Multimed Tools Appl
DOI 10.1007/s11042-014-1890-9

A new fast and efficient active steganalysis based on combined geometrical blind source separation

Hamed Modaghegh · Seyed Alireza Seyedin

Abstract We have presented a new *active* steganalysis method in order to break the block-discrete cosine transform (DCT) coefficients steganography. Our method is based on a combination of the Blind Source Separation (BSS) technique and Maximum A posteriori (MAP) estimator. We have additionally introduced a new geometrical BSS method based on the minimum range of mixed sources which reduces the computational cost of the proposed steganalysis. The high efficiency of this new combined method has been confirmed by enough experiments. These experiments show that, compared to the previous *active* steganalysis methods our *active* steganalysis method not only reduces the error rate but also causes a low computational cost.

Keywords Blind Source Separation (BSS) · *Active* steganalysis · MAP estimator · Independent Component Analysis (ICA) · Block-DCT steganography

1 Introduction

After the seminal works by Johnson and Jajodia [13, 14], steganalysis has attracted many interests [6, 9, 18, 20, 28]. A numerous different types of steganalysis techniques (STs), mostly passive, have been proposed [9, 18, 20, 28]. While Steganography deals with hiding information by embedding a message within another object (*cover*) such as image, steganalysis focuses on revealing those hidden messages from the *cover*. Steganalysis has gained prominence in the international security since the detection of hidden messages can lead to the prevention of disastrous events, such as terrorist attacks.

Current STs focus on detecting the presence of a hidden message in the *cover* (passive manner). A good survey of passive STs is provided by Nissar et al. [18]. They attempted to classify various approaches. They have categorized STs into signature and statistical techniques. Their categorization is either based on the signature of the applied technique or the image statistics which is used to detect the presence of hidden messages. Furthermore, in their classification, each category is sub-divided into specific and universal approaches.

H. Modaghegh (✉) · S. A. Seyedin
Department of Electrical Engineering, Ferdowsi University of Mashhad, Mashhad, Iran
e-mail: hamed.modaghegh@stu-mail.um.ac.ir

S. A. Seyedin
e-mail: seyedin@um.ac.ir

Published online: 14 February 2014

Specific steganalysis targets a particular steganographic technique [9, 10, 28]. These methods analyze the embedding operation and concentrate on some image features or statistics. Consequently, it may fail if any other steganography method is used or a very simple change occurs in the steganography algorithm. As a result, universal steganalysis [3, 16, 27] which mitigates the deficiency of specific STs were introduced. These methods could detect messages embedded using any type of steganographic technique and, moreover, without the prior knowledge of embedding technique. Most of them train a classifier with *cover* and *stego* images in the detection procedure.

After the detection procedure, in some cases, it is necessary to extract and determine the content of the hidden message (*active* steganalysis). In fact by revealing the hidden messages *active* steganalysis provides a complementary task to the passive one. Most of the STs focus on a passive manner; however, there has been a little attempt in developing *active* methods as well. In this scope, some researchers focus on a steganalysis method based on the blind sources separation (BSS) [2, 6, 8, 25, 26]. In the next section all these methods as well as their advantageous and disadvantageous are discussed. Here, we shortly state that most of the present *active* STs are neither fast nor enough efficient. Nevertheless, in this paper we propose an *active* steganalysis method which has a lower computational cost and error rate than those conventional techniques. Our method is based on the Maximum A posteriori (MAP) estimator and BSS which can extract hidden messages using only one *stego* image. Since the computational cost of the MAP estimator is lower than the BSS methods we extract most of the message using this estimator in the first step. Then we use the Independence Component Analysis (ICA) technique as a BSS to separate the rest of message from its *cover* image. Finally, we introduce a new geometrical BSS (GBSS) method based on minimizing the range of mixed signals probability density function (PDF) and we use it rather than ICA to reduce the computational cost even more than before.

To this end, we have organized the paper as follows: in Section 2 we present a brief overview of the current *active* STs and discuss both their advantageous and disadvantageous. We explain the BSS problem briefly in Section 3 and then we introduce our GBSS method in Section 4. In the next section the details of our *active* steganalysis method is presented. We finalize the paper by a discussion on the experimental evaluation in Section 6 while conclusions are drawn in Section 7.

2 A brief history of *active* STs

The first *active* ST was performed by Chandramouli [6]. He presented an *active* method with an effort on a linear steganography. His proposed method was based on the BSS model with a hypothesis that the *cover* image and hidden message were independent. However, his proposed method needed at least two *stego* images with the same message, *cover* and key but different embedding strength factor. However, these conditions are not practical since steganalyst can usually access one *stego* image only.

Fan et al. [8] tried to apply a method to realize *active* steganalysis when there was only one *stego* image copy. Their method was based on ICA and Hidden Morkov Tree (HMT) model [7]. ICA is a popular BSS technique and HMT model is mainly applied to denoise an image in the transform domain. They adopted HMT model to get the second copy of *stego* image and then the optimized ICA was applied to accomplish the *active* steganalysis.

Another research with the view of *active* steganalysis as BSS problem was presented in [26]. It solely used a single copy of *stego* image. The MAP estimator was adopted to obtain an estimate of the *cover* image. Two *active* steganalysis schemes was introduced in this method; the first

scheme was similar to [8] which considered the estimated version as another *stego* image. In the second scheme, in addition to the original *stego* image, two more *stego* images were generated from the estimated image. All the three images were used as input to the ICA algorithm. These schemes were applied to extract messages from the least significant bit (LSB) steganography in spatial, discrete cosine transform (DCT), and discrete wavelet transform (DWT) domains. Their experiments have proven that the second scheme has a better performance than the first one. The method proposed in [25] was similar to that of [26]. However, HMT model was applied in [25] while the MAP estimator was used in [26] to obtain an estimate of the *cover* image.

All these *active* steganalysis methods use ICA technique to separate message from image. This technique is an inherently high computational cost technique. Ambalavanan and Chandramouli, on the other hand, introduced another *active* steganalysis based on a different BSS technique [24] in order to reduce the computational cost and to improve the performance of message extraction [2]. However, their efforts were not successful. They embedded a *known* random signal to the *stego* image (first observed signal) in order to form the second observed signal. This made the columns of mixing matrix, linearly dependent and therefore a deficiency happened in the rank of this matrix. Since the mixing matrix must be a full rank matrix in an underdetermined BSS [24], one cannot use it effectively in steganalysis [2].

