The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (pp. 97–106)
http://www.isecure-journal.org

# Eigenvalues-based LSB Steganalysis☆

Farshid Farhat [1,2,*], Abolfazl Diyanat [1,2], Shahrokh Ghaemmaghami [1], and Mohammad Reza Aref [2]

[1] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran*
[2] *Information Systems and Security Lab, Electrical Engineering Department, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

*Article history:*
**Received:** 15 December 2011
**Revised:** 1 September 2012
**Accepted:** 8 December 2012
**Published Online:** 25 May 2013

*Keywords:*
Correlation Matrix, Eigenvalues Analysis, Rate Estimation, Steganalysis, LSB Embedding.

ABSTRACT

So far, various components of image characteristics have been used for steganalysis, including the histogram characteristic function, adjacent colors distribution, and sample pair analysis. However, some certain steganography methods have been proposed that can thwart some analysis approaches through managing the embedding patterns. In this regard, the present paper is intended to introduce a new analytical method for detecting stego images, which is robust against some of the embedding patterns designed specifically to foil steganalysis attempts. The proposed approach is based on the analysis of the eigenvalues of the cover correlation matrix used for the purpose of the study. Image cloud partitioning, vertical correlation function computation, constellation of the correlated data, and eigenvalues examination are the major challenging stages of this analysis method. The proposed method uses the LSB plane of images in spatial domain, extendable to transform domain, to detect low embedding rates-a major concern in the area of the LSB steganography. The simulation results based on deviation detection and rate estimation methods indicated that the proposed approach outperforms some well-known LSB steganalysis methods, specifically at low embedding rates.





## 1 Introduction

LSB (least significant bit) embedding is a steganography method in which informative bits of the message are replaced with the LSBs of the cover signal. Steganalysis consists of a set of operations that finally determine the existence of the secret message in the cover signal. Image steganalysis methods are classified into non-blind, i.e. algorithm specific methods, or blind ones, which are mostly based on statistical analysis approaches. Information about the steganographic materials, such as the embedding algorithm, the cover signal attributes, patterns of the embedding locations, etc. could help the steganalyzer to improve the detection results. Algorithm-specific steganalysis have been devised to be optimal for certain steganography methods; however the other kind of methods attempt to blindly detect the existence of the secret message without any prior knowledge about the steganography method

LSB steganalysis specifically focuses on the steganalysis of the LSB embedding by means of some statistical or machine learning-based methods. There are some prominent reports on the LSB steganalysis found in the literature. As for the present study, the eigenvalues of the correlation matrix, extracted from a given suspected image have been used. This method is believed to be the first approach to the image steganalysis. Which, through eigenanalysis of the

☆ This article is an extended/revised version of an ISCISC'11 paper.

* Corresponding author.
Email addresses: farhat@ee.sharif.edu (F. Farhat), diyanat@ee.sharif.edu (A. Diyanat), ghaemmag@sharif.edu (Sh. Ghaemmaghami), aref@sharif.edu (M. R. Aref).

ISSN: 2008-2045 

correlation matrix, achieves a higher sensitivity to the LSB embedding at very low rates, compared to the conventional LSB steganalysis methods.

In the same vein, a straightforward approach to LSB-steganalysis has been proposed by Dumitrescu *et al.* [1] which analytically estimates the LSB embedding rate of a stego. Their method is based on a special statistical property of certain sets of odd/even pixels. The LSB replacement properly changes this statistical characteristic, and the difference value of the identity can quantify the embedding rate of the secret message. Steganalysis of LSB Encoding in Color Images [2] is a steganographic method to detect LSB embedding in 24-bit color images using the Raw Quick Pairs (RQP) method that analyzes close pairs of colors created by LSB embedding. Yet RQP method works well only when 30% of the number of pixels is greater than the number of image unique colors. In fact, RQP only provides a hard estimate of the embedding rate.

In [3], a new framework has been proposed for steganalysis of the LSB embedding, based on Closure of Sets, which is not dependent on the type and transformation domain of the cover signal. Likewise, a singular value decomposition (SVD) based blind steganalysis method is suggested in [4] which is aimed at detecting spatial domain steganographic methods. The proposed steganalyzer models linear dependencies of neighboring image pixels and content independency determined through a Wiener filtering process. This algorithm, however, fail to operate in some cases because of the (1), given below. In the cases where some parts of the image are dark, using (1), the other symmetric side of the image could be embedded without changing the singular values, since the SVD of the image is not affected by the correlation of the neighboring pixels.

The set of all m-by-n matrices over the complex numbers field is abbreviated to $Mat_n$. The singular-values of the matrix M shown in (1) are those of the matrix $T_{11}$ together with those of the matrix $T_{22}$ and it is not dependent on those of matrix $T_{12}$. For detailed explanation, see [5].

$$M = \begin{bmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{bmatrix} ; \; T_{ii} \in Mat_{n_i} \;\; i = 1, 2 \qquad (1)$$

In a similar vein, Fridrich *et al.* [6, 7] also proposed the Regular and Singular groups as RS method. This technique saves the frequencies of variations of the regular groups and singular groups in the image in order to approximately guess the LSB embedding rate. Such threshold-free detections are ambiguous, as the method is dependent on the type of image and a steganalyzer is necessary to check if a particular estimated embedding rate is positive or zero.

Elsewhere, Harmsen *et al.* [8] used Histogram Characteristic Function (HCF) to discover additive noise steganography in color images, their algorithm failed in the case of grayscale images though. Ker also attempted to extend the detection of the LSB matching; a skilled variant of the LSB embedding that was undetectable by typical LSB steganalysis methods, e.g. [9]. In fact, Ker employed an empirical matrix in order to develop the probability of detection of the HCF technique [8]. The empirical matrix which resembled the adjacency histogram, improved Ker's detection results. Using the combinatorial structure [10], Ker also proposed a general framework for detection and length estimation of hidden messages.

