coefficients, hidden coefficients and transmitted coefficients respectively for the case where $\rho = 0.1$.

4.3 Problem Setup

This proposed method allows for the transmission of two things: 1) coefficients which are used to recover an arbitrary signal, and 2) a vector of numbers that are invisible to anyone wishing only to recover the signal. We choose to use two signals for our illustrations (shown in Figures 4.3 and 4.4). Note that the signal shown in Figure 4.3 has a relatively low frequency and is not smooth, whereas Signal 2 shown in Figure 4.4 has higher frequency and is smooth.

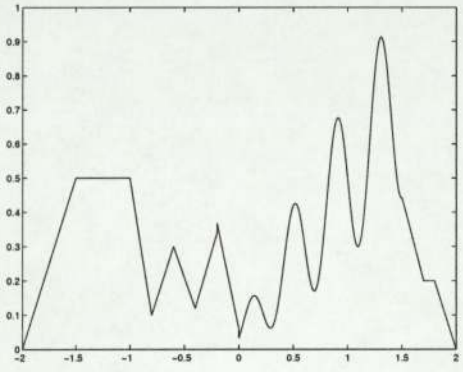


Figure 4.3: Sample Signal 1

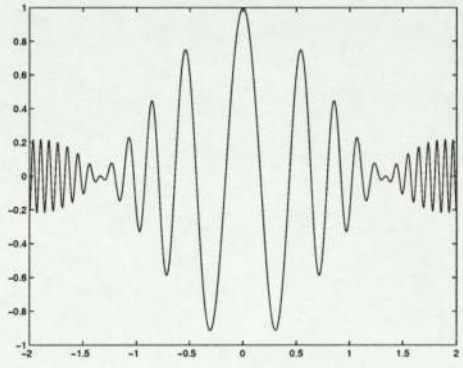


Figure 4.4: Sample Signal 2

The same code of real numbers will be used in all experiments. There is a limitation of how long such a code could be in this system - and that limit is exactly equal to the number of eigenvectors in Null(G) with G defined uniquely for the specific frame $\{f_k\}_{k=1}^{M}$ elementwise by

$$g_{m,n} = \langle f_n, f_m \rangle. \tag{4.6}$$

That is, high redundancy in the frame will allow a greater number of digits to be sent in this code.

Chapter 5

Application: Oversampled Fourier Expansion

Consider that we wish to transmit the signals shown in Figure 4.3 and Figure 4.4 and the hidden code $\vec{h}$ in Table 4.1 through the overcomplete Fourier expansion previously discussed in Section 3.1 given by

$$f(t) = \frac{\sqrt{a}}{\sqrt{2T}} \sum_{k=-M}^{M} c_k \, e^{\imath \frac{ak\pi t}{T}} \quad \text{for } t \in [-T, T],\ a \in (0, 1] \tag{5.1}$$

with

$$c_k = \frac{\sqrt{a}}{\sqrt{2T}} \int_{-T}^{T} f(t) \, e^{-\imath \frac{ak\pi t}{T}} \, dt. \tag{5.2}$$

Let us assume that for the case where $a = 1$, the number of coefficients needed to represent the signal f is $2M + 1 = 2N + 1$. Then we know that for $a \leq 1$, $M = \frac{N}{a}$. Therefore, our system will be completely described by N, $a \leq 1$, the signal-noise ratio S/N defined in (4.4), and ρ defined in (4.5).

5.1 Recovery of Signal and Code without Noise

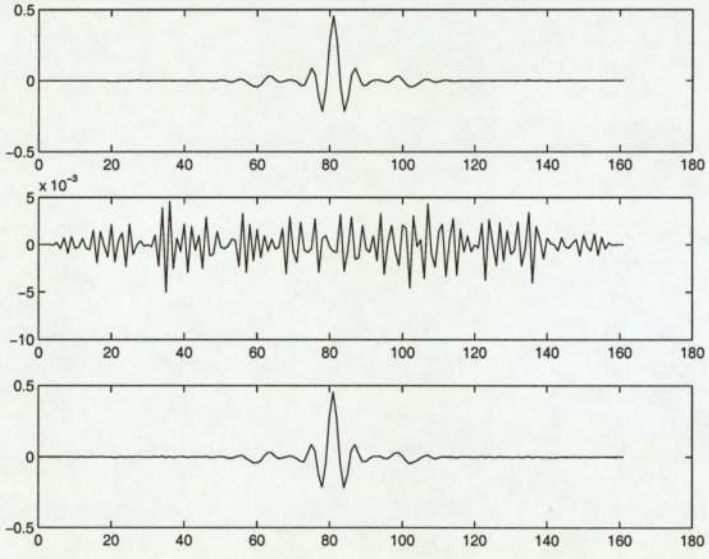
We start with the transmission of the signal and code in a system whereby $\vec{c'} = \vec{c} + \vec{c}$ is transmitted to the receiver without additional noise.

Signal 1: (No noise, $\rho = 100$, $N = 40$, $a = 0.5$)

We may achieve a very good recovery of the signal with the signal coefficients $\vec{c}$ plotted in Figure 5.1a. The hidden code coefficients $\vec{c'}$ are plotted in Figure 5.1b. The transmitted coefficients $\vec{c''} = \vec{c} + \vec{c'}$ are those of Figure 5.1c. In the absence of noise we can scale the $\vec{c'}$ to be arbitrarily small. The value $\rho = 100$ ensures that the hidden coefficients are sufficiently small relative to the signal coefficients (i.e. $\vec{c''} = \vec{c} + \vec{c'} \approx \vec{c}$). This would be useful if we wish to conceal the presence of the coefficients $\vec{c'}$.

As the theory has suggested, our decoding system is capable of reconstructing the hidden code up to the precision of the numerical calculations, although for space limitation reasons we have shown only 5 digits (see Table 5.1).

Figure 5.1: Fourier Coefficients for Signal 1 without Noise



Figures 5.1a-5.1c, from top to bottom. 5.1a depicts the signal coefficients, 5.1b the hidden code coefficients scaled to be small with respect to the signal coefficients, and 5.1c the transmitted coefficients (i.e. the sum of the previous two figures).

Table 5.1: Recovered Code without Noise

code	no noise $\rho = 100$
3.1492	3.1492
2.1271	2.1271
5.1312	5.1312
1.2835	1.2835
7.7976	7.7976
3.7160	3.7160
8.4139	8.4139
1.9791	1.9791
0.5863	0.5863
5.8321	5.8321
8.1032	8.1032
6.4908	6.4908

Signal 2: (No noise, $\rho = 100$, $N = 80$, $a = 0.5$)

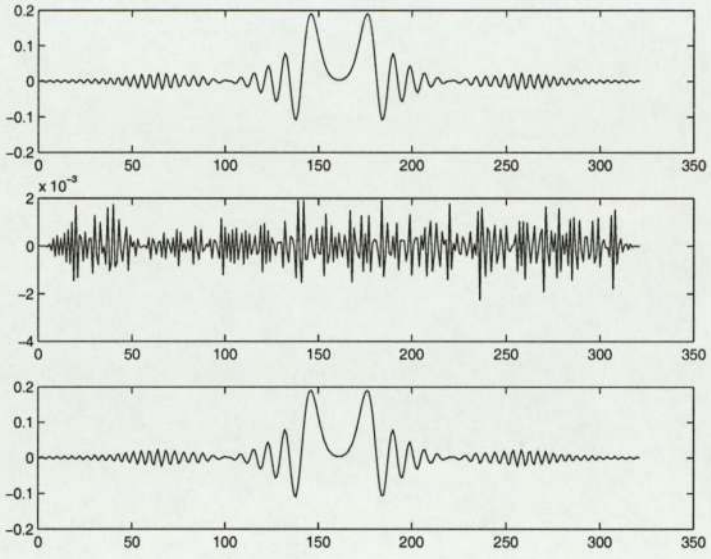
In this experimental setup, we achieve a very good recovery of the original signal with the signal coefficients $\vec{c}$ plotted in Figure 5.2a. The hidden code coefficients $\vec{c'}$ are plotted in Figure 5.2b and the transmitted coefficients $\vec{c''} = \vec{c} + \vec{c'}$ are those of Figure 5.2c. Once again, the code is recovered with accuracy limited only by the precision of the calculations involved (table not given).