3 Preliminary: blind source separation

A brief overview on the blind source separation problem and so far solutions [15] are given in the current section. The goal of source separation is to retrieve unknown source signals, $S(n) = (s_1(n), \ldots, s_m(n))^T$, from observed signals, $X(n) = (x_1(n), \ldots, x_p(n))^T$. The observed signals are an unknown function of the source signals so that:

$$X(n) = F(S(n)), \tag{1}$$

Where $F(.)$ is a function from $\mathbb{R}^m$ to $\mathbb{R}^p$ and denotes the unknown mixture function. Indeed, the main idea for separating the sources is to estimate $G(.)$ which is the inverse of the mixture function $F(.)$. Clearly, we need to make some assumption in order to solve this problem. Basically, it is necessary to have a prior knowledge about:

1) The nature of the mixture function, e.g. we need to know if it is linear, nonlinear, or convolutive. The problem has been solved for linear, instantaneous and convolutive mixtures so far and recently a few researchers have concentrated on nonlinear mixtures.
2) The source properties, e.g. its independency, sparsity, being bounded/unbounded and etc. Those methods which are based on the property of source independency are called independent component analysis (ICA). On the other hand, the sparse component analyses (SCAs) are based on the property of the source sparsity. When the sources are bounded, we can use simple geometrical interpretations and some methods can also be used to separate the source signals [5, 22].

4 Proposed geometrical BSS method

As mentioned in the previous section when the sources are bounded, simple geometrical methods can be applied. In this section a geometrical method based on the range of mixed signals is proposed. The main idea of the presented method is that the marginal distribution

range of two-variate independent random variable (random vector) increase as it rotates around the center of coordinate system. This idea is mathematically proven using three presented propositions.

We rotate the already whitened data around the coordinate system to minimize the marginal range of mixed signals and then extract the independent components. Notice that mixed signals are rotated with both the fixed and variable step size.

The main steps of our proposed method are comprehensively illustrated in the following subsections.

4.1 Whitening

In the first step, the observed signals X should be whitened. A zero mean random vector $Z=(z_1,\ldots,z_m)^T$ is defined as white if its elements z_i are uncorrelated and have unit variances:

$$E\{z_i z_j\} = \delta_{ij} \tag{2}$$

Obviously, this definition can be stated in terms of the covariance matrix, $E\{ZZ^T\}=I$, where I is a unit matrix. Whitening operation is linearly possible since it is a decorrelation process followed by a scaling one. Therefore, the problem of whitening reduces to finding a linear transformation V for a given random vector X such that $Z = VX$ would be white.

One of the popular methods for whitening is the eigenvalue decomposition (EVD) of the covariance matrix:

$$C_x = E\{XX^T\} = EDE^T \tag{3}$$

Where E is the orthogonal matrix of eigenvectors of $E\{XX^T\}$ and D is the diagonal matrix of its eigenvalues, $D = diag(d_1,\ldots,d_m)$. Therefore, whitening matrix V may be defined as:

$$V = D^{-1/2}E^T \tag{4}$$

While D is a diagonal matrix, $D^{-1/2}$ is computed by a simple component wise operation as $D^{-1/2}=diag({d_1}^{-1/2},\ldots,{d_m}^{-1/2})$.

Matrix V always exists when d_i is positive; this condition is respected since C_x is positive semidefinite and in practice positive definite for almost any natural signals.

Since E is an orthogonal matrix which satisfies $E^TE = EE^T = I$, C_z may be denoted by:

$$E\{ZZ^T\} = VE\{XX^T\}V^T = D^{-1/2}E^TEDE^TED^{-1/2} = I \tag{5}$$

The covariance of Z is unity, so Z is white. The linear operator V in (4) is not unique. It is clear that any matrix $U \times V$, where U *is* an orthogonal matrix, is also a whitening matrix. Whitening does not give independent components (ICs) solely. This is because ICs of the mixture are unique while the whitening matrix is not [12].

Besides, whitening is useful as a preprocessing step in ICA. Let Z be the new mixture vector instead of X, So A' would be the new mixing matrix so that: $Z=V\times X=V\times A\times S=A'\times S$. It is obvious from $E\{ZZ^T\}=A'E\{SS^T\}A'^T=A'A'^T=I$ that A' is orthogonal.

This fact reduces our search space of mixing matrix with m^2 degrees of freedom to orthogonal matrices with $m\ (m - 1)/2$ degrees of freedom. For example, in two dimensional case, an orthogonal transformation is determined by a single parameter.

Since there are usually two independent sources in steganalysis problem, the 2×2 orthogonal matrix A' which is a rotation matrix with parameter θ must be estimated as:

$$A' = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{6}$$

In two-dimensional space we can say that whitened signals are rotations of independent signals and matrix A^{-1} rotate them back into the independent signals. So in the second step, in order obtain ICs, the inverse of orthogonal matrix A' must be estimated.

4.2 Obtaining independent component

Some criteria such as nonlinear correlations, kurtosis and etc., are used in BSS methods to obtain ICs [12]. Some other BSS methods exploit geometrical feature of PDF to estimate matrix A' [5, 22]. For example, the parallelepiped edges of PDF is estimated in [22]. As mentioned previously in the beginning of the current section, we use the marginal distribution range criterion in our proposed method to obtain ICs. At this point, we present some prepositions and corollaries to prove this idea mathematically. One may refer to the appendix for the proof.

Proposition 1 *Let s_1 and s_2 be considered as two zero mean finite independent random variables and vector Z be defined as rotation of vector* $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$:

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = rotate(\theta) \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \tag{7}$$

Then:

$$\begin{cases} \min(\max z_1, \max z_2) = \min(\max s_1, \max s_2) & for \quad \theta = 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/_{2} \\ \min(\max z_1, \max z_2) > \min(\max s_1, \max s_2) & otherwise \end{cases} \tag{8}$$

Corollary1 *suppose that the range of random variables s_i is symmetric then we can write*:

$$Range(s_i) = \max s_i - \min s_i = \max s_i - (-\max s_i) = 2 \times \max s_i \tag{9}$$

Now According to proposition 1 we obtain:

$$\begin{cases} \min(\text{Range } z_1, \text{Range } z_2) = \min(\text{Range } s_1, \text{Range } s_2) & for \quad \theta = 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/_{2} \\ \min(\text{Range } z_1, \text{Range } z_2) > \min(\text{Range } s_1, \text{Range } s_2) & otherwise \end{cases} \tag{10}$$

Proposition 2 *suppose that s_1 and s_2 are two zero mean asymmetric range random variables and vector Z is rotation of vector* $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ *then*:

$$\begin{cases} \min(\text{Range } z_1, \text{Range } z_2) = \min(\text{Range } s_1, \text{Range } s_2) & for \quad \theta = 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/_{2} \\ \min(\text{Range } z_1, \text{Range } z_2) > \min(\text{Range } s_1, \text{Range } s_2) & otherwise \end{cases} \tag{11}$$

As it can be seen from preposition 2 and corollary 1, if an independent random vector with symmetric or asymmetric marginal range is rotated around the center of coordinate system the range of marginal distribution will be increased. The minimum range occurs in $\theta = 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/2$ where its marginal random variables are independent. Since in the BSS problem the initial sources are independent, the independency of rotated random vector is equivalent to the source separation.

