# PASSIVE SPREAD-SPECTRUM STEGANALYSIS

*Ming Li, Michel Kulhandjian, Dimitris A. Pados*[†]*, Stella N. Batalama*

Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
E-mail: {mingli,mkk6,pados,batalama}@buffalo.edu

*Michael J. Medley*

Air Force Research Laboratory/RIGF
525 Brooks Rd
Rome, NY 13441
E-mail: michael.medley@rl.af.mil

## ABSTRACT

We consider the problem of passive spread-spectrum steganalysis where the objective is to decide the presence or absence of spread-spectrum hidden data in a given image (a binary hypothesis testing problem). Unlike conventional feature-based approaches, we describe an unsupervised (blind) low-complexity approach based on generalized least-squares principles that may enable rapid high-volume image processing. Extensive experiments on image sets and comparisons with existing steganalysis techniques demonstrate most satisfactory classification performance measured in probability of correct detection versus induced false alarm rate.

***Index Terms***–Blind detection, covert communications, data hiding, spread-spectrum embedding, steganalysis, steganography, watermarking.

## 1. INTRODUCTION

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, audio, or text. The basic purpose of steganography is to establish covert communication between trusting parties and imposes the requirement of concealing (not encrypting) the existence of the hidden message.

Steganalysis is the countermeasure technology to steganography. A primary task of steganalysis is to decide the presence or absence of hidden messages in given media objects. We call this binary hypothesis testing problem *passive* steganalysis. In contrast, *active* steganalysis refers to the effort of extracting the actual hidden data.

In this work, we are interested only in passive steganalysis for rapid, high-volume processing of suspect images. Most existing passive steganalysis approaches [1]-[6] utilize feature classification techniques. With a training set consisting of clean cover and corresponding stego images with hidden information, features can be extracted from cover/stego images and their statistics are studied to design a classifier. The success of the steganalyst heavily depends on the ability to identify the statistical changes induced by the embedding and extract the sensitive features that can indicate these statistical changes. However, for transform domain spread-spectrum (SS) steganography [7]-[9], and in particular optimal spread-spectrum embedding [10],[11], in which random-noise-like secret message signals are added to the host, a limited number of features cannot always differentiate between plain images and their corresponding stego versions. Using a larger number of and/or higher-order statistics features can enhance the sensitivity of the feature detector, but significantly increases computational complexity [6].

In this paper, we describe a novel unsupervised, low-complexity passive SS image steganalysis procedure that is blind in nature (requires no training) and may support high-volume classification processing. Instead of extracting and evaluating features of a tested image, the developed passive steganalysis method makes a small number of independent attempts to blindly extract *potential* hidden data using the iterative generalized least squares (IGLS) algorithm [12]. Cross-correlation of the returned "hidden data" sequences constitutes the decision statistic on which the binary classifier operates. This (unsupervised) classifier performs favorably compared to conventional (supervised) feature-based approaches to SS steganalysis, is image independent, has low computational complexity, and exhibits remarkable sensitivity to small-payload SS data hiding.

## 2. SYSTEM MODEL AND NOTATION

In this section, we describe briefly the spread spectrum data hiding model and introduce our notation. 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 $\frac{N_1 \times N_2}{M}$. Each block $\mathbf{H}_1, \mathbf{H}_2, ...., \mathbf{H}_M$ is to carry $K$ hidden information bits coming -potentially- from $K$ distinct messages. Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform, for example). After transform calculation and vectorization (for example, by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_m) \in \mathbb{R}^{\frac{N_1 \times N_2}{M}}, m = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_m)$ we choose a fixed subset of $L \leq \frac{N_1 \times N_2}{M}$ 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.

[†]Corresponding author.

This work was supported in part by AFOSR under Grant FA9550-07-1-0400. Approved for Public Release; Distribution Unlimited: 88ABW-2011-0587, 16 FEB 11.

