STEGANALYSIS AWARE STEGANOGRAPHY: STATISTICAL INDISTINGUISHABILITY DESPITE HIGH DISTORTION

Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, and Mark F. Bocko

ECE Department, University of Rochester, Rochester, NY, 14627

ABSTRACT

We consider the interplay between steganographer and the steganalyzer, and develop a steganalysis aware framework for steganography. The problem of determining a stego image is posed as a feasibility problem subject to constraint of data communication, imperceptibility, and statistical indistinguishability with respect to steganalyzer's features. A stego image is then determined using set theoretic feasible point estimation methods. The proposed framework is applied effectively on a state of the art steganalysis method based on higher order statistics (HOS) steganalysis. We first show that the steganographer can significantly reduce the classification performance of the steganalyzer by employing a statistical constraint during embedding, although the image is highly distorted. Then we show that steganalyzer can develop a counter-strategy against steganographer's action, gaining back some classification performance. This interchange represents an empirical iteration in this game between the steganographer and steganalyzer. Finally we consider mixture strategies to find the Nash equilibrium of the interplay.

Keywords: Adaptive Steganography, Steganalysis, Steganalysis Aware Steganography, Game between steganographer and steganalyzer

1. INTRODUCTION

The purpose of covert communication, or steganography, is to hide both presence of communication and the secret message itself. The desire for creating innocuous looking *stego objects* dates back to the early stages of human history. Today, proliferation of digital signal processing, advances in multimedia technology and the wide spread use of the Internet switched the secret communication channels from "slowly moving and hard to change" physical media to "lightning-fast propagating and easy to alter" digital multimedia. In digital steganography, the steganographer aims to create a secret private channel inside a publicly or semi-publicly accessible digital communication channel. Steganographer's endeavors are intended to be blocked by a steganalyzer, who seeks for statistical and visual evidence of alteration in transmitted multimedia. The steganalyzer and steganographer can both pick different strategies to advance their objectives against each other's strategies.

The conventional story elucidating steganographic communication takes place in a prison [1]. Alice, the prisoner, wants to share her escape plans with Bob, her potential associate in this escape plan. Alice is allowed to communicate with Bob, however as a security measure, Wendy the warden monitors all outgoing communication traffic. Wendy either blocks or alters the communication when she finds evidence of a secret communication. Based on the type of her actions, she is typified either as passive or active warden respectively. We focus on the "passive warden" scenario where the steganalyzer's goal is to classify each received image into one of two classes corresponding to benign images (with no embedding) or stego images (with embedding).

Steganographer's problem and the dynamics between steganographer and steganalyzer has been formulated and analyzed in many different settings. There are several neat examples of information theoretic [2], game

Further author information: (Send correspondence to A. Orsdemir)
A. Orsdemir: E-mail: orsdemir@ece.rochester.edu, Telephone: 1 585 275 8122
H. O. Altun: E-mail:altun@ece.rochester.edu, Telephone: 1 585 2752390
G. Sharma: E-mail: gsharma@ece.rochester.edu, Telephone: 1 585 275 7313
M.F. Bocko: E-mail: bocko@ece.rochester.edu, Telephone: 1 585 275 40 66
This work is supported by the Air Force Office of Scientific Research (AFOSR) under grant number FA9550-07-1-0017.

Security, Forensics, Steganography, and Watermarking of Multimedia Contents X
edited by Edward J. Delp III, Ping Wah Wong, Jana Dittmann, Nasir D. Memon
Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6819, 681915, © 2008 SPIE-IS&T · 0277-786X/08/$18

theoretic [3] and communication theoretic approaches. In this paper, we examine the steganographic data hiding problem from an alternate perspective. We formulate the problem as a feasibility problem and analyze the empirical results from a game theoretic perspective.