Dumitrescu *et al.* [11, 12] also presented Sample Pair Analysis (SPA) as a technique to detect the LSB steganography. This technique can estimate the embedding ratio accurately when the embedding rate is larger than 3%. Lu *et al.* [13] improved the SPA method for the LSB embedding detection and came up with the one called Least Square Method (LSM) which, in comparison to, SPA and the RS methods, could give a better estimate of the length of hidden message using the cardinality of some pre-defined subsets.

In the same regard, the present paper aims to introduce a new analytical method for steganalysis of the LSB steganography. This steganalysis method relies on the eigenvalues analysis as a powerful mathematical tool that analyzes some correlated parts of the signal to detect the existence of the secret message embedded in the signal through the LSB steganography. The method also gives an estimate of the LSB embedding rate of the stego signal. The simulation results given in Section 5, especially those presented in Figure 6 and Figure 7, provide sufficient evident to confirm this new approach.

In this respect, the remainder of the article is structured as follows. The steganography modeling used in this paper is being explained in Section 2. Next, eigenvalues-based steganalysis stages including partitioning, correlation matrices construction, and eigenvalues analysis will be described in Section 3. A brief analysis of the computational complexity of the method is being offered in Section 4 and the simulation results are subsequently presented in Section 5. Finally, the paper is concluded in Section 6.

## 2 Steganography Modeling

In this section, the steganographic system as a mathematical function is being modeled by means of matrix analysis methods, in which the input is the cover signal and the output is the stego signal.

### 2.1 I/O Domain Definitions

At this stage, it is assumed that the input of the steganographic system is a grayscale image as the cover signal and a binary sequence as an additive message. The cover signal (image) is represented by an m-row n-column ($m \times n$) matrix whose entries (pixels) are integer numbers between 0 and 255, that is to say that the image is considered to be in the spatial domain.

$$Cover\ Signal : C_{m\times n} = [c_{ij}]_{\substack{i=1..m \\ j=1..n}} \quad (2)$$

Additive message is a sequence of bits that are added to some pixels of the cover signal. For simplicity, the message is shown as a vector of length k, as:

$$Message : M_{1\times k} = [m_{ij}]_{\substack{i=1 \\ j=1..k}} \quad (3)$$

The resulting image known as stego signal is also an $m \times n$ matrix whose elements are also integers between 0 and 255.

$$Stego\ Signal : S_{m\times n} = [s_{ij}]_{\substack{i=1..m \\ j=1..n}} \quad (4)$$

For example, sample cover signal, message ($Msg$ = [1 0 1 1 0]), and stego signal could be presented as:

$$C = \begin{bmatrix} 10 & 20 & 1 \\ 30 & 40 & 11 \\ 50 & 60 & 111 \end{bmatrix} \text{ and } S = \begin{bmatrix} 11 & 20 & 0 \\ 31 & 40 & 11 \\ 50 & 60 & 111 \end{bmatrix}$$

### 2.2 Steganography method

In order to have a secure steganography, most methods make use of a shared key between the sender and the receiver. This shared key is usually applied to a pseudorandom number generator (PRNG) as a seed. The output of the PRNG, pseudo-random number sequence (PRNS), determines some random locations of the cover signal that are suitable for steganography of the message bits. Here, it has been assumed that the applied steganography method embeds the informative bits of the message into some least-significant bits (LSBs) of the cover signal accidentally using a PRNG. The PRNG randomly chooses some LSBs of the cover signal to hide the entire message. The relation between the cover and stego signals, the message, and the PRNS (abbreviated as P) could be expressed as:

$$S_{m\times n} = LSB\_Embedding_P(C_{m\times n}, M_{1\times k}) \quad (5)$$

The LSB-Embedding function embeds the message bits in the locations determined by the PRNS. The MATLAB pseudo-code of the LSB-Embedding function is represented in Figure 1.

```
function Stg = LSB_Embedding(Cvr,Msg)
  PermSeq = randperm(Cvr.NumOfPixels);
  for m = 1:Length(Msg)
     if (Msg(m) == 0)
       Cvr(PermSeq(m)) =
         bitset(Cvr(PermSeq(m)),1,0);
     else
       Cvr(PermSeq(m)) =
         bitset(Cvr(PermSeq(m)),1,1);
     end
  end
```

**Figure 1**. The MATLAB pseudo-code of LSB-Embedding function

## 3 Eigenvalues-based Steganalysis

This section serves to describe a new approach to steganalysis of suspected signals which can be shown as a matrix, e.g. an image consisting of $m \times n$ pixels as a data matrix. The proposed steganalysis method, called *Eigenvalues based Steganalysis (EVS)*, uses some mathematical tools in linear algebra and matrix analysis. The present method is mainly inspired by the *Karhunen-Loewe Transform (KLT)* which is a linear transform whose discrete analysis version is known as the principal component analysis [14]. The EVS algorithm works in the spatial domain. In cases of signals given in other time/frequency transform domains, a conversion into the spatial domain is required. All of the operations could be applied to the whole value of an entry of the matrix (e.g. the BYTE value of an image pixel is between 0 and 255) or to the LSB of an entry. The EVS algorithm consists of signal partitioning, correlation matrices construction, and eigenvalues analysis.

### 3.1 Partitioning (A)

The initial stage of the EVS algorithm is the partitioning stage, in which the received signal is segmented into some smaller slices. The partitioning stage reduces the order of complexity of the EVS algorithm, without necessarily having to deviate from ideal steganalysis. In the following subsections,the 1-D and 2-D partitioning procedures are being introduced:

#### 3.1.1 Sequential-Vector Partitioning (A.1)

Sequential-vector partitioning views the whole signal as 1-D sequences of vectors, i.e. it places the columns of the signal matrix sequentially and reads them as FIFO. The MATLAB pseudo-code of the EVS-Seq shown in Figure 2 represents the EVS algorithm with sequential vectors cropping.

#### 3.1.2 Window Partitioning (A.2)

Window partitioning considers the whole signal as 2-D sequences of windows or matrices, i.e. slices the

signal into similar rectangular matrices. The window partitioning makes the signal a puzzle with square slices.