The $K$ distinct message bit sequences $\{b_k(m)\}_{m=1}^M$, $k = 1, 2, \ldots, K$, $b_k(m) \in \{\pm 1\}$, are hidden in the transform-domain host vectors $\{\mathbf{x}(m)\}_{m=1}^M$ via additive SS embedding by means of $K$ spreading sequences (signatures) $\mathbf{v}_k \in \mathbb{R}^L$, $k = 1, 2, \ldots, K$,

$$\mathbf{y}(m) = \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{x}(m) + \mathbf{n}(m),\ m = 1, \ldots, M, \quad (1)$$

where, for the sake of generality, $\mathbf{n}(m) \sim \mathcal{N}(\mathbf{0}, \sigma_n^2 \mathbf{I}_L)$ accounts for external white Gaussian noise[1] with variance $\sigma_n^2$. It is assumed that $b_k(m)$ behave as equi-probable binary random variables that are independent in time, $m = 1, ..., M$, and across messages, $k = 1, ..., K$. The contribution of each individual embedded message bit $b_k$ to the composite stego signal is $b_k \mathbf{v}_k$ and the mean-squared distortion to the original host data $\mathbf{x}$ due to the embedded $k$ message alone is

$$\mathcal{D}_k = \mathbb{E}\{\|b_k \mathbf{v}_k\|^2\} = \|\mathbf{v}_k\|^2,\ k = 1, 2, \ldots, K, \quad (2)$$

where $\mathbb{E}\{\cdot\}$ denotes statistical expectation.

Define the combined "disturbance" *to the hidden data* (host plus noise) $\mathbf{z}(m) \triangleq \mathbf{x}(m) + \mathbf{n}(m)$. Then, SS embedding by (1) can be rewritten as

$$\mathbf{y}(m) = \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{z}(m),\ m = 1, \ldots, M, \quad (3)$$

where $\mathbf{z}(m)$ is modeled as a sequence of zero-mean (without loss of generality) vectors with autocovariance matrix $\mathbf{R}_z = \mathbb{E}\{\mathbf{z}\mathbf{z}^T\}$ where $T$ denotes the transpose operator. For notational simplicity we form the compound data observation matrix as

$$\mathbf{Y} = \sum_{k=1}^{K} \mathbf{v}_k \mathbf{b}_k^T + \mathbf{Z} \quad (4)$$

where $\mathbf{Y} \triangleq [\mathbf{y}(1)...\mathbf{y}(M)] \in \mathbb{R}^{L\times M}$, $\mathbf{b}_k \triangleq [b_k(1) \ldots b_k(M)]^T \in \{\pm 1\}^{M\times 1}$, and $\mathbf{Z} \triangleq [\mathbf{z}(1) \ldots \mathbf{z}(M)] \in \mathbb{R}^{L\times M}$.

## 3. ITERATIVE GENERALIZED LEAST SQUARES PROCESSING

The objective of passive steganalysis is, given the observation matrix $\mathbf{Y}$ in (4), to decide whether $\mathbf{Y}$ is of the form of $\mathbf{Z}$ alone (non-stego image) or of the form $\sum_{k=1}^{K} \mathbf{v}_k \mathbf{b}_k^T + \mathbf{Z}$ (stego image) for some vectors $\mathbf{b}_k$, $\mathbf{v}_k$, $k = 1, ..., K$, and some $K \in \{1, 2, ...\}$.

To facilitate the presentation of our developments let us begin with the given case of $K = 1$ (data hidden with one signature only) where

$$\mathbf{Y} = \mathbf{v}\mathbf{b}^T + \mathbf{Z}. \quad (5)$$

If $\mathbf{Z}$ were to be modeled as Gaussian, the joint maximum-likelihood (ML) estimator of $\mathbf{v}$ and detector of $\mathbf{b}$ would be

$$\widehat{\mathbf{v}}, \widehat{\mathbf{b}} = \arg \min_{\widehat{\mathbf{v}} \in \mathbb{R}^L, \widehat{\mathbf{b}} \in \{\pm 1\}^M} \|\mathbf{R}_z^{-\frac{1}{2}}(\mathbf{Y} - \widehat{\mathbf{v}}\widehat{\mathbf{b}}^T)\|_F^2 \quad (6)$$

where $\|\cdot\|_F$ is the matrix Frobenius norm[2]. If Gaussianity of $\mathbf{Z}$ is not to be invoked, then (6) is simply referred to as the joint generalized least-squares solution of $\mathbf{v}$ and $\mathbf{b}$. In any case, regretfully, joint estimation of $\mathbf{v}$ and detection of $\mathbf{b}$ by (6) has complexity exponential in $M$ (the length of the hidden message in bits). To manage the computational complexity, we may attempt to reach a quality approximation of the solution of (6) by computing a generalized least squares update of one of the unknown vector parameters conditioned on a previously obtained estimate of the other vector parameter, iteratively. That is, pretend $\widehat{\mathbf{b}}$ is fixed/known; then, the least squares estimate of $\mathbf{v}$ is

$$\widehat{\mathbf{v}}_{\text{LS}} = \frac{1}{M}\mathbf{Y}\widehat{\mathbf{b}}. \quad (7)$$