In our development, we consider the higher order statistics (HOS) steganalysis method [4]. We first show that the steganographer can significantly reduce the classification performance of the steganalyzer by employing a statistical indistinguishability constraint during embedding along with other data hiding requirements. The steganalyzer relies on the statistical difference between stego image and original image. If these statistics are kept intact during embedding, the performance of the steganalyzer can be reduced significantly. We show practical application of this idea in a set theoretic framework and obtain a stego-design that meets all constraints along with statistical indistinguishability at the same time.

We then show that steganalyzer can develop a counter-strategy against steganographer's action, gaining back some classification performance.The steganalyzer can take into account of the fact that the steganographer creates stego images by employing the statistical indistinguishability set. A novel aspect of the proposed framework is that the receiver (Bob in the traditional scenario) does not need to be completely aware of the complete set of constraints used by the steganographer (Alice). This allows the steganographer to dynamically change constraints (other than the detection constraints) to stymie steganalysis. We consider several such scenarios. We refer to the steganographer as sophisticated if he incorporates constraints based on statistical indistinguishability in the embedding process and naive otherwise. Similarly we refer to the steganalyzer as sophisticated if he assumes that statistical indistinguishability constraints are used in the embedding and naive otherwise. Then we consider mixture strategies that randomly choose to include/disregard the statistical indistinguishability constraints. These options lead them to a game of picking either naive or sophisticated strategy in the game. Finally mixed strategy Nash equilibrium is determined solving a minmax problem for both agents.We observed that there does not exist any Nash equilibrium in the empirical payoff tables. The game theoretic equilibrium for mixed strategies is illustrated in the practical framework we have developed.

2. A FEASIBILITY FORMULATION OF STEGANALYSIS AWARE STEGANOGRAPHY

A steganographer, aware of being monitored by a passive warden, has to fulfill several challenging and possibly competing requirements to generate a successful stego image. First of all, the stego image should be indistinguishable to the steganalyzer's statistical detector. However, mark embedding without proper adjustment would most likely disrupt the statistical properties of the image, giving the steganalyzer a chance to distinguish those with the mark from the original cover images. Second, the image should look perceptually similar to the original image. A visually distorted stego image will immediately catch attention of a steganalyzer examining the image with his bare eyes. This will defeat the purpose of steganography. And finally, the correct message should be decodable at the receiver side. Inserting a message that interferes partially or totally with the cover fails the mission of steganography as well.

The steganographer in a passive warden scenario intends to find an image that satisfies all three requirements simultaneously. The problem of a steganographer being monitored by a steganalyzer can be formulated as a feasibility problem. In the following sections, we will give the details of this formulation and illustrate the effectiveness of the method.

2.1 Formulating the steganographic requirements:

In this section we introduce the requirements for steganography in images. For visual quality and detectability we utilize our prior work on set theoretic watermarking [5, 6].

2.1.1 Presence of a HOS Steganalyzer and Formulation of Statistical Indistinguishability Requirement:

Steganalysis techniques usually assume that, hiding information into natural images disrupt the statistics of the image. A successful steganalysis method exploits this fact and trains a classifier that distinguishes stego image statistics from natural image statistics. One of the state of the art steganalysis method is steganalysis with

HOS [4]. HOS steganalysis has two main steps: extracting a feature vector consisting statistics from the sample image and classification based on this feature vector.

In the feature vector extraction step, the HOS steganalyzer decomposes inspected image into two dimensional multi-scale wavelet domain representation. The image is decomposed into vertical, horizontal, diagonal and approximation subbands. The low pass approximation subband is decomposed further into upper scales, indicated by subscript i where $i = 1, .., n$. These multiscale subbands are represented by $\mathbf{v_i}(\mathbf{x})$, $\mathbf{h_i}(\mathbf{x})$, $\mathbf{d_i}(\mathbf{x})$ and $\mathbf{a_i}(\mathbf{x})$ respectively throughout the paper, where the subbands are represented as a function of the image ($\mathbf{x}$) in spatial domain. The feature vectors are then estimated by using mean, variance, skewness and kurtosis of each of these subbands. Additionally, a linear predictor is employed to estimate each of the coefficients at each subband from their neighboring coefficients. The statistics of the error between observed coefficients and estimated coefficients are calculated to complete the feature vector.

