Extracting Spread-Spectrum Hidden Data from Digital Media

Ming Li, *Member, IEEE,* Michel Kulhandjian, Dimitris A. Pados, *Member, IEEE,* Stella N. Batalama, *Senior Member, IEEE,* and Michael J. Medley, *Senior Member, IEEE*

***Abstract*—We consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video). We develop a novel multi-carrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multi-carrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host autocorrelation matrix.**

***Index Terms*—Authentication, annotation, blind detection, covert communications, data hiding, information hiding, spread-spectrum embedding, steganalysis, steganography, watermarking.**

I. Introduction

DIGITAL data embedding in digital media is an information technology field of rapidly growing commercial as well as national security interest. Applications may vary from annotation, copyright-marking, and watermarking, to single-stream media merging (text, audio, image) and covert communication [1]. In annotation, secondary data are embedded into digital multimedia to provide a way to deliver side information for various purposes; copyright-marking may act as permanent "iron branding" to show ownership; fragile watermarking may be intended to detect future tampering; hidden low-probability-to-detect (LPD) watermarking may serve as identification for confidential data validation or digital fingerprinting for tracing purposes [2]-[4]. Covert communication or steganography, which literally means "covered writing" in Greek, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio, to establish secret communication between trusting parties and conceal the existence of embedded data [5]-[9]. As a general encompassing comment, different applications of information hiding, such as the ones identified above, require different satisfactory trade-offs between the following four basic attributes of data hiding [10]: (*i*) Payload - information delivery rate; (*ii*) robustness - hidden data resistance to noise/disturbance; (*iii*) transparency - low host distortion for concealment purposes; and (*iv*) security - inability by unauthorized users to detect/access the communication channel.

Recently, developing data embedding technologies are being seen to pose a threat to personal privacy, commercial, and national security interests [11], [12]. In this work, we focus our attention on the blind recovery of secret data hidden in medium hosts via multi-carrier/signature direct-sequence spread-spectrum (DS-SS) transform domain embedding [13]-[20]. Neither the original host nor the embedding carriers (signatures or spreading sequences) are assumed known (fully blind data extraction). This blind hidden data extraction problem has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context [21]-[24].

While passive detection-only of the presence of embedded data is being intensively investigated in the past few years [25]-[33], active hidden data extraction is a relatively new branch of research. In blind extraction of SS embedded data, the unknown host acts as a source of interference/disturbance to the data to be recovered and, in a way, the problem parallels blind signal separation (BSS) applications as they arise in the fields of array processing, biomedical signal processing, and code-division multiple-access (CDMA) communication systems [34]-[38]. Under the assumption that the embedded secret messages are independent identically distributed (i.i.d.) random sequences and independent to the cover host, independent component analysis (ICA) may be utilized to pursue hidden data extraction [24], [39]. However, ICA-based BSS algorithms are not effective in the presence of correlated signal interference as is the case in SS multimedia embedding and degrade rapidly as the dimension of the carrier (signature) decreases relative to the message size. In [19], an iterative generalized least squares (IGLS) procedure was developed to blindly recover unknown messages hidden in image hosts via SS embedding. The algorithm has low complexity and strong recovery performance. However, the scheme is designed solely for *single-carrier* SS embedding where messages are hidden with one signature only and is not generalizable to the *multi-*

Manuscript received November 1, 2012; revised March 08, 2013; accepted May 14, 2013. This work was supported in part by the U.S. Air Force Office of Scientific Research (AFOSR) under Grant FA9550-12-1-0123. This paper was presented in part at the IEEE Intern. Conf. on Comm. (ICC), Ottawa, Canada, June 2012. Approved for Public Release; Distribution Unlimited: 88ABW-2011-3182 dated 6 June 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Z. Jane Wang.

Ming Li, Dimitris A. Pados, and Stella N. Batalama are with the COMSENS Research Center, Department of Electrical Engineering, State University of New York at Buffalo, Buffalo, NY, 14260, USA (e-mail: {mingli, pados, batalama}@buffalo.edu).

Michel Kulhandjian was with the Department of Electrical Engineering, State University of New York at Buffalo. He is now with EION Inc., Ottawa, Ontario, Canada (e-mail: mkk6@buffalo.edu).

Michael J. Medley is with the Air Force Research Laboratory/RIGF, 525 Brooks Rd., Rome, NY, 13441, USA (e-mail: michael.medley@rl.af.mil).

Digital Object Identifier XXXXX

carrier case. Realistically, an embedder would favor *multi-carrier* SS transform-domain embedding to increase security and/or payload rate.

In this paper, we develop a novel multi-carrier iterative generalized least squares (M-IGLS) algorithm for SS hidden data extraction that, to the best of the authors' knowledge, appears for the first time in the broad communication theory and systems literature. For improved recovery performance, in particular for small hidden messages that pose the greatest challenge, experimental studies indicate that a few independent M-IGLS re-initializations and executions on the host can lead to hidden data recovery with probability of error close to what may be attained with known embedding carriers and known original host autocorrelation matrix. Applications of the developed algorithm are, of course, not limited to attacking steganographic covert communications by recovering the secret embedded messages. Since the carriers are also jointly estimated with the embedded data, the developed scheme can also be used for complete message removal or tampering attack as well by reinserting a fabricated message in place of the original. From the opposite data embedding point of view, the developed algorithm can be treated as a tool to test security robustness of SS data hiding schemes.

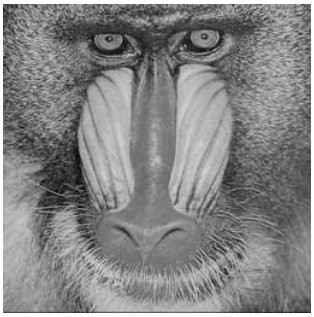
The rest of the paper is organized as follows. In Section II we present the signal model for the multi-carrier SS embedding procedure and formulate the problem of active SS data extraction. The hidden data recovery algorithm is developed in Section III. Experimental studies are presented in Section IV and, finally, some concluding remarks are drawn in Section V.

The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real numbers; $(\cdot)^T$ denotes matrix transpose; $\mathrm{Tr}\{\cdot\}$ is matrix trace; $\mathbf{I}_L$ is the $L \times L$ identity matrix; $\mathrm{sgn}\{\cdot\}$ denotes zero-threshold quantization; and $\mathbb{E}\{\cdot\}$ represents statistical expectation. Finally, $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$ are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

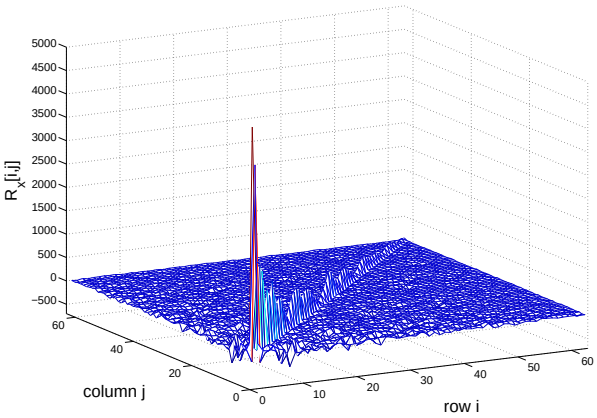
II. Multi-carrier SS Embedding and Extraction: Problem Formulation

Consider a host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\mathbf{H}$ is partitioned into M local non-overlapping blocks of size $\frac{N_1 N_2}{M}$. Each block, $\mathbf{H}_1, \mathbf{H}_2, ..., \mathbf{H}_M$, is to carry K hidden information bits (KM bits total image payload). Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform, a wavelet transform, etc.). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_m) \in \mathbb{R}^{\frac{N_1 N_2}{M}}, m = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_m)$ we choose a fixed subset of $L \leq \frac{N_1 N_2}{M}$ coefficients (bins) to form the final host vectors $\mathbf{x}(m) \in \mathbb{R}^L$, $m = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

The autocorrelation matrix of the host data $\mathbf{x}$ is an important statistical quantity for our developments and is defined as



(a)



(b)

Fig. 1. (a) Baboon image example $\mathbf{H} \in \{0, 1, ..., 255\}^{256 \times 256}$. (b) Host data autocorrelation matrix (8×8 DCT, 63-bin host) [20].

