Available online at www.sciencedirect.com

ScienceDirect

Information Sciences 178 (2008) 21–36

INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL

www.elsevier.com/locate/ins

Image complexity and feature mining for steganalysis of least significant bit matching steganography

Qingzhong Liu [a], Andrew H. Sung [a,*], Bernardete Ribeiro [b], Mingzhen Wei [c], Zhongxue Chen [d], Jianyun Xu [e]

[a] *New Mexico Institute of Mining and Technology, Socorro, NM 87801, USA*
[b] *Department of Informatics Engineering, University of Coimbra, Portugal*
[c] *University of Missouri-Rolla, 1870 Miner Circle, Rolla, MO 65409, USA*
[d] *Department of Statistical Science, Southern Methodist University, Dallas, TX 75275-0332, USA*
[e] *Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA*

Received 6 February 2006; received in revised form 2 August 2007; accepted 6 August 2007

Abstract

The information-hiding ratio is a well-known metric for evaluating steganalysis performance. In this paper, we introduce a new metric of image complexity to enhance the evaluation of steganalysis performance. In addition, we also present a scheme of steganalysis of least significant bit (LSB) matching steganography, based on feature mining and pattern recognition techniques. Compared to other well-known methods of steganalysis of LSB matching steganography, our method performs the best. Results also indicate that the significance of features and the detection performance depend not only on the information-hiding ratio, but also on the image complexity.

Keywords: Steganalysis; LSB matching steganography; Image complexity; Correlation; Classification

1. Introduction

Steganography is the art and science of covert communication without the existence of the hidden messages. In contrast to cryptography, where the existence of the message itself is not disguised but the content is obscured, the advantage of using steganography over using cryptography alone is that the secret messages will not attract attention to persons. In steganography, a covert message can be hidden in digital image, audio, video, and TCP/IP packet. The digital image is currently one of the most popular digital mediums for carrying covert messages. The innocent image is called the carrier or the cover, and the adulterated image carrying some hidden data is called the stego-image or steganogram. In image steganography, the common information-hiding

[*] Corresponding author. Tel.: +1 505 835 5949; fax: +1 505 835 5587.
E-mail address: sung@cs.nmt.edu (A.H. Sung).

0020-0255/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2007.08.007

techniques implement hiding data in digital images by either modifying the pixel values in the space domain (space-hiding system) or modifying the transform coefficients (transform-hiding system) of the images.

In space-hiding systems, one simple method is that of least significant bit (LSB) steganography, or LSB embedding [22]. Each byte of an image represents a different color. The last few bits in a color byte, however, do not hold as much significance as the first few. Therefore, two bytes that only differ in the last few bits can represent two colors that are virtually indistinguishable to the human eye. For example, 00100100 and 00100101 are technically two different shades of red. However, since it is only the last bit that is different, it is impossible to see the color difference. LSB embedding alters these last bits by hiding a message within them. LSB embedding has the merit of simplicity, but suffers from a lack of robustness, and it is easily detected. LSB matching, another information-hiding system in the space domain, randomly alters the bytes by plus or minus one according to the bit of the cipher message, rather than simply replacing the last bits [41].

In transform-hiding systems, a message is embedded by way of modifying transform coefficients. There are three common transform techniques: the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT), and the Discrete Fourier Transform (DFT). For example, by hiding data in the low frequency part of a 2D lossless wavelet transform and utilizing convolution error correction coding, Xu et al. presented an image steganography that was extremely robust against JPEG compression [51]. Derek Upham published JPEG-JSteg for hiding data in JPEG images. Its embedding algorithm sequentially replaces the least significant bit of DCT coefficients with the message's data [35]. Unfortunately, it is easily detected [52]. Instead of replacing the least significant bit of the DCT coefficient with message data, F5 algorithm [48] decrements its absolute value in a process called matrix encoding. Ramkumar et al. proposed an efficient Fast Fourier Transform (FFT)-based signal scheme for multimedia steganography; it permits the use of large dimensional signal sets without drastically increasing the computational complexity [36]. Other information-hiding techniques include spread spectrum steganography [30], statistical steganography, and distortion and cover generation steganography [19].

Steganalysis aims to discover the presence of hidden data. To detect adulterated content in other digital files, Guo et al. proposed a novel fragile watermarking, to verify the integrity of streaming data and to detect malicious modifications of database relations [12,13]. Some information-hiding systems are known to be efficiently detectable in images, including LSB embedding, spread spectrum steganography, the F5 algorithm, and other JPEG steganography systems [3,4,6,8,9,15,20,26,34]. Some other embedding paradigms, such as stochastic modulation [7,32] and LSB matching [41], are much more difficult to detect.

There are a few detectors for LSB matching steganography. A well-known detector is the histogram characteristic function center of mass (HCFCOM) proposed by Harmsen and Pearlman [15]. Based on HCFCOM, Ker proposed Adjacency HCFCOM and Calibrated HCFCOM to improve the probability of detection for LSB matching in grayscale images [21]. Lyu and Farid described a wavelet-like decomposition approach to detect hidden data in images, by building high-order statistical models of natural images [27,28]. Fridrich et al. presented a Maximum Likelihood (ML) estimator for predicting the hiding ratio of non-adaptive $\pm$ K embedding in images [10]. Holotyak et al. demonstrated a blind steganalysis, with classifications based on high order statistics of the estimation signal [17]. Unfortunately, the ML estimator "fail[s] to reliably estimate the message length once the variance of the sample exceeds 9" [10].

The information-hiding ratio is an important reference for evaluating steganalysis performance. Specifically, a higher the hiding ratio indicates a higher detection performance. To our knowledge, however, few publications mention the image complexity, another critical reference for evaluating detection performance. In this paper, based on our previous work [24,25], we introduce a parameter of image complexity that is measured by the shape parameters of the Generalized Gaussian Distribution (GGD) in the wavelet domain. This presents different features for detecting the information-hiding behavior in LSB matching steganography, and demonstrates the relationships between statistical significance, detection performance, information-hiding ratio, and image complexity.

2. Image complexity and GGD model

Several papers [18,40,42,46,49,50] describe statistical models of images, such as Markov Random Field models (MRFs), the Gaussian Mixture Model (GMM), and the Generalized Gaussian Distribution (GGD) model in transform domains, such as the DCT, DWT, or Discrete Fourier Transform (DFT).

Experiments show that adaptively varying two parameters of the GGD [33,40] can achieve a good Probability Distribution Function (PDF) approximation, for the marginal density of coefficients at a particular subband, produced by various types of wavelet transforms. These two parameters are defined as:

$$p(x;\alpha,\beta)=\frac{\beta}{2\alpha(1/\beta)}\mathrm{e}^{-(|x|/\alpha)^{\beta}} \tag{1}$$

where $\Gamma(\cdot)$ is the Gamma function, $\Gamma(z)=\int_0^\infty \mathrm{e}^{-t}t^{z-1}\,\mathrm{d}t, z>0$.

Here the scale parameter, α, models the width of the PDF peak (standard deviation), while the shape parameter, β, is inversely proportional to the decreasing rate of the peak. The GGD model contains the Gaussian and Laplacian PDFs as special cases, using $\beta=2$ and $\beta=1$, respectively.

Generally, an image with high complexity has a high shape parameter of the GGD in the wavelet domain. Fig. 1 shows some grayscale images with different textures on the left, and the histogram distributions of the Haar wavelet HH subband coefficients, and the GGD simulations, are shown on the right. The high peak distribution of the wavelet coefficients is obtained at the value of zero. It indicates that adjacent pixels are highly correlated. More clearly, Fig. 2a shows an 8-bit grayscale image. The variable $v(i,j)$ denotes the grayscale value at point (i,j) and $v(i+1,j)$ denotes the grayscale value at the point $(i+1,j)$. The occurrence probability of the pair $(v(i,j), v(i+1,j))$ represents the joint distribution of the adjacent points, shown in Fig. 2b. Fig. 2 demonstrates the high correlation of adjacent pixels.

3. Feature extraction

Since LSB matching steganography mainly modifies the binary bits in the least significant bit plane (LSBP), we consider the correlation between LSBP and the second least significant bit plane (LSBP2). $M_1(1{:}m,1{:}n)$ denotes the binary bits of the LSBP, and $M_2(1{:}m,1{:}n)$ denotes the binary bits of the LSBP2. Here, m and n are the numbers of pixels in horizontal and vertical directions, and E is the mathematical expectation. The covariance function is defined as:

$$\mathrm{Cov}(x_1,x_2)=E[(x_1-u_1)(x_2-u_2)], \tag{2}$$

where $u_i=E(x_i)$.

