Multi-Dimensional Correlation Steganalysis

Farshid Farhat[1,2], Abolfazl Diyanat[1,2], Shahrokh Ghaemmaghami[1], Mohammad-Reza Aref[2]
[1]Electronics Research Institute
[2]Information Systems and Security Lab, Electrical Engineering Department
Sharif University of Technology, Iran
{farhat, diyanat}@ee.sharif.edu, {ghaemmag, aref}@sharif.edu

Abstract—**Multi-dimensional spatial analysis of image pixels have not been much investigated for the steganalysis of the LSB Steganographic methods. Pixel distribution based steganalysis methods could be thwarted by intelligently compensating statistical characteristics of image pixels, as reported in several papers. Simple LSB replacement methods have been improved by introducing smarter LSB embedding approaches, e.g. LSB matching and LSB+ methods, but they are basically the same in the sense of the LSB alteration. A new analytical method to detect LSB stego images is proposed in this paper. Our approach is based on the relative locations of image pixels that are essentially changed in an LSB embedding system. Furthermore, we introduce some new statistical features including "local entropies sum" and "clouds min sum" to achieve a higher performance. Simulation results show that our proposed approach outperforms some well-known LSB steganalysis methods, in terms of detection accuracy and the embedding rate estimation.**

Keywords: LSB Embedding Steganalysis, Multidimensional Correlation, Local Entropies Sum, Clouds Min Sum, Embedding Rate Estimation.

I. INTRODUCTION

Steganography conceals the presence of communication. Steganography methods, in which informative bits of the message are embedded into the least significant bits (LSBs) of the cover signal, are known as LSB embedding. Steganalysis typically consists of a set of processes that may eventually detect the existence of the secret message embedded in the cover signal. Many papers on the LSB steganalysis can be found in the literature, while a small fraction of them suggest a theoretical approach to the problem. Some of steganalysis methods are algorithm-specific that means the attacker is aware of the steganography method employed to generate the stego signal. Some other steganalysis methods, however, blindly detect the existence of the secret message without any prior knowledge about steganography method.

LSB encoding steganalysis of color images [2] is a method, developed by Fridrich et al., to detect the LSB embedding in 24-bit color images by using the *raw quick pairs (RQP)* algorithm that analyzes close pairs of colors created by the embedding process. In cases 30% of the number of pixels is greater than the number of image unique colors, the RQP method works quite well. The RQP just yields a hard (not soft) estimate of the embedding rate. Estimation of secret message length in the LSB steganography by using *weighted stego (WS)* method [1] has also been investigated that is an effective method based on an optimization procedure. Fridrich et al. [7,10] also proposed the Regular and Singular groups as RS method. This technique saves the frequencies of the variations of regular groups and singular groups in the image to get an estimate of the LSB embedding rate.

Dumitrescu et al. [3] proposed a more straightforward approach to the LSB steganalysis that theoretically estimates the LSB embedding rate of a given stego image. This method is based on an especial statistical property of the sets of odd/even pixels. The LSB replacement changes this statistical characteristic and, accordingly, the difference value of the identity can quantify the message embedding rate. A new framework for steganalysis of the LSB embedding based on Closure of Sets [4] has been proposed which does not depend on the type of the cover signal or the embedding domain.

Dumitrescu et al. [11,12] proposed *sample pair analysis (SPA)* as a technique to detect the LSB steganography. It can estimate the embedding ratio accurately, when the embedding rate is greater than 3%. Lu et al. [14] improved the SPA method for LSB embedding detection called l*east square method (LSM)* that estimates the length of hidden message more accurately, as compared to the SPA and the RS methods, using the cardinality of some pre-defined subsets. A SVD (singular value decomposition) [6] based Steganalysis method is suggested in [5]. This method could fail in cases that some parts of the image are dark; the message could be embedded in the other symmetric side of the image without changing the singular values. This is because the SVD of the image does not represent the correlation of the neighboring pixels.

Harmsen et al. [8] used histogram characteristic function (HCF) to develop an additive noise model based steganalysis of the LSB embedding in color images, but their algorithm almost failed in the case of grayscale images. Ker [9] extended the detection of LSB matching; a skilled variant of the LSB alteration that was undetectable by standard LSB steganalysis methods. An empirical matrix was used by Ker to boost the detection probability of the HCF technique [8]. The empirical matrix equal with the adjacency histogram improved the Ker's detection results. Also Ker proposed a general framework for detection and length estimation of hidden messages [13] using the combinatorial structure.