As a second step, support vector machines (SVM) can be employed for classification purpose. Steganalyzer choses a training set of images. Data is hidden into these images. Feature vectors are extracted for both of the cover and stego images and the classifier is trained. The feature vector pertaining to inspected image is then fed into a classifier.

In the presence of a HOS steganalyzer, the steganographer must generate stego images whose statistical features resemble those of natural images. Otherwise, steganographer's mission of rendering the very presence of steganography fails. One way to ensure this statistical indistinguishability is to formulate constraints on the stego images. *In particular, we can see that a steganalyzer based on a given set of statistics cannot distinguish between the classes of cover and stego images, if the steganographic embedding process preserves the statistics of the cover image that are used by the steganalyzer.* For some statistics, e.g. variance, exact preservation may not be necessary and it may be acceptable if the statistics of the stego image are bounded by those of the cover. Accordingly, we formulate indistinguishability of the stego image from cover images as follows:

$$\mathbb{S}_1^{i,stat,\phi} \equiv \{\mathbf{x} : stat(\phi_\mathbf{i}(\mathbf{x})) \leq stat(\phi_\mathbf{i}(\mathbf{x_o}))\} \quad i = 1, .., n, \qquad \phi = \mathbf{v_i}(\mathbf{x}), \mathbf{h_i}(\mathbf{x}), \mathbf{d_i}(\mathbf{x}) \tag{1}$$

where $\mathbf{x_o}$ represents the original image, $\mathbf{x}$ represents a candidate watermarked image and *stat* represents first and HOS for the normalized moments: mean, variance, skewness and kurtosis.

2.1.2 Visual Quality Requirements

We employ a spatial masking model proposed by Pereira et al [7] in order to ensure the visual fidelity of the stego image to the original image. This model exploits the fact that noise in textured areas are less visible than noise in smooth areas in the image. This model assigns pixel-wise upper and lower bounds to the each pixel. This is the upper and lower bound of the allowed perturbation. The model assumes that the noise within this interval is invisible. We can formulate this constraint as [5]

$$\mathbb{S}_2 \equiv \{\mathbf{x} : \mathbf{l} \leq \mathbf{x} - \mathbf{x_0} \leq \mathbf{u}\} \tag{2}$$

where $\mathbf{u}$ and $\mathbf{l}$ form pixel-wise upper and lower bounds respectively. These values are provided by the texture masking model as a function of the original cover image.

2.1.3 Detectability Requirements

We use a quantization index modulation (QIM) [8] based embedding strategy in which each bit is embedded by using a scalar quantizers on the mean of L randomly selected pixels [6]. If we denote the randomly selected pixels with a $L \times 1$ vector $\mathbf{y}_0$, the mean of these values is $\mu_i = \frac{1}{L}\mathbf{1}^T\mathbf{y}_0$ where $\mathbf{1}$ is a $L \times 1$ vector of 1's. Let's represent Q as the integer scalar quantizer with Δ as scaling parameter, then if we want to embed a bit value b, assuming $b \in \{-1, 1\}$, the mean of these values must be

$$\frac{1}{L}1^T\mathbf{y} = Q(\mu_i - b_i\frac{\Delta}{2}, \Delta) + b_i\frac{\Delta}{2} \equiv \mu_i^{q,b} \tag{3}$$

The detectability set can then be given as [5]:

$$\mathbb{S}_2^i \equiv \{\mathbf{x} : \frac{1}{L} 1^T \mathbf{y}_i = \mu_i^{q,b_i}\} \quad i = 1, .., M \tag{4}$$

where M denotes the number of embedded bits with values $\{b_i\}_{i=1}^N$, $\mathbf{y}_i$ denotes the $L \times 1$ sample vector for i'th bit value. Note that the randomly selected locations for different bits may be overlapping. Receiver is aware of the quantization intervals of different bit values so that he can correctly identify the bit value transmitted. This set is the only requirement for identification of message bits.