Pretend, in turn, $\widehat{\mathbf{v}}$ is fixed/known; then, the hard-limited least squares estimate of $\mathbf{b}$ is

$$\widehat{\mathbf{b}}_{\text{LS}} = \text{sign}(\mathbf{Y}^T \widehat{\mathbf{R}}_y^{-1} \widehat{\mathbf{v}}) \quad (8)$$

where $\widehat{\mathbf{R}}_y = \frac{1}{M}\sum_{m=1}^{M} \mathbf{y}(m)\mathbf{y}(m)^T$.

The *iterative generalized least squares* (IGLS) procedure suggested by the two above equations is now straightforward [12]. Initialize $\widehat{\mathbf{b}} \in \{\pm 1\}^{M\times 1}$ arbitrarily and alternate iteratively between (7) and (8) to obtain at each step conditionally least-squares optimal estimates of one vector parameter given the other. Stop when convergence is observed. The computational complexity of the scheme is dominated by the inversion of the matrix $\widehat{\mathbf{R}}_y$ with general cost $\mathcal{O}(L^3)$. For the sake of mathematical accuracy, we note that there is always a global phase/sign ambiguity present in $\widehat{\mathbf{b}}_{\text{LS}}$ which can be overcome with a few known (or guessed) data symbols for phase/sign correction.

Consider now what can happen when the described IGLS scheme of (7), (8) is applied to an image that has undergone *multi-signature* (i.e. $K > 1$) message embedding. To illustrate the investigation, we consider the familiar $512 \times 512$ Baboon gray image and embed $K = 2$ messages $\mathbf{b}_1$, $\mathbf{b}_2$ of $4,096$ bits each via *multi-signature* SS embedding by (1) with arbitrary signatures $\mathbf{v}_1$ and $\mathbf{v}_2$, correspondingly. The length of the signatures is set at $L = 63$, the per-message distortion is $\mathcal{D}_k = 30$dB, $k = 1, 2$, and white Gaussian noise is added of variance $\sigma_n^2 = 3$dB. Next, we make $P = 100$ independent attempts to blindly extract hidden data by executing (7) and (8) with arbitrary distinct initializations $\widehat{\mathbf{b}}$. We call the corresponding returned decision vectors $\widehat{\mathbf{b}}^{(i)}$, $i = 1, \ldots, P$, and evaluate $\theta_1^{(i)} \triangleq \mathbf{b}_1^T \widehat{\mathbf{b}}^{(i)}/M$ and $\theta_2^{(i)} \triangleq \mathbf{b}_2^T \widehat{\mathbf{b}}^{(i)}/M$, $i = 1, \ldots, P$, which are the normalized cross-correlations between $\widehat{\mathbf{b}}^{(i)}$ and the true hidden message vectors $\mathbf{b}_1$ and $\mathbf{b}_2$, respectively. Under the assumption that message bits are statistically independent from each other, if $\widehat{\mathbf{b}}^{(i)}$ is a satisfactory

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

[2] Bas and Cayre [13] explain that if $\mathbf{z}(m)$, $m = 1, \ldots, M$, were white Gaussian vectors, then independent (principal) component analysis would readily reveal the signature vector $\mathbf{v}$. However, in general transform-domain image -for example- embedding, the structure of the autocorrelation matrix of $\mathbf{z}(m)$ is far from constant-value diagonal [10].