In this paper, we introduce a new analytical method for the LSB steganalysis. Our steganalysis method uses the multi-dimensional correlation between pixels of an image that analyzes correlative parts of the signal to detect the existence of the secret message hidden in the signal through the LSB embedding. This method also gives an estimate of the embedding rate. The simulation data confirm superiority of the new approach, as compared to a number of well-known steganalysis methods.

978-1-4577-1434-4/11/$26.00 ©2011 IEEE

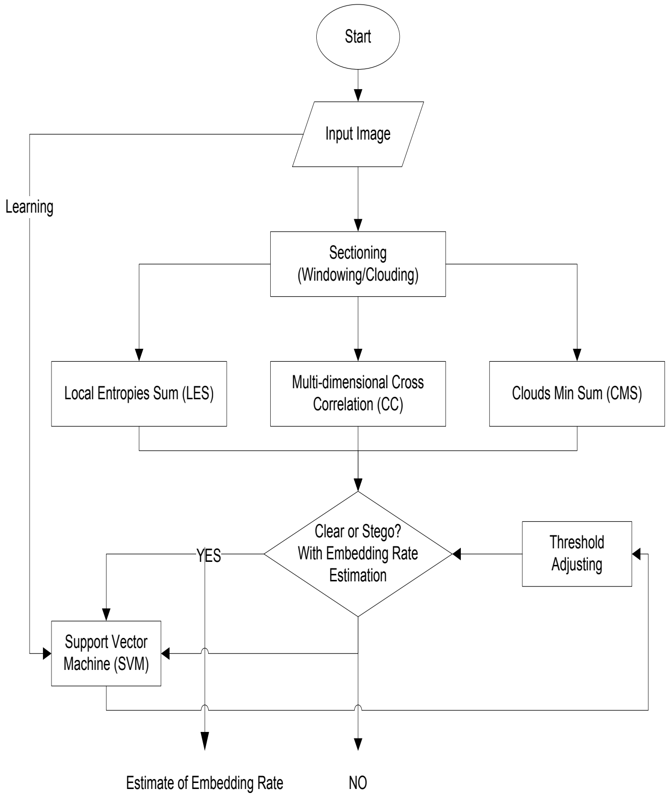


Figure 1. Flowchart of the proposed steganalysis algorithm.

The rest of the paper is structured as follows. In section II steganography model is developed and explained. Multi-dimensional correlation steganalysis including sectioning, cross correlation, feature extraction and analysis are described in section III. Computational complexity analysis is presented in section IV and simulation results are shown and discussed in section V. The conclusions are drawn in section VI.

II. LSB Steganography Modeling

The steganographic system modeling, as a mathematical function, is addressed in this section. The modeling is explained by means of matrix analysis, where the system is simply assumed to take a cover signal and a secret message as its inputs and generate the stego signal at its output.

A. I/O Domain Definitions

It is assumed here that the inputs of the steganographic system are a grayscale image and a binary message. The cover signal (grayscale image) is typified by an m-row, n-column (m*n) matrix whose elements (pixels) are integer numbers between 0 and 255 for an 8-bit digital image. Such a cover image is shown in the spatial domain, as:

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

The secret message is a sequence of bits that are embedded into some pixels of the cover image. The message is shown as a vector of length k:

$$Message: M_{1*k} = \left[m_{ij}\right]_{\substack{i=1\\ j=1..k}} = [m_{1j}]_{j=1..k} \qquad (2)$$

The output image, the stego signal, is also an m-row, n-column (m*n) matrix whose entries are integer numbers between 0 and 255:

$$Stego\ Signal: S_{m*n} = [s_{ij}]_{\substack{i=1..m\\ j=1..n}} \qquad (3)$$

B. Steganography method

Secure steganography methods use a shared key between transmitter and receiver. This secret key ordinarily addresses a *pseudo-random number generator (PRNG)* as seed. The output of the PRNG locates candidate pixels of the cover signal to embed the covert message bits. Specifically, a typical LSB steganography method randomly changes some LSBs of the cover image, based on a pseudo-randomized version of the secret message using a PRNG. To hide the secret message in the cover signal, PRNG selects some LSBs of cover signal, subject to the embedding capacity and the embedding strategy. The mathematical relation between stego, cover, message and PRNG could be defined as:

$$S_{m*n} = LSB\_Embedding_{PRNG}(C_{m*n}, M_{1*k}) \qquad (4)$$

III. Multi-Dimensional Correlattion Steganalysis

The proposed approach to the LSB steganalysis is described in this section. Suspicious signal, supposed to be an image consisting of m*n pixels, can be viewed as a data matrix. Our new steganalysis algorithm, *Multi-Dimensional Correlated Steganalysis (MDCS),* uses some basic mathematical operators in algebra. The MDCS depends on the relative multi-dimensional locations of image pixels.