2.2 Generating An Image Satisfying All Requirements:

We formulated the desired properties of the stego image as *constraint sets*. Now we want to determine the image which satisfies these requirements. The stego image can be obtained using an iterative algorithm that determines a point in the intersection of all the constraint sets. When the sets are convex the method of POCS provides a converging algorithm for this purpose. Given n convex sets $\{S_i\}_{i=1}^n$ the POCS method determines a point in their intersection by successive projections. If the intersection of all the sets is non-empty, the sequence of images $\{f_k\}_{k=0}^\infty$ generated by POCS converges to a point in the intersection, where

$$f_{k+1} = (P_{S_n}(P_{S_{n-1}}...P_{S_1}(f_k)...)), k = 0, 1, .. \tag{5}$$

P_{S_i} is the projection operator onto set S_i defined as $P_{S_i}(x) = arg\ min_{y \in S_i} \|y - x\|$.

The detectability and visual quality requirements are inherently convex [6]. The statistical indistinguishability requirements however are not convex due to the normalized moments. We approximated these sets by convex sets, where we assume the normalizing coefficients (powers of standard deviations in the denominators of the moments) do not change during the iteration. In each iteration we keep the standard deviation same with the original value by projections. This approximation works quite well and the algorithm yields a stego image simultaneously satisfying all constraints. Note that detectibility constraint is needed for communication between the sender and receiver, but for the other constraints sender can decide to incorporate or not without impacting the detectibility.

2.3 Experimental Results:

We performed a set of experiments to test the effectiveness of the statistical indistinguishability set we propose in this framework. We used the images from Kodak's ftp site [9]. It consists of 108 uncompressed* images in Kodak PhotoCD format each having a size of 512×768. The images were converted to grayscale images for our experiments by first decoding the PhotoCD format to RGB TIFF format and then utilizing Matlab's *rgb2gray* function. Stego data is embedded in the images using set theoretic framework. We used a spreading rate of $L = 2000$ pixels/bit. The pixels are selected at random controlled by a pseudo-random key, available for both detector and receiver side.

Experiments indicated that the variance and kurtosis for the wavelet decomposition of the stego images at different scales were the primary contributers to the HOS based steganalyzer's accuracy. We therefore employed a constraint set in the watermark embedding process that constrained these statistics in the stego images to lie below their values in the cover images.

For steganalysis classification purposes we employed a Lagrangian support vector machine (l-SVM) [10, 11] classifier. We inserted data into images in the database with various embedding rates. Half of the stego images in the database along with the corresponding original cover images were used for training the classifier. The other half of the images in the database and the corresponding stego images were used for testing the steganalyzer's performance.

We tested the effectiveness of the statistical indistinguishability set by designing two experiments. In one of these experiments, we only incorporate invisibility and detectability sets but exclude statistical indistinguishability set. Table 1 summarizes the performance of the classifier when the statistical indistinguishability set is

*Apart from chroma downsampling

included. The first row of the table shows the performance of the classifier on the training data set after the training process. The classification results are given as success rate percentage values. As expected, as we increase the embedding rate, the distortion on the cover image increases, giving better training performance for the classifier. The second row of the table shows the test results of the classifier. The results are slightly worse than the training results as one naturally would expect. The third and forth row of this table distinguishes between false positive (F.P.) and false negative (F.N.) values of the testing results of the classifier. The last row shows the average PSNR of the watermarked image with respect to the original image over 108 images. $PSNR = 10 \cdot \log(225^2/(MSE))$ where MSE stands for the average mean square error between the original and stego image.