$C1$ is defined as follows:

$$C1=\mathrm{cor}(M_1,M_2)=\frac{\mathrm{Cov}(M_1,M_2)}{\sigma_{M_1}\sigma_{M_2}}, \tag{3}$$

where $\sigma^2_{M_1}=\mathrm{Var}(M_1)$, and $\sigma^2_{M_2}=\mathrm{Var}(M_2)$.

The autocorrelation $C(k,l)$ of the LSBP is defined as follows:

$$C(k,l)=\mathrm{cor}(X_k,X_l), \tag{4}$$

where $X_k=M_1(1{:}m\text{-}k,1{:}n\text{-}l)$; $X_l=M_1(k+1{:}m,l+1{:}n)$. Setting k and l to different values, the features from C2 to C15 are presented as follows:

$$C2=C(1,0);\quad C3=C(2,0);\quad C4=C(3,0);\quad C5=C(4,0);$$
$$C6=C(0,1);\quad C7=C(0,2);\quad C8=C(0,3);\quad C9=C(0,4);$$
$$C10=C(1,1);\quad C11=C(2,2);\quad C12=C(3,3);\quad C13=C(4,4);$$
$$C14=C(1,2);\quad C15=C(2,1).$$

The variable ρ_k denotes the histogram probability density of coverage at the intensity, k ($k=0, 1,\ldots,N-1$, for 8-bit grayscale image, $N=256$). The variable, ρ'_k, denotes the histogram probability density of adulterated images at the intensity, k. Assuming the hidden data is independent and identically distributed, and if the LSBP hiding ratio is r, ρ'_k is given as follows:

$$\rho'_k=(1-r/2)^*\rho_k+(r/4)^*\rho_{k-1}+(r/4)^*\rho_{k+1}$$

It is too difficult to accurately judge whether the testing image carries some hidden data or not, and to predict the hiding ratio r, without the original cover and based only on the distribution density of the histogram. However, LSB matching steganography definitely modifies the distribution density of the histogram. Based on

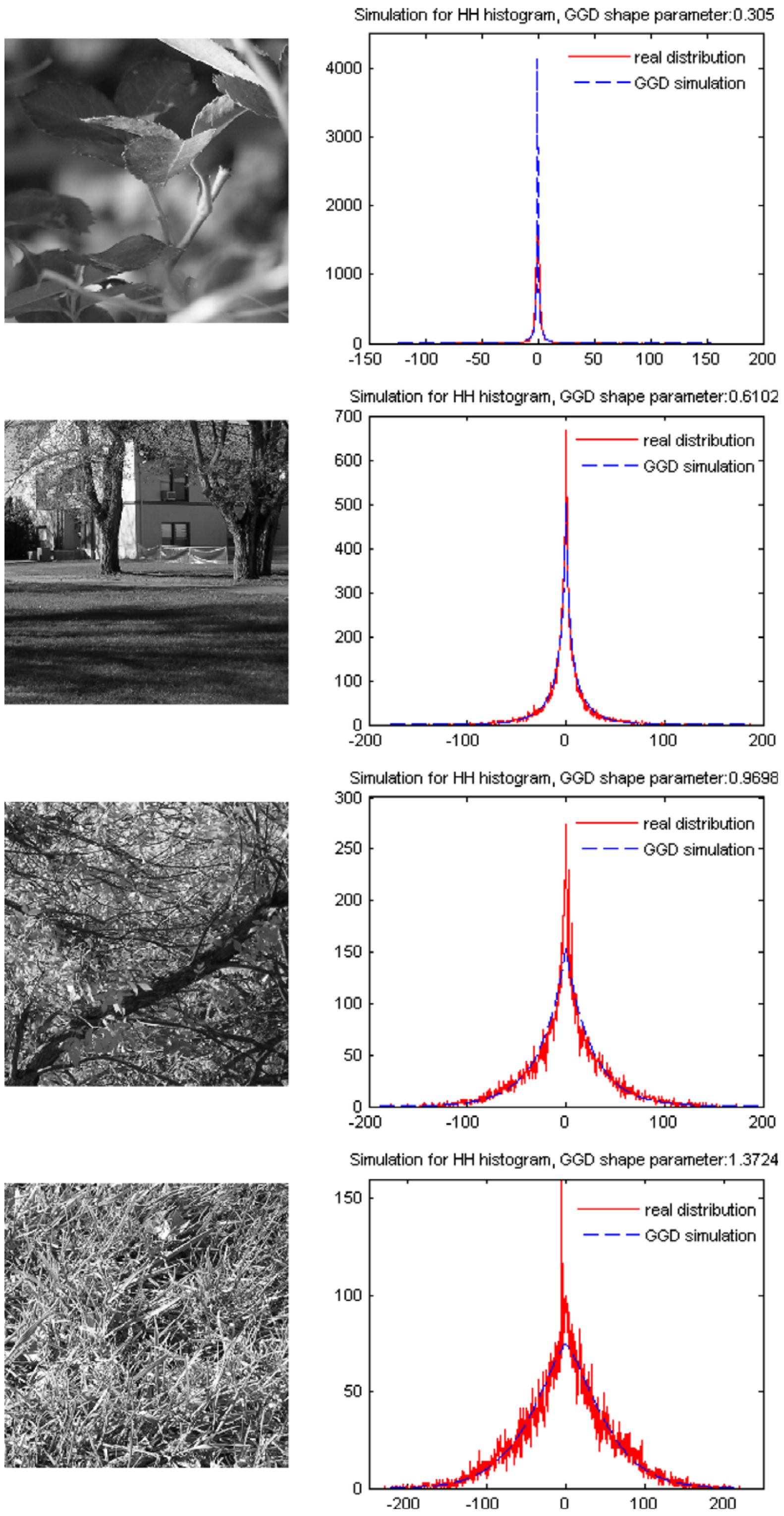


Fig. 1. The 256 × 256 grayscale images with different complexity (left) and the generalized Gaussian distribution of the HH subband coefficients (right), decomposed by Haar wavelet. The figure indicates that the image with low complexity has low shape parameter of the GGD, and the image with high complexity has high shape parameter of the GGD.

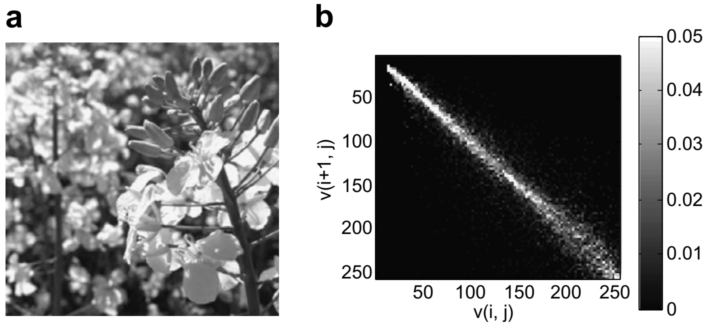


Fig. 2. An 8-bit grayscale image (a) and the joint probability distribution of the adjacent pixels (b). This shows that the adjacent pixels are highly correlated.

this point, we present the correlation features on the histogram. The histogram probability density, H, is denoted as (ρ_0, ρ_1, $\rho_2 \ldots \rho_{N-1}$). The histogram probability densities, H_e, H_o, H_{l1}, and H_{l2} are given:

$$H_e = (\rho_0, \rho_2, \rho_4 \ldots \rho_{\mathrm{N}-2}), \quad H_o = (\rho_1, \rho_3, \rho_5 \ldots \rho_{\mathrm{N}-1});$$
$$H_{l1} = (\rho_0, \rho_1, \rho_2 \ldots \rho_{\mathrm{N}-1-l}), \quad H_{l2} = (\rho_l, \rho_{l+1}, \rho_{l+2} \ldots \rho_{\mathrm{N}-1}).$$

The autocorrelation coefficients C16 and C_{H} (l) are defined as:

$$C16 = \mathrm{cor}(H_e, H_o) \tag{5}$$
$$C_{\mathrm{H}}(l) = \mathrm{cor}(H_{l1}, H_{l2}) \tag{6}$$

Set $l = 1$, 2, 3 and 4; the features C17–C20 are:

$$C17 = C_{\mathrm{H}}(1), \quad C18 = C_{\mathrm{H}}(2), \quad C19 = C_{\mathrm{H}}(3), \quad C20 = C_{\mathrm{H}}(4).$$

Besides the features mentioned above, we consider the difference between the testing image and the denoised image. The symbol CI denotes the original cover and CI′ denotes the stego-image. Embedding information into images may be modeled as the process of adding noise. D (·) is some denoising function. We define the difference between pre-denoised and post-denoised images as follows:

$$E_{\mathrm{CI}} = \mathrm{CI} - D(\mathrm{CI}) \tag{7}$$
$$E_{\mathrm{CI}'} = \mathrm{CI}' - D(\mathrm{CI}') \tag{8}$$