$\mathbf{R}_{\mathrm{x}} \triangleq \mathbb{E}\{\mathbf{x}\mathbf{x}^T\} = \frac{1}{M}\sum_{m=1}^{M} \mathbf{x}(m)\mathbf{x}(m)^T$. It is easy to verify that in general $\mathbf{R}_{\mathrm{x}} \neq \alpha \mathbf{I}_L, \alpha > 0$; that is, $\mathbf{R}_{\mathrm{x}}$ is *not* constant-value diagonal or "white" in field language. For example, 8×8 DCT with 63-bin host data formation (excluding only the dc coefficient) for the 256×256 gray-scale Baboon image in Fig. 1(a) gives the host autocorrelation matrix $\mathbf{R}_{\mathrm{x}}$ in Fig. 1(b) [20].

A. Multi-carrier SS Embedding

We consider K distinct message bit sequences, $\{b_k(1), b_k(2), \ldots, b_k(M)\}$, $k = 1, 2, \ldots, K$, $b_k(m) \in \{\pm 1\}$, $m = 1, \ldots, M$, each of length M bits. The K message sequences may be to be delivered to K distinct corresponding recipients or they are just K portions of one large message sequence to be transmitted to one recipient. In particular, the mth bit from each of the K sequences, $b_1(m), \ldots, b_K(m)$, is simultaneously hidden in the mth transform-domain host vector $\mathbf{x}(m)$ via additive SS embedding by means of K spreading sequences (carriers) $\mathbf{s}_k \in \mathbb{R}^L, \|\mathbf{s}_k\| = 1$, $k = 1, 2, \ldots, K$,

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m) \mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m), \; m = 1, 2, \ldots, M, \tag{1}$$

with corresponding amplitudes $A_k > 0$, $k = 1, \ldots, K$. For the sake of generality, $\mathbf{n}(m)$ represents potential external white

Gaussian noise[1] of mean $\mathbf{0}$ and autocorrelation matrix $\sigma_n^2\mathbf{I}_L$, $\sigma_n^2 > 0$. It is assumed that $b_k(m)$ behave as equi-probable binary random variables that are independent in m (message bit sequence) and k (across messages). The contribution of each individual embedded message bit b_k to the composite signal is $A_k b_k \mathbf{s}_k$ and the block mean-squared distortion to the original host data $\mathbf{x}$ due to the embedded k message alone is

$$\mathcal{D}_k = \mathbb{E}\{\|A_k\mathbf{s}_k b_k\|^2\} = A_k^2, \;\; k = 1, 2, ..., K. \tag{2}$$

Under statistical independence of messages, the block mean-squared distortion of the original image due to the total, multi-message, insertion of data is $\mathcal{D} = \sum_{k=1}^{K} A_k^2$.

The intended recipient of the kth message with knowledge of the kth carrier $\mathbf{s}_k$ can perform embedded bit recovery by looking at the sign of the output of the minimum-mean-square-error (MMSE) filter $\mathbf{w}_{MMSE,k} = \mathbf{R}_{\mathrm{y}}^{-1}\mathbf{s}_k$,

$$\hat{b}_k(m) = \mathrm{sgn}\{\mathbf{w}_{MMSE\,,k}^T\mathbf{y}(m)\} = \mathrm{sgn}\{\mathbf{s}_k^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{y}(m)\} \tag{3}$$

where $\mathbf{R}_{\mathrm{y}}$ is the autocorrelation matrix of the host-plus-data-plus-noise vectors

$$\mathbf{R}_{\mathrm{y}} \triangleq \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{R}_{\mathrm{x}} + \sum_{k=1}^{K} A_k^2\mathbf{s}_k\mathbf{s}_k^T + \sigma_n^2\mathbf{I}_L. \tag{4}$$

The autocorrelation matrix $\mathbf{R}_{\mathrm{y}}$ can be estimated by sample averaging over the set of M received vectors $\{\mathbf{y}(m)\}_{m=1}^{M}$, $\widehat{\mathbf{R}}_{\mathrm{y}} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{y}(m)\mathbf{y}(m)^T$. Using $\widehat{\mathbf{R}}_{\mathrm{y}}$ in (3) in place of $\mathbf{R}_{\mathrm{y}}$, we obtain what is known as the sample-matrix-inversion MMSE (SMI-MMSE) detector implementation [34].

B. Formulation of the Extraction Problem

To blindly extract spread-spectrum embedded data from a given host image, the analyst needs first to convert the host to observation vectors of the form of $\mathbf{y}(m)$, $m = 1, \ldots, M$, in (1). This requires knowledge of (*i*) the partition, (*ii*) transform domain, (*iii*) subset of coefficients, and (*iv*) number of carriers used by the embedder. The host image partition (and block size N_1N_2/M in our notation) may be estimated by neighboring-pixels difference techniques as in [30]. Regarding the subset of coefficients used in embedding, the conservative approach is to assume that all coefficients are used, except maybe the dc value, and set accordingly $L = N_1N_2/M - 1$. The number of carriers K can be estimated by SS signal population identification algorithms such as in [41]. Finally, determination of the transform domain used in embedding seems to be a hurdle not yet tackled by current research. The natural approach would be to consider individually and exhaustively one transform at a time starting from the most common (for example, 2D-DCT, common wavelet transforms, and so on).

In this paper, we focus the technical presentation solely after the point that the analyst obtains transform-domain observations in the form of $\mathbf{y}(m)$ in (1), upon performing appropriate image partition and transform calculation. We denote the combined "disturbance" to the hidden data (host plus noise) by $\mathbf{z}(m) \triangleq \mathbf{x}(m) + \mathbf{n}(m)$ and rewrite SS embedding by (1) as