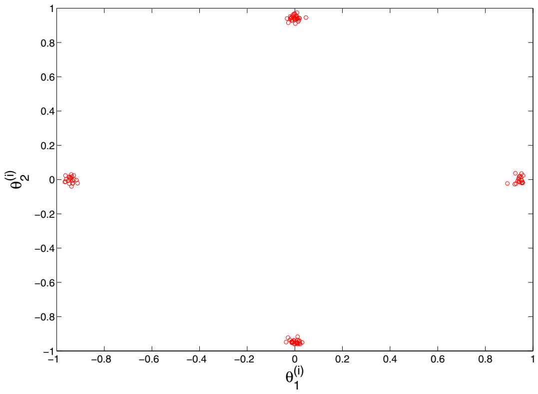


**Fig. 1.** Cross-correlation of $P = 100$ message vector decisions returned by IGLS (eqs. (7), (8)) with the two true hidden messages (Baboon $512 \times 512$ gray-scale host, data hiding by (1), $K = 2$, $L = 63$, $\mathcal{D}_1 = \mathcal{D}_2 = 30$dB, $\sigma_n^2 = 3$dB).

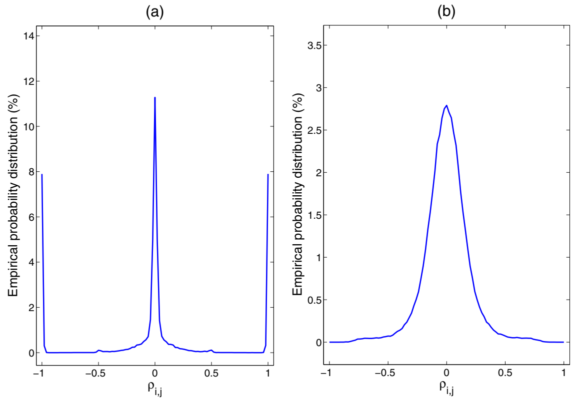


**Fig. 2.** Histogram of cross-correlation $\rho_{i,j}$ between vector decisions $\widehat{\mathbf{b}}_i$, $\widehat{\mathbf{b}}_j$, $i \neq j \in \{1, \ldots, P\}$, returned by IGLS (eqs. (7), (8)) on dataset [14]: (a) Stego tested images ($K \in \{1, 2, \ldots, 5\}$, $L \in \{30, 31, \ldots, 63\}$, $\mathcal{D}_k = 30$dB, $k = 1, \ldots, K$, $\sigma_n^2 = 3$dB); (b) plain tested images.

extraction of $\mathbf{b}_1$, $|\theta_1^{(i)}|$ is close to one and $|\theta_2^{(i)}|$ is near zero; on the other hand, if $\widehat{\mathbf{b}}^{(i)}$ is a satisfactory extraction of $\mathbf{b}_2$, $|\theta_2^{(i)}|$ is close to one and $|\theta_1^{(i)}|$ is near zero. Fig. 1 depicts the correlation of the $P = 100$ returned message decisions with the two hidden message on the two-dimensional Cartesian plane $(\theta_1^{(i)}, \theta_2^{(i)})$. Four tight clusters of correlations are seen around points $(\pm 1, 0)$, $(0, \pm 1)$. While $\mathbf{b}_1, \mathbf{b}_2$ are not known in practice and Fig. 1 cannot be produced, Fig. 1 indicates that the returned decision vectors themselves $\widehat{\mathbf{b}}^{(1)}, \widehat{\mathbf{b}}^{(2)}, \ldots, \widehat{\mathbf{b}}^{(P)}$ are tightly clustered in the $M$-dimensional space. This attribute, then, can form the basis for the development of a blind passive steganalysis algorithm as described in the following section.

## 4. IGLS-BASED PASSIVE SS STEGANALYSIS

Define $\rho_{i,j} \triangleq \widehat{\mathbf{b}}^{(i)T}\widehat{\mathbf{b}}^{(j)}/M$ to be the normalized cross-correlation between vectors $\widehat{\mathbf{b}}^{(i)}$, $\widehat{\mathbf{b}}^{(j)}$, $i \neq j \in \{1, \ldots, P\}$, returned by independent iterative executions of (7), (8). If both $\widehat{\mathbf{b}}^{(i)}$ and $\widehat{\mathbf{b}}^{(j)}$ were to be good estimates of the same message vector, then $|\rho_{i,j}|$ would be close to one. On the other hand, if $\widehat{\mathbf{b}}^{(i)}$ and $\widehat{\mathbf{b}}^{(j)}$ correspond/are estimates of two