The proposed MDCS algorithm is run in spatial domain of 2-d images, hence a stego image, whether or not processed in other time/frequency domains, has to be transformed into the spatial domain prior to the analysis. The MDCS method consists of image sectioning, multi-dimensional cross correlation computation, and feature extraction/analysis. Furthermore, some new statistical features including local entropies sum and clouds min sum are added to achieve a higher performance. Fig.1 shows the proposed algorithm schematically.

A. Sectioning

The inception of the MDCS algorithm is the sectioning stage. At the sectioning stage, the cover image is split into a number of slices. The sectioning stage makes it possible to reduce the order of computational complexity of the MDCS algorithm. As stated in the following section, larger slices result in a higher order of the complexity of MDCS. The sectioning stage does not necessarily overshadow the desired steganalysis performance, but obviously decreases the order of complexity and intelligent analysis of separated sections can help further. In this paper two major types of sectioning are proposed: *Windowing* and *Clouding*.

1) Windowing

The windowing procedure splits the whole cover image into two-dimensional sequences of non-overlapping windows or 2-d blocks, i.e. slices the image into rectangular matrices of the same size.

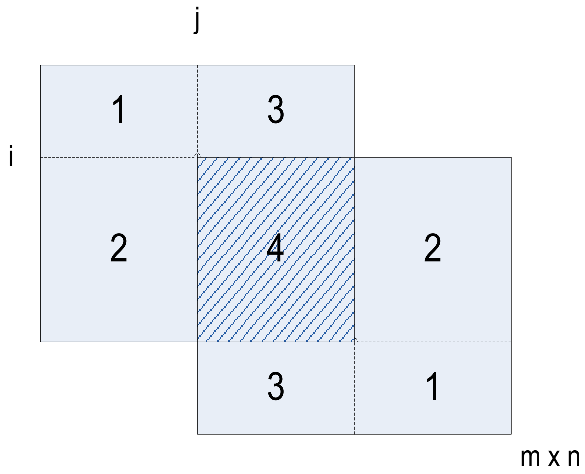


Figure 2. Relative two-dimensional autocorrelation of cover C.

2) Clouding

Clouding adaptively chooses some parts of the signal, something like clouds of an image of the sky. The Cloud selection method could be based on the similarity of the x-most significant bits (x-MSBs) of cover matrix entries. Clouding of a nature picture selects the sections of sky, river, jungle, or an object whose x-MSBs are alike. Entropic analysis of an image could help the steganalyzer to acquire desired clouded data. It is to be noted that Clouds are typically not rectangular in our algorithm but the next step is to build a rectangular matrix to analyze. So, Clouds should be padded by a sufficient number of zero (neutral) pixels to be casted in a rectangular matrix. Clouding could be taken as an intelligent windowing procedure, because almost the same color parts of an image are selected and processed separately. Given by x-MSBs clouding, pixels of cover image are chosen such that x-MSBs of the selected color are the same.

If we have 2^x Cloud types given by x-MSBs, there are 2^{8-x} Rain types given by y-least significant bits (y-LSBs) where y=8-x. Rain types refer to the types of an exact x-MSBs color given by y-LSBs where y<=8-x. To implement the Cloud sectioning, the same x-MSBs pixels are divided into 2^x classes. The analysis process is class oriented, i.e., pixels of the same class are processed together, where applying the analysis procedure to pixels of different classes results in zero.

If the conventional LSB embedding is used, y-LSBs must be set to 1-LSB (y=1). With the LSB Matching, we can set x-LSBs to 2-LSBs or 1-LSB, because just the number of altered LSBs involved in the embedding is of our concern. Also the inequality of x+y<=8 must always be satisfied. To speed up the feature extraction algorithm in our implementation, clouding and the next step to clouding are combined in the main loop of the generated code of the algorithm

B. Multi-Dimensional Cross-Correlation

Following the sectioning stage, the sequence of blocks/clouds of the given image undergoes a multi-dimensional cross-correlation process. For 2-d images, all terms are described for two-dimensional blocks/clouds, which are later generalized to multi-dimensional analysis by making a little effort. Multi-dimensional cross-correlation of two hyper-blocks/clouds is defined below.

