

Compressive Sensing Based Secret Signals Recovery for Effective Image Steganalysis in Secure Communications

Huimin Zhao^{1,3}, J.-C. Ren^{2,3}, Jin Zhan¹, Yinyin Xiao¹, Sophia Y. Zhao²,
Fangyuan Lei^{1,3}, Maher Assaad⁴, Chunying Li¹

¹*School of Computer Sciences, Guangdong Polytechnic Normal University (GPNU), Guangzhou, China.*

²*Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, U.K.*

³*The Guangzhou Key Laboratory of Digital Content Processing and Security Technologies, Guangzhou, China*

⁴*College of Engineering, Ajman University, Dubai, UAE*

Zhaohuimin66@yahoo.com; zhaohuimin@gpnu.edu.cn

Abstract —*Conventional image steganalysis mainly focus on presence detection rather than the recovery of the original secret messages that were embedded in the host image. To address this issue, we propose an image steganalysis method featured in the compressive sensing (CS) domain, where block CS measurement matrix senses the transform coefficients of stego-image to reflect the statistical differences between the cover and stego- images. With multi-hypothesis prediction in the CS domain, the reconstruction of hidden signals is achieved efficiently. Extensive experiments have been carried out on five diverse image databases and benchmarked with four typical stegographic algorithms. The comprehensive results have demonstrated the efficacy of the proposed approach as a universal scheme for effective detection of steganography in secure communications whilst it has greatly reduced the numbers of features requested for secret signal reconstruction.*

Keywords: *Compressive Sensing (CS); Image Steganalysis; Secret Signal Recovery; Secure Communication.*

1. Introduction

Aiming to detect the presence of the embedded secret signal (also namely payload) from the host images coming from a known source, steganalysis has been extensively studied in the last decade. In steganography, the media for embedding a message is denoted as *cover*, which can be texts or images. Also it is defined a *stego-object* is the cover with the secret message embedded. Often, the task of steganalysis can be formulated to a binary classification problem to distinguish between the cover and the stego-objects, where we are more interested in recovering the secret message.

In general, existing approaches for steganalysis include two main steps, i.e. feature extraction and classification based decision making [1]. For feature extraction, a set of handcrafted features is often extracted from each image to capture the impacts of embedding operations [2], which usually determines the success of steganalysis. However, this can be complicated due to the lack of accurate models of natural images, which has facilitated various feature-based steganalysis methods. The most reliable feature design paradigm starts with computing a noise residual and then modelling the residual using conditional or joint probability distributions of adjacent elements [2,3,4,5,6]. In [7], Kodovsky et al proposed to use a completing feature set to solve the relation between feature residuals and complementarity in blind steganalysis. However, the completing feature set is unable to work efficiently with some modern steganalysis functions. To boost feature selection, a feature fusion boosting-based algorithm was proposed in Dong et al [8], which shows a higher accuracy with constructed classifier weights for selecting features. However, the algorithm does not consider the relationship synthetically between selected features, which also suffers from high computational cost.

To achieve better sampling of features, compressive sensing (CS) theory has been proposed recently, which has provided an efficient solution for unifying sensing and compressing feature signal by using a simplified linear measurement. Actually, CS can help to reach the best trade-off between the security and robustness as described in [9], [10], [11], [12]. In Wang *et al.* [12], a CS domain scheme is proposed for integrated secure watermark detection and privacy preserving storage of multimedia data. By combining Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) [30], two new CS-based methods are proposed in [13] for the detection of steganographic content.

In this paper, a CS-based steganalysis approach is proposed, which is mainly focused on the recovery of the secret messages. The aim of the selected CS-based feature space is to improve the accuracy of classification between cover or stego so as to further reconstruct/recover the original signal of the hidden messages. The proposed work is applied on images generated from five steganography tools, i.e. nsF5, PQ, Outguess JPHS, HUGO. The features are extracted from DCT and DWT feature vectors using block CS (BCS) measurement matrix in [14], respectively, where the results from BCS are compared with other state-of-the-art approaches for benchmarking.

The remaining paper is structured as follows. In Section 2, the proposed CS-based steganalysis framework is presented, which include feature measurement, measurement matrix design, hidden signal extraction and recovery of secret signal. In Section 3, the experimental results and analysis are reported. Finally, some concluding remarks are drawn in Section 4.

