ON HIDING MESSAGES IN THE OVERSAMPLED FOURIER COEFFICIENTS

GHANSHYAM BHATT, LORRAINE KRAUS, LAURA WALTERS, AND ERIC WEBER

Abstract. A system using an oversampled Fourier transform for hiding data is given in [J.R. Miotke and L. Rebollo-Neira, Applied Comp. Harmonic Anal., 16 (2004) no. 3, 203–207]. When viewed as a cryptographic algorithm, we demonstrate here that the system is susceptible to a known plaintext attack.

1. Introduction

In [3], a system is developed using an oversampled Fourier transform to hide messages. We shall take the view here that this is an encryption algorithm. Strictly speaking, the system in [3] is proposed for hiding data which is already encrypted. However, we shall demonstrate here that for a typical application of this system the added security of the data hiding scheme is small.

Two principles guide our analysis of the proposed data hiding algorithm. First, Kerckoff's Law states that the security of a system should rely only on the secrecy of the key, not on the secrecy of the algorithm. Stated another way, we assume that an adversary knows the algorithm, but not the key. The second principle is that an encryption system should be robust against a known plaintext attack. This is where an adversary has a list of plaintexts with the corresponding ciphertexts, each encoded using the same key, from which the adversary tries to determine the key used, or more generally, how to decrypt future ciphertexts encrypted using the same key. [2]

We remark that a similar algorithm is proposed in [1], utilizing the orthogonality of certain pairs of frames. The algorithm there is susceptible to the same attack as the algorithm under consideration here.

2. Redundant Frame Scheme for Data Hiding

In the encoding process of [3], the authors propose oversampling the Fourier coefficients to create a space to hide information while transmitting (or storing) a signal. We shall describe the general idea here, and then address the actual implementation in [3] in the next section. Here H is a separable Hilbert space and $\mathbb{J}$ is a denumerable index set. Choose a frame $\mathbb{X} = \{x_j\}_{j \in \mathbb{J}} \subset H$ which is not a basis; let $\Theta_{\mathbb{X}}$ denote the analysis operator of the frame, i.e.

$$\Theta_{\mathbb{X}} : H \to l^2(\mathbb{J}) : x \mapsto (\langle x, x_j \rangle)_j.$$

Since $\mathbb{X}$ is not a basis, the operator $\Theta_{\mathbb{X}}^*$ has nontrivial kernel, say of dimension N. Let $U : l^2(\mathbb{Z}_N) \to l^2(\mathbb{J})$ be an isometric operator (i.e. has columns which are an orthonormal set) such that the range of U is contained in the kernel of $\Theta_{\mathbb{X}}^*$, that is $\Theta_{\mathbb{X}}^* U : l^2(\mathbb{Z}_N) \to H$ is the 0 operator.

Date: September 1, 2004.

The encoding process is as follows. Suppose $h \in l^2(\mathbb{Z}_N)$ is a message, or code, to be hidden; choose a vector $f \in H$, and compute the following:

$$c = \Theta_{\mathbb{X}} f + Uh.$$

The key to this system then is the frame $\mathbb{X}$, along with the operator U (in [3], U can be uniquely determined from $\mathbb{X}$). To decode h, the recipient applies U^* to c:

$$U^* c = U^* \Theta_{\mathbb{X}} f + U^* U h = h \tag{1}$$

since $U^* \Theta_{\mathbb{X}} = \Theta_{\mathbb{X}}^* U = 0$.

If $\mathbb{J}$ is finite, as it would be in any real world implementation, then an adversary can attack this system using a known plaintext attack. We consider h to be a plaintext, and c to be a ciphertext. The adversary collects a list of plaintext-ciphertext pairs $\{(h_i, c_i)\}$ so that $\{c_i\}$ is a basis for $l^2(\mathbb{J})$. The adversary then solves for U^* via the system of equations $\{U^* c_i = h_i\}$, knowing that Equation 1 is valid. Clearly, this system of equations has a solution since we know, a priori, that U exists, and moreover, the solution is unique. Having determined U^*, the adversary can then decode any hidden message which was encoded using the same pair $\mathbb{X}, U$.