Two primary observations that can be made with regard to the noiseless Fourier case:

1. Consistent with the theory previously discussed, the vector $\vec{c''}$ does indeed produce an identical signal to the coefficients $\vec{c}$ on the interval $[-T, T]$ (we will discuss what happens outside that interval in Section 5.3.3).

2. The code $\vec{h}$ can be recovered from the prescribed system with accuracy limited only by the precision of the calculations involved.

Figure 5.2: Fourier Coefficients for Signal 2 without Noise



Figures 5.2a-5.2c, from top to bottom. 5.2a depicts the signal coefficients, 5.2b the hidden code coefficients scaled to be small with respect to the signal coefficients, and 5.2c the transmitted coefficients (i.e. the sum of the previous two figures).

5.2 Recovery of Signal and Code with Noise

Now let us illustrate the effect of adding zero mean random Gaussian noise to the transmitted coefficients. As explained in Section 4.2, the quality of the recovery of our signal and hidden code depends on the variance of the noise (σ^2) relative to the size of the signal and hidden code coefficients respectively.

Signal 1: ($S/N = 20$ dB, $\rho \in \{0.1, 1, 10\}$, $N = 40$, $a = 0.5$)

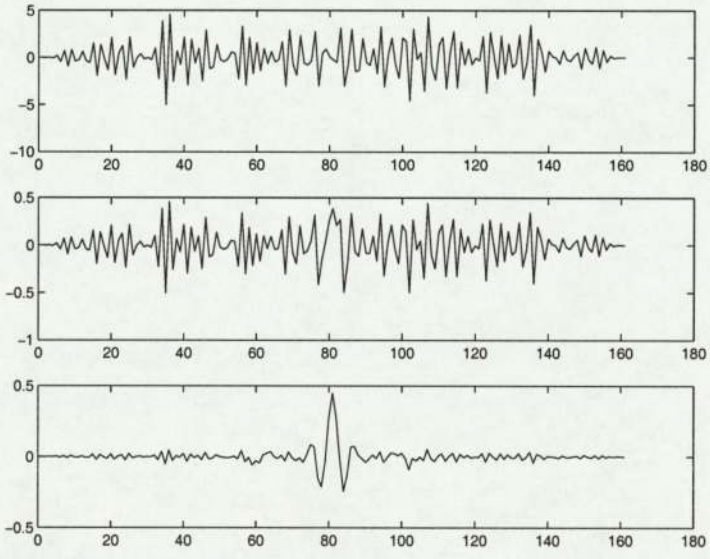
As previously discussed, there is a relationship between the signal-to-noise ratio, redundancy and quality of signal recovery. For most examples considered in this thesis, a signal-to-noise ratio of 20 dB has been chosen because it will allow for a signal recovery with a relatively small amount of noise distortion even for relatively large values of a, like the $a = 0.5$ used here. Once we are able to recover the signal, the focus shifts to the recovery of the code. We will consider three different values of ρ as defined in (4.5): 0.1, 1, and 10.

These three cases appear dramatically different in terms of the transmitted coef-

ficients, but will by definition, produce identical signal reconstructions. Let us recall that $\vec{c'}$ is by definition in Null(G), so these coefficients cannot affect the signal in any way. A plot of the three sets of transmitted coefficients is shown in Figure 5.3.

Note that in the case when $\rho = 0.1$ the transmitted coefficients are dominated by the size of the hidden coefficients (i.e. $\vec{c''} = \vec{c} + \vec{c'} \approx \vec{c'}$) which makes them 'visible' during the transmission, this has no effect whatsoever on the signal reconstruction. The same can be said, although to a slightly lesser degree, of the case where $\rho = 1$. Hence, in these cases the hidden code coefficients $\vec{c'}$ actually play a double role. On one hand they cover the coefficients $\vec{c}$ conveying the information for recovering the signal f and on the other hand they contain the information necessary to recover the hidden code. The recovered code for all three cases is shown in Table 5.2.

Figure 5.3: Transmitted Coefficients for Signal 1 for Fourier Frame with Noise



Figures 5.3a-5.3c, from top to bottom. 5.3a depicts the transmitted coefficients for $\rho = 0.1$, 5.3b shows the transmitted coefficients for $\rho = 1$ and 5.3c the transmitted coefficients for $\rho = 10$.

Table 5.2: Fourier - Recovered Code from Signal 1 with Noise

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.1501	3.1581	3.2383
2.1271	2.1272	2.1285	2.1412
5.1312	5.1319	5.1380	5.1995
1.2835	1.2832	1.2800	1.2490
7.7976	7.7965	7.7867	7.6887
3.7160	3.7169	3.7253	3.8088
8.4139	8.4142	8.4169	8.4438
1.9791	1.9797	1.9850	2.0382
0.5863	0.5862	0.5854	0.5776
5.8321	5.8329	5.8403	5.9142
8.1032	8.1029	8.1006	8.0777
6.4908	6.4906	6.4891	6.4737

Signal 2: ($S/N = 20$ dB, $\rho \in \{0.1, 1, 10\}$, $N = 80$, $a = 0.5$)

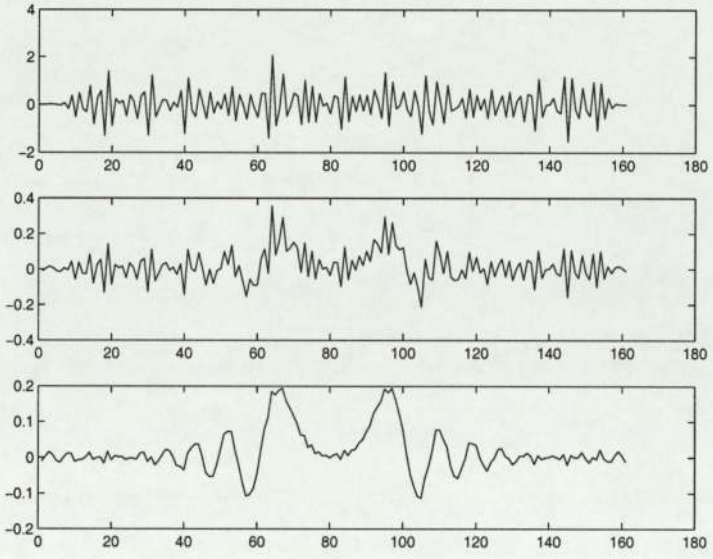
In reference to Signal 2, we find transmitted coefficients as shown in Figure 5.4 for the same three values of ρ and recovered code as shown in Table 5.3.

From these results we make the following observations:

1. The proposed encoding/decoding system is resilient in the face of a small amount of Gaussian noise. The system maintains its ability to recover the hidden code embedded in both of the signals used.

2. By changing the value of ρ (thereby scaling $\vec{c'}$ appropriately) we have some level of control over accuracy of the recovered code.

Figure 5.4: Transmitted Coefficients for Signal 2 for Fourier Frame with Noise



Figures 5.4a-5.4c, from top to bottom. 5.4a depicts the transmitted coefficients for $\rho = 0.1$, 5.4b shows the transmitted coefficients for $\rho = 1$ and 5.4c the transmitted coefficients for $\rho = 10$.