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{z}(m), \;\; m = 1, \ldots, M, \tag{5}$$

where $\mathbf{z}(m)$ is modeled as a sequence of zero-mean (without loss of generality) vectors with autocovariance matrix $\mathbf{R}_{\mathrm{z}} = \mathbb{E}\{\mathbf{z}\mathbf{z}^T\} = \mathbf{R}_{\mathrm{x}} + \sigma_n^2\mathbf{I}$. Let $\mathbf{v}_k \triangleq A_k\mathbf{s}_k \in \mathbb{R}^L$, $k = 1, \ldots, K$, be the amplitude-including embedding carriers. Then, we can further reformulate SS embedding as

$$\begin{aligned} \mathbf{y}(m) &= \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{z}(m) &(6)\\ &= \mathbf{V}\mathbf{b}(m) + \mathbf{z}(m), \;\; m = 1, \ldots, M, &(7)\end{aligned}$$

where $\mathbf{V} \triangleq [\mathbf{v}_1, \ldots, \mathbf{v}_K] \in \mathbb{R}^{L\times K}$ is the amplitude-including carrier matrix and $\mathbf{b}(m) \in \{\pm 1\}^{K\times 1}$ is the vector of bits embedded in the mth host block. For notational simplicity, we can write the whole observation data in the form of one matrix

$$\mathbf{Y} = \mathbf{V}\mathbf{B} + \mathbf{Z} \tag{8}$$

where $\mathbf{Y} \triangleq [\mathbf{y}(1)\;\; \mathbf{y}(2)\;\; ...\;\; \mathbf{y}(M)] \in \mathbb{R}^{L\times M}$, $\mathbf{B} \triangleq [\mathbf{b}(1)\;\; \mathbf{b}(2)\;\; ...\;\; \mathbf{b}(M)] \in \{\pm 1\}^{K\times M}$, and $\mathbf{Z} \triangleq [\mathbf{z}(1)\,\mathbf{z}(2)\,...\,\mathbf{z}(M)] \in \mathbb{R}^{L\times M}$.

Our objective is to blindly extract the unknown hidden data $\mathbf{B}$ from the observation matrix $\mathbf{Y}$ without prior knowledge of the embedding carriers $\mathbf{s}_k$ and amplitudes A_k, $k = 1, \ldots, K$, in $\mathbf{V} = [A_1\mathbf{s}_1, \ldots, A_K\mathbf{s}_K]$ or the host medium itself $\mathbf{x}(1), \ldots, \mathbf{x}(M)$ in $\mathbf{Z} = [\mathbf{x}(1) + \mathbf{n}(1), \ldots, \mathbf{x}(M) + \mathbf{n}(M)]$.

III. Hidden Data Extraction

If $\mathbf{Z}$ were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of $\mathbf{V}$ and decoder of $\mathbf{B}$ would be

$$\widehat{\mathbf{V}}, \widehat{\mathbf{B}} = \arg \min_{\substack{\mathbf{B}\in\{\pm 1\}^{K\times M}\\ \mathbf{V}\in\mathbb{R}^{L\times K}}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2 \tag{9}$$

where multiplication by $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$ can be interpreted as prewhitening of the compound observation data. If Gaussianity of $\mathbf{Z}$ is not to be invoked, then (9) can be simply referred to as the joint generalized least-squares (GLS) solution[2] of $\mathbf{V}$ and $\mathbf{B}$.

The global GLS-optimal message matrix $\widehat{\mathbf{B}}$ in (9) can be computed independently of $\widehat{\mathbf{V}}$ by exhaustive search over all possible choices under the criterion function $\|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2$,

$$\widehat{\mathbf{B}} = \arg \min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2 \tag{10}$$

where $\mathbf{P}_{\perp\mathbf{B}} \triangleq \mathbf{I} - \mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B}$. The derivation of (10) is provided in the Appendix. Exhaustive search has, of course, complexity exponential in KM (total size of hidden messages in bits). We consider this cost unacceptable and attempt to reach a quality approximation of the solution of (10) (or (9), to

[1] Additive white Gaussian noise is frequently viewed as a suitable (most entropic) model for general quantization errors, channel transmission disturbances, and/or image processing attacks [40].

[2] Generalized least-squares solutions are weighted least-squares (WLS) solutions with optimal weighting matrices, here $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$, that yield the lowest variance of the estimation error [35],[36].

that respect) by alternating generalized least-squares estimates of $\mathbf{V}$ and $\mathbf{B}$, iteratively, as described below.

Pretend $\mathbf{B}$ is known. The generalized least-squares estimate of $\mathbf{V}$ is

$$\begin{aligned}\widehat{\mathbf{V}}_{\rm GLS} &= \arg\min_{\mathbf{V}\in\mathbb{R}^{L\times K}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &= \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \end{aligned} \quad (11)$$

Pretend, in turn, that $\mathbf{V}$ is known. Then, the least-squares estimate of $\mathbf{B}$ *over the real field* is

$$\begin{aligned}\widehat{\mathbf{B}}_{\rm GLS}^{\rm real} &= \arg\min_{\mathbf{B}\in\mathbb{R}^{K\times M}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &= (\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{Y}. \end{aligned} \quad (12)$$

Observing that

$$(\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm z}^{-1} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}, \quad (13)$$

we rewrite

$$\widehat{\mathbf{B}}_{\rm GLS}^{\rm real} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y} \quad (14)$$

and suggest the approximate binary message solution

$$\begin{aligned}\widehat{\mathbf{B}}_{\rm GLS}^{\rm binary} &= \arg\min_{\mathbf{B}\in\{\pm1\}^{K\times M}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &\simeq {\rm sgn}\{(\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y}\}. \end{aligned} \quad (15)$$

The proofs of (11), (12), and (13) are provided in the Appendix.

The *multi-carrier iterative generalized least-squares* (M-IGLS) procedure suggested by the two equations (11) and (15) is now straightforward. Initialize $\widehat{\mathbf{B}}$ arbitrarily and alternate iteratively between (11) and (15) to obtain at each step conditionally generalized least squares estimates of one matrix parameter given the other. Stop when convergence is observed. Notice that (15) utilizes knowledge of the autocorrelation matrix $\mathbf{R}_{\rm y}$, which can be estimated by sample averaging over the received data observations, $\widehat{\mathbf{R}}_{\rm y} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{y}(m)\mathbf{y}(m)^T$. The M-IGLS extraction algorithm is summarized in Table I. Superscripts denote iteration index. The computational complexity of each iteration of the M-IGLS algorithm is $\mathcal{O}(2K^3+2LMK+K^2(3L+M)+L^2K)$ and, experimentally, the number of iterations executed is between 20 and 50 in general.

For the sake of mathematical accuracy, we recall that in least-squares there is always a symbol sign (phase in complex domains) ambiguity when joint data extraction and carrier estimation is pursued (i.e., data bits $\mathbf{b}_k \in \{\pm1\}^M$ on carrier $\mathbf{s}_k \in \mathbb{R}^L$ have the same least-squares error with data bits $-\mathbf{b}_k$ on carrier $-\mathbf{s}_k$, $k = 1,\ldots,K$). The sign-ambiguity problem can be overcome with a few known or guessed data symbols for supervised sign correction[3] [42]. Moreover, in a multi-carrier least-squares scenario as the one that we face herein, the index association remains unresolved (i.e., given a recovered (message, carrier) pair ($\mathbf{b}$, $\mathbf{s}$), the corresponding index $k \in \{1,\ldots,K\}$ in (1) cannot be obtained). To the extend that the application of the work presented in this paper is to simply extract blindly the embedded bits with the least possible errors, the carrier indexing problem is not dealt with any further.

[3]If the embedded data are encrypted, then both options $\mathbf{b}_k$ and $-\mathbf{b}_k$ must be separately decrypted and investigated for sign correction for each message $k = 1,\ldots,K$.