In the second set of experiments, we included the statistical indistinguishability set to generate the watermarked images. Table 2 summarizes the performance of the classifier when the statistical indistinguishability set is included. Compared to Table 1, we see a drastic decrease in the test performance of the classifier. The performance is almost random for all embedding rates. And the most significant contribution to classification error comes due to the false negative errors. This indicates that classifier can't distinguish the watermarked images from the original and misclassifies them as originals. Note that the steganalyzer classifier in this scenario was trained on stego images generated without the statistical indistinguishability constraints.

The average PSNR values at Table 2 show the effect of including statistical indistinguishability on the generated image. The statistical indistinguishability set increases the $PSNR$ of the image between $0.5 - 1$ dB in average. This extra distortion is the cost on steganographer for being indistinguishable to the steganalyzer's statistical detector.

In comparison with other steganographic embedding methods, the PSNR values in tables 1 and 2 are relatively high for the corresponding embedding rates. This makes the poor steganalysis performance in Table 2 even more remarkable.

	Embedding Rate (bits)				
	2000	**3000**	**4000**	**5000**	**6000**
Train. Perf.	89.81 %	95.37 %	98.15 %	99.14 %	100.00 %
Test Perf.	71.30 %	78.70 %	85.19 %	89.81 %	91.67 %
F.P.	25.93 %	16.67%	11.11 %	09.26 %	05.56 %
F.N.	31.48 %	25.93 %	18.52 %	11.11 %	11.11 %
Av. PSNR	40.17 dB	38.20 dB	36.68 dB	35.78 dB	34.87 dB

Table 1. Training and testing performance of steganalyzer's SVM classifier, when steganographer does not apply statistical indistinguishability set.

	Embedding Rate (bits)				
	2000	**3000**	**4000**	**5000**	**6000**
Train. Perf.	89.81 %	95.37 %	98.15 %	99.14 %	100.00 %
Test Perf.	50.00 %	50.93 %	50.93 %	50.00 %	50.93 %
F.P.	25.93 %	16.67%	11.11 %	09.26 %	05.56 %
F.N.	74.07 %	81.78 %	87.04 %	90.74 %	92.59 %
Av. PSNR	39.03 dB	37.27dB	36.19 dB	34.98 dB	34.04 dB

Table 2. Training and testing performance of steganalyzer's SVM classifier, when steganographer applies statistical indistinguishability set.

3. GAME BETWEEN STEGANOGRAPHER AND STEGANALYZER

The feasibility formulation of data hiding brings an interesting dynamics between steganographer and steganalyzer. Each agent can view the opponent agent's strategy in a naive way or in a sophisticated way. We identify these agents either naive steganographer/steganalyzer or sophisticated steganographer/steganalyzer. The fundamental difference between naive and sophisticated approach is the way that each agent formulates his own problem.

Naive steganographer would not consider the fact that steganalyzer is exploiting the statistical difference between stego and original image. In simpler terms, he employs only invisibility and detectability sets. On the other hand, a sophisticated steganographer views the problem in a different point of view: he is aware of the fact that, he can do better by employing a statistical indistinguishability set while embedding information.

Steganalyst's problem mirrors steganographer's formulation. In the proposed framework in Section 2, steganalyst is a naive agent since he trains his classifier with the stego images generated by only invisibility and detectability sets. He does not consider the fact that steganographer can take a counteraction to depreciate his classification performance. Sophisticated steganalyzer, on the other hand, takes the steganographer's action into account to gain back his performance. In this scenario, he trains his classifier with stego images where they are generated by employing invisibility, detectability and statistical indistinguishability sets. In statistical indistinguishability set only some statistics are preserved. Steganalyzer relies on the other statistics. Feasibility formulation of the framework allows steganographer to change his strategy at will. *We note that the terms naive and sophisticated should be only interpreted in this context as using/not using the statistical indistinguishability constraint and should not be interpreted literally.*

The game between steganographer and steganalyzer can be summarized in a classical payoff matrix listed in Table 3. The payoffs are expressed in terms of steganalyst's classification performance. The game can be identified as a zero-sum game, since they have to share a 100% performance over test images. For naive-naive[†] scenario the performance of the steganalyzer increase with increasing embedding rate. When steganographer chooses to employ the indistinguishability set to create stego images, the performance of the steganalyzer decreases drastically. This was the main result of Section 2.