Contrary to proposition 1, 2 and corollary 1 which was about the feature of a rotated random vector, proposition 3 helps us to develop a BSS method.

Proposition 3 *Suppose s_1 and s_2 are two zero mean finite independent random variables and we define Z^θ as below*:

$$\begin{bmatrix} z_1^\theta \\ z_2^\theta \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = Rotate(\theta) \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \tag{12}$$

we also define Z^{θ_i} as a rotation of Z^θ; i.e.,;

$$\begin{bmatrix} z_1^{\theta_i} \\ z_2^{\theta_i} \end{bmatrix} = Rotate(\theta_i) Z^\theta \tag{13}$$

Now

$$\begin{aligned} &if\ \forall \theta_i \quad \exists \theta_0 \quad \ni \min\left(\max z_1^{\theta_0}, \max z_2^{\theta_0}\right) \le \min\left(\max z_1^{\theta_i}, \max z_2^{\theta_i}\right) \\ &then \begin{cases} z_1^{\theta_0} = \pm s_1 \\ z_2^{\theta_0} = \pm s_2 \end{cases} \quad or \quad \begin{cases} z_1^{\theta_0} = \pm s_1 \\ z_2^{\theta_0} = \pm s_2 \end{cases} \end{aligned} \tag{14}$$

Proposition 3 may be proved based on proposition 1. Proposition 3 has been achieved for the *maximum* of marginal variable. Accordingly a similar proposition may be found for the *range* of marginal variable and can be proved based on proposition 2.

This preposition is used to develop the proposed geometrical BSS method. Proposition 3 states that the rotated random vector Z^{θ_0} which is obtained by θ_0 is independent. In order to estimate θ_0, one should rotate whitened signals for different value of θ_i and then calculate the range of marginal PDF. Eventually, the *i*th θ_i which corresponds to the minimum range is selected as θ_0. Different algorithms can be applied to generate θ_i. In the beginning, we use a simple algorithm to generate θ_i . We present $\theta_{i+1} = \theta_i + \Delta\theta$ where $\Delta\theta$ is a fix value and the initial value θ_1 is chosen to be zero. The accuracy of method increases as $\Delta\theta$ decreases. In the proposed method it is enough to select θ_i in the range $0<\theta_i<90$ rather than $0<\theta_i<360$. This is because the minimum is repeated in each 90° interval. It can be seen from proposition 3 that these minima provide similar independent sources with different orders and signs.

We also implement our method with variable step sizes, i.e.; $\Delta\theta_i = Sgn \times k \times \Delta\theta$, where $k \in \{1,2,3,\ldots\}$ and *Sgn* determines the sign of k . This method is similar to adaptive delta modulation [1] method which is used in digital communications. The algorithm starts with the initial value $k=+1$ and arbitrary value θ_i. If the minimum range of rotated signals decreases then k increases by one otherwise *Sgn* is changed and k is returned to its initial value i.e. $k=1$. In fixed step size algorithm signals must be rotated $N = {}^{90}/_{\Delta\theta}$ times and this algorithm helps us to decrease the N without loss of the accuracy. The experimental results also show that N decreases nearly to ¼.

The mixing matrix cannot be exactly estimated so there is some indeterminacy in the estimation of sources. The amplitude of source cannot be determined due to the whitening process. Proposition 3 causes ambiguities in the sign and order of sources as well. However, these ambiguities are fortunately insignificant in steganalysis.

5 Proposed steganalysis method

Common steganography techniques can be modeled as an additive embedding – the sum of image features and message - and their steganalysis can be formulated as a BSS problem. From

a BSS viewpoint, the image features and message are sources which are mixed to form the *stego* image as an observation. In this case the number of observations is less than the number of sources, hence the problem is underdetermined, and therefore there is an infinite number of solutions. As a result, in order to select one solution among all available solutions it is necessary to impose certain additional constraints based on previous knowledge. Since most of the sources in steganography are sparse, the sparsity of sources may be used as a constraint to solve the problem.

Here, we introduce our *active* steganalysis method which can be used for breaking the block-DCT coefficients steganography techniques. In order to solve an underdetermined BSS problem (steganalysis) we exclusively take the advantage of the sparsity feature of sources and do not add a random message to the *stego* image for generating the second observation [2].

Initially, a MAP estimator is designed based on the sparsity of DCT coefficients and message PDF to select samples (DCT coefficient of the *stego* image) which corresponds to the message event. Then ICA technique is used for the rest of samples in order to extract message bits which remain. Finally, with the goal of reducing computational cost, the proposed GBSS method is alternatively used (instead of the common ICA method). At this point, we are ready to illustrate the detail of our proposed method.

Let us consider a sparsity model for the PDF of the sources as follows,

$$p_{s_j}(s_j) = p_j \delta(s_j) + \left(1 - p_j\right) f_{S_j}(s_j) \tag{15}$$

where pj is sparsity factor of the source and f_{Sj} denotes the distribution of s_i when the corresponding source is active. The probabilistic model of (15) can be used for DCT coefficients and low rate message embedding since both of them are sparse enough.

In order to formulate the MAP estimator, we define the events based on the sources that are active at a particular sample as follows:

- Case 1: when the image source is only active
- Case 2: when the message source is only active
- Case 3: when message and image sources are both active
- Case 4: when the sources are all inactive.

In order to calculate a posterior probability of events occurring given the observations, we should find the priori probability of events and the conditional probability of the observations given events occurring. The priori probability of each event can be obtained by:

$$P\left(ac_{i,j}\right) = \prod_{k=i,j} (1 - p_k) \prod_{k \neq i,j} p_k \tag{16}$$

where $ac_{i,j}$ represents the event when s_i and sj are active. In general, linear mixing of sources is defined as $y = a_1 s_1 + a_2 s_2$. This equation can be written as: $y = c + \alpha w$ in the additive DCT steganography:

$$Y = [\, a_1 \quad a_2 \,] \times \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = [\, 1 \quad \alpha \,] \times \begin{bmatrix} c \\ w \end{bmatrix} \tag{17}$$

where y denotes the DCT coefficient of *stego* image as observation, α is the embedding coefficient and w and c are respectively the message source and DCT coefficient of image as the second source. Now, the conditional probability of events can be computed as follows:

When none of the sources are active then the conditional probability is $P(y|c_0) = \delta(y)$. If only one source s_i is active then the conditional probability is given by,

$$P\left(y\middle|ac_i\right)=\frac{1}{|a_i|}f_{s_i}\left(\frac{y}{a_i}\right) \tag{18}$$

In general, if two random variables are added together then the PDF of their summation will be the convolution of the initial random variable PDFs [19]. Therefore, when two sources are active, the conditional probability can be written as:

$$P\left(y\middle|ac_{i,j}\right)=\frac{1}{|a_1|}f_{s_i}\left(\frac{y}{a_1}\right)\otimes\frac{1}{|a_2|}f_{s_j}\left(\frac{y}{a_2}\right) \tag{19}$$

As soon as the prior and conditional probabilities for the different events are obtained, the probability of the events occurring given the observation can be defined using Bayesian rule:

$$P\left(ac_i\middle|y\right)\propto P\left(y\middle|ac_i\right)P(ac_i) \tag{20}$$

Once the *a posterior* probability of all the events are known then the MAP estimator can be used to choose the specific event which maximizes $P(ac_i|y)$. Based on the chosen event we obtain the estimation of the sources.