Table 5.3: Fourier - Recovered Code from Signal 2 with Noise

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.1504	3.1610	3.2668
2.1271	2.1326	2.1818	2.6745
5.1312	5.1331	5.1498	5.3175
1.2835	1.2846	1.2943	1.3913
7.7976	7.7994	7.8153	7.9741
3.7160	3.7154	3.7098	3.6540
8.4139	8.4100	8.3744	8.0190
1.9791	1.9755	1.9431	1.6194
0.5863	0.5860	0.5837	0.5607
5.8321	5.8351	5.8622	6.1335
8.1032	8.1010	8.0811	7.8821
6.4908	6.4901	6.4834	6.4165

5.3 Importance of Oversampling Parameter a

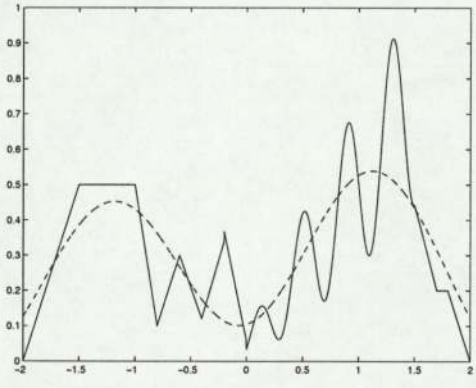
5.3.1 Recovery of Code Only

It is interesting to note that it is not necessary to have an accurate recovery of the signal to recover the hidden code through this system.

Signal 1: ($S/N = 20$ dB, $\rho = 1$, $N \in \{2, 40\}$, $a = 0.2$)

Recall that the previous signal reconstruction used $N = 40$ and we obtained a very good signal recovery. Now assume that we have no interest in the signal and hence choose to use only $N = 2$. Although if we oversample with $a = 0.2$, $M = N/a = 10$. If we once again use a small amount of noise at the level of $S/N = 20$ dB, the admittedly horrible recovery of the signal will look like that shown in Figure 5.5.

Figure 5.5: Poor Signal Recovery for Fourier Frame



Yet even with this woefully inadequate recovery of the signal, the recovery of the code through this system is remarkably good. If we compare the results with the code recovery for a system with $N = 40$ (and hence $2(N/a) + 1 = 401$ total terms with $a = 0.2$) we see in Table 5.4 that the less accurate signal reconstruction does not affect the code recovery greatly.

Table 5.4: Recovered Code - Poor Signal Recovery

code	$N = 2$	$N = 40$
3.1492	3.1296	3.1594
2.1271	2.1673	2.1315
5.1312	5.1461	5.1245
1.2835	1.3414	1.3096
7.7976	7.8149	7.8045
3.7160	3.7059	3.7319
8.4139	8.3966	8.4019
1.9791	2.0146	1.9904
0.5863	0.6040	0.5890
5.8321	5.7937	5.8308
8.1032	8.1281	8.1142
6.4908	6.5392	6.4983

5.3.2 Increased Redundancy vs. Code Recovery

As discussed in Section 4.2 as the redundancy increases the noise apparent in the signal reconstruction decreases. This, however is not the case for the hidden code. For the fixed $N = 40$, and $\rho = 1$ and $S/N = 10$ dB we compare the code recovery for two different values of a in Table 5.5 (recall that the signal recovery for these two cases was shown in Figure 4.1). Increased redundancy improves the signal reconstruction noticeably but has made minimal impact to the quality of reconstruction of the hidden code.

Therefore we make the following observations for a system as $a \to 0$:

- K (the size of the hidden code $\vec{h}$) may increase. This is because the upper limit on the number of numbers that may be sent in this coding system is exactly the size of Null(G). As redundancy increases the number of vectors in Null(G) increases as well.

- The signal reconstruction improves, but as shown in Section 5.3.1, there is not a tight relationship between the quality of signal reconstruction and the quality of the code recovery. The quality of code reconstruction is largely unchanged with increased redundancy.

Table 5.5: Recovered Code - Two different values of a

code	$a = 0.05$	$a = 0.5$
3.1492	3.1265	3.0661
2.1271	2.1319	2.1073
5.1312	5.1033	5.1013
1.2835	1.2928	1.2476
7.7976	7.7589	7.8460
3.7160	3.7377	3.6617
8.4139	8.3576	8.3950
1.9791	2.0156	1.9189
0.5863	0.5797	0.5765
5.8321	5.8048	5.8274
8.1032	8.0923	8.1097
6.4908	6.4298	6.4555

5.3.3 Recovery of Signal Only - IFFT

As discussed in Section 4.1, the receiver needs to know the particular frame expansion used in order to recover the signal and the code. In the case of an oversampled Fourier expansion, this amounts to knowing the value of $a \in (0, 1]$. In all of the previous applications it was assumed that the receiver knows the exact value for the oversampling parameter a, although for some signals it is possible to estimate the value of a by extending the signal reconstruction outside the interval $[-T, T]$.

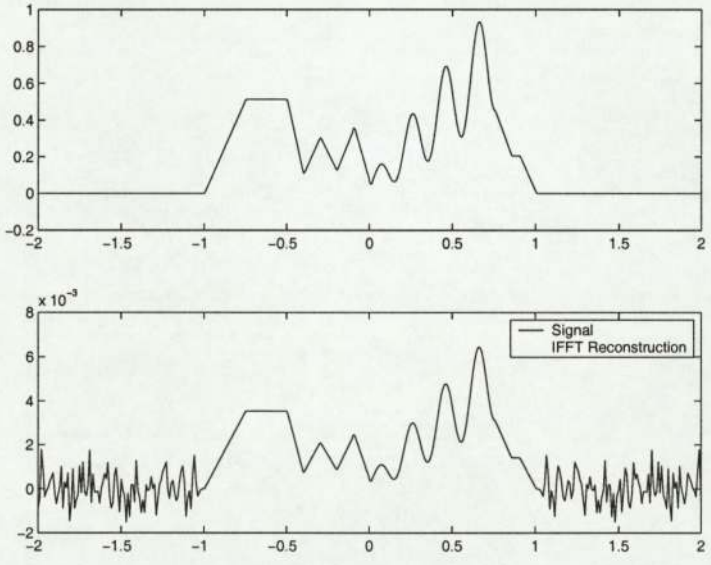
Note how the expansion in (5.1) was specifically limited to the interval $[-T, T]$. That is, of course, because the functions $e^{\imath\frac{ak\pi t}{T}}$ are periodic with period $2T/a$. Further recall the discussion in Section 3.1.2 regarding how the frame expansion assumes that the signal f is identically zero outside the interval $[-T, T]$. However, if one takes advantage of the periodicity of the complex exponentials $e^{\imath\frac{ak\pi t}{T}}$, an astute observer can approximate the value of a from the relative number of zeros that appear on either side of the signal. Let us now illustrate exactly how this might work.

Consider that we transmit the coefficients representing Signal 1 given in 5.1. It is not necessary to know the value of a to recover the signal. If we simply perform an IFFT on the signal $\vec{c}$ and transmitted coefficients $\vec{c'}$, we are able to recover the signal shown in Figure 5.6. Due to the oversampling, the desired signal is only a portion of what we

reconstruct. In the reconstruction from $\vec{c}$ seen in Figure 5.6a we see zeros on either side of our signal and in the reconstruction from $\vec{c''}$ shown in Figure 5.6b we see something else shows up in the region 'outside' the desired signal. Either way, now a may be estimated from the fraction of the 'signal' portion of the reconstruction divided by the total length of the reconstruction. In our case, it can be seen that the ratio is about 0.5.

It is interesting to note though that the reconstruction from $\vec{c''} = \vec{c} + \vec{c'}$ is not exactly zero outside the 'signal region'. In fact, this equates to the hidden coefficients $\vec{c'}$ being 'invisible' to the signal reconstruction on the interval $[-T, T]$, *not* for $|t| \in [T, T/a]$. This might prove to be misleading to the supposed intruder who recovers the signal without knowing our system. He/she might suppose that this is also part of signal (and hence not realize the oversampling used).