2. The Proposed CS-based Steganalysis Framework

As steganography may cause image content changed imperceptibly, it is expected such changes can be detected by using transform domain coefficients in a fine scale, where CS can play an important role to characterize the changes from the local transform coefficients introduced by the embedded secret messages. Therefore, we aim to BCS to detect DCT or Discrete Wavelet Transform (DWT) steganographic embedding data in images, especially to reconstruct the original secret signal. As illustrated in Figure 1, the proposed framework contains five modules, i.e. CS domain feature extraction, measurement matrix design, hidden signal extraction and recovery of secret signal as well as performance assessment. These are detailed in the next sections.

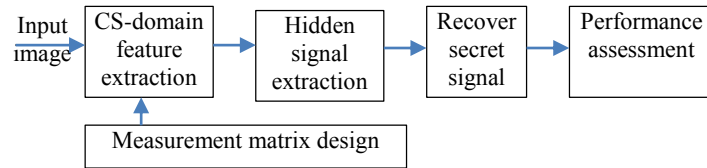


Figure 1. Flowchart of the proposed framework

2.1. The Measurement of the Feature Data in CS Domain

In the proposed framework, for simplicity we assume the total numbers of pixels in the input image X is $N \times N$. The image X is divided into four sub-images denoted by X_1, X_2, X_3 and X_4 , and all the four sub-images are divided into $n_1 \times n_2$ blocks. For the given $N \times N$ image X , the subsampling procedure is given as follows:

$$\begin{cases} X_1(n_1, n_2) = X(2n_1, 2n_2) \\ X_2(n_1, n_2) = X(2n_1 + 1, 2n_2) \\ X_3(n_1, n_2) = X(2n_1, 2n_2 + 1) \\ X_4(n_1, n_2) = X(2n_1 + 1, 2n_2 + 1) \end{cases} \quad (1)$$

where $n_1, n_2 = 1, 2, \dots, \text{INT}[\frac{N}{2}]$.

For each block of the four sub-images, it is transformed by using a sparse basis matrix Ψ_i , which can be DCT or DWT according to the distinction of image types [15], respectively. Accordingly, four blocks of transform coefficients can be formed as $X_i, i=1,2,3,4$. Let $\Phi_{n_1 \times n_2}$ be the blocking measurement matrix of the CS, it can be deployed to sense these coefficients independently within each block. The resulting subsampled measurement Y_i can be decided by

$$Y_i = \Phi_{n_1 \times n_2} \cdot X_i, \quad i = 1, \dots, 4 \quad (2)$$

where the length of the signal Y_i is m , and $\Phi_{n_1 \times n_2}$ is a $n_1 \times n_2$ measurement matrix. Fig. 2 shows sub-sampling process for image signal in CS domain.

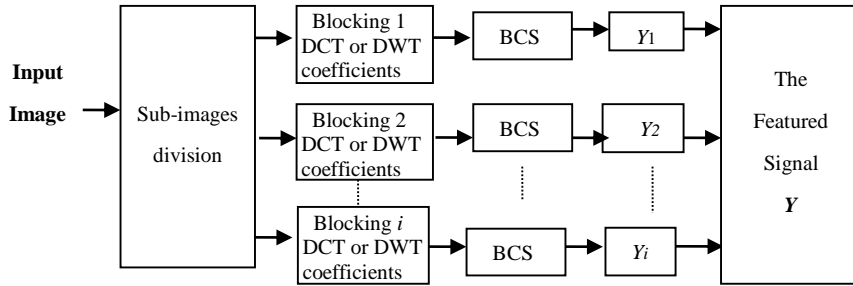


Figure 2. Sub-sampling process of the CS-based feature data

In Fig. 2, for each sub-image block, the number of measurement samples can be determined as $M = \lfloor m \cdot n_1 \times n_2 / N \rfloor$, where M is the size of the feature samples required by the CS measurement for the whole image. In this way, the fusion measurement matrix Φ for the CS has a block-diagonal structure as follows:

$$\Phi = \text{diag}[\Phi_{n_1 \times n_2}] \quad (3)$$

The overall CS-based sub-sampling technique above is called block-CS (BCS) [14]. This process is simply a random linear projection, which can be achieved by the inner product operation of the two corresponding elements between sparse matrix Ψ_i and the measurement matrix $\Phi_{n_1 \times n_2}$. According to the CS theory [15, 16], the selected $\Phi_{n_1 \times n_2}$ can be incoherent with Ψ_i , and this has been formalized into the restricted isometry property (RIP) [15]. Since the sparse basis Ψ_i is a type of DCT or DWT