The hypothesis is that the statistics of E_{CI} and $E_{\mathrm{CI}'}$ are different. We apply wavelet hard-threshold denoising without shrinkage [29] to the image. First, we apply wavelet transform to the testing image, find the wavelet coefficients in HL, LH, and HH sub-bands whose absolute values are smaller than some threshold value t, set these coefficients to zero, and reconstruct the image by applying the inverse wavelet transform to the modified wavelet coefficients. The reconstructed image is treated as the denoised image. The difference between the original and the denoised image is E_t. The correlation features in the difference domain are given as follows:

$$C_E(t; k, l) = \mathrm{cor}(E_{t,k}, E_{t,l}) \tag{9}$$

where $E_{t,k} = E_t(1{:}m\text{-}k, 1{:}n\text{-}l)$; $E_{t,l} = E_t(k+1{:}m, l+1{:}n)$. Setting different values to t, k, and l, features C21–C41 are presented as follows:

$$C21 = C_E(1.5;0,1); \quad C22 = C_E(1.5;1,0); \quad C23 = C_E(1.5;1,1); \quad C24 = C_E(1.5;0,2); \quad C25 = C_E(1.5;2,0);$$
$$C26 = C_E(1.5;1,2); \quad C27 = C_E(1.5;2,1);$$
$$C28 = C_E(2;0,1); \quad C29 = C_E(2;1,0); \quad C30 = C_E(2;1,1); \quad C31 = C_E(2;0,2); \quad C32 = C_E(2;2,0);$$
$$C33 = C_E(2;1,2); \quad C34 = C_E(2;2,1);$$
$$C35 = C_E(2.5;0,1); \quad C36 = C_E(2.5;1,0); \quad C37 = C_E(2.5;1,1); \quad C38 = C_E(2.5;0,2); \quad C39 = C_E(2.5;2,0);$$
$$C40 = C_E(2.5;1,2); \quad C41 = C_E(2.5;2,1).$$

In RGB color images, the matrices M_{r1}, M_{g1}, and M_{b1} stand for the least significant bit planes of red, blue, and green channels, respectively. The correlation coefficients C_{rg}, C_{rb}, and C_{gb}, are given as follows, where abs(·) denotes the absolute value function.

$$C_{\mathrm{rg}} = \mathrm{abs}(\mathrm{cor}(M_{\mathrm{r1}}, M_{\mathrm{g1}})) \tag{10}$$

$$C_{\mathrm{rb}} = \mathrm{abs}(\mathrm{cor}(M_{\mathrm{r1}}, M_{\mathrm{b1}})) \tag{11}$$

$$C_{\mathrm{gb}} = \mathrm{abs}(\mathrm{cor}(M_{\mathrm{g1}}, M_{\mathrm{b1}})) \tag{12}$$

Similar to (9), $E_{t,c}$ $(c = r, g, b)$ is the difference across the color channels (red, green, and blue) of the original and the reconstructed. The correlation features are defined as follows:

$$C_{E_{\mathrm{rg}}}(t) = \mathrm{cor}(E_{t,r}, E_{t,g}); \tag{13}$$

$$C_{E_{\mathrm{rb}}}(t) = \mathrm{cor}(E_{t,r}, E_{t,b}); \tag{14}$$

$$C_{E_{\mathrm{gb}}}(t) = \mathrm{cor}(E_{t,g}, E_{t,b}). \tag{15}$$

After extracting the features defined above, we apply analysis of variance (ANOVA) [2,37] and choose the features with high statistical significance as the final detector.

4. Experiments and results

4.1. Experimental setup

Generally, in the steganalysis of space-hiding systems, the detection of images compressed once is easier than that of images never compressed. To solve the puzzles in the detection of never compressed images, the original covers in our experiments are 5000 TIFF raw format, 24-bit, 640 × 480 pixels, lossless, true color and digital images that have never been compressed.

According to the method in [27,28], we cropped the original images into 256 × 256 pixels in order to get rid of the low complexity parts of the images. The cropped images are the covers in the steganalysis of color images. We categorize the covers according to the parameters of their image complexity.

The image complexity for color images is calculated as follows:

$$\beta = (\beta_{\mathrm{r}} + \beta_{\mathrm{g}} + \beta_{\mathrm{b}})/3 \tag{16}$$

The variable β_c $(c = r, g, b)$ is the shape parameter of the GGD of the HH subband coefficients in the color channel (red, green, and blue). Fig. 3 lists some color cover samples with different image complexities.

The cropped color images are converted into grayscales which are the covers in the steganalysis of grayscale images. The image complexity in grayscale images is measured by the shape parameter of the GGD of the HH subband coefficients.

Stego-images are produced with the LSB matching algorithm. The hidden messages include digital images, audios, texts, pdf files, zipped files, executable software code, source code, and random signals. The hidden data in any two covers is different.

In the steganalysis of color images, the feature set consists of the following features: (a) $C1$, $C2$, $C6$, $C10$, $C14$, $C15$, $C16$, $C17$, C_E (2.5;1,0), C_E(2.5;0,1), C_E(2.5;1,1), C_E(3;0,1), C_E (3;1,0), and C_E(3;1,1), defined in Section 3, corresponding to red, green, and blue channels, for 14 × 3 = 42 features; (b) $C_{E_{\mathrm{rg}}}(t)$, $C_{E_{\mathrm{rb}}}(t)$, $C_{E_{\mathrm{gb}}}$ (t) ($t = 1$, 1.5, and 2), for 3 × 3 = 9 features; and (c) C_{rg}, C_{rb}, and C_{gb}, with a total 54 features. We compare the proposed feature set against other well-known feature sets: Histogram Characteristic Function Center of Mass (HCFCOM) [15] and High-Order Moment statistics in the Multi-Scale decomposition domain (HOMMS) [48,49]. There are 3-dimension features of HCFCOM and 216-dimension features of HOMMS in color images.

In the steganalysis of grayscale images, the correlation feature set consists of the 41 features, C1 to C41, as defined in Section 3. The HOMMS feature set consists of 72 features in grayscale images. We extend the HCFCOM feature set to the high order moments. HCFHOM stands for HCF center of mass High Order Moments, and HCFHOM (r) denotes the rth order moment. In our experiments, the HCFHOM feature set consists of