Definition-1 (Relative Cross-Correlation): Assume that C_1 and C_2 are two 2-d block-wise/cloud-wise m*n covers, as given in (1). 2-d relative cross-correlation (CC) of C_1 and C_2 with 2-d shift $(i,j) \in [-m+1,m] \times [-n+1,n]$ is defined as:

$$CC_{C1,C2}(i,j) \triangleq \sum_{(k,l)=(1,1)}^{(m,n)} C_1(k,l) \oplus C_2((k+i)\ mod\ m, (\ l+j)\ mod\ n) \tag{5}$$

where $\oplus$ stands for XOR operation.

Defnition-2 (Relative Autocorrelation): If C_2 in Definition-1 is the same as C_1=C, relative autocorrelation of C with 2-d shift $(i,j) \in [-m+1,m] \times [-n+1,n]$ is defined as:

$$CC_C(i,j) \triangleq CC_{C,C}(i,j) = \sum_{(k,l)=(1,1)}^{(m,n)} C(k,l) \oplus C((k+i)\ mod\ m, (\ l+j)\ mod\ n) \tag{6}$$

As defined in (6), the same regions, depicted in fig.2, are bitwise xor-ed, and then summed up together. Similar to 2-d DFT (Discrete Fourier Transform), the 2-d interval of cross-correlation (autocorrelation) must be: $[-m+1,m] \times [-n+1,n]$, as the range of (i,j). Consequently, the area of cross-correlation is 2*2=4 times of the areas of the images. The 3-d view of relative autocorrelation of a sample *Cloud*-ed cover, subject to (i,j) plane, is like a mountain remembering the 3-d Gaussian distribution.

Lemma 1: Assume that image I is a 2-d m*n image given by (1) and CC_I is the autocorrelation function as stated in Definition-2. So, we have:

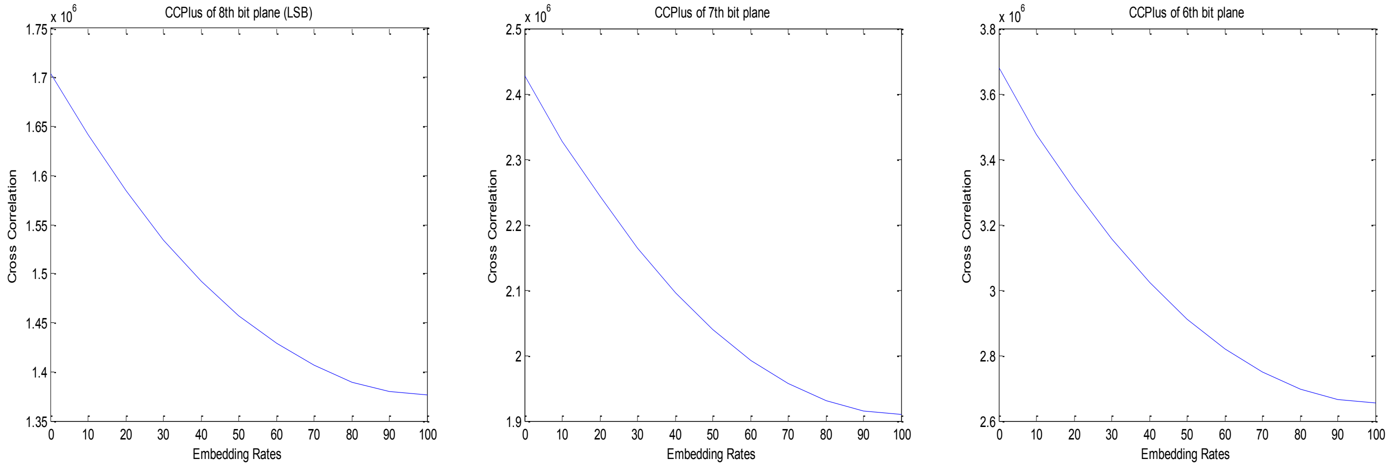
$$CC_I(i,j) = CC_I(-i,-j) = CC_I(i-m,j) = CC_I(i,j-n) = CC_I(i-m,j-n) = CC_I(m-i,n-j) \tag{7}$$

It can easily be shown that the above property is trivial. By checking all of intersection positions of the two images, it can be derived that (7) meets our needed characteristics.