#### 3.1.3 Cloud partitioning (A.3)

In cloud partitioning stage, some parts of the signal are intelligently selected like clouds of anatural image. The cloud selection method could be based on the similarity of , for e.g. four most significant bits (4MSBs) of the signal matrix entries. In an image of nature, for instance, the cloud cropping chooses the sections of the sky, jungle, river, or an object whose 4MSBs are alike. Entropic analysis of the signal could help steganalyzer to locate the clouded data.

### 3.2 Correlation Matrices Construction(B)

In this stage, a zero-mean correlation matrix is constructed for every cropped part of the partitioning stage. The correlation operator could be multiplication, bitwise-XOR, or absolute of subtraction. The function $CorrMat(u, v)$ constructs the correlation matrix of vectors $u$,$v$ by manipulating each entry of the vectors. It could calculate the cross-correlations between each element of cropped matrix of the previous section. Therefore, four types of correlated-data constellations are proposed in this paper, one for vector-structured and three for matrix-structured data.

#### 3.2.1 Correlation Matrix of a Vector (B.1)

Zero-mean cross-correlation matrix ($CM_{v,w} = CorrMat(v, w)$) of sequential vectors $v$,$w$ (resulting from section A.1) is simply derived by multiplying zero-mean vector $v - mean(v)$ and zero-mean transposed vector $(w - mean(w))^T$, as:

$$CorrMat(v, w) = CM_{v,w} \triangleq (v - mean(v)) \times (w - mean(w))^T \quad (6)$$

It is assumed that $CorrMat(v, v) \triangleq CorrMat(v)$.

#### 3.2.2 Horizontal Correlation Matrix of a Matrix (B.2)

The cropped matrix ($CM_{m\times n}$), resulting from section A2 or A3, could be written as:

$$CM_{m\times n} = [cm_{ij}]_{\substack{i=1..m \\ j=1..n}} = \begin{bmatrix} r_1^T \\ r_2^T \\ \vdots \\ r_m^T \end{bmatrix} = [c_1\ c_2\ \cdots\ c_n] \quad (7)$$

where $r_i^T$ is the i-th row vector, and $c_j$ is the j-th column of the matrix $CM_{m\times n}$. Horizontal zero-mean cross-correlation matrix of the cropped matrix ($CM_{m\times n}$) is defined as:

$$CorrMatH(CM) \triangleq [CorrMat(r_i^T, r_j^T)]_{\substack{i=1..m \\ j=1..m}} \quad (8)$$

where the $CorrMatH(CM)$ is an $m^2 \times n^2$ matrix with $n \times n$ entries.

#### 3.2.3 Vertical Correlation Matrix of a Matrix (B.3)

Vertical zero-mean cross-correlation matrix of the cropped matrix ($CM_{m\times n}$) can be defined as follows.

$$CorrMatV(CM) \triangleq [CorrMat(c_i, c_j)]_{\substack{i=1..n \\ j=1..n}} \quad (9)$$

where the $CorrMatV(CM)$ is an $m^2 \times n^2$ matrix with $m * m$ entries. Simulation results are usually based on this function.

#### 3.2.4 Horizontal-to-Vertical Correlation Matrix of a Matrix (B.4)

Horizontal-to-vertical zero-mean cross-correlation matrix of the cropped matrix ($CM_{m\times n}$) is stated as:

$$CorrMatHV(CM) \triangleq [CorrMat(r_i, c_j)]_{\substack{i=1..m \\ j=1..n}} \quad (10)$$

where the *CorrMatH(CM)* is an $m^2 \times n^2$ matrix with $n \times m$ entries.

### 3.3 Eigenvalues Analysis (C)

In this stage, the eigenvalues of the correlation matrices of the previous stage are extracted. To analyze these eigenvalues the following cost functions were used:

(1) Mean
(2) Variance
(3) Maximum
(4) Sum
(5) $L^2$Norm

As shown in Figure 2, for the different percentages of the embedding, from zero to 100, the A, B, and C stages are run to get the reference curve. This reference curve can help the steganalyzer to distinguish the innocent signal from the stego signal. In the simulation section, it is viewed that for different increasing embedding rates of an image, the eigenvalue analyzer gets a new initial point increasingly and reference curve augments almost linearly, where the final point is an almost constant value even for messages with different pseudo-random binary sequences. Hence, higher embedded images have a lower gradient.

```
for EmbdRate = EmbdRates
LSBEmbdCvr=LSB_Embedding(Cvr,Msg);
  for cSeq=1:SequenceLength:NumOfPixels
     Sequence=
     LSBEmbdCvr(cSeq:min(cSeq+
     SequenceLength-1,NumOfPixels));
     MeanOSeq=double(Sequence)-
     mean(Sequence);
     CorrelationMatrix=MeanOSeq'*MeanOSeq;
     Eigenvalues(cSeq:min(cSeq+
     SequenceLength-1,NumOfPixels))=
     eig(CorrelationMatrix);
  end
  EVsMeans(EmbeddingRate+1)=
  mean(Eigenvalues);
  EVsVARs(EmbeddingRate+1)=
  var(Eigenvalues);
end
```

**Figure 2**. The MATLAB pseudo-code of EVS-Seq

### 3.4 Deviation Detection

The steganalysis method proposed here observes the behavior of the reference curve of a suspicious image, through injecting a new random message into the image. It has been revealed that the reference curve of a stego image is supposed to show quite noisier, as compared to an innocent image, because the noise power of the LSB sequence is sometimes the sum of the noise power of the message sequence and injected sequence. However, in some other cases, it is only the noise power of the injected sequence as injected sequence overwrites all of the message sequence in the cover. To parameterize the noise of the reference curve as *Deviation-Ratio* (DR), a cubic spline of the curve is given in (11), where the difference of the spline and the reference curve are normalized.