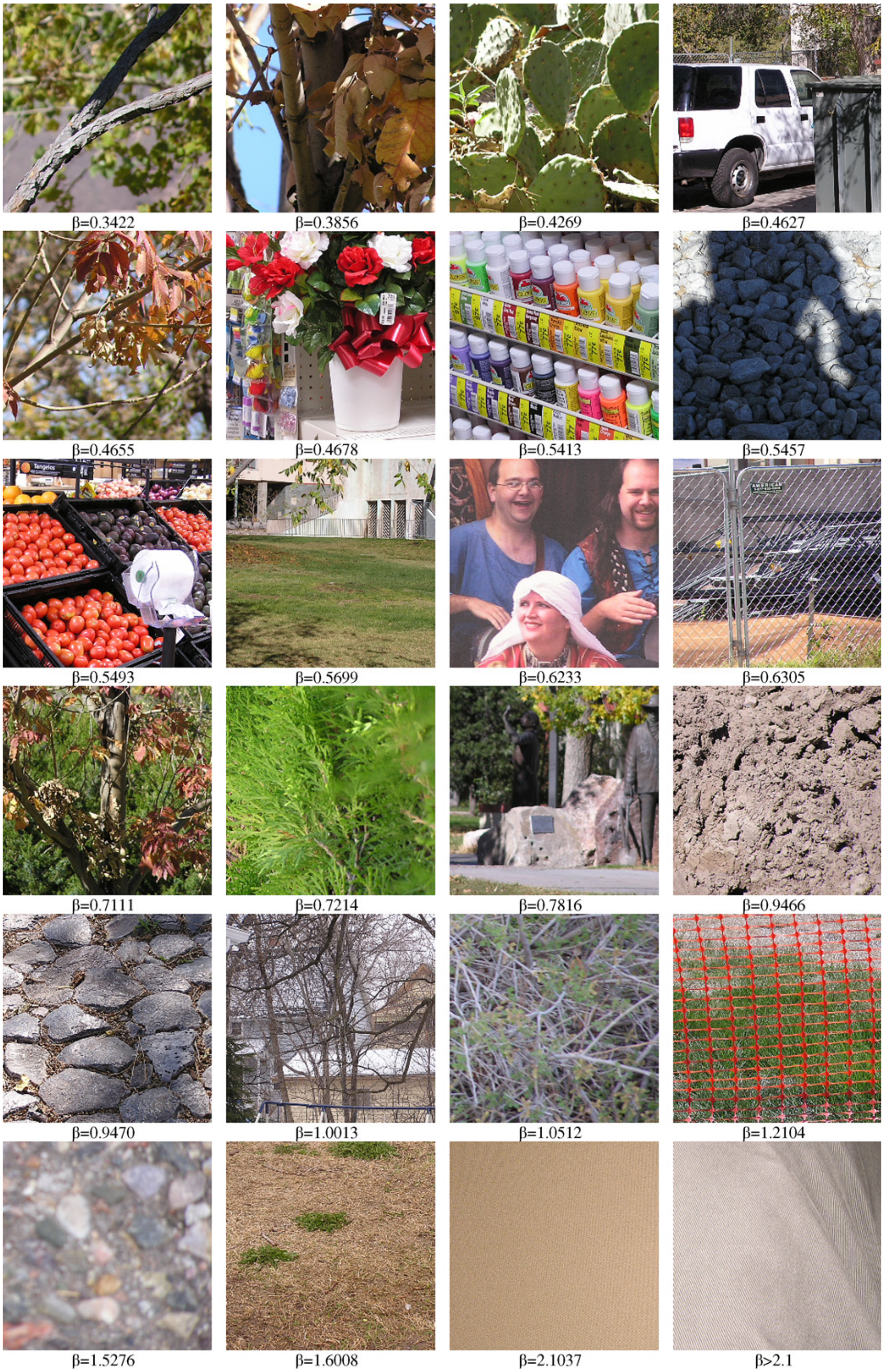


Fig. 3. Some cover samples with different image complexity in our experiments.

HCFCOM and HCFHOM(r) ($r = 2$, 3, and 4). Additionally, Adjacency HCFCOM (A.HCFCOM) and Calibrated Adjacency HCFCOM (C.A.HCFCOM) [21] are compared.

Generally, different classifiers have different classification performances on different feature sets. In our experiments, we utilize the following classifiers:

1. Fisher Linear Discriminate (FLD),
2. Optimization of the Parzen Classifier (ParzenC),
3. Naive Bayes classifier (NBC),

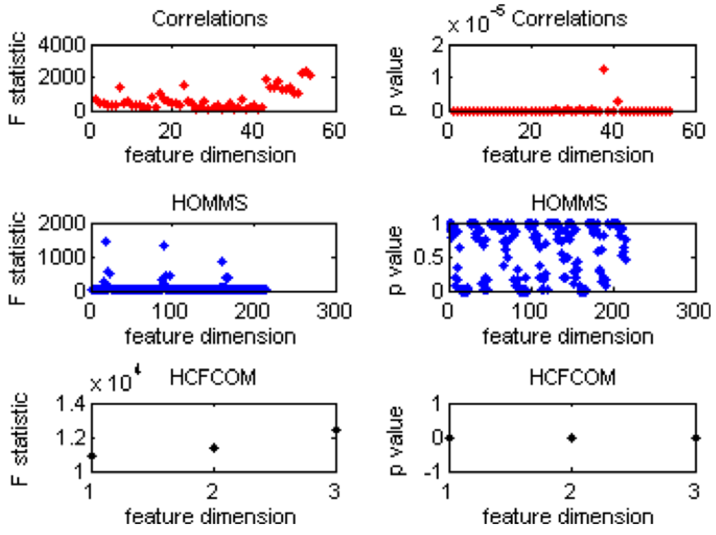


Fig. 4. *F* statistics and *p*-values of correlations, HOMMS, and HCFCOM features in color images. The information-hiding ratio is 12.5%.

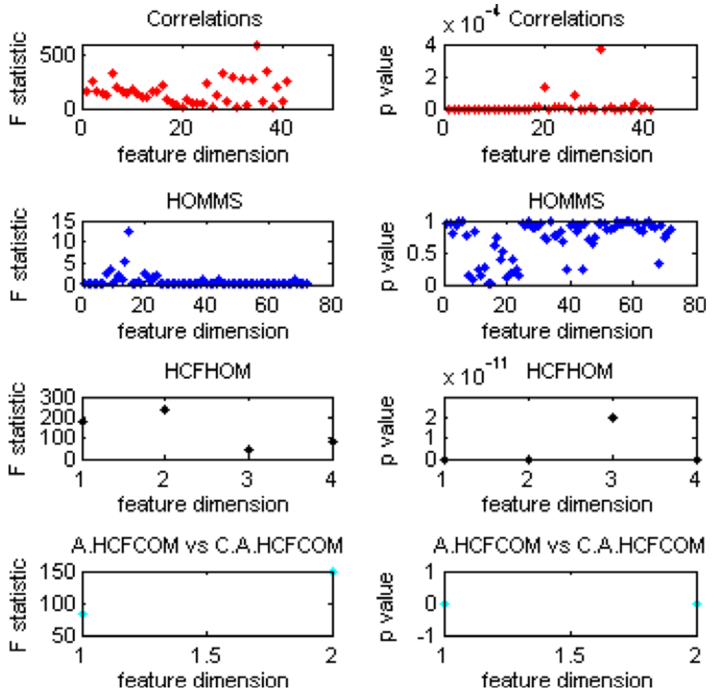


Fig. 5. *F* statistics and *p*-values of correlations, HOMMS, HCFHOM, A. HCFCOM and C.A.HCFCOM features in grayscale images. The information-hiding ratio is 12.5%.

4. Support Vector Machines (SVM),
5. Linear Bayes Normal Classifier (LDC),
6. Quadratic Bayes Normal Classifier (QDC),
7. Bayes Classifier (BC) that is based on maximal likelihood estimation of Gaussian mixture model,
8. Adaboost algorithm (Adaboost) which produces a classifier composed from a set of weak rules.

The details of these classifiers are described in the references [5,11,16,38,39,44,45,47]. We apply each classifier to each feature set in each category of image complexity sixteen times. Each time, the training samples are randomly chosen, and the remaining samples are tested. The ratio of training sets to testing sets is 2:3.

4.2. Comparison of statistical significances

Parametric tests work well with large samples, even if the population is non-Gaussian [1,31]. Fig. 4 lists the F statistics and p-values of correlation features (CF), HOMMS, and HCFCOM features extracted from 5000 covers and 5000 LSB matching steganograms in color images. The LSBP hiding ratio of these stego-images is