Lemma 2: If f is an incremental or decremental function, $f(feature)$ cannot learn a Support Vector Machine (SVM) more than the $feature$ lonely.

By applying any incremental or decremental function to the data, the n-tuple threshold as a distinguisher is not changed, because the order of the data with respect to their magnitude remains unchanged. So we can only take into account the real original information about the image and ignore redundant data to improve the performance of the analyzer. In the next lemma you can see the only needed region for MDCS is the ¼ region of the whole-size image.

Corollary1: Due to Lemma-1 and Lemma-2, to calculate 2-d cross-correlation feature of an image, it is only sufficient to calculate 2-d cross-correlation of 2-d interval $\left[1,\frac{m}{2}\right] \times \left[1,\frac{n}{2}\right]$.



(a) (b) (c)

Figure 3. CCPlus features of 6th, 7th, and 8th bit plane of a typical image from COREL database.

Lemma 3: Assume that PRNSeq$_1$ and PRNSeq$_2$ are two binary pseudorandom number sequences, so we have:

$$\forall(i,j)\epsilon[1,m]\times[1,n]: CC_{PRNSeq1,PRNSeq2}(i,j)\approx\frac{m*n}{2} \tag{8}$$

Also for a PRNSeq alone, we have:

$$\forall(i,j)\epsilon[1,m]\times[1,n];(i,j)\neq(0,0)$$
$$CC_{PRNSeq}(i,j)\approx\frac{m*n}{2} \tag{9}$$

Lemma 4: Assume that C is a 2-d cloud-wise correlated cover, i.e.

$$\forall(i,j)\in Cloud_k; k\in[1,N]$$
$$CC_C(i,j)\approx CC_C(i+1,j)\approx CC_C(i,j+1)\gtrsim N \tag{10}$$

If $S=LSB\_Embedding_{PRNG}(\mathrm{C},\mathrm{M})$ as C, M, and S specified in equations (1), (2), and (3), statistically:

$$CC_C(i,j)\gtrsim CC_S(i,j) \tag{11}$$

Corollary2: For a 2-d cloud-wise correlated cover, it could be deduced that if $S=LSB\_Embedding_{PRNG}(\mathrm{C},\mathrm{M})$, statistically:

$$\sum_{(i,j)=(1,1)}^{(\frac{m}{2},\frac{n}{2})} CC_C(i,j)>\sum_{(i,j)=(1,1)}^{(\frac{m}{2},\frac{n}{2})} CC_S(i,j) \tag{12}$$

So, the multi-dimensional cross correlation of a *Cloud*-ed image is a good statistical feature with relative 2-d location-aware characteristic to distinguish innocent images from stego ones.

C. Feature Extraction/Analysis

Inputs of the system could be of different sizes, thus first and second features of the feature vector is set to image dimensions, number of rows, and number of columns. Length and width of any 2-d image are maintained to help the steganalysis process. Discrimination of the stego images from the clean ones needs intrinsic features normally increased or decreased, subject to the embedding operation. Next, two statistical features are derived following the Clouding (7-MSBs, 1-LSB) stage.

The frequency sequence of (x-MSBs, y-LSB)-Clouded $m*n$ image is $\{f_0^0,\dots,f_0^{2^y-1},f_1^0,\dots,f_1^{2^y-1},\dots,f_{2^x-1}^0,f_{2^x-1}^{2^y-1}\}$ that f_i^j is related to ith cloud type of jth rain type. Note that always $0\leq i<2^7, 0\leq j<2^1$ and $0<x+y\leq 8$. Frequency is the count of how many pixels. Therefore, the first statistical feature, called *Local Entropies Sum (LES),* is derived as:

$$LES=\sum_{i=0}^{2^x-1}\frac{\sum_{j=0}^{2^y-1}f_i^j}{m*n}h(f_i^0,\dots,f_i^{2^y-1}) \tag{13}$$

where $h(.)$ is the Shannon's entropy function [15]. LES feature increases, when the embedding rate is incremented gradually. LES means that when some random bits, e.g. the embedded bits, are added to an m*n cover, most of Clouds entropies increase and the outcome of the Clouds entropies reaches its limit of one. Consequently, the sum of local entropies of Clouds increases to reach one.