When the chosen event is Case 1, the observed sample is an estimation of the message. In Case 2, the observed sample is an estimation of the image source and it is not useful in steganalysis. In Case 3 when two sources are active the ICA technique will be used to separate the message from image. Based on the assumption of ICA we need two different observations of the sources while in practice we have only one. Therefore, another observation from the *stego* image must be generated. Since embedding causes changes in *cover*, these changes can be considered as noises and a denoising method can be applied to reduce the noise rate:

$$\widehat{c}=c+\beta w \tag{21}$$

Where β is constant ($\beta<\alpha$) and $\widehat{c}$ represents the denoised version of *stego* image that will be used as the new observation. The experimental results show it is feasible and the results are acceptable.

There are many types of denoising algorithms which remove noise from the image. Each algorithm is suitable for a special kind of noise [4]. In this paper, one denoising algorithm is employed to obtain an acceptable performance for many different types of noise. "Bayesian Least Squares-Gaussian Scale Mixture" (BG) is one of the most effective denoising algorithms for removing homogeneous additive noise from natural images [21] which we use it here.

Now we have two observations: the original *stego* image y and a denoised image $\widehat{c}$. Therefore, we can complete (17) as:

$$\underbrace{\begin{bmatrix} y \\ \widehat{c} \end{bmatrix}}_{O}=\underbrace{\begin{bmatrix} 1 & \alpha \\ 1 & \beta \end{bmatrix}}_{A_{2\times 2}}\underbrace{\begin{bmatrix} c \\ w \end{bmatrix}}_{S} \tag{22}$$

Since $\beta\neq\alpha$, A is a full rank matrix and we can use the ICA method to solve (22). As mentioned above, we only use samples of the Case 3 as the input to ICA and we do not need all samples in our method. This effectively reduces the computational cost of

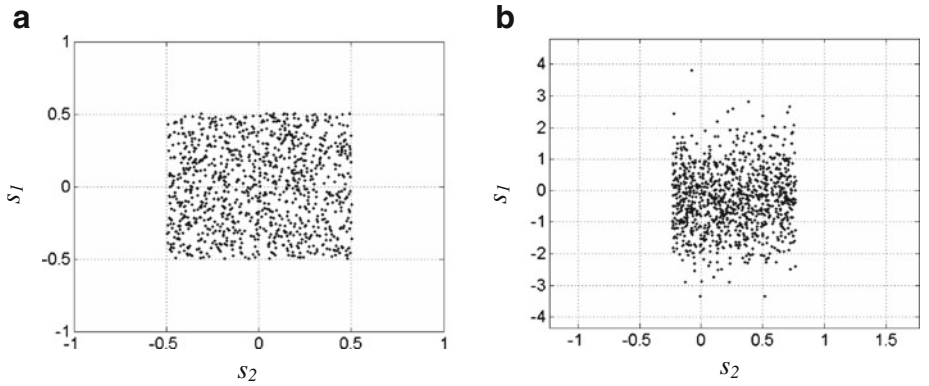

Fig. 1 The joint distribution of independent components s_1 and s_2 with uniform distributions (**a**), s_1 with uniform and s_2 with Gaussian distribution (**b**)

our proposed steganalysis method. There are many ICA methods which can be applied into our steganalysis. Here, FastICA [11] is adopted due to its fast convergence speed and high reliability among the other available methods. After applying FastICA on the observations we have:

$$\left(\widehat{S}, \widehat{A}\right) = FastICA(O) \tag{23}$$

where $\widehat{S}$ and $\widehat{A}$ represent estimation of sources and mixing matrix A, respectively. Since we have two observations in our steganalysis method, the GBSS method can be applied instead of FastICA. We present some experimental results to compare the performance of these two methods. Experimental results show that the computational cost of GBSS method is obviously less than FastICA.

It is important to mention here that the overall computational cost of our proposed steganalysis compared to the common *active* methods using ICA is reduced in two stages: Firstly, by using GBSS method which has lower computational cost. Secondly, by reducing the number of samples that GBSS method uses as its input.