Figure 5.6: Recovery of Signal via IFFT



Figures 5.6a-5.6b, from top to bottom. 5.6a depicts the actual signal reconstruction from IFFT($\vec{c}$), 5.6b signal reconstruction from IFFT($\vec{c''}$)

5.3.4 Code Recovery with Estimated Value of a

Although the value of a is not necessary to reconstruct the signal, it is necessary to construct the matrix G (and hence the vector $\vec{c'}$). As shown in the previous section,

Table 5.6: Recovered code with using estimated value of a

code	$\tilde{a} = 0.45$	$\tilde{a} = 0.49$	$\tilde{a} = 0.5$	$\tilde{a} = 0.51$	$\tilde{a} = 0.55$
3.1492	2.9084	-0.3558	3.1492	-0.8148	-0.1612
2.1271	-0.3329	-2.4142	2.1271	0.3971	-0.9358
5.1312	0.6310	1.7099	5.1312	1.3653	1.3704
1.2835	4.3648	3.6917	1.2835	-2.8833	0.4765
7.7976	-0.2767	-1.6103	7.7976	0.9148	-2.5939
3.7160	-0.7192	3.5668	3.7160	2.1330	5.1632
8.4139	1.9982	-2.9628	8.4139	1.6322	2.3983
1.9791	-2.8462	-1.4827	1.9791	1.0098	0.9996
0.5863	-0.8905	1.4986	0.5863	5.1530	-3.3656
5.8321	1.2973	3.3235	5.8321	-0.0694	-2.6822
8.1032	2.0936	-0.3457	8.1032	2.7877	-0.2217
6.4908	2.1772	0.5635	6.4908	-2.7708	-0.8845

we can estimate the value of a via the IFFT (the estimate of a will be called $\tilde{a}$. In practice, however, it is not feasible to reconstruct the hidden code from $\tilde{a}$. That is, even very small values of $|a - \tilde{a}|$ lead to very large errors in the recovered hidden code. Observe the recovery of code when the value of $a = 0.5$ is perturbed by a small error like 0.05 or 0.01 as shown in Table 5.6. In fact, we have found that in order to recover the code one needs to know the value of a up to machine precision (i.e. $|a - \tilde{a}| \approx 10^{-16}$). The feature that extremely small perturbations yield extremely large errors is a typical effect of ill-posed problems.

5.4 An Additional Safeguard for the Hidden Code

We examine the case where we add another safeguard against recovery of the hidden code ($\vec{h}$ containing K elements). Recall that we previously defined

$$\vec{c'} = U\vec{h}$$

where U is a $(2M+1)\times K$ matrix, the columns of which are the K selected eigenvectors. We may instead consider

$$\vec{c'} = UB_s\vec{h}$$

where B_s is a $K \times K$ unitary random matrix. Note: the subindex s indicates the random generator used for constructing the matrix is initialized at state s. Such a state is needed to be known at the decoding stage. Hence, when the intended receiver goes to recover $\vec{h}$ they may do so by noticing that

- For constructing the matrix U one can use all eigenvectors of the matrix G corresponding to eigenvalues less than a previously specified tolerance parameter. Matrix U is unitary, i.e. $U^{-1} = U^*$ and then we have $B_s\vec{h} = U^*\vec{c'}$ where U^* indicates the transpose conjugate of matrix U.

- The dimension of matrix B_s can be determined from the number of non-zero components of vector $U^*\vec{c'}$. Thereby, state s allows the reproduction of the random matrix B_s. Since this is also a unitary matrix, $B_s^{-1} = B_s^*$.

Hence the vector $\vec{h}$ is obtained as:

$$\vec{h} = B_s^*U^*\vec{c'}.$$

Let us now see how this addition of the random matrix B_s affects the recovery of the signal and hidden code. Consider the case where $a = 0.2$, $N = 40$, $S/N = 20$ dB and $\rho = 1$ which yields the recovered code shown in Table 5.7. The second column of Table 5.7 shows the results when B_s is the identity matrix and the third column shows the code recovery when B_s is a randomized matrix with initialization value s.

This method allows for an additional layer of protection for the hidden code, with

Table 5.7: Recovered Code with Random Matrix B_s

code	$B_s = I$	$RandomB_s$
3.1492	3.1594	3.1317
2.1271	2.1315	2.1391
5.1312	5.1245	5.1392
1.2835	1.3096	1.2887
7.7976	7.8045	7.7916
3.7160	3.7319	3.7148
8.4139	8.4019	8.4196
1.9791	1.9904	1.9856
0.5863	0.5890	0.5878
5.8321	5.8308	5.8257
8.1032	8.1142	8.0946
6.4908	6.4983	6.4737

at minimal cost (i.e. the initialisation value s). Accuracy in the signal and code reconstruction is largely unaffected by this safeguard.

5.5 Summary of Results

A Fourier expansion provides a natural way to take an orthonormal basis and then alter it so as to make an overcomplete frame capable of transmitting hidden information in a novel way. In the absence of noise, the accuracy of the recovery is only limited by the precision of the calculations involved. When there is a small amount of noise, the code may still be recovered, with precision affected primarily by the relative size of the hidden coefficients to that noise. The highly efficient and well-known fast Fourier transform may also be utilised in both sending and recovering the signal and hidden information as described in Section 3.1.2.

The recovery of both the signal and code is possible with accuracy limited only by the size of the noise with respect the coefficients $\vec{c}$ and $\vec{c'}$ respectively, but only the code is substantially hidden. The recovery of the signal is straightforward (for both the intended receiver and anyone else) with a simple application of an IFFT. Once the signal has been recovered, the value of the oversampling parameter a may be estimated, although not with sufficient accuracy to recover the code. In fact, accurate recovery of

the code requires that the value of a needs to be known exactly.

Therefore, even though we can get a rough estimate of a from the signal reconstruction, the estimate can not possibly be of sufficient accuracy to recovery the code. Therefore, the value of a in this system will need to be predetermined instead of either being transmitted (with added error) or estimated from the signal reconstruction. It is therefore concluded that the Fourier case, because of its common use and efficient FFT algorithm, likely provides a very good framework for exploring such a coding system.

Chapter 6

Application: Gabor Frames

Here we will employ the methods outlined in 3.2 for the frame expansion to represent the signal. As previously discussed, the frame is $\{g_{m,n}\}_{m,n\in\mathbb{Z}}$ defined by

$$g_{m,n}(x) = e^{2\pi\imath max} g(x - nb) \quad a, b \in \mathbb{R}^+, \; g \in L^2(\mathbb{R}) \tag{6.1}$$

which also satisfies the frame condition (2.3). We will consider g a Gaussian with mean x_0 and standard deviation σ_x.

$$g(x) = \frac{1}{\sigma_x\sqrt{2\pi}} e^{-\frac{(x-x_0)^2}{2\sigma_x^2}}$$

with $x_0 = 0$, $\sigma_x = 0.4$.

Recall that we have discussed two ways of computing the coefficients c_k.

1. For any frame $\{f_k\}_{k=1}^M$ the coefficients $c_k = \langle f, S^{-1}f_k\rangle$ may be computed via the pseudo-inverse of the pre-frame operator by

$$T^\dagger f = \{\langle f, S^{-1}f_k\rangle\}_{k=1}^M. \tag{6.2}$$

where the operator T was defined by

$$T\{c_k\}_{k=1}^M = \sum_{k=1}^M c_k f_k.$$

This will be referred to the *general case* or the *pseudo-inverse method.*

2. In the case where $\{f_k\}_{k=1}^M$ forms a tight frame (which we used exclusively in Chapter 5), we may compute the coefficients c_k of the expansion $f = \sum_{k=1}^M c_k f_k$ as

$$c_k = \frac{1}{A}\langle f, f_k \rangle \tag{6.3}$$

where A is the frame bound. In this chapter and Chapter 7 we will only deal with general frames, but we will also compute the coefficients as in (6.3) and refer to it as a *tight approximation.* We choose to do this because of our preference for the compuational methods utilised for tight frames. We then attempt to see if the more straightforward computations of this estimation (which do not require inversion of the frame operator S) will yield an adequate representation of either the signal or code.