Some categorized stego images may exceed some DRs, while innocent images of that category remain below of that DR. To detect an embedded signal, one needs to evaluate the DR of the image. If this parameter exceeds the normal threshold of that category, that image will be labeled as stego; otherwise, it is regarded as an innocent one.

$$D.R. = \frac{\sqrt[2]{\sum_{rate=\%0}^{\%100}(EVS_{rate} - Spline(EVS_{rate}))^2}}{|EVS_{\%100} - EVS_{\%0}|} \tag{11}$$

Combining the different methods of the stages A, B, and C could result in a new route to the EVS. The number of the possible routes is thus $1\times1\times5+2\times3\times5=35$. Following regular inspections, the routes which

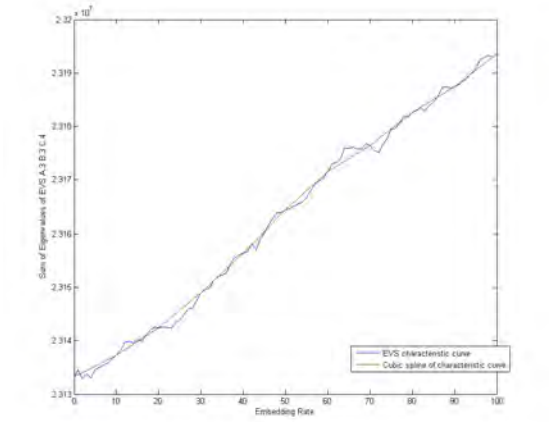



**Figure 3**. Characteristic curve of Lena's image by EVS(A.3 B.3 C.4) given by embedding rate, as compared to its cubic spline

were found to yield the best response were chosen to be executed. Figure 3 shows the real curve of a sample image computed by the EVS algorithm as A.3 (with norms of $16\times16$ clouds) B.3 (Vertical Correlation Matrix) C.4 (sum of eigenvalues) given by the embedding percentage (from 0 to 100), as compared to its cubic spline (smoothed curve). It is noteworthy that the DR may increase, when there is a larger difference between these two curves due to a higher embedding rate. Figure 4 illustrates the surface of Lena's picture

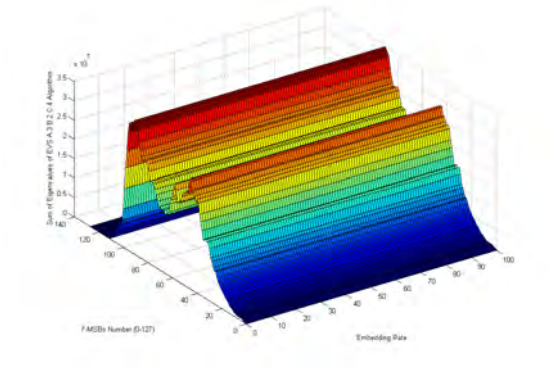



**Figure 4**. Characteristic curve of Lena's image by EVS algorithm as A.3 B.2 C.4 given by embedding percentage and 7-MSBs colors

by the EVS algorithm as A.3 (with norms of $8\times8$ clouds) B.2 C.4 (sum of eigenvalues) given by the embedding percentage (from 0 to 100) and 7-MSBs colors (from 0 to 127). Some 7-MSBs colors are more informative than the others. In general, intermediate colors are more sensitive to the embedding than near black/white colors in natural images, because natural images are more or less greyish rather than exactly white/black and the color distribution is more dense in middle colors. Furthermore, more pixels in a specific color establish a good covert channel for hiding,

and more pixels can help steganalyzer to detect stego. Figure 5 displays the characteristic curves of Lena's image with different initial embedding rates by EVS algorithm as A.3 (with norms of $8 \times 8$ clouds) B.3 C.4 (sum of eigenvalues) given by embedding rate percentage (from 0 to 100). As indicated by the figure, higher initial embedding rate results in a noisier characteristic curve.

### 3.5 Rate Estimation

One of the crucial steps in the LSB steganalysis is believed to be rate estimation of the bits embedded in the image. In this regard, the present section is aimed at introducing an easy efficient method to estimate the amount of bits existing in the cover. Assuming a stego image (I0) as the input of the system, the stego image I0 is resulted from the cover image I.

First, the Characteristic curve of the image (I0) is calculated using the EVS algorithm as A.3 B.3 C.4 given by the embedding percentage. Then, the polynomial approximation of the characteristic curve can be considered as $y = a_{I0}x^n + b_{I0}$ , in which, $n$ is regarded as optional.

Second, the image (I0) bits are right-shifted for one bit, therefore, the 8th bit-plane (LSBs) is replaced by the $7^{th}$ bit-plane. We call this new image I1 and then calculate its Characteristic curve by means of the EVS algorithm, as A.3 B.3 C.4 given by the embedding percentage. Next, the polynomial approximation of the characteristic curve is taken as $y = a_{I1}x^n + b_{I1}$.

Subsequently, similar to the previous stage, the image (I1) bits are right-shifted for one bit so that the $7^{th}$ bit-plane (LSBs) of I0 is replaced by the $6^{th}$ bit-plane of the image. This image is called I2 and again the Characteristic curve is computed using the EVS algorithm, as A.3 B.3 C.4 given by the embedding percentage.

Then, the linear approximation of the characteristic curve is obtained as $y = a_{I2}x^n + b_{I2}$. The main objective, however, is to estimate $y = a_I x^n + b_I$ as the polynomial approximation of the characteristic curve of the cover image I. From the similarity of the polynomials $y = a_I x^n + b_I$, $y = a_{I1}x^n + b_{I1}$, and $y = a_{I2}x^n + b_{I2}$ , it can be concluded that almost $\frac{a_I}{a_{I1}} = \frac{a_{I1}}{a_{I2}}$ . Thus, an approximation to $a_I$ can be achieved.

Moreover, from $y_1 = a_I \times 1 + b_I$, we can get $b_I$ as $y_{1,I0} = y_{1,I}$. a comparison of $y = a_I x^n + b_I$ and $y = a_{I0}x^n + b_{I0}$ yields the estimate rate as $(b_{I0} - b_I)/a_I$. It is worth noting here that, with the help of this method, the stego rate in real-time can be estimated as well. In this regard, the next section is dealing with the complexity of different routes of the EVS method, and subsequently, the related experimental results obtained from some of the best routes will be reported on.