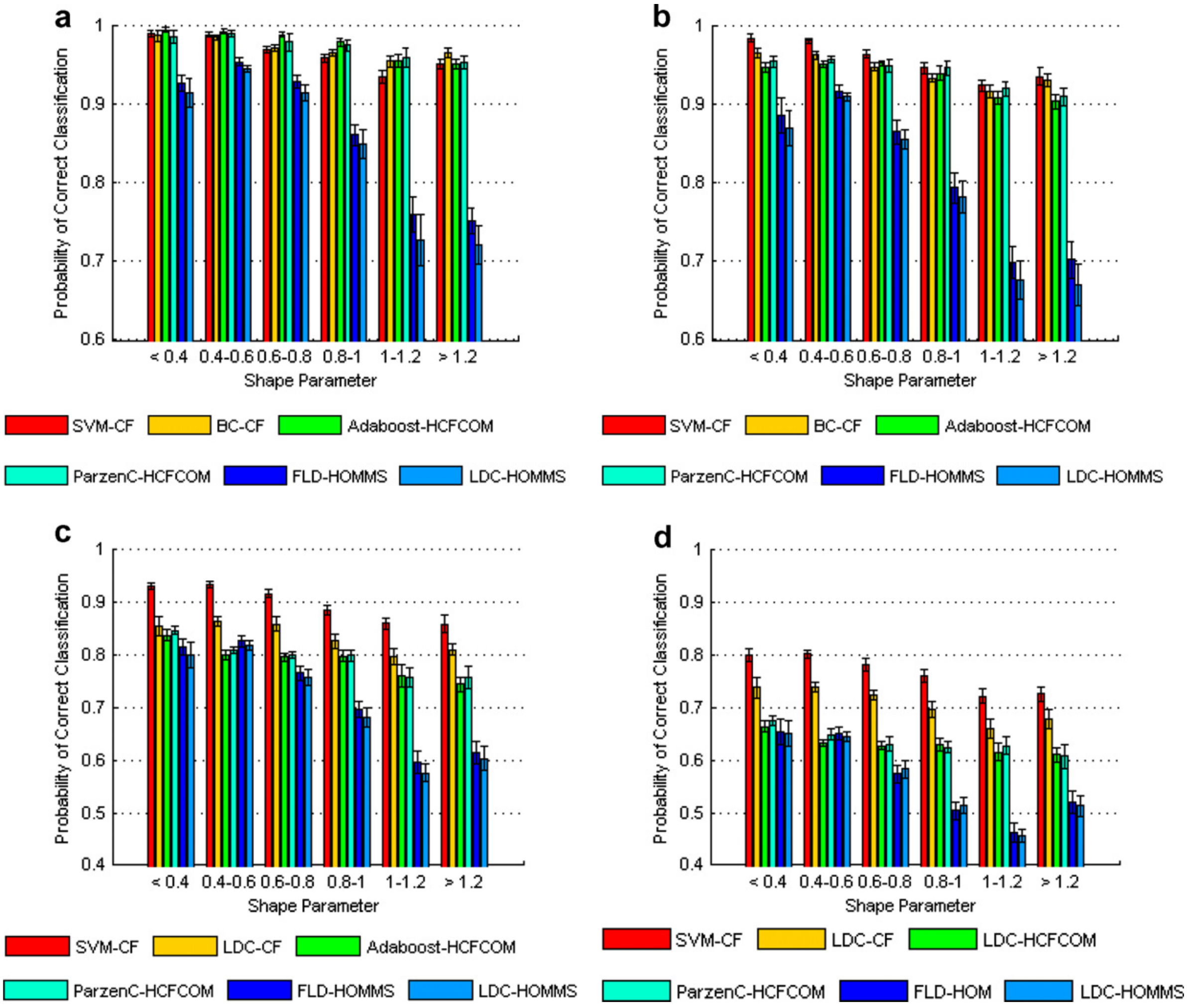


Fig. 6. Top two classifications (mean values and standard deviations) on each feature set and the corresponding classifiers (steganalysis of color LSB matching steganography). LSBP hiding ratios are 1 (a), 0.75 (b), 0.5 (c), and 0.25 (d), respectively. In the legends for (a)–(d), SVM-CF denotes applying SVM to Correlation Features (CF), Adaboost-HCFCOM denotes applying Adaboost to HCFCOM features, and so on.

1, so the information-hiding ratio is 12.5% of the maximum hiding ratio. Fig. 4 shows that the HCFCOM features with the highest *F* statistics and lowest *p*-values are better than correlation features; correlation features with high *F* statistics and low *p*-values are better than HOMMS features. In HOMMS, there are many features with high *p*-values. This indicates that these features are weak in discriminating cover images and stego-images. In correlation features, generally the inter-channel features (dimensions 43–54) have higher *F* statistics than the intra-channel features (dimensions 1–42), which shows that the inter-channel features are better discriminators than the intra-channel ones.

Fig. 5 lists the *F* statistics and *p*-values of CF, HOMMS, HCFHOM, A. HCFCOM, and C.A.HCFCOM features extracted from 5000 covers and 5000 LSB matching stego-images in grayscale images. The LSBP hiding ratio is 1 so the information-hiding ratio is 12.5% the maximum hiding ratio. This shows that correlation features with the highest *F* statistics and lowest *p*-values are better than other features. The HOMMS features are not good because the *p*-values of many HOMMS features are close to 1, meaning that the statistical significance of these HOMMS features are low, and their classification performance is the worst.

4.3. Comparison of the detection performance

Fig. 6 shows the top two testing accuracy values on each feature set in color images under the LSBP hiding ratios of 1, 0.75, 0.5, and 0.25 (Fig. 6a–d). Regarding the detection performance, the set of correlation features (CF) outperforms HCFCOM, and HCFCOM is superior to HOMMS. The detection performance is consistent with the statistical significance presented in Section 4.2. Fig. 6 indicates that, while the information-hiding ratio decreases, the detection performance also decreases when the image complexity increases. The detection performance on HOMMS is not very good when the parameter of image complexity, β, is greater than one.

Fig. 7 lists the best classifications in grayscale images under different hiding ratios and different image complexities. On average, the classification performance of CF is the best, and the performance of HOMMS is the

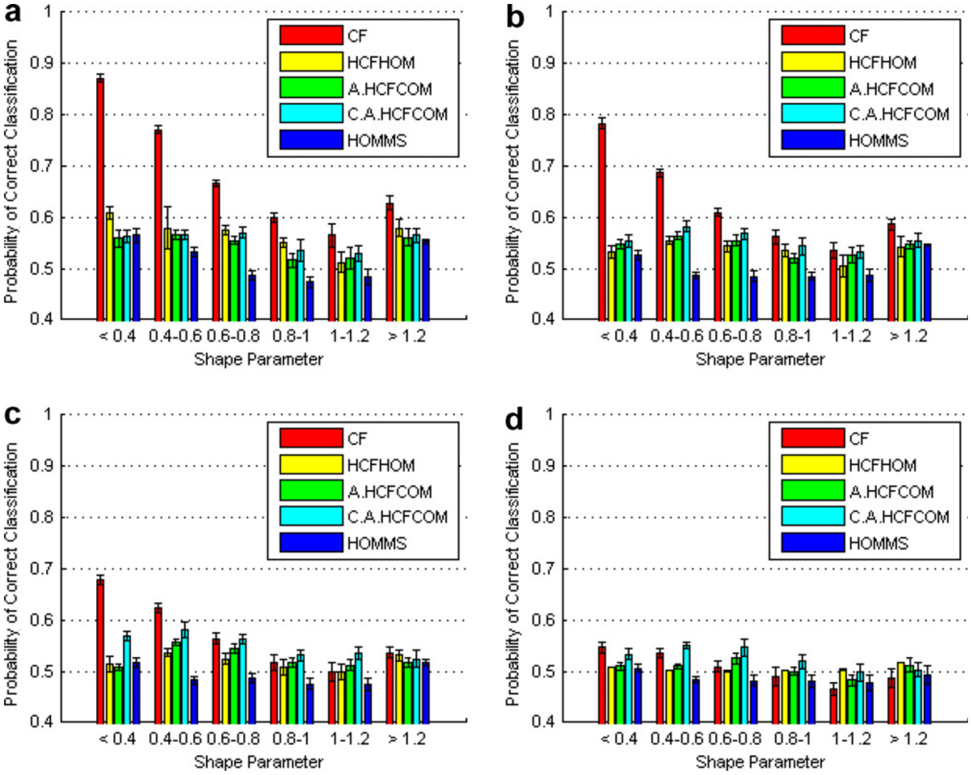
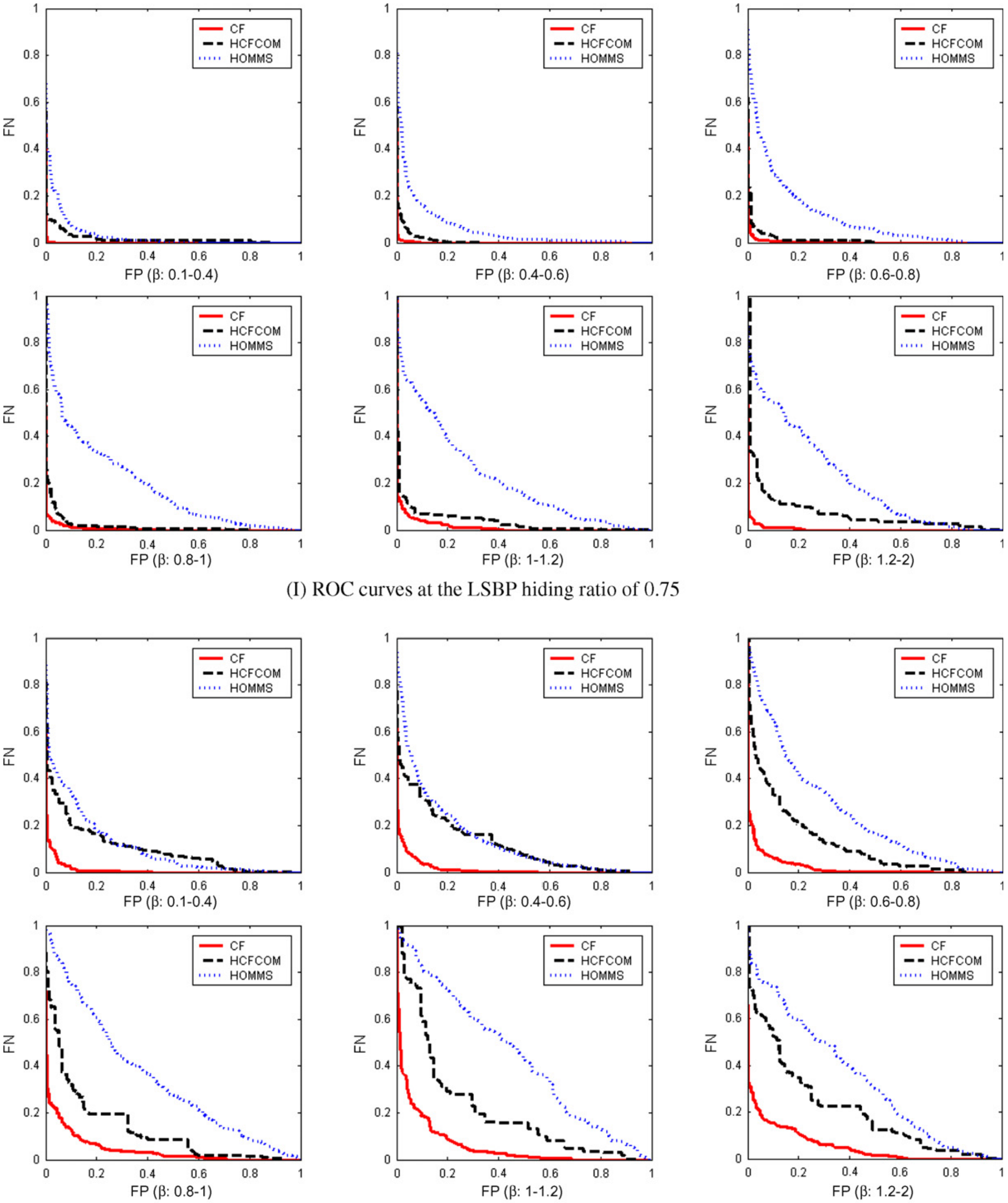