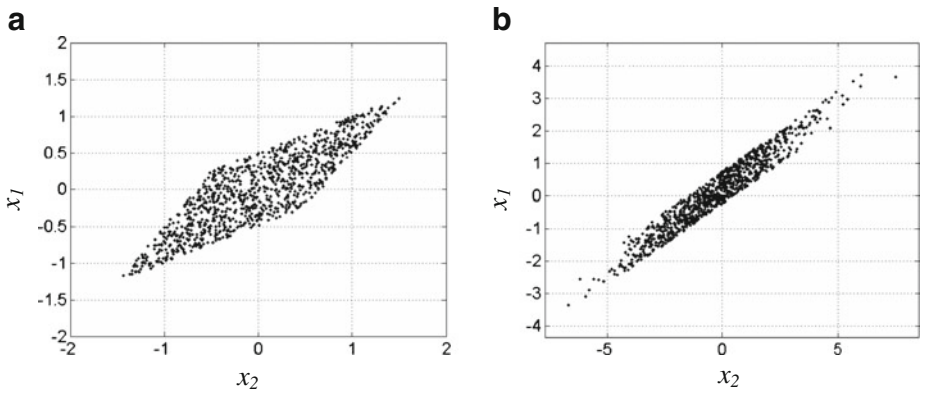

Fig. 2 The joint distribution of the observed signals x_1 and x_2

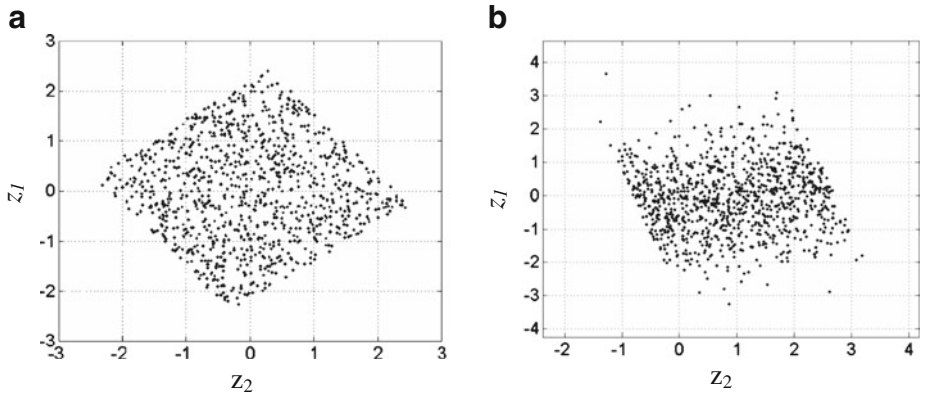

Fig. 3 The joint distribution of the whitened signals z_1 and z_2

6 Experimental results

The simulation results of the proposed GBSS and steganalysis method are presented in this section in order to evaluate their performance. All simulations are done using MATLAB [17].

6.1 Geometrical BSS experimental results

Initially, GBSS method is simulated using 1000 i.i.d. random vectors (two dimensional) with two different distributions as independent sources. Figure 1 illustrates the distribution of sources. In case (a) the distribution of two sources is uniform but in case (b) one of the sources has Gaussian distribution with the zero mean and unit variance. The mixture of two sources with mixing matrix $A = \begin{bmatrix} 1 & 2 \\ 1.5 & 1 \end{bmatrix}$ is shown in Fig. 2. As mentioned in Section 2, the first step of GBSS is whitening. The result of this step is shown in Fig. 3. In the next step whitened signals is rotated for $\theta_i \in (0,90)$ with the fixed $\Delta\theta=1$. The range of marginal PDF is calculated and shown in Fig. 4. As it can be seen from Fig. 4, the i*th* θ_i which corresponds to

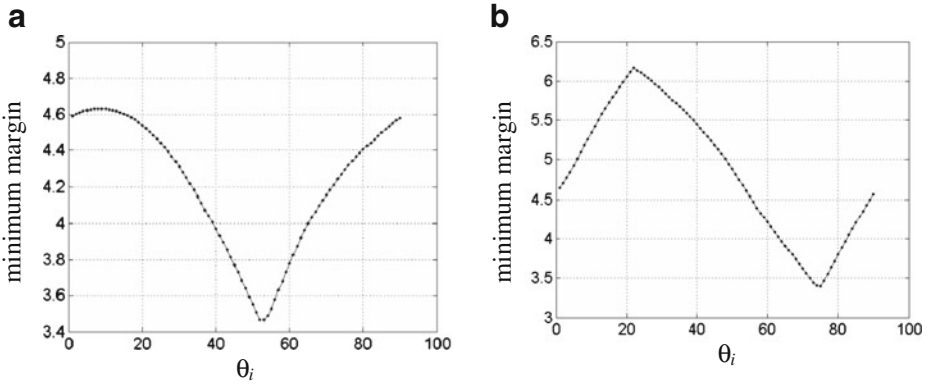

Fig. 4 Minimum marginal distribution range of the whitened signals which are rotated by$\theta_i \in (0,90)$ with a fixed step size

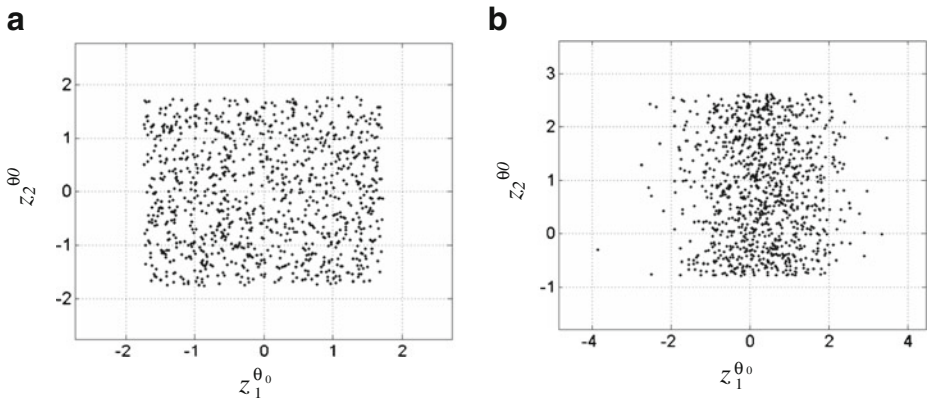

Fig. 5 Joint distribution of the whitened signals which are rotated by θ_0 (extracted independent components)

the minimum range of marginal PDF (θ_0) is 53° in Fig. 4a and 75° in Fig. 4b. In order to obtain independent sources we rotate the whitened signals by θ_0 (Fig. 5). As it can be seen from Figs. 1 and 5 it is clear that the scale and order of separated independent sources have been changed compared to the initial sources.

The simulations of our proposed method with variable step size have also been performed with an initial step size of $\Delta\theta = 1$. Figure 6 shows the minimum range and θ_i of our method while $i = 1, \ldots, N$. As can be seen from Fig. 6 the convergence speed of variable step size algorithm is high. The signal rotation is only performed N=21 times which is significantly less than fixed step size algorithm ($N = 90$ for $\Delta\theta = 1$).

To evaluate the computational cost of our GBSS method we compare it with the FastICA algorithm. We have run these methods on a 2.00 GHz Pentium 4 workstation and obtain their computational time for random inputs. We did this experiment 500 times (Table 1). The mixed sources which described above are used as the input of these methods.

As it can be seen from Table 1 the proposed method significantly reduces the computational cost of the source separation in comparison with the FastICA method. The very low obtained variance indicates that all the resulting times are close to the mean value so that our results supposed to be (reduction of the computational time) correct for about all inputs.