For the computation of the pseudo-inverse we will use a tolerance of 10^{-7}, i.e. any singular value less than this tolerance will be treated as zero. We will continue in both this chapter and Chapter 7 to compute the coefficients, signal reconstruction and code recovery using both the appropriate method for the general case and the tight approximation to compare the results.

6.1 Recovery of Signal and Code with Noise

Signal 1: $a = 2$, $b = 0.25$, $S/N = 20$ dB, $\rho \in \{0.1, 1, 10\}$, $m \in \{0, \pm 1 \pm 2, \pm 3, \pm 4\}$, $n \in \{0, \pm 1, \ldots, \pm 20\}$

This problem setup will give us a total number of coefficients $M = 369$ where 208 of those have singular values less than our tolerance of 10^{-7}. We see in Figure 6.1 the signal recovery is very good from the pseudo-inverse method but the tight approximation is inadequate.

The associated signal and hidden code coefficients for the pseudo-inverse method are shown in Figure 6.2. Notice how many coefficients we are using in this case compared to the Fourier, and how very few coefficients are significantly close to zero in 6.2a.

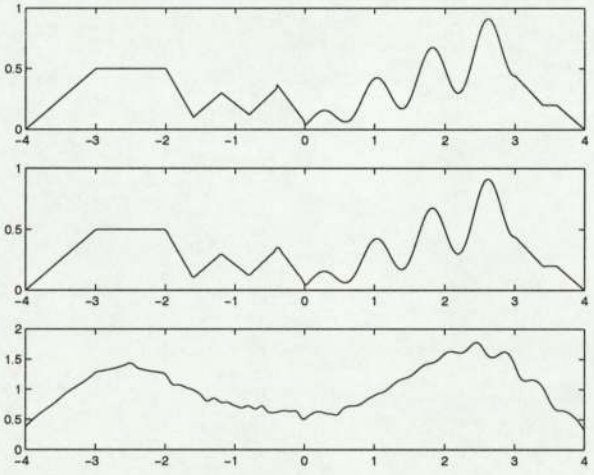
The code recovery shown in Table 6.1, however, is roughly the same as was achieved

Table 6.1: Gabor - Recovered code from Signal 1

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.1478	3.1353	3.0105
2.1271	2.1255	2.1107	1.9628
5.1312	5.1337	5.1562	5.3816
1.2835	1.2810	1.2589	1.0376
7.7976	7.7956	7.7773	7.5944
3.7160	3.7115	3.6712	3.2684
8.4139	8.4150	8.4244	8.5189
1.9791	1.9792	1.9799	1.9873
0.5863	0.5892	0.6149	0.8721
5.8321	5.8323	5.8339	5.8500
8.1032	8.1054	8.1251	8.3227
6.4908	6.4949	6.5314	6.8965

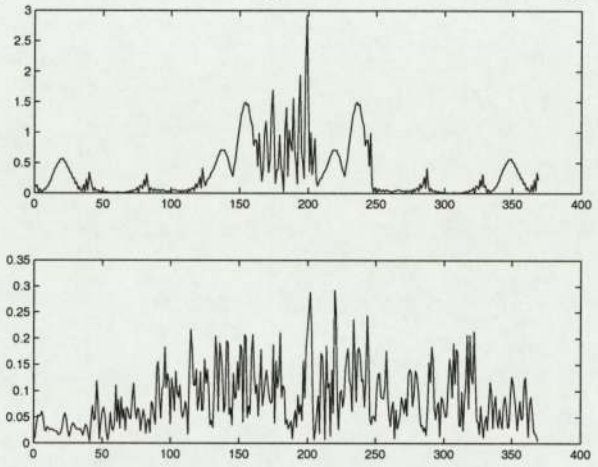
from the oversampled Fourier frame, as can be seen in Table 5.2.

Figure 6.1: Signal 1 Reconstruction from Gabor Frame



Figures 6.1a-6.1c, from top to bottom. 6.1a depicts Signal 1, 6.1b the recovered signal through the equation through the pseudo-inverse method and 6.1c the recovered signal from the tight approximation

Figure 6.2: Gabor - Signal coefficients for Signal 1



Figures 6.2a-6.2b, from top to bottom. Plot of modulus of the 6.2a signal coefficients and 6.2b hidden code coefficients in the general case. Sorted in ascending order of m and n respectively.

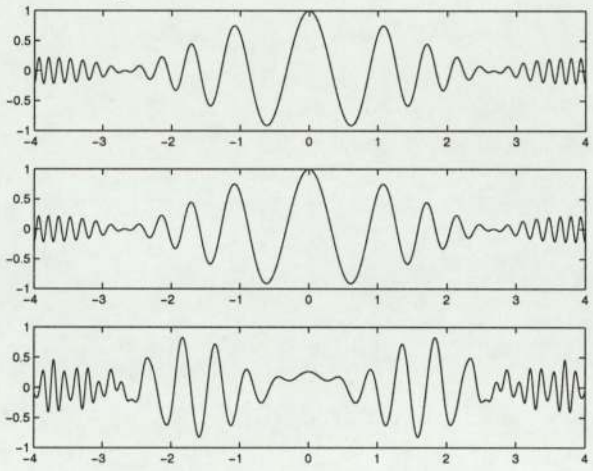
Signal 2: $a = 2$, $b = 0.25$, $S/N = 20$ dB, $\rho \in \{0.1, 1, 10\}$, $m \in \{0, \pm 1 \pm 2, \pm 3, \pm 4\}$, $n \in \{0, \pm 1, \ldots, \pm 20\}$

We see in Figure 6.3 the signal recovery for both the pseudo-inverse and tight frame approximation. The tight approximation shown in Figure 6.3c is a little better than seen with the previous signal, but still not very good. We therefore conclude that this frame setup (which is the same as used in the analysis of Signal 1) is not substantially tight.

The coefficients for the general (pseudo-inverse) case are shown in Figure 6.4 (6.4a shows the signal coefficients and 6.4b shows the hidden code coefficients).

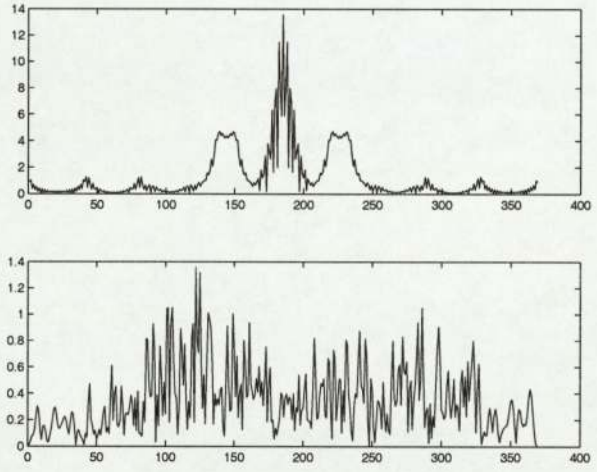
The code recovery from the general case is shown in Table 6.2 and the accuracy is similar to what we saw in the Fourier case (in Table 5.3).

Figure 6.3: Signal 2 Reconstruction from Gabor Frame



Figures 6.3a-6.3c, from top to bottom. 6.3a depicts Signal 2, 6.3b the recovered signal through the pseudo-inverse method, and 6.3c the recovered signal from the tight approximation

Figure 6.4: Gabor - Signal and Code Coefficients for Signal 2



Figures 6.4a-6.4b, from top to bottom. Plot of modulus of the 6.4a signal coefficients and 6.4b hidden code coefficients in the general case. Sorted in ascending order of m and n respectively.