One interesting scenario is when the steganographer behaves naively while the steganalyst assumes steganographer's complicated action. This scenario also favors steganographer and leaves steganalyst with a performance equivalent to random guessing. When both of them chooses to play sophisticated, the classification performance of the steganalyzer is better than the naive-sophisticated strategies however worse than the naive-naive strategy.

We need a simple game theoretic analysis to read the payoff table and predict each player's strategy. Observing the table, we can tell that the pure strategies does not have a Nash equilibrium. In each strategy in the game, one of the player can do better by deviating from it. In naive-naive scenario, the steganographer can do better by deviating to sophisticated-naive strategy. In sophisticated-naive strategy, steganalyzer is better off by changing to sophisticated-sophisticated strategy. Similar arguments can be observed for the rest of the two options.

Since the Nash equilibrium does not exist among pure strategies, an equilibrium must exist in the mixed strategies [12]. We will examine mixed strategies in section 4.

4. MIXED STRATEGIES

The steganographer can do better in the presence of mixed strategies. The steganalyzer can randomize to choose employment of statistical indistinguishability set while generating the stego images. And correspondingly, the steganalyzer can do the same to generate his training set.

The mixed strategy Nash equilibriums can be calculated by a minmax strategy. We solved this problem for the payoff Table 2(a) for embedding rate 4000. The Nash equilibrium exists when steganalyzer chooses naive strategy with probability $p = 0.38$ and sophisticated strategy with $1 - p = 0.62$, and steganographer chooses naive strategy with probability $q = 0.37$ and sophisticated strategy with $1 - q = 0.63$. This Nash equilibrium correponds to the situation where steganographer alternates between generating the stego image

[†]In A-B notation, A stands for steganographer's strategy and B stands for steganalyzer's strategy.

(a) E.R.=2000

E.R.=2000		Steganographer	
		Naïve	Sophisticated
Steganalyzer	Naive	71.3 %	50 %
	Sophisticated	51.85 %	64.81 %

(b) E.R.=3000

E.R.=3000		Steganographer	
		Naïve	Sophisticated
Steganalyzer	Naive	78.70 %	50.93 %
	Sophisticated	54.62 %	66.67 %

(c) E.R.=4000

E.R.=4000		Steganographer	
		Naïve	Sophisticated
Steganalyzer	Naive	85.19 %	50.93 %
	Sophisticated	50.00 %	71.29 %

(d) E.R.=5000

E.R.=5000		Steganographer	
		Naïve	Sophisticated
Steganalyzer	Naive	89.81 %	50.00 %
	Sophisticated	53.70 %	72.22 %

Table 3. Payoff table for steganographer-steganalysis game for various embedding rates. Payoff values are expressed in terms of steganalyst's classification performance.

by using statistical indistinguishability set with 0.63 probability and not using statistical indistinguishability by 0.37 probability. Similarly, steganalyzer uses the sophisticated classifier with probability 0.62 and naive classifier with probability 0.38. At this point steganalyzer's payoff, which corresponds to expected classification accuracy, is approximately 63%. However in reality steganalyzer would train the classifier by a mixture of stego images instead of switching between different classifiers. For the Nash equilibrium mixture, 62% of the images are obtained by using the statistical indistinguishability set 38% of the images are generated by excluding the statistical indistinguishability set. Using this mixture training dataset we found the empirical classification accuracy as 66%. The empirically obtained payoffs for the case when the steganographer uses a $50-50$ mixture strategy and the steganalyzer trains on a corresponding number of images is shown in Table 4. The numbers indicate that the linearity assumption in the computation of Nash equilibrium does not introduce too much error.

