AN ALTERNATIVE SIGNATURE DESIGN USING L1 PRINCIPAL COMPONENTS FOR SPREAD-SPECTRUM STEGANOGRAPHY

Colleen P. Bailey[◇] *Shubham Chamadia*[†] *Dimitris A. Pados*[⋆]

[◇] University of North Texas
[†] Massachusetts General Hospital
[⋆] Florida Atlantic University

ABSTRACT

As methods for detecting hidden data evolve, there exits an ever increasing need to develop new steganographic solutions. This paper introduces novel spread spectrum (SS) and improved spread spectrum (ISS) multimedia data embedding techniques using L_1 principal component signatures. The design presented performs well in terms of bit error rate and the structural similarity index metric.

Index Terms— Steganography, spread-spectrum, L1 PCA, data hiding

1. INTRODUCTION

Steganography, data hiding, data embedding, and watermarking are all variants of a similar problem. All four describe the act of secretly embedding messages, signals, or other information into various forms of multimedia. The secret message is insterted into the original signal using some type of key or signature.

As opposed to many watermarking or cryptography systems, steganography aims not only to securely embed the hidden message, but also to hide the act of embedding. For images, this means embedding the message without any perceptual change between the host and stego images. In addition to being successfully hidden, the message must also be accurately recovered at the system output.

There are many areas of data hiding research including embedding procedure, key or signature design, as well as receiver/decoder selection. In general, embedding can be performed in either the data or transfer domain. Spread spectrum steganography is typically executed in some transform domain.

Cox et al. [1] originally introduced the concept of spread spectrum steganography with two basic methods for inserting the message, additive and multiplicative. Malvar and Florencio [2] improved additive spread spectrum by reducing the interference caused by the host itself. Gkizeli et al. [4] presented the optimal signature design for additive spread spectrum and improved spread spectrum when recovering the message using a maximum signal to interference plus noise filter at the receiver.

The signature design from [4] is based on L_2-norm principal component analysis (PCA). Since the introduction of optimal [5] and near optimal [6] L_1 PCA solutions, there has been a lot of interest in finding L_1-norm PCA based solutions to problems that have traditionally used L_2-norm PCA. Several applications potentially benefit from the outlier resistance provided by switching from L_2 to L_1. An alternative signature design for spread spectrum steganography utilizing L_1 PCA is developed in this paper.

2. SPREAD SPECTRUM EMBEDDING

The general spread spectrum embedding procedure for images begins with a host image $\mathbf{H}$ of dimension $M_1 \times M_2$ pixels with values taken from alphabet $\mathcal{M}$. For grayscale images, the alphabet takes values from 0 to 255 ($\mathcal{M} = \{0, 1, \ldots, 255\}$). The host image $\mathbf{H} \in \mathcal{M}^{M_1 \times M_2}$ can be viewed as a matrix of pixels. The matrix $\mathbf{H}$ is then divided into N blocks of size $m \times m$ for the purpose of embedding one bit per block. Next, a real two dimensional transform is applied to each block $\mathbf{H}_n$ for $n \in \{1, \ldots, N\}$ so that embedding can be carried out in a transform domain.

For image applications, the transform performed on each block is typically the $m \times m$ 2D-DCT (discrete cosine transform) that converts the matrix $\mathbf{H}$ from the data domain to frequency domain. The 2D-DCT produces a matrix of frequency coefficients arranged such that lower frequency coefficients are toward the upper left quadrant and high frequency components are in the lower right quadrant. Performing zigzag scanning vectorization of each transformed $m \times m$ block provides a $m^2 \times 1$ vector spanning the low to high frequency coefficients.

The resulting vectors $(\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_N)$ are concatenated to create a transform coefficient matrix. The final host vector matrix $X^{D \times N}$ is created by taking any row subset of the previous matrix. It is common practice in data embedding to remove the first row as it is the lowest frequency coefficient (or DC component) and any change affects the original image

the most. The secret message is to be hidden in the matrix $X^{D\times N}$.