TABLE I
MULTI-CARRIER ITERATIVE GENERALIZED LEAST-SQUARES DATA EXTRACTION

1) $d := 0$; initialize $\widehat{\mathbf{B}}^{(0)} \in \{\pm1\}^{K\times M}$ arbitrarily.
2) $d := d+1$;
$\widehat{\mathbf{V}}^{(d)} := \mathbf{Y}(\widehat{\mathbf{B}}^{(d-1)})^T\left[(\widehat{\mathbf{B}}^{(d-1)})(\widehat{\mathbf{B}}^{(d-1)})^T\right]^{-1}$;
$\widehat{\mathbf{B}}^{(d)} := {\rm sgn}\left\{\left((\widehat{\mathbf{V}}^{(d)})^T\widehat{\mathbf{R}}_{\rm y}^{-1}(\widehat{\mathbf{V}}^{(d)})\right)^{-1}(\widehat{\mathbf{V}}^{(d)})^T\widehat{\mathbf{R}}_{\rm y}^{-1}\mathbf{Y}\right\}$.
3) Repeat Step 2 until $\widehat{\mathbf{B}}^{(d)} = \widehat{\mathbf{B}}^{(d-1)}$.

Returning to the proposed data extraction algorithm, we understand that with arbitrary initialization convergence of the M-IGLS procedure described in Table I to the optimal GLS solution of (9) is not guaranteed in general. Extensive experimentation with the algorithm in Table I indicates that, for sufficiently long messages hidden by each carrier ($M = 4$Kbits or more, for example), satisfactory quality message decisions $\widehat{\mathbf{B}}$ can be directly obtained. However, when the message size is small, M-IGLS may very well converge to inappropriate points/solutions. The quality (generalized-least-squares fit) of the end convergence point depends heavily on the initialization point and arbitrary initialization -which at first sight is unavoidable for blind data extraction- offers little assurance that the iterative scheme will lead us to appropriate, "reliable" (close to minimal generalized least-squares fit) solutions. To that respect, re-initialization and re-execution of the M-IGLS procedure, say P times, is always possible. To assess which of the P returned solutions, say $(\widehat{\mathbf{V}}_1,\widehat{\mathbf{B}}_1),\ldots,(\widehat{\mathbf{V}}_P,\widehat{\mathbf{B}}_P)$, has superior generalized-least-squares fit, we simply feed $(\widehat{\mathbf{V}}_i,\widehat{\mathbf{B}}_i)$ to (9) (using $\widehat{\mathbf{R}}_{\rm y}$ in place of $\mathbf{R}_{\rm z}$) and choose

$$\widehat{\mathbf{V}}_{\rm final},\widehat{\mathbf{B}}_{\rm final} = \arg\min_{(\mathbf{V},\mathbf{B})\in\left\{(\widehat{\mathbf{V}}_1,\widehat{\mathbf{B}}_1),\ldots,(\widehat{\mathbf{V}}_P,\widehat{\mathbf{B}}_P)\right\}} \|\widehat{\mathbf{R}}_{\rm y}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2. \quad (16)$$

The computational complexity of the P-times re-initialized M-IGLS is, of course, $\mathcal{O}(PD(2K^3+2LMK+K^2(3L+M)+L^2K))$ where D represents the number of internal iterations in d in Table I.

IV. EXPERIMENTAL STUDIES

A technically firm and keen measure of quality of a hidden-message extraction solution is the difference in bit-error-rate (BER) experienced by the intended recipient and the analyst. The intended recipient in our studies may be using any of the following three message recovery methods: (*i*) Standard carrier matched-filtering (MF) with the known carriers $\mathbf{s}_k$, $k = 1,...,K$; (*ii*) sample-matrix-inversion MMSE (SMI-MMSE) filtering with known carriers $\mathbf{s}_k$ and estimated host autocorrelation matrix $\widehat{\mathbf{R}}_{\rm y}$ (see (3)); and (*iii*) ideal MMSE filtering with known carriers $\mathbf{s}_k$ and known true host autocorrelation matrix $\mathbf{R}_{\rm x}$, which serves as the ultimate performance bound

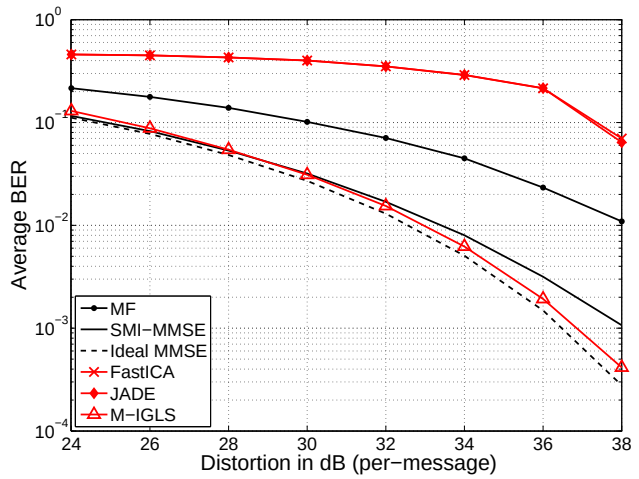


Fig. 2. Average BER versus per-message block distortion (512×512 Baboon, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.49$dB).

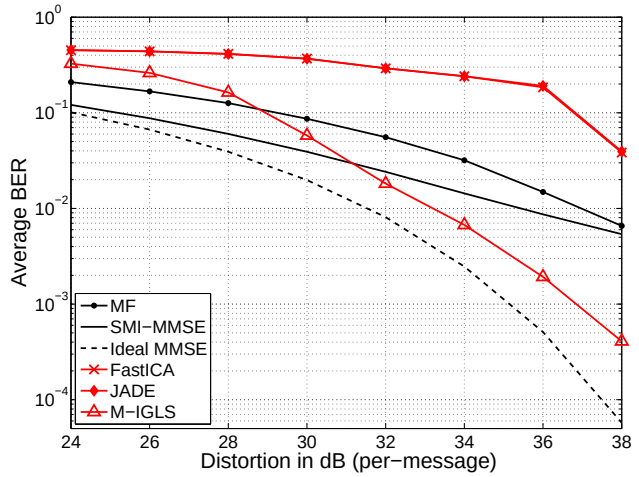


Fig. 3. Average BER versus per-message block distortion (256×256 Baboon, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 45.45$dB).

reference for all methods. In terms of blind extraction (neither $\mathbf{s}_k$ nor $\mathbf{R}_{\rm x}$ known), we will examine: (*iv*) The developed M-IGLS algorithm in Table I with $P = 20$ re-initializations and, for comparison purposes, the performance of two typical independent component analysis (ICA) based blind signal separation (BSS) algorithms (*v*) FastICA [44], and (*vi*) JADE [45].

We first consider as a host example the gray-scale 512×512 "Baboon" image. We perform 8×8 block DCT embedding by (1) over all bins except the dc coefficient with $K = 4$ distinct arbitrary carriers $\mathbf{s}_k \in \mathbb{R}^{63}$, $k = 1,\ldots,K$. The hidden message embedded by each carrier is $\frac{512^2}{8^2} = 4,096$ bits long. The per-message block mean square distortion due to each embedded message is set to be the same for all messages, i.e. $\mathcal{D}_k = A_k^2 = \frac{\mathcal{D}}{K}$, $k = 1,\ldots,4$. With per-message 8×8-block MSE distortion $\mathcal{D}_k$, $k = 1,\ldots,K$, the peak signal-to-noise ratio (PSNR) of the image due to embedding can be calculated by $\text{PSNR} \triangleq 20\log_{10}(255) - 10\log_{10}(\sum_{k=1}^K \mathcal{D}_k/64)$. Another metric that reflects the relationship between host and embedding distortion is the block document-to-watermark power ratio (DWR) defined as $\text{DWR} \triangleq 10\log_{10}\sigma_x^2 - 10\log_{10}(\sum_{k=1}^K \mathcal{D}_k)$ where $\sigma_x^2 \triangleq \text{Tr}\{\mathbf{R}_{\rm x}\}$ is the (total) host block variance. The value of σ_x^2 depends on the nature of each host image and is provided in each experiment that we run (see figure captions) to facilitate translation by the reader between MSE and DWR if desired. For the sake of generality, in our studies we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$dB.