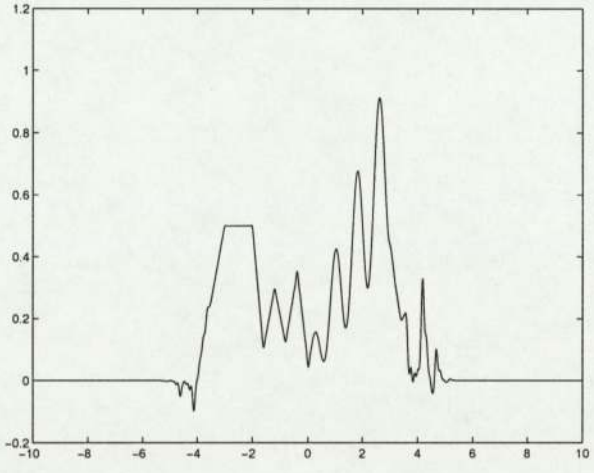
Table 6.2: Gabor - Recovered Code from Signal 2

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.1515	3.1725	3.3826
2.1271	2.1294	2.1505	2.3616
5.1312	5.1334	5.1534	5.3536
1.2835	1.2819	1.2677	1.1252
7.7976	7.7986	7.8074	7.8953
3.7160	3.7191	3.7466	4.0221
8.4139	8.4170	8.4452	8.7274
1.9791	1.9758	1.9462	1.6500
0.5863	0.5829	0.5520	0.2433
5.8321	5.8298	5.8088	5.5989
8.1032	8.1025	8.0961	8.0320
6.4908	6.4925	6.5079	6.6620

6.2 Other Investigations

It is also interesting to note what happens if we extend the signal recovery outside of the interval $[-T, T]$. Recall that in the Fourier case the periodicity of the functions $e^{\imath \frac{ak\pi t}{T}}$ ensured that the signal would repeat with period $2T/a$. Because our chosen function g is a Gaussian (and hence local in time), this will not be the case here. In fact, outside the interval on which the signal is defined, the signal reconstruction goes to zero (except at the borders).

Figure 6.5: Gabor - Signal Reconstruction Outside $[-T, T]$



6.3 Summary of Results

The Gabor frame with function g as a Gaussian allowed for an adequate recovery of the signals and the code, albeit with more coefficients than in the Fourier case. Neither signal was well approximated by tight frame approximation. The code recovery in the Gabor case was similar to that achieved in the Fourier case.

We also note that although the results were not given here, the code recovery from the tight approximation of this non-tight frame does produce a good recovery of the code, even though it does not produce an accurate recovery the signal.

Chapter 7

Application: Mexican Hat Wavelets

Recall the definition of the Mexican hat wavelet frame as $\{\psi_{m,n}\}_{m,n\in\mathbb{Z}}$ for $L^2(\mathbb{R})$ consisting of functions of the form

$$\psi_{m,n}(x) = a^{-m/2}\psi(a^{-m}x - nb) \quad a, b \in \mathbb{R}^+$$

with

$$\psi(x) = \frac{2}{\sqrt{3}}\pi^{-1/4}(1-x^2)e^{-x^2/2}.$$

We will consider the values of $a = 2$, $b = 0.25$ which was reported in [4] to be a frame with bounds 13.091 and 14.183. The ratio of frame bounds $14.183/13.091 \approx 1$, so we will examine the frame signal reconstruction and signal coefficients through the pseudo-inverse and tight frame approximation as set up in Chapter 6.

7.1 Recovery of Signal and Code with Noise

Signal 1: $a = 2$, $b = 0.25$, $S/N = 20$ dB, $\rho = \{1, 10, 100\}$, $m \in \{0, 1, 2, 3\}$, $n \in \{0, \pm 1, \ldots, \pm N\}$ where N is defined by $N = 5(1/(2^m) - 1)/b$.

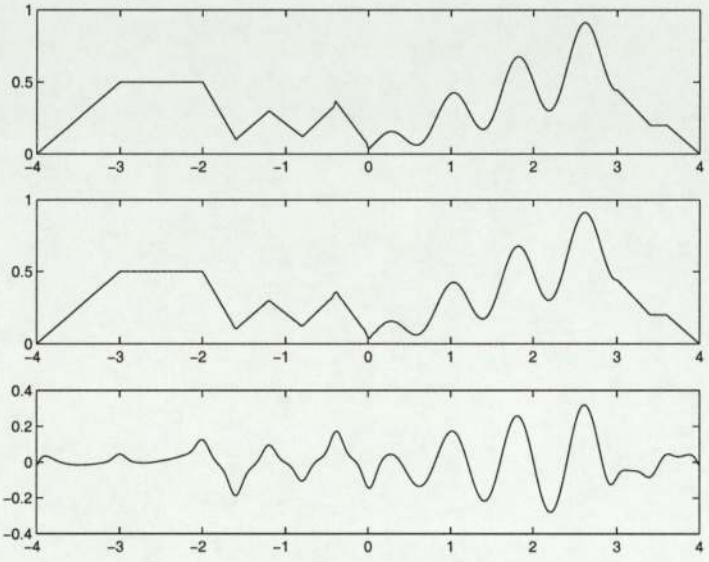
This will yield 1045 with 820 of which have singular values below the previously specified tolerance of 10^{-7}. The number of coefficients is far greater than used in either the Fourier or Gabor cases, but sufficiently represents the signal in the general case given in Figure 7.1b. The tight approximation shown in 7.1c is still not very good.

The associated signal and hidden code coefficients for the general case are shown in

Figure 7.2. As we see in the plot of Figure 7.2a there are a few large coefficients at the low scales (scale or m increases moving left to right) then a lot of high scale coefficients.

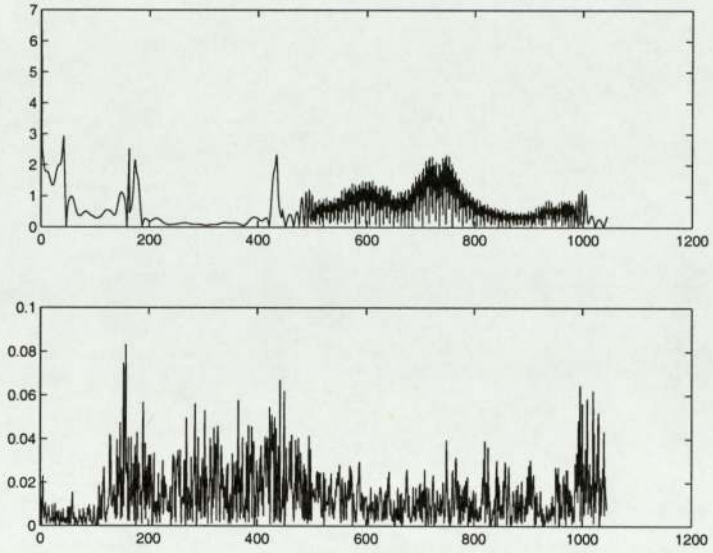
The code recovery is shown in Table 7.1 which when compared to the Fourier case in Table 5.2 we see the Mexican hat expansion appears to give a similar code recovery.

Figure 7.1: Signal 1 Reconstruction from Mexican Hat Frame



Figures 7.1a-7.1c, from top to bottom. 7.1a depicts Signal 1, 7.1b the recovered signal in the general case and 7.1c the recovered signal from the tight approximation

Figure 7.2: Mexican Hat - Signal 1 Coefficients



Figures 7.2a-7.2b, from top to bottom depicting the modulus of the signal and hidden code coefficients for the general case. Note that the coefficients are ordered in ascending order by m and n respectively.