3. SIGNATURE DESIGN

The standard basic spread spectrum embedding scheme is additive spread spectrum (SS). Information is embedded by adding the positive amplitude normalized signature manipulated message bits to the host in the presence of added white Gaussian noise (AWGN) with variance σ_n^2.

$$\mathbf{y} = Ab\mathbf{s} + \mathbf{x} + \mathbf{n} \tag{1}$$

where $A > 0$, $b \in \{\pm 1\}$, $\|\mathbf{s}\|_2 = 1$, and $\mathbf{n} \sim \mathcal{N}\left(\mathbf{0}, \sigma_n^2 \mathbf{I}_D\right)$. The mean-squared distortion caused by the embedding operation (not the noise) is as follows.

$$\mathcal{D} = E\{\|Ab\mathbf{s} + \mathbf{x} - \mathbf{x}\|^2\} = A^2 \tag{2}$$

Message bits are recovered at the receiver using a simple matched filter.

$$\hat{\boldsymbol{b}} = \text{sign}(\mathbf{s}^T\mathbf{y}) \tag{3}$$

To improve on the basic additive scheme, improved spread spectrum (ISS) offers superior performance by reducing the interference to the signal of interest ($Ab\mathbf{s}$) caused by the host ($\mathbf{x}$). The parameter λ is introduced to direct the host interference removal.

$$\mathbf{y} = Ab\mathbf{s} + (\mathbf{I}_D - \lambda\mathbf{s}\mathbf{s}^T)\mathbf{x} + \mathbf{n} \tag{4}$$

where $A > 0$, $b \in \{\pm 1\}$, $\|\mathbf{s}\|_2 = 1$, $0 < \lambda < 1$, and $\mathbf{n} \sim \mathcal{N}\left(\mathbf{0}, \sigma_n^2 \mathbf{I}_D\right)$. Note that SS can be viewed as a special ISS case for $\lambda = 0$. The distortion due only to the embedding operation in the mean-squared sense for ISS is

$$\mathcal{D} = E\{\|Ab\mathbf{s} + (\mathbf{I}_D - \lambda\mathbf{s}\mathbf{s}^T)\mathbf{x} - \mathbf{x}\|^2\} = A^2 + \lambda^2\mathbf{s}^T\mathbf{R}_x\mathbf{s} \tag{5}$$

where the autocorrelation $\mathbf{R}_x = E\{\mathbf{x}\mathbf{x}^T\}$. The λ that minimizes the probability of error for any distortion level $\mathcal{D}$ is

$$\lambda = \frac{\mathbf{s}^T\mathbf{R}_x\mathbf{s} + \sigma_n^2 + \mathcal{D} - \sqrt{\left(\mathbf{s}^T\mathbf{R}_x\mathbf{s} + \sigma_n^2 + \mathcal{D}\right)^2 - 4\mathbf{s}^T\mathbf{R}_x\mathbf{s}\mathcal{D}}}{2\mathbf{s}^T\mathbf{R}_x\mathbf{s}} \tag{6}$$

Similar to SS, message bits can be recovered using a simple matched filter.

$$\hat{\boldsymbol{b}} = \text{sign}(\mathbf{s}^T\mathbf{y}) \tag{7}$$

The previous schemes, SS and ISS, typically utilize arbitrary signatures. When the signature is optimized to maximize the signal to interference plus noise ratio (SINR) filter at the receiver, the performance dramatically improves. Finding the optimal signature amounts to the eigenvalue decomposition (EVD) of $\mathbf{R}_x$ where is eigenvector corresponding to the smallest eigenvalue is that signature. The EVD of the host autocorrelation matrix is equivalent to the singular value decomposition (SVD) of the host matrix $\mathbf{X}$ in the L_2-norm sense. Another way to view the maxSINR optimal signature design is as the solution to the following L_2 norm principal component analysis (PCA) problem.

$$\mathbf{s}_{L_2} = \underset{s\in R^{D\times 1},\, \|s\|_2=1}{arg\,min} \|\mathbf{s}^T\mathbf{X}\|_2 \tag{8}$$

In steganographic and PCA terms, finding the optimal signature is equivalent to finding the principal component that *least* describes the host. The transition from the L_2 norm problem to a L_1 norm signature design problem begins with a brute force switch.