## 4 Computational Complexity Analysis

The EVS method could be run in some different ways. The computational bottleneck of the EVS algorithm is when it calculates the eigenvalues. In order to find the most computationally expensive part of the algorithm, MATLAB's *profiler* was employed. It was revealed that Stage C consumes the most of the CPU clocks. Furthermore, using the LAPACK [14] algorithm to get eigenvalues, the computational complexity has been found to be nearly $O(n^3)$.

It has to be noted that, in case the length of the sequence in Sequential EVS is $l$ for an $m \times n$-pixel image, the order of the complexity of Sequential EVS is almost $O(m \times n/l \times l^3) = O(m \times n \times l^2)$. The same rule applies for the Windowed EVS (EVS_Window), i.e., if the size of the window is $l_1 \times l_2 = l$ for an $m \times n$-pixel image, the order of the complexity of the EVS_Window is nearly $O(m \times n \times l^2)$.

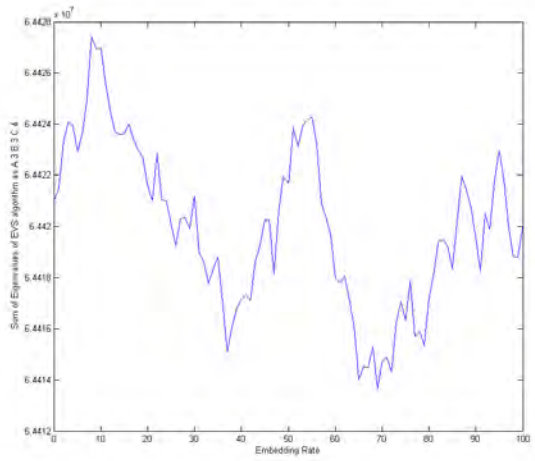
In addition, if stage D of the EVS_Window is run at s-sample rate (usually 100 samples), for an $m \times n$-pixel c-color (usually true-color or $2^{24}$-color) RGB image, the complexity of the algorithm is more accurately $30000 \times m \times n \times l^2$, computed as:

$$s \times \frac{m \times n}{l} \times \sum_{i=1}^{l_1 \times l_2} \{l \times (l-i) \times (\log_2 c + (\log_2 c)^2)\} \tag{12}$$

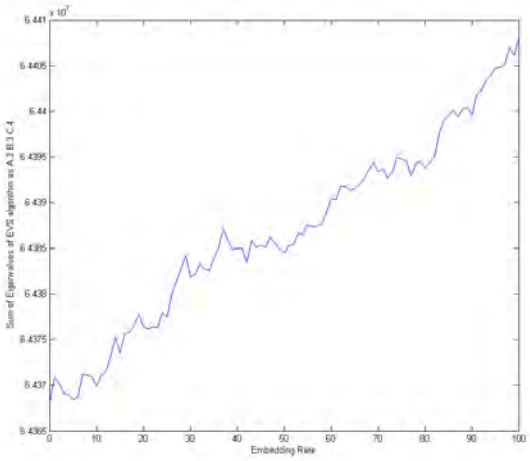
## 5 Experimental Results

As for the purpose of this study, BOSS [15], NRCS [16] and COREL [17] databases of images were used in order to run the simulation on a Pentium IV Quad-Core 2.83GHz PC for five days using MATLAB. During the simulation, 4 thousands images were used for the training stage and about 6 thousands images (3000 clear and 3000 stego images), taken from different databases, were processed in the testing stage.

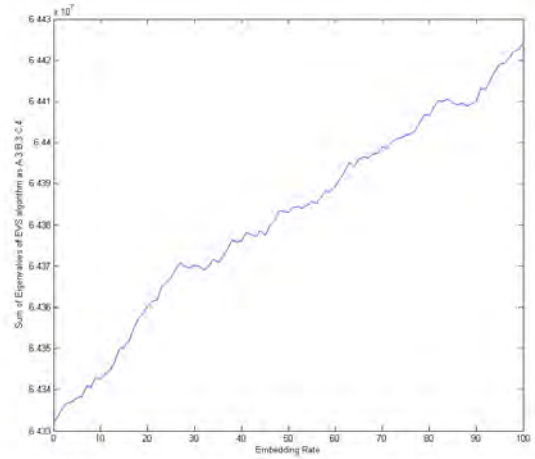
Among all the methods presented in Section 3, the one having the highest performance was selected to detect the stego images. Having a window size of $8 \times 8$ (JPEG-like), the norm-based (C.4) vertical (B.2) windowed (A.2) EVS algorithm (EVS_Window_V) was found to be the best among the others to arrive at the desired results in a reasonable time of about one hour. As expected, increasing the window size could yield better results according to 12.