5. CONCLUSION

We consider steganalysis aware steganography that incorporates statistical indistinguishability with respect to the original cover as an embedding requirement. Combining this constraint with prior work in set theoretic watermarking, we obtain a feasibility formulation for steganography in which stego image is obtained by successive projections onto the constraint sets. We demonstrate that, by adding the statistical indistinguishability constraint the steganographer significantly reduces the classification accuracy of steganalyzer. The game between steganographer and steganalyzer reduces to either viewing the problem in a naive or sophisticated way. The empirical payoff table for various embedding rates indicates us that there does not exists a pure strategy Nash equilibrium. However, agents can choose to randomize strategies and obtain a Nash equilibrium.

REFERENCES

1. G. J. Simmons, "The prisoners' problem and the subliminal channel," in *CRYPTO*, pp. 51–67, 1983.
2. P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Transactions on Information Theory* **49**(3), pp. 563–593, 2003.
3. A. D. Ker, "Batch steganography and the threshold game," in *Security, Steganography, and Watermarking of Multimedia Contents IX. Edited by Delp, Edward J., III; Wong, Ping Wah. Proceedings of the SPIE, Volume 6505, pp. 650504 (2007).*, *Presented at the Society of Photo-Optical Instrumentation Engineers (SPIE) Conference* **6505**, Feb. 2007.
4. S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics and Security* **1**(1), pp. 111–119, 2006.
5. O. Altun, G. Sharma, M. Celik, and M. Bocko, "A set theoretic framework for watermarking and its application to semifragile tamper detection," *IEEE Trans. Info. Forensics and Security* **1**, pp. 479–492, Dec. 2006.
6. O. Altun, G. Sharma, and M. Bocko, "Set theoretic quantization index modulation watermarking," in *Proc. IEEE Intl. Conf. Acoustics Speech and Sig. Proc.*, **II**, pp. 229–232, May 2006.
7. S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Third International Workshop on Information Hiding*, pp. 211–236, 1999.
8. B.Chen and G.W.Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory* **47**, pp. 1423–1443, 2001.
9. "Kodak PhotoCD images." ftp://ftp.kodak.com/www/images/pcd.
10. O. Mangasarian and D. R. Musicant, "LSVM Software: active set support vector machine classification software," 2000. www.cs.wisc.edu/∼musicant/lsvm/.
11. O. L. Mangasarian and D. R. Musicant, "Lagrangian support vector machine classification," Tech. Rep. 00-06, Data Mining Institute, Computer Sciences Department, University of Wisconsin, Madison, Wisconsin, June 2000. ftp://ftp.cs.wisc.edu/pub/dmi/tech-reports/00-06.ps.
12. J. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences of the United States of America* **36**, pp. 48–49, 1950.

(a) E.R.=2000

E.R.=2000		Steganographer		
		Naive	Mix	Sophisticated
Steganalyzer	Naive	71.30 %	62.03 %	50.00 %
	Mix	67.59 %	59.26 %	54.63 %
	Sophisticated	51.85 %	59.26 %	64.81 %

(b) E.R.=3000

E.R.=3000		Steganographer		
		Naive	Mix	Sophisticated
Steganalyzer	Naive	78.70 %	65.74 %	50.93 %
	Mix	75.00 %	62.04 %	56.48 %
	Sophisticated	54.62 %	62.96 %	66.67 %

(c) E.R.=4000

E.R.=4000		Steganographer		
		Naive	Mix	Sophisticated
Steganalyzer	Naive	85.19 %	69.44 %	50.93 %
	Mix	79.63 %	64.81 %	54.63 %
	Sophisticated	50.00 %	62.96 %	71.29 %

(d) E.R.=5000

E.R.=5000		Steganographer		
		Naive	Mix	Sophisticated
Steganalyzer	Naive	89.81 %	71.30 %	50.00 %
	Mix	85.19 %	67.59 %	59.33 %
	Sophisticated	53.70 %	63.89 %	72.22 %

Table 4. Payoff table for steganographer-steganalysis game for various embedding rates including uniformly randomized mixed strategy.