matrix, the constraint can be solved by designing an appropriate measurement matrix $\Phi_{n_1 \times n_2}$ which will be discussed in a later subsection. Finally, the fused feature signal \mathbf{Y} is generated by combining the sub-sampling values Y_i from the measurement matrix $\Phi_{n_1 \times n_2}$ of each sub-image block. In this case, the signal \mathbf{Y} is as follow:

$$\mathbf{Y} = \sum_{i=1}^{n_1 \times n_2} Y_i = \begin{bmatrix} \Phi_{n_1 \times n_2} & 0 & \cdots & 0 \\ 0 & \Phi_{n_1 \times n_2} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \Phi_{n_1 \times n_2} \end{bmatrix} \begin{bmatrix} X_1(n_1, n_2) \\ X_2(n_1, n_2) \\ \cdots \\ X_i(n_1, n_2) \end{bmatrix} = \begin{bmatrix} Y_1 \\ Y_2 \\ \cdots \\ Y_i \end{bmatrix} \quad (4)$$

When applying BCS to two adjacent sub-images, in total $2m$ measurements Y_k^i are produced, where $k=1,2,3$ or 4 , $1 \leq i \leq m$. As proved in [14], ~96% of the image energy of \mathbf{X} can be preserved in the first 1000 transform coefficients, or ~1.5% of 65536. Here, we choose K_1 coefficients from the transform domain and K_2 coefficients from the sparse domain, provided that $K_1+K_2=M$. We divide measurements Y_k^i into a pair of groups $Y_{k_1}^i$ and $Y_{k_2}^i$, $k_1, k_2 = 1,2,3$, or 4 and denoted as $(Y_{k_1}^i, Y_{k_2}^i)$.

2.2. Designing of the Measurement Matrix

The measurement matrix Φ is a key factor to obtain the CS-feature signal. Cands *et al* have proved that the Gaussian random matrix statistically satisfies the RIP requirement [14][17]. The main criteria for design the CS matrix Φ is to enable the unique identification of some featured signal of image \mathbf{X} from its measurements $\mathbf{Y} = \Phi\mathbf{X}$. When considering K -sparse signals $\sum_K \mathbf{X}$, we should have $M > K$ for the number of measurements. Here, the sparsity level K is given by the coherence $K = O(\sqrt{M})$, and the matrix Φ should have its columns corresponding to the indices in signal support $\Lambda = \text{supp}(X)$.

As suggested in [26], we first check the properties of Φ to ensure that different measurement vectors $\Phi_{n_1 \times n_2} X_i \neq \Phi_{n_1 \times n_2} X_{i-1}$ are produced by distinct sub-image signals $X_i, X_{i-1} \in K$. This means that each vector $Y_{k_1}^i \in \mathbb{R}^{K_1}$ and $Y_{k_2}^i \in \mathbb{R}^{K_2}$ is to be matched to no more than one vector $X_i \in \sum_K X$ when we have $\mathbf{Y} = \Phi\mathbf{X}$. These prior properties for the CS matrix actually help to guarantee the uniqueness of the obtained error-free measurement vector \mathbf{Y} . This is quite important for secure communications [27].

2.3. Extraction of the Hidden Signal

After subsampling the test image X into four sub-images X_1, X_2, X_3, X_4 and applying the DCT or DWT onto the selected two sub-images, we can obtain the transformation coefficients matrix $X_i(n_1, n_2), i = 1,2,3,4; k_1, k_2 = 1,2, \dots, INT[N/2]$. The hidden signal can be extracted as follows.

- 1) Turn X_i into a sparse representation \bar{X}_i by using a sparse base Ψ_i , i.e. $\bar{X}_i = \Psi_i X_i$;
- 2) Sort the sparse vector \bar{X}_i in descending order according to its signal support $\Lambda = \text{supp}(X)$, where the first 1500 coefficients are selected for compressive sensing;
- 3) Let the extracted bit from the secret message be w , which can be determined in Eq. (5) below.

$$w = \begin{cases} 1 & \text{if } T_{D_1} < |\bar{X}_i^{(k_1)} - \bar{X}_i^{(k_2)}| < T_{D_2} \\ 0 & \text{if } |\bar{X}_i^{(k_1)} - \bar{X}_i^{(k_2)}| < T_{D_1} \\ NULL & \text{otherwise} \end{cases} \quad (5)$$

where w has a value of 0 or 1, and T_{D_1} and T_{D_2} are two thresholds for data extraction. In our framework, the two thresholds are calculated using the SSIM algorithm [17] between two successive residual reconstructed sub-images.