$$\mathbf{s}_{L_1} = \underset{s\in R^{D\times 1},\, \|s\|_2=1}{arg\,min} \|\mathbf{s}^T\mathbf{X}\|_1 \tag{9}$$

The above problem of finding the L_1 principal component that *least* describes the data has no known solution. Optimal and suboptimal solutions do exist to the problem of finding the L_1 principal component that *most* describes the host data.

$$\mathbf{s}_{L_1} = \underset{s\in R^{D\times 1},\, \|s\|_2=1}{arg\,max} \|\mathbf{s}^T\mathbf{X}\|_1 \tag{10}$$

An iterative solution can be used to approximate the solution to the original problem (9).

$$\mathbf{s}_{L_1} = \underset{s\in R^{D\times 1},\, \|s\|_2=1}{arg\,max} \|\mathbf{s}^T\mathbf{X}\|_1 \quad \longleftrightarrow \quad \mathbf{X} = \mathbf{X} - \mathbf{s}_{L_1}\mathbf{s}_{L_1}^T\mathbf{X} \tag{11}$$

The process involves finding the L_1 principal component that *most* describes the data, subtracting it from the data via orthogonal projection, then repeating with the new data matrix for some desired number of iterations.

Algorithm 1 L1 Signature Generation

1: **Input:** $\mathbf{X}_{D\times N}$ data matrix, $K \leq \text{rank}(\mathbf{X})$
2: **for** $k \leftarrow K$ **do**
3: $\quad \mathbf{b} \leftarrow \text{findL1}\left(\mathbf{X}, sign([\mathbf{X}^T\mathbf{X}]_{:,1})\right)$
4: $\quad \mathbf{q} = \mathbf{X}\mathbf{b}/\|\mathbf{X}\mathbf{b}\|_2$
5: $\quad \mathbf{X} = \mathbf{X} - \mathbf{q}\mathbf{q}^T\mathbf{X}$
6: **end for**
7: **Output:** $\mathbf{s}_{L_1} = \mathbf{q}$

The function $\text{findL1}(\cdot)$ can be any algorithm that calculates L_1 principal components. The embedding scheme and decoder equations are updated for the L_1 signature. For the SS scheme, the following equation describes the received signal.

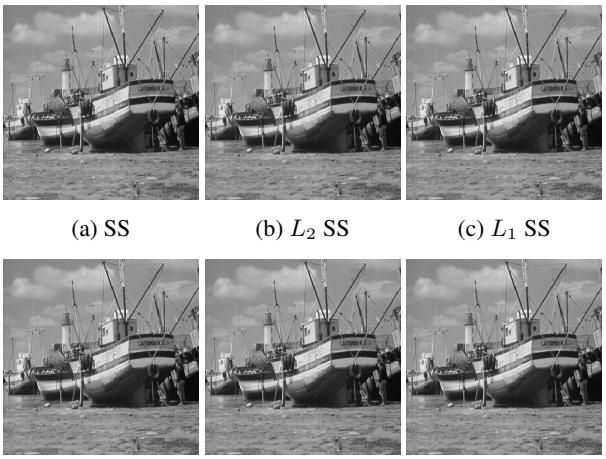
$$\mathbf{y} = Ab\mathbf{s}_{L_1} + \mathbf{x} + \mathbf{n} \tag{12}$$

Information bit recovery is performed using the maxSINR filter at the receiver.

$$\hat{\boldsymbol{b}} = \text{sign}(\mathbf{w}_{maxSINR}^T\mathbf{y}) \tag{13}$$

where $\mathbf{w}_{maxSINR} = (\mathbf{R}_x + \sigma_n^2\mathbf{I}_D)^{-1}\mathbf{s}_{L_1}$.