**Table 1**. Blind IGLS-based Passive SS Steganalysis

**Input**: Data matrix $\mathbf{Y} \in \mathbb{R}^{L \times M}$.
**Initialization**: $\widehat{\mathbf{R}}_y^{-1} := [\frac{1}{M}\mathbf{Y}\mathbf{Y}^T]^{-1} \in \mathbb{R}^{L \times L}$; $P$; $\gamma$;
Stego $= 0$; $i = 0$.
**While** $i \leq P$
  $i = i + 1$
  Execute (7), (8) iteratively to convergence and obtain $\widehat{\mathbf{b}}^{(i)}$
  **If** $|\rho_{i,j} := \widehat{\mathbf{b}}^{(i)T}\widehat{\mathbf{b}}^{(j)}/M| > \gamma$ for any $1 \leq j < i$
    Stego $= 1$; $i = P + 1$.
  **End**
**End**

different message vectors, $|\rho_{i,j}|$ is to be near zero. To gain some experimental insight in the statistical properties of $\rho_{i,j}$, we consider the data set of [14] and embed a random number of messages $K \in \{1, 2, ..., 5\}$ via *multi-signature*, as needed, SS embedding by (1) with arbitrary signatures. The length of the signatures $L$ is drawn randomly from $\{30, 31, ..., 63\}$, the per-message distortion is fixed at $\mathcal{D}_k = 30$dB, $k = 1, \ldots, K$, and $\sigma_n^2 = 3$dB. We carry out $P = 100$ independent executions of (7), (8) with arbitrary distinct initializations $\widehat{\mathbf{b}}$ and plot in Fig. 2(a) the empirical probability distribution of $\rho_{i,j}$, $i \neq j \in \{1, \ldots, P\}$. A clear bimodal distribution around 0 and $\pm 1$ appears. In contrast, when $\rho_{i,j}$ is evaluated on non-stego, plain images (Fig. 2(b)), the distribution is much different, unimodal and Gaussian-like with very low probability of $|\rho_{i,j}| > 0.5$ [3].

The proposed blind binary classifier uses $|\rho_{i,j}|$ as its decision statistic. For a tested image, we execute (7), (8) iteratively $P$ times, to obtain returned vectors $\widehat{\mathbf{b}}^{(1)}, \widehat{\mathbf{b}}^{(2)}, \ldots, \widehat{\mathbf{b}}^{(P)}$. Then, we calculate $\rho_{i,j}$ for all $i \neq j \in \{1, ..., P\}$. If for a given threshold $0 \leq \gamma \leq 1$ there exists a pair $i, j$, $i \neq j$, such that $|\rho_{i,j}| > \gamma$, we classify the image as stego; else, we declare it plain. A larger $\gamma$ threshold value will induce lower probability of false alarm $P_{FA}$ and lower probability of correct identification $P_C$; a smaller $\gamma$ will raise both $P_{FA}$ and $P_C$.

To further reduce complexity and increase speed of processing, an on-line scheme is preferred over performing the classification after collecting all $P$ extraction vectors. When (7), (8) present us with a new extracted vector $\widehat{\mathbf{b}}^{(i)}$, $i > 1$, we examine all cross-correlations $\rho_{i,j}$ for $1 \leq j \leq i - 1$. If $|\rho_{i,j}| > \gamma$ for any $1 \leq j \leq i - 1$, we classify the tested image as a stego image; else, we continue to generate the next vector $\widehat{\mathbf{b}}^{(i+1)}$ until we exceed the pre-set number of trials $P$. We summarize the complete on-line IGLS-based passive steganalysis procedure in Table 1.

[3] In [13], Bas and Cayre present an interesting signature-based additive embedding approach different to (1) that is host-vector-by-host-vector dependent and would withstand passive steganalysis based on $|\rho_{i,j}|$ as we describe herein. The embedding is, however, sensitive to disturbance/noise that would lead to high recovery error rates by intended recipients and limit the applicability to general covert communication problems.