2.4. Recovery of the Secret Signal in the CS Domain

Assume the size of the hidden message W is s , i.e. $W = [w_1, w_2, \dots, w_s]$, $w_s \in \{0, 1\}$. By repeating the aforementioned detection process in Eq. (5), the embedded security message W can be extracted bit by bit. Herein a L_2 penalty is applied on the norm of w for predicting the hidden message of a stego-image, where the secret bit w is estimated by:

$$w_s = \arg \min_w \|\bar{Y}_l - \Phi_{n_1 \times n_2} H_l w\|_2^2 + \lambda \|w\|_2^2 \quad (6)$$

where H_l is the hypothesis matrix from an initial reconstruction \bar{X}_l of the cover image X_l using BCS-SPL in [14], w is the extracted secret data bit from Eq. (5), and Γ is known as the Tikhonov matrix for prediction as initially proposed in [18]. The term Γ allows the imposition of prior knowledge to our approach, and the parameter λ controls the regularization.

In the proposed approach, less weight is assigned to the hypotheses which are most dissimilar from the sub-image blocks than those from similar ones. Specifically, we propose a diagonal Γ by

$$\Gamma_{jj} = \|\bar{Y}_l - \Phi_{n_1 \times n_2} H_{j,i}\|_2^2 \quad (7)$$

where $H_{j,i}$ is the columns of H_l , $j=1, 2, \dots, k$.

For each block, w_s can be calculated directly by the closed form solution,

$$w_s = ((\Phi_{n_1 \times n_2} H_{j,i})^T (\Phi_{n_1 \times n_2} H_{j,i}) + \lambda^2 \Gamma)^{-1} (\Phi_{n_1 \times n_2} H_{j,i})^T \bar{Y}_l \quad (8)$$

The calculated residual after the projection will become:

$$R = \|\bar{Y}_{k_2}^i - \bar{Y}_{k_1}^i\|_2 \quad (9)$$

which means that R should be a condition of iteration end in formula (8) when recovering the secure signal of hidden images.

3. Experiment Results and Analysis

3.1 Datasets

In our experiments, image sources are BOSS 2, UCID, DI101 and HYBRID image databases respectively, where the HYBRID database contains images from all three databases above. We have prepared these image databases with varying image patterns of 2000 jpeg images with resolution ranging from 800×600 and 1024×768. All the images were resized to 640×480 and converted to grey scale. Each cover image is embedded with varying message capacities to generate 2000 stego images using five popular embedding algorithms F5 [19], PQ [20], Outguess [21], JPHS [21], and HUGO [22]. The embedding rates are 0.15 bpp-0.25 bpp (bit per pixel) respectively.

Feature vector of 274 DCT features and 72 wavelet coefficient features are extracted from all covers and stego images by measurement samples of $B \times B$ dense Gaussian matrix in [14], and with $B=32, 16$ respectively. Total generated 32000(4000×4×2) images.

For experiment I, we have selected 1200 original cover images and 1200 equivalent stego images for training dataset, creating a dataset of 2400 images for 4 embedding algorithms and 2 sets of feature vectors (2400×4×2=19200). The remaining 800 images are used to generate a test dataset of total

1600×4×2=12800 images with different embedding capacities that used to evaluate the performance of the generalized model which generated by training dataset.

In the next three sub-sections, we design separate experiments to evaluate the performance of the proposed approach in terms of the detection accuracy of the hidden signal, the effectiveness of the extracted features and the quality of the recovered secret signals, respectively. Both qualitative and quantitative criteria are used for subjective and objective assessment. Relevant results are summarized in detail as follows.

3.2. Comparison of the Detection Accuracy

We compare our proposed method with the following three steganalytic algorithms:

(1) Optimized feature extraction for steganalysis (OCF). In [23], Wang et al. extracted both PDF and moment features from wavelet and prediction error subbands. Also demonstrated this algorithm was superior to the previous detectors. Contrary to the original features, we extracted 104-dimensional (104D) features in experiment I.

(2) Textural features based universal steganalysis [local linear transform probability density function (LLTPDF)]. In [24], Li et al. extracted a 110-dimensional (110D) textural feature set from the PDFs of the LLT coefficients for universal steganalysis. Compared with the state-of-the-art steganalytic feature sets, it has proved that the LLTPDF performed best in most situations.

(3) Steganalysis by subtractive pixel adjacency matrix (SPAM). In [1], Penvy et al. extracted a 686-dimensional (686D) feature set from the second-order subtractive pixel adjacency model with a different threshold $T=3$, and demonstrated that it outperformed the previous detectors.