Table 7.1: Mexican Hat - Recovered code from Signal 1

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.1503	3.1601	3.2578
2.1271	2.1264	2.1203	2.0589
5.1312	5.1328	5.1470	5.2895
1.2835	1.2836	1.2846	1.2950
7.7976	7.7972	7.7938	7.7596
3.7160	3.7180	3.7356	3.9122
8.4139	8.4119	8.3937	8.2123
1.9791	1.9776	1.9640	1.8279
0.5863	0.5859	0.5827	0.5505
5.8321	5.8325	5.8363	5.8739
8.1032	8.1035	8.1063	8.1342
6.4908	6.4902	6.4849	6.4315

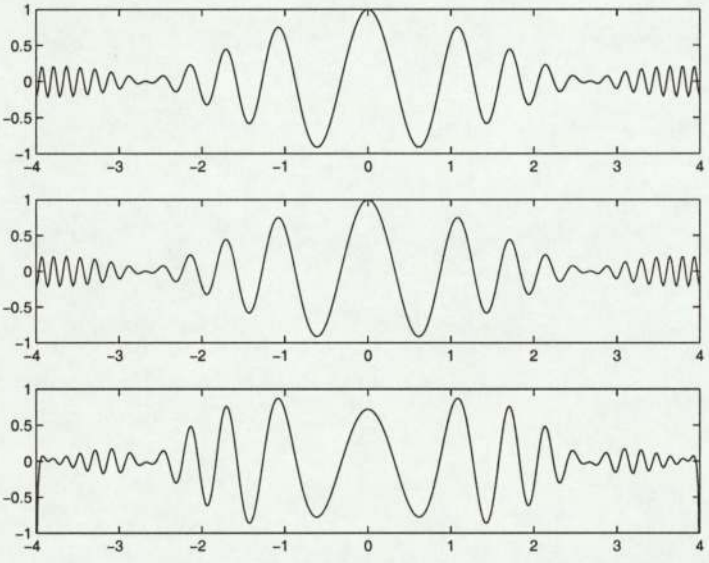
Signal 2: $a = 2$, $b = 0.25$, $S/N = 20$ dB, $\rho = \{1, 10, 100\}$, $m \in \{0, 1, 2, 3, 4\}$, $n \in \{0, \pm 1, \ldots, \pm N\}$ where N is defined by $N = 5(1/(2^m) - 1)/b$.

Here we see the closest match yet between the signal (Figure 7.3a) and the tight approximation of the signal recovery (Figure 7.3c). The recovery from the pseudo-inverse is shown Figure 6.3b and is still far superior to the tight approximation.

The associated signal and hidden code coefficients for the general case are shown in Figure 7.4. As we see in the plot of Figure 7.4a there are some large coefficients at the low scale (note that m increases moving left to right) then a lot of high scale coefficients of smaller magnitude.

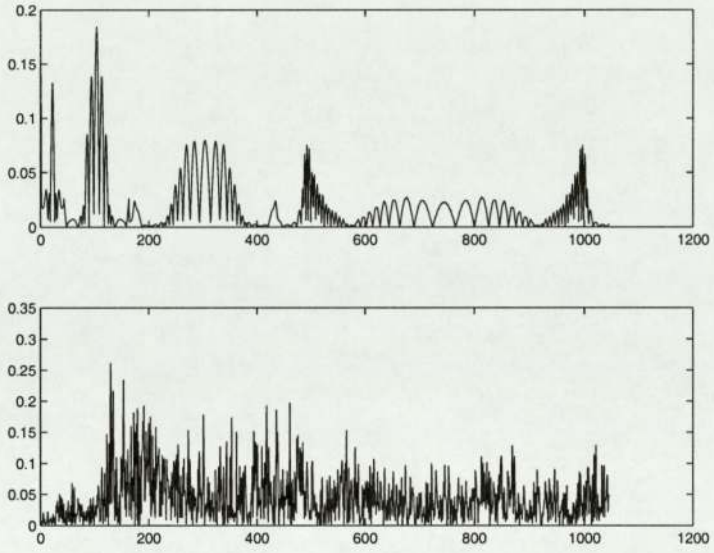
The code recovery is shown in Table 7.2 which when compared to the Fourier case in Table 5.3 and Table 6.2 we find that the recovery here is not as good as in either the Gabor of Fourier cases.

Figure 7.3: Signal 2 Reconstruction from Mexican Hat Frame



Figures 7.3a-7.3c, from top to bottom. 7.3a depicts Signal 2, 7.3b the recovered signal through the pseudo-inverse method and 7.3c the recovered signal from the tight approximation

Figure 7.4: Mexican Hat - Signal 2 Coefficients



Figures 7.4a-7.4b, from top to bottom depicting the modulus of the signal and hidden code coefficients for the general case. Note that the coefficients are ordered in ascending order by m and n respectively.

Table 7.2: Mexican Hat - Recovered code from Signal 2

code	$\rho = 0.1$	$\rho = 1$	$\rho = 10$
3.1492	3.2211	3.8682	10.3396
2.1271	2.3855	4.7107	27.9630
5.1312	5.0440	4.2597	-3.5842
1.2835	1.4452	2.9005	17.4535
7.7976	7.9956	9.7775	27.5965
3.7160	3.7938	4.4939	11.4946
8.4139	8.5550	9.8250	22.5248
1.9791	1.9589	1.7770	-0.0424
0.5863	0.5314	0.0377	-4.8998
5.8321	5.9817	7.3286	20.7967
8.1032	8.2156	9.2274	19.3455
6.4908	6.5963	7.5461	17.0434

7.2 Other Investigations

Like in the Gabor case, the lack of periodicity in the expansion functions means that outside the interval of $[-T, T]$ the signal reconstruction goes to zero except at the borders.

7.3 Summary of Results

The Mexican hat wavelet provides yet another frame expansion with which to examine the proposed system for transmitting a hidden code while sending a signal. Even though the ratio of frame bounds for the case used here is nearly 1, the estimation of this frame by the methods derived for use with tight frames yields an inadequate signal recovery. The number of coefficients used was much higher, and hence required a greater deal of computation time, but small changes in the values of a and b both have great impact on the number of coefficients needed. In addition the tolerance used to compute the pseudo-inverse has a very large impact on the signal coefficients and code recovery. The code recovery is similar to that achieved from the Fourier and Gabor for Signal 1, although was inferior for Signal 2.

Chapter 8

Conclusions

The fact that redundant representations are necessarily not unique has been used as a vehicle to transmit additional information. An encoding/decoding system was proposed that is capable of transmitting 1)an arbitrary signal, 2)a code of digits whose presence is not obvious in the signal reconstruction. The mathematical setting for such a development was the one provided by the theory of frames.

Three types of frames were examined - Fourier, Gabor and Mexican hat wavelets. As expected, in all three frame expansions the code was recovered to the level of machine accuracy in the case without noise. The presence of noise in the transmission channel has also been considered. It was seen that when a relatively small amount of zero-mean Gaussian noise is added to the transmitted coefficients the code may still be recovered within some error margin, which does not disqualify the procedure in the presence of noise.

Two different signals for transmitting an identical code were considered. Interestingly, in all three frame representations the code recovery with Signal 1 was largely similar across the fixed range of errors. However, with Signal 2 the accuracy of the code recovery was different - we found the accuracy from the Gabor and Fourier frames to be superior to that from the Mexican hat. In fact, for the most noisy case considered, only the Mexican hat reconstruction was not even accurate in the first digit. The signal recovery was shown to be dependent on the level of noise (signal-to-noise ratio) and the level of redundancy. - high redundancy yielding reduction of the noise.

Out of the three frames considered here, only the Fourier case formed a tight frame. The Gabor and Mexican hat wavelet dual frames were computed via a general (non-tight) method. The tight frame approximation was shown to be inappropriate in both types of frames. The number of coefficients used in each different expansion was wildly different in each case, with the smallest number needed in the Fourier case for both signals.

The quality of the signal reconstruction and level of redundancy used was found to have little effect on the accuracy in the recovery of the code. In fact, we examined a case where a very poor signal yielded a recovery of the code with a good deal of accuracy. This suggests the possibility of designing a more efficient coding system, resigning the goal of transmitting an arbitrary signal at the same time. This matter seems to be worth looking at and it is left as a proposal for future work.