Intuitively, y-LSBs rain types' distribution of x-MSBs Clouds, by increasing the embedding rate, tends to uniform distribution, so LES of 1-LSB rain type's distribution tends to reach one as entropy of the uniform binary distribution.

The second statistical feature, known as *Cloud Min Sum* (CMS) is defined as:

$$CMS=\sum_{i=0}^{2^x-1}\frac{\min(f_i^0,\dots,f_i^{2^y-1})}{m*n} \tag{14}$$

For $x=7\ and\ y=1$, the two features LES and CMS are either incremental, subject to the embedding operation, or between zero and one. CMS probably increases by adding some random multi-bits (y-LSBs) to an m*n cover. Multi-bits (y-LSBs) frequencies reach to each other, when embedding rate is incremented gradually.

If we use 1-LSB rain type, only zeros and ones of Clouds are analyzed and, by adding random bits to an m*n cover, the number of zeros and ones in each cloud will be nearly the same.

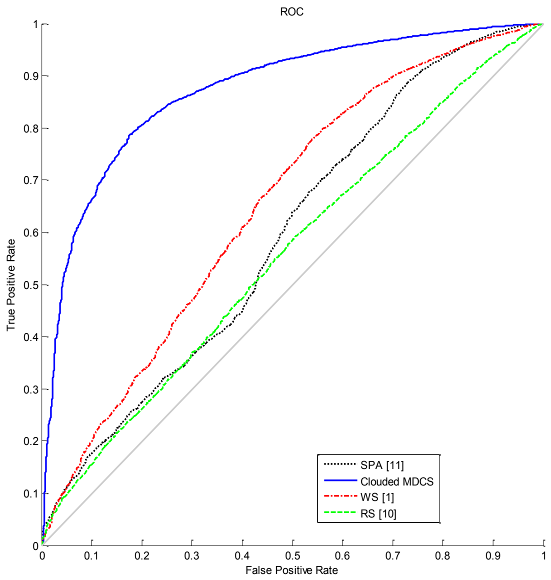


Figure 4. ROC Curves of Clouded MDCS vs. some other methods for 5% embedding rate.

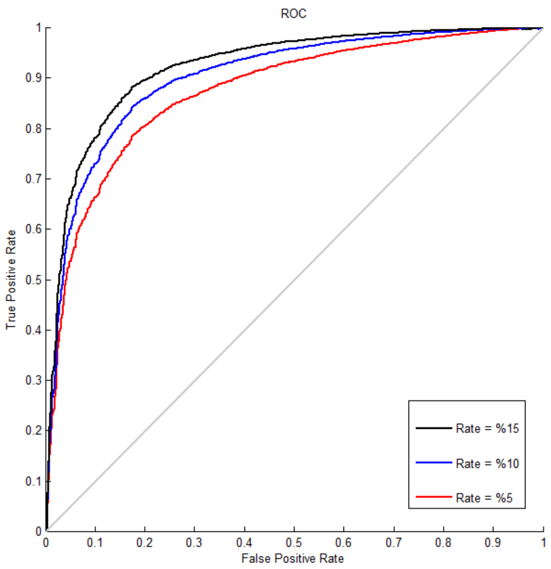


Figure 5. ROC Curves of Clouded MDCS for 5%, 10%, and 15% embedding rates.

Consequently, the sum of Clouds' minimum frequency bit (zero or one) per m*n increases to 0.5 or the sum of Clouds' maximum frequency bit per m*n decreases to 0.5. Intuitively, y-LSBs rain types' distribution of x-MSBs Clouds, by increasing the embedding rate, tends to uniform distribution, so CMS of 1-LSB rain type's distribution is willing to reach 0.5, as median of the uniform binary distribution.

The third incremental feature, as the main contributing feature, is multi-dimensional relative cross-correlation, as defined in Definition-1, is called CCMinus, as it measures the number of different pixels of an image (I) based on the cross-correlation, as:

$$CCMinus = \sum_{(i,j)=(1,1)}^{\left(\frac{m}{2},\frac{n}{2}\right)} CC_I(i,j) \qquad (15)$$

Moreover, CCPlus feature similar to CCMinus feature could be extracted as a multi-dimensional relative cross-correlation as defined in Definition-2, which measures the number of similar pixels of an image through cross-correlations. The main property of CCMinus/CCPlus is the smooth quadratic characteristic curve. Two previous features (LES and CMS) are statistical but they cannot be compensated by some steganographic methods, because they take advantage of intrinsic characteristic of steganography to reach uniform distribution that cannot be avoided as secret message is assumed random. CCMinus or CCPlus take the intrinsic advantage of most natural images. Natural images are locally (here Cloud-ly) correlated and CCMinus traces the cross-correlation of Clouds of an image quite well.