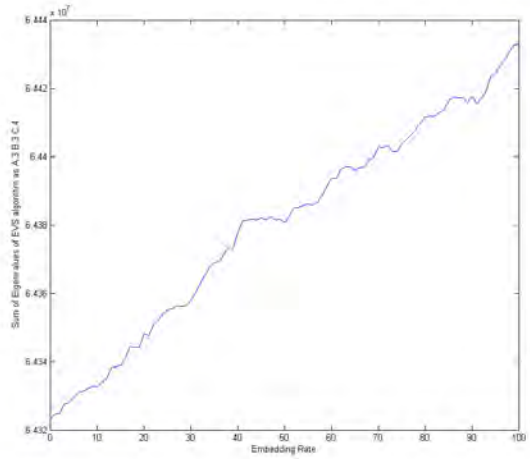

(a) Initial embedding percentage = %100



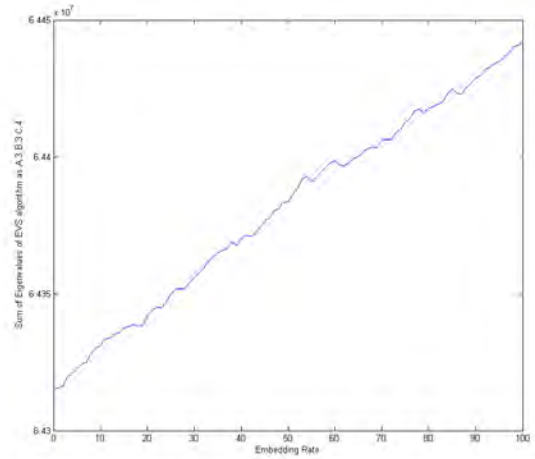

(b) Initial embedding percentage = %50



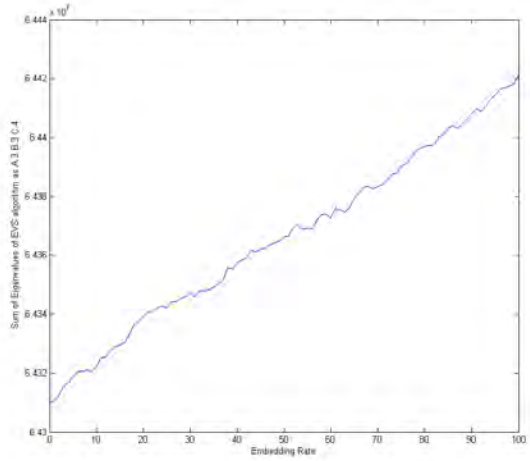

(c) Initial embedding percentage = %25




(d) Initial embedding percentage = %20




(e) Initial embedding percentage = %15




(f) Initial embedding percentage = %10

**Figure 5**. The characteristic curves of Lena's image with different initial embedding rates by EVS algorithm as A.3 B.3 C.4 given by embedding rate percentage

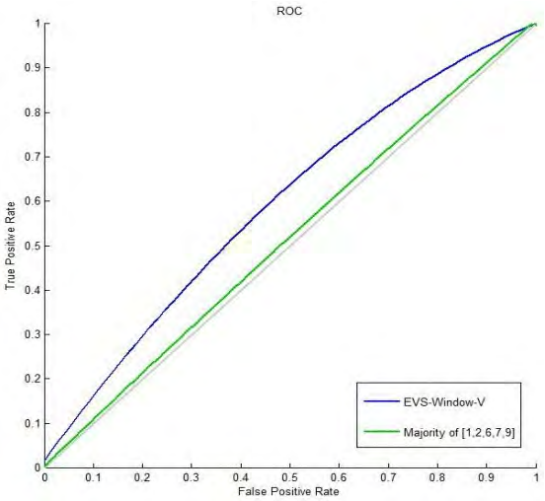



**Figure 6**. Characteristic curve of Lena's image by EVS(A.3 B.3 C.4) given by embedding rate, as compared to its cubic spline

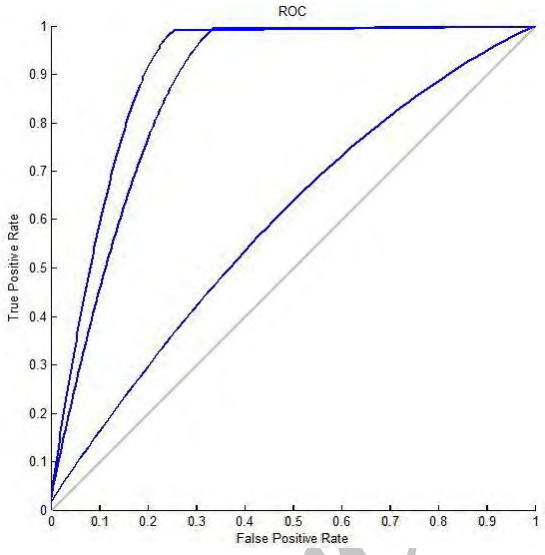



**Figure 7**. Characteristic curve of Lena's image by EVS(A.3 B.3 C.4) given by embedding rate, as compared to its cubic spline

The image database is classified into different categories according to a measure of their noise. The noise levels of the images are estimated by the DWT (Discrete Wavelet Transform) HH partial coefficients of a robust median estimator [18] called RiskShrink. The images are transformed into wavelet domain using symmetric Daubechies' transformation of the length 8. Then, the HH coefficients are selected from the wavelet coefficients and the noise variance of the images is computed as:

$$\hat{\sigma} = \frac{Median(|Y_i|)}{0.6745} \qquad (13)$$

In the next stage, based on 13, a number of features are selected to classify the database. The first feature is the Noise estimation (NE) of the image based on 13. To compute the second feature in the analysis, we set the LSB levels of the images to zero, making *imageSet0* files. The noise estimation of the seventh bit-level of the imageSet0 files is then chosen as the second feature. This is based on the fact that, in the LSB steganography, only the LSB levels are changed and the other bit-levels of the image are kept the same as those in the innocent image.

Deviation Ratio (DR) parameter, image dimensions, noise estimation of LSB, $7^{th}$ level, and the whole image are taken as a 5-feature set of a support vector machine (SVM) with 5-degree polynomial core with 5000 iterations of quadratic programming for convergence. About four thousands pictures taken from BOSS, NRCS and COREL database are added to train the machine.

In the first experiment, all of the data was given to the SVM for learning. Given the second one, the innocent images and the stego images with embedding rates greater than 5% were given to the SVM. Table I shows the EVS results as compared to the best performance achieved by some well-known methods introduced earlier for steganalysis of the LSB steganography [1, 2, 6–8]. Besides, the receiver operating characteristic (ROC) curves were also computed for the EVS_Window_V and the other methods for 5% embedding rate, as depicted in Figure 6.

As observed from Table 1 and Figure 6, the EVS_Window_V algorithm achieves a quite better detection performance when compared to the best performance of the other schemes. Figure 7 illustrates the ROC curve of the EVS_Window_V for 15% (the inner), 10% (the middle), and 5% (the outer) embedding rates.