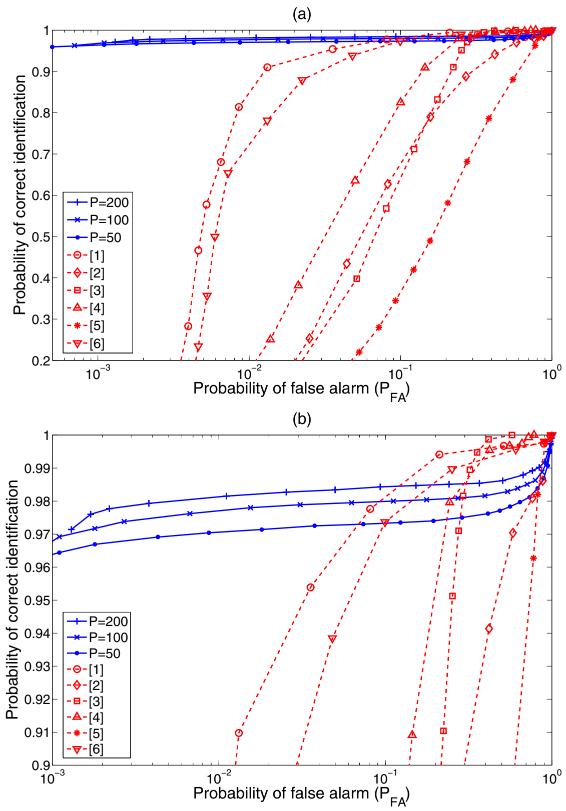


**Fig. 3.** (a) ROC curves of passive steganalysis procedures on dataset of about $1,500$ images [14], [15] ($K \in \{1, 2, \ldots, 5\}$, $L \in \{30, 31, \ldots, 63\}$, $\mathcal{D}_k = 26$dB, $k = 1, \ldots, K$, $\sigma_n^2 = 3$dB). (b) Zoom-in of (a).

## 5. EXPERIMENTAL STUDIES AND DISCUSSION

In this section we examine the performance of the blind passive SS steganalysis procedure described in Table 1. The experimental image data set consists of more than $1,500$ 8-bit gray-scale photographic images ([14] and [15] combined) 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-signature SS embedding by (1) with arbitrary signatures and payload between $0.016$ and $0.078$ bits per pixel (bpp). The length of the embedding signatures varies between $30$ and $63$ ($L \in \{30, 31, \ldots, 63\}$) and the per-message distortion is $\mathcal{D}_k = 26$dB, $k = 1, \ldots, K$. For the sake of generality, we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$dB in each image.

In Fig. 3(a) (and its zoom-in in Fig. 3(b)), we plot the "receiver operating characteristic" (ROC) curves that show the probability of correct identification ($P_C$) of a given passive steganalysis system versus probability of false alarm ($P_{FA}$). The threshold $\gamma$ of our proposed algorithm in Table 1 varies between $0.3$ and $0.97$ ($\gamma \in [0.3, 0.97]$) to obtain the varying $(P_C, P_{FA})$ paired values. Three ROC curves of the proposed algorithm are shown with run parameter $P = 50, 100$, and $200$. For comparison purposes, successful recent feature-based algorithms from [1]-[6] are also studied (dashed lines). Successful classification algorithms provide high probability of correct identification with low $P_{FA}$. Our proposed passive steganalysis procedure -although blind- is seen, for example, to offer more than $96\%$ identification success rate at $0.1\%$ false alarm rate with only $P = 50$ IGLS-based extraction attempts. Since each attempt uses the same pre-computed inversion of the data correlation matrix $\widehat{\mathbf{R}}_y$, the proposed method has quite low computational complexity in comparison with other passive steganalysis approaches [1]-[6].

## 6. REFERENCES


[1] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inform. Forensics and Security*, vol. 1, pp. 111-119, Mar. 2006.

[2] İ. Avcıbaş, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Trans. Image Proc.*, vol. 12, pp. 221-229, Feb. 2003.

[3] W. Lie and G. Lin, "A feature-based classification technique for blind image steganalysis," *IEEE Trans. Multimedia*, vol. 7, pp. 1007-1020, Dec. 2005.

[4] 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.

[5] 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.

[6] —, "Optimized feature extraction for learning-based image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 2, pp. 31-45, March 2007.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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 Proc. (ICIP)*, Singapore, Oct. 2004, vol. 2, pp. 1561-1564.

[12] 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.

[13] 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.

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

[15] 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.