From the experiments given here, the Fourier case appears to be the least costly. The main advantage is the fact that it can be implemented by a FFT tool, but this also seems to be the main weakness. Namely, by using the IFFT on the transmitted coefficients the oversampling and inclusion of hidden coefficients may become evident from the noisy ends in the reconstructed signal. However, even if the existence of hidden information were evident, the hidden code would be impossible to obtain without an exact value for the oversampling parameter. Additionally, a random transformation could be used to further protect the code.

The proposed encoding/decoding system seems to be difficult to crack, yet is completely indefensible against attacks. The hidden coefficients can easily be eliminated without destroying the information containing the signal. Hence it would be useful to consider more sophisticated redundant representations to prevent the easy elimination of the information relevant to the code.

Possible modifications and improvements

There are many forseeable extensions and/or modifications that could be made to this setup to make it more useful and practical for transmitting secret information. A few obvious and rather straightforward modifications that might yield to a system with appealing properties are:

- Although we defined the coefficients $\vec{c}$ to be the set of minimal l^2 norm it might also be possible to use some other definition, e.g. those of minimal l^1-norm. These coefficients and some of the properties associated with them are discussed in [2].

- The hidden code coefficients could be redefined such that the code $\vec{h}$ is encoded as the coefficients themselves. That is, if $\vec{h}$ consists of K numbers, then the first K elements in $\vec{c}$ could be exactly $\vec{h}$.

- The code could be used to carry some useful information about the signal, such that without it the recovered signal from the transmitted coefficients would be useless (or misleading).

Additional investigations are certainly needed so as to be able to evaluate whether the proposed encoding/decoding system could be transformed into one suitable for real-world scenarios. However, this project has produced evidence that redundant representations are worthy of consideration as a possibility in that direction. Some other suggestions for future work include: measurement and maximization of the efficiency of the system, other tight (and non-tight) frame expansions, and protection of the information containing the hidden code from distortion and/or data loss.

Appendix A

Time-Frequency Limitedness

A basic assumption of direct sampling is that the signal to be sampled is *band-limited.* A band-limited function is one where

$$\hat{f}(\lambda) = 0 \text{ for } |\lambda| > \omega.$$

When ω is the smallest frequency for which the preceding equation is true, the natural frequency

$$\nu = \frac{\omega}{2\pi}$$

is called the *Nyquist frequency* [1]. However, this assumption presents a bit of a dilemma. On the one hand, it is intuitive that practical signals can have neither infinite duration nor infinite bandwidth; yet, on the other hand, fundamental mathematical considerations preclude the existence of simultaneously time-limited and bandlimited signals. This is the so-called paradox of simultaneously time-limited and bandlimited signals. One cause of this paradox comes from the very concept of limitedness itself, that is, the idea that a signal is *exactly* zero outside some finite interval. From a practical viewpoint, it is not possible to measure a signal to enough accuracy to determine if it is exactly zero and, hence, assuming so is nothing more than a mathematical convenience. An assumption of limitedness has ramifications that may lead to various paradoxes and must therefore be used with caution. Even so, it is undeniable that real-world signals are of finite duration [10]. In defence of this paradox, we offer the result of the Shannon-Whittaker Sampling Theorem [1].

Shannon-Whittaker Sampling Theorem

Theorem A.1. *(Shannon-Whittaker Sampling Theorem) Suppose that $\hat{f}(\lambda)$ is piecewise smooth, continuous, and bandlimited for some fixed, positive frequency ω. Then f is completely determined by its values at the points $t_j = j\pi/\omega, j \in \mathbb{Z}$. More precisely, f has the following series expansion:*

$$f(t) = \sum_{j=-\infty}^{\infty} f(t\pi/\omega) \frac{\sin(\omega t - j\pi)}{(\omega t - j\pi)} \tag{A.1}$$

where the series on the right converges uniformly.

Proof: Using a standard Fourier expansion of $\hat{f}(\lambda)$ in a Fourier series on the interval $[-\omega, \omega]$:

$$\hat{f}(\lambda) = \sum_{k=-\infty}^{\infty} c_k e^{\imath\pi k\lambda/\omega}, \quad c_k = \frac{1}{2\omega} \int_{-\omega}^{+\omega} \hat{f}(\lambda) e^{-\imath\pi k\lambda/\omega} d\lambda.$$

Since $\hat{f}(\lambda) = 0$ for $|\lambda| \geq \omega$, the limits in the integrals defining c_k can be changed to $-\infty \ldots \infty$:

$$c_k = \frac{\sqrt{2T}}{2\omega} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(\lambda) e^{-\imath\pi k\lambda/\omega} d\lambda.$$

As defined in 3.1,

$$c_k = \frac{\sqrt{2\pi}}{2\omega} f(-k\pi/\omega).$$

If we use this expression for c_k in the preceding series, and if at the same time we change the summation index from k to $j = -k$, we obtain

$$\hat{f}(\lambda) = \frac{\sqrt{2\pi}}{2\omega} \sum_{j=-\infty}^{\infty} f(j\pi/\omega) e^{-\imath\pi j\lambda/\omega}. \tag{A.2}$$

Since $\hat{f}$ is a continuous, piecewise smooth function, the series A.2 converges uniformly [1]. Using the definitions in 3.1 again, we have

$$\begin{aligned} f(t) &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(\lambda) e^{\imath\lambda t} d\lambda \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\omega}^{+\omega} \hat{f}(\lambda) e^{\imath\lambda t} d\lambda \text{ since } \hat{f}(\lambda) = 0 \text{ for } |\lambda| > \omega. \end{aligned}$$

Using A.2 for $\hat{f}$ and interchanging the order of integration and summation, we obtain

$$f(t) = \sum_{j=-\infty}^{\infty} \frac{\sqrt{2\pi}}{2\omega} f(j\pi/\omega) \frac{1}{\sqrt{2\pi}} \int_{-\omega}^{+\omega} e^{-\imath\pi j\lambda/\omega + \imath\lambda t} d\lambda. \tag{A.3}$$

The integral in A.1 is

$$\int_{-\omega}^{+\omega} e^{-\imath\pi j\lambda/\omega+\imath\lambda t} d\lambda = 2\frac{\omega \sin(t\omega - j\pi)}{t\omega - j\pi}$$

which leads directly to A.1 after a small amount of algebra [1]. □

Bibliography

[1] Boggess, A. and Narcowich, F.J., *A First Course in Wavelets with Fourier Analysis*, Prentice Hall, Upper Saddle River, NJ 2001.

[2] Christensen, O., *An Introduction to Frames and Riesz Bases*, Birkhauser, Boston, MA 2002.

[3] Cvetkovic, Z., Vetterli, M., *Tight Weyl-Heisenberg Frames in* $l^2(\mathbb{Z})$ IEEE Trans. Signal Processing 46, 1256-1259, 1998.

[4] Daubechies, I., *Ten Lectures on Wavelets*, SIAM, Philadelphia, PA 1992.

[5] Daubechies, I., *The wavelet transformation, time-frequency localization and signal analysis*, IEEE Trans. Inform. Theory 36, 961-1005, 1990.

[6] Feichtinger, H., Strohmer, T., *Gabor Analysis and Algorithms*, Birkhauser, Boston, MA 1998.

[7] Jansen, M., *Noise Reduction by Wavelet Thresholding*, Springer-Verlag, New York, NY 2001.

[8] Rebollo-Neira, L., Constantinides, A.G., *Power spectrum estimation from noisy autocorrelations* Signal Processing 50, 223-231, 1996.

[9] Shen, W., *Wavelets and Other Orthogonal Systems*, Second Edition, Chapman and Hall, Boca Raton, FL 2001.

[10] Teolis, A., *Computational Signal Processing with Wavelets*, Birkhauser, Boston, MA 1998.

[11] Vetterli, M. and Kovacevic, J., *Wavelets and Subband Coding*, Prentice Hall, Englewood Cliffs, NJ 1995.

[12] Young, R.M. *An Introduction to Nonharmonic Fourier Series*, Revised First Edition, Academic Press, San Diego, CA 2001.