Fig. 1: Fishing Boat (512 × 512 grayscale)



(a) SS (b) L_2 SS (c) L_1 SS

(d) ISS (e) L_2 ISS (f) L_1 ISS

Fig. 2: Fishing Boat with 4096 Embedded Information Bits at $\mathcal{D} = 20$dB and AWGN $\sigma_n^2 = 3$dB

The improved spread spectrum scheme is also updated for a L_1 signature. Here the host influence removal is handled by the parameter k.

$$\mathbf{y} = Ab\mathbf{s}_{L_1} + (\mathbf{I}_D - k\mathbf{s}_{L_1}{\mathbf{s}_{L_1}}^T)\mathbf{x} + \mathbf{n} \tag{14}$$

The maxSINR filter receiver is used to retrieve the embedded information bits.

$$\hat{\boldsymbol{b}} = \text{sign}(\mathbf{w}_{maxSINR}^T \mathbf{y}) \tag{15}$$

where $\mathbf{w}_{maxSINR} = [(\mathbf{I}_D - k\mathbf{s}_{L_1}{\mathbf{s}_{L_1}}^T)\mathbf{R}_x(\mathbf{I}_D - k\mathbf{s}_{L_1}{\mathbf{s}_{L_1}}^T) + \sigma_n^2\mathbf{I}_D]^{-1}\mathbf{s}_{L_1}$ and the parameter k is of the same form as (6).

$$k = \frac{{\mathbf{s}_{L_1}}^T\mathbf{R}_x\mathbf{s}_{L_1} + \sigma_n^2 + \mathcal{D}}{2{\mathbf{s}_{L_1}}^T\mathbf{R}_x\mathbf{s}_{L_1}} - \frac{\sqrt{({\mathbf{s}_{L_1}}^T\mathbf{R}_x\mathbf{s}_{L_1} + \sigma_n^2 + \mathcal{D})^2 - 4{\mathbf{s}_{L_1}}^T\mathbf{R}_x\mathbf{s}_{L_1}\mathcal{D}}}{2{\mathbf{s}_{L_1}}^T\mathbf{R}_x\mathbf{s}_{L_1}} \tag{16}$$

4. EXPERIMENTAL STUDIES

The following studies are performed on the 512 × 512 grayscale Fishing Boat image (Figure 1) from the USC-SIPI image database [8].

The near optimal single bit flipping (SBF) algorithm [6] is used in each iteration of the proposed signature design algorithm to find the L_1 principal component. For result comparison with the L_2 signature, the L_1 signature generation algorithm is executed for D iterations.

The simulation studies presented in this paper compare the performance of the SS and ISS schemes for arbitrary, L_2, and L_1 signatures. Figure 2 shows the resulting image for each scheme with embedding distortion $\mathcal{D} = 20$ dB, noise variance $\sigma_n^2 = 3$ dB, and 4096 embedded bits. In all cases, the data hiding is not perceptible to the human eye.

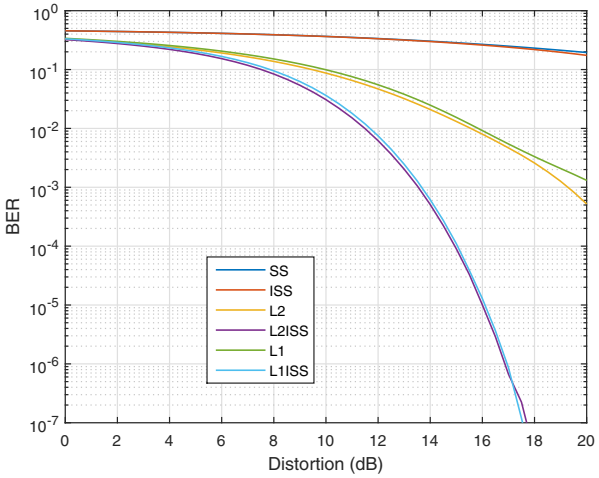


Fig. 3: Fishing Boat for 8x8 Block Size

In typical image applications the 2D-DCT uses a block size of 8×8. For a 512×512 grayscale image, this amounts to embedding 4096 information bits. By comparison, only 1024 bits are embedded in the same image for 16 × 16 2D-DCT block size. The Figures 3 and 4 show the bit error rate (BER) curves under each scheme for a range of distortion values $\mathcal{D}$.

The L_1 signature design achieves a BER near that of the optimally designed L_2 for SS and ISS. Both the L_1 and L_2 signatures have much lower bit error rate than arbitrary signatures. For 16 × 16 block size and higher distortion, the L_1 signature is superior for the fishing boat image.