Fig. 7. The best classification (mean values and standard deviations) on each feature set (steganalysis of grayscale LSB matching steganography). The LSBP hiding ratios are 1 (a), 0.75 (b), 0.5 (c), and 0.25 (d), respectively.

worst. As the image complexity increases and/or the information-hiding ratio decreases, the classification performance decreases. When the parameter of image complexity is greater than 0.8 or the LSBP hiding ratio is less



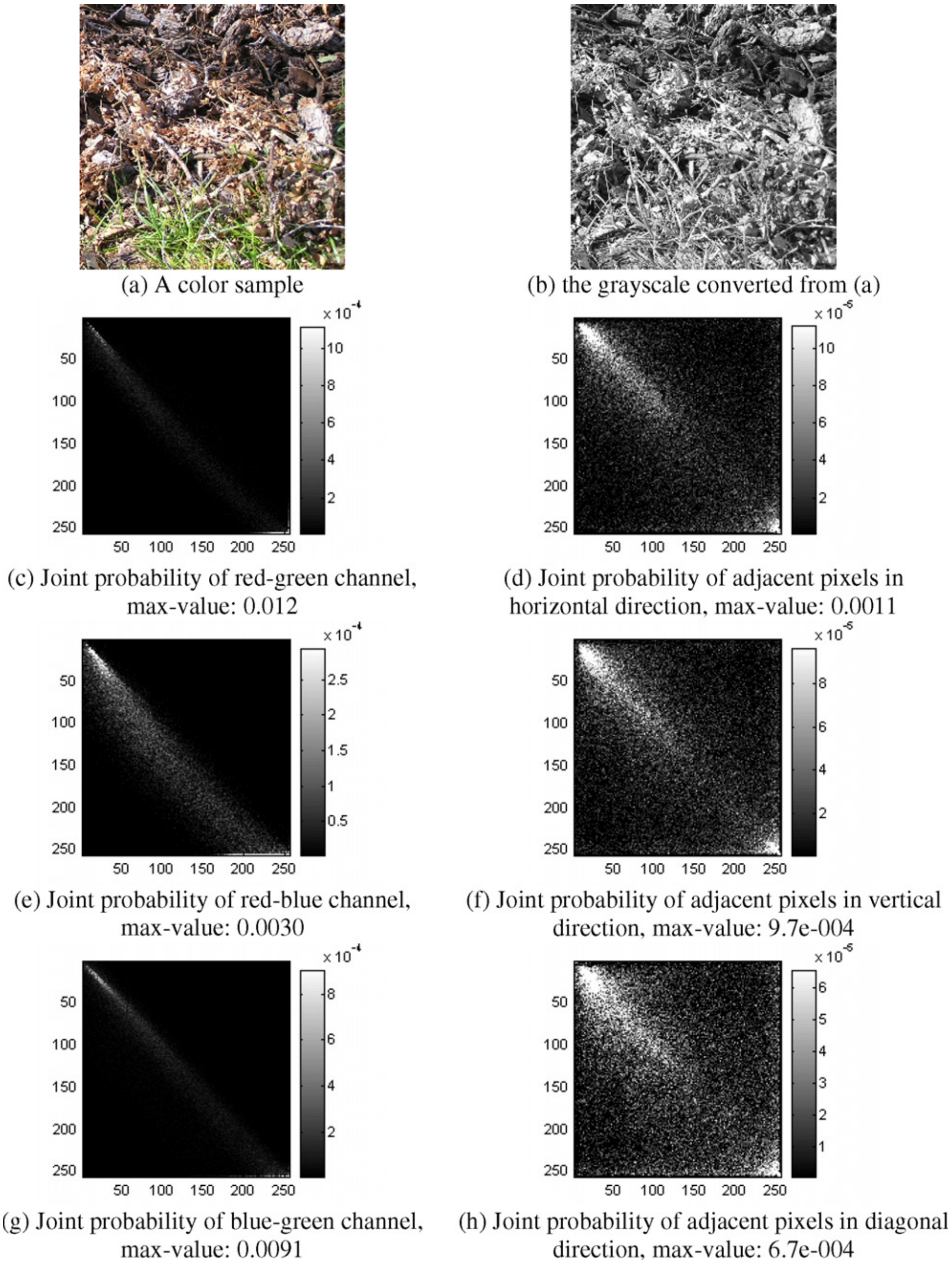
(I) ROC curves at the LSBP hiding ratio of 0.75

(II) ROC curves at the LSBP hiding ratio of 0.5

Fig. 8. ROC curves in the steganalysis of LSB matching steganography in color images at the LSBP hiding ratios of 0.75 (I) and 0.5 (II). X-label gives the False Positive (FP) and y-label gives the False Negative (FN). The shape parameter, β, at the bottom of each figure indicates the range of the image complexity under the experiment.

than 0.25, the performances are not good. This shows that the steganalysis of LSB matching steganography in grayscale images is still very challenging in cases with high image complexity or low information-hiding ratios.

Fig. 8 gives the Receiver Operating Characteristic (ROC) curves under different levels of image complexity in color images. To save page space, we only list the ROC curves with the LSBP hiding ratios of 0.75 and 0.5. Fig. 8 shows that CF outperforms HCFCOM and HOMMS. The detection performance depends not only on the information-hiding ratio, but also on the parameter of image complexity. As information-hiding ratio decreases and image complexity increases, the detection performance decreases.



(a) A color sample

(b) the grayscale converted from (a)

(c) Joint probability of red-green channel, max-value: 0.012

(d) Joint probability of adjacent pixels in horizontal direction, max-value: 0.0011

(e) Joint probability of red-blue channel, max-value: 0.0030

(f) Joint probability of adjacent pixels in vertical direction, max-value: 9.7e-004