As shown in Fig.3 (a,b,c), when more random bits are embedded into the image (I), CCPlus feature of the image (I) quadratically decreases. To estimate the rate of embedding, we also extracted the statistical features of other higher bit-planes (6th and 7th) of the image (I) that remain by embedding operation. By comparing fig.3(a), fig.3(b), and fig.3(c), we could find the quadratic coefficient of CCPlus curve of innocent 8th bit plane (LSB), and then the constant or free term of CCPlus curve of the LSB plane of the image (I) could be determined. This is because the full embedding rate point is a local minimum point that could always be attained. Therefore, by comparing free term with original term, an estimate of the embedding rate could be achieved.

IV. Computational Complexity

The MDCS method could be run in multiple ways. The bottleneck of the MDCS is when it executes the cross-correlation part. In our MATLAB simulation, we used MATLAB's profiler to find the most complex part of the algorithm. The Stage B of section III consumes the most of the CPU clocks. The Clouded MDCS in worst case is of the same order of complexity, as compared to the Windowed MDCS, if the window and the cloud are of the same size.

The main implementation parameters of the Clouded MDCS include: l as cloud size (normally 512*512), s as number of samples (usually 100 samples), d as depth of correlation (normally $0.001l \cong 16 * 16$ pixels) for an $m * n$-pixel c-bit (usually true-bit or 24-bit) RGB image. The complexity of the MDCS algorithm ($O(N)$), based on (15), is then given as a linear function of the system parameters, as:

$$m * n/l * d * s * l * c \qquad (16)$$

that is independent of the cloud size. This simple relation also shows that the Clouded MDCS needs no sophisticated hardware to get implemented. As discussed in the next section, we have examined some other LSB steganalyzers whose computational complexity is an almost linear function of the image size, so are basically of the same order of the complexity as that of the MDCS. However, the main difference between the computational burdens essentially comes from the learning pre-processing stage that could be omitted in our algorithm, in which the rate estimation could be realized merely based on the information extracted from the image without any prior information from the image database.

V. Experimental Results

We used COREL and NRCS commonly used databases of images to execute our simulation on Pentium IV Quad-Core 2.8 GHz PC for two days using MATLAB. During the simulation period, more than ten thousands images were processed. Among ways explained in parts A, B, and C of section III, we select the approach of the highest performance to detect stego images. The steganography method, as defined in Sec. II.B, is LSB replacement. The Clouded MDCS algorithm with LES, CMS, CCMinus and CCPlus features found to be the best among the others with cloud size of 512*512, depth size of 32*32, and sample rates of 0 to 40 for 512*512-pixel 8-bit images to get results within a reasonable processing time.

The features were set as features vector of a SVM classifier with multi-degree polynomial core with 10000 iterations of quadratic programming for convergence, and a half of images were used in the training stage. In the first experiment, a half of the data were given to the SVM for learning. The second half, including both the innocent images and stego images with embedding rates greater than 5% were used for the steganalysis test by the SVM. In the final stage, stego images with embedding rate of 10%, 15%, and 20% were also given to the SVM.

Based on the simulation results, the Clouded MDCS outperformed the reference methods [1,10,11] tested and compared to our method in the experiments. We compared our approach to other works that were merely based on analytical approaches. Works such as those reported in [2-5] are limited to some conditions like colorful images or non-uniform images that cannot be extended to a wide range of images. In addition, we compared our method to some well-known, basic steganalysis methods, on which some new approaches were relied on. Results are illustrated in figures 4 and 5.

Fig.4 depicts receiver operating characteristic (ROC) curves of the MDCS, WS [1], RS [1], and SPA [11] for 5% embedding rate. As shown, the Clouded MDCS algorithm achieves a better detection performance, as compared to the other schemes. Fig.5 illustrates the ROC curve of the Clouded MDCS for 15% (the inner), 10% (the middle), and 5% (the utter) embedding rates. Furthermore, we have examined our method on other LSB steganography methods, LSB Matching [16] and LSB+ [17]. The observations are almost alike, because the Clouded MDCS depends on the statistical features of LSBs, as shown earlier with CCPlus and CCMinus. The detection performance for both the conventional LSB replacement and the LSB Matching are almost the same. This is while the LSB+ method is detected even faster than the others, because it embeds more bits to resist some other steganalysis methods.