**Table 1**. Detection rates for comparison between the EVS and the best of some other algorithms

| Algorithm \ Emb. Rates | 0 | 5 | 10 | 15 | 20 | 25 |
|---|---|---|---|---|---|---|
| EVS_Window_V | 94.5 | 64.8 | 80.6 | 95.1 | 99 | 99.5 |
| Best outputs of [1, 2, 6–8] | 89.1 | 51.7 | 66 | 78.3 | 85.9 | 90.1 |

In addition, the proposed method has been tested on other LSB-based methods like LSB Matching [19] and LSB+ [20]. The LSB+ method is detected more easily compared to the others, as it embeds even more bits to compensate some other steganalysis methods. The intuition, observations, and results are almost the same, mostly due to the fact that the EVS method is basically dependent on the statistical distribution of LSBs. The detection results obtained from both the

conventional LSB replacement and LSB Matching-like algorithms such as HUGO [21] are nearly the same.

Finally, comparisons were made between some of the new steganalysis methods participated in the recent competition called BOSS [22] and the EVS algorithm. To this end, the EVS was trained by BOSSBase database and tested with BOSSRank database taken by Leica M9 camera [15] as it was randomly embedded by the well-known algorithm HUGO [21].

Table 2 facilitates the comparison between the EVS algorithm and the other ones mentioned in [22] for a half subset of BOSSRank. The results indicate that, in some image subsets, the algorithms proposed here could outperform new approaches, though those non-universal methods are found to achieve a slightly higher detection accuracy due to their adaptation to that specific algorithm, HUGO.

**Table 2**. Detection rates for comparison between the EVS and Boss competition algorithms

| Algorithm | EVS (our algorithm) | Hugobreakers [15, 22] | Gul & Kurugollu [15, 22] | Andreas Westfeld [15, 22] |
|---|---|---|---|---|
| Classifier Score | 65%-75% | 68%-82% | 73%-77% | 67% |

## 6 Conclusion

The present paper was aimed at introducing a new eigenvalues based steganalysis method, called EVS algorithm. To this end, the sum of the eigenvalues of the correlation matrix extracted from the suspected image were used for steganalysis. The phases of the proposed algorithm, including image partitioning, correlation computation, and the detection analysis were also investigated and explained.

It has to be noted that the stages of the EVS algorithm have different implementations that make the complete EVS algorithm marvelous for different applications. The better route over stages the better the steganalyzer will work. The EVS is designed in a way that is feasible in terms of complexity. Besides, the performance of the EVS is comparable with similar LSB steganalysis methods. It is also worth mentioning that the LSB embedding rate of the stego could be estimated by using EVS when the thresholds of different categories of images are used by RiskShrink estimator.

A comparison between the simulation results obtained from the application of the EVS versus those of the conventional steganalysis methods provides sufficient evidence as for the superiority of the EVS algorithm for the LSB image steganalysis, particularly in challenging cases of low embedding rates. Moreover, comparisons were drawn between the results of EVS algorithm on BOSS database and those achieved from some new methods participated in BOSS competition.

## References


[1] S. Dumitrescu, X. Wu, and N. Memon. On steganalysis of random lsb embedding in continuous-tone images. In *Proceedings IEEE International Conference on Image Processing, ICIP 2002*, pages 324–339, Rochester, NY, September 22–25, 2002.

[2] J. Fridrich, R. Du and L. Meng. Steganalysis of lsb encoding in color images. In *Proceedings IEEE International Conference on Multimedia and Expo*, July 30–August 2, New Yourk, NY, 2000.

[3] S.R. Khosravi-rad, T. Eghlidos, and S. Ghaemmaghami. Higher-order statistical steganalysis of random lsb steganography. In *IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, pages 629–632, May 2009.

[4] G. Gul and F. Kurugollu. Svd-based universal spatial domain image steganalysis. *IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 2, JUNE 2010.

[5] R.A. Horn and C.R. Johnson. *Matrix analysis*. Cambridge university press, 1990.

[6] J. Fridrich and M. Goljan. Practical steganalysis of digital images-state of the art. In *Proceedings of SPIE*, volume 4675, pages 1–13, 2002.

[7] J. Fridrich and M. Goljan. Reliable detection of lsb steganography in color and grayscale images. *Proceedings ACM Workshop on Multimedia and Security*, pages 27–30, 2001.

[8] J. Fridrich, M. Goljan, and D. Soukal. Higher-order statistical steganalysis of palette images. In *Electronic Imaging 2003*, pages 178–190. International Society for Optics and Photonics, 2003.

[9] A.D. Ker. Steganalysis of lsb matching in grayscale images. *IEEE Signal Processing Letters*, 12(6):441–444, 2005.

[10] A. Ker. A general framework for structural steganalysis of lsb replacement. In *Proceedings of the 7th Information Hiding Workshop*, volume 3727, pages 296–311. Springer, 2005.

[11] S. Dumitrescu, X. Wu, and Z. Wang. Detection of lsb steganography via sample pair analysis. In *IEEE Transactions on Signal Processing, vol. 51, no. 7*, pages 1995–2007, 2003.

[12] S. Dumitrescu and X. Wu. Steganalysis of lsb embedding in multimedia signals. In *IEEE International Conference on Multimedia and Expo, 2002.*

*ICME02.*, volume 1, pages 581–584, August 2002.
[13] P. Lu, X. Luo, Q. Tang, and L. Shen. An improved sample pairs method for detection of lsb embedding. In *Proceedings of the 6th Information Hiding Workshop, Springer LNCS 3200*, pages 116–127, 2004.
[14] L.I. Smith. A tutorial on principal components analysis. *Cornell University, USA*, 2002.
[15] Boss website. http://www.agents.cz/boss/BOSSFinal/.
[16] Nrcs website. http://photogallery.nrcs.usda.gov/.
[17] Nrcs website. http://wang.ist.psu.edu/docs/ related/.
[18] D.L. Donoho and I.M. Johnstone. Adapting to unknown smoothness via wavelet shrinkage. *Journal of the american statistical association*, 90(432): 1200–1224, 1995.
[19] J. Mielikainen. Lsb matching revisited. *IEEE Signal Processing Letter*, 13(5):285–287, May 2006.
[20] H. Wu, J.L. Dugelay, and Y. Cheung. A data mapping method for steganography and its application to images. In *Lecture notes in computer science.Proceedings of the 10th information hiding workshop*, pages 236–250. Berlin:Springer, 2008.
[21] T. Pevnỳ, T. Filler, and P. Bas. Using high-dimensional image models to perform highly undetectable steganography. In *Information Hiding, 12th International Workshop, Lecture Notes in Computer Science, Calgary, Canada*, pages 161–177. Springer, 2010.
[22] Patrick Bas, Tomáš Filler, and Tomáš Pevnỳ. Break our steganographic system: The ins and outs of organizing boss. In *Information Hiding*, pages 59–70. Springer, 2011.