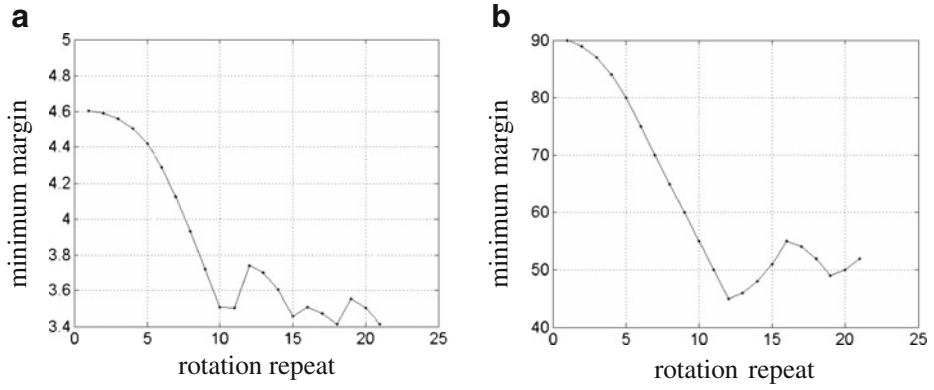

Fig. 6 Minimum marginal distribution range of the rotated whitened signals (**a**) and θ_i (**b**) in each step of variable step size algorithm

Table 1 The computational time of GBSS and FastICA algorithm for random inputs (mean and variance have been obtained from 500 times of running the algorithm)

Method	Computational time (second)	
	Mean	Variance
FastICA	0.0055	7.1024×10^{-4}
our GBSS (fixed step size = 2.5°)	0.0036	7.4155×10^{-6}
our GBSS (variable step size)	0.0019	1.3747×10^{-6}

6.2 Experimental results of the proposed steganalysis

At this point, we show the simulation results of our *active* steganalysis method. For evaluating of our steganalysis method we use Berkeley Segmentation Data Set and Benchmarks 500 (BSDS500) [23] which is a dataset consists of 500 natural color images. These color images span a range of indoor and outdoor scenes and they are JPEG compressed with the quality of 75 %. We convert these images into the uncompressed grayscale images and use only the central 256×256 region of each image.

Quality factor 75 is selected because the default quality setting on most digital cameras and image editors is 75, which gives a good tradeoff between the file size and perceived quality.

The sparsity factor of DCT Coefficient (p_{S1}) for our dataset is about 0.8 and p_{S2} which is the sparsity factor of embedded message is selected to be 0.5 (i.e. message is embedded in 50 % of DCT coefficient) in the first simulation (Table 2) and different embedding rate would be selected in the next (Table 3). Binary message bits (±1) is randomly embedded in the DCT coefficients with α=4. For an example, an original, a denoised and a *stego* image with 50 % embedded data rate have been shown in Fig. 7.

The results of extracting message from 500 *stego* image with the proposed steganalysis method and ICA based steganalysis method (old *active* steganalysis methods which are based on the ICA [8, 25, 26]) are shown in Table 2.

Threshold is applied on the extracted independent signal to detect the message. The threshold is selected so that the length of detected message becomes almost equal to the length of embedded one. In Table 2, two types of error have been presented: Not detected message bits are those embedded message bits that their location have not been detected correctly whereas the false detected message bits are embedded message bits that their location have been detected correctly but the sign of detected sample is not equal to those embedded. Error rate is defined as:

$$Error = \frac{\text{Not detected bits} + \text{False detected bits}}{\text{Number of embedded message}} \tag{24}$$

Table 2 Comparison between our proposed steganalysis and the ICA based steganalysis method for the message extraction from 500 *stego* images

Active steganalysis method	Mean of not detected message bits	Mean of false detected message bits	Mean of true detected message bits	Mean of error bits	mean of error rate (%)
ICA based steganalysis (previous methods)	7079	1990	23830	9068	27.56
proposed steganalysis method	6055	807	25878	6922	21.10

Table 3 Mean of the error rate for message extraction from 100 *stego* images. Message embedding rate varies from 10 % to 90 %

Message embedding rate	10 %	20 %	30 %	40 %	50 %	60 %	70 %	80 %	90 %
Error rate mean of proposed steganalysis method	22.89 %	21.98 %	21.82 %	21.58 %	21.13 %	21.39 %	21.32 %	21.27 %	21.33 %
Error rate mean of ICA based steganalysis	24.68 %	25.64 %	26.11 %	26.93 %	27.51 %	28.39 %	29.11 %	30.00 %	30.80 %

As can be seen from Table 2 our proposed method has a lower error and higher true detected bits compared to the ICA based steganalysis methods. Table 3 shows the comparative error rate of steganalysis methods for different message embedding rate as well. The results confirm that our method has almost similar performance for all embedding rates but the error rate in ICA based steganalysis increases for a higher embedding rate .It was expected because when the embedding rate increases the quality of image decreases and denoising algorithm cannot provide a good estimated version of the *cover* image. Our proposed method, in contrast, extracts most of the data in MAP estimation phase which is independent of the denoising algorithm.

We have also plotted the comparative figure for different embedding rate (Fig. 8).

When the *cover* image is an uncompressed image most of the DCT coefficients are non-zero and therefore the sparsity factor of DCT coefficient is low and the image source is *active* in most of the samples. As a result, in our proposed method the MAP estimator cannot detect message and the BSS method must be used to extract them. In this case, the result of our steganalysis method would be similar to of ICA based steganalysis methods.

Finally, we compare the computational time of ICA based steganalysis methods with our proposed steganalysis method when using FastICA and GBSS. The computational time of applying steganalysis methods on *stego* image with different random message have been shown in Table 4.

Fig. 7 Original Lena image (**a**) *stego* image (**b**) denoised image (**c**)

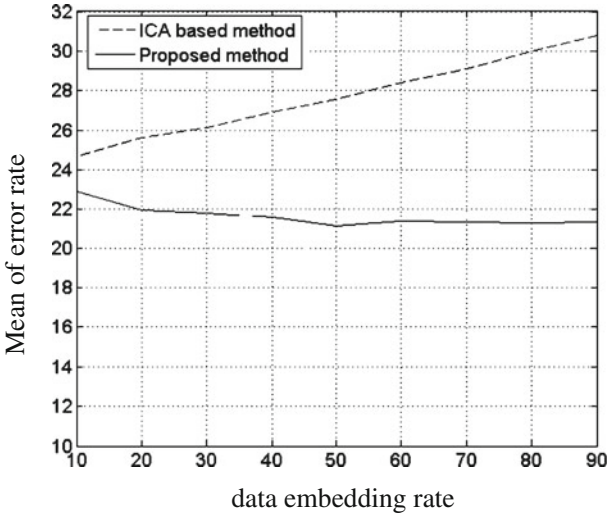

Fig. 8 Mean of the error rate for message extraction from 100 *stego* images

In order to make a better comparison the time of common parts such as denoising algorithm and DCT calculations are removed in this table.

As we had expected, the computational time of our proposed steganalysis method is lower than ICA based steganalysis methods. When GBSS is alternatively used instead of FastICA in steganalysis method the computational time is reduced again.

7 Conclusions

In this paper a new *active* steganalysis method based on the combination of MAP and BSS algorithms has been proposed. It is proved here that this method has a good performance on *cover* which had previously been stored in the JPEG format. A comparison between our proposed method with the previous *active* steganalysis schemes shows that applying MAP and BSS improve the steganalysis performance. Experiments show that nearly 78 % of the message bits can be estimated.