Furthermore, the area under the receiver operating characteristic curve (ROC) is used to evaluate the steganalyzer performance. A ROC curve displays the true positive probability P_{TP} (the fraction of the stego images that are classified correctly) in terms of the false positive probability P_{FP} (the fraction of the cover images that are misclassified as stegoimages).

We apply the area under the ROC curve (AUC) to measure the overall goodness of the ROC curve, which is calculated by the formula:

$$AUC = \int_0^1 P_{TP}(P_{FP})dP_{FP} \quad (10)$$

The value of AUC equals to 1 [$P_{TP}(P_{FP}) = 1$] for any $P_{TP} \in [0,1]$ represents perfect detection; $AUC = 0.5[P_{TP}(P_{FP}) = P_{FP}]$ corresponding to random guessing has the worst ROC curve.

Figure 3 shows all AUCs of the steganalyzers using our proposed CS algorithm, OCF, LLTPDF, SPAM features calculated on four databases with five steganographys. In all cases, the steganalyzers employing our proposed CS features (subrate of BCS $S=2$) performed the best, which demonstrates that our proposed CS steganalyzers improve the detection accuracy among the low embedding rate scenario, such as the 0.25 bpp. In addition, the image data of DI101 and BOWS2 come from the natural images showed better detection performance than UCID, which validates again that our presented CS features satisfy with the characteristic of the real images.

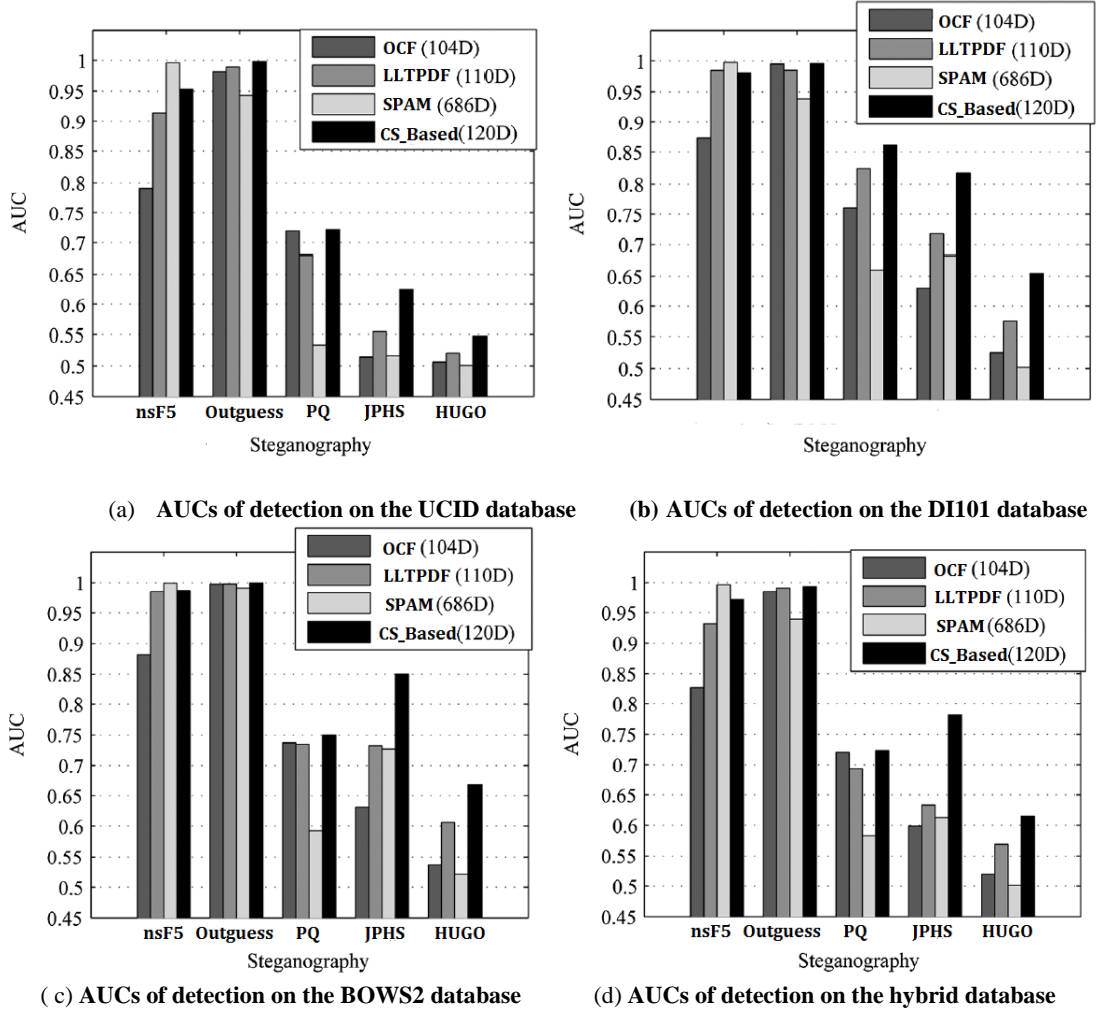


Figure 3. AUCs of steganalyzers using proposed CS algorithm (subrate $S=2$), OCF, LLTPDF, SPAM features calculated on four databases and five steganographies with 0.25 bpp embedding, respectively.