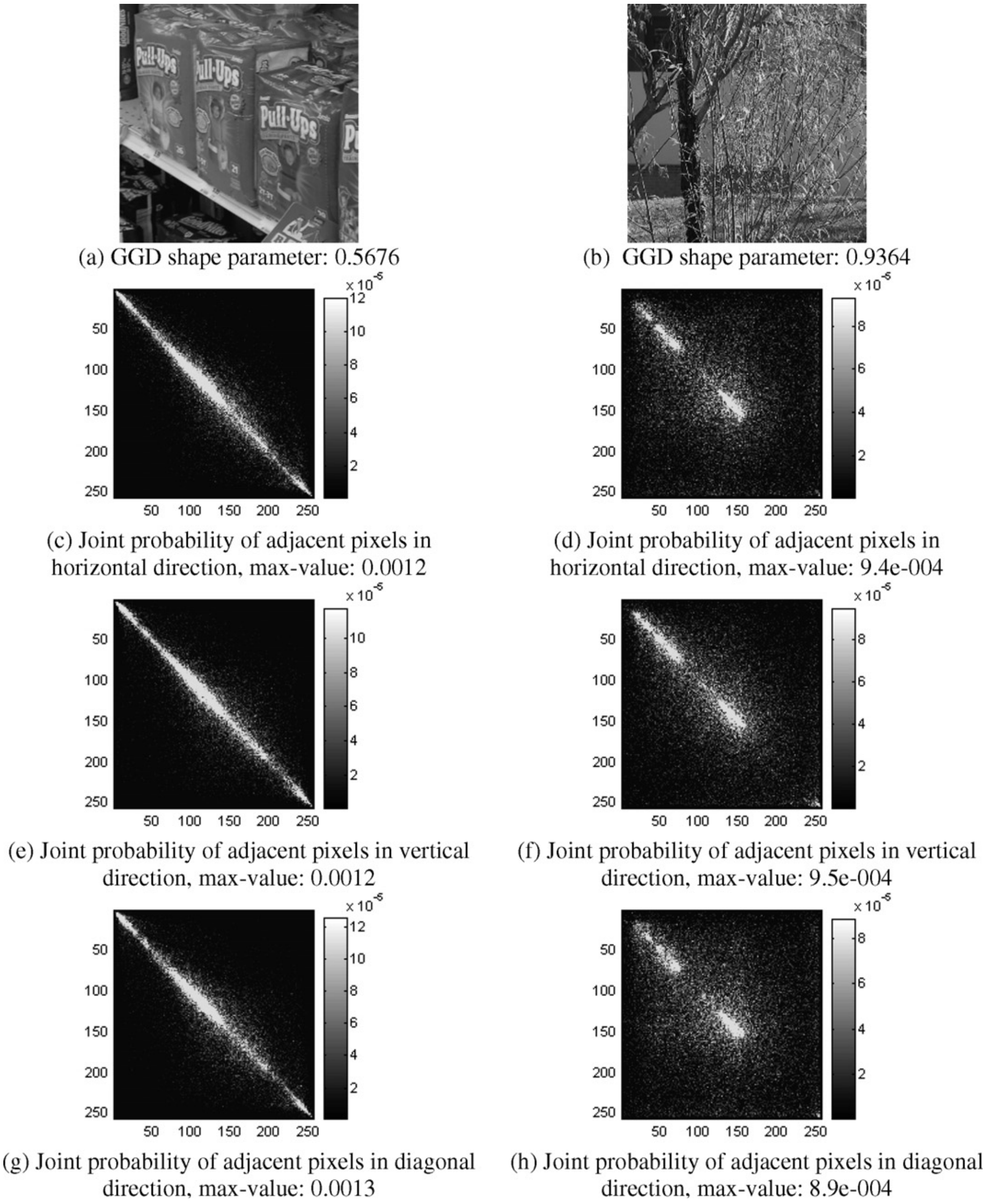
(g) Joint probability of blue-green channel, max-value: 0.0091

(h) Joint probability of adjacent pixels in diagonal direction, max-value: 6.7e-004

Fig. 9. Comparison of correlation in color and correlation in grayscale. Left column is a color sample and the correlations of the inter-channels; the right column is the grayscale sample converted from (a) and the correlation of the adjacent pixels. This indicates that the correlation information on inter-channel is higher than that on intra-channel by comparing the joint probabilities in the left column to the joint probabilities in the right column.

5. Discussions

All experiments show that the classification performances in color images are better than grayscale images. Fig. 4 illustrates that the statistical significance of the most inter-channel correlation features are higher than those of the most intra-channel correlation features, meaning that there are strong correlations across the color channels. This is why the detection in color images is better than that in grayscale images. To clearly explain the detection difference in color images and grayscale images, Fig. 9a shows a color image and



(a) GGD shape parameter: 0.5676

(b) GGD shape parameter: 0.9364

(c) Joint probability of adjacent pixels in horizontal direction, max-value: 0.0012

(d) Joint probability of adjacent pixels in horizontal direction, max-value: 9.4e-004

(e) Joint probability of adjacent pixels in vertical direction, max-value: 0.0012

(f) Joint probability of adjacent pixels in vertical direction, max-value: 9.5e-004

(g) Joint probability of adjacent pixels in diagonal direction, max-value: 0.0013

(h) Joint probability of adjacent pixels in diagonal direction, max-value: 8.9e-004

Fig. 10. Comparison of correlations of low complexity and high complexity grayscales. The left column is a grayscale sample with low complexity and the correlations of the adjacent pixels. The right column is the grayscale sample with high complexity and the correlation of the adjacent pixels. This indicates that the correlation information of the image with low complexity is higher than that of the image with high complexity.

Fig. 9b is the converted grayscale. Fig. 9c, e, and g are the joint probability of the red-green, red-blue, and green-blue channels of the color image. Fig. 9d, f, and h are the joint probability of the adjacent pixels in the horizontal, vertical, and diagonal directions of the grayscale image. The joint distribution of the grayscale is more sparse, and the joint distribution of the color is more concentrated. The maximum values of the joint probability of the color are 0.012, 0.0030, and 0.0091, respectively, which are bigger than the maximum values of the grayscale, 0.0011, 0.00097, and 0.00067. This indicates that the inter-channel correlation features are more significant than the intra-channel correlation features.

As the image complexity increases, the variation of the adjacent pixels increases, and the correlation decreases. Fig. 10 shows two grayscale images with low image complexity (Fig. 10a) and high image complexity (Fig. 10b). Fig. 10c, e, and g give the joint distribution of the adjacent pixels of Fig. 10a. Fig. 10d, f, and h give the joint distribution of the adjacent pixels of Fig. 10b. These clearly indicate that the correlation information at the adjacent pixels of Fig. 10a is stronger than that of Fig. 10b. With the increase in image complexity, the variation of the adjacent pixels increases. As a result, the detection performance and the statistical significance of the features decrease. This strongly implies that the statistical significance of the features closely depend not only on the hiding ratio, but also on the image complexity.

6. Conclusions and future work

In steganalysis, the information-hiding ratio is a well-known reference for evaluating steganalysis performance. However, few publications clearly mention the relevance of image complexity and detection performance. In this paper, we introduce a parameter of image complexity and adopt the shape parameter of Generalized Gaussian Distribution (GGD) in the wavelet domain to measure the image complexity. To detect the presence of hidden data in LSB matching steganography, we present different correlation features. Comparing against other well-known features of HCFCOM and HOMMS in color images, and HCFHOM, HOMMS, A.HCFCOM, and C.A.HCFCOM in grayscale images, our feature set performs the best overall. Our experiments show that the statistical significance of features and the detection performance closely depend, not only on the information-hiding ratio, but also on the image complexity. While the hiding ratio decreases and the image complexity increases, the significance and detection performance decrease. Meanwhile, the steganalysis of LSB matching steganography in grayscale images is still very challenging in the case of complicated textures or low hiding ratios.

Feature selection is a general problem. We did not optimize the feature set. In bioinformatics research, there are some feature selections, such as Support Vector Machine Recursive Feature Elimination (SVMRFE) [14], leave-one-out calculation sequential forward selection (LOOCSFS) [43], gradient based leave-one-out gene selection (GLGS) [43], and recursive feature addition, based on supervised learning and similarity measures [23]. The optimization of the feature set and the improvement of detection in grayscale images are our tasks in the future.

Acknowledgements

Partial support for this research was received from ICASA (Institute for Complex Additive Systems Analysis, a division of New Mexico Tech). A DoD IASP Capacity Building grant and an NSF SFS Capacity Building grant are gratefully acknowledged.

The authors acknowledge Farid, Lyu, Simoncelli and Harmsen for offering us their codes. We thank the reviewers for their insightful comments and helpful suggestions. Professor Pedrycz's very good comments and corrections are gratefully appreciated as well as his precious time!

References

[1] R. Agostino, L. Sullivan, A. Beiser, Introductory Applied Biostatistics, Brooks Cole, 2005.

[2] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, IEEE Trans. Image Process. 12 (2) (2003) 221–229.

[3] M. Choubassi, P. Moulin, A new sensitivity analysis attack, in: E. Delp III, P. Wong (Eds.), Security, Steganography, and Watermarking of Multimedia Contents, VII, in: Proceedings of SPIE-IS&T Electronic Imaging, SPIE vol. 5681, 2005, pp. 734–745.

[4] I. Cox, M. Miller, J. Bloom, Digital Watermarking, Morgan Kaufman, 2001.

[5] R. Duda, P. Hart, D. Stork, Pattern Classification, second ed., John Wiley and Sons, New York, 2001.

[6] S. Dumitrescu, X. Wu, Z. Wang, Detection of LSB steganography via sample pair analysis, in: F.A.P. Petitcolas (Ed.), Information Hiding, Fifth International Workshop, Lecture Notes in Computer Science, vol. 2578, Springer-Verlag, New York, 2002, pp. 355–372.