Fig. 4. 512×512 gray-scale Boat image.

Fig. 2 shows the average BER (over all $K = 4$ messages) of all methods (*i*) through (*vi*) listed above as a function of the host block distortion per-message. FastICA and JADE have computational complexity $\mathcal{O}(2(K-1)(K+M)+5MK(K+1)/2)$ per iteration and $\mathcal{O}(K(K-1)(4K^2+21K+75)/2)$, respectively. In particular, on an Intel i5-2550K 3.40GHz processor running standard Matlab software for experimentation, the average execution time of the M-IGLS algorithm with $P = 20$ initializations was 1.51 sec, the average execution time of FastICA was 0.20 sec, and the average execution time of JADE was 0.08 sec. While the two independent/principal-component methods (FastICA and JADE) are failing to carry out effective hidden data extraction, to our satisfaction M-IGLS analysis is very close in BER performance to the ideal MMSE detector bound in which both the embedding carriers and the clean host autocorrelation matrix $\mathbf{R}_{\rm x}$ are treated as perfectly known.

In Fig. 3, we repeat the exact same experimental study on the smaller 256×256 version of the Baboon image in Fig. $1(a)$ with $K = 4$ hidden messages of length only $\frac{256^2}{8^2} = 1,024$ bits per message (compared to $4,196$ bits per message in Fig. 2). Comparing with Fig. 2, the gap between M-IGLS and ideal MMSE increases as the hidden message size decreases, but the extraction performance of M-IGLS can still be deemed satisfactory. For additional experimental validation, the studies of Fig. 2 and Fig. 3 are repeated on the familiar "Boat" image

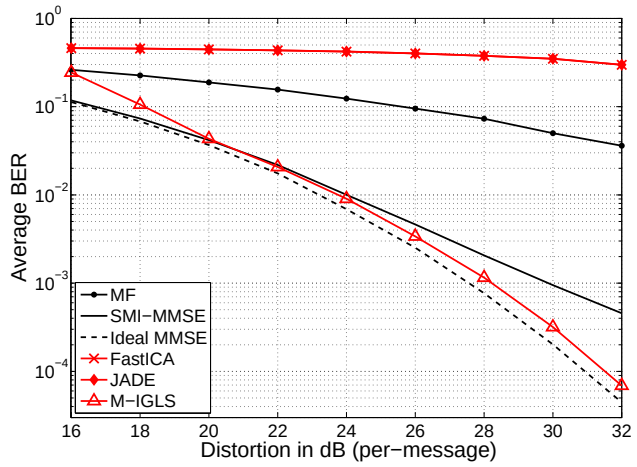


Fig. 5. Average BER versus per-message block distortion (512×512 Boat, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 44.15$dB).

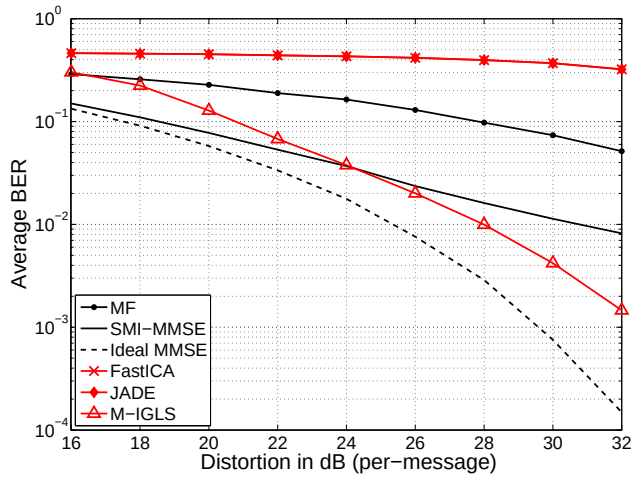


Fig. 6. Average BER versus per-message distortion, 256×256 Boat, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 45.57$dB).

Fig. 7. 256×256 gray-scale Aircraft image.

(shown in Fig. 4) in its 512×512 and 256×256 gray-scale versions (Fig. 5 and Fig. 6, correspondingly).

To examine the behavior of M-IGLS under increasing-density small-message hiding, we consider the 256×256 gray-

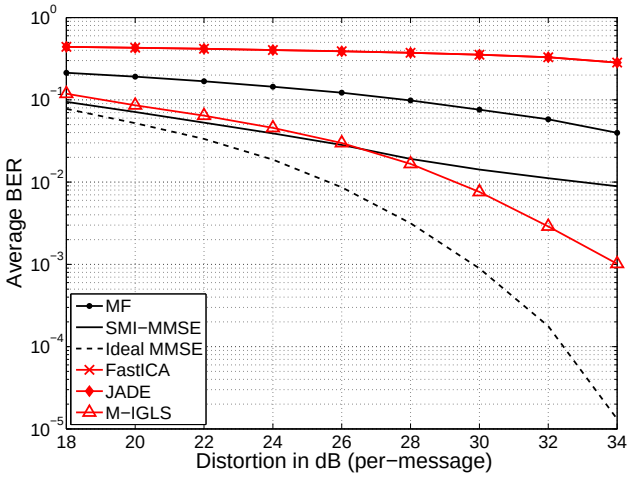


Fig. 8. Average BER versus per-message block distortion (256×256 F16 Aircraft, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.23$dB).

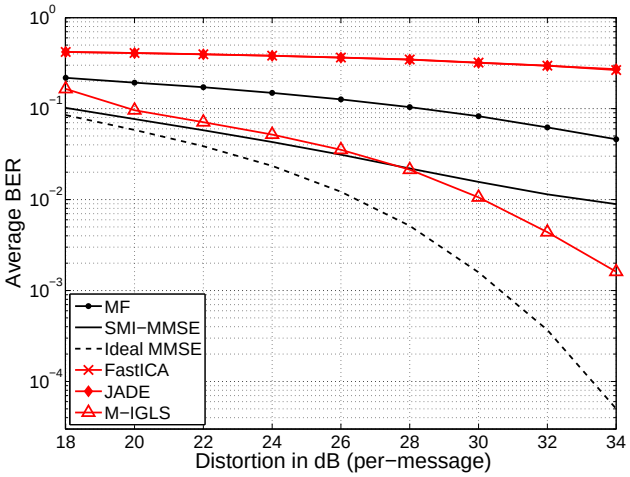


Fig. 9. Average BER versus per-message block distortion (256×256 F16 Aircraft, $L = 63$, $K = 8$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.23$dB).

scale "F-16 Aircraft" image (shown in Fig. 7) with $K = 4$ and $K = 8$ hidden messages of length 1Kbit each. The recovery performance plots for $K = 4$ and $K = 8$ are given in Figs. 8 and 9, correspondingly.