A new geometrical BSS method has been introduced based on a minimum marginal PDF. This method is analyzed theoretically. Experimental results show that its computational cost is

Table 4 The computational time of extracting message from 500 *stego* images by our steganalysis and ICA based steganalysis

Method	Computational time (second)	
	Mean	Variance
FastICA (old method)	0.2183	0.0052
MAP and FastICA (our method 1)	0.1684	0.1774
MAP and GBSS (our method 2)	0.1223	0.0035

lower compared to the FastICA. Finally, the new GBSS method is used in order to reduce the computational cost of our proposed steganalysis method.

Appendix

Proof of Propositions which was stated in paper.

Proof of Proposition 1:

We have by (7):

$$\theta = 0, \pi \Rightarrow \begin{cases} z_1 = \pm s_1 \\ z_2 = \pm s_2 \end{cases}, \quad \theta = {}^{\pi}/_{2}, {}^{3\pi}/2 \Rightarrow \begin{cases} z_1 = \pm s_2 \\ z_2 = \pm s_1 \end{cases} \tag{25}$$

So it is clear that:

$$\min(\max z_1, \max z_2) = \min(\max s_1, \max s_2) \tag{26}$$

Now let us proof (8) for other θ. Without loss of generality assume:

$$\max s_1 = K \max s_2 \tag{27}$$

Then according to (1–1), we have:

$$\begin{aligned} \max z_1 &= \max s_2 \times (|\cos\theta| K + |\sin\theta|) \\ \max z_2 &= \max s_2 \times (|\sin\theta| K + |\cos\theta|) \end{aligned} \tag{28}$$

$$\begin{aligned} \max z_1 &= \max s_1 \times \left(|\sin\theta|/K + |\cos\theta|\right) \\ \max z_2 &= \max s_1 \times \left(|\cos\theta|/K + |\sin\theta|\right) \end{aligned} \tag{29}$$

Using (28) gives us:

$$\begin{aligned} &K \geq 1 \Rightarrow \min(\max s_1, \max s_2) = \max s_2 \\ &\quad , \max z_1 \geq \max s_2 \times (|\sin\theta| + |\cos\theta|) \\ &\quad , \max z_2 \geq \max s_2 \times (|\sin\theta| + |\cos\theta|) \\ &\Rightarrow \max z_1, \max z_2 \geq \min(\max s_1, \max s_2) \times (|\sin\theta| + |\cos\theta|) \quad (1\text{–}6) \end{aligned} \tag{30}$$

And for other value of K we use (29):

$$\begin{aligned} &K < 1 \Rightarrow \min(\max s_1, \max s_2) = \max s_1 \\ &\quad , \max z_1 \geq \max s_1 \times (|\sin\theta| + |\cos\theta|) \\ &\quad , \max z_2 \geq \max s_1 \times (|\sin\theta| + |\cos\theta|) \\ &\Rightarrow \max z_1, \max z_2 \geq \min(\max s_1, \max s_2) \times (|\sin\theta| + |\cos\theta|) \end{aligned} \tag{31}$$

As it can be seen (30) and (31) are equal so it can be written:

$$\max z_1, \max z_2 \geq \min(\max s_1, \max s_2) \times (|\cos\theta| + |\sin\theta|) \tag{32}$$

Since $\theta \neq 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/2$ and triangle inequality theorem:

$$\begin{aligned} &|\cos\theta| + |\sin\theta| > 1 \Rightarrow \max z_1, \max z_2 > \min(\max s_1, \max s_2) \\ &\Rightarrow \min(\max z_1, \max z_2) > \min(\max s_1, \max s_2) \end{aligned} \tag{33}$$

Proof of Proposition 2:

According to (7), we have:

$$\begin{aligned} \max z_1 &= |\cos\theta|\max s_1 + |\sin\theta|\max s_2 \\ \max z_2 &= |\sin\theta|\max s_1 + |\cos\theta|\max s_2 \\ \min(z_1) &= |\cos\theta|\min(s_1) + |\sin\theta|\min(s_2) \\ \min(Z_2) &= |\sin\theta|\min(S_1) + |\cos\theta|\min(S_2) \end{aligned} \tag{34}$$

Without loss of generality assume:

$$Range(s_1) = K \times Range(s_2) \tag{35}$$

Using (34) gives us:

$$\begin{aligned} Range(z_1) &= \max z_1 - \min z_1 = (|\cos\theta|\max s_1 + |\sin\theta|\max s_2) - (|\cos\theta|\min s_1 + |\sin\theta|\min s_2) \\ &= |\cos\theta|(\max s_1 - \min s_1) + |\sin\theta|(\max s_2 - \min s_2) = |\cos\theta| Range(s_1) + |\sin\theta| Range(s_2) \\ &= |\cos\theta| K \times Range(s_2) + |\sin\theta| Range(s_2) = Rang(s_2) \times (|\cos\theta| K + |\sin\theta|) \end{aligned} \tag{36}$$

$$Range(z_1) = |\cos\theta| Range(s_1) + |\sin\theta| / K Range(s_1) = Range(s_1) \times \left(|\cos\theta| + |\sin\theta| / K \right) \tag{37}$$

In a similar way, we write above equations for *Range(z₂)*:

$$Range(z_2) = |\sin\theta| K \times Range(s_2) + |\cos\theta| Range(s_2) = Range(s_2) \times (|\sin\theta| K + |\cos\theta|) \tag{38}$$

$$Range(z_2) = |\sin\theta| Range(s_1) + |\cos\theta| / K Range(s_1) = Range(s_1) \left(|\sin\theta| + |\cos\theta| / K \right) \tag{39}$$

By using (35),(36) and (38) we obtain:

$$\begin{aligned} &K \geq 1 \Rightarrow Range(s_1) > Range(s_2) \Rightarrow \min(Range(s_1), Range(s_2)) = Range(s_2) \\ &Range(z_1) > Range(s_2) \\ &Range(z_2) > Range(s_2) \\ &Range(z_2), Range(z_1) > Range(s_2) = \min(Range(s_1), Range(s_2)) \end{aligned} \tag{40}$$

Also (35), (37) and (39) give us:

$$\begin{aligned} &K < 1 \Rightarrow Range(s_1) < Range(s_2) \Rightarrow \min(Range(s_1), Range(s_2)) = Range(s_1) \\ &Range(z_1) > Range(s_1) \\ &Range(z_2) > Range(s_1) \\ &Range(z_1), Range(z_2) > Range(s_1) = \min(Range(s_1), Range(s_2)) \end{aligned} \tag{41}$$

So we can write for every K:

$$\begin{aligned} &Range(z_1), Range(z_2) > \min(Range(s_1), Range(s_2)) \\ &\min(Range(z_1), Range(z_2)) > \min(Range(s_1), Range(s_2)) \end{aligned} \tag{42}$$