3.3. Comparison of the Extracted Features

To contrast the impact of features numbers for the steganalyzers conveniently, we extract 2000 stego images using F5, PQ, Outguess, and JPHS embedding algorithms with 0.15 bpp embedding rate, respectively. Meanwhile, we use the support vector machine (SVM) to train all features to derive the best fitness function as it has demonstrated good performance in various applications [28][33]. Figure 4 shows two statistical results of average feature extracted from four image databases in CS-DCT domain [38] and CS-SVM domain, respectively. Then we have applied our improved nature inspired CS algorithm and compared with optimized DPSO algorithm. The number of iterations for each algorithm is 35 and population size is 30. In this case, the thresholds are $T_{D_1} = 1$, and $T_{D_2} = 3$, respectively.

3.3.1. DCT Features Description

In Figure 4(a), a feature set comprising of 193 features derived from DCT coefficients and 81 features derived from Markov model of DCT plane could achieve good performance independently with certain limitations. To overcome the limitation of single feature set method, such as biased detection for different embedding algorithms, the DCT and Markov features were merged to produce a 274-dimensional feature vector.

3.3.2. DWT Features Description

The proposed scheme extracted 72-dimension feature set from three level quadrature mirror filter wavelet coefficients in Figure 4(b). Four statistical moments: mean, variance, kurtosis and skewness are extracted from wavelet coefficient of each nine high-frequency subbands, generating 36 features. Another set of 36 features are extracted from predicted errors of nine high frequency subbands, and finally form 72- dimensional feature vector for steganalysis. In all these algorithms, fitness function is obtained by training the selected features with SVM [3] Gaussian kernel and averaging the accuracy by 10-cross validation. Figure 4 reveals that the proposed CS algorithm reduces the DCT features by almost 67% and DWT by 38% in Figure 4 (a) and Figure 4(b), respectively. The reason a higher percentage of DCT features is reduced is due to the fact that DCT features contain more redundancy than DWT features.

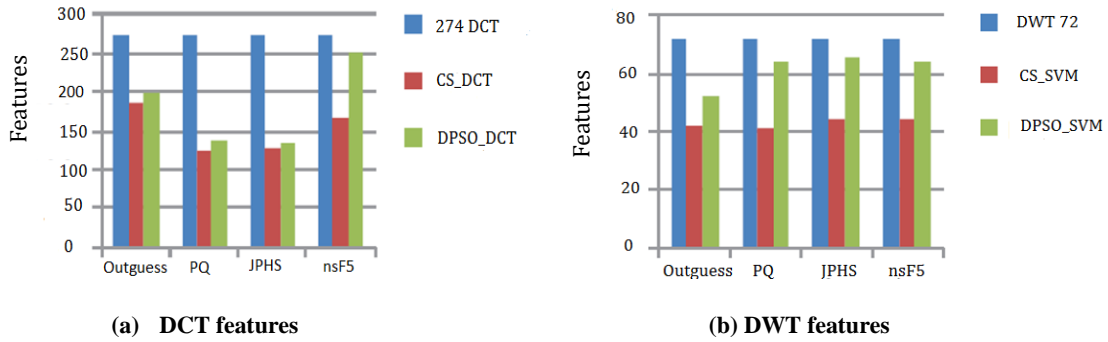


Figure 4. CS-based features for different steganography algorithms with 0.15 bpp embedding rate.

3.4 Quality of the Recovered Secret Signal

In our approach, we tried to find a CS-based criterion for secret signal recovery with extracted features from stego images. A final experiment is performed by combining four steganographic algorithms and applying the most effective features sensed by BCS measurement matrix, and recovering hidden signals by multi-hypothesis predictions with a Tikhonov regularization in the CS domain [18] [29]. The original signals that are hidden in cover images are 2-D grey fingerprint images with a size of 128×128 from the FVC2004 database (DB3) [25]. Figure 5 shows the reconstructed fingerprint images with 40 features using different algorithms. We can observe that reconstructed fingerprint images from nsF5 can achieve the best, closest to the original signal with 40 features were detected by BCS as compared to other embedding algorithms, and JPHS is the weakest among embedding algorithms.