An encompassing conclusion over all executed experiments is that M-IGLS remains a most effective technique to blindly extract hidden messages, while extraction becomes more challenging as the length of the hidden message per used embedding carrier decreases or the number of hidden messages (number of used carriers) increases. It is also worth pointing out that, in these experimental studies, M-IGLS may outperform (in moderate to high distortion values) SMI-MMSE in which the true carriers/signatures are known. This is because SMI-MMSE suffers from performance degradation due to small-sample-support adaptation (estimation of matrix $\mathbf{R}_y$). The unsatisfactory performance of the ICA-based methods is due to the interference from high-amplitude (low-frequency)

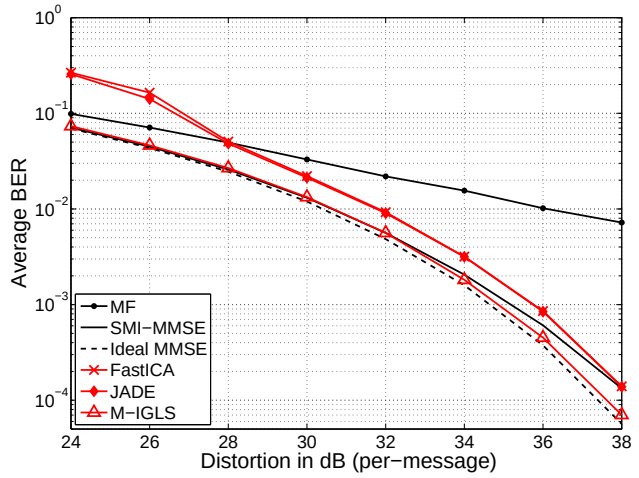


Fig. 10. Average BER versus per-message block distortion (512×512 Baboon, $L = 20$ highest-frequency coefficients, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.49$dB).

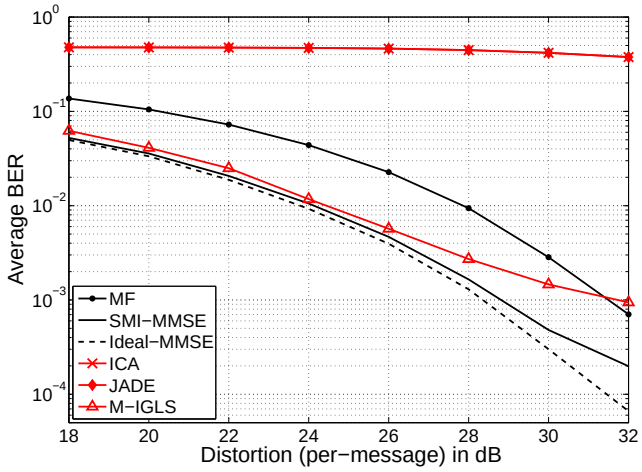


Fig. 12. Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], ISS embedding [13], $K = 1$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$).

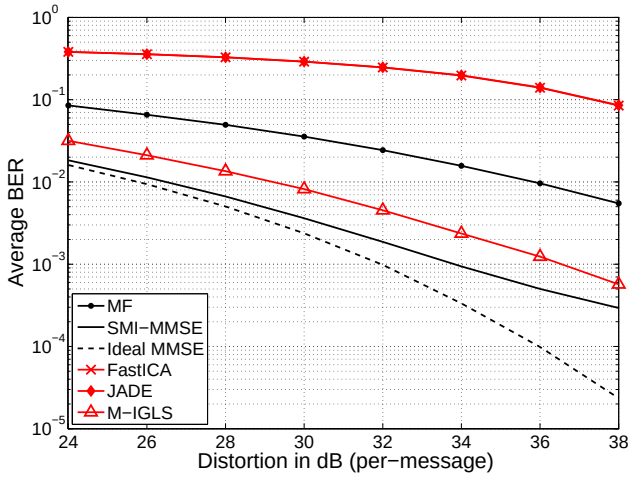


Fig. 11. Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], $K \in \{1, 2, \ldots, 5\}$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$dB).

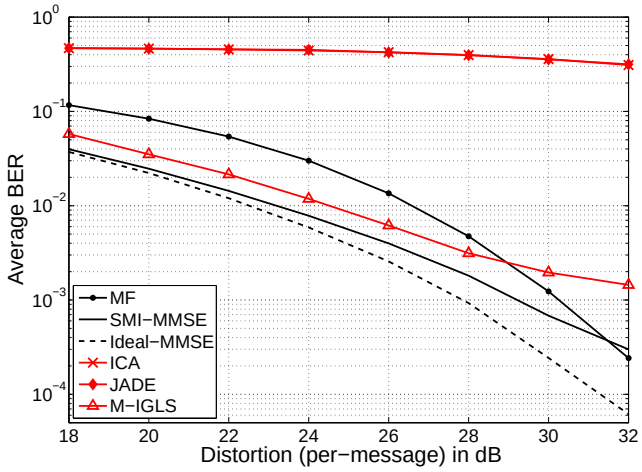


Fig. 13. Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], CAISS embedding [43], ($\eta = 0.7$), $K = 1$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$dB).

host coefficients. To demonstrate this point, in Fig. 10 we repeat the exact same experiment of Fig. 2 using this time only the $L = 20$ highest-frequency DCT coefficients as our host vector. It can be observed that, in this moderate host interference environment, ICA-based methods can provide satisfactory performance (not superior to M-IGLS, however). Of course, we may not expect that data are always embedded exclusively in low-amplitude coefficients alone.

Next, for the sake of enhanced experimental credibility, we examine the average performance of the proposed M-IGLS algorithm over a large image database. The experimental image data set, [46] and [47] combined, consists of more than $11,500$ 8-bit gray-scale photographic images which have great variety (e.g., outdoor/indoor, daylight/night, natural/man-made) and different sizes. We embed one up to five messages, $K \in \{1, 2, \ldots, 5\}$, via multi-carrier SS embedding with arbitrary carriers and payload between 0.016 and 0.078 bits per pixel (bpp). The length of the embedding carriers varies between 30 and 63, $L \in \{30, 31, \ldots, 63\}$. Recovery performance plots are given in Fig. 11. Similar conclusions can be drawn as in the previous individual image host experimentations.

While our blind data extraction algorithmic development was based on the most common SS embedding form (1) for convenience in presentation, the developed algorithm can also be applied to more advanced SS embedding schemes such as improved spread-spectrum (ISS) [13] and correlation-aware improved spread-spectrum (CAISS) [43]. In Fig. 12, we go again over the whole [46], [47] databases under ISS embedding and in Fig. 13 under CAISS embedding (with amplitude-proportion parameter $\eta = 0.7$)[4]. It can be noted from Figs. 12,

[4]Both ISS [13] and CAISS [43] are proposed as single carrier embedding schemes ($K = 1$ in the experiments).

13 that M-IGLS analysis can also carry out effective hidden data extraction for the ISS and CAISS schemes.

V. Conclusions

We considered the problem of blindly extracting unknown messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. We developed a low complexity multi-carrier iterative generalized least-squares (M-IGLS) core algorithm. Experimental studies showed that M-IGLS can achieve probability of error rather close to what may be attained with known embedding signatures and known original host autocorrelation matrix and presents itself as an effective countermeasure to conventional SS data embedding/hiding[5].

Acknowledgement

The authors would like to thank the anonymous reviewers for a wealth of comments and suggestions that helped improve significantly the presentation and content of this manuscript.