VI. Conclusion

The new multi-dimensional correlation steganalysis, called MDCS, has been proposed in this paper. Major stages of the proposed algorithm include sectioning, relative cross-correlation, and feature extraction/analysis. The MDCS algorithm specifically uses new features for steganalysis, such as clouds min sum and local entropies sum. This algorithm also gives an estimate of the LSB embedding rate when applied to an stego image. The MDCS complexity is adjustable based on the tradeoff between the processing time and the steganalysis accuracy. Simulation results, based on our ROC curve analysis, have shown that the MDCS significantly improves over some well-known methods introduced earlier for steganalysis of the LSB steganography.

References

[1] J. Fridrich and M. Goljan, “On estimation of secret message length in LSB steganography in spatial domain,” in Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI, E. J. Delp III and P. W. Wong, Eds., vol. 5306, pp. 23–34, , 2004.

[2] J. Fridrich, R. Du, and L. Meng, “Steganalysis of LSB Encoding in Color Images,” Proceedings IEEE International Conference on Multimedia and Expo, July 30–August 2, New Yourk, NY, 2000.

[3] S. Dumitrescu, X. Wu, and N. D. Memon, “On steganalysis of random LSB embedding in continuous-tone images,” In Proceedings IEEE International Conference on Image Processing, ICIP 2002, pp. 324–339, Rochester, NY, September 22–25, 2002.

[4] S. R. Khosravi-rad, T. Eghlidos, S. Ghaemmaghami, “Higher-order Statistical Steganalysis of Random LSB Steganography,” IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), pp. 629-632, May 2009.

[5] G. Gul, F. Kurugollu, "SVD-Based Universal Spatial Domain Image Steganalysis," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp. 349-353, June 2010.

[6] R. A. Horn, C. R. Johnson, “Matrix Analysis,” Cambridge University Press, 1990.

[7] J. Fridrich, M. Goljan, “Practical steganalysis of digital images – state of the art,” in Proc. SPIE Security and Watermarking of Multimedia Contents, E. J. Delp III and P. W. Wong (eds.), vol. 4675, pp. 1–13, 2002.

[8] J. Harmsen, W. Pearlman, “Higher-order statistical steganalysis of palette images,” in Proc. SPIE Security Watermarking Multimedia Contents, E. J. Delp III and P. W. Wong (eds.), vol. 5020, pp. 131–142, 2003.

[9] Andrew D. Ker, “Steganalysis of LSB Matching in Grayscale Images,” IEEE Signal Processing Letters, vol. 12(6), pp. 441–444, 2005.

[10] J. Fridrich, M. Goljan, R. Du, “Reliable detection of LSB steganography in color and grayscale images,” Proc. ACM Workshop on Multimedia and Security, pp. 27-30, 2001.

[11] S. Dumitrescu, X. Wu, Z. Wang, “Detection of LSB steganography via sample pair analysis,” IEEE Transactions on Signal Processing, vol. 51, no. 7, pp. 1995-2007, 2003.

[12] S. Dumitrescu, X. Wu, “Steganalysis of LSB Embedding in Multimedia Signals”, in IEEE ICME'02, pp. 581–584, August 2002.

[13] Andrew D. Ker, “A general framework for structural steganalysis of LSB replacement,” in Proc. 7th Information Hiding Workshop, vol. 3727 of Springer LNCS, pp. 296–311, 2005.

[14] P. Lu, X. Luo, Q. Tang and L. Shen, "An Improved Sample Pairs Method for Detection of LSB Embedding," in Proc. 6th Information Hiding Workshop, Springer LNCS 3200, pp. 116-127, 2004.

[15] Shannon, C.E., “A Mathematical Theory of Communication,” The Bell System Technical Journal 27, 379-423, pp. 623-656, 1948.

[16] J. Mielikainen, “LSB matching revisited,” IEEE Signal Processing Letter,vol. 13, no. 5, pp. 285-287, May 2006.

[17] Wu, H., Dugelay, J., Cheung, Y., “A data mapping method for steganography and its application to images,” In Lecture notes in computer science, Vol. 5284. Proceedings of the 10th information hiding workshop, pp. 236–250,. Berlin: Springer, 2008.