Proof of Proposition 3:

According to (12) and (13) for $\theta_i = -\theta$ we have:

$$\begin{bmatrix} z_1^{-\theta} \\ z_2^{-\theta} \end{bmatrix} = rotate(-\theta) rotate(\theta) \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \tag{43}$$

The Eq. (14) is true for every θ_i so we can substitute it for $-\theta$:

$$\min\left(z_1^{\theta_0}, z_2^{\theta_0}\right) \le \min\left(z_1^{-\theta}, z_2^{-\theta}\right) = \min(s_1, s_2) \tag{44}$$

Also preposition 1 gives us:

$$\min\left(z_1^{\theta_0}, z_2^{\theta_0}\right) \ge \min(s_1, s_2) \tag{45}$$

From (44) and (45) and sandwich theorem we obtain:

$$\min\left(z_1^{\theta_0}, z_2^{\theta_0}\right) = \min(s_1, s_2) \tag{46}$$

Finally according to preposition 1 and (46) we can conclude that $\theta_0 = 0, {}^{\pi}/_{2}, \pi, {}^{3\pi}/2$ or:

$$\begin{cases} z_1^{\theta_0} = \pm s_1 \\ z_2^{\theta_0} = \pm s_2 \end{cases} \quad or \quad \begin{cases} z_1^{\theta_0} = \pm s_2 \\ z_2^{\theta_0} = \pm s_1 \end{cases} \tag{47}$$

References

1. Abate JE (1967) Linear and adaptive delta modulation. Proc IEEE 55:298–308
2. Ambalavanan A, Chandramouli R (2007) Blind source separation for steganalytic secret message estimation. Proc SPIE. p 650507
3. Avcibas I, Memon N, Sankur B (2003) Steganalysis using image quality metrics. Image Process IEEE Trans On 12:221–229
4. Azzabou N, Paragios N, Guichard F (2007) Uniform and textured regions separation in natural images towards MPM adaptive denoising. Scale Space Var Methods Comput Vis 418–429
5. Babaie-Zadeh M, Jutten C, Nayebi K (2002) A geometric approach for separating post non-linear mixtures. Proc XI Eur. Signal Process. Conf. EUSIPCO 2002. pp 11–14.
6. Chandramouli R (2003) A mathematical framework for active steganalysis. Multimed Syst 9:303–311
7. Crouse MS, Nowak RD, Baraniuk RG (1998) Wavelet-based statistical signal processing using hidden Markov models. Signal Process IEEE Trans On 46:886–902
8. Fan F, Jiazhen W, Xiaoqin L, Huijuan F (2007) An Active Steganalysis Method of Block-DCT Image Information Hiding. Electron Meas Instrum. 2007 ICEMI07 8th Int Conf On. pp 2–849

9. Fridrich J, Kodovsk J (2013) Steganalysis of LSB replacement using parity-aware features. Inf Hiding pp 31–45
10. Harmsen JJ, Pearlman WA (2003) Steganalysis of additive-noise modelable information hiding. Proc SPIE pp 131–142
11. Hyvarinen A (1999) Fast and robust fixed-point algorithms for independent component analysis. Neural Netw IEEE Trans On 10:626–634
12. Hyvrinen A, Karhunen J, Oja E (2001) Independent component analysis. John Willey Sons
13. Johnson NF, Jajodia S (1998) Steganalysis of images created using current steganography software. Inf. Hiding. pp 273–289
14. Johnson NF, Jajodia S (1998) Steganalysis: the investigation of hidden information. Inf Technol Conf IEEE pp 113–116
15. Jutten C, Jutten Zadeh M (2006) Source separation: principles, current advances and applications. IAR Annu Meet Nancy Fr 1–10
16. Lyu S, Farid H (2006) Steganalysis using higher-order image statistics. Inf Forensic Secur IEEE Trans On 1: 111–119
17. MATLAB - The language of technical computing - math works. http://www.mathworks.com/products/matlab/. Accessed 10 Dec 2013
18. Nissar A, Mir A (2010) Classification of steganalysis techniques: a study. Digit Signal Process 20:1758–1770
19. Papoulis A, Probability RV (1991) Stochastic processes. McGraw-hill New York
20. Pevny T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. IEEE Trans Inf Forensic Secur 5:215–224. doi:10.1109/TIFS.2010.2045842
21. Portilla J, Strela V, Wainwright MJ, Simoncelli EP (2003) Image denoising using scale mixtures of Gaussians in the wavelet domain. Image Process IEEE Trans On 12:1338–1351
22. Puntonet C, Mansour A, Jutten C (1995) geometrical algorithm for blind separation of sources. Actes XVeme Colloq. GRETSI. pp 273–276.
23. UC Berkeley Computer Vision Group - Contour Detection and Image Segmentation - Resources. http://www.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/resources.html#bsds500. Accessed 31 Mar 2013
24. Vielva L, Erdogmus D, Principe JC (2001) Underdetermined blind source separation using a probabilistic source sparsity model. Proc Int Conf Indep Compon Anal Blind Source Sep ICA. pp 675–679
25. Wenzhe L, Bo X, Zhe Z, Wenxia R (2009) Active steganalysis with only one stego image. Fuzzy Syst Knowl Discov. 2009 FSKD09 Sixth Int Conf On. pp 345–348
26. Xu B, Zhang Z, Wang J, Liu X (2007) Improved BSS based schemes for Active steganalysis. Softw Eng Artif Intell Netw ParallelDistributed Comput 2007 SNPD 2007 Eighth ACIS Int Conf On. pp 815–818
27. Yan Y, Li LT, Xue JB et al (2013) Study on universal steganalysis for BMP images based on multi-domain features. Appl Mech Mater 278:1906–1909
28. Yu X, Tan T, Wang Y (2004) Reliable detection of BPCS-steganography in natural images. Image Graph Proc Third Int Conf On pp 333–336

Hamed Modaghegh was born in Mashhad, Iran. In 2005 he received the B.Sc. in Electrical Engineering from Iran University of Science and Technology and the M.Sc. in Communication from Sharif University of Technology in 2007 and he is Ph.D student in communication in Ferdowsi University of Mashhad now. His current research interests include signal processing and data hiding. Email: hamed.modaghegh@stu-mail.um.ac.ir

Seyed Alireza Seyedin was born in Iran. He received the B.S. degree in Electronics Engineering from Isfehan University of Technology, Isfehan, Iran in 1986, and the M.E. degree in Control and Guidance Engineering from Roorkee University, Roorkee, India in 1992, and the Ph.D. degree from the University of New South Wales, Sydney, Australia in 1996. He has been an Associate Professor with the Department of Electrical Engineering, the University of Mashhad (Ferdowsi), Mashhad, Iran.