3. Implementation Using Fourier Frames

In [3], the algorithm proposed uses $H = L^2[-T, T]$, and the frame is $\{e^{i\pi ant/T}\} \subset L^2[-T, T]$ for some $a \in (0, 1)$. The oversampling parameter a is the key for retrieving the hidden data. The matrix U is derived from the matrix G, which acts on $l^2(\mathbb{Z})$, given by

$$G_{m,n} = \frac{1}{2T} \int_{-T}^{T} e^{-i\pi amt/T} e^{i\pi ant/T} dt = \text{sinc } a(m-n)\pi.$$

Then, U is a matrix whose columns correspond to vectors in the nullspace of G.

The practical implementation then involves a $M \times M$ submatrix of G, which we still call G, and U an $M \times N$ matrix whose columns are the (normalized) eigenvectors corresponding to the N smallest eigenvalues of G (we assume that all of those eigenvalues are sufficiently small). Again, if $h \in l^2(\mathbb{Z}_N)$ is a message to be hidden, one computes M Fourier coefficients of a function $f(t) \in L^2([-T, T])$ by

$$c_m = \frac{a}{\sqrt{2T}} \int_{-T}^{T} f(t) e^{-i\pi amt/T} dt;$$

then Uh, and finally

$$\overrightarrow{c''} = \overrightarrow{c} + Uh,$$

where $\overrightarrow{c}$ is the vector of Fourier coefficients c_m.

Note that $\|GU\| \approx 0$, since the range of U corresponds to the subspace spanned by the eigenvectors of G with eigenvalue almost 0. The matrix G is a positive matrix, and is in fact the Gram matrix for the collection of functions $\{e^{iamt/T} : m = 0, \dots M-1\}$, which form a frame for their closed span. We can identify $\overrightarrow{c}$ with $\Theta_E f$, where Θ_E is the analysis operator for the collection of exponentials. We have the following:

- $G = \Theta_E \Theta_E^*$;
- $\|U^* \Theta_E\| \approx 0$ since $\|\Theta_E \Theta_E^* U\| \approx 0$, and the range of U corresponds to a space spanned by eigenvectors for G;

- $U^*\overrightarrow{c''} = U^*\Theta_E f + U^*Uh \approx h$. The reconstruction error $\|U^*\overrightarrow{c''} - h\|$ depends upon the magnitude of the eigenvalues of G to which U corresponds.

Therefore, we can apply a known plaintext attack to this system.

3.1. **Numerical Experiment.** In [3], they consider an example using 81 nonoversampled coefficients, an oversampling parameter of $a = \frac{1}{2}$, and the function $f(t) = \mathrm{sinc}(t-2)t^3$. They obtain a reconstruction error of 5.1×10^{-11}.

We ran a simulation of the known plaintext attack on their system using the same parameters. Since the attack requires a list of plaintext-ciphertext pairs, we use plaintexts of randomly generated numbers, and functions $f_j(t) = \mathrm{sinc}(t-2j)t^3$. After computing the matrix U^* and applying it to a new ciphertext, we obtain a reconstruction error of 1.1×10^{-13}.

Acknowledgement

The second and third authors are undergraduate students, and performed this work while supported by the NSF REU grant DMS-0353880. The fourth author was supported by NSF grant DMS-0355573.

References

1. R. Harkins, E. Weber, and A. Westmeyer, *Encryption schemes using finite frames and Hadamard arrays*, submitted, 2004.
2. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, 1996.
3. J. R. Miotke and L. Rebollo-Neira, *Oversampling of Fourier coefficients for hiding messages*, Appl. Comput. Harmon. Anal. **16** (2004), no. 3, 203–207.

Department of Mathematics, Iowa State University, 400 Carver Hall, Ames, IA 50011
E-mail address: gbhatt@iastate.edu

The College of New Jersey, Ewing, NJ 08628
E-mail address: kraus2@tcnj.edu

Culver-Stockton College, Canton, MO 63435
E-mail address: lawalters@culver.edu

Department of Mathematics, Iowa State University, 400 Carver Hall, Ames, IA 50011
E-mail address: esweber@iastate.edu