**Farshid Farhat** was born in Tehran in 1983. He received his B.S. in 2005 and M.S. in 2007 from Sharif University of Technology in Electrical Engineering. He is a Ph.D. candidate at Sharif University of Technology. His research interests include data network communications, cellular communications security, and game-theoretic approach in networking. He has currently focused on signal processing and information forensics.

**Abolfazl Diyanat** received his B.S. degree in Electrical and Computer Engineering from University of Tehran, Iran, in 2009. He was an M.S. student at Sharif University of technology, Tehran, Iran. He is now a Ph.D. candidate in Electrical and Computer Engineering at University of Tehran. His main research interests include steganalysis, multimedia, telecommunication systems, distributed optimization, and analytical modeling of wireless ad hoc networks.

**Shahrokh Ghaemmaghami** (M'95) received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, and the Ph.D. degree from the Queensland University of Technology, Brisbane, Australia. He is an Associate Professor of signal processing, a Member of the Communications and System Engineering Group of the Electrical Engineering Department, and Director of the Electronics Research Institute, Sharif University of Technology, Tehran, Iran. He has been leading many large research projects and teaching courses in signal processing, including speech, audio, image, and video processing, and also in information hiding, e.g., watermarking, steganography and steganalysis. Dr. Ghaemmaghami is a member of the Association for Computing Machinery. He has served as a member of technical committees and advisory boards of several international conferences and journals.

**Mohammad Reza Aref** was born in city of Yazd in Iran in 1951. He received his B.S. in 1975 from University of Tehran, his M.S. and Ph.D. in 1976 and 1980, respectively, from Stanford University, all in Electrical Engineering. He returned to Iran in 1980 and was actively engaged in academic and political affairs. He was a faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of Electrical Engineering at Sharif University of Technology since 1995 and has published more than 260 technical research papers in communication and information theory and cryptography in international journals and conference proceedings. His current research interests include areas of communication theory, information theory, and cryptography with special emphasis on network information theory and security for multiuser wireless communications. During his academic activities, he has been involved concomitantly in political positions. First Vice President of I. R. Iran, Vice President of I. R. Iran and Head of Management and Planning Organization, Minister of ICT of I. R. Iran, and Chancellor of University of Tehran, are the most recent ones.

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 167)
http://www.isecure-journal.org

# Persian Abstract

## تحلیل سیستم‌های پنهان‌سازی با استفاده از مقادیر ویژه

**فرشید فرحت[۱،۲]، ابوالفضل دیانت[۱،۲]، شاهرخ قائم‌مقامی[۱]، و محمدرضا عارف[۲]**

[۱] پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

[۲] آزمایشگاه تئوری اطلاعات و مخابرات امن، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

روش‌های نهان‌کاوی عکس‌ها کلاً می‌توانند به دو صورت باشند. روش‌های نهان‌کاوی بینا که به منظور تحلیل الگوریتم پنهان‌سازی خاصی بکار می‌روند و یا روش‌های نهان‌کاوی کور که بیشتر بر مبنای روش‌های آماری، دسته‌ای از الگوریتم‌های پنهان‌سازی را تحلیل می‌کنند. روش‌های کور از این جهت که قابلیت آشکارسازی تغییرات اعمال شده به مشخصات آماری سیگنال پوشش را دارند، بیشتر مورد پسند هستند. به هر صورت اطلاعاتی درباره مواد مورد نیاز سیستم پنهان‌ساز مانند نوع الگوریتم پنهان‌سازی، خصوصیات سیگنال پوشش، الگوی مکان‌های جاسازی و غیره، می‌تواند تحلیلگر را برای بدست آوردن نتایج تشخیص بهتر کمک کند. بسیاری از مؤلفه‌های خصوصیات عکس‌ها مانند تابع مشخصه هیستوگرام، توزیع رنگ‌های مجاور و تحلیل جفت نمونه برای نهان‌کاوی مورد استفاده قرار گرفته است، اگرچه روش‌های نهان‌سازی معینی پیشنهاد شده است که قادر است این‌گونه تحلیل‌ها را با مدیریت جاسازی خنثی کند.

در این مقاله روش جدید تحلیلی برای تشخیص عکس نهان‌نگاری شده مطرح می‌شود که در مقابل بسیاری از الگوهای جاسازی مختلف که در صدد فریب تحلیلگران هستند، مقاوم است. روش اخیر بر مبنای تحلیل مقادیر ویژه ماتریس همبستگی پوشش است و برای اولین بار مورد استفاده قرارگرفته است. تجزیه عکس، محاسبه تابع همبستگی، چیدمان داده‌های همبسته و آزمایش مقادیر ویژه، از موضوعات چالش برانگیز روش تحلیلی اخیر محسوب می‌شود. روش پیشنهادی از سطح کم ارزش‌ترین بیت عکس در دامنه فضایی برای تشخیص نرخ‌های پنهان‌سازی کم که نگرانی اصلی حوزه‌ی پنهان‌سازی در کم ارزش‌ترین بیت است، بهره می‌برد و قابل گسترش به حوزه‌های تبدیل دیگر نیز می‌باشد. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی جدید در نرخ‌های کم از برخی روش‌های مشهور دیگر در این حوزه بهتر عمل می‌کند.

**واژه‌های کلیدی:** ماتریس همبستگی، تحلیل مقادیر ویژه، تخمین نرخ، نهان‌کاوی اطلاعات، جاسازی در کم‌ارزش‌ترین بیت.