Appendix

A. Derivation of (10)

The minimization in (9) can be carried out in two steps. First, we minimize (9) with respect to $\mathbf{V}$: $\mathbf{V} = \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}$ (see also Appendix B). Then, substituting $\mathbf{V}$ back into (9) we obtain

$$\begin{aligned}\widehat{\mathbf{B}} &= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B})\|_F^2 \quad (17)\\ &= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}(\mathbf{I}-\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B})\|_F^2 \quad (18)\\ &= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2 \quad (19)\end{aligned}$$

where $\mathbf{P}_{\perp\mathbf{B}} \triangleq \mathbf{I}-\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B}$. ■

B. Proof of (11)

The GLS cost function in (9) can be rewritten as

$$\begin{aligned}J &\triangleq \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}-\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{V}\mathbf{B}\|_F^2 \quad (20)\\ &= \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\mathbf{V}^T\right\} - \\ &\quad \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\mathbf{V}^T\right\} \quad (21)\end{aligned}$$

where $\mathrm{Tr}\{\cdot\}$ denotes the trace of a matrix.

For a given message matrix $\mathbf{B}$, the GLS optimal estimate of $\mathbf{V}$ can be obtain by differentiating the cost function J with respect to $\mathbf{V}^T$ and setting the outcome equal to the zero matrix,

$$\begin{aligned}\frac{\partial J}{\partial \mathbf{V}^T} &= -\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T + \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{B}\mathbf{B}^T) = \mathbf{0}\\ &\Rightarrow \mathbf{V} = \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \quad (22)\end{aligned}$$

■

[5]In [39], Bas and Cayre presented an interesting signature-based additive embedding approach different to (1) that is host-vector-by-host-vector dependent and would withstand IGLS-based analysis. The embedding is, however, sensitive to noise which would lead to high recovery error rates by intended recipients and limit the applicability to general covert communication problems.

C. Proof of (12)

We rewrite the GLS cost function in (21) as

$$\begin{aligned}J &= \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{Tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\right\} - \\ &\quad \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{Tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\right\}. \quad (23)\end{aligned}$$

Pretend that $\mathbf{V}$ is known and relax the domain of the symbol information matrix to the real space, $\mathbf{B}\in\mathbb{R}^{K\times M}$. The GLS optimal estimate of $\mathbf{B}\in\mathbb{R}^{K\times M}$ can be calculated again by differentiation

$$\begin{aligned}\frac{\partial J}{\partial \mathbf{B}^T} &= -\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B} = \mathbf{0}\\ &\Rightarrow \mathbf{B} = (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}. \quad (24)\end{aligned}$$

■

D. Proof of (13)

Since $\mathbf{R}_{\mathrm{y}} = \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{V}\mathbf{V}^T + \mathbf{R}_{\mathrm{z}}$, by the Matrix Inverse Lemma (also known as Woodbury's matrix identity) [48], we obtain

$$\mathbf{R}_{\mathrm{y}}^{-1} = \mathbf{R}_{\mathrm{z}}^{-1} - \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. \quad (25)$$

Then,

$$\begin{aligned}\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V} &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V} - \\ &\quad \mathbf{V}^T\mathbf{R}_{z}^{-1}\mathbf{V}(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}[\mathbf{I}-(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}]\\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\\ &\quad [(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})-\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}]\\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}. \quad (26)\end{aligned}$$

By the property of the inverse of a product of matrices [48], the inverse of $(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})$ is

$$\begin{aligned}(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1} &= (\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})(\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\\ &= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}+\mathbf{I}. \quad (27)\end{aligned}$$

We combine the results of (25) and (27) and finally obtain

$$\begin{aligned}(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1} &= \left((\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}+\mathbf{I}\right)\\ &\quad \mathbf{V}^T\left(\mathbf{R}_{\mathrm{z}}^{-1}-\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I}+\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\right)\\ &= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. \quad (28)\end{aligned}$$

■

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.
[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.
[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.
[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.
[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.
[11] *Federal plan for cyber security and information assurance research and development*, Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.
[12] R. Chandramouli, "A mathematical framework for active steganalysis," *ACM Multimedia Systems Special Issue on Multimedia Watermarking*, vol. 9, pp. 303-311, Sept. 2003.
[13] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Proc.*, vol. 51, pp. 898-905, Apr. 2003.
[14] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc.*, vol. 6, pp. 1673-1687, Dec. 1997.
[15] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Proc.*, vol. 9, pp. 55-68, Jan. 2000.
[16] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, pp. 273-284, Sept. 2001.
[17] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," *IEEE Trans. Image Proc.*, vol. 13, pp. 126-144, Feb. 2004.
[18] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Intern. Conf. Image Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.
[19] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley, "Blind iterative recovery of spread-spectrum steganographic messages," in *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, Genova, Italy, Sept. 2005, vol. 2, pp. 11-14.
[20] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Proc.*, vol. 16, pp. 391-405, Feb. 2007.
[21] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Proc.*, vol. 53, pp. 3976-3987, Oct. 2005.
[22] L. Pérez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Watermarking security: A survey," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.
[23] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *ACM Journal Signal Proc. - Special Section: Security of Data Hiding Technologies*, vol. 83, pp. 2069-2084, Oct. 2003.
[24] L. Pérez-Freire and F. Pérez-González, "Spread-spectrum watermarking security," *IEEE Trans. Inform. Forensics and Security*, vol. 4, pp. 2-24, Mar. 2009.
[25] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inform. Forensics and Security*, vol. 1, pp. 111-119, Mar. 2006.
[26] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis for Markov cover data with applications to images," *IEEE Trans. Inform. Forensics and Security*, vol. 1, pp. 275-287, June 2006.
[27] İ. Avcıbaş, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Trans. Image Proc.*, vol. 12, pp. 221-229, Feb. 2003.
[28] W. Lie and G. Lin, "A feature-based classification technique for blind image steganalysis," *IEEE Trans. Multimedia*, vol. 7, pp. 1007-1020, Dec. 2005.
[29] G. Gul and F. Kurugollu, "SVD-based universal spatial domain image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 5, pp. 349-353, June 2010.
[30] Y. Wang and P. Moulin, "Steganalysis of block-DCT image steganography," in *Proc. IEEE Workshop on Statistical Signal Processing*, Saint-Louis, MO, Sept. 2003, pp. 339-342.
[31] Y. Wang and P. Moulin, " Optimized feature extraction for learning-based image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 2, pp. 31-45, Mar. 2007.
[32] B. Li, J. Huang, and Y. Q. Shi, "Steganalysis of YASS," *IEEE Trans. Inform. Forensics and Security*, vol. 4, pp. 369-382, Sept. 2009.
[33] M. Li, D. A. Pados, S. N. Batalama, and M. J. Medley, "Passive spread-spectrum steganalysis," in *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, Brussels, Belgium, Sept. 2011, pp. 1997-2000.
[34] D. G. Manolakis, V. K. Ingle, and S. M. Kogon. *Statistical and adaptive signal processing: Spectral estimation, signal modeling, adaptive filtering and array processing*. Boston, MA: McGraw-Hill, 2000.
[35] J. M. M. Anderson, B. A. Mair, M. Rao, and C.-H. Wu, "Weighted least-squares reconstruction methods for positron emission tomography," *IEEE Trans. Medical Imaging*, vol. 16, pp. 159-165, Apr. 1997.
[36] J. Eriksson and M. Viberg, "Asymptotic properties of nonlinear weighted least squares in radar array processing," *IEEE Trans. Signal Proc.*, vol. 52, pp. 3083-3095, Nov. 2004.
[37] S. Talwar, M. Viberg, and A. Paulraj, "Blind seperation of synchronous co-channel digital signals using an antenna array - Part I: Algorithms," *IEEE Trans. Signal Proc.*, vol. 44, pp. 1184-1197, May 1996.
[38] T. Li and N. D. Sidiropoulos, "Blind digital signal separation using successive interference cancellation iterative least squares," *IEEE Trans. Signal Proc.*, vol. 48, pp. 3146-3152, Nov. 2000.
[39] P. Bas and F. Cayre, "Achieving subspace or key security for WOA using natural or circular watermarking," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, Sept. 2006.
[40] T. M. Cover and J. A. Thomas. *Elements of Information Theory*, 2nd ed. Hoboken, NJ: John Wiley, 2006.
[41] M. Li, S. N. Batalama, and D. A. Pados, "Population size identification for CDMA eavesdropping," in *Proc. IEEE Military Comm. Conf. (MILCOM)*, Orlando, FL, Oct. 2007, pp. 1-6.
[42] G. N. Karystinos and D. A. Pados, "Supervised phase correction of blind space-time DS/CDMA channel estimates," *IEEE Trans. Commun.*, vol. 55, pp. 584-592, Mar. 2007.
[43] A. Valizadeh and Z. J. Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," *IEEE Trans. Inform. Forensics and Security*, vol. 6 , pp. 267-282, June 2011.
[44] A. Hyvärinen and E. Oja, "A fast fixed-point algorithm for independent component analysis," *Neural Computation*, vol. 9, pp. 1483-1492, Oct. 1997.
[45] J. F. Cardoso, "High-order contrasts for independent component analysis," *Neural Computation*, vol. 11, pp. 157-192, Jan. 1999.
[46] T. Filler, T. Pevny, and P. Bas. *BOSS, Break Our Steganography System*. Available: http: //www.agents.cz/boss/
[47] G. Schaefer and M. Stich, "UCID–An uncompressed colour image database," in *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, San Jose, CA, Jan. 2004, pp. 472-480.
[48] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*, Philadelphia, PA: SIAM, 2000.