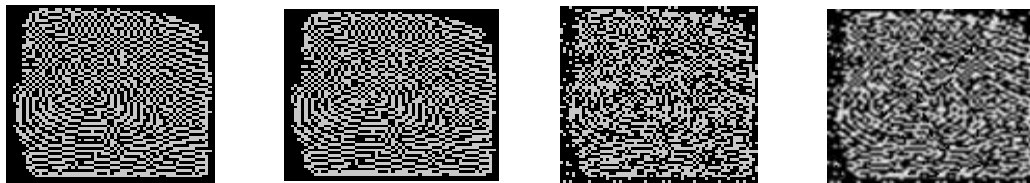


Figure 5. CS-based reconstructed fingerprint images with 40 features.

All above experiment results demonstrate that the following three goals are achieved: a) proposed CS-based algorithm increases detection accuracy; b) the algorithm reduces the number of features to be trained by SVM classifier; c) the algorithm can efficiently recover the secret signal with fewer features

extracted from stego image.

4. Conclusion

We have addressed an efficient recovery method of secret signal for image steganalysis in this paper. Various statistical features from DCT, DWT, and CS domain have been developed from the stego image and used to investigate secret signal recovery algorithms combining multi-hypothesis prediction with Tikhonov regularization. The experiments are performed in five advanced embedding algorithms nsF5, Outguess, PQ, JPHS and HUGO. Extensive experiments show that proposed CS-based algorithm improves the detection accuracy by 5-10% and reduces the features set dimensionality by almost 67% for DCT features and 37.5% for DWT features, and efficiently recover the secret signal with fewer features extracted from stego image.

For future work, efficient processing can be applied including gradient-based subspace feature extraction [31] and saliency detection [34]. Image enhancement to ensure the quality of the recovered signal can also be applied [32][36]. In addition, more state-of-the-art optimization algorithms will be explored to search the best fitness function such as gravitational search algorithm [35] and deep learning [37] in this context.

Acknowledgment

This work was partly supported by the National Natural Science Foundation of China (61672008, 61772144), Guangdong Provincial Application-oriented Technical Research and Development Special fund project (2016B010127006, 2017A050501039), the Natural Science Foundation of Guangdong Province (2016A030311013, 2015A030313672), International Scientific and Technological Cooperation Projects of Education Department of Guangdong Province (2015KGGHZ021), and the Scientific and Technological Projects of Guangdong Province (2017A050501039).

References

- [1] Pevný T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security* 5(2): 215–224
- [2] Fridrich J, Kodovsky J (2012) Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security* 7(3): 868–882
- [3] Shi YQ, Sutthiwan P, Chen L (2012) Textural features for steganalysis. In *Proc. Int. Workshop on Information Hiding*, pp.63–77
- [4] Holub V, Fridrich J, Denmark T (2013) Random projections of residuals as an alternative to cooccurrences in steganalysis. In *Proc. SPIE Electronic Imaging 8665: 0L01–0L11*
- [5] Holub V, Fridrich J (2013) Random projections of residuals for digital image steganalysis. *IEEE Transactions on Information Forensics and Security* 8(12): 1996–2006
- [6] Li YB, Guo ZH (2016) Image Steganography in a Karhunen-Loeve Transform Optimization Model. *International Journal of Security and Its Applications* 10(5): 19-128
- [7] Kodovský J, Fridrich J (2008) On completeness of feature spaces in blind steganalysis. In *Proc. the 10th ACM Workshop on Multimedia and Security*, pages 123-132
- [8] Dong J, Chen X, Guo L, Tan T (2008) Fusion based blind image steganalysis by boosting feature selection. In: *LNCS 6387: 87-98*
- [9] Orsdemir A, Altun HO, Sharma G, Bocko MF (2008) On the security and robustness of encryption via compressed sensing. In *Proc. IEEE Military Communications Conference*, pages1040-1046