[7] J. Fridrich, M. Goljan, Digital image steganography using stochastic modulation, in: E. Delp (Ed.), Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V 5020, 2003, pp. 191–202.

[8] J. Fridrich, M. Goljan, D. Hogea, Steganalysis of JPEG Images: breaking the F5 algorithm, in: F.A.P. Petitcolas (Ed.), Information Hiding, Lecture Notes in Computer Science, vol. 2578, Springer-Verlag, New York, 2002, pp. 310–323.

[9] J. Fridrich, M. Goljan, D. Hogea, D. Soukal, Quantitative steganalysis: estimating secret message length, ACM Multimedia Systems Journal 9 (3) (2003) 288–302 (Special Issue on Multimedia Security).

[10] J. Fridrich, D. Soukal, M. Goljan, Maximum likelihood estimation of length of secret message embedding using ±K steganography in spatial domain, security, steganography, and watermarking of multimedia contents, VII, in: Proceedings of SPIE-IS &T Electronic Imaging, SPIE vol. 5681, 2005, pp. 595–606.

[11] J. Friedman, T. Hastie, R. Tibshirani, Additive logistic regression: a statistical view of boosting, The Annals of Statistics 38 (2) (2000) 337–374.

[12] H. Guo, Y. Li, A. Liu, S. Jajodia, A fragile watermarking scheme for detecting malicious modifications of database relations, Information Sciences 176 (10) (2006) 1350–1378.

[13] H. Guo, Y. Li, S. Jajodia, Chaining watermarks for detecting malicious modifications to streaming data, Information Sciences 177 (1) (2007) 281–298.

[14] I. Guyon, J. Weston, S. Barnhill, V. Vapnik, Gene selection for cancer classification using support vector machines, Machine Learning 46 (1–3) (2002) 389–422.

[15] J. Harmsen, W. Pearlman, Steganalysis of additive noise modelable information-hiding, in: E. Delp III, P. Wong (Eds.), Security, Steganography, and Watermarking of Multimedia Contents V, Proceedings of the SPIE, vol. 5020, 2003, pp. 131–142.

[16] F. Heijden, R. Duin, D. Ridder, D. Tax, Classification, Parameter Estimation and State Estimation, John Wiley, 2004.

[17] T. Holotyak, J. Fridrich, S. Voloshynovskiy, Blind statistical steganalysis of additive steganography using wavelet higher order statistics, in: Proceedings of the Ninth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, 2005, pp. 273–274.

[18] J. Huang, D. Mumford, Statistics of natural images and models, 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'99) – vol. 1, 1999, doi:10.1109/CVPR.1999.786990.

[19] S. Katzenbeisser, F. Petitcolas, Information Hiding Techniques for steganography and Digital Watermarking, Artech House Books, 2000.

[20] A. Ker, Improved detection of LSB steganography in grayscale images, in: Fridrich (Ed.), Information Hiding, Sixth International Workshop, Lecture Notes in Computer Science, vol. 3200, Springer-Verlag, New York, 2005, pp. 97–115.

[21] A. Ker, Steganalysis of LSB matching in grayscale images, IEEE Signal Processing Letters 12 (6) (2005) 441–444.

[22] C. Kurak, J. McHugh, A cautionary note on image downgrading, in: Proceedings of the 8th Computer Security Application Conference, 1992, pp. 153–159.

[23] Q. Liu, A. Sung, Recursive feature addition for gene selection, in: Proceedings of 19th International Joint Conference on Neural Networks, 2006, pp. 2339–2346.

[24] Q. Liu, A. Sung, J. Xu, B.M. Ribeiro, Image complexity and feature extraction for steganalysis of LSB matching steganography, in: Proceedings of 18th International Conference on Pattern Recognition, vol. 2, 2006, pp. 267–270.

[25] Q. Liu, A. Sung, B. Ribeiro, in: B. Ribeiro et al. (Eds.), Statistical Correlations and Machine Learning for Steganalysis, Adaptive and Natural Computing Algorithms, Springer, Wien/NewYork, 2005, pp. 437–440.

[26] Q. Liu, A. Sung, J. Xu, V. Venkataramana, Detect JPEG steganography using polynomial fitting, in: Proceedings of the 16th artificial neural networks in engineering, 2006, pp. 547–556.

[27] S. Lyu, H. Farid, Steganalysis using color wavelet statistics and one-class support vector machines, in: SPIE Symposium on Electronic Imaging, San Jose, CA, 2004.

[28] S. Lyu, H. Farid, How realistic is photorealistic, IEEE Transactions on Signal Processing 53 (2) (2005) 845–850.

[29] S. Mallat, A Wavelet Tour of Signal Processing, Academic, San Diego, CA, 1998.

[30] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Transactions on Image Processing 8 (8) (1999) 1075–1083.

[31] H. Motulsky, Intuitive Biostatistics, Oxford University Press, 1995.

[32] P. Moulin, A. Briassouli, A stochastic QIM algorithm for robust, undetectable image watermarking, in: Proceedings of ICIP 2004, vol. 2, 2004, pp. 1173–1176.

[33] P. Moulin, J. Liu, Analysis of multiresolution image denoising schemes using generalized Gaussian and complexity priors, IEEE Transactions on Information Theory 45 (1999) 909–919.

[34] T. Pevny, J. Fridrich, Multiclass blind steganalysis for JPEG images, in: Proceedings of the SPIE Electronic Imaging Security, Steganography, and Watermarking of Multimedia Contents, vol. VIII, 2006, San Jose, CA, pp. 257–269.

[35] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security & Privacy 1 (3) (2003) 32–44.

[36] M. Ramkumar, A. Akansu, A. Alatan, A. Robust, Data hiding scheme for digital images using DFT, in: Proceedings of IEEE ICIP, vol. II, 1999, pp. 211–215.

[37] A. Rencher, Methods of Multivariate Analysis, John Wiley, New York, 1995.

[38] R. Schapire, Y. Singer, Improved boosting algorithms using confidence-rated predictions, Machine Learning 37 (3) (1999) 297–336.

[39] M. Schlesinger, V. Hlavac, Ten Lectures on Statistical and Structural Pattern Recognition, Kluwer Academic Publishers, 2002.

[40] K. Sharifi, A. Leon-Garcia, Estimation of shape parameter for generalized gaussian distributions in subband decompositions of video, IEEE Transactions Circuits on System and Video Technology 5 (1995) 52–56.

[41] T. Sharp, An implementation of key-based digital signal steganography, in: I. Moskowitz (Ed.), Information Hiding. Fourth International Workshop, Lecture Notes in Computer Science, vol. 2137, Springer-Verlag, New York, 2001, pp. 13–26.

[42] A. Srivastava, A. Lee, E. P Simoncelli, S. Zhu, On advances in statistical modeling of natural images, Journal of Mathematical Imaging and Vision 18 (1) (2003) 17–33.

[43] E.K. Tang, P.N. Suganthan, X. Yao, Gene selection algorithms for microarray data based on least square support vector machine, BMC Bioinformatics 7 (95) (2006), doi:10.1186/1471-2105-7-95.

[44] J. Taylor, N. Cristianini, Kernel Methods for Pattern Analysis, Cambridge University Press, 2004.

[45] V. Vapnik, Statistical Learning Theory, John Wiley, 1998.

[46] M. Wainwright, E. Simoncelli, in: S. Solla, T. Leen, K. Müller (Eds.), Scale Mixtures of Gaussians and the Statistics of Natural Images, vol. 12, MIT Press, Cambridge, MA, 2000, pp. 855–861.

[47] A. Webb, Statistical Pattern Recognition, John Wiley & Sons, New York, 2002.

[48] A. Westfeld, High capacity despite better steganalysis (F5–A Steganographic Algorithm), in: Proceedings of the Fourth Information Hiding Workshop, Lecture Notes in Computer Science, vol. 2137, 2001, pp. 289–302.

[49] G. Winkler, Image Analysis, Random Fields and Dynamic Monte Carlo Methods, Springer-Verlag, New York, 1996.

[50] G. Wouwer, P. Scheunders, D. Dyck, Statistical texture characterization from discrete wavelet representations, IEEE Transactions on Image Processing 8 (4) (1999) 592–598.

[51] J. Xu, A. Sung, P. Shi, Q. Liu, JPEG compression immune steganography using wavelet transform, in: International Conference on Information Technology: Coding and Computing, 2004. Proceedings (ITCC 2004), vol. 2, 2004, pp. 704–708.

[52] T. Zhang, X. Ping, A fast and effective steganalytic technique against JSteg-like algorithms, Proceedings of the 8th ACM Symposium on Applied Computing, ACM Press, 2003.