Ming Li (S'05, M'11) received the M.S. and Ph.D. degrees in electrical engineering from the State University of New York at Buffalo, Buffalo, in 2005 and 2010, respectively. He is currently a Post-Doctoral Research Associate with the Signals, Communications, and Networking Research Group, Department of Electrical Engineering, State University of New York at Buffalo.

His research interests include spread-spectrum communications and adaptive multiuser detection, cognitive radios and networks, covert communications and steganography, physical layer secrecy, and compressed sensing.

Dr. Li is a member of the IEEE Communications and Signal Processing Societies.

Michel K. Kulhandjian received his M.S. and Ph.D. degree in Electrical Engineering from the State University of New York at Buffalo in 2007 and 2012, respectively. He had previously received his B.S. degree in Electronics Engineering and Computer Science (Minor) "Summa Cum Laude" from the American University in Cairo (AUC) in 2005. Since 2012, he has been with Alcatel-Lucent, in Ottawa, Ontario, in 2012, performing R&D in the area of Next Generation Cloud Based Wireless Network Architecture. In the same year he was appointed as a Research Associate at EION Inc. and received the Natural Science and Engineering Research Council of Canada (NSERC) Industrial R&D Fellowship (IRDF) to carry out research on reliability enhancement and performance optimization of broadband wireless networks.

His research interests include wireless multiple access communications, signature waveform design for overloaded code-division multiplexing applications, adaptive multiuser detection, statistical signal processing, covert communications, spread-spectrum steganography and steganalysis. Dr. Kulhandjian was a Technical Program Committee (TPC) member for the IEEE Vehicular Technology Conferences VTC2012-Fall (Wireless Multiple Access Techniques) and VTC2013-Fall (Wireless Access).

Dimitris A. Pados (M'95) was born in Athens, Greece, on October 22, 1966. He received the Diploma degree in computer science and engineering (five-year program) from the University of Patras, Greece, in 1989, and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in 1994.

From 1994 to 1997, he held an Assistant Professor position in the Department of Electrical and Computer Engineering and the Center for Telecommunications Studies, University of Louisiana, Lafayette. Since August 1997, he has been with the Department of Electrical Engineering, State University of New York at Buffalo, where he is presently a Professor. He served the Department as Associate Chair in 2009-2010. Dr. Pados was elected three times University Faculty Senator (terms 2004-06, 2008-10, 2010-12) and served on the Faculty Senate Executive Committee in 2009-10.

His research interests are in the general areas of communication theory and adaptive signal processing with applications to interference channels and signal waveform design, secure wireless communications, cognitive radios and networks.

Dr. Pados is a member of the IEEE Signal Processing, Communications, Information Theory, and Computational Intelligence Societies. He served as an Associate Editor for the IEEE Signal Processing Letters from 2001 to 2004 and the IEEE Transactions on Neural Networks from 2001 to 2005. He received a 2001 IEEE International Conference on Telecommunications best paper award, the 2003 IEEE Transactions on Neural Networks Outstanding Paper Award, and the 2010 IEEE International Communications Conference Best Paper Award in Signal Processing for Communications for articles that he coauthored with students and colleagues. Professor Pados is a recipient of the 2009 SUNY-system-wide Chancellor's Award for Excellence in Teaching and the 2011 University at Buffalo Exceptional Scholar - Sustained Achievement Award.

Stella N. Batalama (S'91, M'94, SM'13) received the Diploma degree in computer engineering and science (5-year program) from the University of Patras, Greece in 1989 and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in 1994.

In 1995 she joined the Department of Electrical Engineering, State University of New York at Buffalo, Buffalo, NY, where she is presently a Professor. From 2009 to 2011, she served as the Associate Dean for Research of the School of Engineering and Applied Sciences and since 2010, she is serving as the Chair of the Electrical Engineering Department. During the summers of 1997-2002 she was Visiting Faculty in the U.S. Air Force Research Laboratory (AFRL), Rome, NY. From Aug. 2003 to July 2004 she served as the Acting Director of the AFRL Center for Integrated Transmission and Exploitation (CITE), Rome NY.

Her research interests include small-sample-support adaptive filtering and receiver design, cooperative communications, cognitive networks, underwater communications, covert communications, steganography, compressive sampling, adaptive multiuser detection, robust spread-spectrum communications, supervised and unsupervised optimization.

Dr. Batalama was an associate editor for the IEEE Communications Letters (2000-2005) and the IEEE Transactions on Communications (2002-2008).

Michael J. Medley (S'91, M'95, SM'02) received his Ph.D. in Electrical Engineering in 1995 from Rensselaer Polytechnic Institute, Troy, NY, where he previously was awarded B.S. and M.S degrees in electrical engineering in 1990 and 1991. He currently serves as an Associate Professor of Electrical and Computer Engineering at the State University of New York Institute of Technology (SUNYIT) as well as Senior Research Engineer at the United States Air Force Research Laboratory (AFRL). Since 1991, he has been involved in AFRL communications and signal processing research related to adaptive interference suppression, spread spectrum waveform design, covert messaging, and airborne networking and communications links. Since joining SUNYIT in 2002, he has been responsible for the development of the electrical and computer engineering program and continues to actively pursue research and development related to software defined radios, cognitive radio networking and engineering education. In 2012, Professor Medley received the IEEE Region I Outstanding Teaching Award for the development of an undergraduate electrical and computer engineering program in the Mohawk Valley.