- [10] Davenport M, Boufounos P, Wakin M, Baraniuk R (2010) Signal processing with compressive measurements. *IEEE Journal of Selected Topics in Signal Processing* 4(2): 445-460
- [11] Lu W, Varna AL, Wu M (2010) Security analysis for privacy preserving search for multimedia. In *Proc. IEEE 17th Inter. Conf. on Image Processing*, pages 68-72
- [12] Wang Q, Zeng W, Tian J (2013) Integrated secure watermark detection and privacy preserving storage in the compressive sensing domain. In *Proc. IEEE Int. Workshop on Information Forensics and Security*, pages 67-72
- [13] Patsakis C, Aroukatos NG (2014) LSB an DCT steganographic detection using compressive sensing. *Journal of Information Hiding and Multimedia Signal Processing* 5(1): 20-32
- [14] Fowler JE, Mun S, Tramel EW (2011) Multiscale block compressed sensing with smoothed projected landweber reconstruction. In *Proc. 19th European Signal Processing Conf.*, pages 564-568
- [15] Donoho D (2006) Compressed sensing. *IEEE Trans. on Information Theory* 52(4): 1289–1306
- [16] Candes E, Tao DC (2006) Near optimal signal recovery from random projections: universal encoding strategies. *IEEE Trans. on Information Theory* 52(12): 5406–5425
- [17] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing* 13(4): 600-612
- [18] Sullivan GJ (1993) Multi-hypothesis motion compensation for low bit-rate video coding. In *Proc. Int. Conf. on Acoustics, Speech, and Signal Processing* 5: 437-440
- [19] Westfeld A (2001) High capacity despite better steganalysis (F5 – a steganographic algorithm). *Lecture Notes in Computer Science* 2137: 289–302
- [20] Fridrich J, Goljan M, Soukal D (2004) Perturbed quantization steganography with wet paper codes. In *Proc. ACM Multimedia Workshop*, pages 4-15
- [21] Steganography software tools, <http://members.tripod.com/steganography/stego/software.html> [Assessed on 12 Sept. 2017].
- [22] Pevný T, Filler T, Bas P (2010) Using high-dimensional image models to perform highly undetectable steganography. *LNCS* 6387: 161–177
- [23] Wang Y, Moulin P (2007) Optimized feature extraction for learning based image steganalysis. *IEEE Trans. Inf. Forens. Security* 2(1): 31–45
- [24] Li B, Huang JW, Shi YQ (2008) Textural features based universal steganalysis. In *Proc. SPIE* 6819
- [25] Fingerprint verification competition, <http://biometrics.cse.msu.edu/fvc2004db/index.html>. [Assessed on 25 August 2017].
- [26] Duarte MF, Eldar YC (2011) Structured compressed sensing: from theory to applications. *IEEE Trans. Signal Processing* 59(9): 4053-4085
- [27] Gao P, Ren J (2006) Analysis and realization of snort-based intrusion detection system. *Computer Application and Software* 23(8):134–135
- [28] Zabalza J et al (2014) Robust PCA micro-Doppler classification using SVM on embedded systems. *IEEE Trans Aerospace Electron Syst* 50(3):2304-2310
- [29] Zhou Y et al (2016) Hierarchical visual perception and two-dimensional compressive sensing for effective content-based color image retrieval. *Cogn Comput* 8(5):877–889
- [30] AlKhateeb JH et al (2008) Word-based handwritten Arabic scripts recognition using DCT features and neural network classifier. In *Proc. 5th Int. Multi. Conf. Systems, Signals and Devices*, pages 1-5
- [31] Ren J et al (2014) Gradient-based subspace phase correlation for fast and effective image alignment. *J Visual Commun Image Represent* 25(7):1558–1565
- [32] Gill K et al (2011) Quality-assured fingerprint image enhancement and extraction using hyperspectral imaging. In *Proc. IEEE Int. Conf. Imaging for Crime Detection and Prevention*

- [33] Qiao T et al (2017) Effective denoising and classification of hyperspectral images using curvelet transform and singular spectral analysis. *IEEE Trans. Geoscience and Remote Sensing* 55(1): 119-133
- [34] Yan YJ et al (2018) Unsupervised image saliency detection with gestalt-laws guided optimization and visual attention based refinement. *Pattern Recognition* 79(7): 65-78
- [35] Zhang AZ et al (2018) A dynamic neighbourhood learning-based gravitational search algorithm. *IEEE Transactions on Cybernetics* 48(1): 436-447
- [36] Ren J, Vlachos T (2007) Efficient detection of temporally impulsive dirt impairments in archived films. *Signal Processing* 87(3): 541-551
- [37] Wang Z et al (2018) A deep-learning based feature hybrid framework for spatiotemporal saliency detection inside videos. *Neurocomputing* 287: 68-83
- [38] Zhao HM et al (2017) Robust information hiding in low-resolution videos with quantization index modulation in DCT-CS domain. *Multimedia Tools and Applications*, in press, pages 1-21