While previous work has focused on comparing signature performance using BER curves, it is not the only important metric. A strictly numerical method for determining the degree of similarity between the embedded image and the host

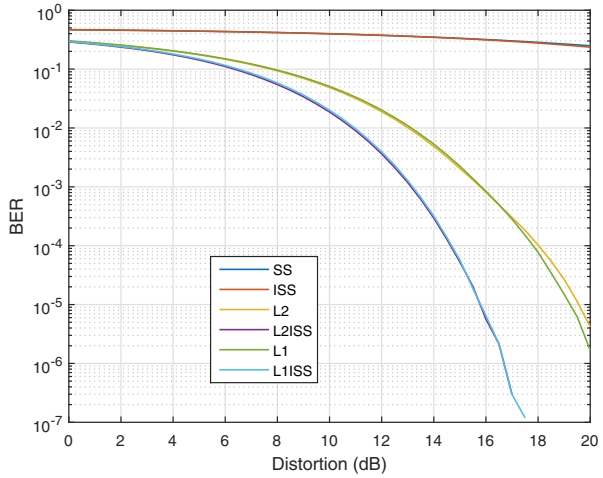


Fig. 4: Fishing Boat for 16x16 Block Size

is the structural similarity (SSIM) index [7], which is based on luminance (l), contrast (c), and structure (s). They are defined, respectively, by the local mean, variance, and covariance of the images ($\mu_x, \mu_y, \sigma_x, \sigma_y, \sigma_{xy}$).

$$\text{SSIM}(x,y) = \left[l(x,y)^{\alpha} \cdot c(x,y)^{\beta} \cdot s(x,y)^{\gamma}\right] \tag{17}$$

$$\begin{aligned} l(x,y) &= \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} \\ c(x_y) &= \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} \\ s(x,y) &= \frac{\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3} \end{aligned} \tag{18}$$

Constants $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ are stabilization variables where $k_1 \ll 1$, $k_2 \ll 1$, and L is pixel value dynamic range. Parameters have default values of $\alpha = \beta = \gamma = 1$ and $c_3 = \frac{c_2}{2}$.

Table 1 contains SSIM values for the Fishing Boat image. The L_1 signature has equal or greater SSIM values than the L_2 signature, providing further support for the proposed new method.

Table 1: SSIM Values for Fishing Boat with 4096 Embedded Bits, 8×8 DCT, and AWGN $\sigma_n^2 = 3$dB

$\mathcal{D}$	L_2 SS	L_2 ISS	L_1 SS	L_1 ISS
0	0.988455	0.988459	0.988457	0.988459
5	0.988273	0.988288	0.988277	0.988288
10	0.987676	0.987718	0.987680	0.987732
15	0.985789	0.985856	0.985792	0.985873
20	0.979898	0.979983	0.979919	0.979989

5. CONCLUSION

The spread-spectrum signature design proposed in this paper is an important alternative steganographic solution. As the L_2 solution was optimized for BER performance, no other signature design should be able to outperform based on that metric. The simulation studies performed confirm that the proposed solution approaches the optimal BER L_2 performance while achieving superior SSIM results.

6. REFERENCES

[1] I. J. Cox, J. Killian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898-905, Apr. 2003.

[3] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.

[4] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 391-405, Feb. 2007.

[5] P. P. Markopoulos, G. N. Karystinos, and D. A. Pados, "Optimal algorithms for $L1$-subspace signal processing," *IEEE Trans. Signal Process.*, vol. 62, no. 19, pp. 5046-5068, Oct. 2014.

[6] S. Kundu, P. P. Markopoulos, and D. A. Pados, "Fast computation of the L_1-principal component of real-valued data," in *Proc. IEEE Int. Conf. Acoustic, Speech, Signal Process. (ICASSP)*, Florence, Italy, May 2014, pp. 8028-8032.

[7] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assesment: from error visibility to structural similarity," in *IEEE Trans. Image Process.*, col. 13, no. 4, pp. 600-612, Apr. 2004.

[8] *USC-SIPI Image Database*, [Online] Available: http://sipi.usc.edu/database /database.php?volume=misc.